

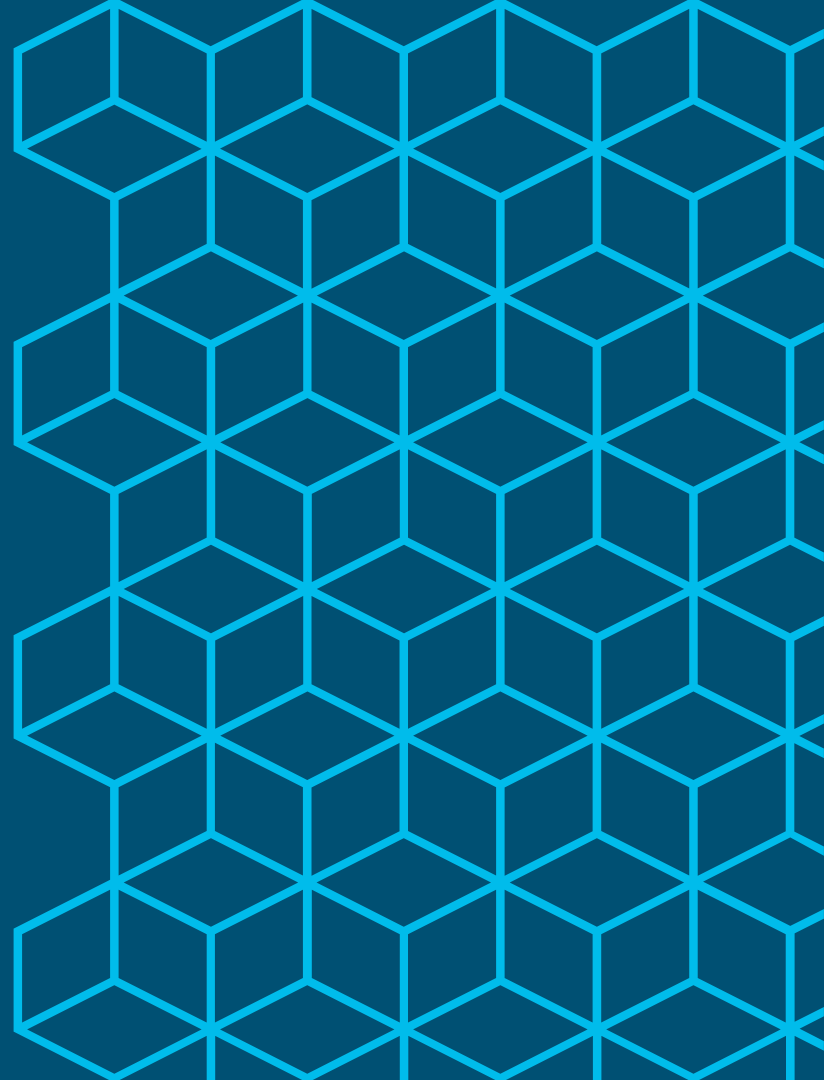


# Jak jinak na podnikové síti s Cisco DNA Center

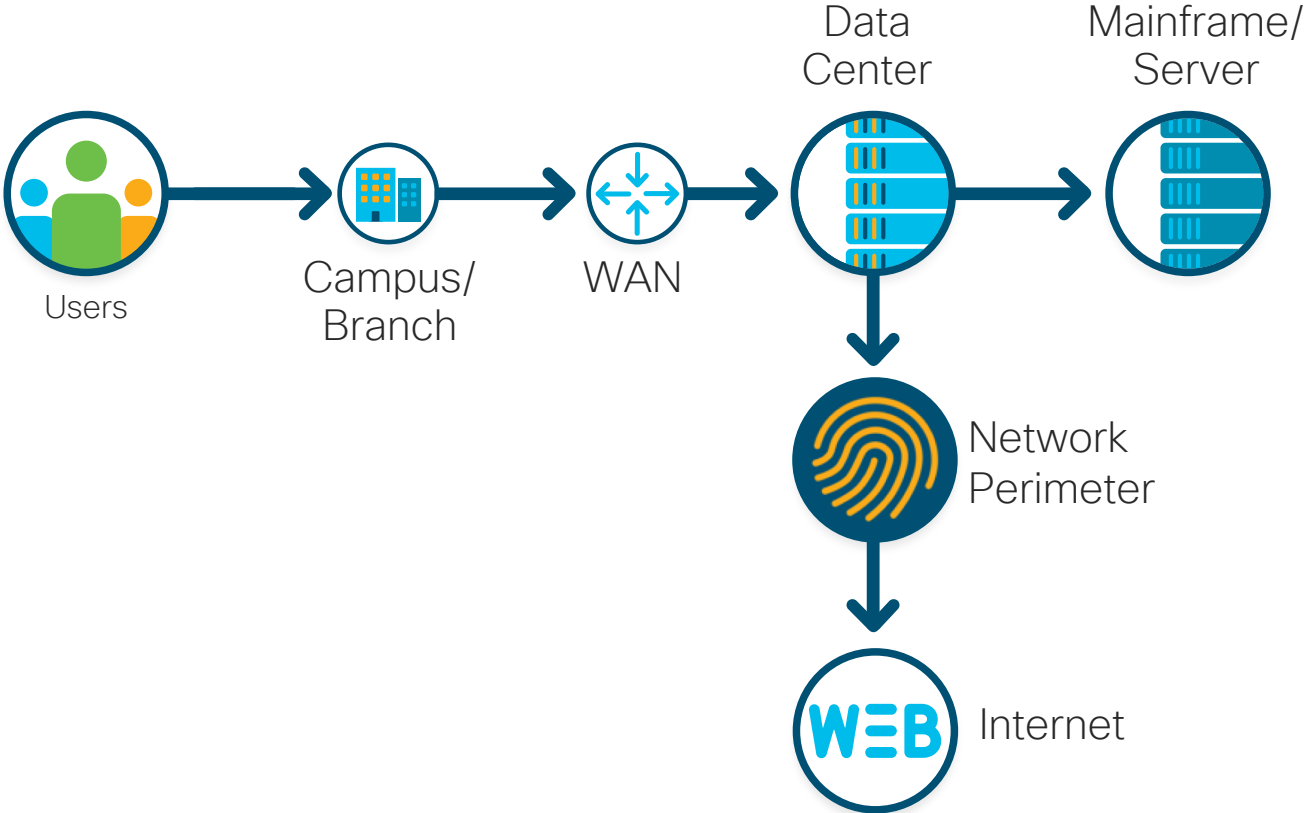
Zdeněk Roubal, SE

Cisco TechClub – 19.února 2019

# The Need for Intent- Based Networking

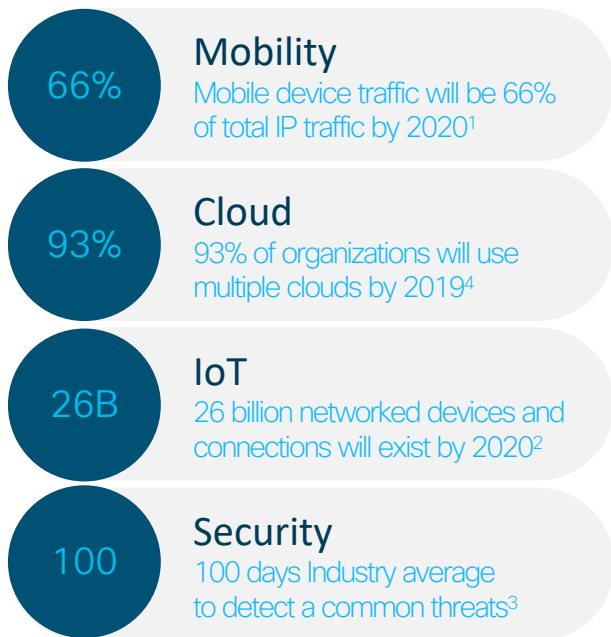


# Traditional Network Topology

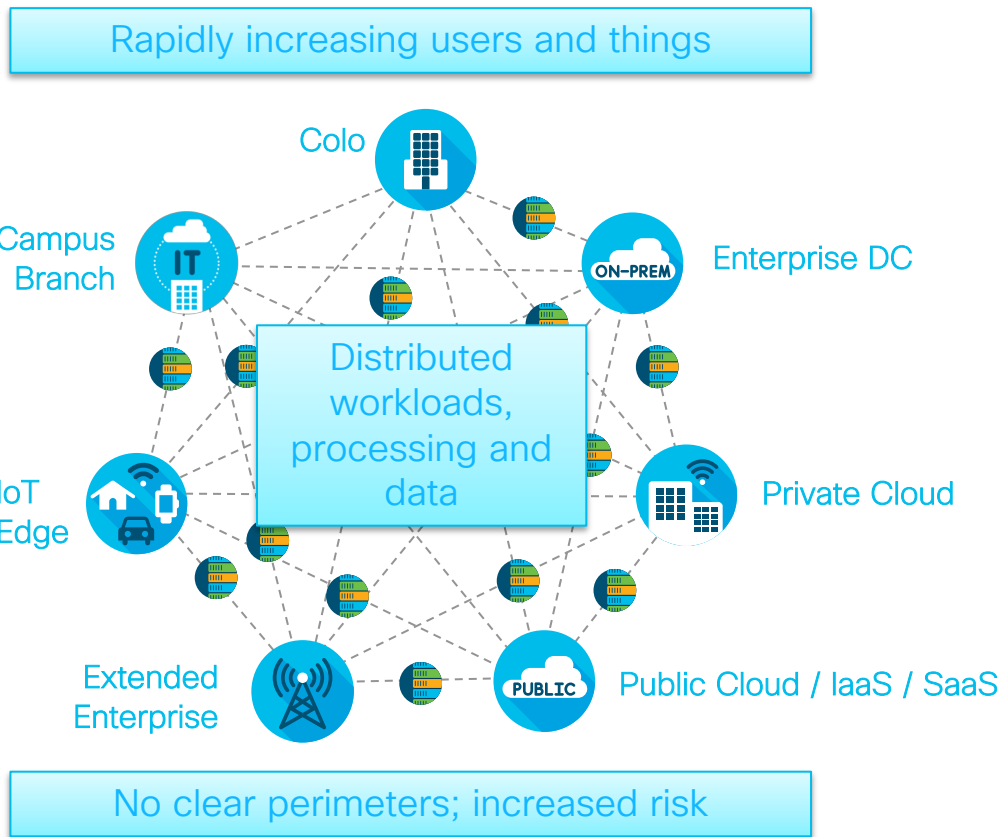


# New world network requirements:

## Increased application distribution, device scale and threats







[2017 Cisco Security report](#)  
[Cisco Complete VNI Forecast](#)  
[Cisco 2016 Mid-Year Cybersecurity Report](#)  
[Cisco Global Cloud Index Whitepaper](#)

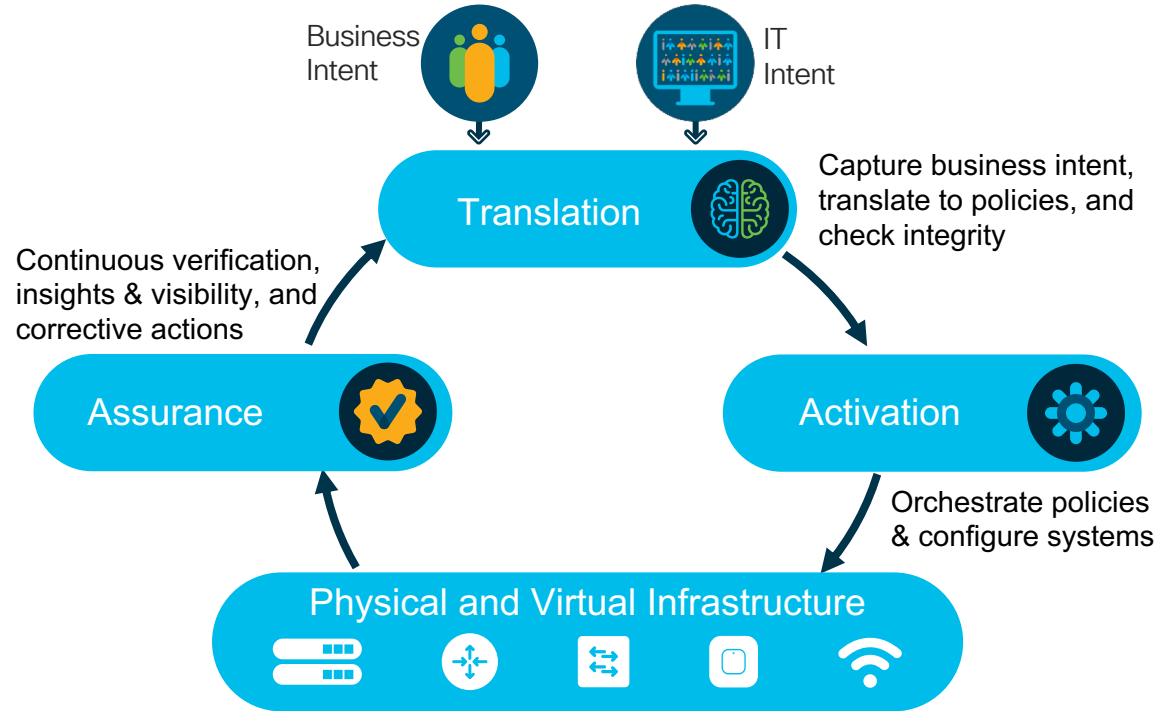




# How? The Intent-Based Model

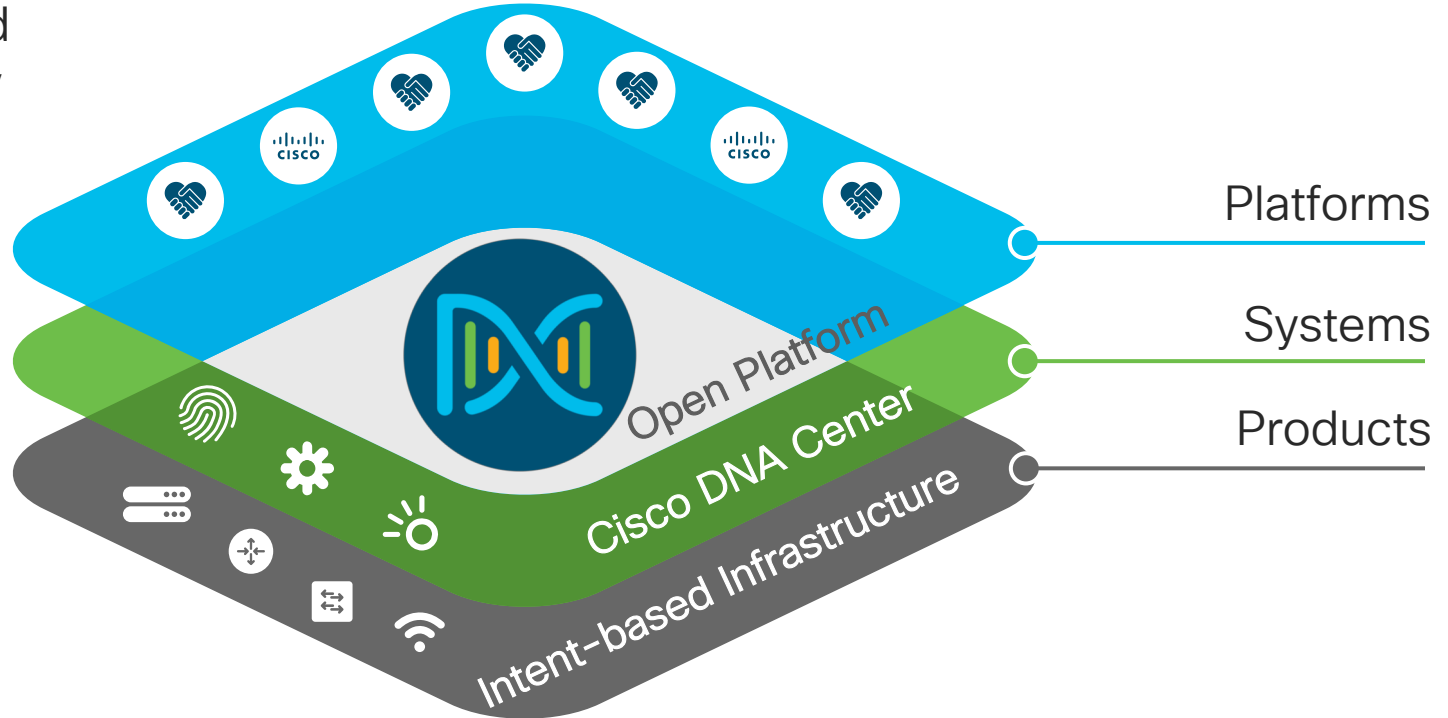
## Intent-Based Networking Industry Initiative

-  Bridging between business intent and IT performance
-  Building on software-defined networking fundamentals
-  Integrating security into the network model
-  Automating the complete network lifecycle

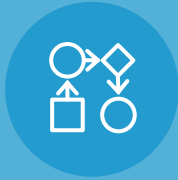


# The Journey to Intent-based Networking

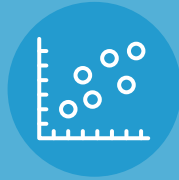
Increased  
IT Agility



# Cisco DNA Center



**Logical workflow to design,  
provision, set policy**  
Respond to changes faster



**Monitor end-to-end  
network performance**  
Predict and act on problems  
before they happen



**Pinpoint problems faster**  
Reduce downtime with an  
end-to-end view instead of  
hop by hop

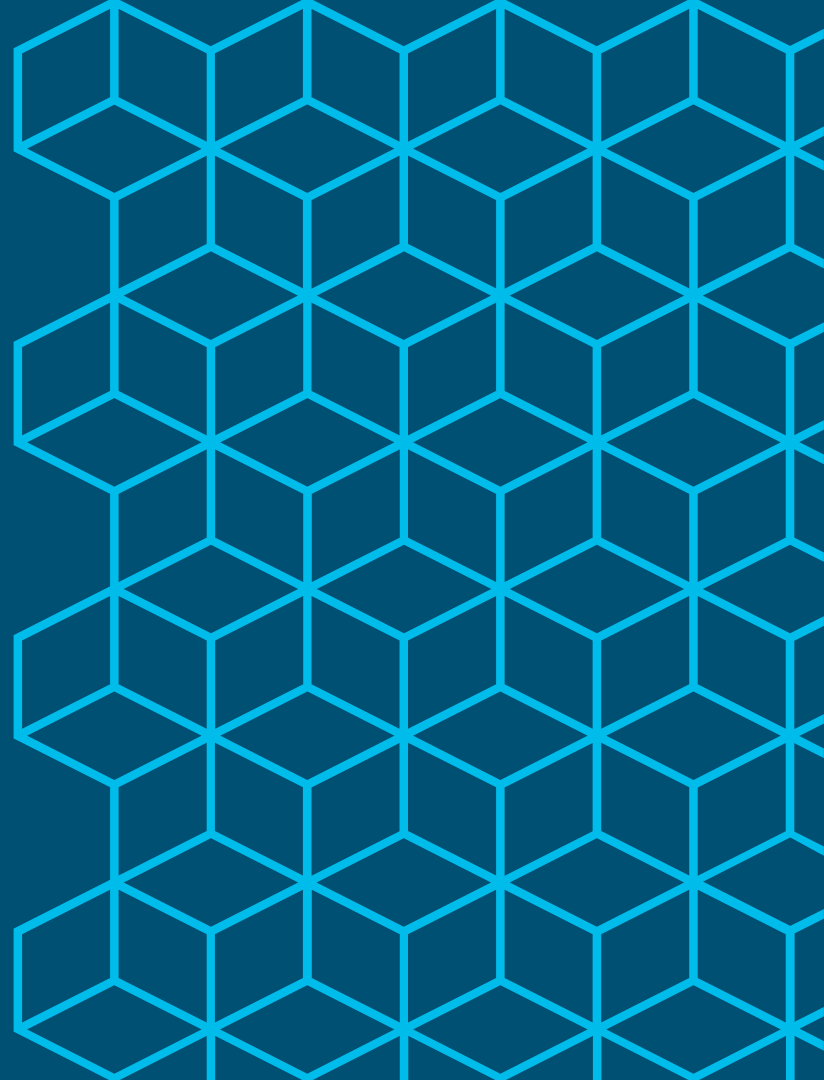


**Manage hardware and  
software lifecycles**  
Keep up to date, meet  
compliance and plan for refresh



**Cisco DNA Center: Design,  
provision, automate policy and  
assure services from one place**

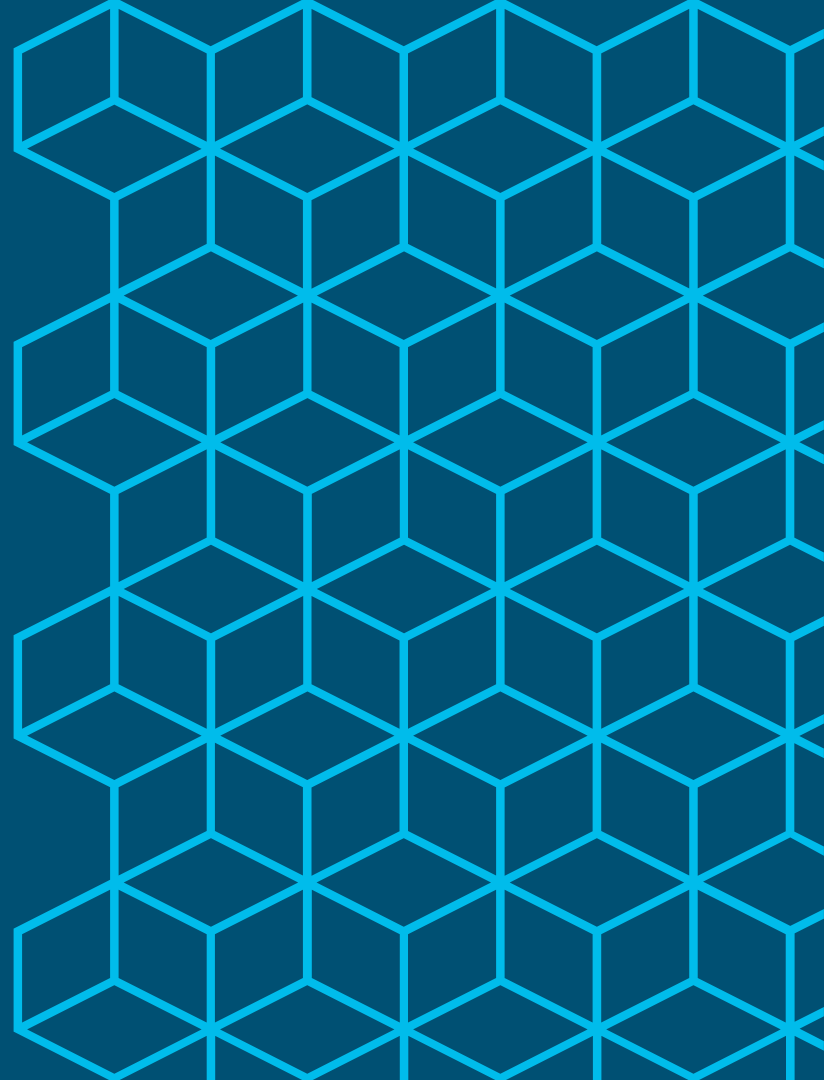
# Cisco DNA Automation



# Automation Use Cases covered in this session

- **Use Case #1** - New device onboarding
- **Use Case #2** - Software and Image Management
- **Use Case #3** - Wireless Deployment
- **Use Case #4** - Application Policy – End to End QoS Deployment

# Preparing Cisco DNA Center



# Step 1 – Define your network hierarchy

The screenshot displays the Cisco DNA Center interface for defining a network hierarchy. The main navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. Below this, the 'Network Hierarchy' section is active, showing a tree view on the left with 'Global', 'USA', 'SJC', 'Branch', 'Floor 1', and 'Campus'.

The central map shows a geographical area with buildings and streets. A 'Branch' location is marked with a blue pin and labeled 'Branch'. A 'Campus' location is also marked with a blue pin and labeled 'Campus'. A dialog box titled 'Branch' is open over the map, containing the following information:

Branch	
Building Name	Branch
Hierarchy	Global > USA > SJC > Branch
Address	325 East Tasman Drive, San Jose, California 95134, United States
Geolocation	Lat 37.414... Long -121.931...
<a href="#">Edit Building</a>	<a href="#">Delete Building</a>
<a href="#">Add Floor</a>	<a href="#">Sync with CMX</a>

The map interface includes a search bar 'Find Buildings' and navigation controls. The 'Branch' dialog box also has a close button (X) in the top right corner.

# Step 2 – Define Network Settings and Device Credentials

Network Hierarchy   **Network Settings**   Image Repository   Network Profiles   Auth Template

Find Hierarchy

Global  
USA  
SJC  
Branch  
Campus

**Network**   Device Credentials   IP Address Pools   SP Profiles   Wireless

Setup network properties like AAA, NTP, Syslog, Trap and NetFlow using the "Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings. [Network Telemetry](#) | [+ Add Servers](#)

**DHCP Server**

DHCP  
1.1.1.1 +

**DNS Server**

Domain Name  
cisco.com

Primary  
44.44.44.44 +

**SYSLOG Server**

SYSLOG  
55.55.55.55 +

Feedback



# Step 3 – Discover existing network

**DNA**  
CENTER

Discovery

1
🔍
☰
⚙️
☰

EQ 🔍 Search by Discovered Device IP
+

Network-Wide
🔄 Completed
6 Reachable Devices
00h:00m:23s

History ▾

🟢 Network-Wide | 6 Reachable Dev...  
CDP 10.1...

8

Devices

DEVICE STATUS
▾

- Success(6)
- Unreachable(0)
- Discarded(2)

🔍 Filter

IP Address	Device Name	Status	ICMP	SNMP	CLI	HTTP(S)	NETCONF
10.10.70.23		✔️ 1	●	●	●	●	●
10.10.70.41		✔️ 1	●	●	●	●	●
10.1.8.2	HQ-SW1.cisco.local	✔️	✔️	✔️	✔️	●	●
10.10.64.2	BR-SW1	✔️	✔️	✔️	✔️	●	●
10.1.8.1	HQ-R1.cisco.local	✔️	✔️	✔️	✔️	●	●
10.1.5.50	5520	✔️	✔️	✔️	✔️	●	●
10.10.64.7	BR-SW2.cisco.com	✔️	✔️	✔️	✔️	●	●
10.2.252.2	BR-R1.cisco.local	✔️	✔️	✔️	✔️	●	●

Show 25 ▾
Showing 1 to 8 of 8
Page 1 of 1
?

✔️ SUCCESS
 🚫 UNREACHABLE
 ❌ FAILURE
 ● NOT TRIED
 ❓ UNAVAILABLE

### Discovery Details

CDP Level	16	LLDP Level	None
Protocol Order	ssh	Retry Count	3
Timeout	5 second(s)	IP Range	10.1.8.1
IP Filter List	None	Preferred Management IP	None
CLI Credentials	admin	SNMPv2c READ	RO
SNMPv2c WRITE	RW	SNMPv3	None
HTTP(S) READ	None	HTTP(S) WRITE	None
NETCONF	None		

↶  
Feedback

# Step 4 – Check Inventory

Last updated: 9:34 am [Refresh](#) [Import](#) [Export](#) [Add](#)

[Filter](#) | [Actions](#) [EQ Find](#)

<input type="checkbox"/>	Device Name <span>▲</span>	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status	Site	⋮
<input type="checkbox"/>	<a href="#">5520</a>	10.1.5.50	<span>✔</span> Reachable	18 hrs 42 mins	3 minutes ago	00:25:00	Managed	...SA/SJC/Campus	
<input type="checkbox"/>	<a href="#">ap1</a>	10.10.70.41	<span>✔</span> Reachable	17 hrs 42 mins	3 minutes ago	N/A	Managed	Unassigned	
<input type="checkbox"/>	<a href="#">ap2</a>	10.10.70.23	<span>✔</span> Reachable	17 hrs 43 mins	3 minutes ago	N/A	Managed	Unassigned	
<input type="checkbox"/>	<a href="#">BR-R1.cisco.local</a>	10.2.252.2	<span>✔</span> Reachable	1 day 21 hrs 01 mins	12 minutes ago	00:25:00	Managed	...SA/SJC/Branch	
<input type="checkbox"/>	<a href="#">BR-SW1</a>	10.10.64.2	<span>✔</span> Reachable	7 days 23 hrs 34 mins	16 minutes ago	00:25:00	Managed	...SA/SJC/Branch	
<input type="checkbox"/>	<a href="#">BR-SW2.cisco.com</a>	10.10.64.7	<span>✔</span> Reachable	19 hrs 24 mins	22 minutes ago	00:25:00	Managed	...SA/SJC/Branch	
<input type="checkbox"/>	<a href="#">HQ-R1.cisco.local</a>	10.1.8.1	<span>✔</span> Reachable	1 day 14 hrs 31 mins	8 minutes ago	00:25:00	Managed	...SA/SJC/Campus	
<input type="checkbox"/>	<a href="#">HQ-SW1.cisco.local</a>	10.1.8.2	<span>✔</span> Reachable	217 days 5 hrs 33 mins	9 minutes ago	00:25:00	Managed	...SA/SJC/Campus	

Show **10** entries Showing 1 - 8 of 8

[Previous](#) **1** [Next](#) [Feedback](#)

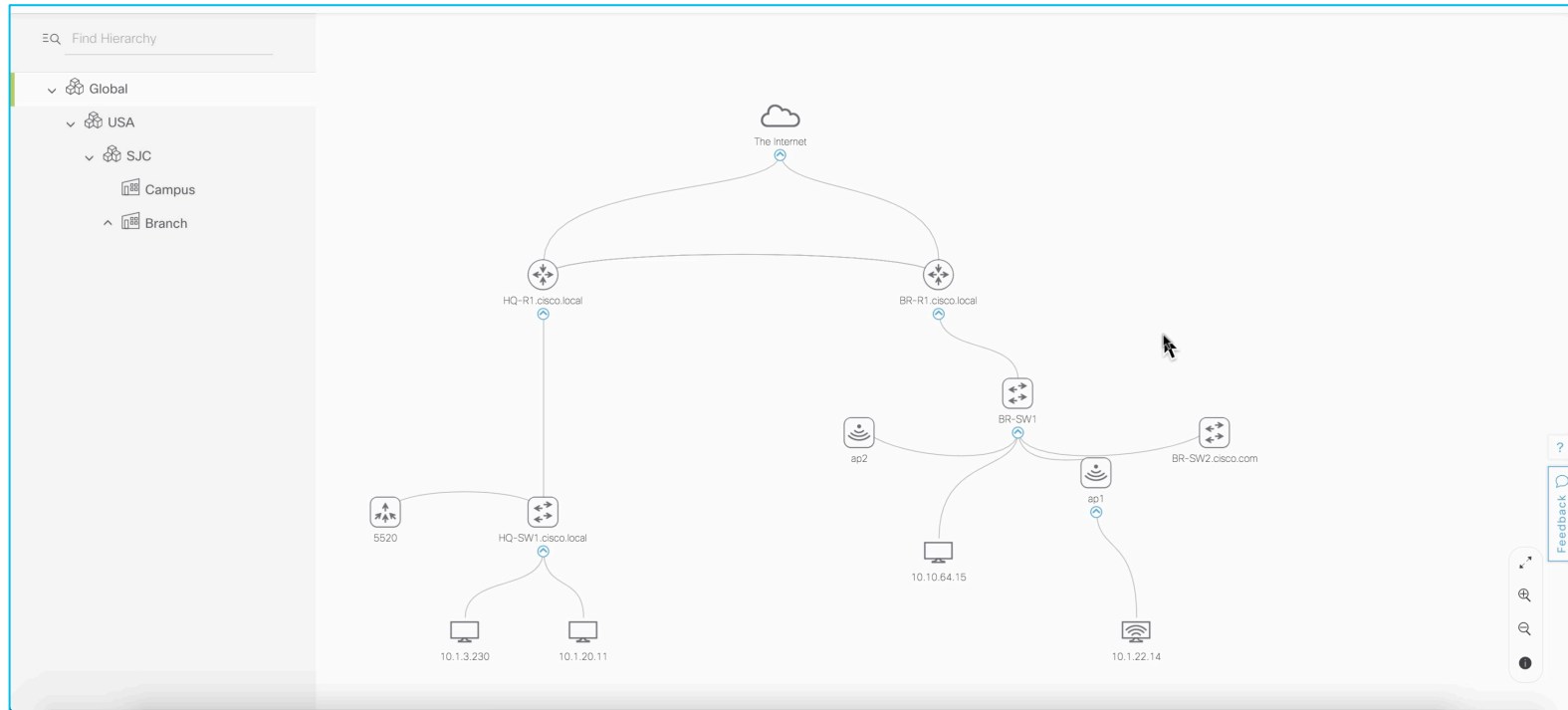
# Step 5 – Assign Devices to Sites

Filter | Actions | Tag Device | LAN Automation

<input type="checkbox"/>	Device Name	Device Family	Site	OS Version	OS Image	Last Sync Status	Device series	
<input type="checkbox"/>	<a href="#">5520</a>	Wireless Controller	...SA/SJC/Campus	8.7.102.0	Cisco Control... Tag Golden	Managed	Cisco 5500 Series Wireless LAN Controllers	
<input type="checkbox"/>	<a href="#">ap2</a>	Unified AP	...ranch/Floor 1	8.7.102.0		Managed	Cisco 3800I Series Unified Access Points	
<input type="checkbox"/>	<a href="#">BR-R1.cisco.local</a>	Routers	...SA/SJC/Branch	16.3.6	isr4300-unive... Tag Golden	Managed	Cisco 4300 Series Integrated Services Routers	
<input type="checkbox"/>	<a href="#">BR-SW1</a>	Switches and Hubs	...SA/SJC/Branch	16.6.1	cat9k_iosxe.1...	Managed	Cisco Catalyst 9300 Series Switches	
<input type="checkbox"/>	<a href="#">BR-SW2.cisco.com</a>	Switches and Hubs	...SA/SJC/Branch	16.6.2	CAT9K[16.6.2] Outdated	Managed	Cisco Catalyst 9300 Series Switches	
<input type="checkbox"/>	<a href="#">HQ-R1.cisco.local</a>	Routers	...SA/SJC/Campus	16.3.6	isr4300-unive... Tag Golden	Managed	Cisco 4300 Series Integrated Services Routers	
<input type="checkbox"/>	<a href="#">HQ-SW1.cisco.local</a>	Switches and Hubs	...SA/SJC/Campus	03.06.03E	packages.conf Tag Golden	Managed	Cisco Catalyst 3850 Series Ethernet Stackable Switch	

