From Prime Infrastructure to Software Defined Network (SDN) Management with Cisco DNA-Center

Soren Dulong Andreasen
Stefan Leemann

DGTL-BRKNMS-2573

Our Mission statement

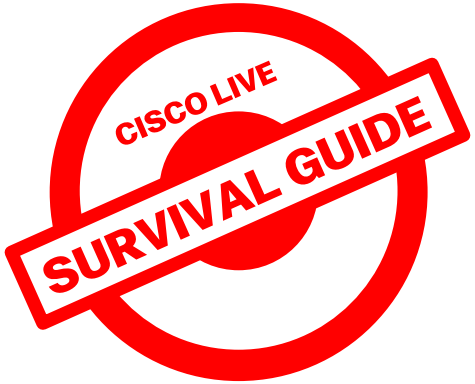
Get all the benefits of Cisco DNA-Center with Co-Existence to Prime Infrastructure

Soren Dulong Andreasen

soren@cisco.com

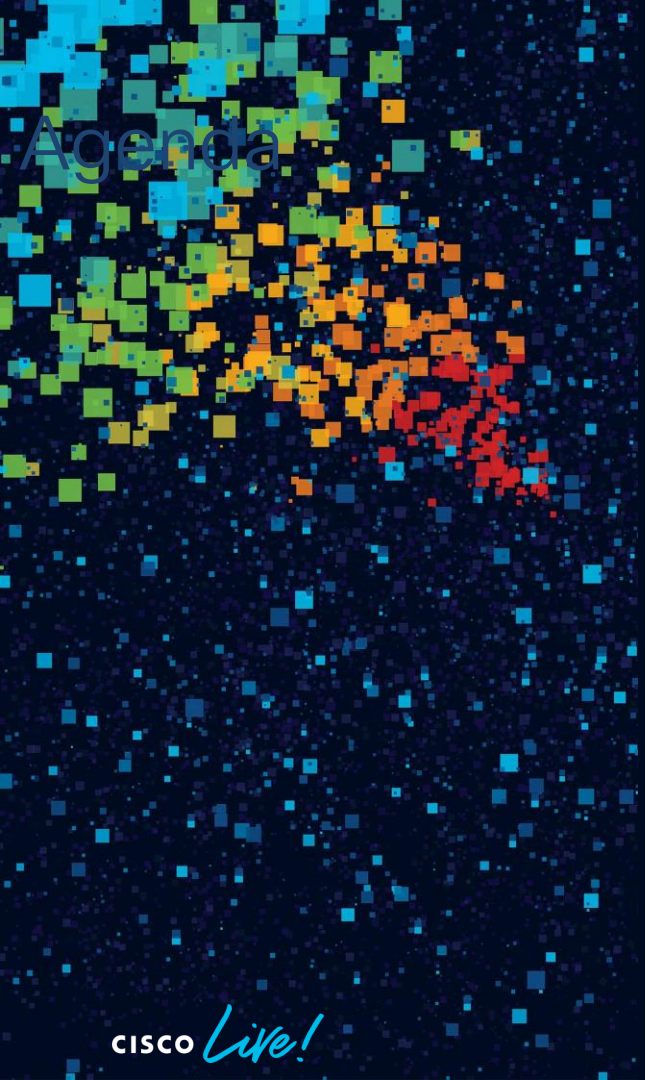
Stefan Leemann

stleeman@cisco.com



We broke our session into parts, so you can skip sections if you prefer so.

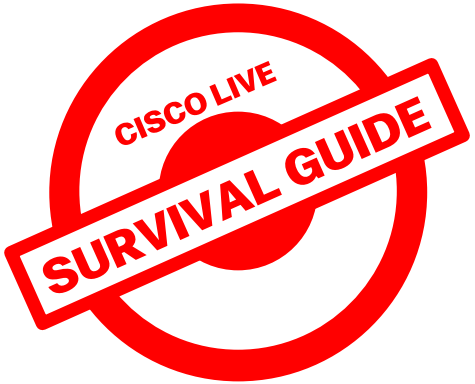
- Use the Agenda slide which includes timing to jump to the sections that interest you.
- If you are watching the session form start to end, we suggest you take a few breaks in between, in the breaks drink some water, tea or coffee. We also suggest to do some light exercise in the breaks



Agenda

1. Introduction
2. Change in Paradigm in Network Management
3. Migration from Prime Infrastructure to Cisco DNA-Center
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

