



We're ready.  
Are you?

# *APIC-EM*

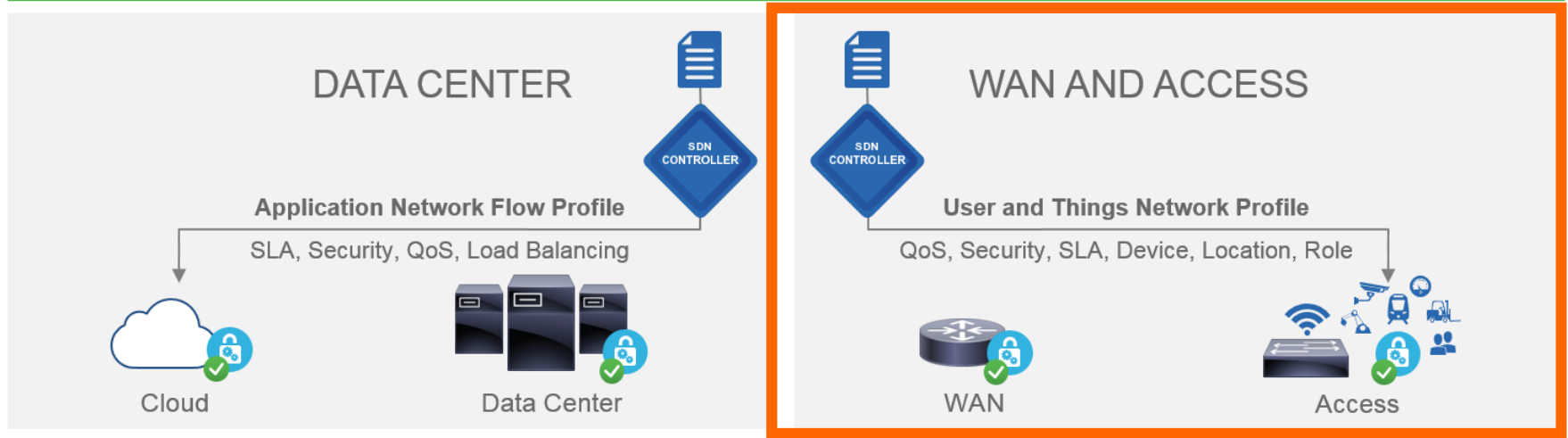
Adam Radford – Distinguished Systems Engineer

# Agenda

- Introduction
- Inventory/Topology
- Path Trace
- Plug and Play
- IWAN
- EasyQoS

# Common Policy Model from Branch to Data Center

## POLICY



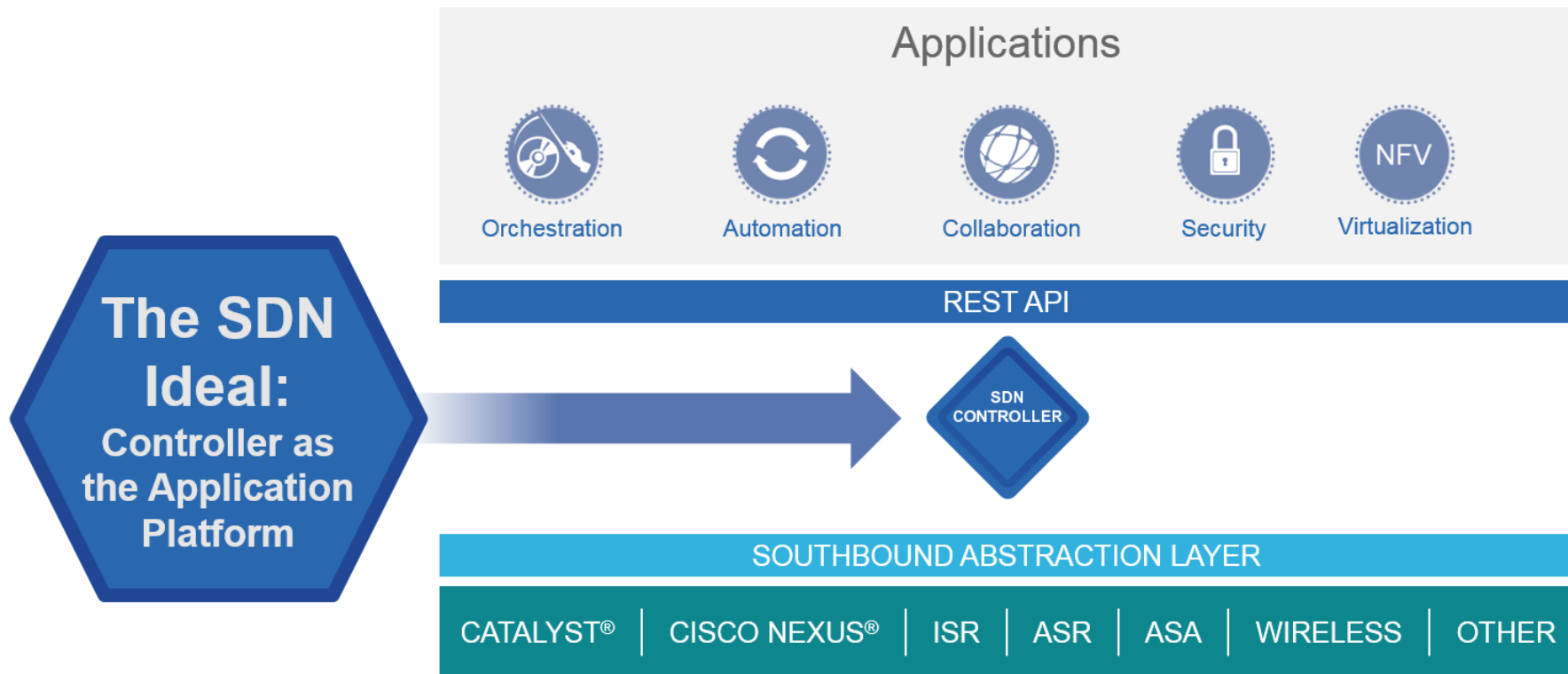
## CISCO® ADVANTAGE

BROWNFIELD AND  
GREENFIELD

END TO END

POLICY FRAMEWORK: FOCUS ON  
APPLICATION AND USER ENABLEMENT

# Network-Wide Abstractions Simplify the Network



# APIC-EM Controller Architecture



## Scalable Platform

Elastic service infrastructure and auto scale service model



## Highly Available

Maximum uptime for mission-critical applications and seamless upgrade



## Single Touch Point

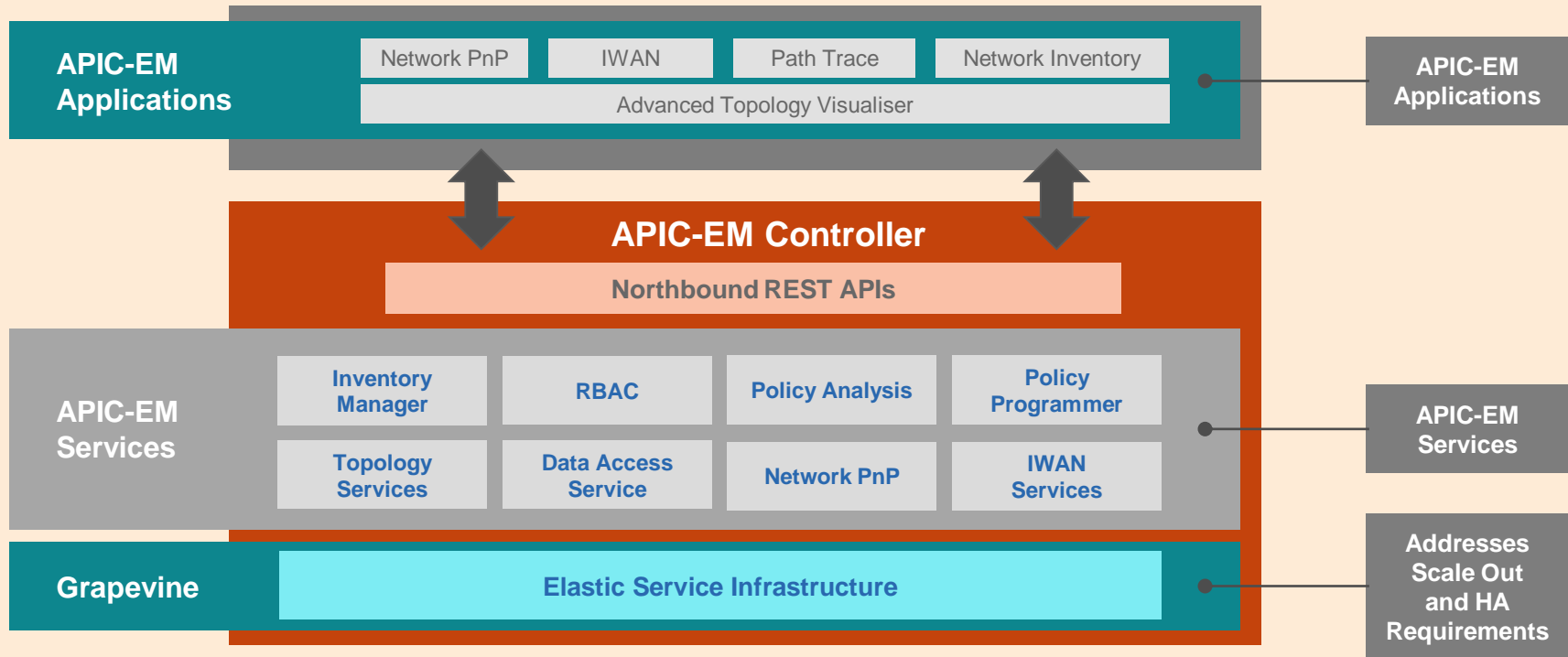
Fast and easy installation



## Northbound RESTful APIs

RBAC-enabled

# APIC-EM - Platform Architecture



# Manual to Systemic Policy Deployment

## Manual Policy Deployment

Admin  
Driven

### The What

*“Security Policy for  
Branches A-N”*

### The How

*“Change ACLs in  
the following  
elements”*

Cisco *live!*



## Controller Led Policy Deployment

### The What

*“Security Policy for  
Branches A-N”*

Admin  
Driven



### The How

*“Change ACLs in  
the following  
elements”*

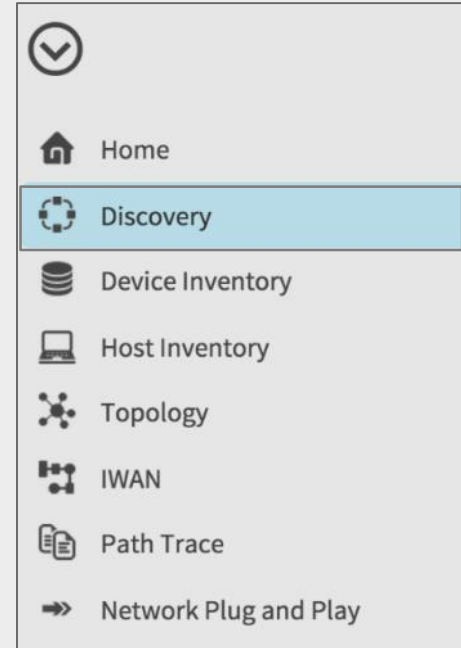
System  
Driven



# *Inventory/Topology*

# Controller Application - Network Discovery

- Quick, easy, and efficient network discovery functionality
- Flexible discovery options -
  - Based on CDP and IP address range
- Ability to start, stop, and delete the scan at anytime
- Auto-discovery of newly added network devices
- Ability to initiate a discovery job through the UI or northbound REST APIs



# Controller Application - Network Discovery

Home Discoveries Add New

**Discovery** No Scans to show. Fill out the form to the right and start your first scan!

Device Inventory

Host Inventory

Topology

IWAN

Path Trace

Network Plug and Play

Logs

### Discovery Name

Give this discovery a unique name

### IP Ranges

IPs of the devices you want to scan

Discovery Type **CDP**

### SNMP

Try different SNMP settings than global ones

> show SNMP settings

### CLI Credentials

Credentials are what you use to log in the devices.

> show CLI Credentials settings

### Advanced

Specify advanced settings

> show Advanced settings

**Start Discovery**

## Add a New Discovery

Use Discovery to scan and find devices in your network and place them in your inventory. When you run Discovery again, APIC-EM will scan the network and update your inventory with any new devices it finds.

### DISCOVERY TYPE

Choose from two types of scans: Cisco Discovery Protocol (**CDP**) or **Range** (range of IP addresses). For **CDP**, you enter a single IP address, which CDP uses to begin the process of obtaining information about other directly connected Cisco devices. For **Range**, you enter beginning and ending IP addresses that APIC-EM scans sequentially beginning with the first IP address and stopping with the ending IP address.

### CREDENTIALS

Enter the CLI Credentials used to log into the device. If an Enable Password is used for added security on the devices in your network, enter that password as well.

### SNMP

**SNMPv2c** uses a community-based form of security. The community of SNMP managers that are able to access the agent MIB is defined by an IP address access control list (ACL) and password.

**SNMPv3** uses authentication and encryption to ensure SNMP data packet integrity. It provides AuthPriv (authentication based on the HMAC-MD5 or HMAC-SHA algorithms), DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) and AES-128 standards, AuthNoPriv (authentication based on the HMAC-MD5 or HMAC-SHA algorithms), and NoAuthNoPriv (uses a username match for authentication).

# Network Discovery - Input Parameters

**Discovery Name**  
Give this discovery a unique name

**IP Ranges**  
IPs of the devices you want to scan  
Discovery Type: **CDP** (selected), Range

**SNMP**  
Try different SNMP settings than global ones  
[show SNMP settings](#)

**CLI Credentials**  
Credentials are what you use to log in the devices  
[show CLI Credentials settings](#)

**Advanced**  
Specify advanced settings  
[show Advanced settings](#)

Seed IP address for CDP-based network discovery

**Discovery Name**  
Give this discovery a unique name

**IP Ranges**  
IPs of the devices you want to scan  
Discovery Type: **Range** (selected), CDP

Entered ranges will appear here. Click 'Add' to add a range.