1 to 7 of 7

# Step 6 (Optional) - Check Topology

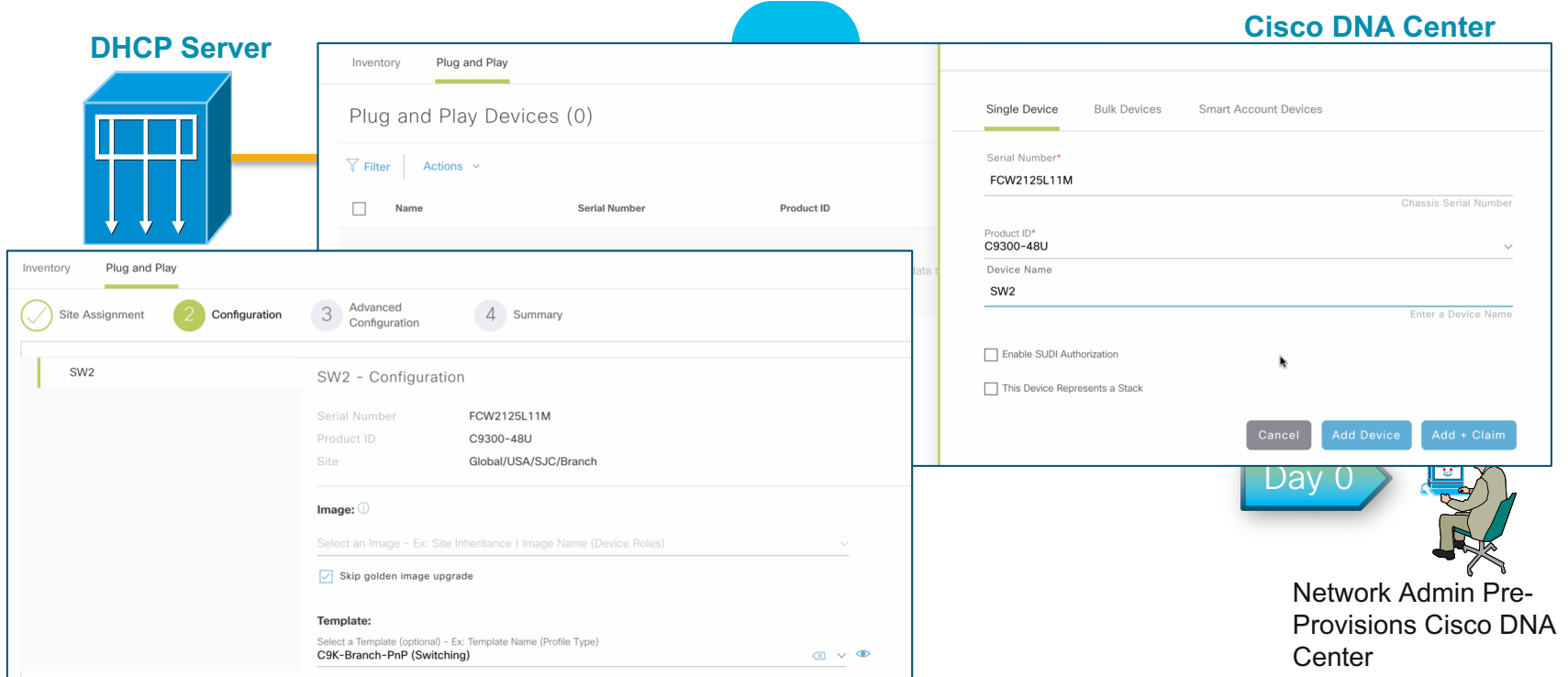


# Use Case #1 - Network Plug and Play



# Use Case Example

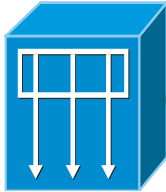
## Device Deployment in Campus



# Use Case Example

## Device Deployment in Campus

DHCP Server



```
<..snip..>  
CISCO_PNP.pnpserver  
"5A;B2;K4;I10.11.11.11;J80"  
<..snip..>
```

Day 1



Installer

Remote Install

- Mount and devices
- Power-on

SW2  
SUDI: Authenticated

Refresh Edit Delete

Details History Configuration

History  
Last updated: 7:54 am Refresh

Status	Time	Details	Info
✓	01/04/2019 12:57:30 UTC	Device added to Site Global/USA/SJC/Branch	Info
✓	01/04/2019 12:57:29 UTC	Device added to Inventory	Info
✓	01/04/2019 12:57:29 UTC	Task: System Backup Config Task Completed	Info
✓	01/04/2019 12:57:28 UTC	Executing Task: System Backup Config Task	Info
✓	01/04/2019 12:57:23 UTC	Task: Site Config Task Completed	Info
✓	01/04/2019 12:57:03 UTC	Executing Task: Site Config Task	Info
✓	01/04/2019 12:56:58 UTC	Task: System Backup Config Task Completed	Info
✓	01/04/2019 12:56:57 UTC	Day 0 Config Generated	Info

Device validates server's location and establishes a communication with the server

(PnP Server)



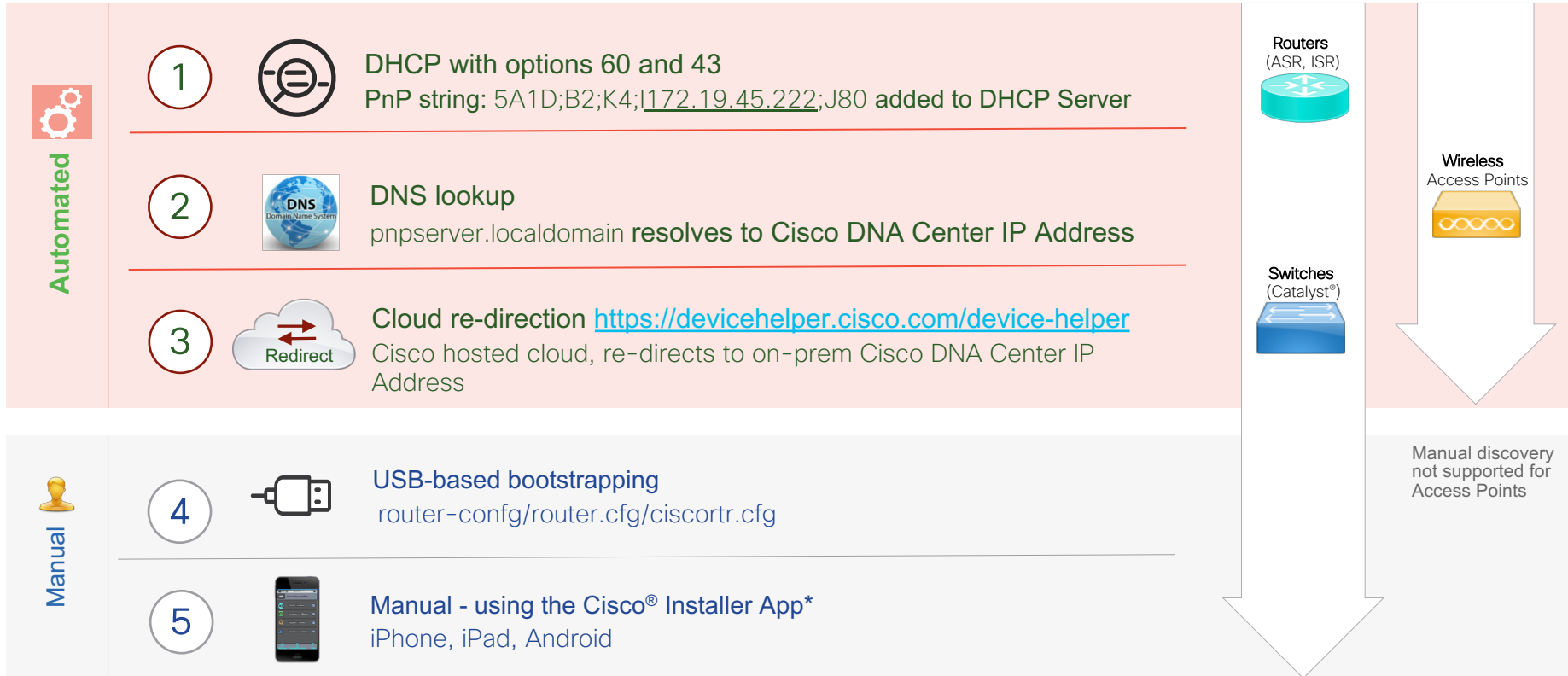
IP Address  
10.11.11.11

Day 1



Network Admin remotely monitors status of install while in progress.

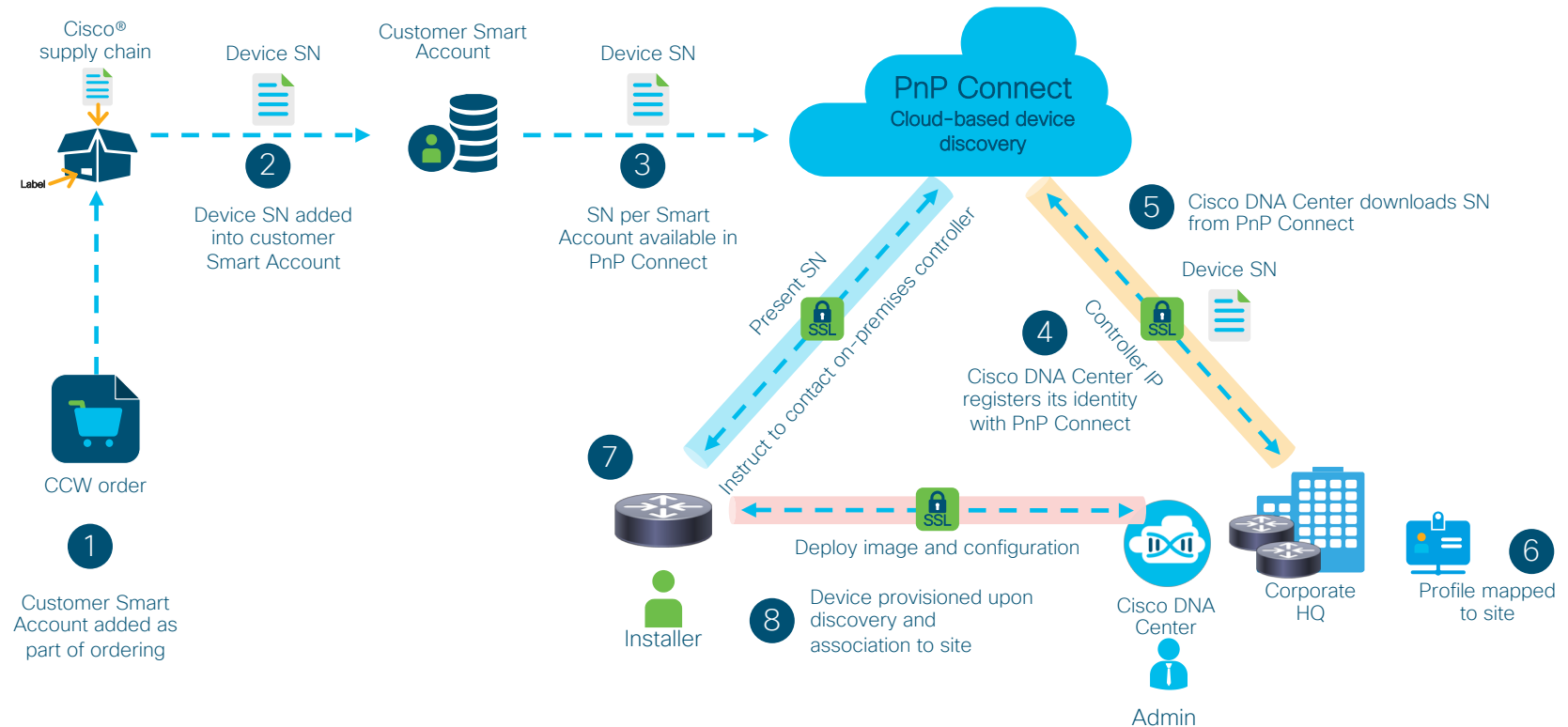
# PnP Server Discovery Options



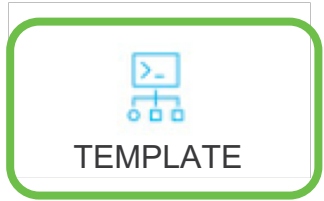
\* Cisco DNA Center Support in Roadmap



# Day-0 deployment using PnP Connect

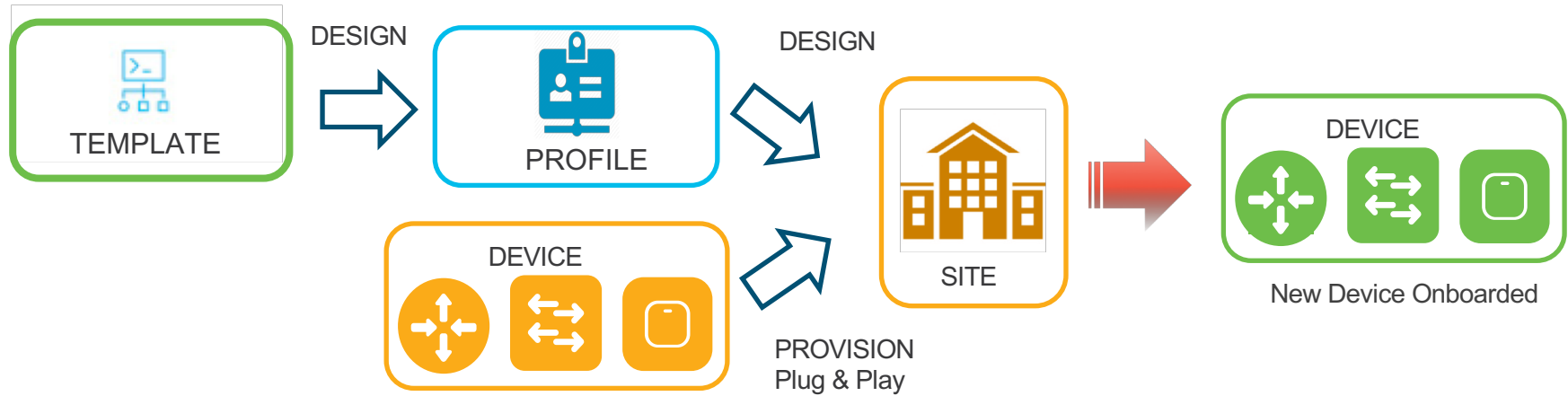


# Onboarding new devices using profiles

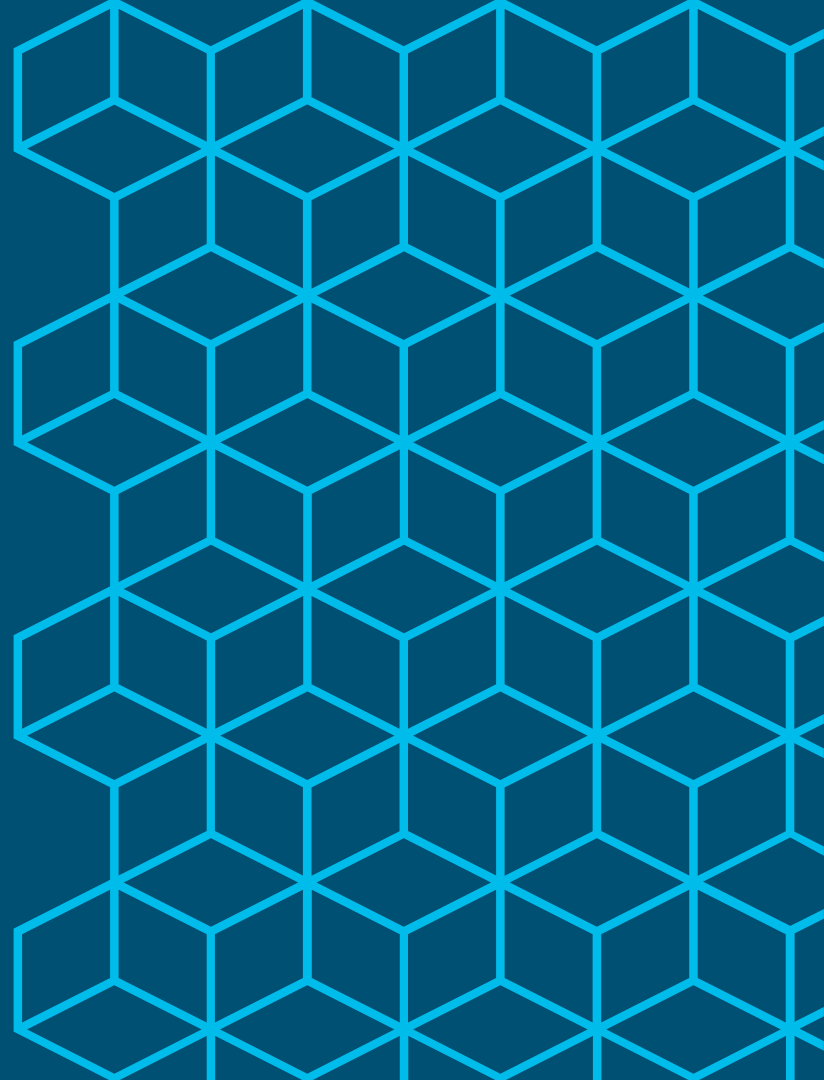


```
Template
35 no ip address
36 shutdown
37 !
38 interface Vlan64
39 ip address 10.10.64.7 255.255.255.0
40 no shut
41 !
42 ip default-gateway 10.10.64.1
43 ip http client source-interface Vlan64
44 ip route 0.0.0.0 0.0.0.0 10.10.64.1
45 !
46 !
47 ip ssh version 2
48 !
49 snmp-server community cisco R0
50 snmp-server community cisco123 RW
51 !
52 !
53 !
54 line vty 0 4
55
56 login local
57
58 transport input ssh
59
60
61 !
62 line vty 5 15
63
64 login local
65
66 transport input ssh
67
68 !
69 !
70 ntp server 10.2.254.1
71 !
72 !
```

# Onboarding new devices using profiles



## Use Case #2 - SWIM



# Complete support for SWIM Workflow

How to interpret the colors

Indicates ITSM Process Steps

Actions outside of NMS, mostly manual

Steps covered in NMS Tool

Steps covered in Cisco DNA-C

## General Steps to Update Software Image Update

Plan a Image Upgrade

Select Golden Image

Identify devices to upgrade

Create a Change Request

Approval of CR

Pre-Check validations

Distribute Image

Activate Image

Post Upgrade Validation

Close CR

## Traditional NMS Software Image Update

Plan a Image Upgrade

Select Golden Image

Identify devices to upgrade

Create a Change Request

Approval of CR

Pre-Check validations

Distribute Image

Activate Image

Post Upgrade Validation

Close CR

## Cisco DNA Center Software Image Update

Plan a Image Upgrade

Select Golden Image

Identify devices to upgrade

Create a Change Request

Approval of CR

Pre-Check validations

Distribute Image

Activate Image

Post Upgrade Validation

Close CR

# Software Upgrade Workflow: Recommended Images

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco Catalyst 36xx stack-able ethernet switch	cat3k_caa-universalk9.16.06.03.SPA.bin	2	Everest-16.6.3 (Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9ldpe.16.03.06.SPA.bin	0	Denali-16.3.6 (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9ldpe.SPA.03.06.08.E.152-2...	0	3.6.8E (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9.SPA.03.06.08.E.152-2.E8...	0	3.6.8E (Suggested, Latest) Add On (N/A)	★	+	🗑️

## Recommended Images:

- Cisco DNA Center can display the Cisco-recommended software images for the devices that it manages (by device type).
- Cisco Credentials are required
- If the recommended Golden Image is selected as Golden, Cisco DNA Center automatically uploads from cisco.com.

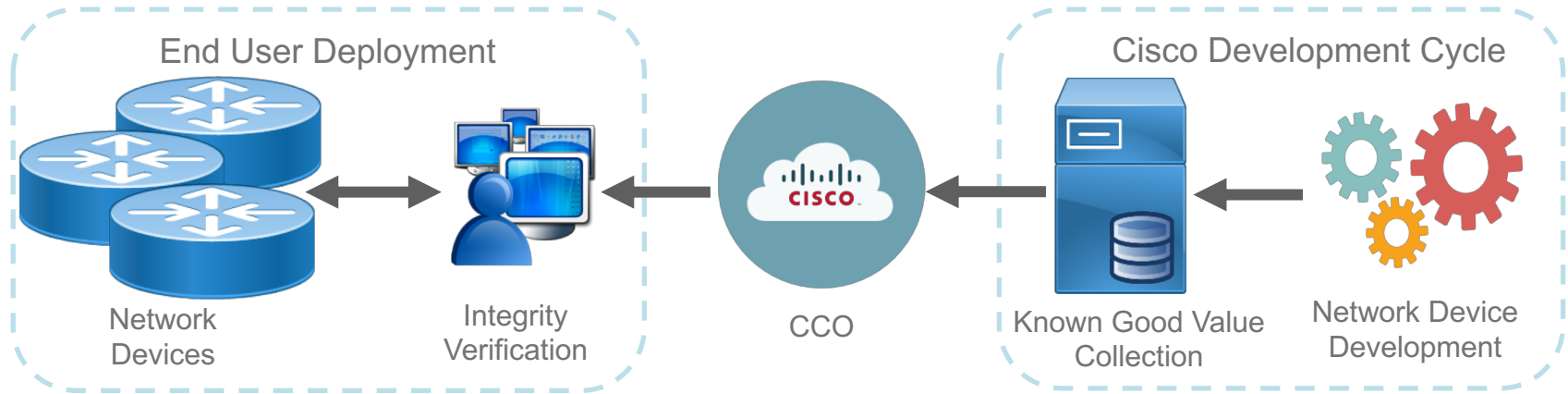
# Software Upgrade Workflow: Image Repository

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco Catalyst 36xx stack-able ethernet switch	cat3k_caa-universalk9.16.06.03.SPA.bin Unable to verify	2	16.6.3 (Latest) Add On (N/A)	☆	+ DISTRIBUTION ☆	🗑️
	cat3k_caa-universalk9ldpe.16.03.06.SPA.bin	0	Denali-16.3.6 (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9ldpe.SPA.03.06.08.E.152-2...	0	3.6.8E (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9.SPA.03.06.08.E.152-2.E8....	0	3.6.8E (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9.16.03.06.SPA.bin	0	Denali-16.3.6 (Suggested, Latest) Add On (N/A)	★	+	🗑️
	cat3k_caa-universalk9.16.08.01a.SPA.bin Unable to verify	0	16.8.1a (Latest) Add On (N/A)	★	+ Importing ○	🗑️

When are images uploaded into the Image Repository:

- Images can be uploaded directly from the device, from cisco.com (using the Recommended Images functionality) and via manual upload.
- When using manual upload, image is uploaded into the image repository automatically
- Images from devices and recommended images are only uploaded into the image repository when they are marked Golden

# Software Upgrade – Integrity Verification

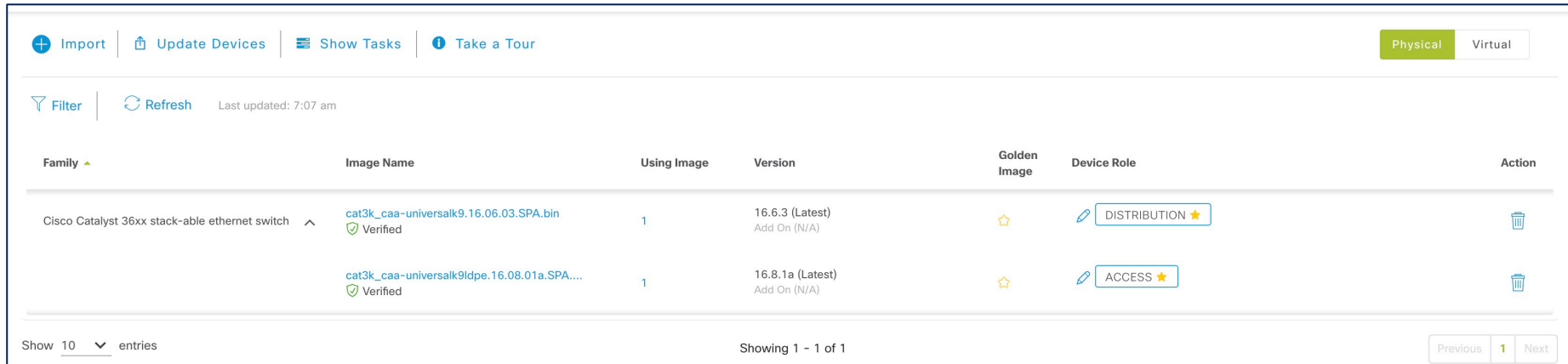


**Software** Is the software used by the device authentic? Includes checks of the software files (Known Good Value) and in-memory (Imprint Value) contents. Also includes shell access attempts (Event Occurrence)



# Software Upgrade – Integrity Verification

- To provide a level of security integrity devices must run authentic and valid software
- Cisco DNA Center Integrity Verification uses a system to compare collected image integrity data to Known Good Values (KGV) for Cisco software.
- Cisco produces and publishes a KGV Data file that contains KGV's for many of its products.
- The MD5 or SHA values of the images are validated against KGV's.

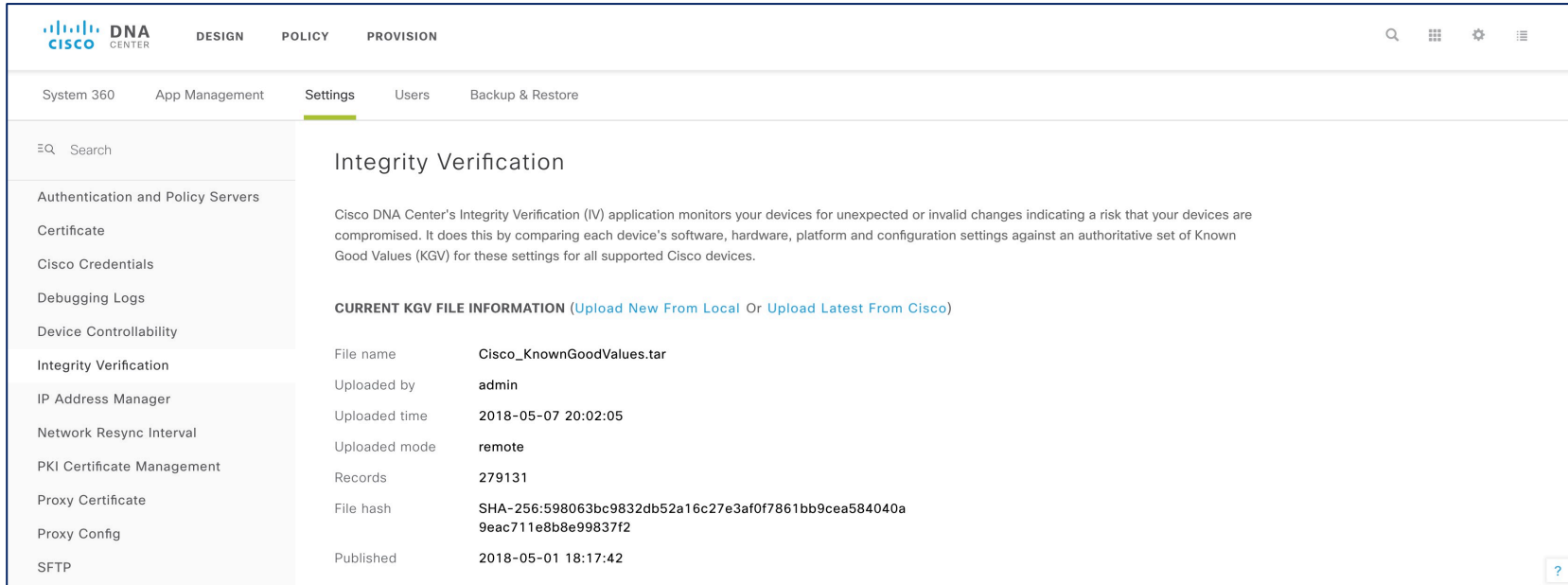


The screenshot displays the Cisco DNA Center Integrity Verification interface. At the top, there are navigation links: 'Import', 'Update Devices', 'Show Tasks', and 'Take a Tour'. A 'Physical' button is highlighted in green, and a 'Virtual' button is next to it. Below the navigation, there is a 'Filter' button, a 'Refresh' button, and a timestamp 'Last updated: 7:07 am'. The main content is a table with the following columns: Family, Image Name, Using Image, Version, Golden Image, Device Role, and Action. The table contains two entries for 'Cisco Catalyst 36xx stack-able ethernet switch'. The first entry is for image 'cat3k\_caa-universalk9.16.06.03.SPA.bin' with version '16.6.3 (Latest)' and role 'DISTRIBUTION'. The second entry is for image 'cat3k\_caa-universalk9ldpe.16.08.01a.SPA...' with version '16.8.1a (Latest)' and role 'ACCESS'. Both images are marked as 'Verified' and have a '1' in the 'Using Image' column. The bottom of the interface shows 'Show 10 entries' and 'Showing 1 - 1 of 1'.