Introduction

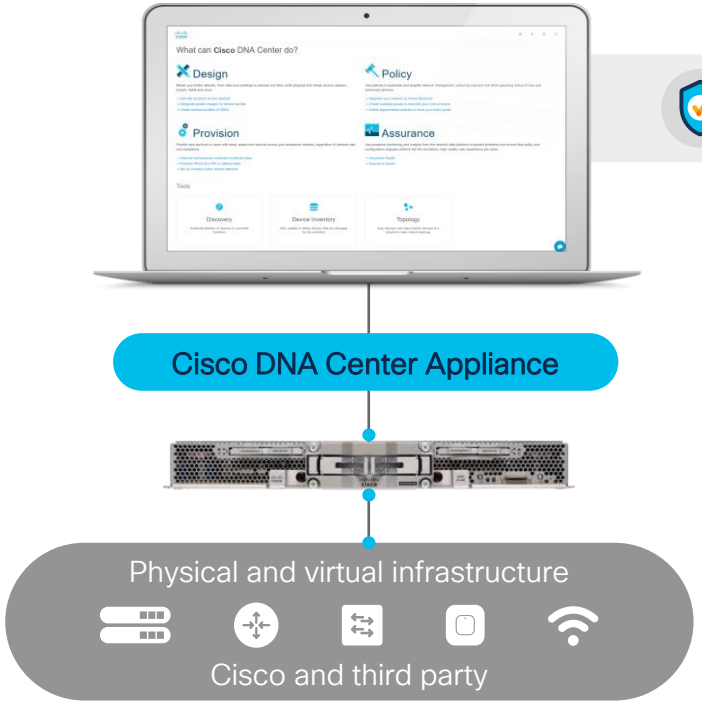


For Your Reference

Cisco DNA Center

Intent-based controller for the enterprise

Cloud-Enabled



Policy | Provision | Design | Assurance

- Controller-based automation and analytics
- Campus, branch, extended enterprise, wired and wireless
- 360-degree open platform
- Fully integrated, distributed security
- Analytics, machine-learning driven

Agenda

1. Introduction
2. Change in Paradigm in Network Management
3. Migration from Prime Infrastructure to Cisco DNA-Center
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

Prime Infrastructure

Traditional Network Management

- Software Image Distribution
- Configuration Archive/Backup
- Templating for Automation
- Reporting
- Assurance
- Events
- Tons of data, but not enough insights.
- Semiclosed system with predefined configurations.