**SNMP**  
Try different SNMP settings than global ones  
[show SNMP settings](#)

**CLI Credentials**  
Credentials are what you use to log in the devices  
[show CLI Credentials settings](#)

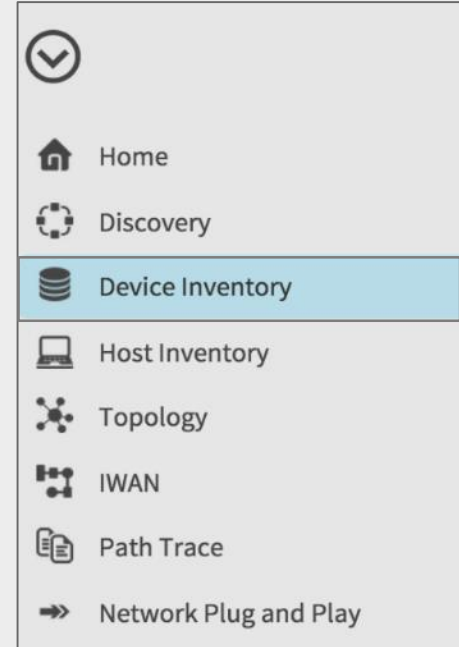
**Advanced**  
Specify advanced settings  
[show Advanced settings](#)

IP address range for discovery scope - Click on the Add icon to provide multiple IP address ranges

# Controller Applications - Device Inventory

## Single Source of Truth

- Real-time network device inventory and asset service management
- Includes all network devices with an abstraction for the entire network:
  - **Full knowledge** of network
  - Awareness of the overall **operational health** of the physical network
  - **Detailed inventory** information for easier consumption by controller services and applications
  - Allows applications to be device-agnostic
- Inventory service runs in the background to maintain an accurate database



# Controller Applications - Device Inventory

Device Name	IP Address	MAC Address	IOS/Firmware	Platform	Serial Number	Config	Device Role	Device Family
<a href="#">AP7081_059f.19ca</a>	55.1.1.3	68:bc:0c:63:4a:b0	8.1.14.16	AIR-CAP3502I-A-K9	FGL1548S2YF	<a href="#">View</a>	ACCESS	Unified AP
<a href="#">Branch-Access1</a>	207.1.10.1	64a0.e7d4.9bc1	12.2(55)SE3	WS-C2960S-48LPS-L	FOC1537W1ZY	<a href="#">View</a>	ACCESS	Switches and Hubs
<a href="#">Branch-Router1</a>	207.3.1.1	7c0e.ce9f.3cd9	15.2(4)M6a	CISCO2911/K9	FTX1840ALC1	<a href="#">View</a>	BORDER ROUTER	Routers
<a href="#">Branch-Router2</a>	207.3.1.2	107f.06bb.dc81	15.2(4)M6a	CISCO2911/K9	FTX1840ALBY	<a href="#">View</a>	BORDER ROUTER	Routers
<a href="#">CAMPUS-Access1</a>	212.1.10.1	1029.295c.30e2	03.03.00.SE	WS-C3850-48U	FOC1703V36B	<a href="#">View</a>	ACCESS	Switches and Hubs
<a href="#">CAMPUS-Core1</a>	211.1.1.1	24e9.b33f.b180	15.1(1)SY3	WS-C6503-E	FXS1825Q1PA	<a href="#">View</a>	CORE	Switches and Hubs
<a href="#">CAMPUS-Core2</a>	211.2.1.1	24e9.b33f.b1c0	15.1(1)SY3	WS-C6503-E	FXS1825Q1P8	<a href="#">View</a>	CORE	Switches and Hubs
<a href="#">CAMPUS-Dist1</a>	55.1.1.100	0007.7dc5.e7ff	03.02.00.XO	WS-C4507R+E	FOX1524GV2Z	<a href="#">View</a>	DISTRIBUTION	Switches and Hubs
<a href="#">CAMPUS-Dist2</a>	212.3.1.2	30e4.db25.753f	03.04.00.SG	WS-C4507R+E	FOX1525G5S1	<a href="#">View</a>	DISTRIBUTION	Switches and Hubs
<a href="#">CAMPUS-Router1</a>	210.1.1.1	144e.05cf.2e30	15.4(3)S	ISR4451-X/K9	FTX1842AHM2	<a href="#">View</a>	BORDER ROUTER	Routers

# Device Inventory - Hardware Layout

APIC - Enterprise Module

API [Settings] [User] [Notifications] admin [Settings]

Filters **Layout: Hardware**

Device Name	IP Address	MAC Address	IOS/Firmware	Platform	Serial Number	Config	Device Role	Device Family
<a href="#">AP7081.059f.19ca</a>	55.1.1.3	68:bc:0c:63:4a:b0	8.1.14.16	AIR-CAP3502I-A-K9	FGL1548S2YF	<a href="#">View</a>	ACCESS	Unified AP
<a href="#">Branch-Access1</a>	207.1.10.1	64a0.e7d4.9bc1	12.2(55)SE3	WS-C2960S-48LPS-L	FOC1537W1ZY	<a href="#">View</a>	ACCESS	Switches and Hubs
<a href="#">Branch-Router1</a>	207.3.1.1	7c0e.ce9f.3cd9	15.2(4)M6a	CISCO2911/K9	FTX1840ALC1	<a href="#">View</a>	BORDER ROUTER	Routers
<a href="#">Branch-Router2</a>	207.3.1.2	f07f.06bb.dc81	15.2(4)M6a	CISCO2911/K9	FTX1840ALBY	<a href="#">View</a>	BORDER ROUTER	Routers
<a href="#">CAMPUS-Access1</a>	212.1.10.1	f029.295c.30e2	03.03.00.SE	WS-C3850-48U	FOC1703V36B	<a href="#">View</a>	ACCESS	Switches and Hubs

Detailed device inventory information

# Device Inventory - Tagging Layout

Device Name	IP Address	MAC Address	Device Role	Location	Tag
AP7081_059f.19ca	55.1.1.3	68:bc:0c:63:4a:b0	ACCESS	San Jose, CA	3
Branch-Access1	207.1.10.1	64a0.e7d4.9bc1	ACCESS	New York, NY	1
Branch-Router1	207.3.1.1	7c0e.ee9f.3cd9	BORDER ROUTER	New York, NY	1
Branch-Router2	207.3.1.2	f07f.06bb.dc81	BORDER ROUTER	New York, NY	1
CAMPUS-Access1	212.1.10.1	f029.295c.30e2	ACCESS	San Jose, CA	3

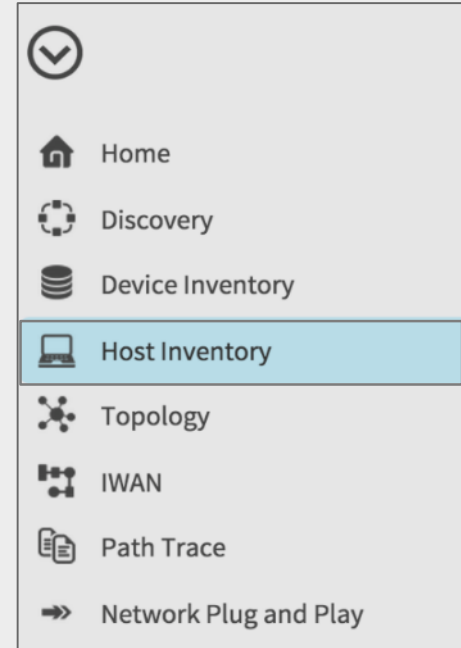
Sophisticated and automated devices are given a role assignment based on intelligent matching against pre-set templates and attributes

Geo-site (location) and custom tags for complete flexibility in grouping and classification of devices based on business logic (for example, lines of business, service mix, etc.)



# Controller Applications - Host Inventory

- Real-time network host and endpoint inventory (PCs, wireless devices, IP phones, printers, etc.)
- Detailed information about each host and endpoint:
  - Network attachment point for the host to the network device
  - Host name, IP, and MAC address information
- Host inventory service runs in the background to maintain the accuracy of the database:
  - Information collected through CDP, LLDP, and P device-tracking database lookup
  - SNMP traps are used to update the host inventory database (wireless host only for Release 1.0)



# Controller Applications - Host Inventory

Host MAC Address	Host IP Address	Host Type	Connected Network Device IP Address	Connected Interface Name	Host Name
30:e4:db:25:75:3f	212.1.20.2	WIRED	212.1.10.1	GigabitEthernet1/0/2	
5c:f9:dd:52:07:78	212.1.10.20	WIRED	212.1.10.1	GigabitEthernet1/0/47	
e8:9a:8f:7a:22:99	207.1.10.20	WIRED	207.1.10.1	GigabitEthernet1/0/47	

10 per page ▼ 3 Hosts < Previous 1 of 1 Next >

Detailed host information

Network attachment point for host

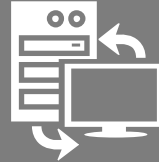
# Scale Numbers – General Availability



Network  
Devices:  
2000

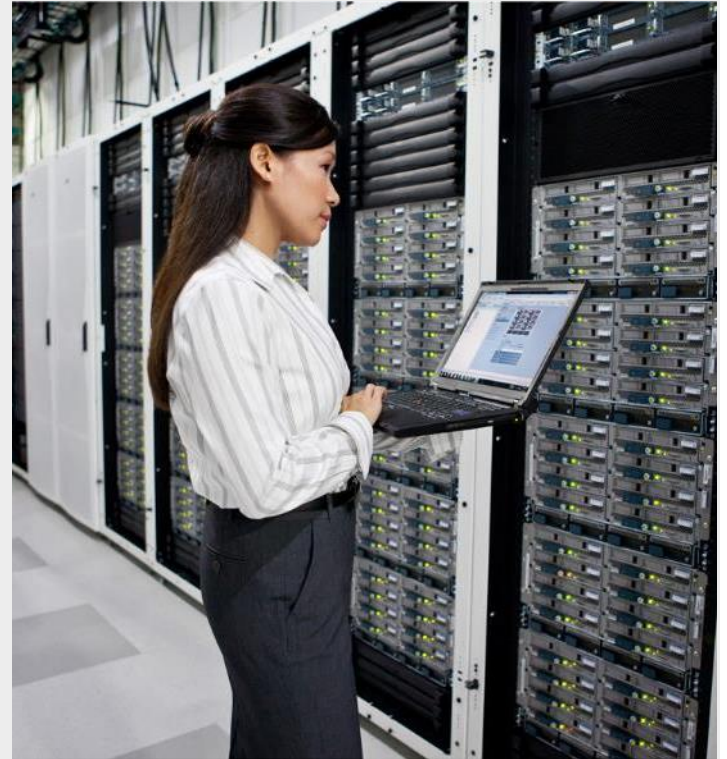


Access  
Points:  
2000



End  
Hosts:  
20,000

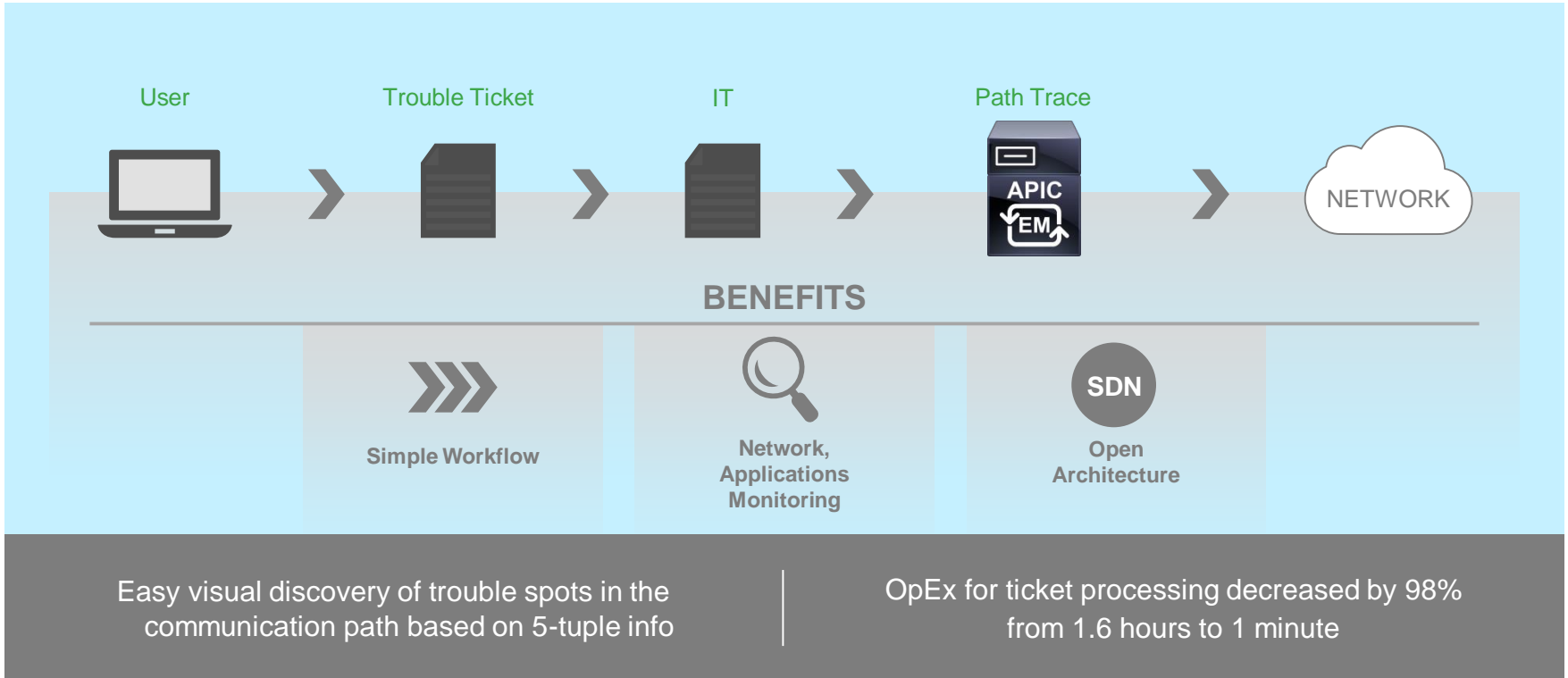
Note: These scale numbers are for the APIC-EM platform and the base applications. Some other APIC-EM applications might have different scale numbers.