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco Catalyst 36xx stack-able ethernet switch	cat3k_caa-universalk9.16.06.03.SPA.bin Verified	1	16.6.3 (Latest) Add On (N/A)	☆	DISTRIBUTION ☆	🗑️
	cat3k_caa-universalk9ldpe.16.08.01a.SPA... Verified	1	16.8.1a (Latest) Add On (N/A)	☆	ACCESS ☆	🗑️

# Software Upgrade – Integrity Verification

- KGV file:
  - Standard JSON format and Signed by Cisco
  - Can be retrieved from Cisco and uploaded into Cisco DNA Center



The screenshot displays the Cisco DNA Center web interface. The top navigation bar includes the Cisco DNA Center logo and tabs for DESIGN, POLICY, and PROVISION. Below this, a secondary navigation bar shows System 360, App Management, Settings (highlighted), Users, and Backup & Restore. A search bar is located on the left side of the main content area. The main content area is titled "Integrity Verification" and contains a descriptive paragraph about the application's function. Below the description, there is a section for "CURRENT KGV FILE INFORMATION" with a table of details.

Authentication and Policy Servers

- Certificate
- Cisco Credentials
- Debugging Logs
- Device Controllability
- Integrity Verification**
- IP Address Manager
- Network Resync Interval
- PKI Certificate Management
- Proxy Certificate
- Proxy Config
- SFTP

Integrity Verification

Cisco DNA Center's Integrity Verification (IV) application monitors your devices for unexpected or invalid changes indicating a risk that your devices are compromised. It does this by comparing each device's software, hardware, platform and configuration settings against an authoritative set of Known Good Values (KGV) for these settings for all supported Cisco devices.

**CURRENT KGV FILE INFORMATION** ([Upload New From Local](#) Or [Upload Latest From Cisco](#))

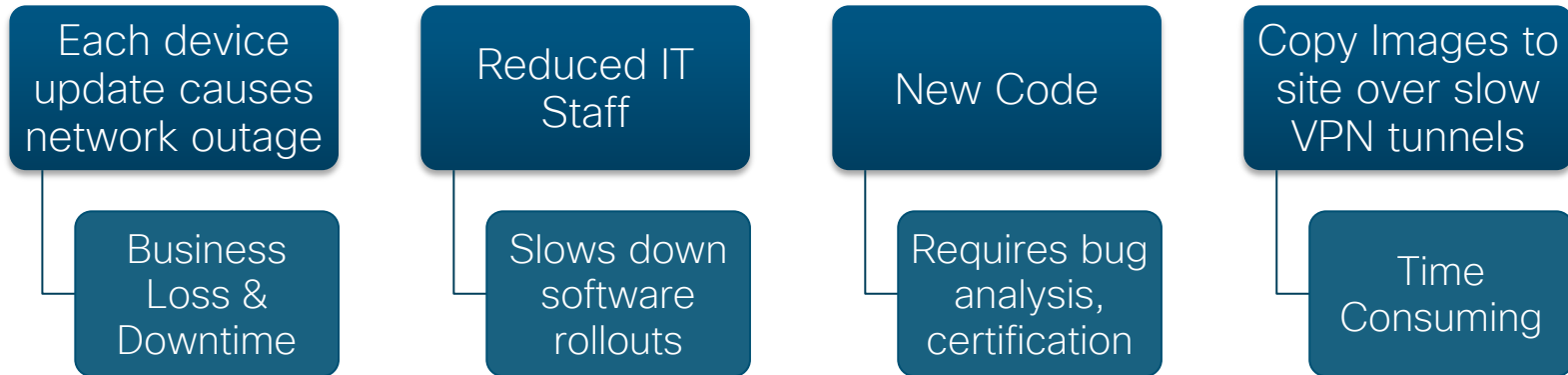
File name	Cisco_KnownGoodValues.tar
Uploaded by	admin
Uploaded time	2018-05-07 20:02:05
Uploaded mode	remote
Records	279131
File hash	SHA-256:598063bc9832db52a16c27e3af0f7861bb9cea584040a9eac711e8b8e99837f2
Published	2018-05-01 18:17:42

# SMU (Software Maintenance Update)

## What is SMU ?

- Point Fixes for the IOS-XE images (16.x onwards)
- Provides the ability to just update what is needed

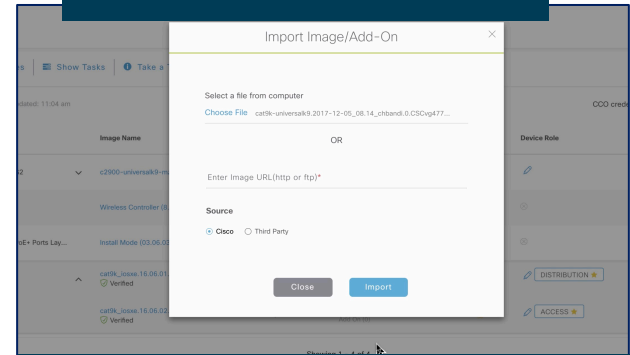
## Why SMU ?



# SMUs in Cisco DNA Center

## Step 1: Upload SMU

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco 2921 Integrated Services Router G2	c2900-universalk9-mz.SPA.155-3.M.bin	1	15.5(3)M Add On (N/A)	*		
Cisco 5508 Wireless LAN Controller	Wireless Controller (8.5.124.43)	1	8.5.124.43 Add On (N/A)			
Cisco Catalyst 3850 24P 10/100/1000 PoE+ Ports Lay...	Install Mode (03.06.03E)	1	03.06.03E Add On (N/A)			
Cisco Catalyst 9300 Switch	cat9k_iosxe.16.06.01.SPA.bin Verified	1	16.6.1 Add On (0)		DISTRIBUTION	
	cat9k_iosxe.16.06.02.SPA.bin Verified	1	16.6.2 Add On (0)		ACCESS	



## Step 3: Mark SMU as Golden

## Step 2: SMU is automatically associated with corresponding image

Family	Image Name	Using Image	Version	Image	Device Role	Action
Cisco 2921 Integrated Services Router G2	c2900-universalk9-mz.SPA.155-3.M.bin	1	15.5(3)M Add On (N/A)	*		
Cisco 5508 Wireless LAN Controller	Wireless Controller (8.5.124.43)	1	8.5.124.43 Add On (N/A)			
Cisco Catalyst 3850 24P 10/100/1000 PoE+ Ports Lay...	Install Mode (03.06.03E)	1	03.06.03E Add On (N/A)			
Cisco Catalyst 9300 Switch	cat9k_iosxe.16.06.01.SPA.bin Verified	1	16.6.1 Add On (0)		DISTRIBUTION	
	cat9k_iosxe.16.06.02.SPA.bin Verified	1	16.6.2 Add On (1)		ACCESS	

Family : Cisco Catalyst 9300 Switch  
Image Name : cat9k\_iosxe.16.06.02.SPA.bin

Using Image

SMU (1) Sub-package (0)

- cat9k-universalk9.2017-12-05\_08\_14\_chbandi.0.CSCvg4772.SSA.smu.bin

Description : Cisco IOS-XE Patch package  
Defect ID : CSCvg47772  
Reboot Required : Yes  
Category : bulk-patch  
Supersedes : Not Available  
Compliant Devices : 0  
Image Verification : Unable to verify image using the current KGV file. Click here to see the KGV file used or upload an updated one

Showing : Device Role : ACCESS

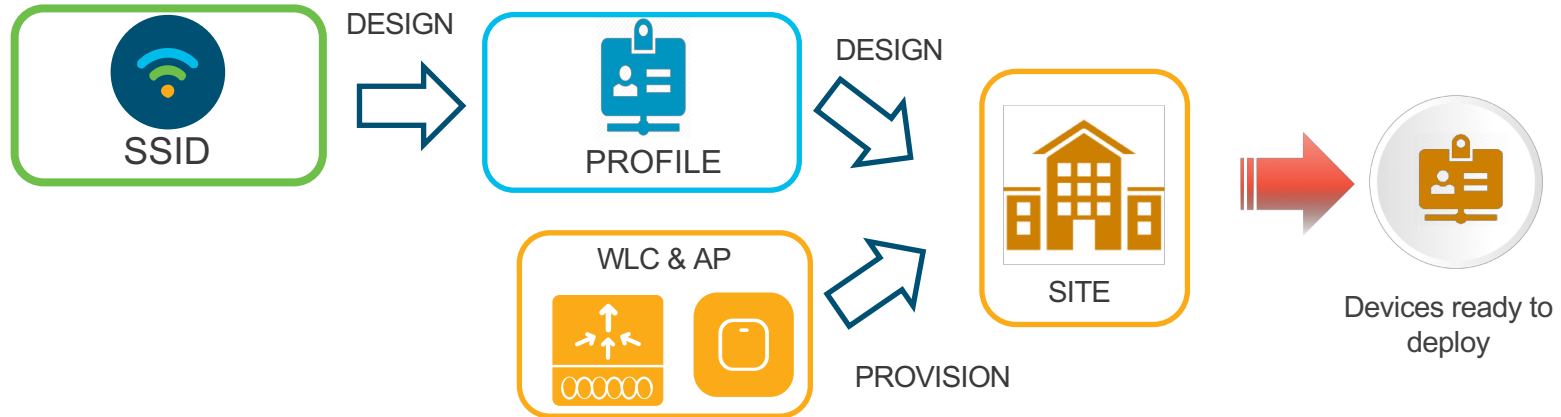
# Use Case #3 - Wireless Deployment



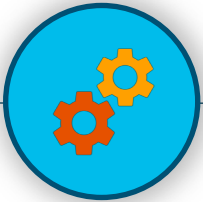
# Use Case #3: Wireless Deployment Made Simple



SSIDs and RF Parameters that represent wireless network



# Same Workflows for different Wireless Branch Deployments



## Centralized

Ease of Deployment  
and management



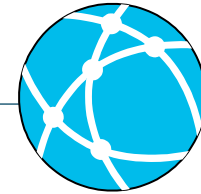
## Flex Connect

Eliminate the need  
for a Controller at  
every Site



## Mobility Express

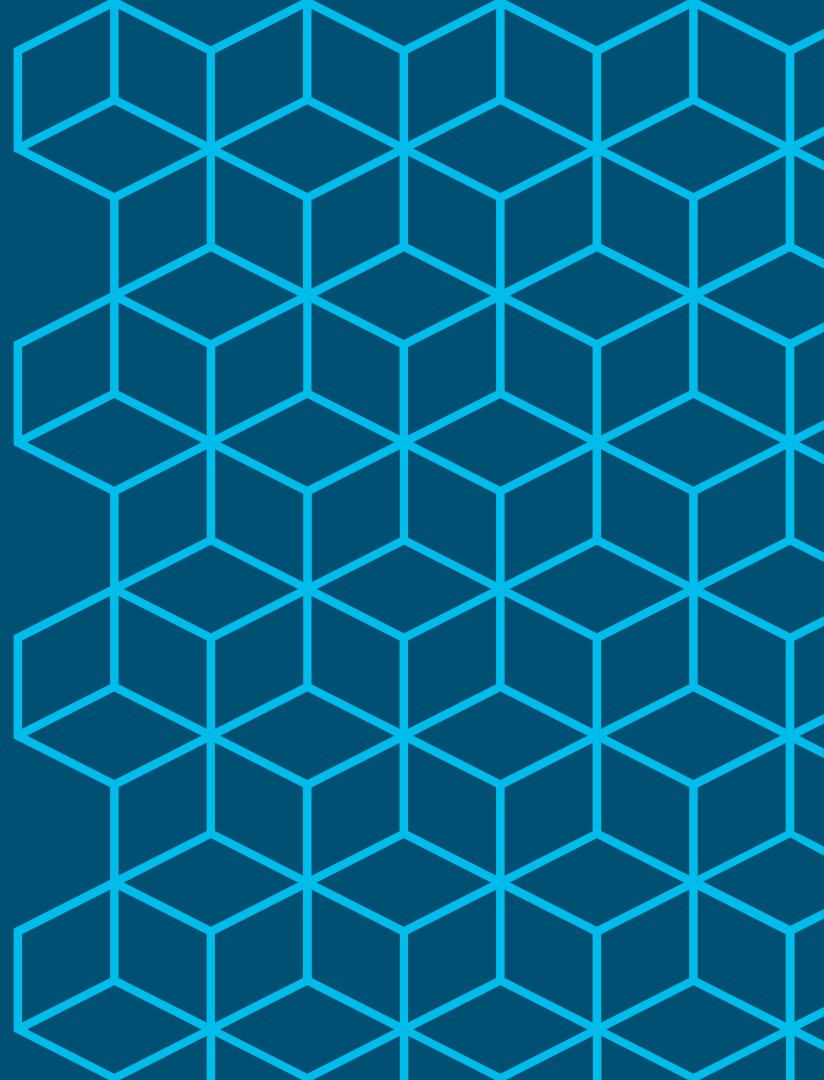
Controller  
Functionality  
Embedded in the  
Access Point



## Catalyst WLC

Next Gen  
WLC

# Use Case #4 - Application Policy



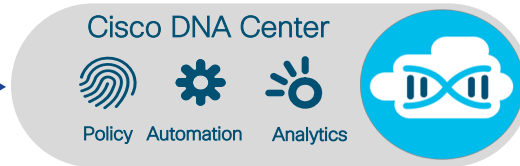


# Application Policy

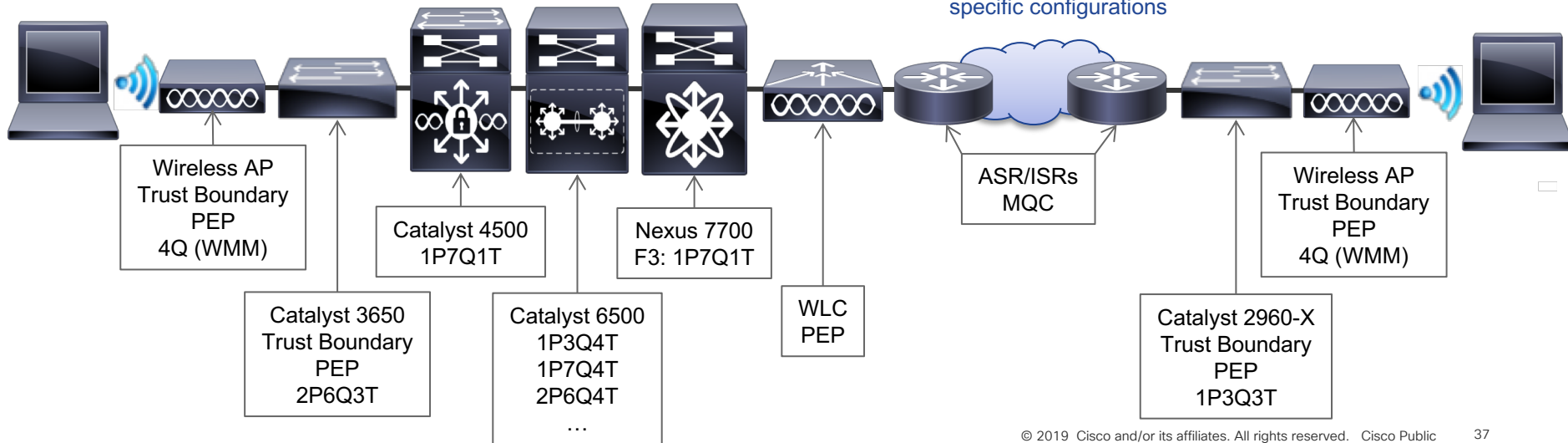


Applications can interact with Cisco DNA Center via Northbound APIs, informing the network of application-specific and dynamic QoS requirements

Network Operators express high-level business-intent to Cisco DNA Center Application Policy



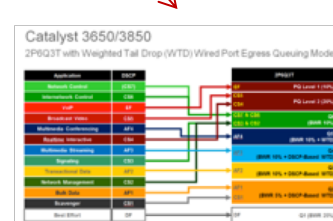
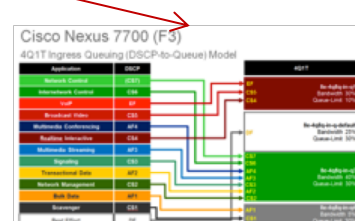
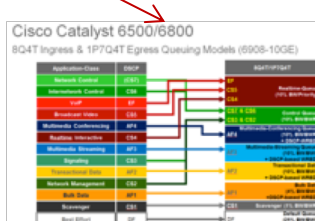
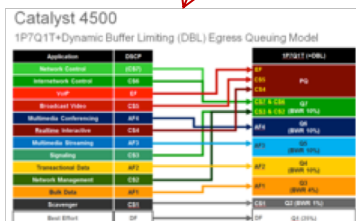
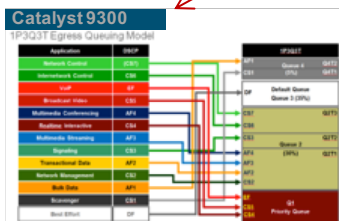
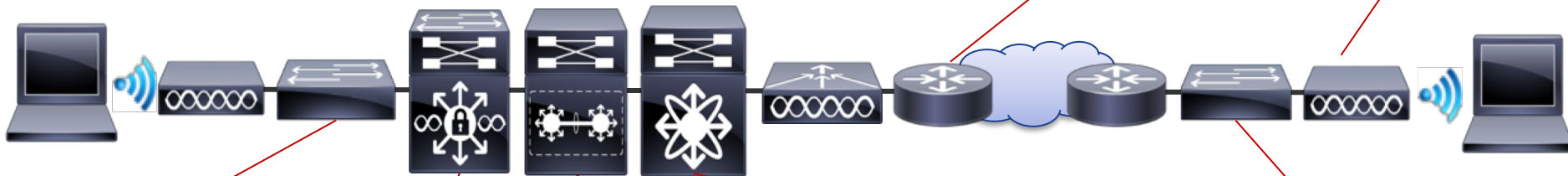
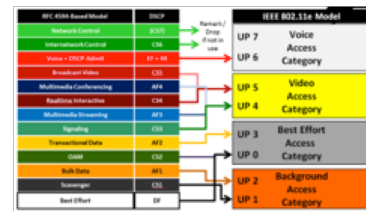
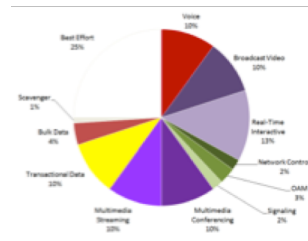
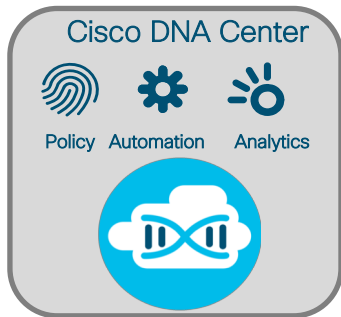
Southbound APIs translate business-intent to platform-specific configurations



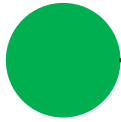
# Application Policy Leverages QoS CVDs

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

Application Policy in Cisco DNAC will **seamlessly interconnect all types of hardware and software queueing models** to achieve consistent and compatible end-to-end treatments aligned with the expressed business-intent

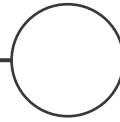


# Solicit Application Business-Relevance



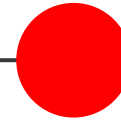
Relevant

- These applications directly supports business objectives
- Applications should be classified and marked according to **RFC 4594**-based rules



Default

- 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**)

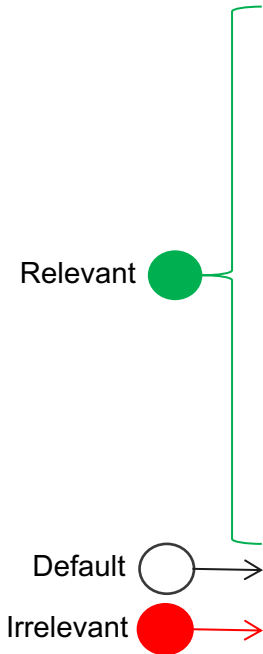


Irrelevant

- 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 , per (**RFC 3662**)

# What Do We Do Under-the-Hood?

Apply RFC 4594-based Marking / Queuing / Dropping Treatments



Application Class	Per-Hop Behavior	Queuing & Dropping	Application Examples
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
Signaling	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 Forwarding	DF	Default Queue + RED	Default Class
Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

# Application Policy Workflow

## Based on Business Relevance for the applications

The screenshot displays the Cisco DNA Center interface for Policy Administration. The top navigation bar includes 'DESIGN', 'POLICY', 'PROVISION', and 'ASSURANCE'. The 'POLICY' section is active, showing 'Policy Administration' and 'Registry' tabs. The main content area is titled 'Application Policies' and features a search bar and a 'Host Tracking' toggle set to 'Off'. The policies are organized into three columns: 'Business Relevant (16)', 'Default (6)', and 'Business Irrelevant (6)'. Each policy card shows the name and the number of applications it covers. A 'Feedback' button is visible on the right side of the interface.

**Policy Administration** Registry

**Application Policies**

Application Policy Name\* \_\_\_\_\_

Site Scope 0 Sites LAN Queuing Profiles CVD\_QUEUING\_PROFILE SP Profiles 0 Profiles Host Tracking  Off

EQ \_\_\_\_\_

**Business Relevant (16)**

- Authentication-Services (39 applications)
- Backup-And-Storage (14 applications)
- Collaboration-Apps (42 applications)
- Database-Apps (33 applications)
- Desktop-Virtualization-Apps (18 applications)
- Email (29 applications)
- Enterprise-Ipc (20 applications)

**Default (6)**

- File-Sharing (32 applications)
- General-Browsing (9 applications)
- General-Media (12 applications)
- General-Misc (485 applications)
- Software-Updates (15 applications)
- Tunneling (20 applications)

**Business Irrelevant (6)**

- Consumer-Browsing (223 applications)
- Consumer-File-Sharing (38 applications)
- Consumer-Gaming (15 applications)
- Consumer-Media (98 applications)
- Consumer-Misc (9 applications)
- Consumer-Social-Networking (13 applications)

**Unassigned Application Sets (1)**

- Custom-Apps (1 applications)

Feedback

# Application Policy Workflow

## Deploy Policy based on Site

The screenshot displays the Cisco DNA Center interface for Policy Administration. The main view shows a list of application policies categorized into 'Business Relevant' and 'Default'. A 'Site Scope' dialog is open on the right, showing a tree view of site categories.

**Policy Administration** | Registry

**Application Policies**

Application Policy Name\*  
Branch-App-Policy

Site Scope 1 Sites | LAN Queuing Profiles CVD\_QUEUING\_PROFILE | SP Profiles 0 Profiles | Host Tracking  Off

**Business Relevant (16)**

- Authentication-Services (39 applications)
- Backup-And-Storage (14 applications)
- Collaboration-Apps (42 applications)
- Database-Apps (33 applications)
- Desktop-Virtualization-Apps (18 applications)
- Email (29 applications)
- Enterprise-Ipc (20 applications)

**Default (6)**

- File-Sharing (32 applications)
- General-Browsing (9 applications)
- General-Media (12 applications)
- General-Misc (485 applications)
- Software-Updates (15 applications)
- Tunneling (20 applications)

**Site Scope**

Find: Site | Show: All

- Global
- USA
- SJC
  - Campus
  - Branch

Buttons: Cancel, OK

Feedback

# Policy Overview for Device Role = Border Router

## Under the Hood – SP Profiles

Policy Provision Assurance

Image Repository Network Profiles Auth Template

Network Device Credentials IP Address Pools **SP Profiles** Wireless

QoS

Profile Name	WAN Provider	Model	
Demo-SP-Profile	Demo-WAN-Provider	Select...	+ Add

4 Class  
5 Class  
6 Class  
8 Class

Reset Save

CAMPUS-Dist2.cisco.com	DISTRIBUTION	Exclude Interfaces	N/A
CAMPUS-Access1	ACCESS	Exclude Interfaces	N/A
CAMPUS-Core1.cisco.com	DISTRIBUTION	Exclude Interfaces	N/A

Feedback

< Back to Devices in "SJC-Bldg-1"

### SP Profile Settings for Device "CAMPUS-Router1.cisco.com"

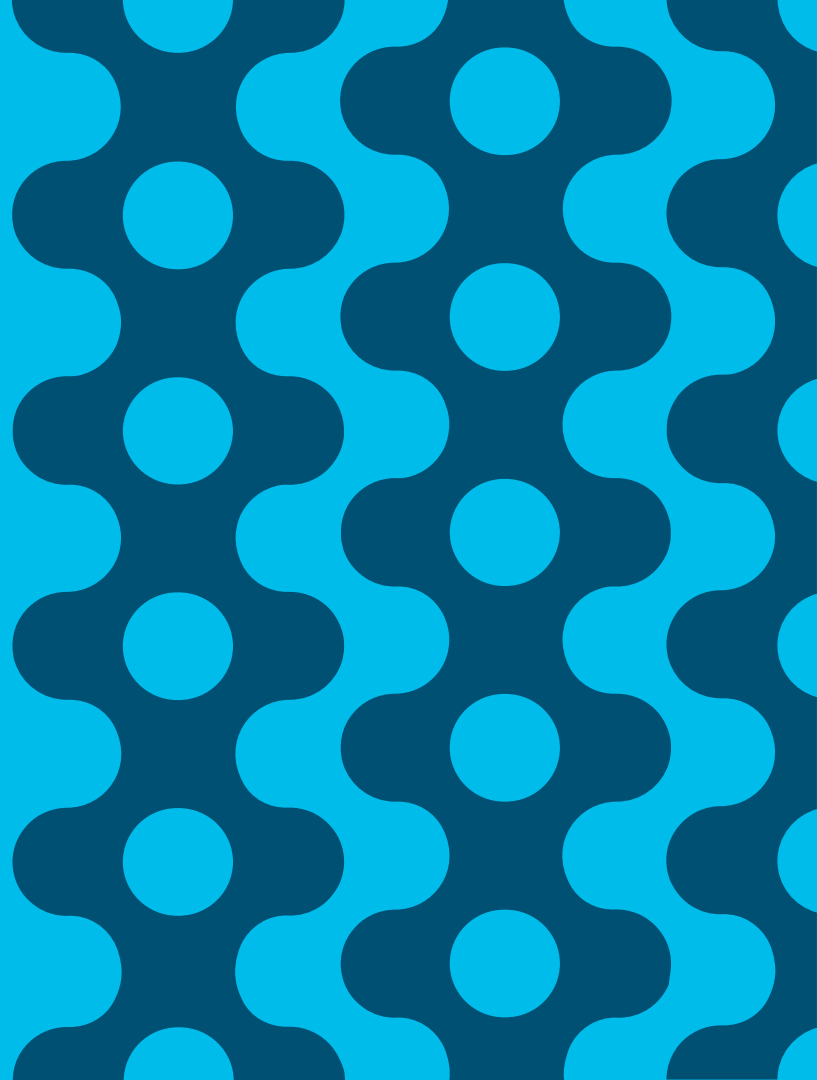
WAN Interface	Service Provider Profile	Upstream Bandwidth (Mbps)	
GigabitEthernet0/0/0	Demo-SP-Profile1	100	×
GigabitEthernet0/0/1	Demo-SP-Profile2	200	+

Cancel Save

Feedback

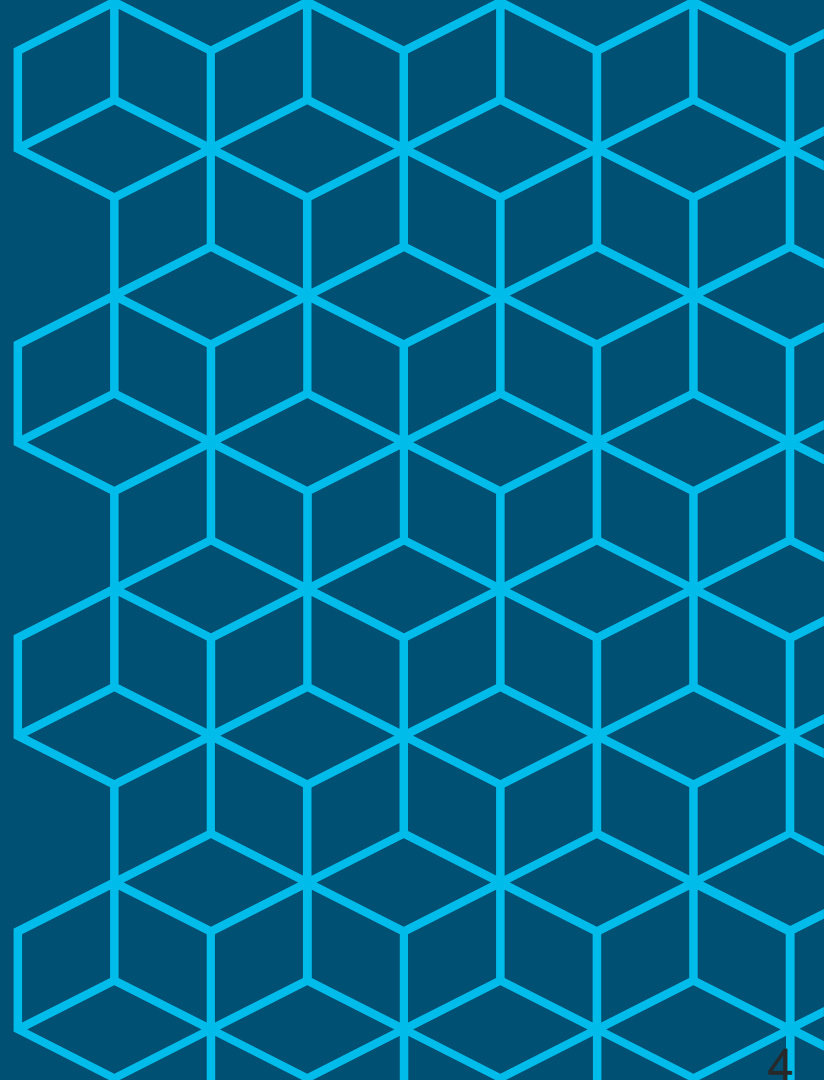
Router → WAN Interface → SP Profile → Upstream Bandwidth

# Cisco DNA Automation Demo - Templates



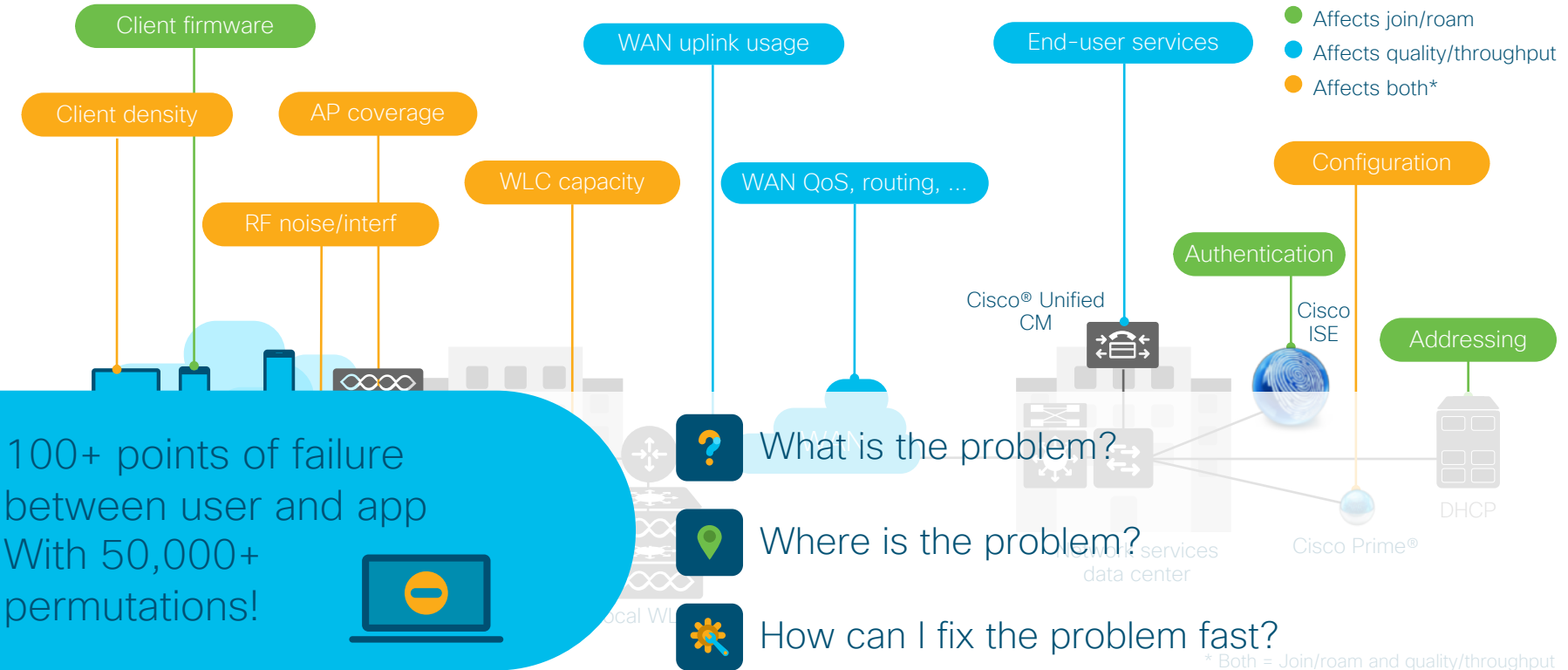


# Cisco DNA Assurance



# Network Quality

## A Complex, End-to-End Problem



# Today's Tools

Too Limited, and Do Not Address Network Needs



## Too Many Tools

- Fragmented visibility
- Closed interfaces / Silo'd views
- Devices queried multiple times
- Different protocols/mechanisms