Cisco DNA Center

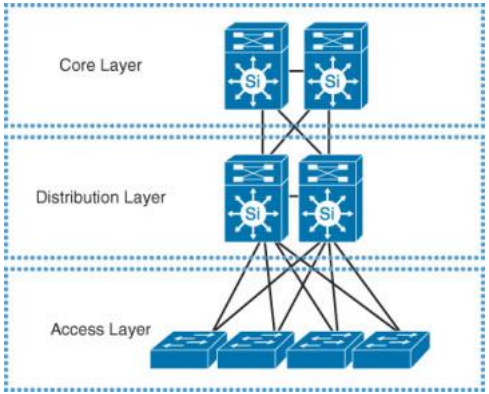
PARADIGM SHIFT

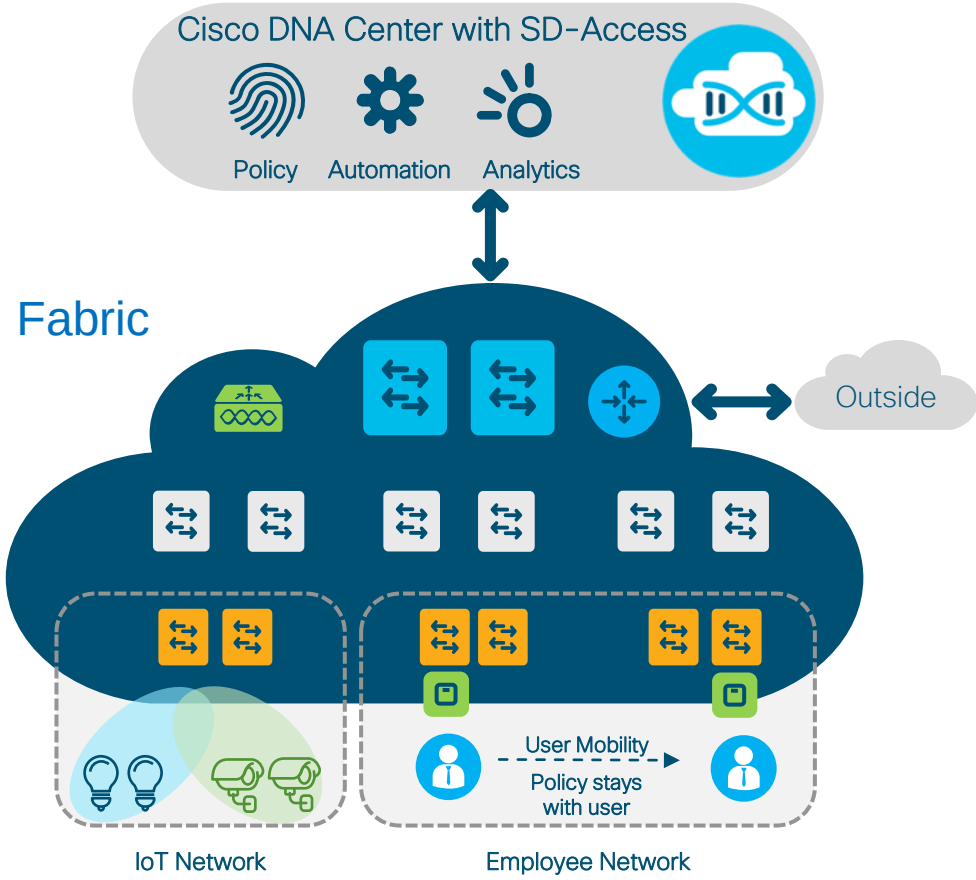
Intent base Network Management

- No events/alarms, but insights and impact analytics with Guided remediation
- Automation, day0, day1, day2
- Policy and segmentation control
- Software update (ITSM, Compliance)
- Network telemetry data collection
- Baselining over time, baseline against others
- No manual configuration required
- API and Business API

You decide what Cisco DNA-Center will do for you

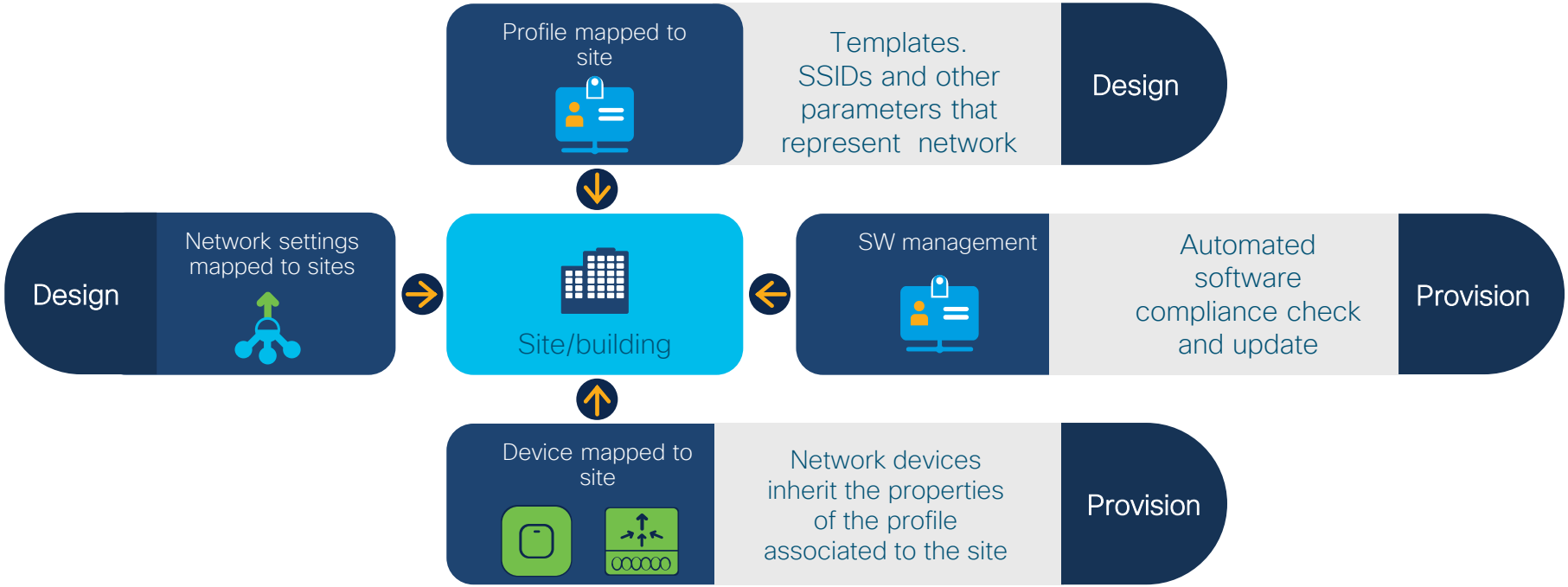
Network Management of classic-Design Enterprise networks