# *Path Trace Application: Controller based Troubleshooting*

# APIC-EM Path Trace Application

## Accelerate Trouble-Ticket Processing



# Path Trace App: 5-Tuple Input Through User Interface

APIC - Enterprise Module

Path Trace

Enter in two host IP's (required) and their ports and protocol (optional) to visualize the path

Host Source IP: 65.1.1.6

Host Destination IP: 207.1.10.20

Source Port (Optional): 10101

Destination Port (Optional): 20101

Protocol (Optional): tcp

Trace

Trace Results

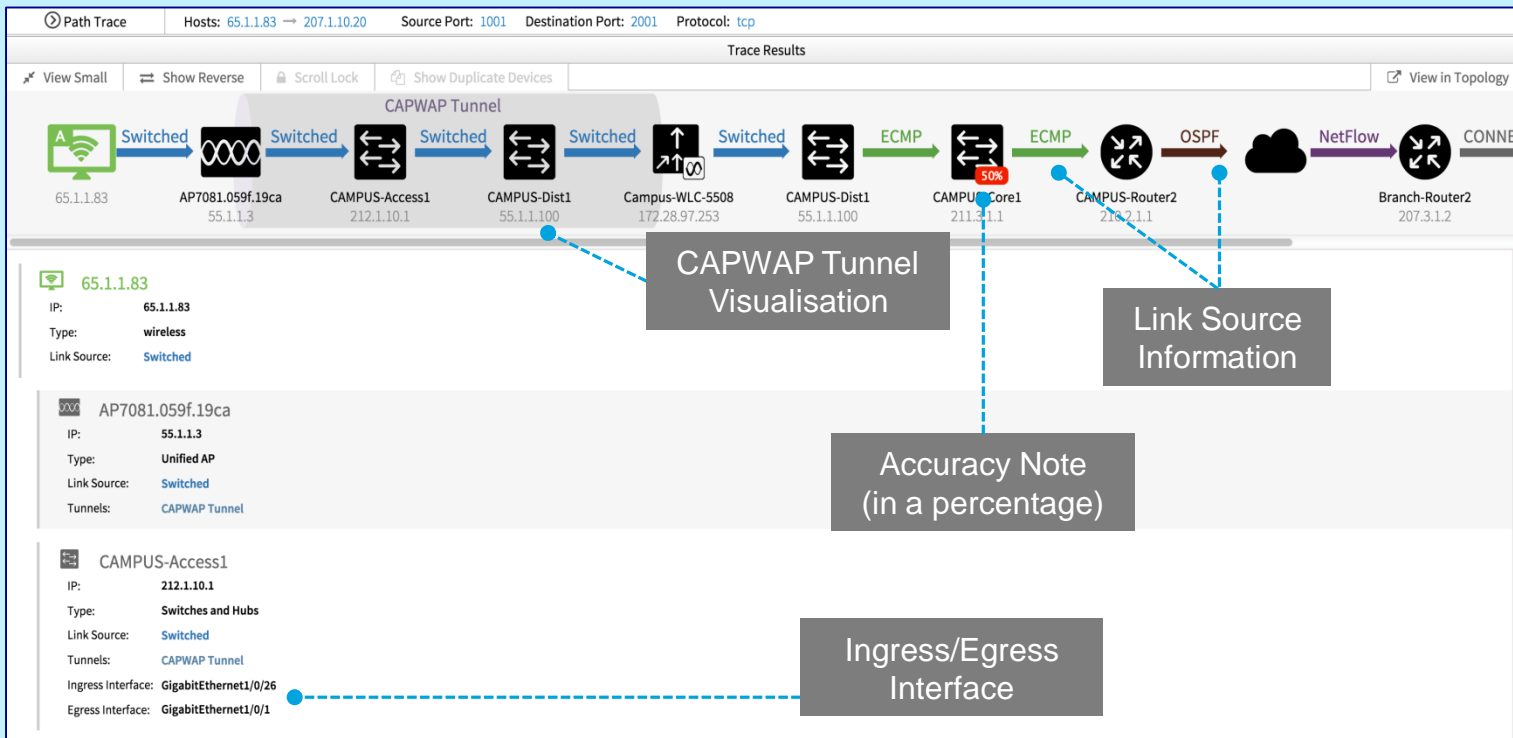
Please enter the fields above and press Trace to view a path.

**Required Information**  
SRC and DEST IP address  
[End host or L3 interface]

**Optional Information**  
SRC and DEST L4 port numbers;  
L4 protocol (TCP or UDP)

Note: Layer 4 port and protocol information is optional but highly recommended for accurate path calculation

# Path Trace App: Enhanced Application Flow Visibility

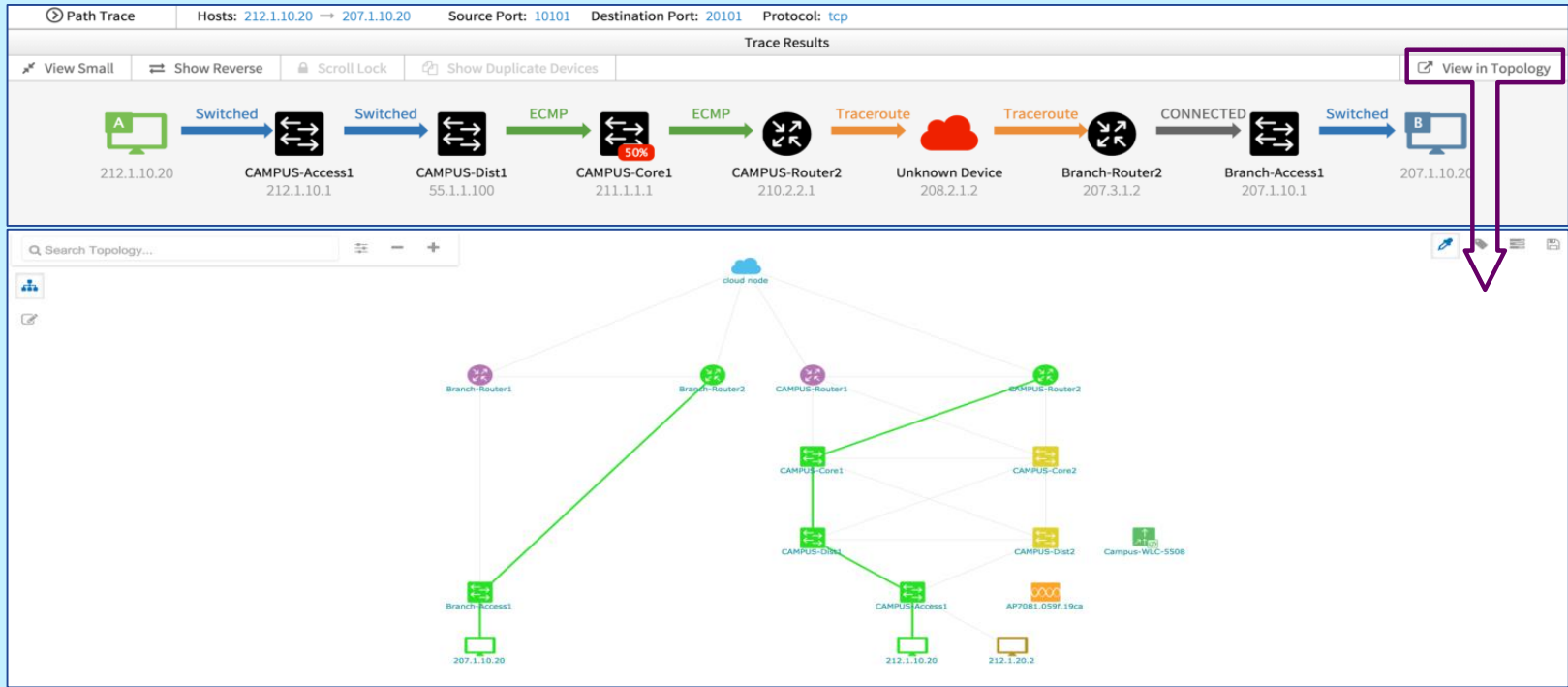


# Path Trace App: Detailed Device Information

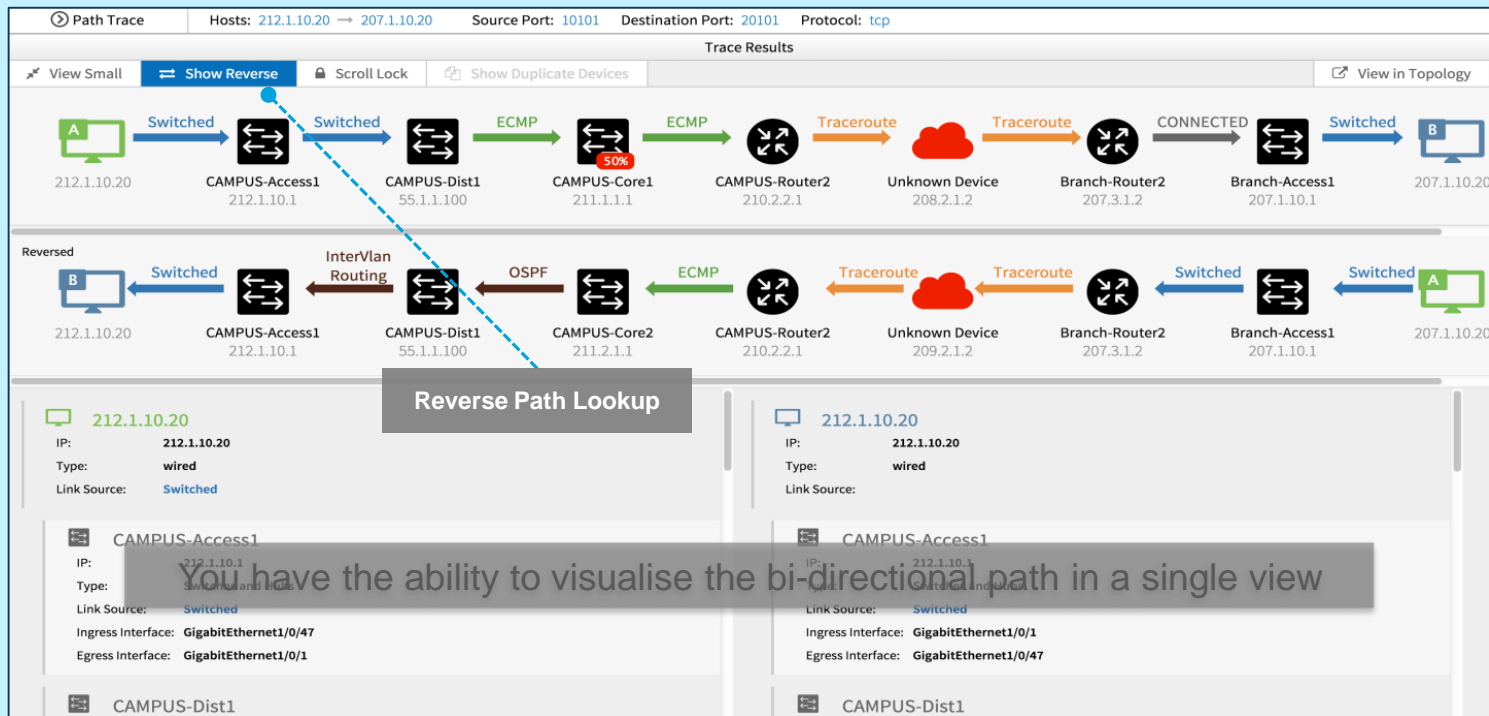
Device Information	Description
Device IP address	IP address of the network device or end host
Type	Type of network device or end host
Link information source	<p>For all the links along the application flow path trace, the link information source is displayed. Some examples for this particular field include:</p> <ul style="list-style-type: none"><li>▪ Routing protocols (OSPF, BGP etc.) - The link is based on the routing protocol table</li><li>▪ ECMP - The link is based upon a Cisco® Express Forwarding load-balancing decision</li><li>▪ NetFlow - The link is based upon NetFlow cache records collected on the device</li><li>▪ Static - The link is based on a static routing table</li><li>▪ Wired and wireless - The end host is a wired or wireless endpoint connected to the network device</li><li>▪ Switched - The link is based on Layer 2 VLAN forwarding information</li><li>▪ Traceroute - The link is based on information collected by the trace route app</li></ul>
Tunnels	<p>Relevant tunnel information is present along the application flow path trace. For APIC-EM Release 1.0, only CAPWAP and mobility tunnels are supported.</p> <p>Note: The Path Trace UI provides a visual graphic of the CAPWAP tunnel along the path trace</p>
Ingress interface	Ingress interface of the device for the application flow path trace (physical or virtual)
Egress interface	Egress interface of the device for the application flow path trace (physical or virtual)
Accuracy note	<p>If there is uncertainty about the path trace on a segment between devices, a note about the accuracy of the computed path on this segment will be displayed as a percentage. Click on the note to view suggestions of corrective actions to take to improve the path trace accuracy. The accuracy note is not displayed unless the APIC-EM is certain about the path.</p> <p>Example: If the APIC-EM is unable to obtain the exact egress interface for an ECMP scenario with two paths, the accuracy value would be calculated as 50%.</p>