## Reactive Systems

- Always playing catch up
- Not designed for analytics
- Inconsistent API architecture
- Specialized knowledge required



## Limited Insights

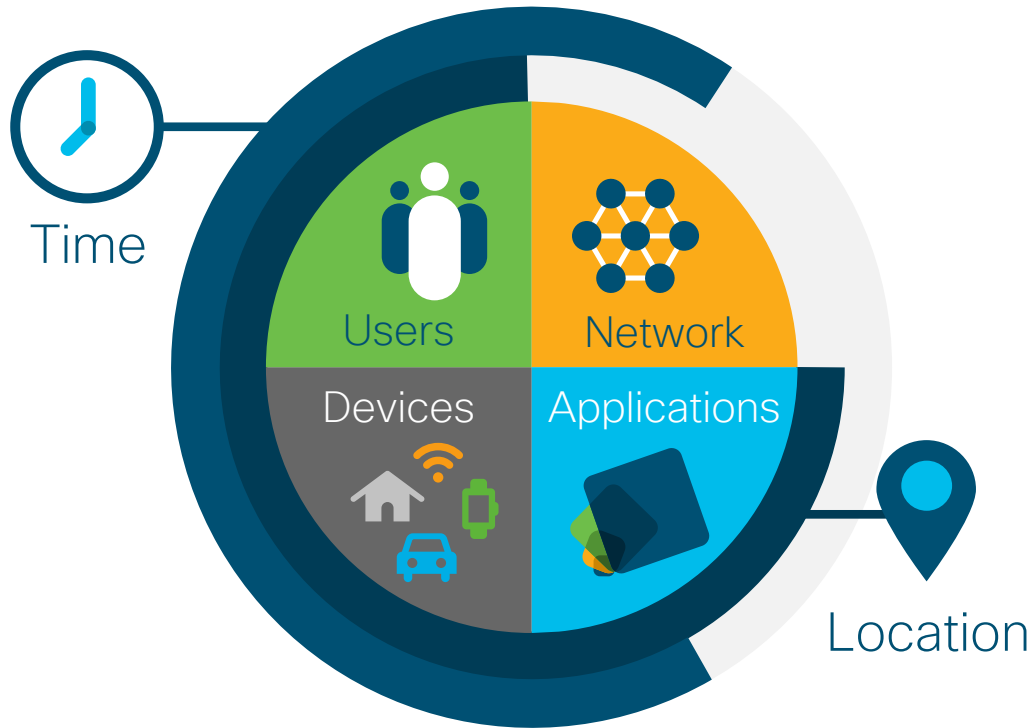
- Limited data that is not actionable
- My report vs your report
- No view of state changes
- Lacking context or feedback loop

Rigid

Closed/Proprietary

Lack of Intelligence

# Context is Key



## Cisco Context

360-degree Visibility



Data Granularity

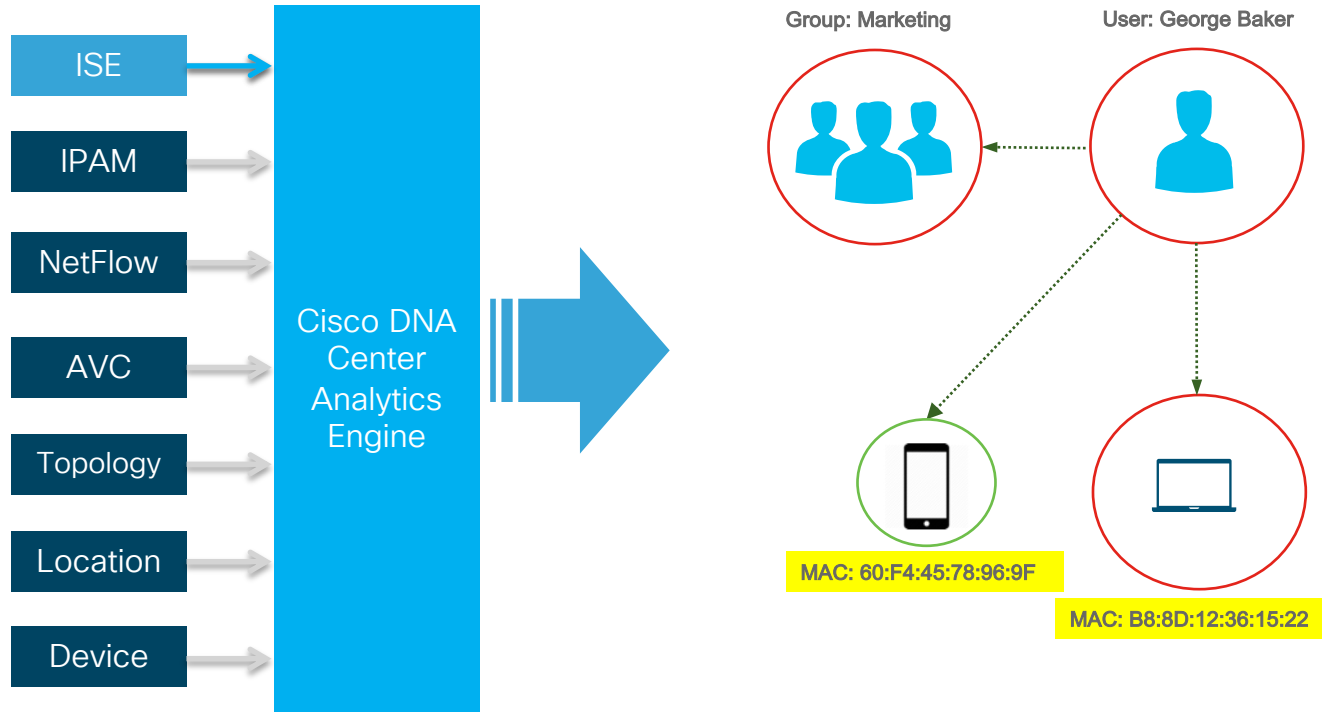


Historical, Real-time, Future

Rich Context Increase Business Productivity and Frees Up IT Time

# Delivering Context for Network Troubleshooting

## Use Case Example

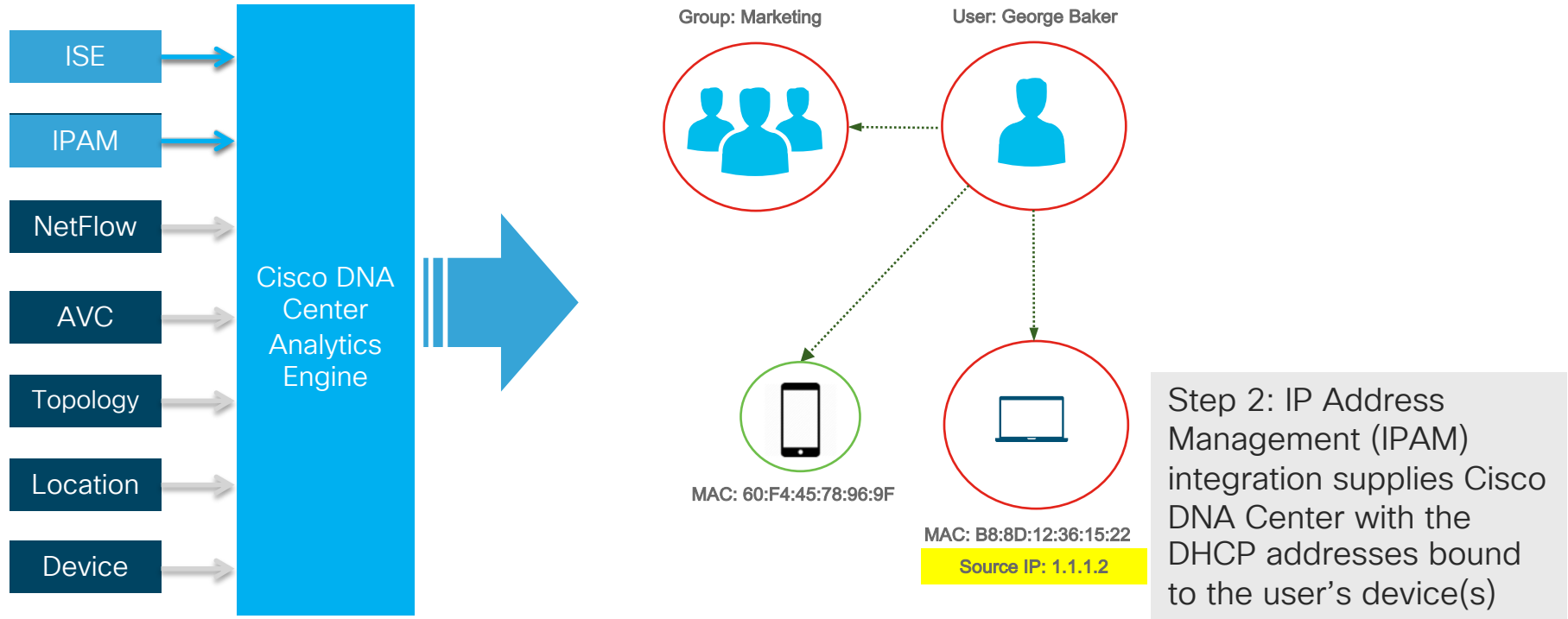


An unhappy user calls in to report a problem with his WebEx experience

Step 1: Identity Services Engine integration provides Cisco DNA Center with the user's information, group-policies and device information

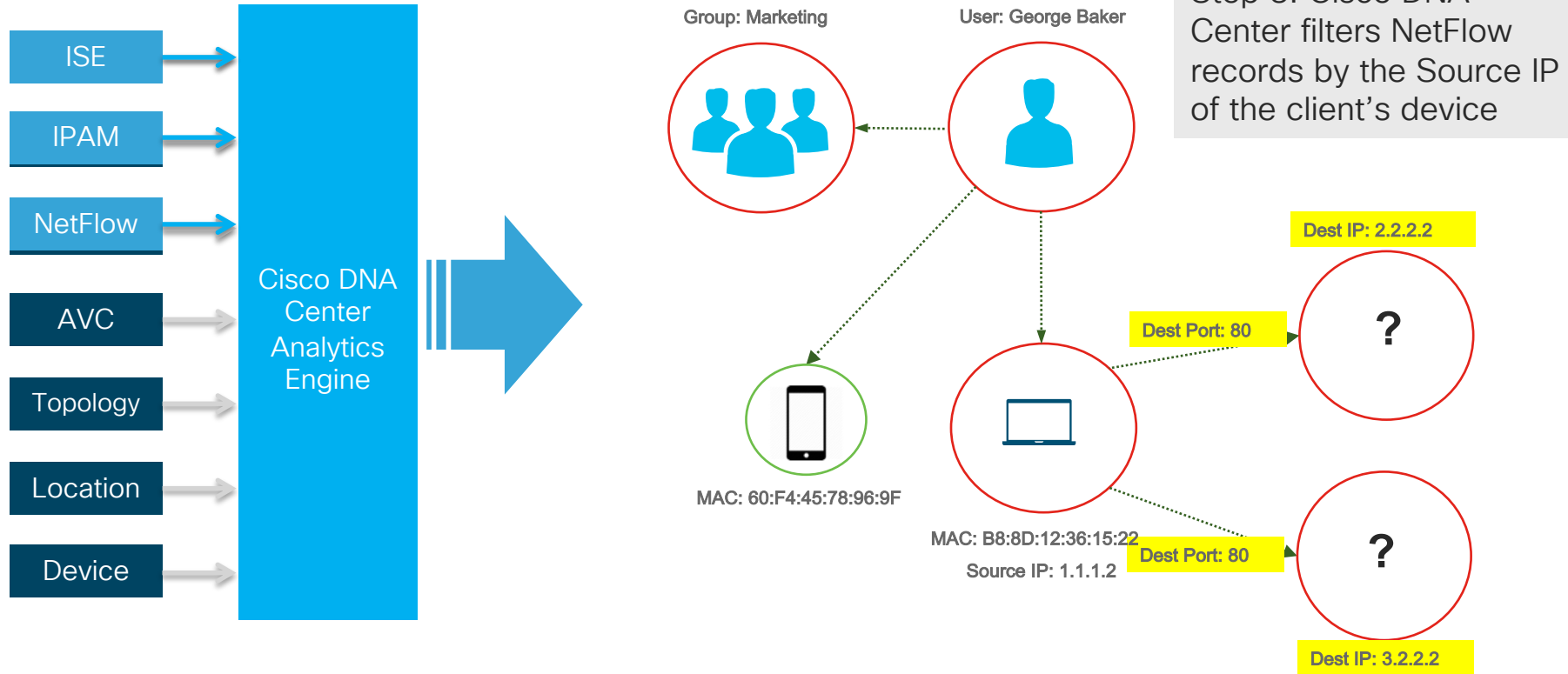
# Delivering Context for Network Troubleshooting

## Use Case Example



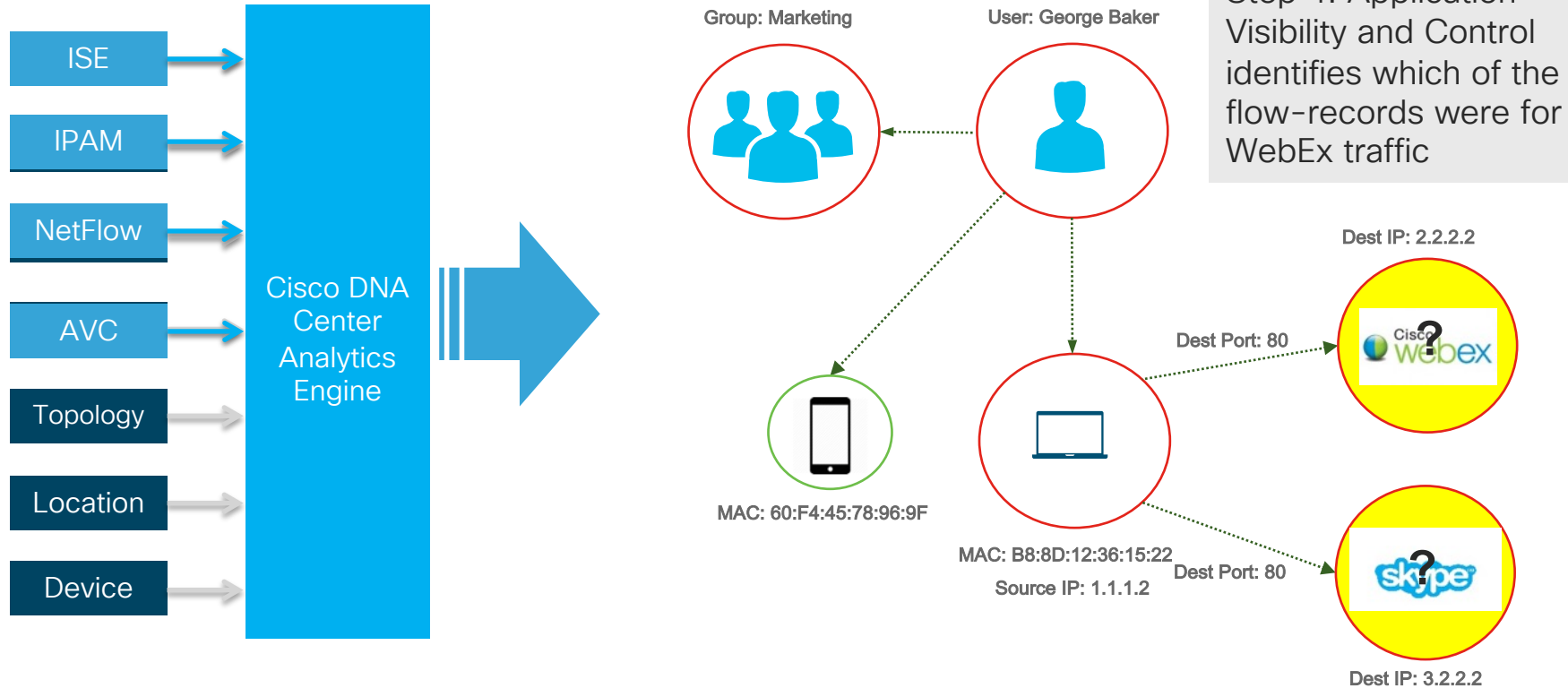
# Delivering Context for Network Troubleshooting

## Use Case Example



# Delivering Context for Network Troubleshooting

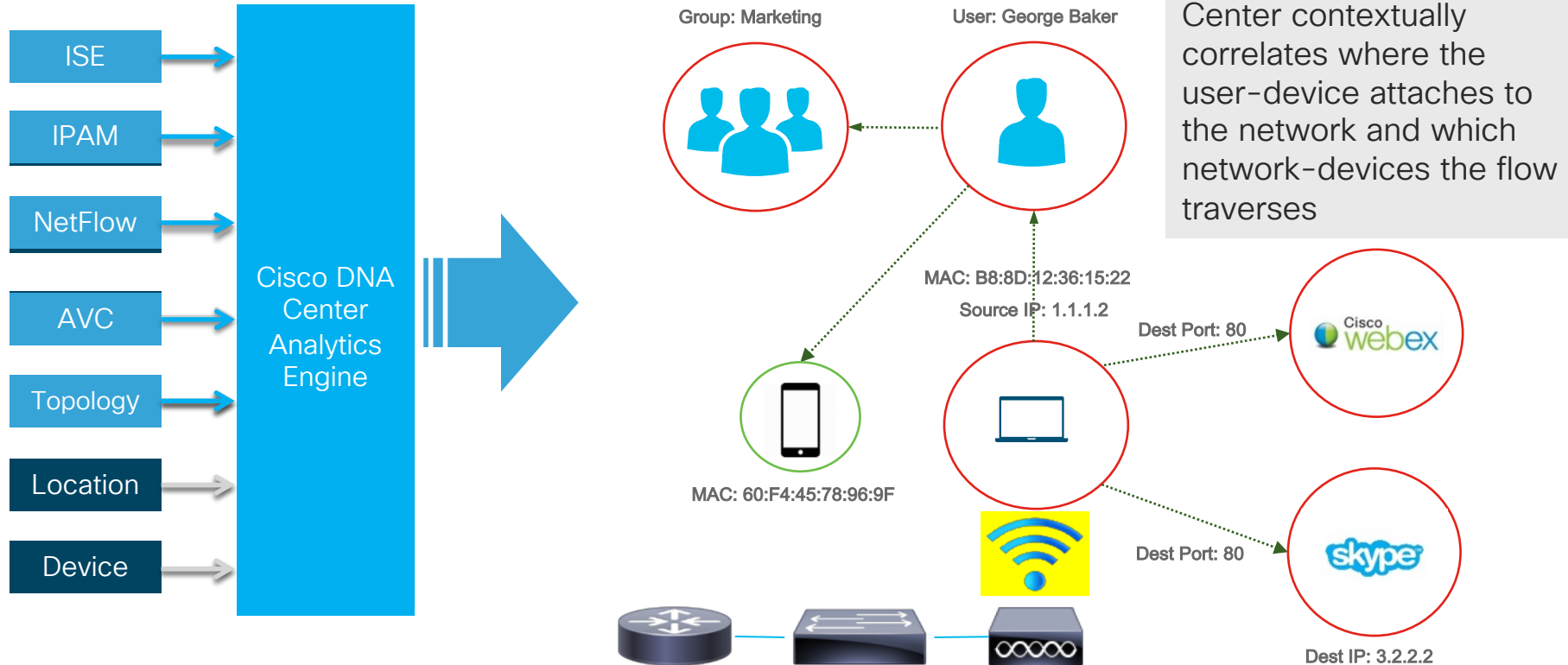
## Use Case Example





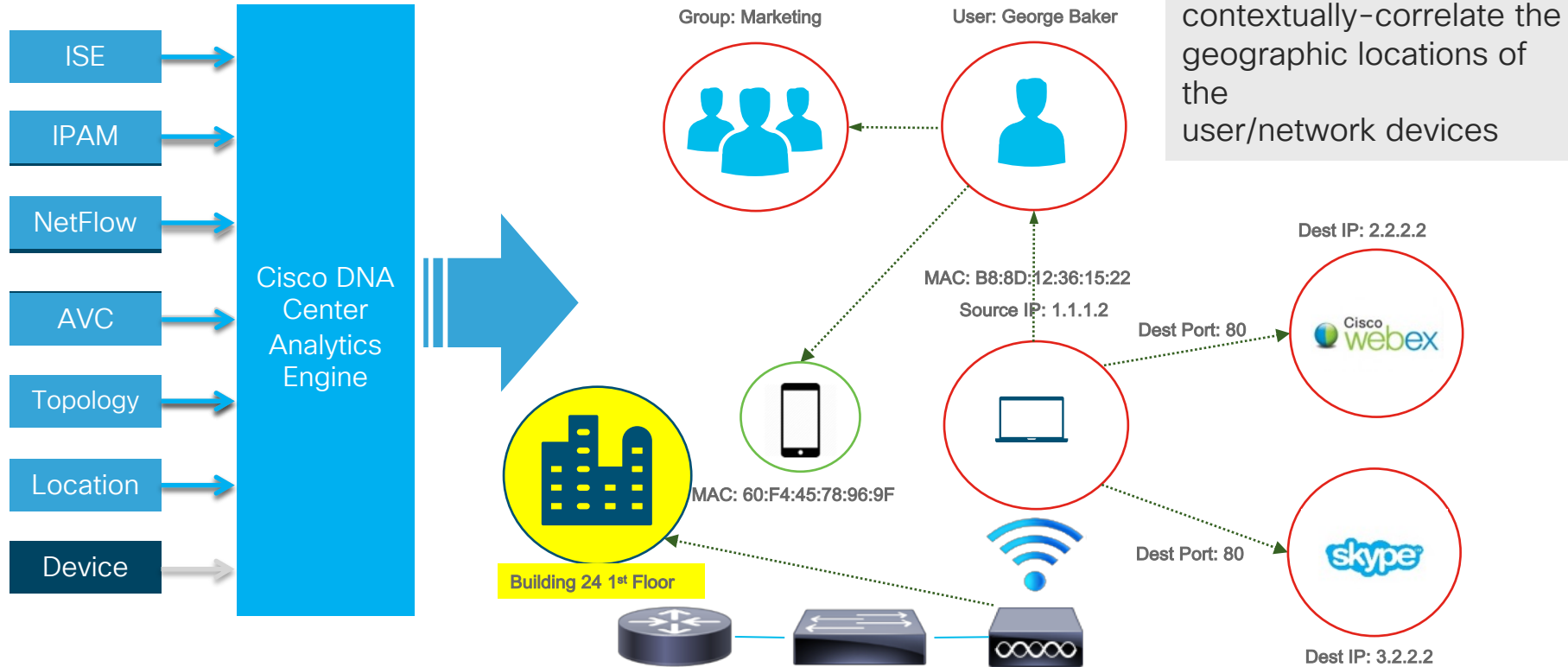
# Delivering Context for Network Troubleshooting

## Use Case Example



# Delivering Context for Network Troubleshooting

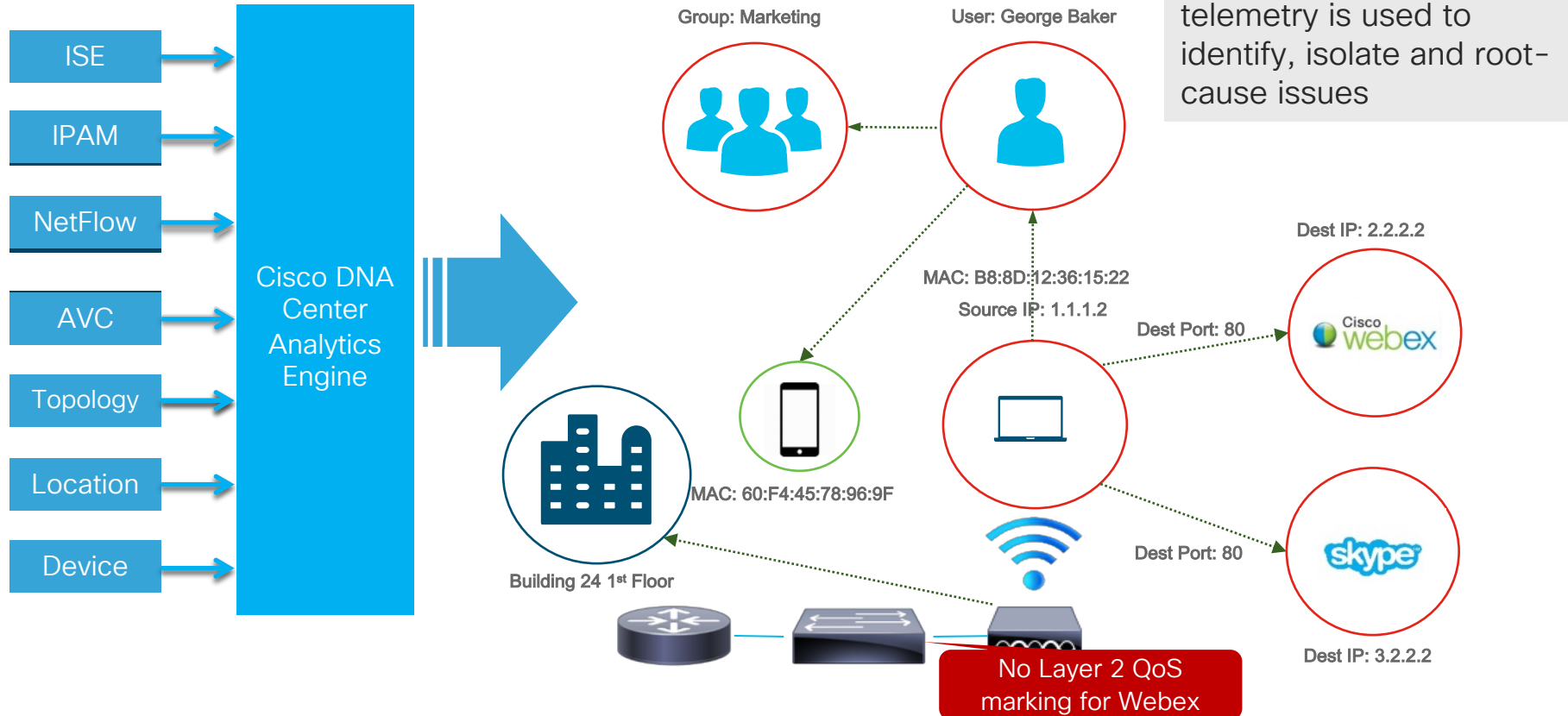
## Use Case Example



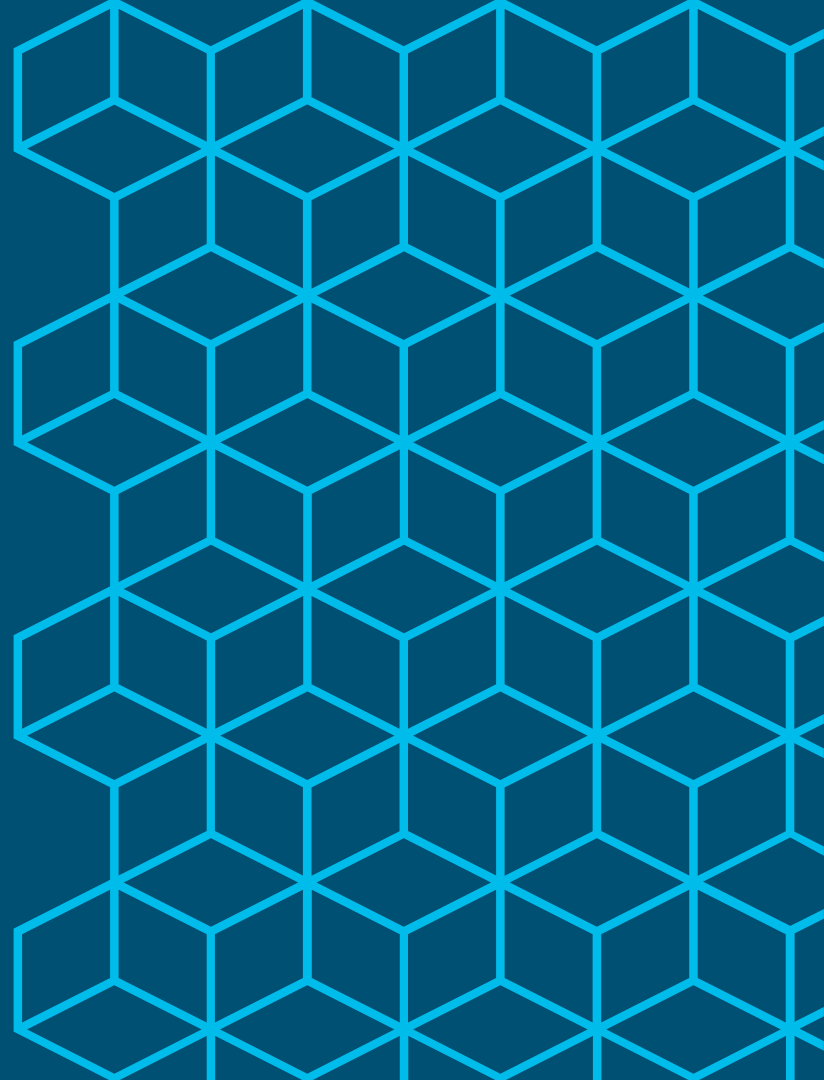
Step 6: Location services contextually-correlate the geographic locations of the user/network devices

# Delivering Context for Network Troubleshooting

## Use Case Example

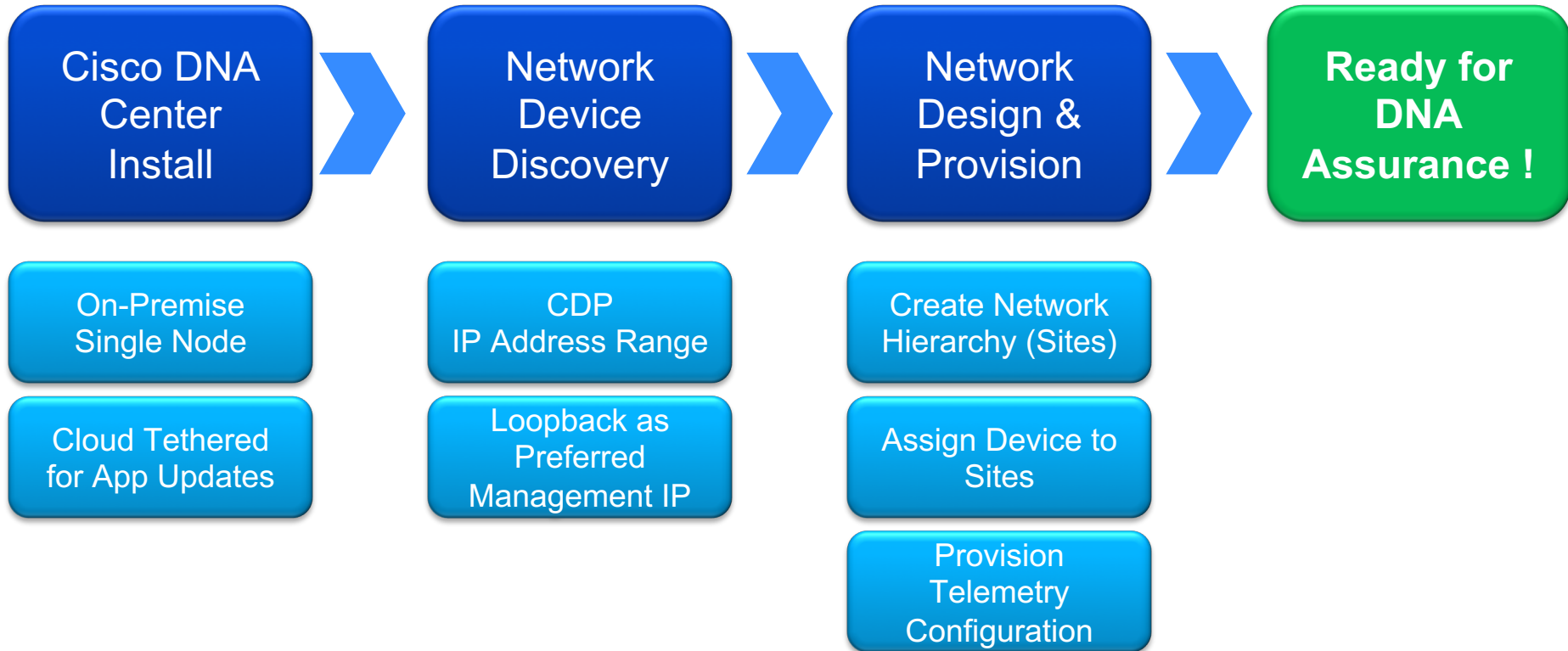


# Cisco DNA Assurance Getting Started Workflow



# Cisco DNA Assurance

## Getting Started Workflow



# Getting Started Workflow – Network Discovery

### SD-AccessSwitches

Delete Clone Edit **Start**

Complete 9

DISCOVERY DETAILS


<b>CDP LEVEL</b> ⓘ None	<b>PROTOCOL ORDER</b> ⓘ telnet ssh
<b>RETRY COUNT</b> ⓘ 3	<b>TIMEOUT</b> ⓘ 5
<b>IP RANGE</b> ⓘ 192.168.120.1- 192.168.120.5 192.168.130.1- 192.168.130.10 192.168.110.1- 192.168.110.10	<b>IP FILTER LIST</b> ⓘ None
<b>PREFERRED MANAGEMENT IP</b> ⓘ Use LoopBack	

### Devices

LIST

Filter  SUCCESS  UNREACHABLE  FAILURE

IP Address	Device Name	Status	ICMP	SNMP	CLI
192.168.130.1	border_cp	✓	✓	✓	✓
192.168.110.2	C6840-X-LE	✓	✓	✓	✓
192.168.130.2	asr1k-border	✓	✓	✓	✓
192.168.130.3	c9500	✓	✓	✓	✓
192.168.120.5	c9300	✓	✓	✓	✓
192.168.120.2	p1-edge2	✓	✓	✓	✓
192.168.120.1	p1-edge1	✓	✓	✓	✓
192.168.110.1	dist2	✓	✓	✓	✓
192.168.110.10	dist1	✓	✓	✓	✓



# Getting Started Workflow – Assign Devices to Sites

The screenshot shows the Cisco DNA Center interface in the Provision tab. The 'Device Inventory' section is active, displaying a table of devices. A dropdown menu is open over the 'Device' column, with the 'Assign Device to Site' option highlighted. The table lists five devices with their respective details.