PARADIGM SHIFT

An Intent Based deployment model



Intent-based workflows

Automated deployment

Cisco best practices

DNA Center and Prime – Automation

		Prime	DNA Center
Core Functions	Wireless Maps for AP Placements		★
	CMX Integration	MSE Integration	★
	AP Onboarding		★
	AP Day 2 Changes		Roadmap *
	WLC Configuration – Day 0/N		★
	Brownfield Support (Learning from WLC)		★
	SWIM		★
	Reports		Three reports today (more in roadmap *)
Advanced	Configuration Audit & Compliance		Roadmap *
	Rolling AP Upgrades		
	Bulk Configuration changes on multiple WLC's		
	Position by 2 walls and 3 points		Roadmap *
Differentiators	Auto Placement of AP's using CAD Files		Roadmap *
	Location/IP/Switchport based AP Onboarding		Roadmap *
	Unified configuration flow for all architectures		
	Flex Enhancements for SWIM		Roadmap *

For Your Reference

★ Better in DNAC

* subject to change

DNA Center and Prime – Assurance

		Prime	DNA Center
Core Functions	Wireless heatmaps for troubleshooting		★
	Application Visibility		★
	Reporting		Three reports today (more in roadmap *)
	Health Dashboards		★
	Real Time Client, Network and App Data	SNMP Based	2-90 Sec ★ (Streaming Telemetry)
	Rogue Management & Detection		★
	wIPS		Roadmap *
	*Switch Port Tracing		Roadmap *
	*ISE Integration		
	WGB Client Support		Roadmap *
	CMX Integration for Tracking Clients		
Differentiators	Intelligent Packet Capture		
	Proactive Sensor Testing		
	iOS Wi-Fi Analytics		
	Guided Issue Remediation		
	Application Experience		★
	Historical Troubleshooting		★
	Integration with ITSM (ServiceNow)		

For Your Reference

★ Better in DNAC

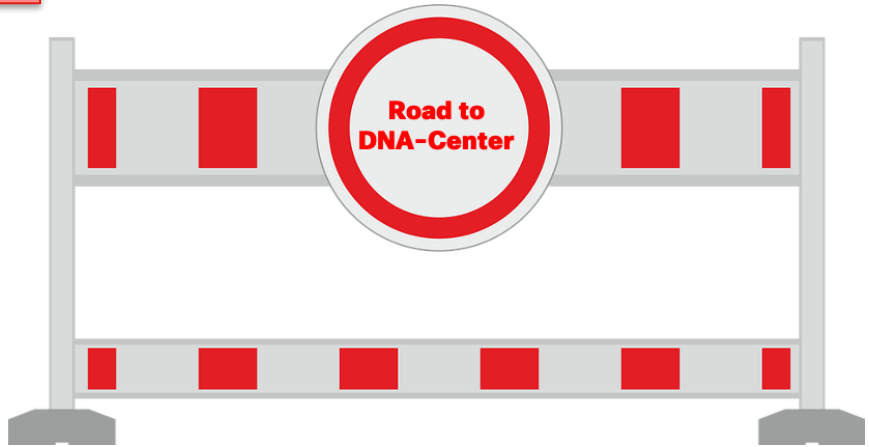
* subject to change

Agenda

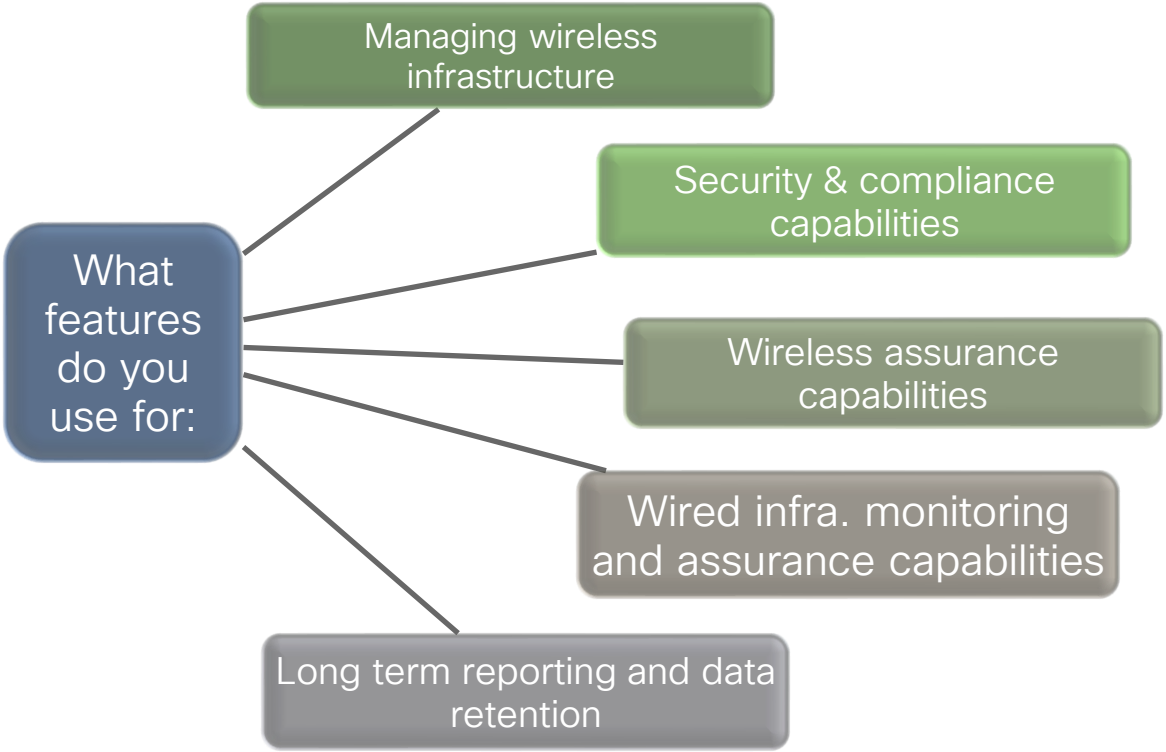
1. Introduction
2. Change in Paradigm in Network Management
3. Migration from Prime Infrastructure to Cisco DNA-Center
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