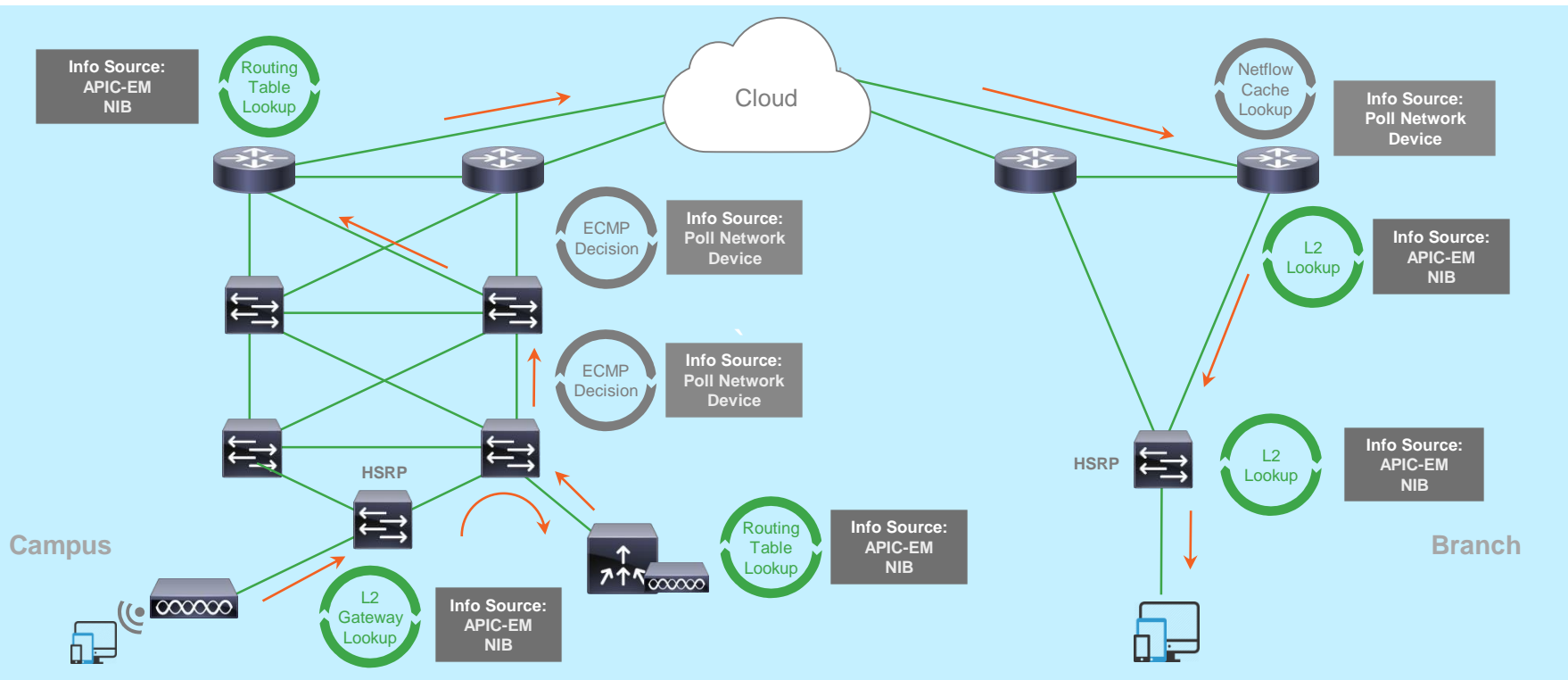
# Path Trace App: Topology View



# Path Trace App: Enhanced Application Flow Visibility



# Path Trace App: Path Trace Flow Diagram



# *Network Plug and Play: Controller based Deployment*

# 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

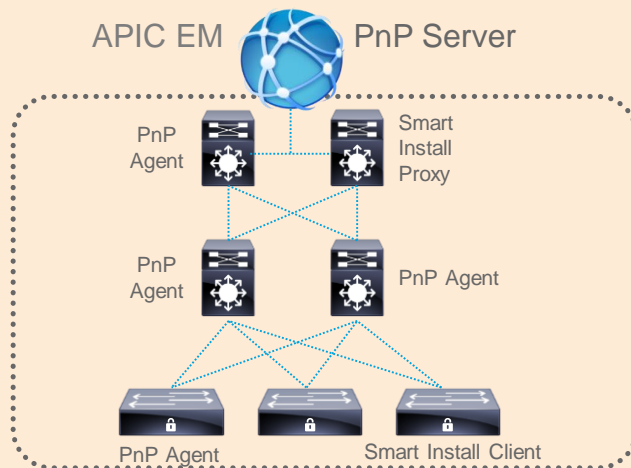
## Remote Installer

- 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

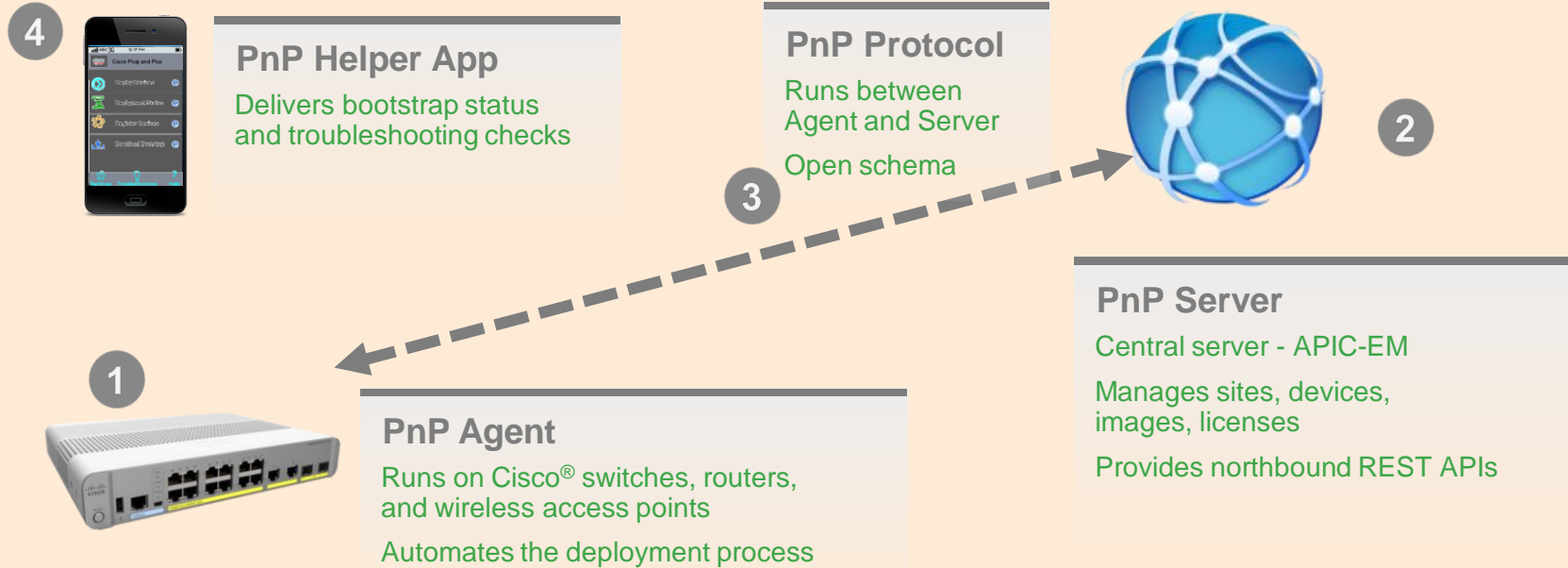
Consistent for Devices and Pin (Campus, Branch)

Highly Secure

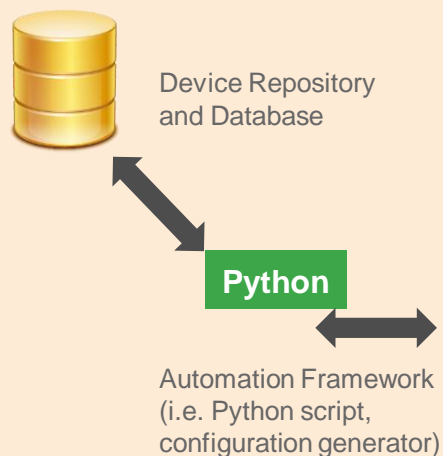
End to End

Greenfield and Brownfield

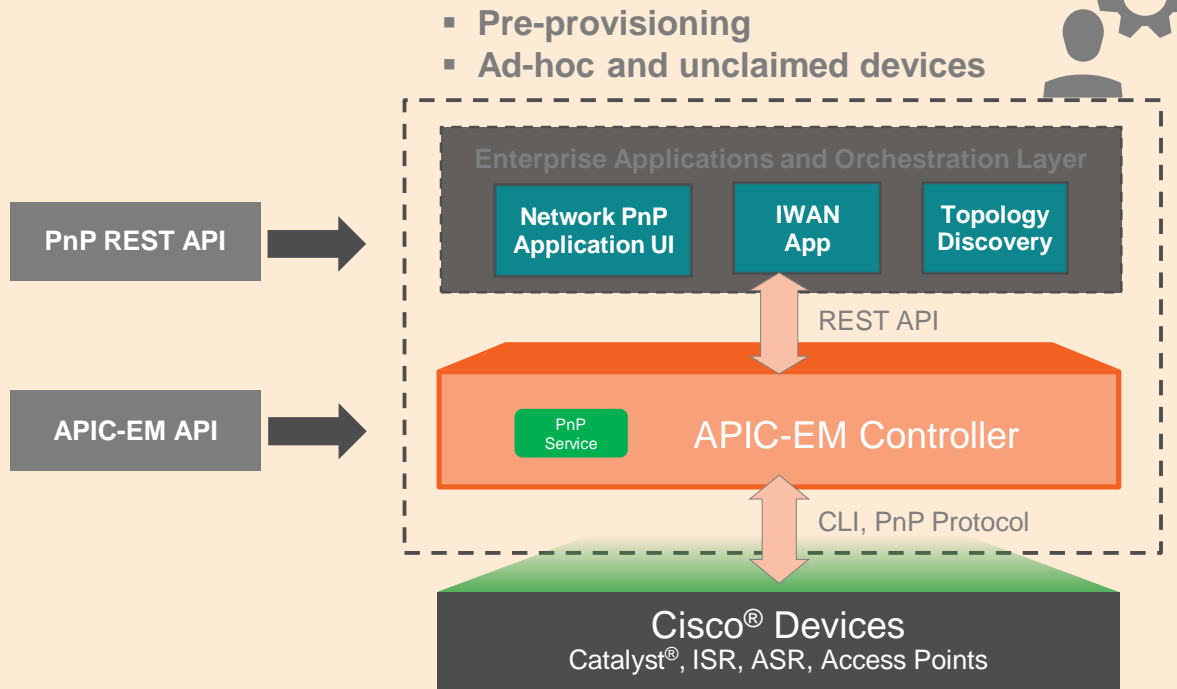
# Network Plug and Play - Components



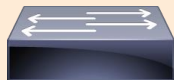
# Cisco APIC EM: PnP Server Workflow-Based and REST API



Customer's Existing Automation Framework



# 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;I172.19.45.222;J80

2

DNS  
Server

**DNS lookup**

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

3



**Cloud re-direction - roadmap (Q4CY2015)**

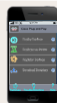
<https://devicehelper.cisco.com/device-helper> re-directs to 172.19.45.22 (PnP Server)

4



**USB-based bootstrapping**

5



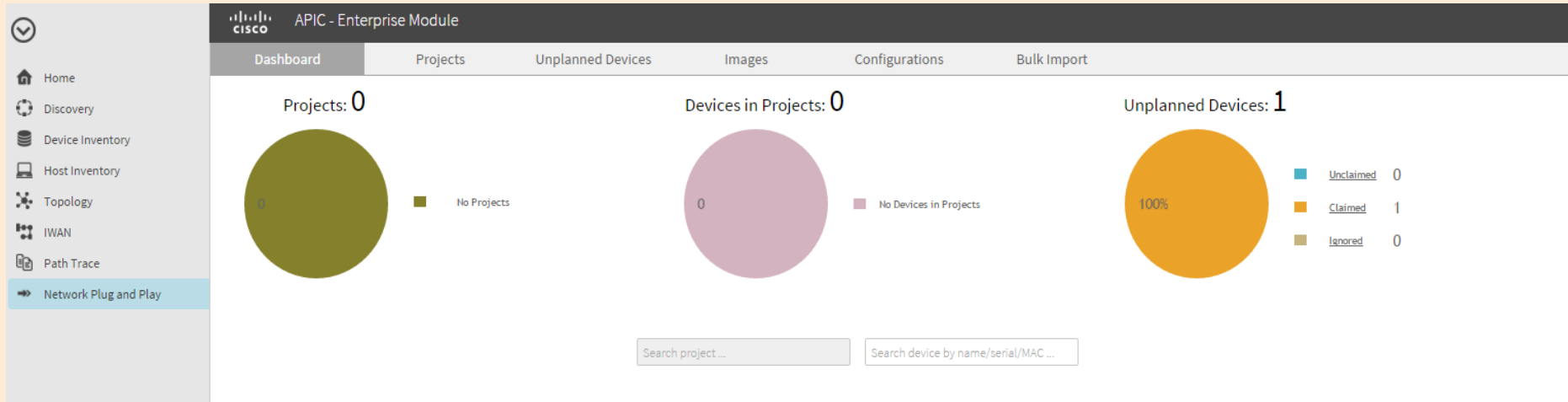
**Manual - using the Cisco® Installer App**

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





# APIC-EM PnP Login Screen





# 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

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

Name of device	Device type	Serial Number of device								
SRDL-SPOKE										

Device Name	Product ID	Serial Number/MAC Address	Config	Bootstrap	Image	Device Certificate	SUDI Required	Last Contact Time	Status
SRDL-SPOKE		ISR4331/K9	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>