Navigation: DESIGN, POLICY, **PROVISION**, ASSURANCE

Buttons: LAN Automation, LAN Auto Status

Inventory (36) Unclaimed Devices (0)

Network Telemetry Upgrade Status Refresh

Device	Address	Site	Serial Number	Uptime	OS Version	OS Image	Sync Status	Last Provision	Provision Status	
<input checked="" type="checkbox"/> AMS-AP3802-34	Unified AP	10.11.19.1	...MS/AMS-Level3	FCW2136NCCJ	15days 11:40:08.840	8.5.110.0	Not Available	Managed	-	Not Provisioned
<input checked="" type="checkbox"/> AMS-ASR1K-INET	Routers	10.11.255.2	...MS/AMS-Level3	FOX1817GSM2	45 days, 19:51:29.15	15.5(3)S2	asr1002x-univ... Tag Golden	Managed	-	Not Provisioned
<input checked="" type="checkbox"/> AMS-SW3650.test.com	Switches and Hubs	10.11.255.100	...MS/AMS-Level3	FDO1852E264	139 days, 10:16:58.88	03.06.05E	packages.conf Tag Golden	Managed	-	Not Provisioned
<input type="checkbox"/> ASR1K-CORE1	Routers	10.0.255.42	.../DC/DC-Level1	FOX1521G5SN	139 days, 10:09:03.84	15.5(3)S2	asr1000rp1-ad... Tag Golden	Partial Collection Failure	-	Not Provisioned
<input type="checkbox"/> ASR1K-CORE2	Routers	10.0.255.52	.../DC/DC-Level1	FOX1521G5SM	131 days, 18:20:44.51	15.5(3)S2	asr1000rp1-ad... Tag Golden	Partial Collection Failure	-	Not Provisioned

Feedback

# Getting Started Workflow – Telemetry Configuration

DESIGN
POLICY
PROVISION
ASSURANCE

Devices
Fabric

Device Inventory

LAN Automation
LAN Auto Status

Telemetry

Telemetry Assessment and Configuration

Site View
Profile View

Sites Hierarchy

- Global
- Canada
- TO
- Mexico
- Netherlands
- USA

Actions
Show All

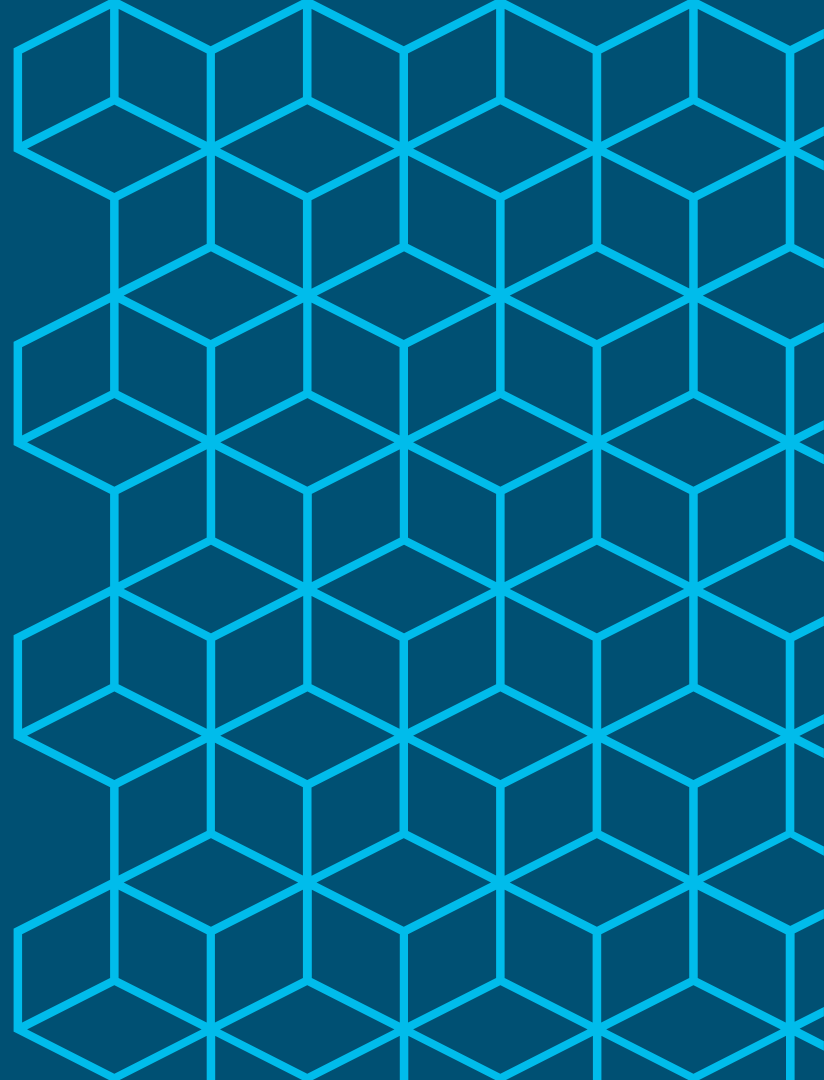
Device Na...	Address	Type	Family	Version	Profile	Details	
<input type="checkbox"/>	MX1-3850-ACC-1...	10.32.255.102	Cisco Catalyst38xx...	Switches and Hubs	16.6.2	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-3850-CSW-...	10.32.255.100	Cisco Catalyst38xx...	Switches and Hubs	16.6.2	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-3850-CSW-...	10.32.255.101	Cisco Catalyst38xx...	Switches and Hubs	16.6.2	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-9300-ACC-1...	10.32.255.103	Cisco Catalyst 930...	Switches and Hubs	16.6.2	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-ASR1001X-1...	10.32.255.1	Cisco ASR 1001-X...	Routers	16.6.1	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-ISR4431-3.c...	10.32.255.3	Cisco 4431 Integra...	Routers	15.5(3)S4b	Maximal Visibility	<span style="color: green;">i</span>
<input type="checkbox"/>	MX1-ISR4451-2.e...	10.32.255.2	Cisco 4451 Series ...	Routers	15.5(3)S4b	Maximal Visibility	<span style="color: green;">i</span>

Network Telemetry
Upgrade Status
Refresh

OS Version	OS Image	Sync Status	Last Provision	Provision Status
8.5.110.0	Not Available	Managed	-	Not Provisioned
15.5(3)S2	asr1002x-univ... <a href="#">Tag Golden</a>	Managed	-	Not Provisioned
03.06.05E	packages.conf <a href="#">Tag Golden</a>	Managed	-	Not Provisioned
15.5(3)S2	asr1000rp1-ad... <a href="#">Tag Golden</a>	Partial Collection Failure	-	Not Provisioned
15.5(3)S2	asr1000rp1-ad... <a href="#">Tag Golden</a>	Partial Collection Failure	-	Not Provisioned



# Cisco DNA Assurance Capabilities





# Cisco DNA Assurance

## Health Scores

Site Health Score

== **function** ( Client Health Score,  
Device Health Score )

Client Health Score

== **function** ( Onboarding Score,  
Connectivity Score )

Device Health Score

== **function** ( System Health Score,  
Control Plane Score,  
Data Plane Score )

Application Health Score

== **function** ( Traffic Class,  
Latency, Packet Loss )



Client 360

10/10 daphine.blake

Daphine-iPad Daphine-PC

This screenshot shows the 'Client 360' health score interface. At the top, it says 'Client 360'. Below that, there is a score of '10/10' with a blue information icon, followed by the name 'daphine.blake'. At the bottom, there are two device icons: 'Daphine-iPad' and 'Daphine-PC', both with green status indicators.



Device 360

6/10 AP LA1-AP3802-21 Global / USA / Los Angeles / Level 26

Device Model: AIR-AP3802I-B-K9 IP Address: 10.30.16.12 Software Version: 8.5.107.102

This screenshot shows the 'Device 360' health score interface. At the top, it says 'Device 360'. Below that, there is a score of '6/10' with a blue information icon and a star icon, followed by the device name 'AP LA1-AP3802-21' and location information 'Global / USA / Los Angeles / Level 26'. At the bottom, there is a line of technical details: 'Device Model: AIR-AP3802I-B-K9 IP Address: 10.30.16.12 Software Version: 8.5.107.102'.

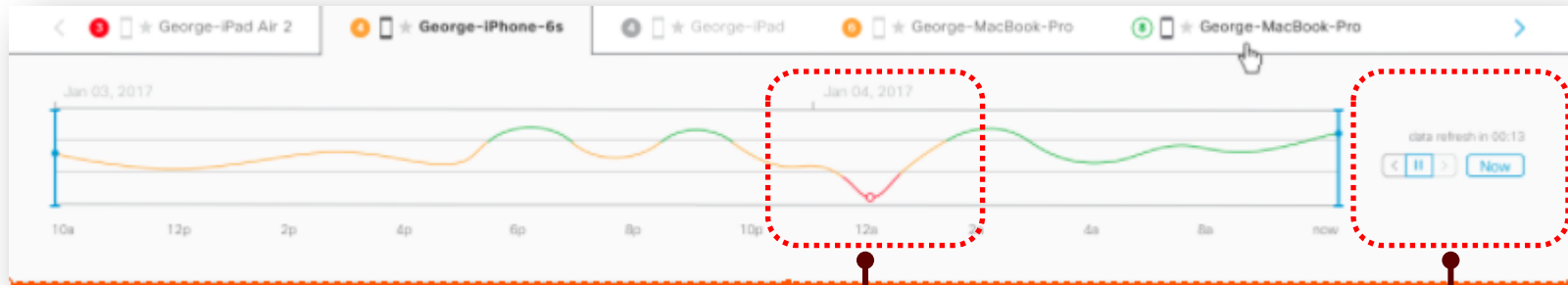


Name	Domain Name	Health	
		Most Recent	Last 24 Hours
All Applications			
disney-web-portal	www.disney.com	10	<a href="#">View</a>
espn-browsing	www.espn.com	1	<a href="#">View</a>

This screenshot shows a table of application health scores. The table has four columns: 'Name', 'Domain Name', 'Most Recent', and 'Last 24 Hours'. There are two rows of data: 'disney-web-portal' with a score of 10 and 'espn-browsing' with a score of 1. Both rows have a 'View' link in the 'Last 24 Hours' column.

# Network Time Travel

“Go Back In Time” to Understand the Network State when the Issue Occurred



- History shows critical events
- Identifies when issues occurred!

- Rewind time to when the issue occurred
- All the information on the user or network device 360 changes to the selected time!

# Cisco DNA Assurance

## Network Health

Time Travel

Toggle Overview

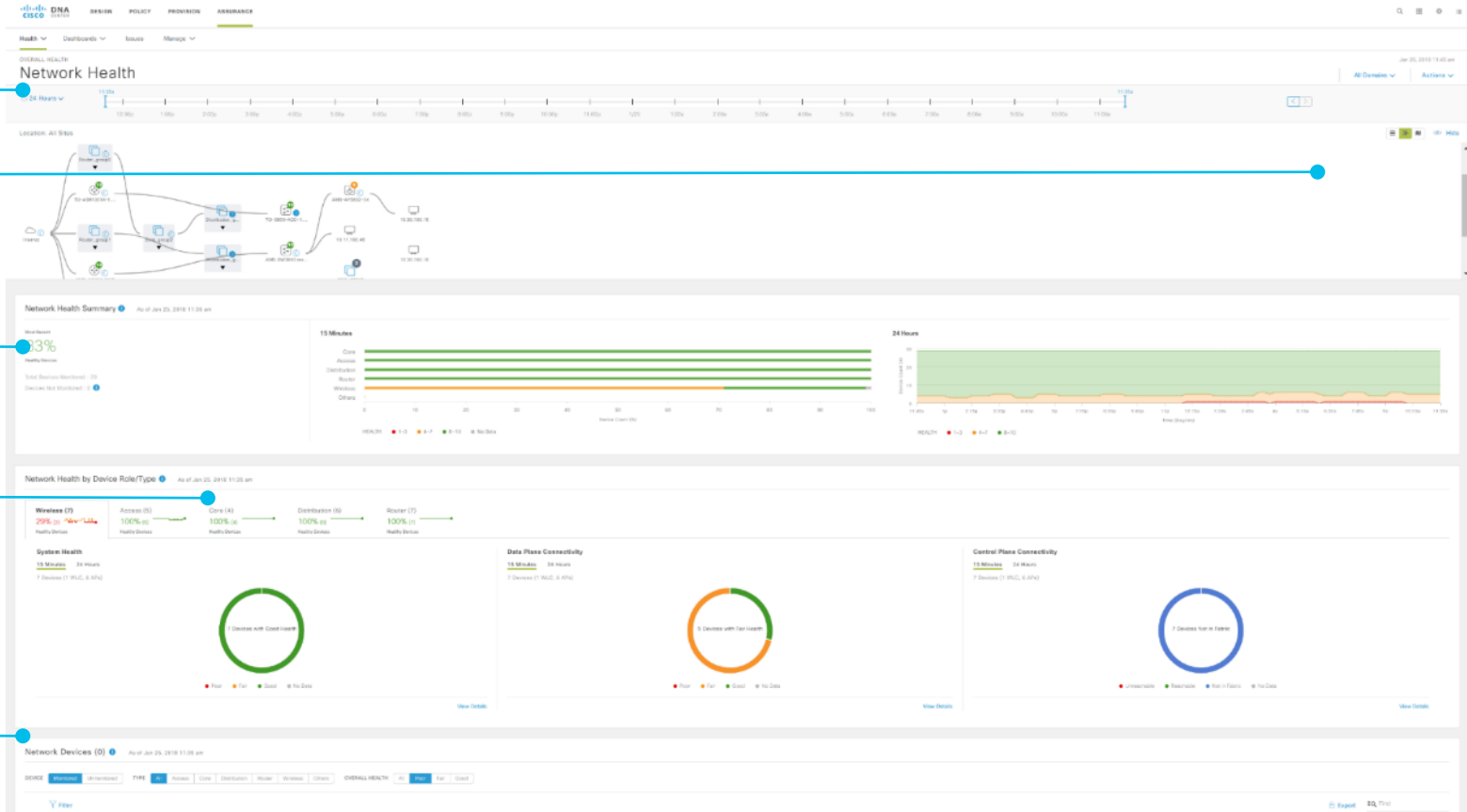
Topology | Map | List

Health Summary

Health by Role

- Wireless vs Wired
- Core vs Access
- Data vs Control
- etc

Quick Filters

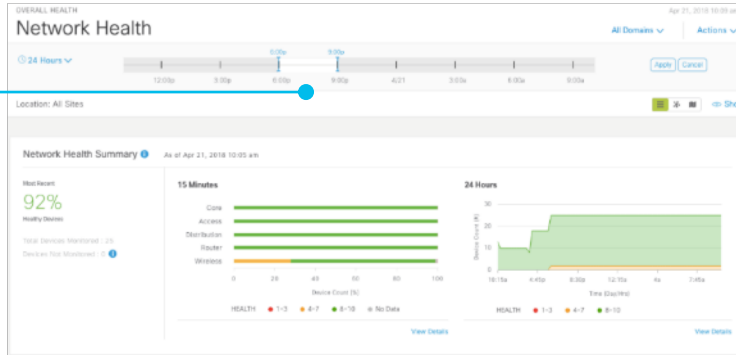


# Cisco DNA Assurance

## Network Health

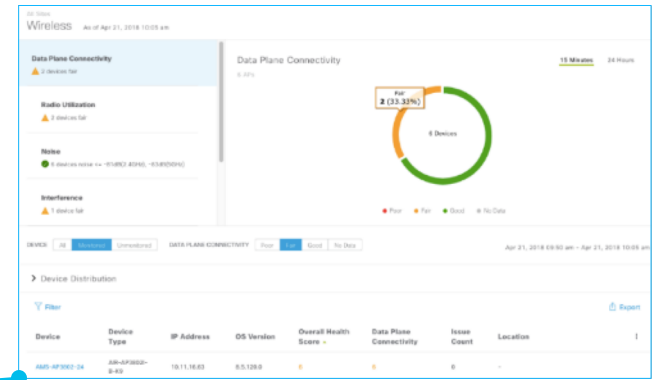
### Time Travel

Travel to Time of Issue



### Health Summary

- Routers
- Switches
- APs and WLCs
- etc



# Cisco DNA Assurance

## Client Health

Time Travel

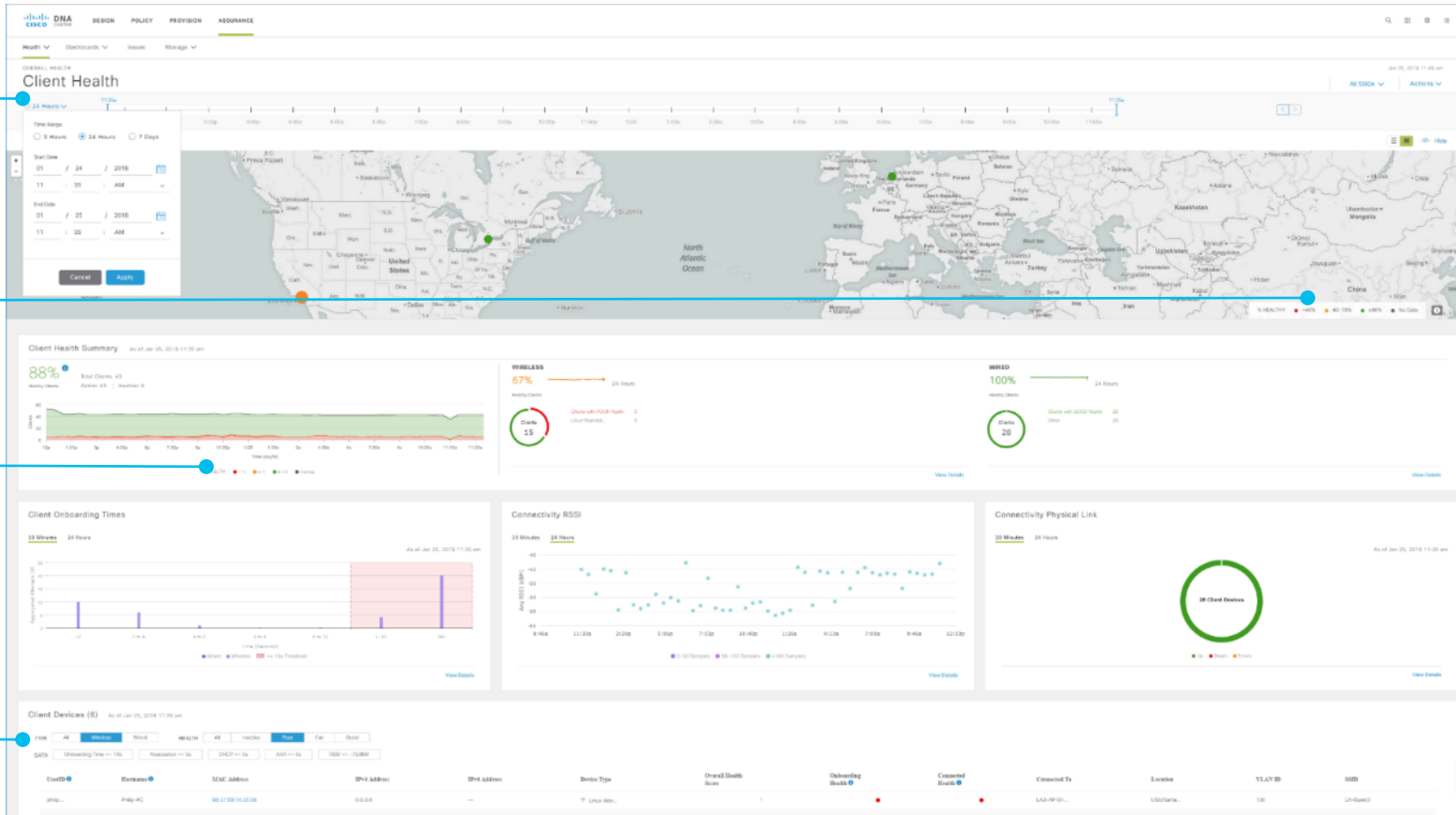
Toggle Overview

Map | List

Health Summary

- Wireless vs Wired
- Onboarding Times
- RSSI
- etc

Quick Filters



# Cisco DNA Assurance

## Client 360 (1/3)

### Client Devices

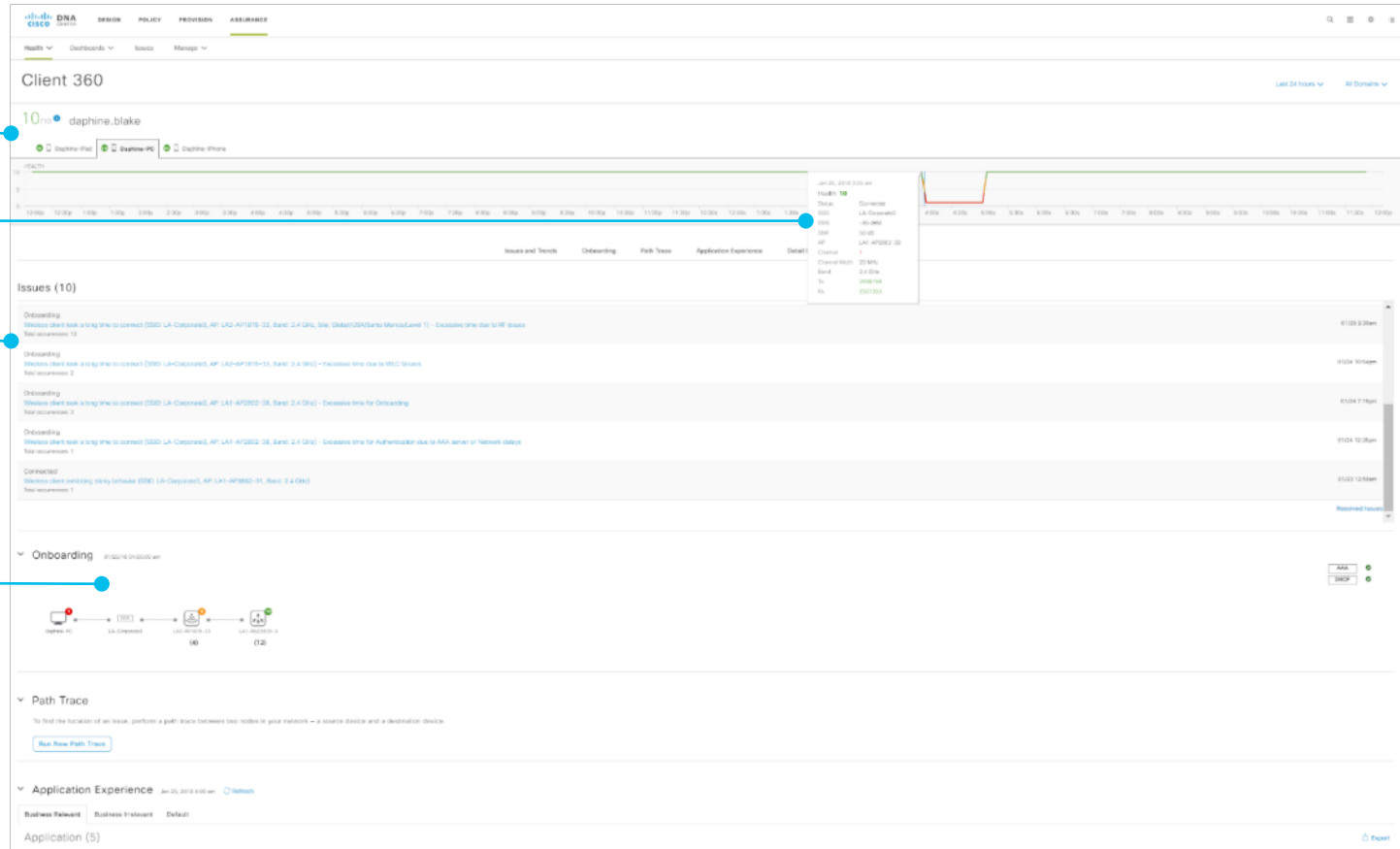
### Time Travel

### Client Issues

- Correlated
- Integrated with ITSM

### Local Topology

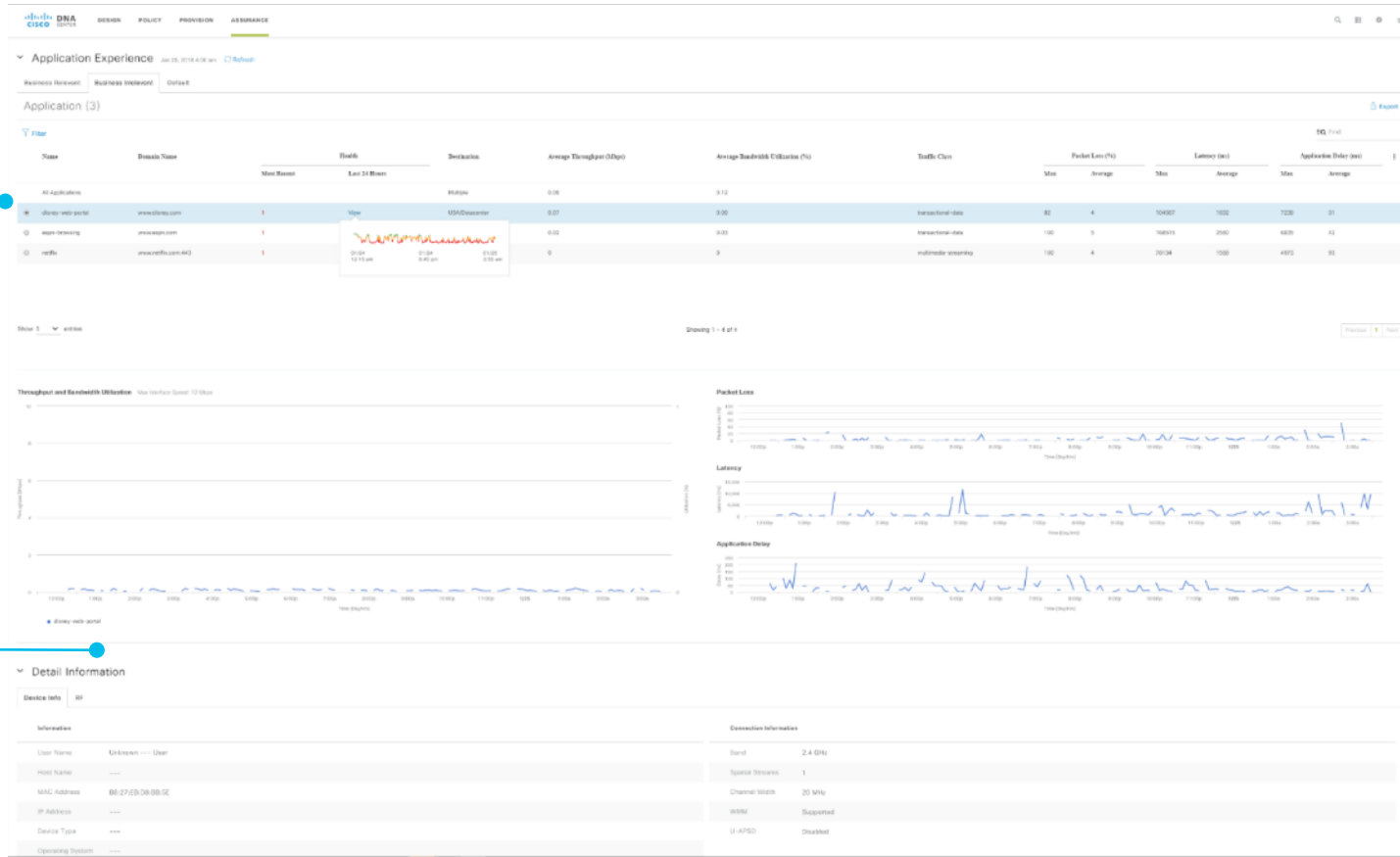
- Health Summary
- Devices Summary
- Device 360 Links
- etc





# Cisco DNA Assurance

## Client 360 (2/3)



## Application Experience

- Business Relevant vs. Default vs. Irrelevant
- Bandwidth and Usage
- App 360 Links

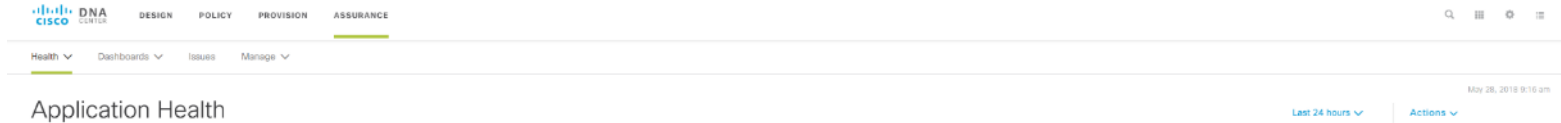
## Device Details

- Hardware / Firmware
- RF Details
- Apple iOS Analytics



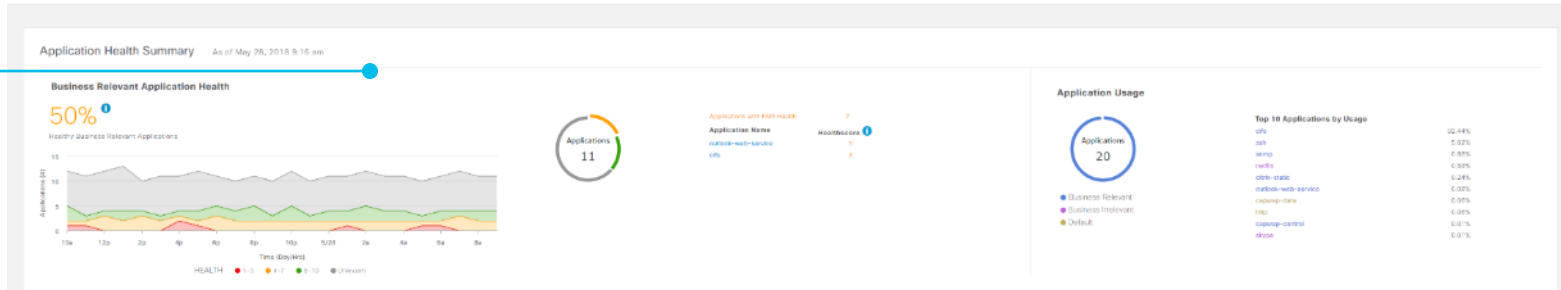
# Cisco DNA Assurance

## Application Health



### Health Summary

- By Relevance
- Top 10 Usage



### App Experience

- By Application
- Filter / Sort
- etc

**Application (32)** As of May 28, 2018 9:16 am

TYPE:  All  Business-relevant  Business-irrelevant  Default HEALTH:  All  Poor  Fair  Good

Filter Export EQ Find

Name	Health	Business Class	Traffic Class	Usage	Average Throughput	Packet Loss (%)	Latency	Application Delay
o3e	10	business-relevant	o3s-admin-mgmt	177.14 KB	17 bps	--	--	--
o3p	10	business-relevant	o3s-admin-mgmt	129.81 KB	12 bps	--	--	--
o3b-geo-accounts	10	business-irrelevant	transactional-data	99.14 KB	9 bps	--	--	--
o3p	10	business-irrelevant	transactional-data	91.65 KB	9 bps	0	0 ms	5 ms
o3s-geo-data	5	business-relevant	bulk-data	38.35 KB	4 bps	0	0 ms	12 ms
o3b-over-http	10	default	bulk-data	34.82 KB	2 bps	0	1 ms	86 ms
o3b-geo-m	10	business-relevant	o3s-admin-mgmt	34.43 KB	3 bps	--	--	--
o3b-service	10	business-relevant	o3s-admin-mgmt	22.86 KB	2 bps	--	--	--

Showing 26 of 32 [Show More](#)

# Cisco DNA Assurance

## Issue Details

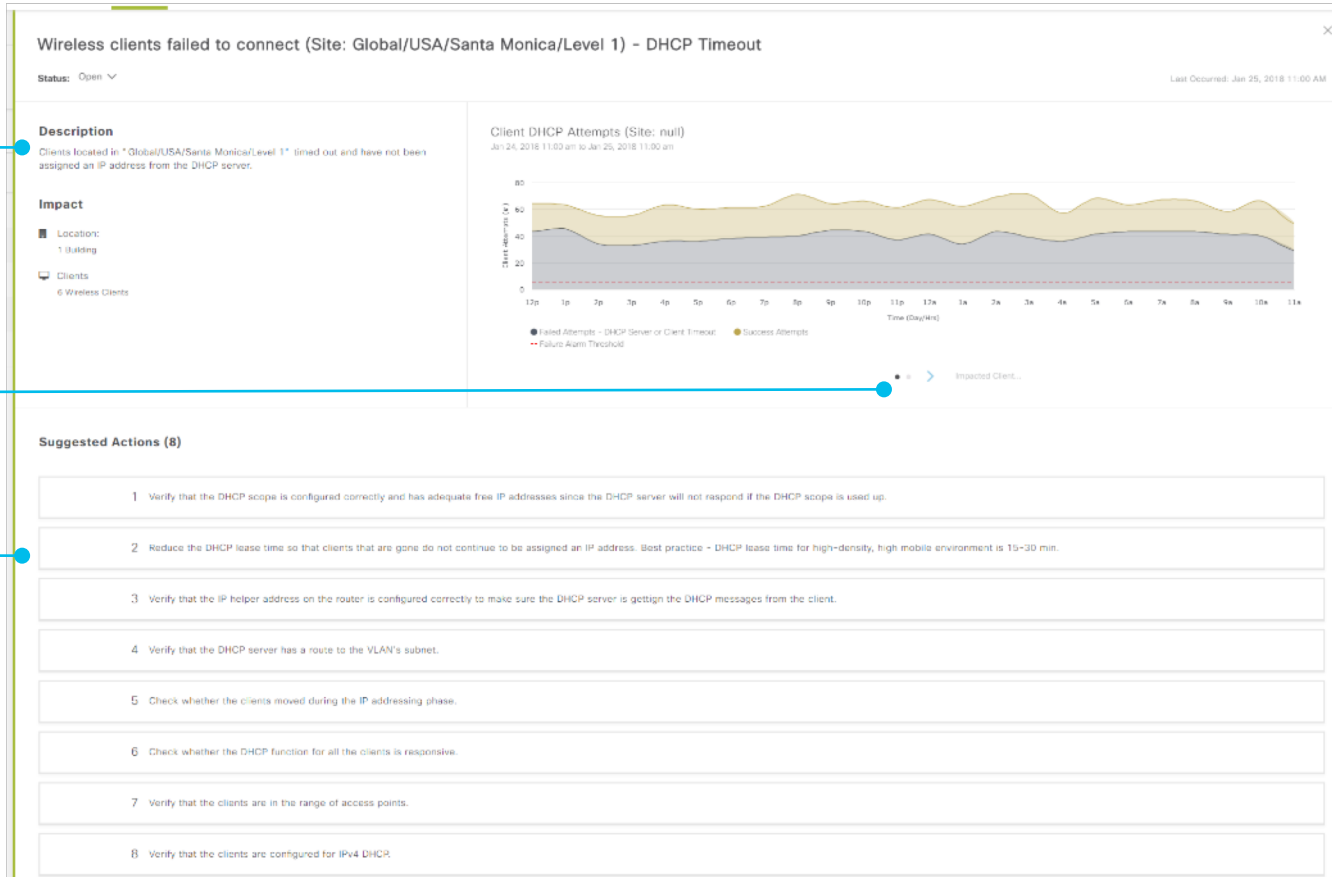
### Issue Summary

- Description
- Impact
  - Locations
  - Clients

### Context Information

### Guided Resolution

- Step by Step
- Automation on managed Devices



# Cisco DNA Assurance

## Issue Details

### Issue Summary

- Description
- Impact
  - Locations
  - Clients

### Context Information

### Guided Resolution

- Step by Step
- Automation on managed Devices

#### Wireless clients failed to connect (Site: Global/USA/Santa Monica/Level 1) - DHCP Timeout

Status: Open ▼ Last Occurred: Jan 25, 2018 11:00 AM

**Description**  
Clients located in "Global/USA/Santa Monica/Level 1" timed out and have not been assigned an IP address from the DHCP server.

**Impact**

- Location: 1 Building
- Clients: 6 Wireless Clients

**Impacted Wireless Clients**    **Impacted Locations**

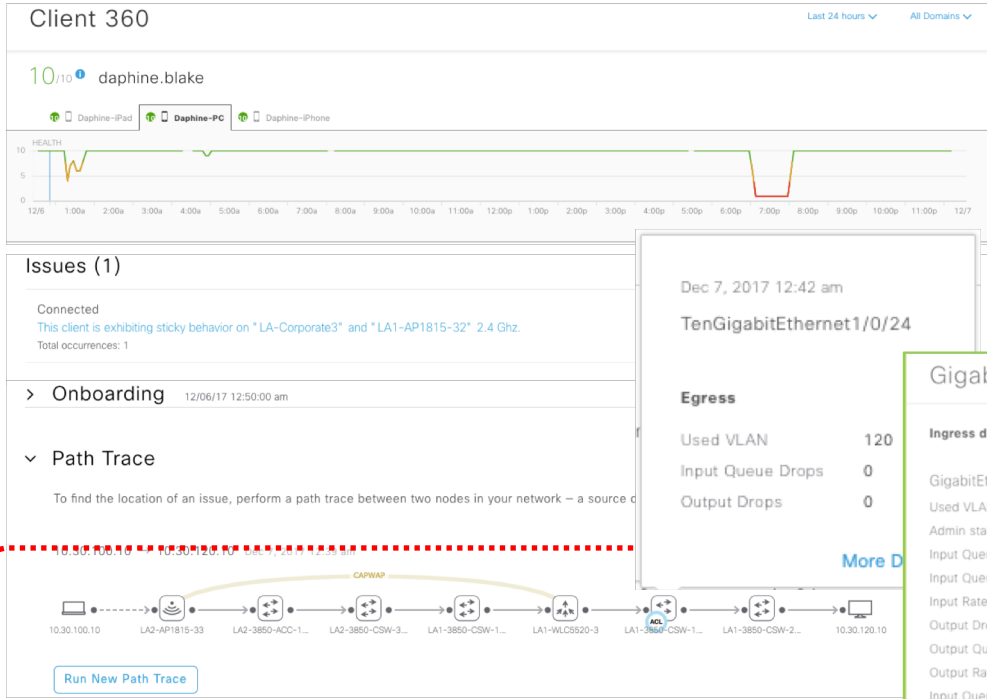
Hostname	Mac Address	Device Type	AP	SSID / VLAN	WLC
Unknown	98:27:EB:7A:2A:A0	WIRELESS	LA2-AP1815-33	LA-Guest3 / 130	LA1-WLC0520-3
Unknown	88:27:EB:7A:32:70	WIRELESS	LA2-AP1815-33	LA-Guest3 / 130	LA1-WLC0520-3
Unknown	98:27:EB:7A:38:58	WIRELESS	LA2-AP1815-33	LA-Guest3 / 130	LA1-WLC0520-3
Philip-PC	88:27:EB:7A:2E:88	WIRELESS	LA2-AP1815-33	LA-Guest3 / 130	LA1-WLC0520-3

**Suggested Actions (8)**

1. Verify that the DHCP scope is configured correctly and has adequate free IP addresses since the DHCP server will not respond if the DHCP scope is used up.
2. Reduce the DHCP lease time so that clients that are gone do not continue to be assigned an IP address. Best practice - DHCP lease time for high-density, high mobile environment is 15-30 min.
3. Verify that the IP helper address on the router is configured correctly to make sure the DHCP server is getting the DHCP messages from the client.
4. Verify that the DHCP server has a route to the VLAN's subnet.
5. Check whether the clients moved during the IP addressing phase.
6. Check whether the DHCP function for all the clients is responsive.
7. Verify that the clients are in the range of access points.
8. Verify that the clients are configured for IPv4 DHCP.

# Path Trace

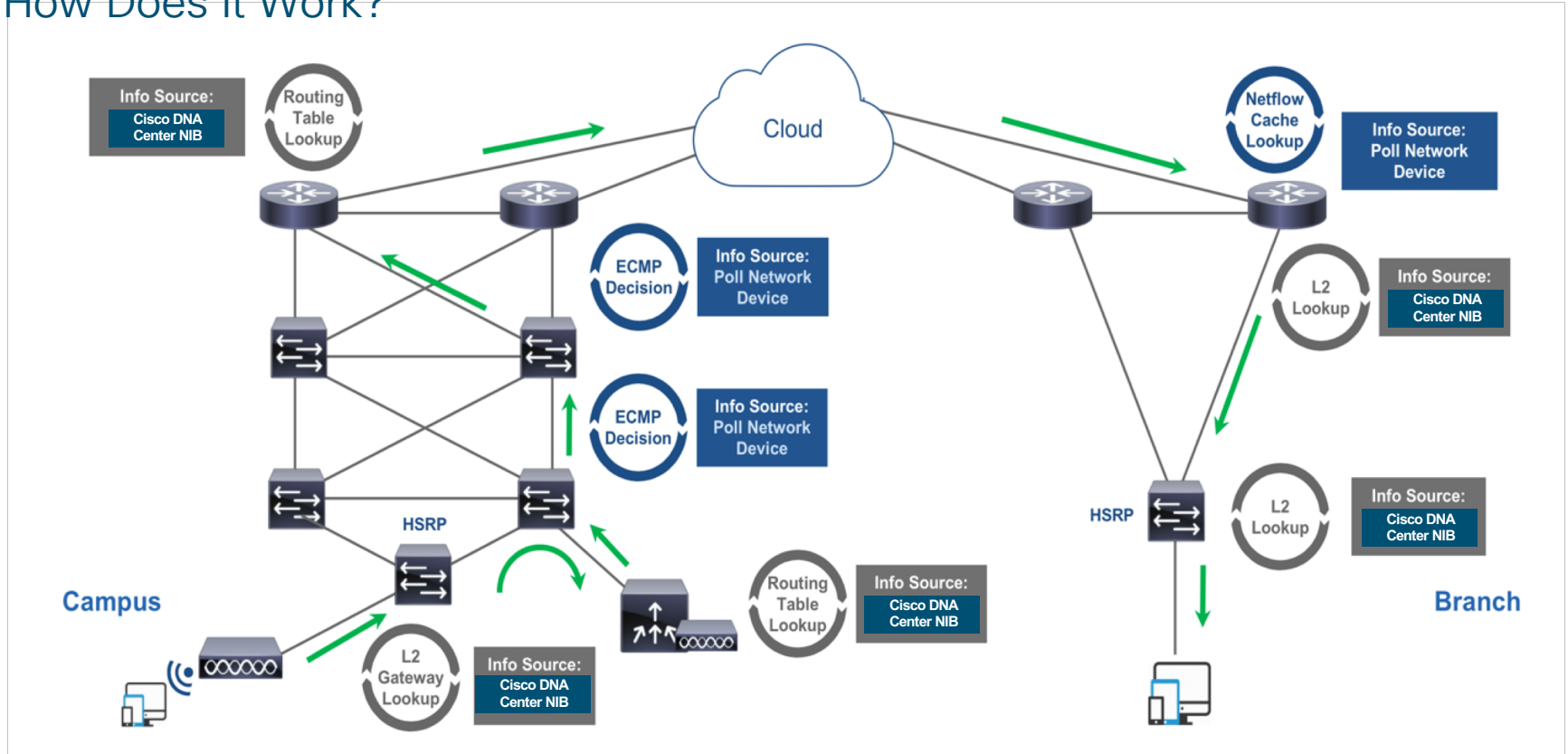
## Troubleshoot Issues Along the Network Path



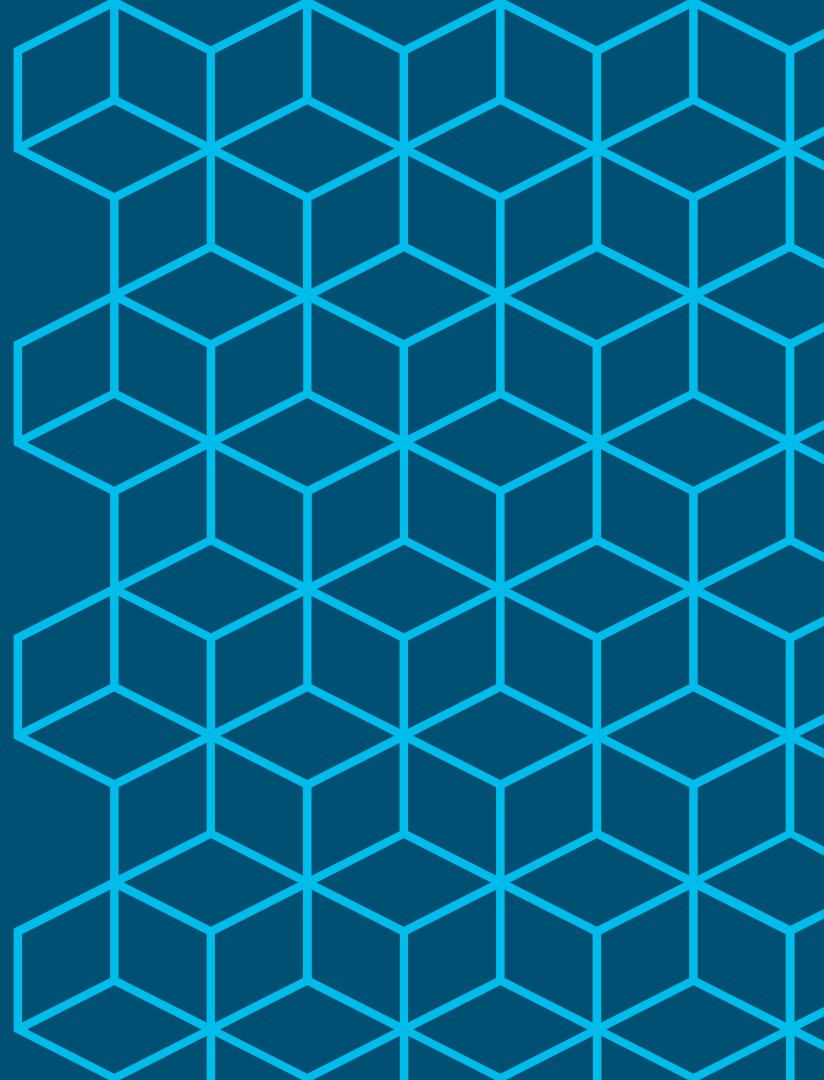
- Run pathtrace from source to destination to quickly get key performance statistics for each device along the network path
- Identify ACLs that may be Blocking or affecting the traffic flow

# Path Trace

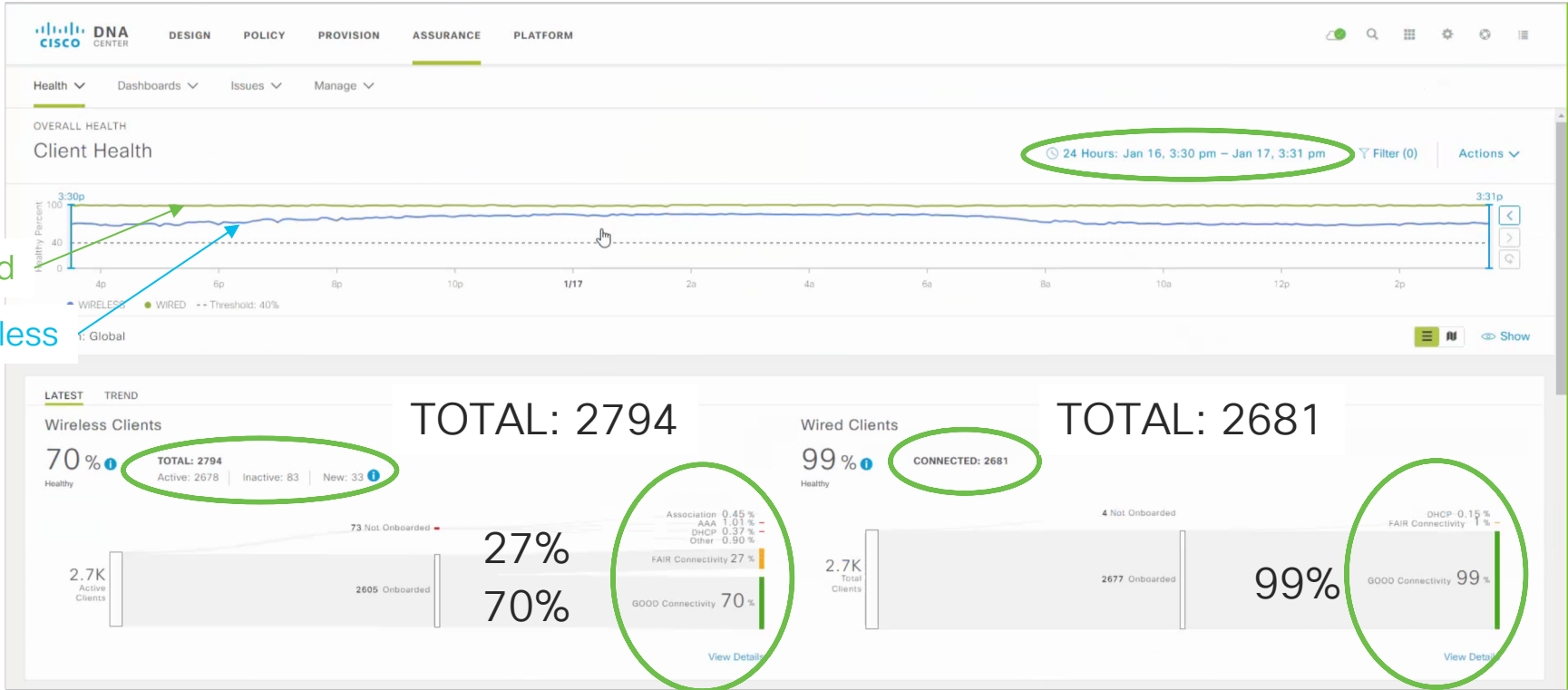
## How Does It Work?



# Cisco DNA Assurance Real World Example







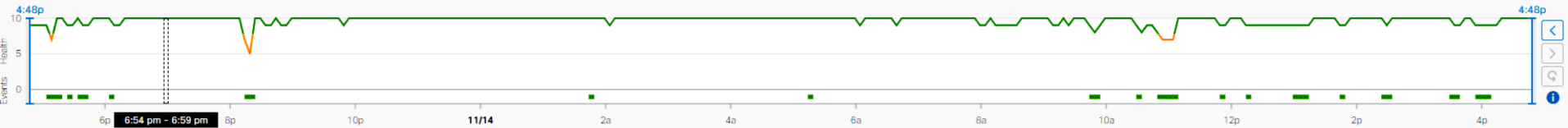
# Client #1

10/10 ⓘ

## VoWLAN Client #1

10 📱 10.152.35.115

Device: -- OS: -- MAC: 01:02:03:1A:FB:4A IPv4: 10.152.35.115 IPv6: -- VLAN ID: 235 Status: **Connected** Last seen: Nov 14, 2018 4:44 pm Connected Network Device: ap-li-e\_55-mt Last Known Location: -- SSID: **WLAN-VOICE**



Nov 13, 2018 6:54 pm - 6:59 pm

Client Health: 10

\*Only metrics with color code contribute to the Health Score

### Onboarding

Status ● Passed

### Connectivity

RSSI ● -38 dBm  
SNR ● 55 dB  
Data Rate 65 Mbps  
Tx 5.64 kB  
Rx 5.85 kB

### Connection Details

Status **Active**  
SSID **WLAN-VOICE**  
AP **ap-li-e\_55-mt**  
Channel **56 (40 MHz)**  
Band **5 GHz**

### Major Events

[See Full List](#) (0 Failures, 0 Successes)

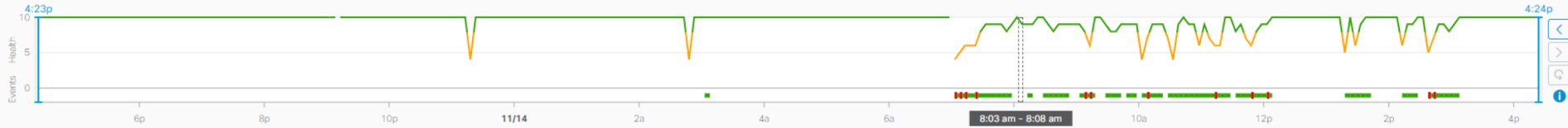
# Client #2

10/10 ⓘ

## VoWLAN Client #2

10 📶 -1A-FB-A1

Device: Unclassified OS: 1.3.6.1.4.1.27614.2.2 MAC 01:02:03:1A:FB:A1 IPv4: 10.152.35.123 IPv6: -- VLAN ID: 235 Status: Connected Last seen: Nov 14, 2018 4:23 pm Connected Network Device: ap-li-e-16-g-ingest Last Known Location: --  
SSID: WLAN1



Nov 14, 2018 8:03 am - 8:08 am

Client Health: 10

\*Only metrics with color code contribute to the Health Score

Onboarding

Status

● Passed

Connectivity

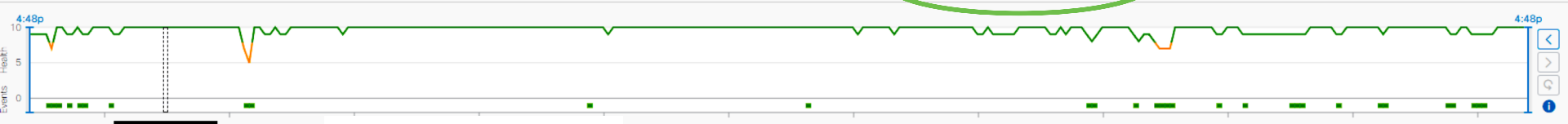
RSSI ● -52 dBm  
SNR ● 42 dB  
Data Rate 65 Mbps  
Tx 7.04 kB  
Rx 7.32 kB

Connection Details

Status Active  
SSID WLAN1  
AP ap-li-e-16-g-ingest  
Channel 44 (40 MHz)  
Band 5 GHz

Major Events

[See Full List](#) (0 Failures, 0 Successes)



- -38 dBm
- 55 dB
- 65 Mbps
- 5.64 kB
- 5.85 kB

- -38 dBm
- 55 dB
- 65 Mbps
- 5.64 kB
- 5.85 kB

Connection Details

Status: Active

SSID: WLAN-VOICE

AP: ap-li-e\_55-mt

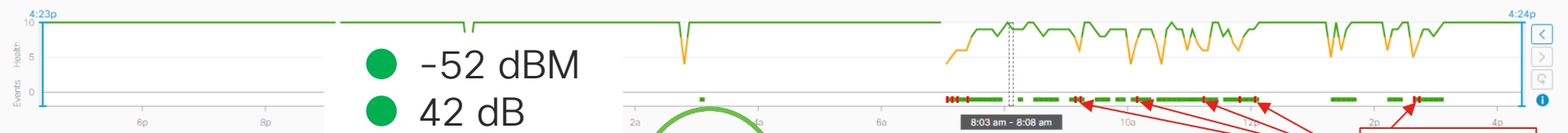
Channel: 56 (40 MHz)

Band: 5 GHz

Major Events

See Full List (0 Failures, 0 Successes)

SSID:WLAN-VOICE



- -52 dBm
- 42 dB
- 65 Mbps
- 7.04 kB
- 7.32 kB

- -52 dBm
- 42 dB
- 65 Mbps
- 7.04 kB
- 7.32 kB

Connection Details

Status: Active

SSID: WLAN1

AP: ap-li-e-16-g-ingest

Channel: 44 (40 MHz)

Band: 5 GHz

Major Events

See Full List (0 Failures, 0 Successes)

ISSUES

SSID:WLAN1

# Cisco DNA Assurance Active Sensors



# Cisco DNA Assurance

## Sensor Everywhere

Test Your Network Anywhere at Any time at Real-world Client Level

### Aironet 1800S Active Sensor



- 2x2 with 2 spatial streams
- **Multiple powering options**
  - PoE Power
  - USB Type "C" power
  - Direct AC Power Plug
- Integrated BLE
- Ultra compact form factor

### AP as a Sensor (1800/2800/3800/4800)



**Purpose-built Hardware for Analytics**  
In-line monitoring to DNA for analytics and insights while serving clients



SLA Dashboard

Onboarding &  
Services Tests

Configure Tests  
Remotely

Global Issue  
Creation

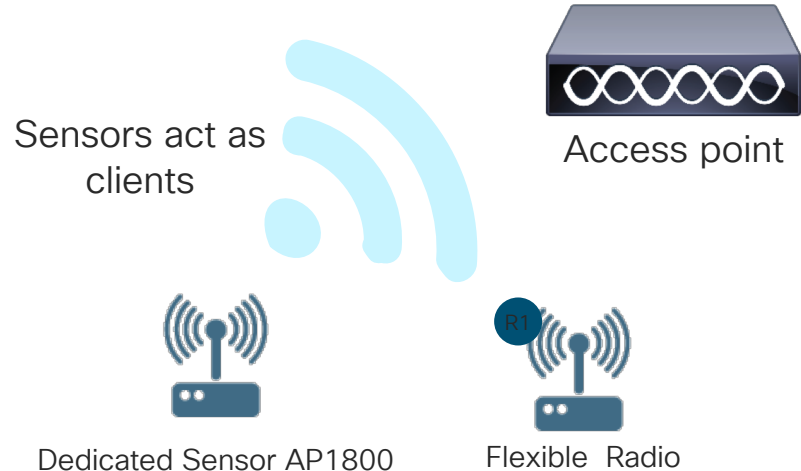
Dynamic Sensor  
Test Trigger

# Wireless Sensors

## Proactive Performance Assessment for Wireless

Test your network anywhere at any time

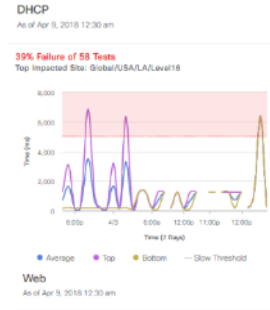
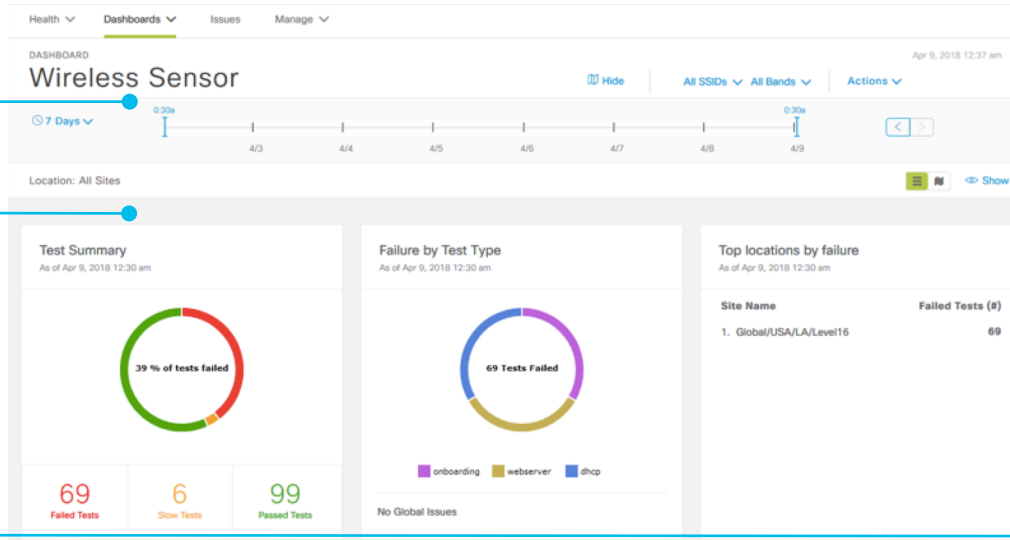
- On-Boarding Tests
  - 802.11 Association
  - 802.11 Authentication & Key Exchange
  - IP Addressing DHCP (IPv4)
- Network tests
  - DNS (IPv4)
  - RADIUS (IPv4)
  - First Hop Router/Default gateway (IPv4)
  - Intranet Host
  - External Host (IPv4)
- Application tests
  - Email: POP3, IMAP, Outlook Web Access (IPv4)
  - File Transfer: FTP (IPv4), TFTP (IPv4)
  - Web: HTTP & HTTPS (IPv4)



Flexible Radio Assignment Algorithm intelligently identifies excessive radios and seamlessly converts those into Sensor mode without client impact


# Cisco DNA Assurance

## Active Sensor Dashboard



**Test Results** As of Apr 9, 2018 12:30 am

Filter: EQ Find

Test Name	Location	SSIDs	Test Types	Test Results
LA-Sensor	USA / LA / Level16	LA-Corporate1	Onboarding Test IP Addressing Test Web Server Test	

### Time Travel

### Sensor Test Summary

- Past Failures by
  - Locations
  - Type
  - ...