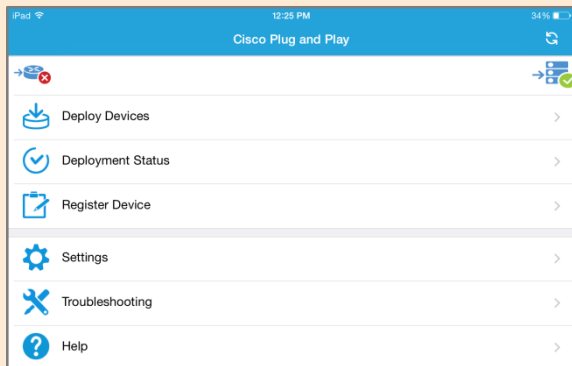
10

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

# Network PnP: Installer App



Apple

Android

## Redpark



RJ45 to  
Apple 8pin

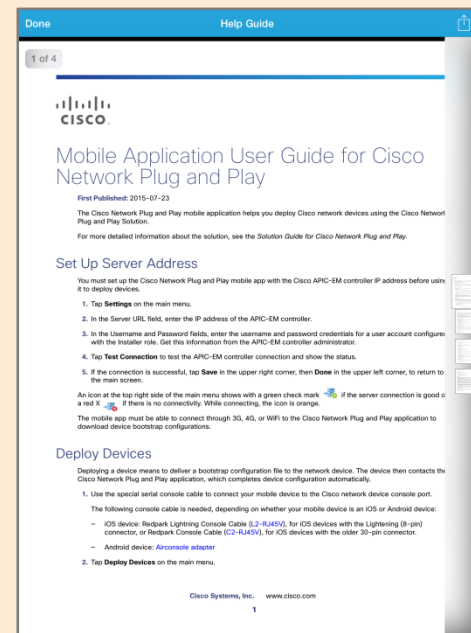


RJ45 to  
Apple 30pin

## Get Console

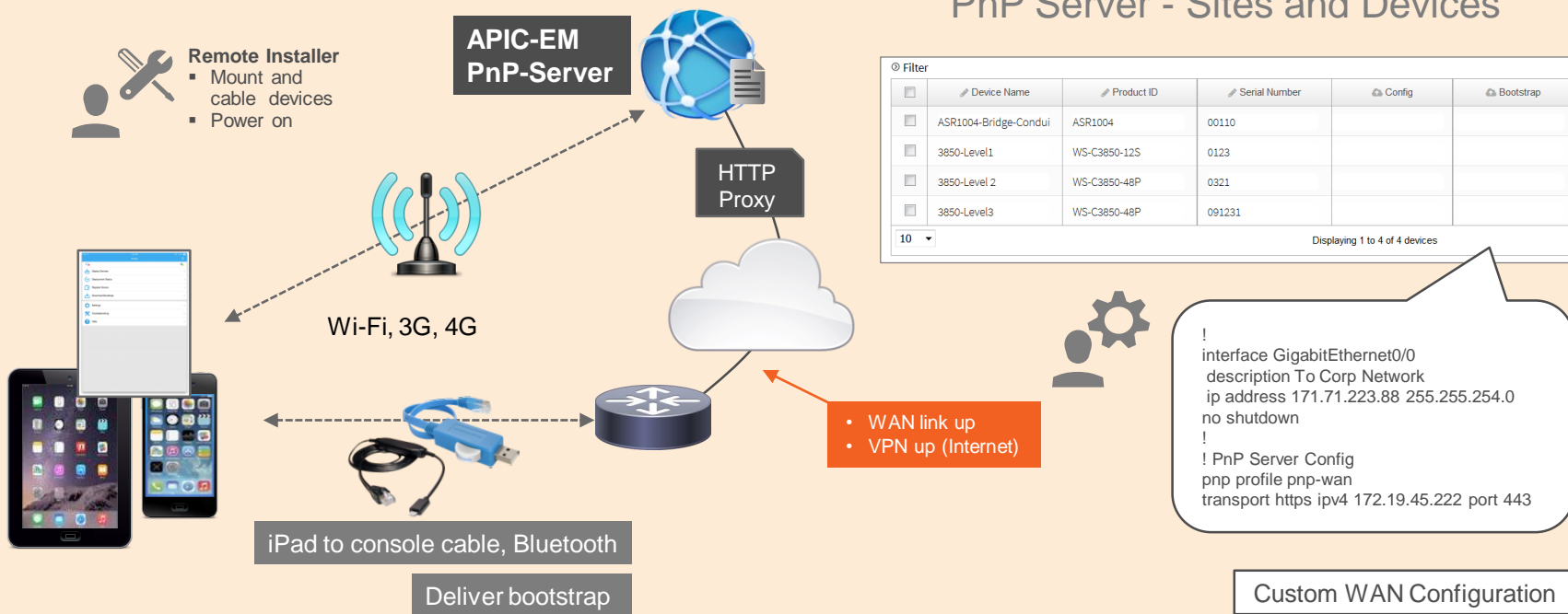


Airconsole 2.0  
Bluetooth Adapter



\* Tested with Network-PnP Solution

# Installer App - Workflow

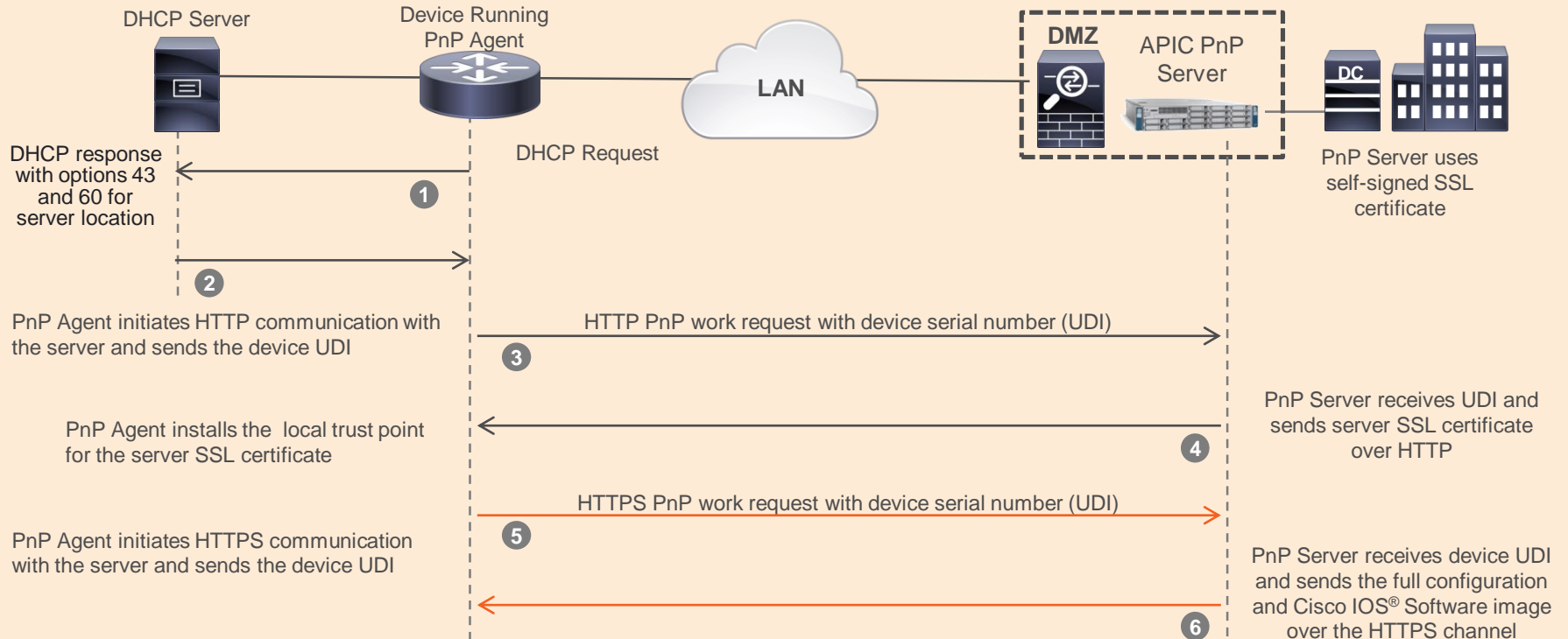


## PnP Server - Sites and Devices

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

# PnP Deployment for Campus - Self-Signed Certificate Method



# 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>Wave2 802.11ac &amp; Outdoor AP support (Roadmap)</p> <p>WLC Supported : AireOS and IOS-XE</p>	Nov2015

# *iWAN Application: Controller based Policy*

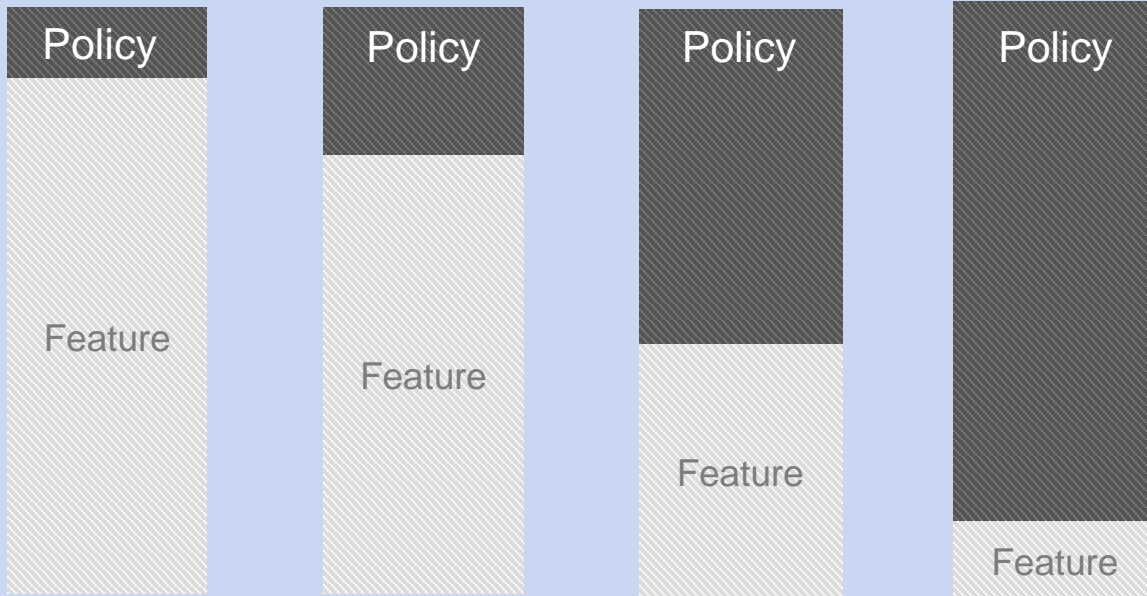
# Evolution to Policy Automation

## Policy-based Automation:

- Dynamic
- Business intent to network intent
- Executed by APIC-EM apps
- Prescriptive
- Business driven

## Feature-based Configuration:

- Static
- Focused on configuration
- Executed by Prime™ Infrastructure
- Customisable
- Expert-led



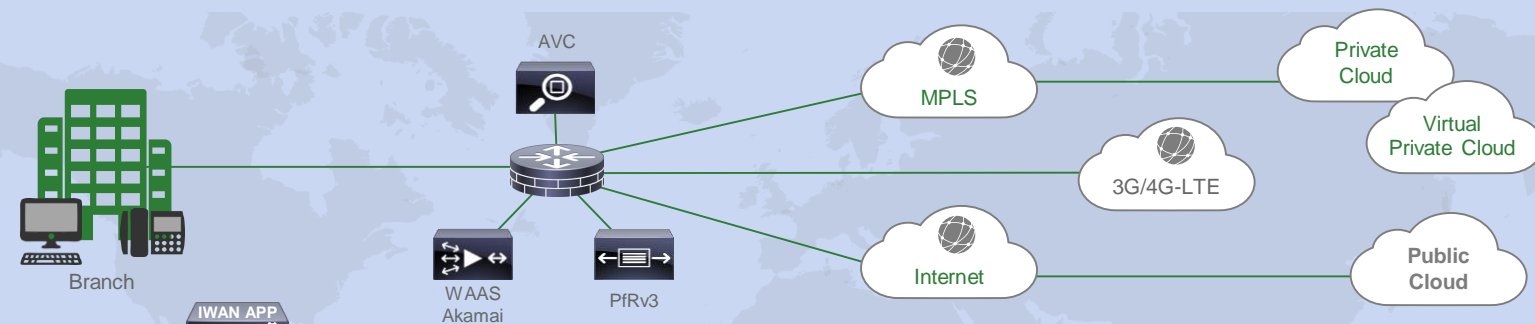
## Steady State:

- Cisco leads market adoption so that a large majority of enterprises adopt policy-based automation
- A small set of larger enterprises or MSPs will continue to use customisable feature configuration

Increasing Policy Coverage Through More Apps and Services



# Intelligent WAN (IWAN) Solution Components



## Management and Orchestration



### Transport Independence

- ▶ IPsec WAN overlay
- ▶ Consistent operational model

**DMVPN, PKI**



### Intelligent Path Control

- ▶ Optimal application routing
- ▶ Efficient use of bandwidth

**Performance Routing (PfR) QoS**



### Application Optimisation

- ▶ Performance monitoring
- ▶ Optimisation and caching

**AVC, WAAS, Akamai**



### Secure Connectivity

- ▶ NG strong encryption
- ▶ Threat defence

**Suite-B, CWS, ZBFW**

## Greenfield for Cisco® 4000 ISRs

### Branch

4000 ISR



## IWAN Transport

MPLS

Internet

## Data Centre – Cisco ASR 1000

### Data Centre

DMZ

DMVPN HUB  
ASR 1000

HTTP/HTTPS  
Proxy for PnP

Master  
Controller  
ASR 1000

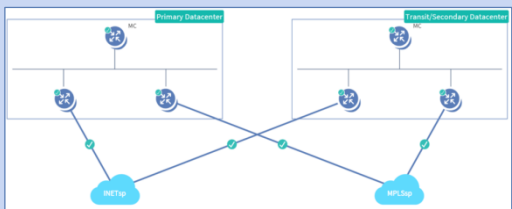
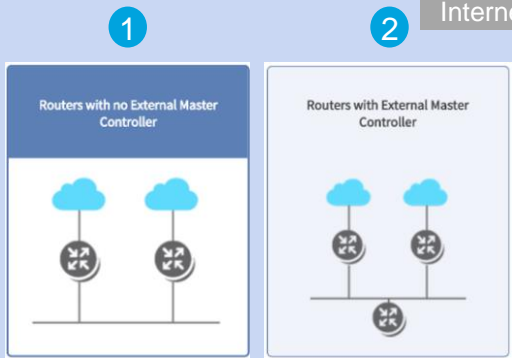


# Possible Architectures – General Availability

SP links can be:  
Internet + MPLS  
Internet + Internet

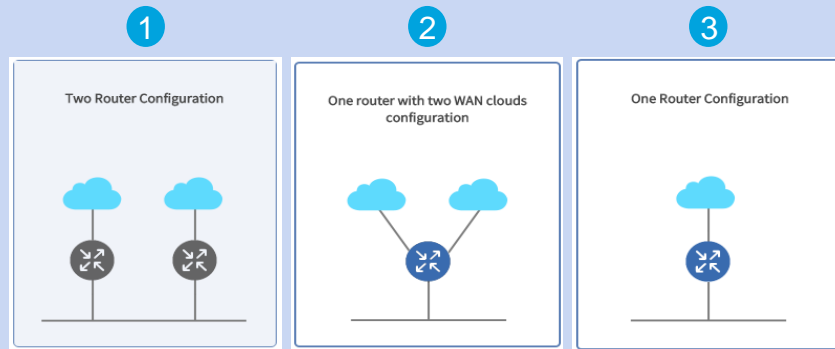
## Data Centre

1. For a lab or POC, MC can run in one of the DMVPN hubs
2. Single data centre with a separate MC
3. Dual data centre with primary and transit



## Branch

1. Dual router dual links
2. Single router dual links
3. Single router single links



APIC - Enterprise Module

API 3.3 admin


### Application Policy

#### Categorize Applications

voice-and-video	35
consumer-streaming	20
business-and-product...	18
file-sharing	11
consumer-file-sharin...	10

Top 5 Application Categories

#### Define Application Policy



Business Critical Scavenger Default

Apply Changes

**Add Application**

Applications can be dragged and dropped to other categories; By default not all the applications are shown. Not all Categories are shown by default, [Show](#) hidden categories.

backup-and-storage	0	browsing
consumer-internet	10	consumer-messaging
email	9	epayment
instant-messaging	7	other
voice-and-video	35	

#### Add Application

**Name** My-Custom-App1

**Type**  URL  Server IP/Port  DSCP

**Protocol**  UDP  TCP

**Value** 172.16.3.2 : 5500

**Similar to App** sip-tls

**Category** voice-and-video

**Jitter(ms)** 1

**Packet loss(%)** 5

**Delay(ms)** 100

Page loaded in 296ms

I wish this page would..