### Trending Charts

- For Key Services (DHCP, DNS, AAA, Web, Email, ...)

### Spark Charts

- Results per Location over Time



# Cisco Intelligent Capture

Real-Time Client and App Insights to Enhance Cisco DNA Wireless Assurance



## Client and App Real-time Forensics

- Real-time client RF view
- In-service packet captures using Live Assurance analytics
- Monitor Client Onboarding real-time
- Real-time App performance insights



## Hyperlocation – Real- Time Client Location

- Enhance Sticky client issue analysis with Real-time location
- Identify coverage holes with real-time accuracy (<3 mtr.)



## Total Secure Coverage Monitoring

- 24x7 monitoring of Wi-Fi and non-Wi-Fi interference using AirSense radio
- 24x7 wIPS forensics to prevent over the air attacks using Live Assurance radio



## Active Sensor Testing

- Onboarding Tests
- Network Services Tests
- App Connectivity Tests
- App Experience Tests

Cisco Intelligent Capture with Real-time Client and App insights would enhance guided remediation and also allow On-Demand VIP client Troubleshooting

# Cisco Intelligent Capture Overview

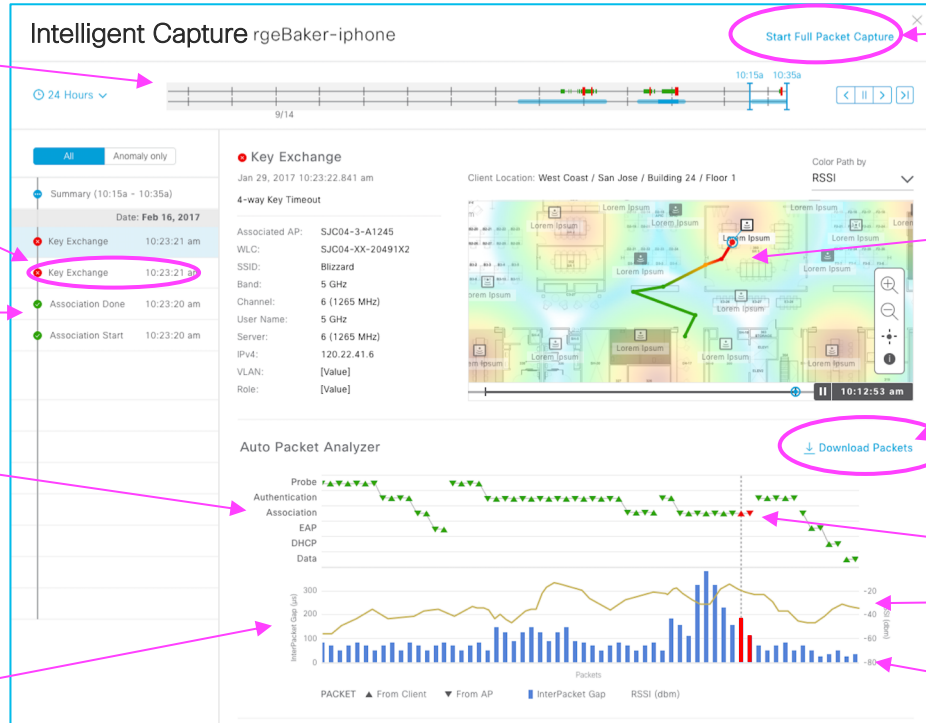
Network Time Travel view

Failed Onboard

Real-time Event Viewer

Onboard Packet stage identifier

Auto Packet Analyzer



AP4800 3rd radio Full packet capture

Real-time Client location Map with trail of movement

Download Onboard Packet

Failed Packet

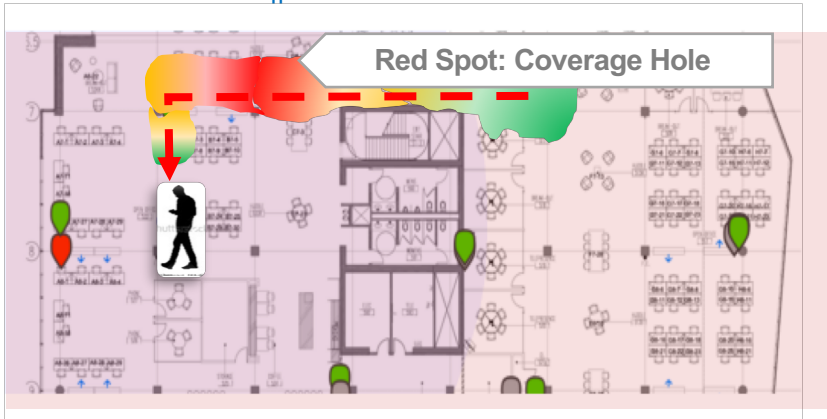
RSSI Chart per Packet

Interpacket Gap (ms) bar chart

# Troubleshooting Use Cases using Intelligent Capture

## 1 On-Demand RF Scanner

Live RF Network || Pause 11:50:32 Record



Green Spot: Voice-quality Throughput

Orange Spot: Browsing-quality Throughput

Red Spot: Coverage Hole

KPI List Graph\*

SNR

RSSI

MCS

Throughput

Packet retry

### Situation

- A large logistics company uses Wi-Fi operated Auto-guided vehicles (AGV) in its logistics warehouses. Due to high ceilings and large moving metal structures, these warehouse have dynamic RF scenarios
- Due to little human involvement sometimes these machines don't take optimal paths due to temporal coverage hole

### Solution

- IT staff uses the On-Demand RF scanner tool to validate AGV's RF coverage during the live operation and detect coverage holes in a highly dynamic RF environment
- This helps IT staff immensely in RF design, planning and optimization

### Key Issues addressed

- Poor RF Zones
- RF design optimization
- Sticky client analysis with real-time location
- VoIP performance and audio issues

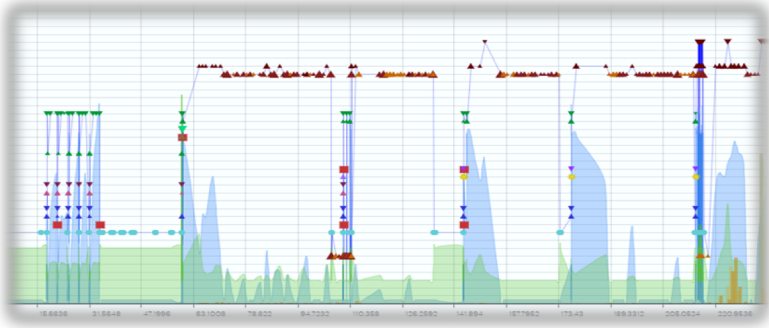
### Key Industries

Healthcare, Distribution, Logistics, Retail and Higher Ed.

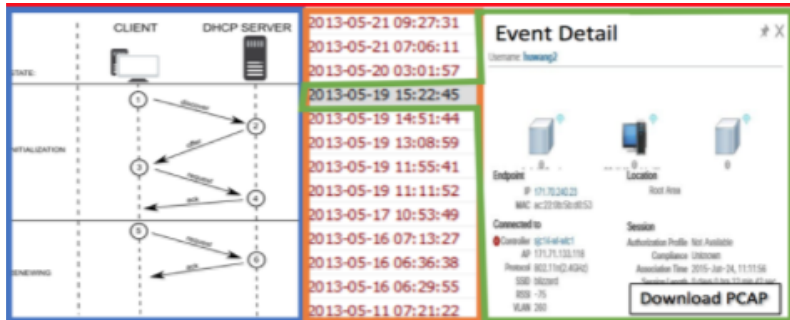
# Troubleshooting Use Cases using Intelligent Capture

## 2 Automated Packet Captures

### Visual Packet Trace Analyzer (<5 sec)



### Real-time Anomalies with Auto PCAPs (<5 sec)



OnBoarding Handshake TimeStamp of each event Issue detail section

### Situation

- A Financial services giant decided to adopt to BYOD to encourage people to use its Virtual Desktop Infrastructure for a certain critical applications. In the first week, John discovered longer Onboarding time from mobile device compare to laptop and received complaints from several end-users

### Solution

- IT staff turned on the Auto PCAP to capture onboarding and roaming failure anomalies for the BYOD device at a specific site. This allowed IT staff to capture de-authentication packets that are typically observed when the client has driver issues
- IT staff also had access to detailed PCAP analysis that enabled them to identify the root cause behind onboarding and roaming failures

### Key Issues addressed

- On-boarding and roaming failures
- VOIP Performance issues
- Sticky client analysis with real-time location

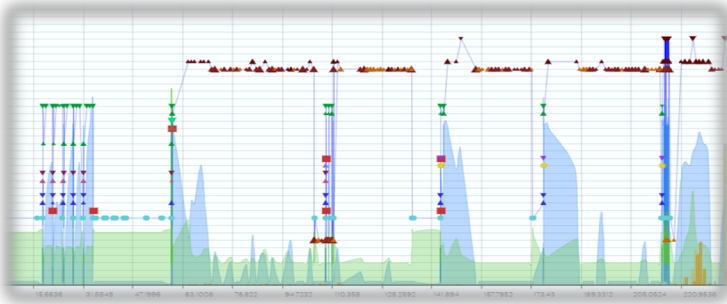
### Key Industries

All segments

# Troubleshooting Use Cases using Intelligent Capture

## 3 VIP Service Assurance

### Visual Packet Trace Analyzer (<5 sec)



### Real-time Client Location Tracking (<5 sec)



### Situation

- A large healthcare deployed 5000 vital sign monitor for every in-patient. These vital sign allow doctors to monitor critical parameters on a real-time basis
- Wi-Fi connection of vital sign monitor starts to get disrupted on an intermitted basis during the middle of the day and if not addressed it can be

### Solution

- IT staff uses Live Troubleshooting tool to perform detailed forensics on both the client state and the location
- Using packet trace analyzer, the IT staff is able to visualize frequent roaming and re-authentication failures from the device along with lower RSSI than anticipated in particular location

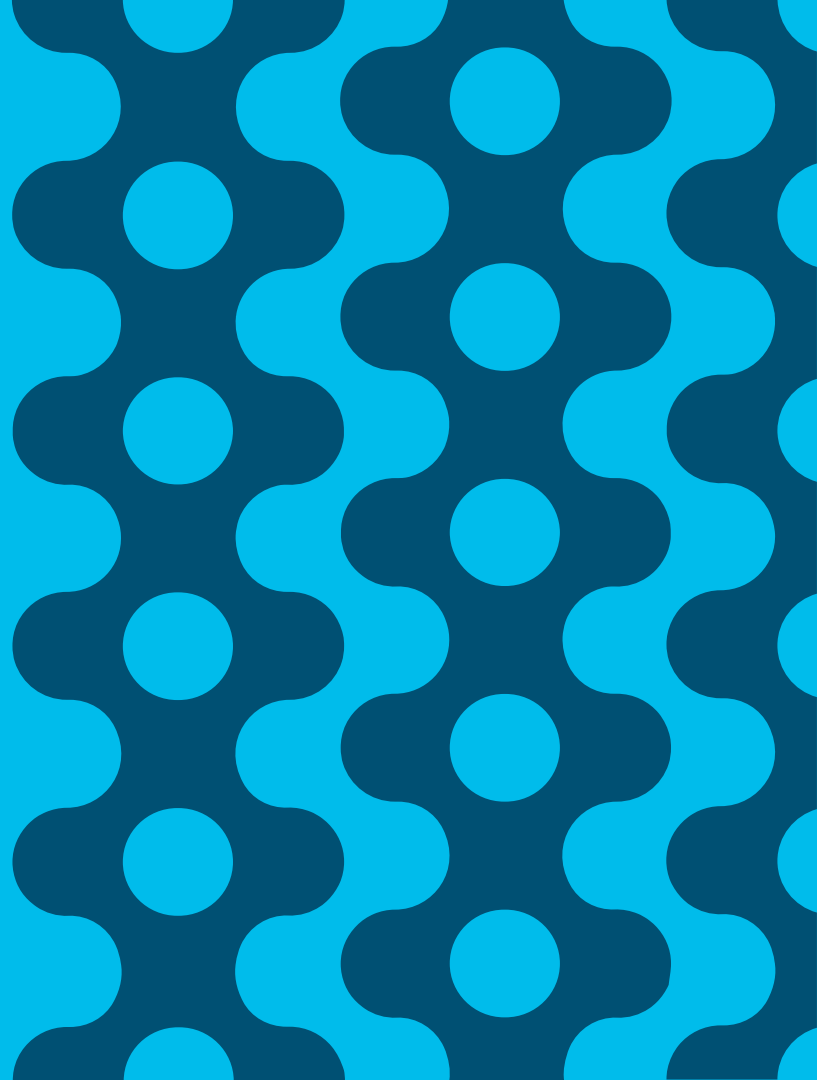
### Key Issues addressed

- On-boarding and roaming failures w/ PCAP
- Sticky client analysis with real-time location
- Service Level Assurance for critical apps/users
- Remote Wireless troubleshooting through Full PCAP

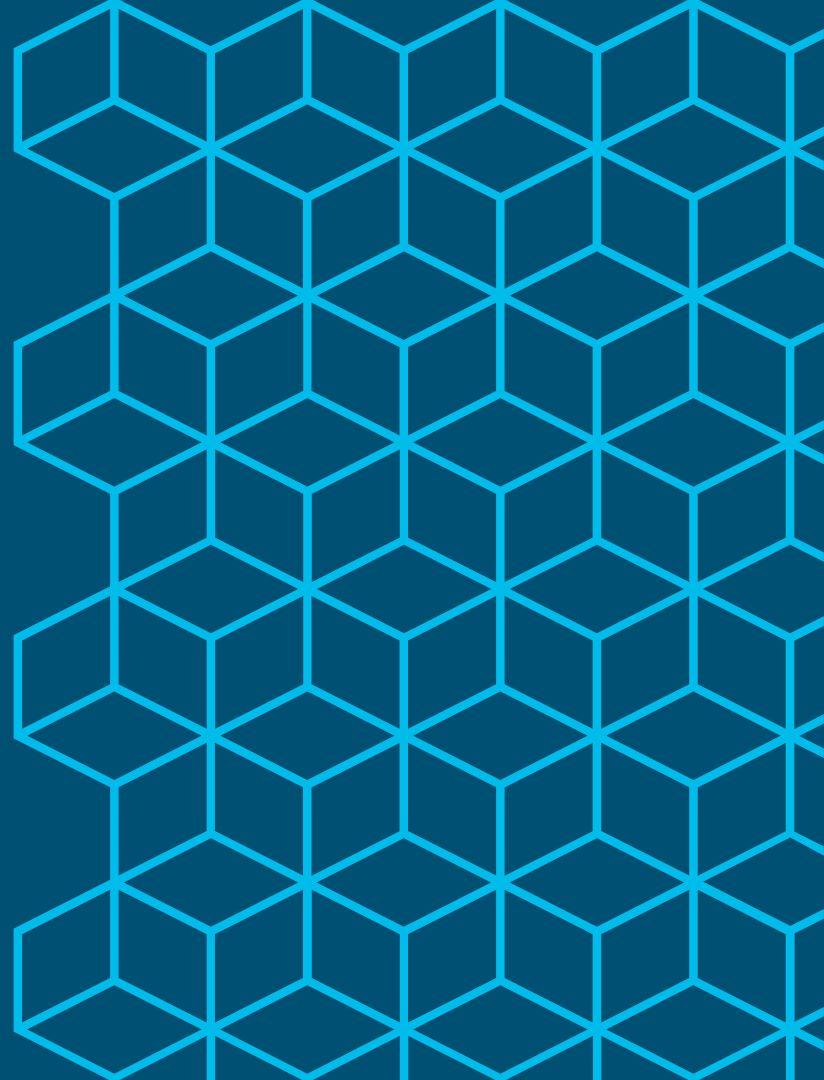
### Key Industries

Healthcare, Distribution, Logistics, Retail, Higher Ed, MSPs

# Cisco DNA Assurance Troubleshooting Example




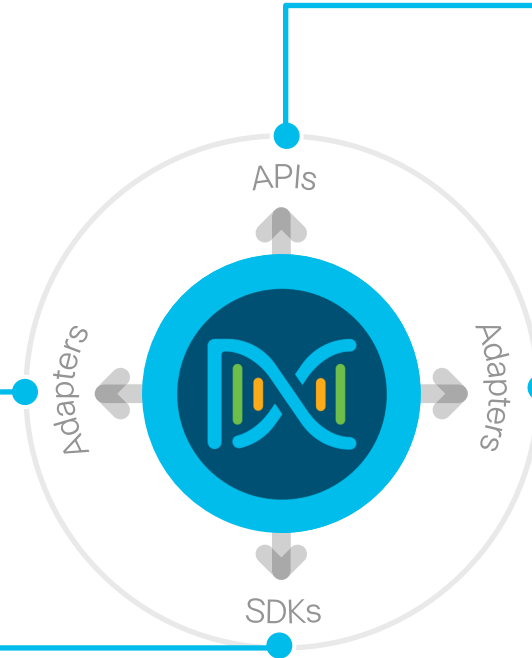
# Cisco DNA Center Platform



# Platform Capabilities – APIs, Adapters & SDKs

## IT and Network System Process

   ITSM
   IPAM
   IPAM
   Reporting



## Intent APIs

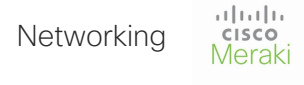
- Assurance
- Path Trace
- Command Runner
- Template Programmer
- NFV Provisioning
- Wireless Provisioning
- Network Inventory / Discovery / Tagging
- SDA
- Topology
- Plug-n-Play
- Software Image Management (SWIM)

## X-Domain Integration

## 3<sup>rd</sup> Party SDKs

Map 3<sup>rd</sup> Party Network Devices to Data Model

Level 1 Operations support:  
Discovery, Inventory, Topology, Availability, Command Runner





# Intent APIs



## Network APIs

- Network Level - Features based API
- Consistent model for feature across all devices types
- All UI capabilities of Cisco DNA Center available via the API
- Example: SWIM workflow
  - Create Sites and Network Profiles
  - Create sub-pool for sites
  - Assign site to network profiles
  - Assign Claim device to site
  - Trigger Provision request for ENCS device

## Business APIs

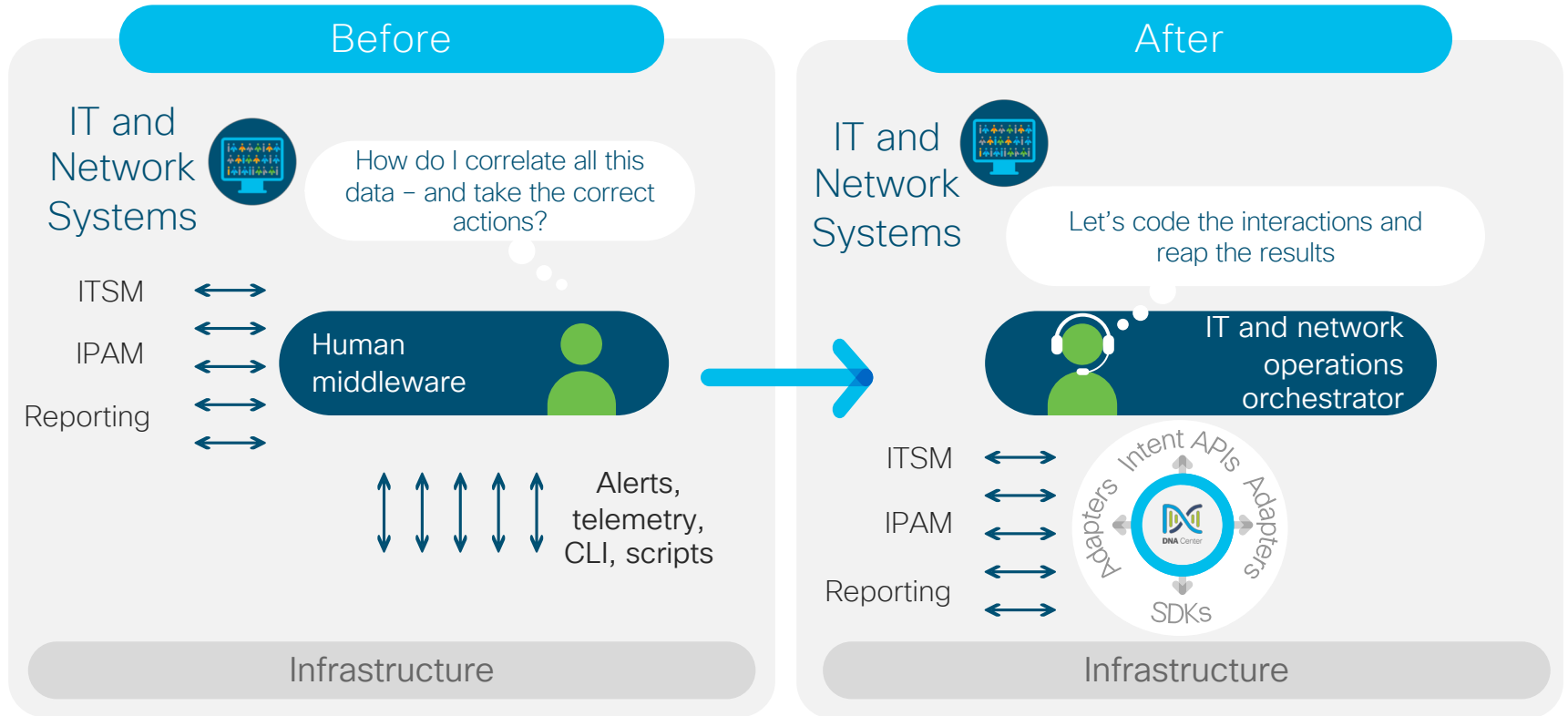
- Intent Based API for network operations
- Network capabilities abstraction
- API's aligned with business constructs
- Custom Business API from an aggregation of network APIs
- Example: SWIM Workflow
  - Provision NFV - Design and Provision single/multi NFV device with given site/area/building/floor

# Example of Business Intent API: SSID Creation

- Create Dynamic Interface
- Create SSID
- Create Wireless Network Profile
- Associate device physical location
- Associate managed AP locations
- Provision WLC

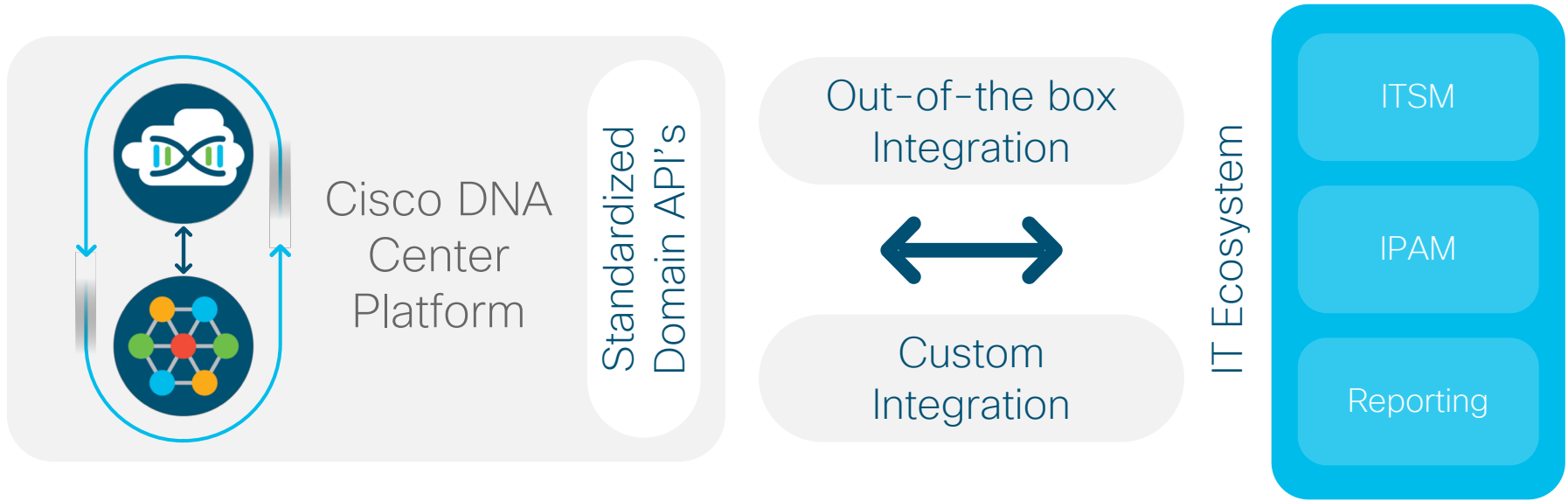
- **Create and Provision SSID**

# Streamlining IT Processes



From "human middleware" to "IT orchestrator"

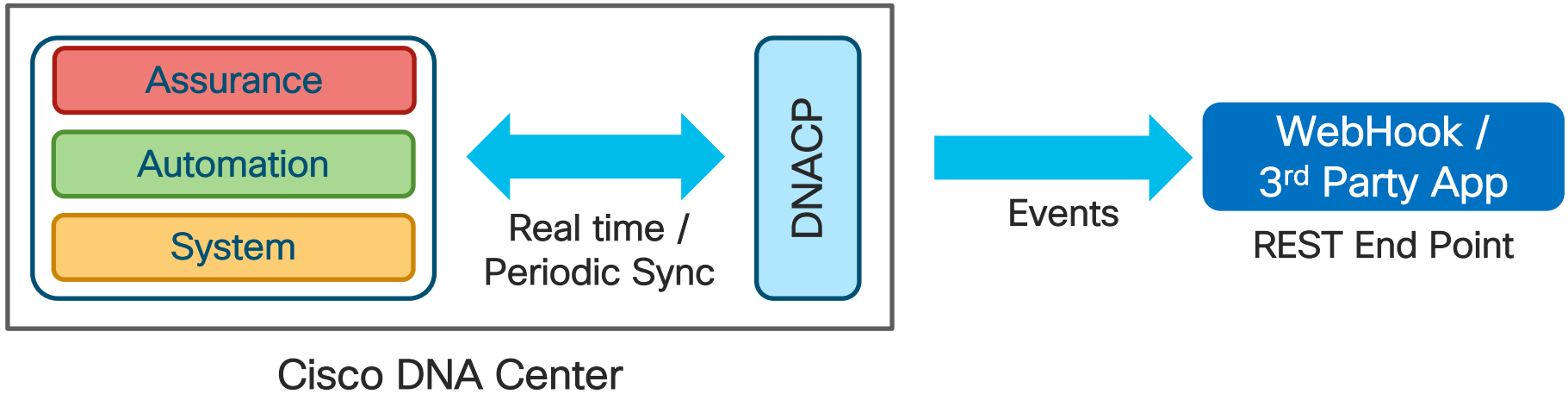
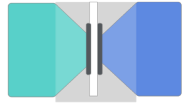
# Integration Adapters with Cisco DNA Center



*Out-of-the-box integration available Today: ITSM(ServiceNow), IPAM (Infoblox, Bluecat) and Reporting (Tableau)*

# Cisco DNA Center Platform

## Events & Notifications



# Cisco DNA Center: Southbound – Device SDK

Cisco DNA Center



Policy



Automation



Analytics



Cisco DNA Center Uses Device Packs to Understand the Characteristics of a Network Device

SDK provides an Easy Way to Develop Device Packs for ANY Type of Network Device

Device Packs



Device Packs



Hewlett Packard  
Enterprise

Device Packs



JUNIPER  
NETWORKS

Device Packs



HUAWEI

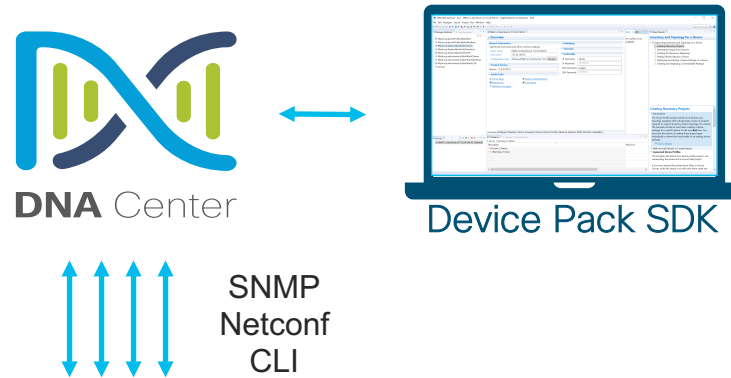
Device Packs

Internet of Things

The Cisco DNA SDK is based on Eclipse – see <https://developer.cisco.com/dnacenter/multivendorsupport/>

# Cisco DNA Center Platform – Device Pack SDK

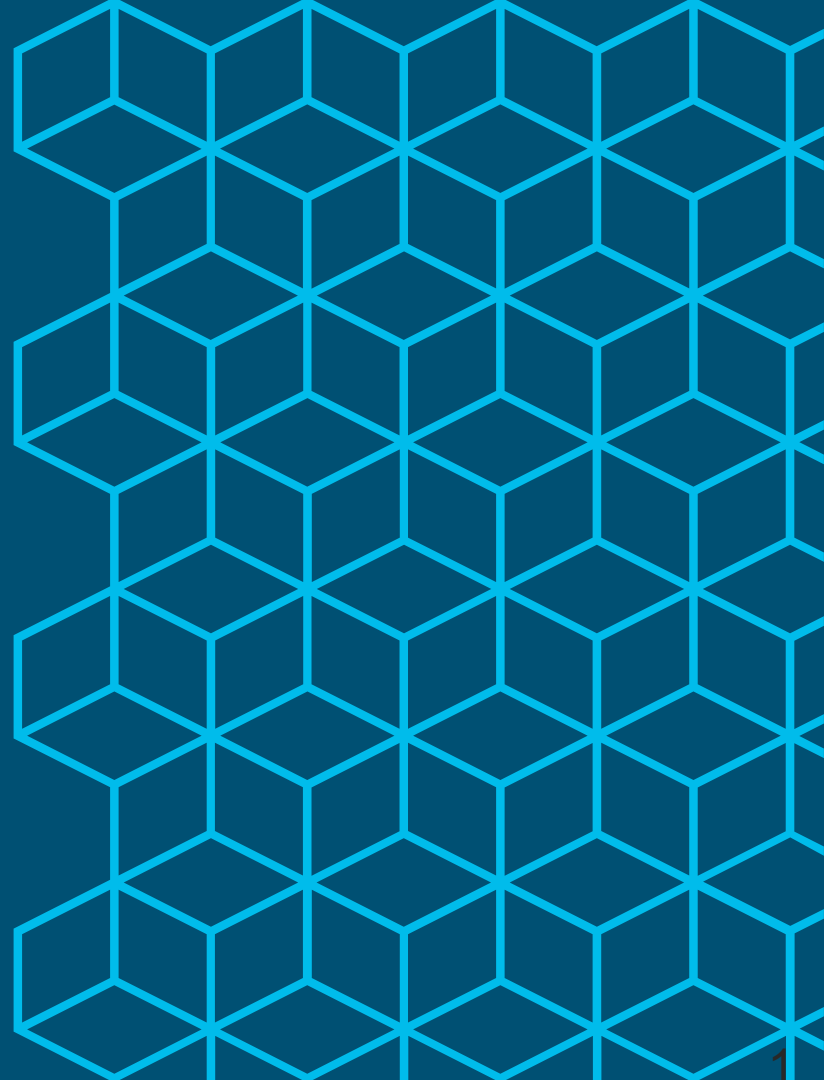
- Discovery
- Inventory
- Topology
- Availability
- Command Runner



**Infrastructure**

Physical | Virtual | Programmable | App Hosting

How to get started?





# Introducing Cisco DNA Center Platform

The screenshot shows the Cisco DNA Center Platform website. The navigation bar includes the Cisco DNA Center logo and menu items: DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The main content area is divided into five sections: Design, Policy, Provision, Assurance, and Platform. Each section has an icon, a title, a brief description, and a list of key features. A blue callout box with a rounded border highlights the Platform section, and a blue arrow points from the right side of the callout box towards the Platform section. On the right edge of the screenshot, there is a vertical sidebar with a question mark icon and the text 'Make a Wish'.

**DESIGN**   **POLICY**   **PROVISION**   **ASSURANCE**   **PLATFORM**

## Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

## Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

## Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover Devices
- Manage Unclaimed Devices
- Set up fabric across sites

## Assurance

Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.

- Assurance Health
- Assurance Issues

## Platform

Use DNA Center Platform, to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

- View the API Catalog
- Configure DNA Center - to - Third Party Integrations
- Schedule and Download - Data and Reports

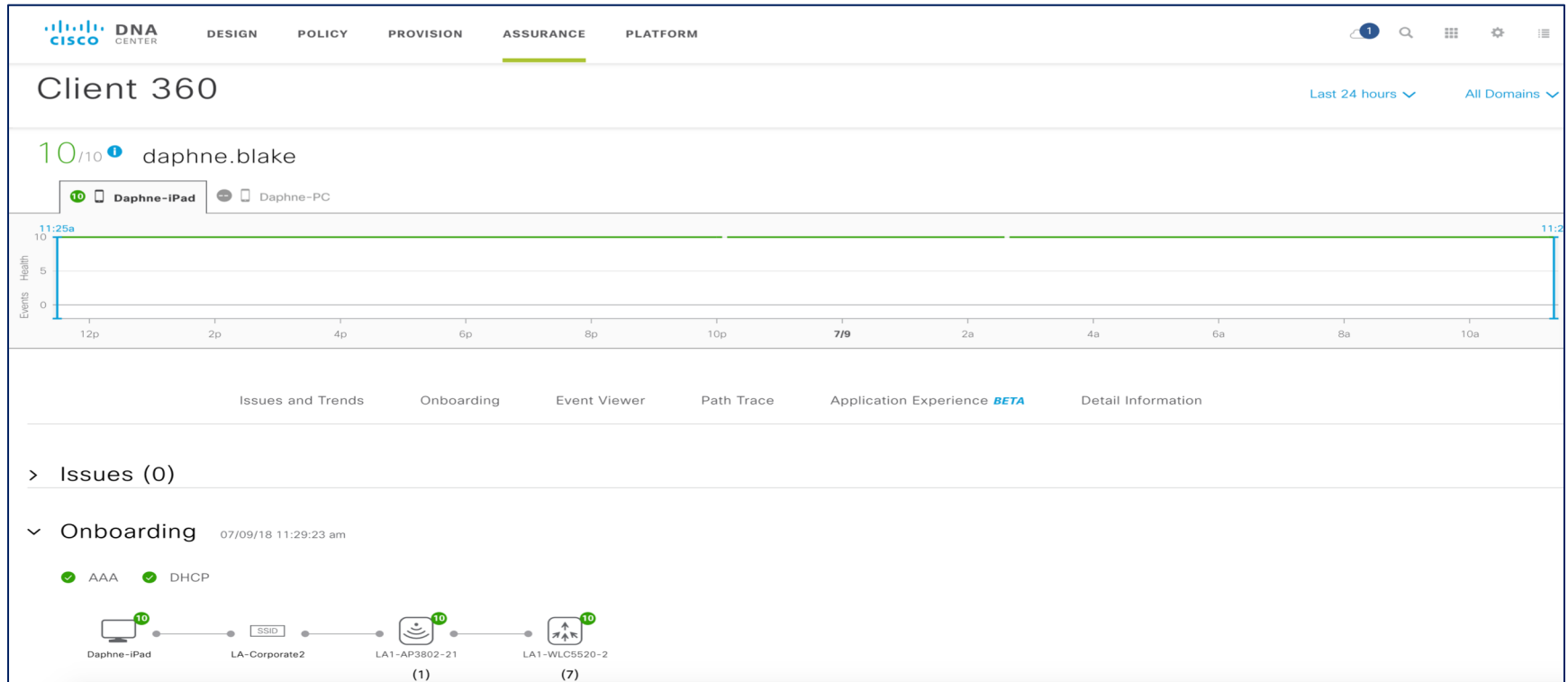
Make a Wish

# API Catalog

The screenshot shows the Cisco DNA Center API Catalog interface. The top navigation bar includes the Cisco DNA Center logo and tabs for DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The PLATFORM tab is selected. Below the navigation, the page title is 'Platform' with sub-headers 'North America' and 'Version 1.12.0 - Released 8/31/2018'. A secondary navigation bar contains 'Overview', 'Manage', 'Developer Toolkit' (selected), and 'Runtime Dashboard'. The main content area is titled 'APIs' and features a search bar. A sidebar on the left lists navigation categories: Know Your Network (expanded), Sites, Networks, Devices, Clients, Site Management, Operational Tools, and Authentication. The 'Networks' section is expanded, showing a table of APIs.

Method	Name	Description
GET	<a href="#">getPhysicalTopology</a>	This method is used to obtain the raw physical topology and filter based on nodeType
GET	<a href="#">getL3Topology</a>	This method is used to obtain Layer 3 device topology by routing protocol type
GET	<a href="#">getSiteTopology</a>	This method is used to obtain the site topology
GET	<a href="#">getVlanNames</a>	This method is used to obtain the list of vlan names
GET	<a href="#">getL2Topology</a>	This method is used to obtain the Layer 2 topology by Vlan ID
GET	<a href="#">Network HealthIntent</a>	Network Devices and their health by category

# Example: Assurance Client Detail



# Assurance Client Detail – Intent API

```
{
  "response": {
    "detail": {
      "id": "6C:19:C0:BD:87:C9",
      "connectionStatus": "CONNECTED",
      "hostType": "WIRELESS",
      "userId": "daphne.blake",
      "hostName": "Daphne-iPad",
      "hostOs": "Workstation",
      "hostVersion": null,
      "subType": "Apple-iPad",
      "lastUpdated": 1530989200429,
      "healthScore": [
        {
          "healthType": "OVERALL",
          "reason": "",
          "score": 10
        },
        {
          "healthType": "ONBOARDED",
          "reason": "",
          "score": 4
        },
        {
          "healthType": "CONNECTED",
          "reason": "",
          "score": 6
        }
      ],
      <.snip.>
    }
  }
}
```

```
<.snip.>
  "hostMac": "6C:19:C0:BD:87:C9",
  "hostIpV4": "10.30.100.27",
  "hostIpV6": [],
  "authType": null,
  "vlanId": "100",
  "ssid": null,
  "frequency": null,
  "channel": null,
  "apGroup": null,
  "location": "USA/LA/Level16",
  "clientConnection": "LA1-AP3802-21",
  "connectedDevice": [],
  "issueCount": 0,
  "rssi": null,
  "avgRssi": null,
  "snr": null,
  "avgSnr": null,
  "dataRate": null,
  "txBytes": null,
  "rxBytes": null,
  "dnsSuccess": null,
  "dnsFailure": null,
  "onboarding": {
    "averageRunDuration": null,
    "maxRunDuration": null,
    "averageAssocDuration": null,
    "maxAssocDuration": null,
    <.snip.>
  }
}
```

```
<.snip.>
  "connectionInfo": {
    "hostType": "WIRELESS",
    "nwDeviceName": "LA1-AP3802-21",
    "nwDeviceMac": "00:A7:42:CB:AC:E0",
    "protocol": "802.11ac",
    "band": "5",
    "spatialStream": "2",
    "channel": "60",
    "channelWidth": "20",
    "wmm": "Supported",
    "uapsd": "Disabled",
    "timestamp": 1531103267416
  },
  "topology": {
    "nodes": [
      {
        "role": "Client",
        "name": "Daphne-iPad",
        "id": "6C_19_C0_BD_87_C9",
        "description": "Client",
        "deviceType": "Apple-iPad",
        "platformId": null,
        "family": null,
        "ip": "10.30.100.27",
        "softwareVersion": null,
        "userId": "daphne.blake",
        "nodeType": "Interface",
        <.snip.>
      }
    ]
  }
}
```

What is happening in  
the market already?



# Cisco DNA Center Solution

Conscia Port Utilization monitors port usage for highly improved network business analytics

## Problem

Measuring switch port usage requires logging in to each switch and manually running CLI commands.

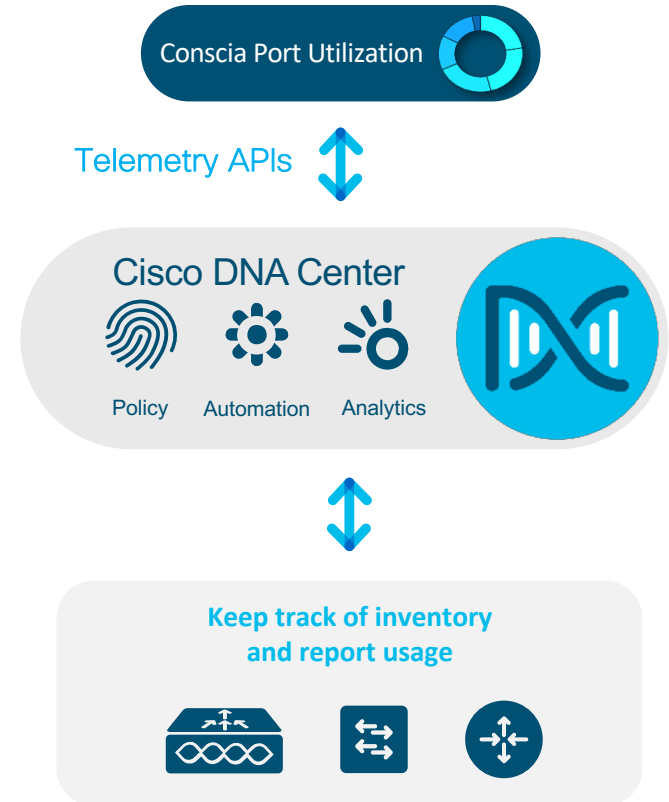
## Solution

Cisco DNA Center tracks all network hardware and is a single source of truth.

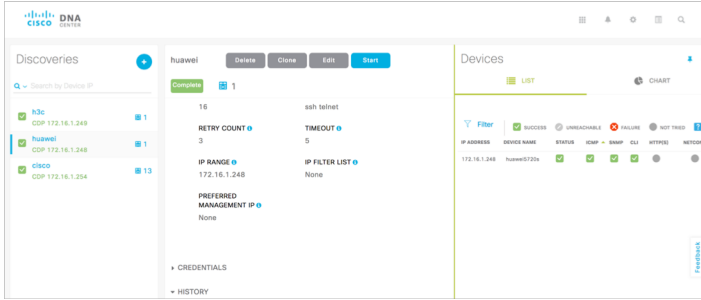
- Conscia application uses a single API across all switches to gather critical information
- Tracks switch status over time to gather and keep port usage information

## Benefits

- Eliminate tedious manual processes that need to be repeated periodically
- Focus on business logic and leave inventory, credential, and connections detail to Cisco DNA Center



# Example: AnyRover and Cisco DNA Center



Device Overview

Name	AnyRover-Test01	#	Interface Name	MAC Address	Status
IP Address	10.101.1.81	1	sif0		Down
MAC Address	N/A	2	tun0		Down
OS Version	N/A	3	lo		Up
Uptime	1 day, 16:29:01.67	4	eth0	00:1e:ac:00:00:20	Up
Product Id	N/A	5	ppp0		Up
		6	wlan0	00:0e:8e:46:16:37	Down

Show 10 entries    Showing 1 - 6 of 6    Page 1 of 1

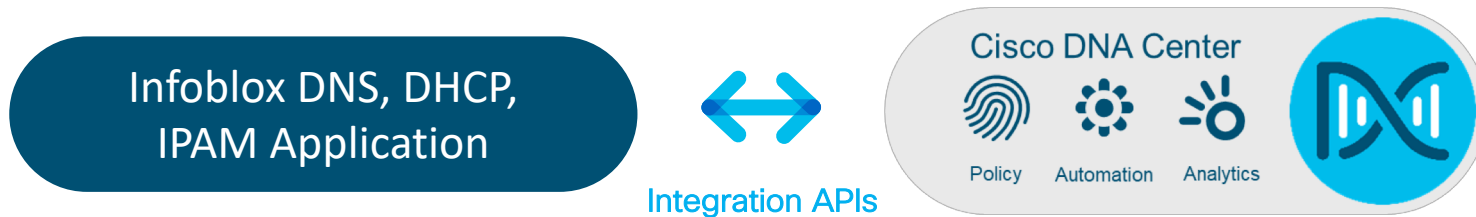
↑↑↑↑  
 SNMP  
 Netconf  
 CLI



AnyRover is a robust metall device, high temperature range with flexible power option (8 - 52V) and offers Mobile IP access via GSM for LAN and WLAN connection.

# Cisco DNA Center Solution

## Consistent IP address pools management



### Problem

IP addresses managed by a standalone system means manual monitoring and no oversight

### Solution

Infoblox DNS, DHCP, and IPAM (DDI) application uses Integration APIs to send IP address data to Cisco DNA Center

1. Operator uses Cisco DNA Center GUI to set up pools that get configured on Infoblox DDI
2. Infoblox DDI sends usage information to Cisco DNA Center for real-time monitoring

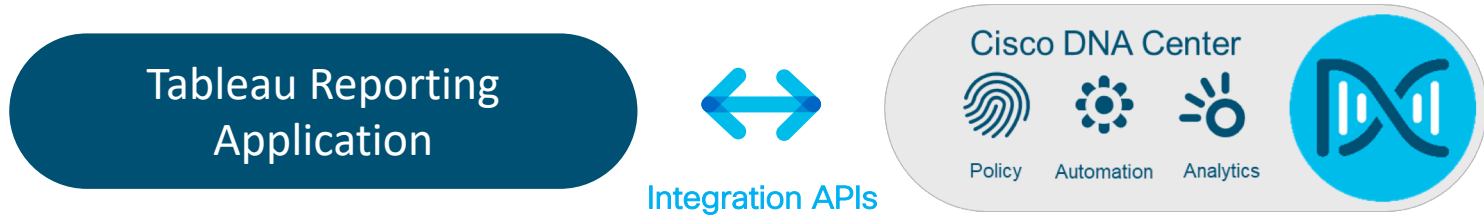
### Benefits

- Ensure full visibility into your IP address usage and effectively monitor endpoints
- Benefit from critical insights obtained from IPAM tools for Assurance



# Cisco DNA Center Solution

## IT service management integration



### Problem

Collected data is not useful in raw. Reporting capabilities are needed to extract useful insights

### Solution

Cisco DNA Center collects a wealth of data that can provide deep actionable insights into network usage and growth

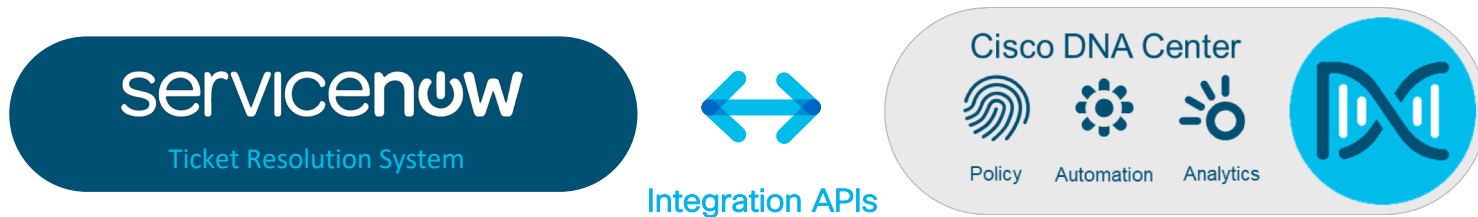
1. Tableau reporting application uses integration APIs to retrieve data from Cisco DNA Center
2. Application merges Cisco DNA Center data with other datasets that provide a comprehensive view across operations

### Benefits

- Key data is collected, stored and correlated
- Use data to benchmark, trend and analyze

# Cisco DNA Center Solution

## IT service management integration



### Problem

Every IT incident needs manual analysis and assessment, requiring multiple handoffs between support teams, all leading to elongated time for resolution

### Solution

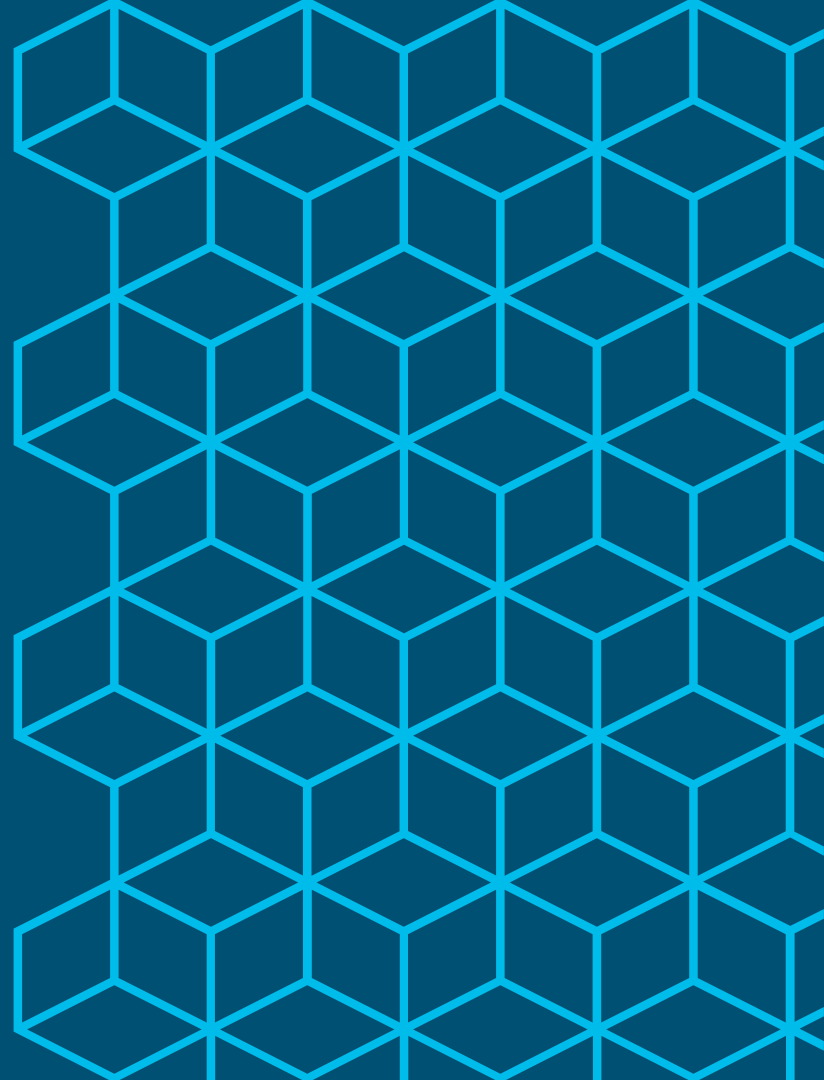
ServiceNow Ticket Resolution System application uses Integration APIs to exchange data with Cisco DNA Center on trouble tickets and their resolution

1. Cisco DNA Center detects network problems and sends information to ServiceNow
2. ServiceNow opens trouble ticket, obtains approvals, and schedules fixes through Cisco DNA Center

### Benefits

- Efficient workflows - flexible integration with reviews, approvals, and change management
- Minimal handoffs – quicker decision making and faster problem resolution

# Cisco DNA Center Platform - References



# Cisco DNA Center Platform Portal



The screenshot shows the Cisco DNA Center Platform Portal homepage. The top navigation bar includes the Cisco logo, 'DEVNET', and the user name 'Saurav Prasad'. Below the navigation bar, there are links for 'DNA CENTER PLATFORM', 'Solutions', 'Capabilities', and 'Use Cases'. On the right side, there are links for 'Learn' and 'Docs'. The main content area features a blue background with a city skyline silhouette. In the center, there is a white oval containing the DNA Center logo, which consists of a stylized 'DNA' in blue and green. Below the logo, the text reads 'The Network Is Open for Business'. Underneath this, a paragraph states: 'Create connections never before possible. Integrate devices from any provider. Transform slow, manual processes into fast, automated workflows.' At the bottom of the main content area, there is a smaller line of text: 'Our suite of developer tools is easy to learn and simple to use. Skip ahead to learn about platform capabilities'.

<https://developer.cisco.com/dnacenter/>  
<https://developer.cisco.com/ecosystem/dnacenter/>

# Cisco DNA Center Platform - Documentation

Documentation > DNA Center Platform

## Cisco DNA Center Platform Overview

Cisco DNA Center is the foundational controller and analytics Center at the heart of Cisco's intent-based network. DNA Center supports the expression of intent for multiple use cases, including base automation capabilities, fabric provisioning, and policy-based segmentation in the enterprise network. DNA Center adds context to this journey through the introduction of Analytics and Assurance. DNA Center provides end-to-end visibility into the network with full context through data and insights.

DNA Center Platform provides an open extensible platform that Cisco customers and partners can use to create value added applications that can be built on top of its native capabilities. You can leverage the DNA Center Intent APIs, Integration APIs, Events and Notification and Multi-Vendor support to enhance the overall network experience by optimizing end-to-end IT processes, Total Cost of Ownership (TCO) and develop new value networks.

### IT and Network System Process

servicenow		ITSM
Infoblox		IPAM
+ a b l e o u		Reporting
인원관리		ITSM
LiveAction		Analytics

### Business and Network Intent APIs

Application Policy Assurance	Software Image Management (SWIM)
Wireless Provisioning	Network Inventory / Discovery
Plug-n-Play Topology	Command Runner
	Template Programmer
	eNFV Provisioning

### X-Domain Integration

Networking	
Security	
Data Center	

### 3rd Party SDKs

Map 3rd Party Network Devices to Data Model  
Level 1 Operations support:  
Discovery, Inventory, Topology, Availability, Health Score

<https://developer.cisco.com/docs/dna-center/>

# Cisco DNA Center Platform – API Reference

The screenshot shows the Cisco DevNet API Reference page for the Intent API. The page is titled "Intent API" and is for Cisco DNA Center Platform v. 1.2.8 (GA). It includes a search bar, a "Select API Version" dropdown, and a list of API endpoints categorized by method (GET, POST, PUT, DELETE). The endpoints are color-coded by method: GET (blue), POST (green), PUT (orange), and DELETE (red). The page also includes a "Tag" section for "Network Discovery" and "PnP".

Select API Version ▾

Intent API  
Cisco DNA Center Platform v. 1.2.8 (GA)  
[Terms of service](#)

**Template Programmer** Show/Hide | List Operations | Expand Operations

GET	/dna/intent/api/v1/template-programmer/project	Get Projects
POST	/dna/intent/api/v1/template-programmer/project	Create Project
PUT	/dna/intent/api/v1/template-programmer/project	Update Project
GET	/dna/intent/api/v1/template-programmer/template	Gets the templates available
PUT	/dna/intent/api/v1/template-programmer/template	Update Template
POST	/dna/intent/api/v1/template-programmer/template/deploy	Deploy Template
POST	/dna/intent/api/v1/template-programmer/template/version	Version Template
DELETE	/dna/intent/api/v1/template-programmer/template/{templateId}	Delete Template
GET	/dna/intent/api/v1/template-programmer/template/{templateId}	Get Template Details
GET	/dna/intent/api/v1/template-programmer/template/deploy/status/{deploymentId}	Get Template deployment status
DELETE	/dna/intent/api/v1/template-programmer/project/{projectId}	Delete Project
GET	/dna/intent/api/v1/template-programmer/template/version/{templateId}	Get Template Versions
PUT	/dna/intent/api/v1/template-programmer/template/preview	Preview Template
POST	/dna/intent/api/v1/template-programmer/project/{projectId}/template	Create Template

**Tag** Show/Hide | List Operations | Expand Operations

**Network Discovery** Show/Hide | List Operations | Expand Operations

**PnP** Show/Hide | List Operations | Expand Operations

POST	/dna/intent/api/v1/onboarding/pnp-device/unclaim	Un-Claim Device
GET	/dna/intent/api/v1/onboarding/pnp-device/sacct/{domain}/vacct/{name}/sync-result	Get Sync Result for Virtual Account

<https://developer.cisco.com/site/dna-center-rest-api/>

# Cisco DNA Center Platform – Code Exchange

The screenshot shows the Cisco DevNet Code Exchange interface. At the top, there is a navigation bar with the Cisco DevNet logo, a search bar, and links for 'SIGN UP FREE' and 'LOG IN'. Below the navigation bar, the main heading reads 'Discover code repositories related to Cisco technologies'. A sub-heading states: 'Discover, learn, build, and collaborate on curated GitHub projects to jumpstart your work with Cisco platforms, products, APIs, and SDKs'. A search bar with the placeholder text 'What listing are you looking for?' is present. Below the search bar, there are four product category buttons: 'Cisco DNA Center', 'Cisco Webex', 'Cisco Kinetic', and 'Cisco Meraki'. The 'Cisco DNA Center' button is highlighted. Below the categories, there are two dropdown menus for 'Language' and 'Technology'. The 'Sort by' dropdown is set to 'Recommended'. The main content area displays three code repository cards:

- Java** (9 stars, 1 fork): CiscoDevNet **DNAC-Android-SDK**. Sample android app created with DNAC android SDK; app intent - list the managed devices.
- Swift** (2 stars, 1 fork): CiscoDevNet **DNAC-Assurance-on-the-go-iOS-App**. DNA Center (DNAC) Assurance on-the-go IOS sample app that gives you business-critical insights on mobile devices.
- JavaScript** (8 stars, 0 forks): CiscoDevNet **DNAC-ClaimAP-Mobile-App**. DNACenter ClaimDevices mobile app to claim Day-0 or DNA-C supported Plug-n-Play(PnP) devices and provision it.

<https://developer.cisco.com/codeexchange/platforms/dnac>

# Sandboxes and Learning Labs

## Cisco DNA Center Sandboxes

Version 1.2.6

**ALWAYS ON**

### DNA Center v.1.2.6 Always-On Sandbox

- Access at any time without making a reservation or using VPN connection
- Perfect for learning the DNA Center GUI or experimenting with the REST API
- Provides access to a pre-configured network topology running on genuine Cisco hardware
- Cannot configure the network or devices on it
- Cannot activate and enforce policy on network devices
- Because this sandbox is always available to all users, any other user may potentially overwrite your work at any time.

Version 1.2.6

**REQUIRES RESERVATION**

### Cisco DNA Center v.1.2.6 Lab 1

- Requires a reservation and setup of VPN
- Provides your own private lab environment for the duration of the reservation, and you can allow other users to access the lab by invitation.
- Perfect for working on lighter-weight application development projects that do not require a large network
- Provides access to pre-configured network topologies running on genuine Cisco hardware
- You can configure the hardware and network topology.
- Provides a Linux VM development machine that resides on the lab network.
- Supports automated discovery of the hardware by Cisco DNA Center as well as enforcement of policy

Version 1.2.6

**REQUIRES RESERVATION**

### Cisco DNA Center v.1.2.6 Lab 2

- Requires a reservation and setup of VPN
- Provides your own private lab environment for the duration of the reservation, and you can allow other users to access the lab by invitation.
- Perfect for working on lighter-weight application development projects that do not require a

## Learning Labs

Tracks Modules Labs Challenges Help Feedback

### Cisco DNA Center Programmability

This learning track explores the programmability capabilities of Cisco DNA Center. You'll see how to leverage the APIs to explore what makes up, and who is on your network, gain a better understanding of how the network is operating with Cisco DNA Assurance, manage the software lifecycle, and so much more!

2 Modules  
7 Learning Labs  
2 Hours 15 Minutes

### Choose a module to start learning

Please login to see your progress....

#### Introduction to Cisco DNA Center REST APIs

Learn how to get started with the Cisco DNA Center REST APIs. Covering authentication and some simple examples, these Python samples will set you on your way to automating the Intuitive Network with Cisco DNA Center.

45 Minutes

#### End to End Visibility and Assurance with Path Trace and Cisco DNA Center Platform

Ever wish you could see exactly how traffic went from Point A to Point B across the network? Would it be helpful to get device and interface details for every hop across the network? With Cisco DNA Center Path Trace your wish is fulfilled. Even better, with the Cisco DNA Center Platform APIs, you can put Path Trace to work wherever you want.

#### Execute Commands Across the Network with Cisco DNA Center Platform and Command Runner

With Command Runner and Cisco DNA Center, you can quickly execute operational and configuration commands across your entire network. And with the Cisco DNA Center Platform APIs, you can now use this feature as part of any other script or integration. Learn how in this lab.

#### Quickly Deploy Configuration Templates with Cisco DNA Center Platform and Template Programmer

Configuration templates are common methods of building and maintaining consistent network configurations, and Cisco DNA Center offers template based configurations for the network. And with the Template Programmer APIs offered with Cisco DNA Center Platform, you can now extend this feature to your own scripts and integrations.

1 Always On and 4 Reservation based Sandboxes



# *Summary*

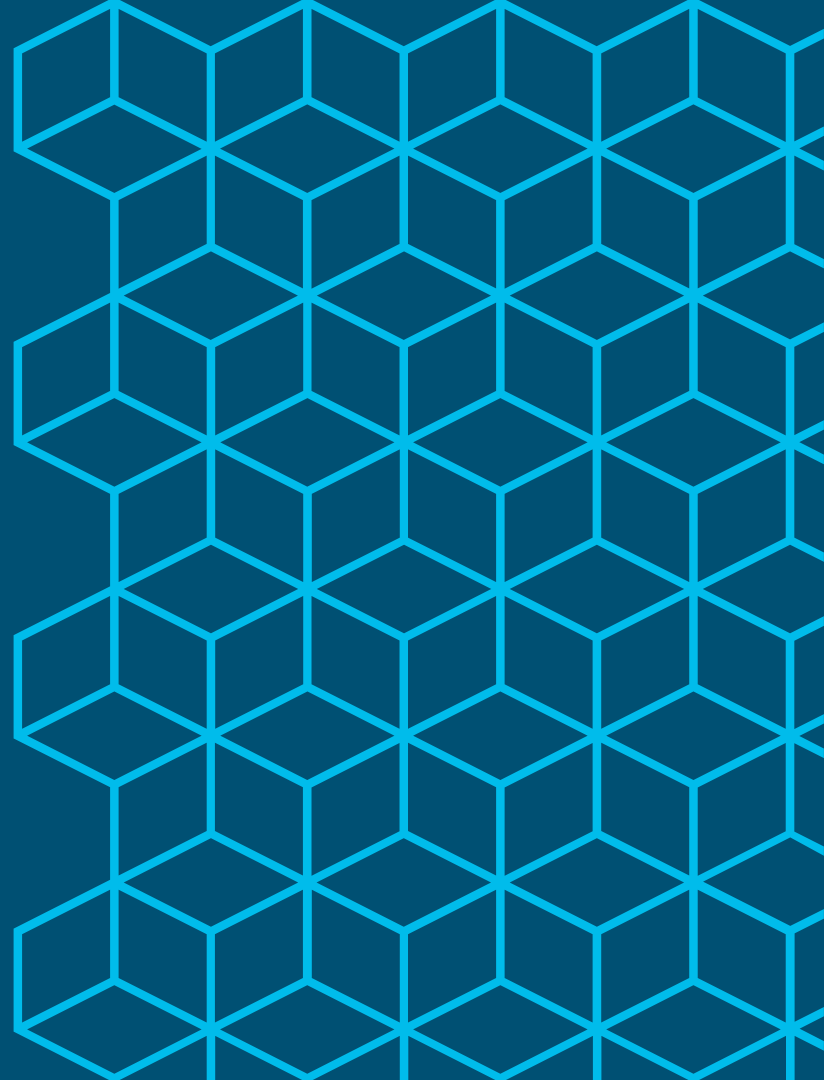
The Need for Intent-Based Networking

Cisco DNA Automation

Cisco DNA Assurance

Cisco DNA Center Platform

Q & A





Thank you