Categorise applications  
Add custom applications

APIC - Enterprise Module


Application Policy

Categorize Applications

Category	Count
voice-and-video	35
consumer-streaming	20
business-and-product...	18
file-sharing	11
consumer-file-sharin...	10

Top 5 Application Categories

Define Application Policy



Business Critical Scavenger Default

Apply Changes

Add Application

Search Apps

Applications can be dragged and dropped to other categories; By default not all the applications are visible, you can make them visible [Teach me](#).  
Not all Categories are shown by default, [Show](#) hidden categories.

backup-and-storage	4	browsing	6	business-and-productivity-tools	18	consumer-file-sharing	10
consumer-internet	6	consumer-messaging	7	consumer-streaming	20	database	3
email	9	epayment	0	file-sharing	11	gaming	1
instant-messaging	7	other	10	social-networking	7	software-updates	9
voice-and-video	35						

Name

- yahoo-messenger-video ✖
- webex-app-sharing ✖
- ms-lync ✖

Drag and drop each application (one or more) from one business class to the other

APIC - Enterprise Module

API [Settings] [User: HI, admin]

### Application Policy

#### Categorize Applications

consumer_apps	48
voice-and-video...	28
business-and-pr...	18
other	17
file-sharing	12

Top 5 Application Categories

#### Define Application Policy

Business Critical | Scavenger | Default

Apply Changes

#### Business Critical

- business-and-prod... mpls
- email mpls
- software-updates mpls
- voice-and-video mpls
- database mpls
- file-sharing mpls
- browsing mpls
- backup-and-storage mpls

#### Scavenger

- gaming No App Performance
- consumer\_apps No App Performance
- instant-messaging No App Performance
- social-networking No App Performance

Application Performance

No path preference

Path Preference

Path 1 inet

Path 2 mpls

Save Drop

#### Default

- other No App Performance

Drag and Drop a business category among: business critical | scavenger | default

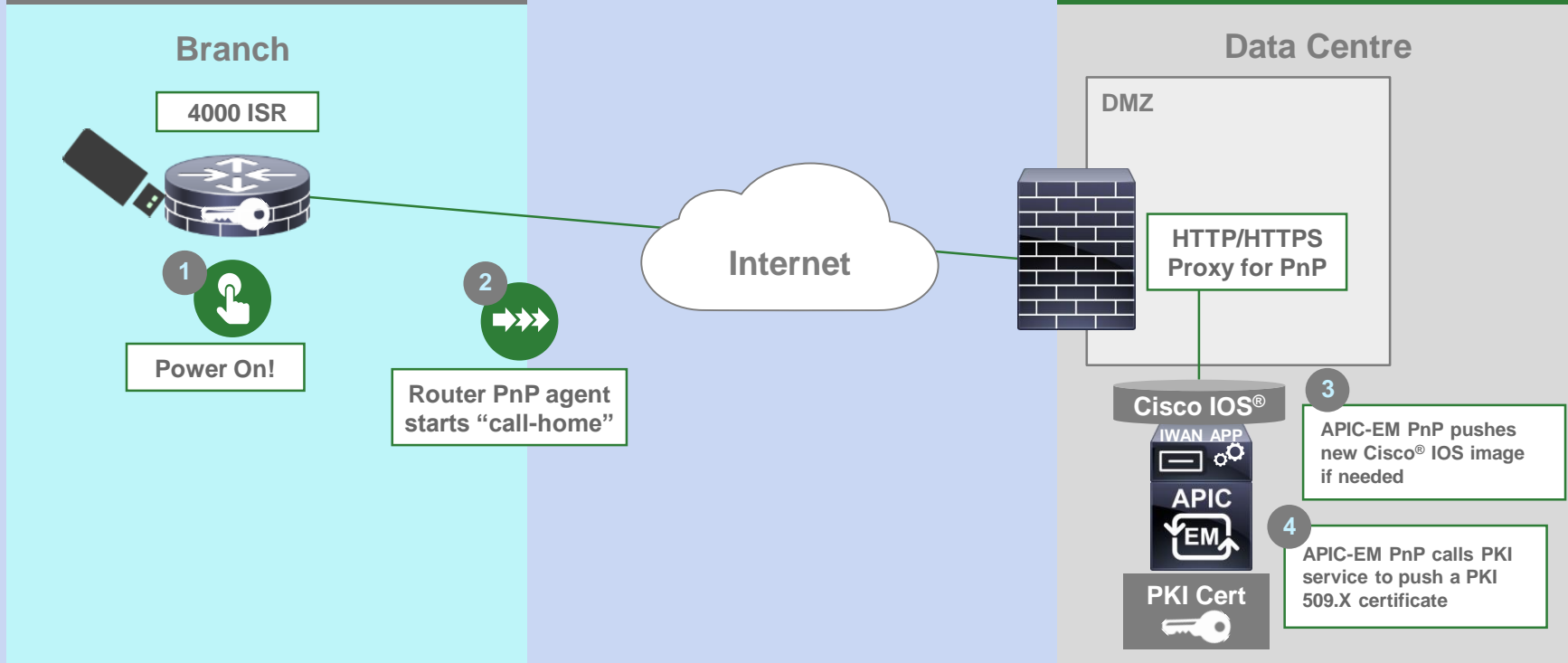
Application priority policy setting in IWAN app

- Path preference: Set primary and action on threshold crossing, which can be a second path or drop traffic
- Drag and drop business buckets

- Connect Internet and MPLS cables
- Insert PnP bootstrap USB stick
- Power up the Cisco 4000 ISR

## IWAN Transport

- Network-wide settings have been defined
- Data centre has been configured
- Application policies have been set



- IWAN configuration is applied
- Hybrid WAN tunnel comes up

## Branch

4000 ISR



MPLS

Internet

## Data Centre

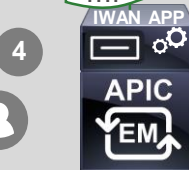
DMZ

ASR 1000

6  
Site is in production with IWAN enabled

5

Config policies



4  
Admin sees unclaimed device and starts deployment

4

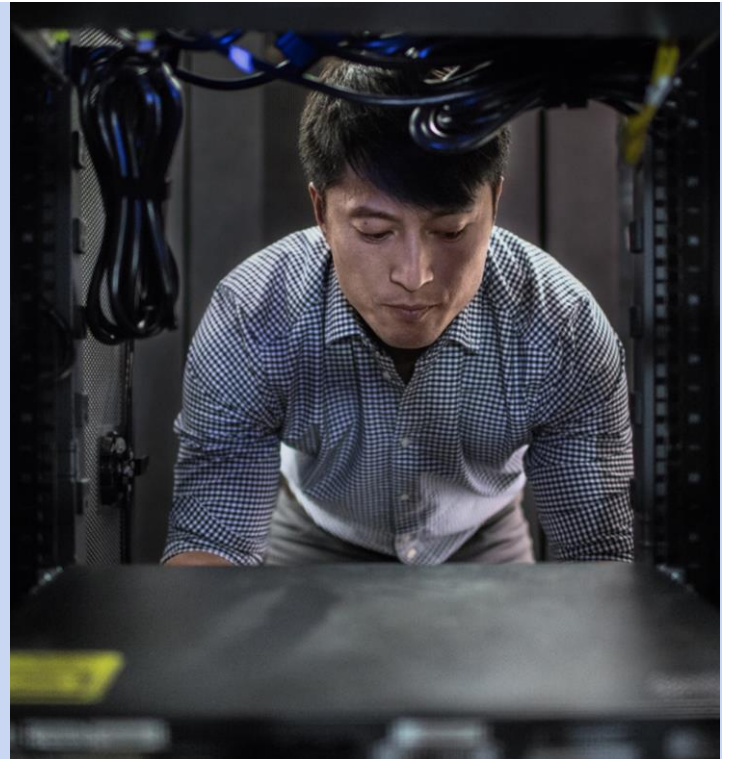


- IWAN service generates device configuration based on current policy settings and network-wide settings
- Config is pushed to device line by line:
  - DMVPN
  - Routing
  - Front-door VRF
  - AVC (NBAR2)
  - 8-class CoS
  - MPLS CoS translation
  - Start netflow collection
  - Start syslog exporting

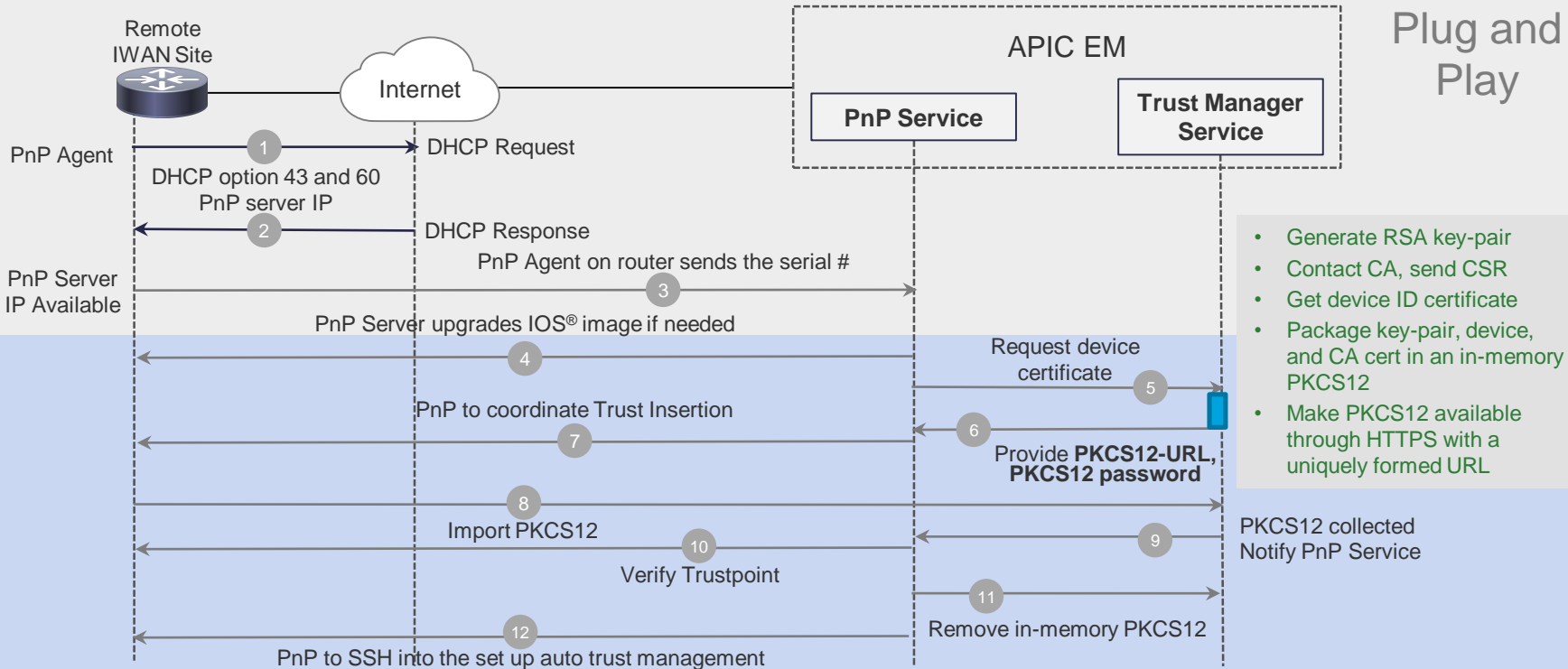


# PKI Service and Trust Manager Settings

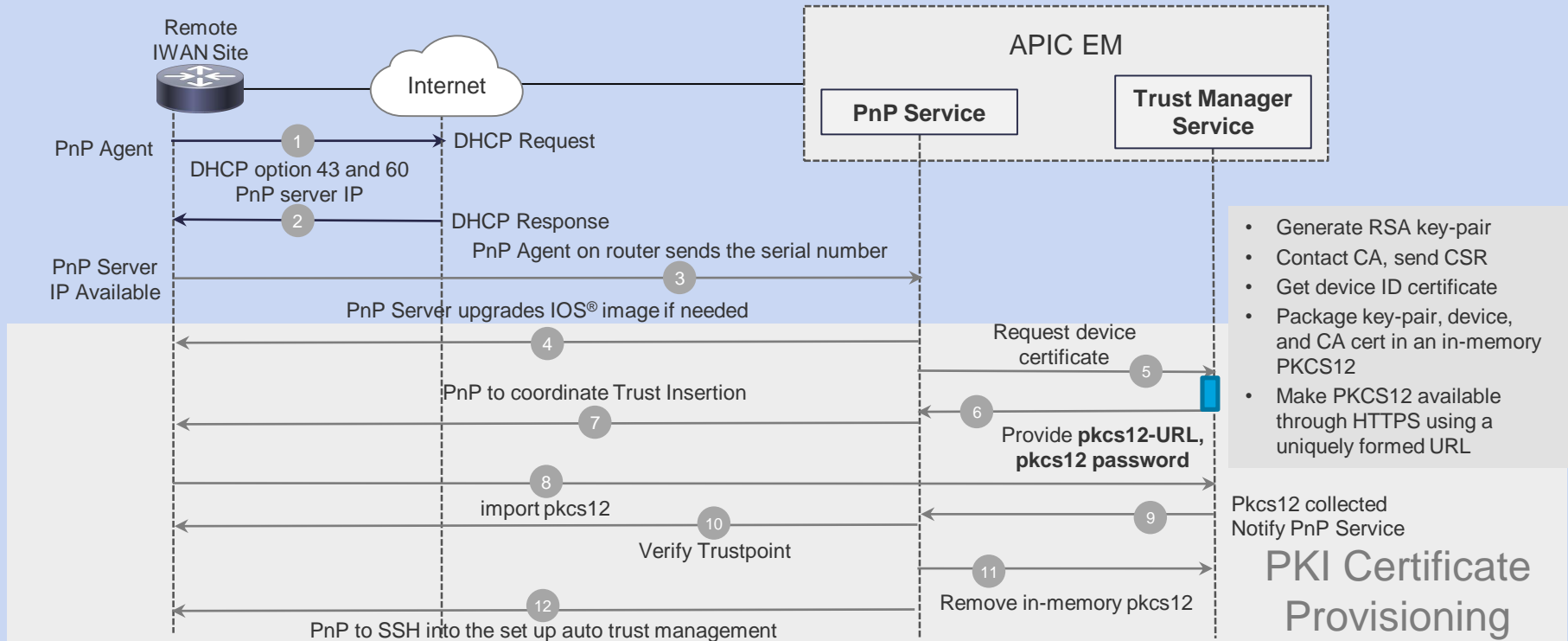
- PKI lifecycle is automated and simplified - deploy, renew, revoke - are driven using NB API calls
- APIC-EM runs a “CA Server” internally. This CA comes with APIs, which makes it a Trust Manager. It is designed for the purpose of DMVPN during ISAKMP authentication
- Root certificate has a 10-year lifecycle
- Device certificates have a 2-year lifecycle
- Certificates are renewed automatically when they pass 80% of their life
- RSA keys for devices generate with a 2048 key length
- PKI certificates are pushed to devices using PKCS12 encapsulation with an internal random password
  - PKCS12 includes private RSA keys and an X.509 certificate
- PKCS12 is encrypted with: SSLv3/TLSv1 - RSA Key Exchange; RSA Authentication; 256-bit AES encryption; and SHA1 HMAC
- PKCS12 files are pushed to devices using HTTPS
- PKI certificate reports are available through REST APIs into the PKI broker service. These include certificate management operations, as well as PKI broker services. Choose “API” in the APIC-EM to get more information



# IWAN Greenfield Deployment with Ethernet Hand-Off



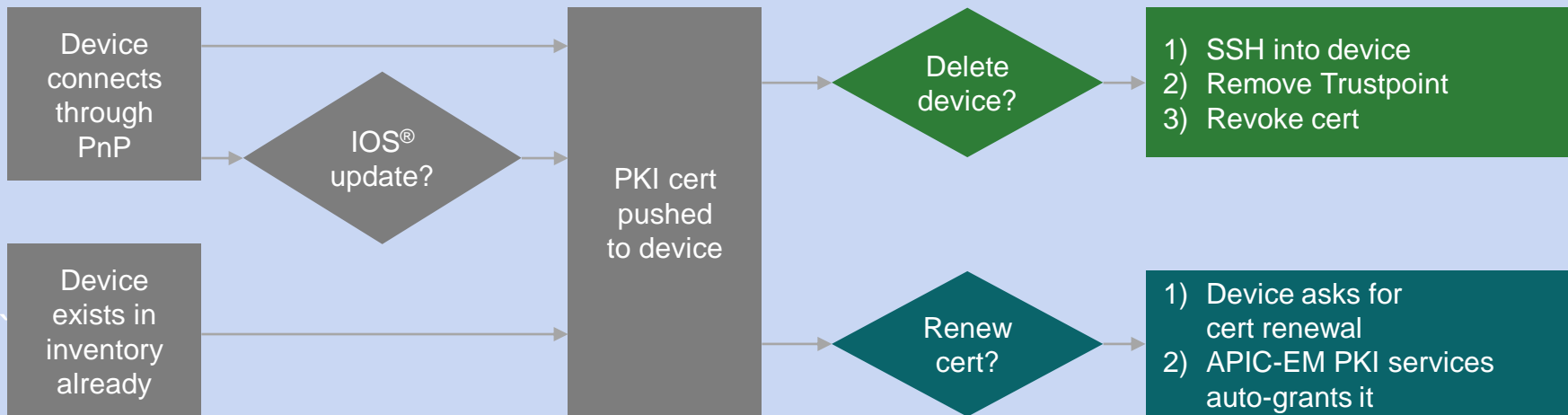
# IWAN Greenfield Deployment with Ethernet Hand-Off



- Generate RSA key-pair
- Contact CA, send CSR
- Get device ID certificate
- Package key-pair, device, and CA cert in an in-memory PKCS12
- Make PKCS12 available through HTTPS using a uniquely formed URL

PKI Certificate Provisioning

# PKI Lifecycle



## Notes:

- With the IWAN app, branch sites connect using PnP
- Data centre DMVPN hubs are discovered into the controller
- Both DMVPN hubs and branch sites get a PKI certificate

# *Easy QoS Application: Controller based Policy*

# Levels of QoS Policy Abstraction

## Strategic vs Tactical

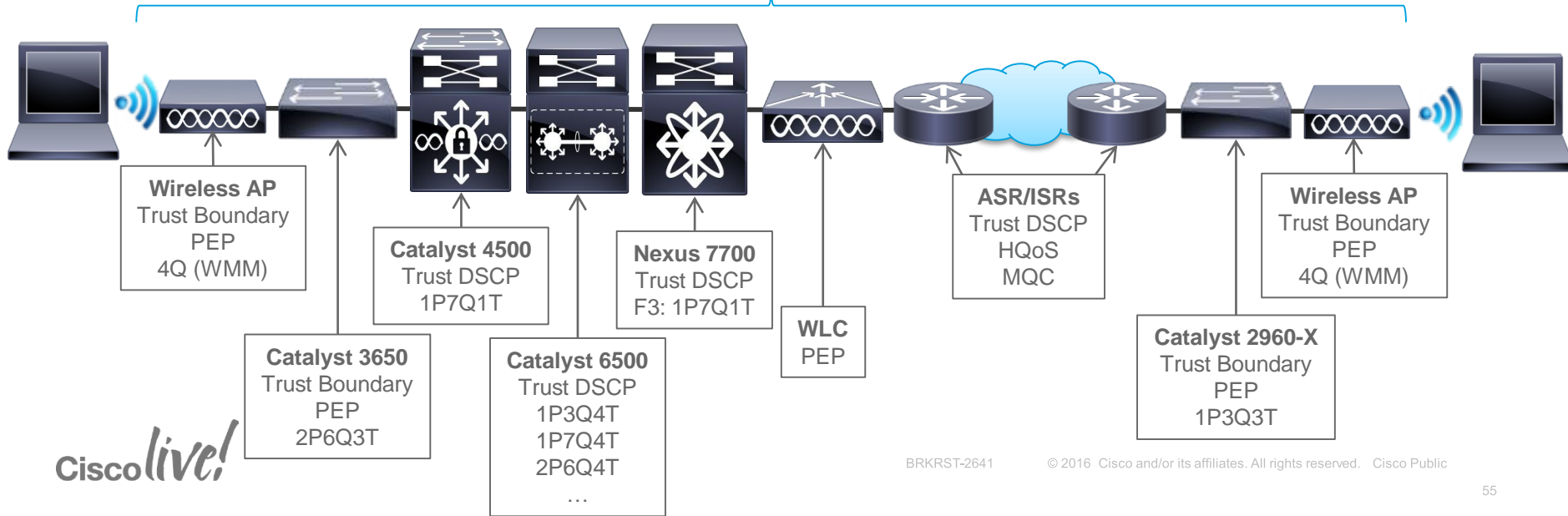
- Strategic QoS Policy (The **WHY** / **WHAT** you want to do)
  - reflects business **intent**
  - is not constrained by any technical or administrative limitation
  - is end-to-end
  
- Tactical QoS Policy (The **HOW** is it to be done)
  - adapts the strategic business intent to the maximum of platform's capabilities
  - is limited by various **tactical constraints**, including:
    - PIN-specific constraints
    - Platform constraints
    - Interface constraints
    - Role constraints

# Converting Business Intent to Tactical Policies

- the **principle goal** of the tactical QoS policy is to **express the strategic QoS policy with maximum fidelity**

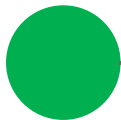


- QoS design **best practices** will be used to generate platform-specific configurations
- QoS features will be **selectively enabled** if they directly contribute to expressing the strategic policy on a given platform



# Determining Business Relevance

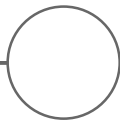
How Important is a Given Application to Business Objectives



Business  
Relevant

- These applications directly supports business objectives

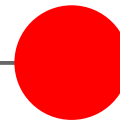
- 
- Applications should be classified and marked according to **RFC 4594**-based rules



Default /  
Maybe / Unknown

- These applications may/may not support business objectives
  - E.g. HTTP/HTTPS
- Alternatively, administrator may not know the application (or how its being used in the org)

- 
- Applications in this class should be marked DF and provisioned with a **default** best-effort service (**RFC 2474**)



Business  
Irrelevant

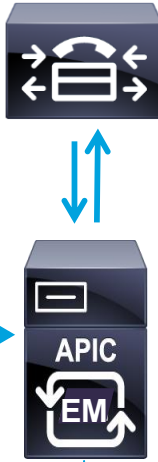
- These applications are known and do not directly support any business objectives; this class includes ***all personal/consumer applications***

- 
- Applications in this class should be marked CS1 and provisioned with a **“less-than-best-effort”** service (**RFC 3662**)



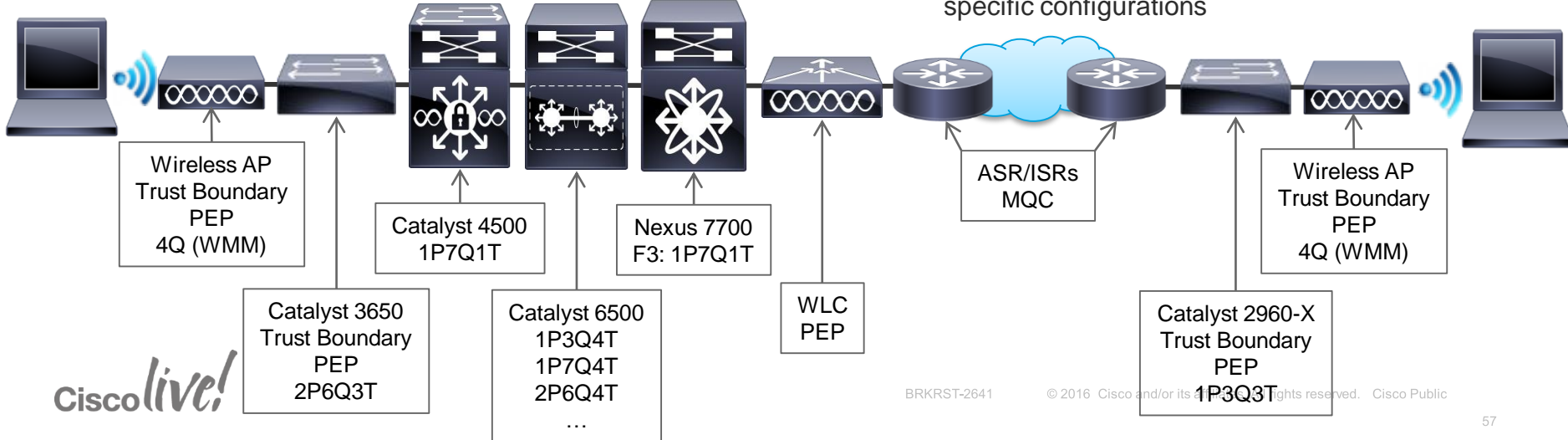
# EasyQoS Solution

Network Operators express high-level business-intent to APIC-EM EasyQoS



Applications can interact with APIC-EM via Northbound APIs, informing the network of application-specific and dynamic QoS requirements

Southbound APIs translate business-intent to platform-specific configurations



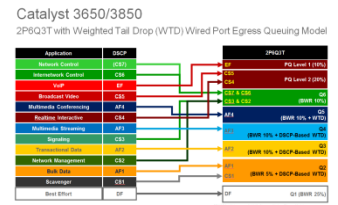
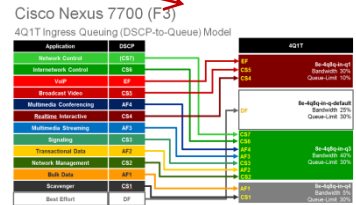
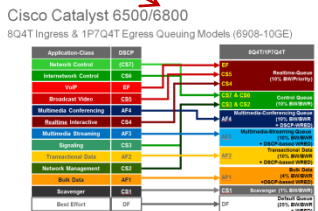
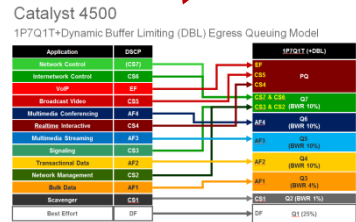
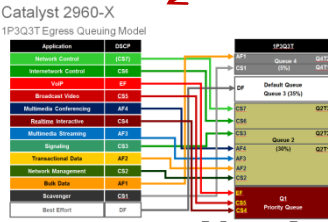
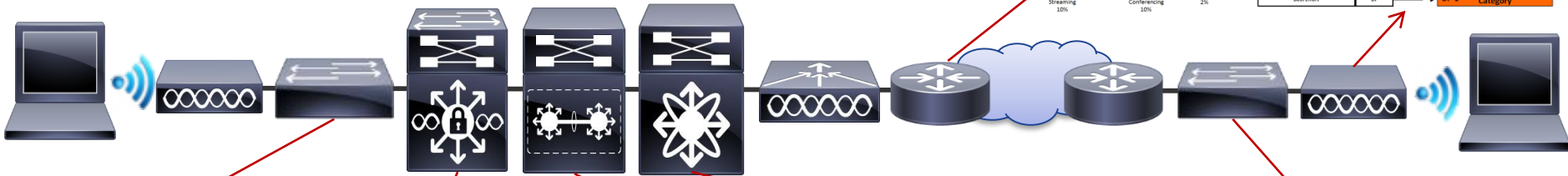
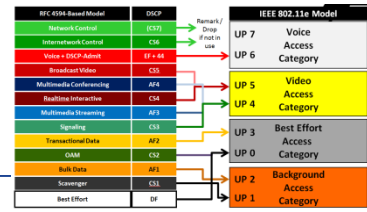
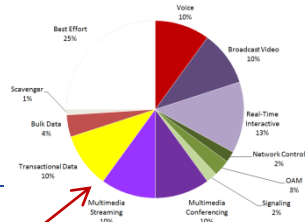
CiscoLive!

BRKRST-2641

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Public

# Deploy End-to-End DSCP-Based Queuing Policies

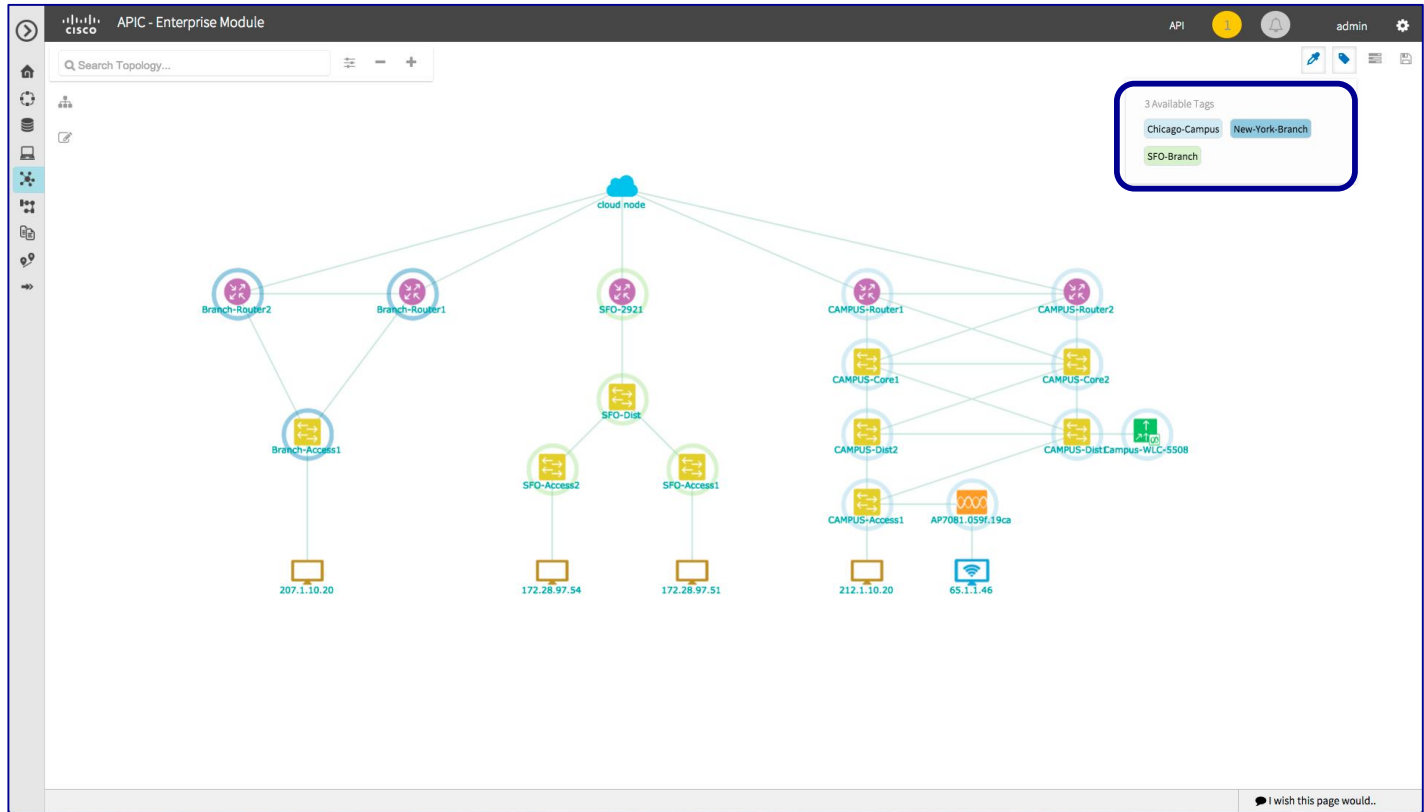
EasyQoS *seamlessly interconnects all types of hardware and software queuing models* to achieve consistent and compatible end-to-end treatments aligned with the expressed business-intent



# EasyQoS GUI



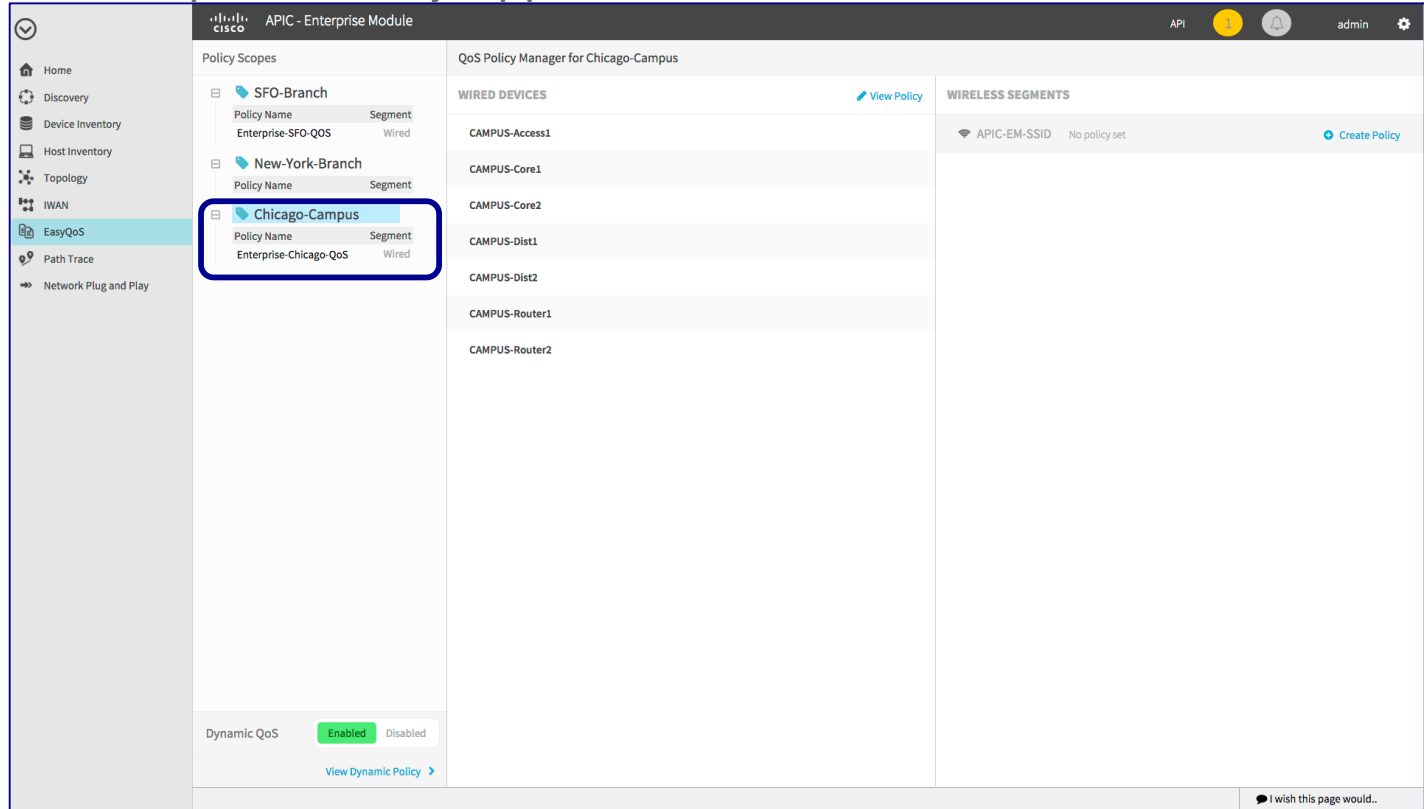
## Step 1: Select a Scope for Policy Application



# EasyQoS GUI



## Step 1: Select a Scope for Policy Application



The screenshot shows the Cisco APIC - Enterprise Module interface. The left sidebar contains navigation options: Home, Discovery, Device Inventory, Host Inventory, Topology, IWAN, EasyQoS (highlighted), Path Trace, and Network Plug and Play. The main content area is titled "QoS Policy Manager for Chicago-Campus". It features a "Policy Scopes" section on the left with a tree view containing "SFO-Branch", "New-York-Branch", and "Chicago-Campus". The "Chicago-Campus" node is selected and highlighted with a blue border. Below this, a table lists policies for "Enterprise-Chicago-QoS" with columns for "Policy Name" and "Segment". The "Segment" column shows "Wired". To the right, there are two main sections: "WIRED DEVICES" and "WIRELESS SEGMENTS". The "WIRED DEVICES" section lists several device types: CAMPUS-Access1, CAMPUS-Core1, CAMPUS-Core2, CAMPUS-Dist1, CAMPUS-Dist2, CAMPUS-Router1, and CAMPUS-Router2. The "WIRELESS SEGMENTS" section shows "APIC-EM-SSID" with "No policy set" and a "Create Policy" button. At the bottom, there is a "Dynamic QoS" toggle set to "Enabled" and a "View Dynamic Policy" link.

# EasyQoS GUI

## Step 2: (Optional) Change Application Business-Relevance



The screenshot displays the Cisco EasyQoS GUI for the 'Chicago-Campus' scope. The 'Applications' section is active, showing a list of applications with their current business relevance. A red box highlights the 'Business-Irrelevant' dropdown menu for the application '4chan - Website that hosts found images and discussions on them.'. A blue arrow points from this dropdown to a callout box that shows the available options: 'Business-Irrelevant' (selected), 'Business Relevant', 'Default', and 'Business Irrelevant'.

Application	Business Relevance
3Com AMP3	Default
3Com TSMUX	Default
4chan - Website that hosts found images and discussions on them.	Business-Irrelevant
58 City - Classified information about 58 cities in China.	Business-Irrelevant
A network traffic monitoring and IP information collection protocol	Default
A network traffic monitoring and IP information collection protocol	Default
A remote network server system	Default
ABC - Web Portal for television network.	Business-Irrelevant
ACA Services	Default
ACAP	Business-Relevant
ACR-NEMA Digital Img	Default

Summary statistics on the right:

- 411 BUSINESS RELEVANT
- 539 DEFAULT
- 377 BUSINESS IRRELEVANT

# EasyQoS GUI

## Step 3: (Optional) Add Custom Applications






The screenshot displays the Cisco APIC EasyQoS GUI. The interface is divided into several sections:

- Policy Scopes:** A sidebar on the left shows a tree view with branches: SFO-Branch, New-York-Branch, and Chicago-Campus. Under Chicago-Campus, there is a sub-section for Enterprise-Chicago-QoS with a 'Wired' segment.
- Application Form:** The main area shows a form to add a new application. A blue box highlights the 'Add Application' button. The form fields include:
  - Name: Application Name
  - Type: Radio buttons for URL, Server IP/Port (selected), and DSCP.
  - Protocol: Radio buttons for TCP (selected) and UDP.
  - Value: Two input fields separated by a colon.
  - Traffic Class: A dropdown menu currently set to BULK\_DATA.
  - or -
  - Similar To: An input field containing the word 'Application'.
  - A 'Create Application' button at the bottom right of the form.
- Summary Dashboard:** On the right, a summary panel shows three categories:
  - 411 BUSINESS RELEVANT** (light blue background)
  - 539 DEFAULT** (light blue background)
  - 377 BUSINESS IRRELEVANT** (light red background)Below this, a list of application categories and their counts is shown:
  - BUSINESS RELEVANT**
    - Bulk Data: 56 apps
    - Transactional Data: 57 apps
    - Ops Admin Mgmt: 190 apps
    - Network Control: 41 apps
    - Voip Telephony: 7 apps
    - Multimedia Conferencing: 22 apps
    - Multimedia Streaming: 8 apps
    - Broadcast Video: 2 apps
    - Real Time Interactive: 3 apps
    - Signaling: 25 apps
  - DEFAULT**
    - Other: 539 apps
  - BUSINESS IRRELEVANT (SCAVENGER)**
    - Scavenger: 377 apps
- Dynamic QoS:** At the bottom left, a toggle switch is set to 'Enabled' (green).

CiscoLive!

# What Do We Do Under-the-Hood?

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

	Application Class	Per-Hop Behaviour	Queuing & Dropping	Application Examples
Relevant 	VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
	Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
	Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
	Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
	Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
	Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
	Signalling	CS3	BW Queue	SCCP, SIP, H.323
	Ops / Admin / Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
	Transactional Data	AF2	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
	Bulk Data	AF1	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Default 	Default Forwarding	DF	Default Queue + RED	Default Class
Irrelevant 	Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Cisco *live!*

# Current Differences between IWAN and EQ Policy

	IWAN	EasyQoS
Scope	Global (until May)	Tag based
Relevance Categorisation	Per Application Category	Per Application
Devices Supported	Routers – IWAN deployed	Routers/switches/WLAN
Dynamic Policy	NA	Yes, Voice, Video



# Dynamic QoS

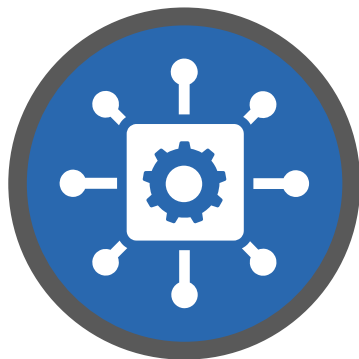
The screenshot displays the Cisco APIC Enterprise Module interface. On the left, the 'Policy Scopes' sidebar shows a tree view with 'SFO-Branch' expanded, containing 'Enterprise-SFO-QoS' (Wired) and 'New-York-Branch'. Below it is 'Chicago-Campus'. The main area shows a table of 'Dynamic QoS Policies' with the following data:

Status	Source IP	Source Port	Dest IP	Dest Port	Flow Type	Protocol
CONFIG_ADD_SUCCESS	172.28.97.51	30672	172.28.97.54	28452	VIDEO	udp
CONFIG_ADD_SUCCESS	172.28.97.54	21054	172.28.97.51	23614	VOICE	udp
CONFIG_ADD_SUCCESS	172.28.97.54	28452	172.28.97.51	30672	VIDEO	udp
CONFIG_ADD_SUCCESS	172.28.97.51	23614	172.28.97.54	21054	VOICE	udp

At the bottom left, a 'Dynamic QoS' toggle is shown with 'Enabled' selected. A blue box labeled 'Dynamic QoS Enabled' has an arrow pointing to this toggle. Another blue box labeled 'Dynamic QoS Policies' has an arrow pointing to the table of policies.

# *Summary*

# Changes



## Simplification

Network-wide abstraction supporting both Greenfield and Brownfield

## Automation

OPEX reduction through adoption of Cisco best practices

## Abstraction - Policy

Dynamic network that adapts to business intent policy

## Open Programmability

Open NB REST API's with agnostic SB interfacing

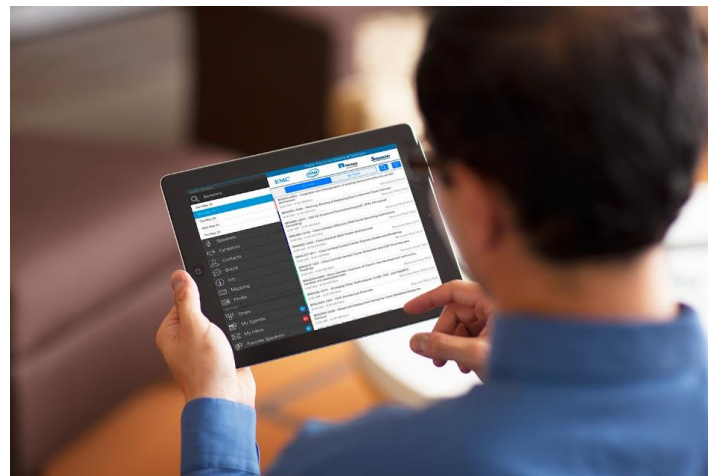
# Q & A

# Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the 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 <http://showcase.genie-connect.com/ciscolivemelbourne2016/>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected Friday 11 March at Registration



**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)

*Thank you*