Let's first address the Prime Infrastructure to Cisco DNA-Center Roadblocks

- Prime/DNA-Center feature parity?
- What size Appliance will I need?
- How do I manage legacy Cisco devices?



Prime/DNA-Center feature parity considerations



What size Appliance will I need?

The two main parameters that decides which Cisco DNA-Center appliance that you need are :

How many sites do you manage today with Prime?

How many devices do you need to manage? No. of Aps, WLCs and Switches

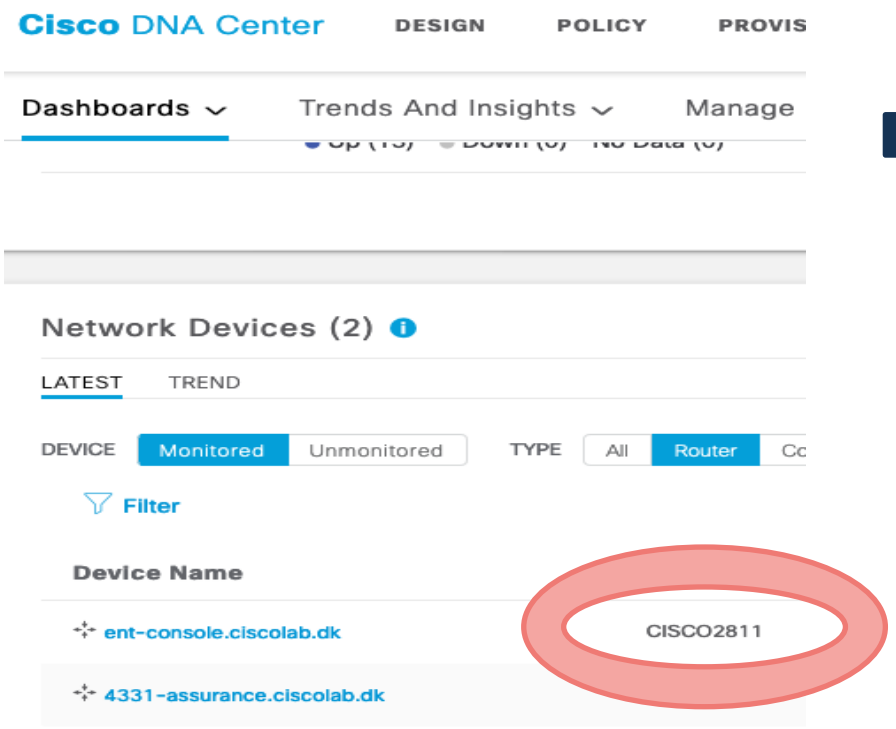
For Your Reference



Hardware description	DN2-HW-APL (entry) Cisco UCS C220 M5 Rack Server 44 cores	DN2-HW-APL-L (mid-size) Cisco UCS C220 M5 Rack Server 56 cores	DN2-HW-APL-XL (large) Cisco UCS C480 M5 Rack Server 112 cores
Number of devices (switch, router, wireless controller)	1,000	2,000	5,000
Number of wireless access points	4,000	6,000	13,000
Number of wireless sensors	600	800	1,600
Number of concurrent endpoints	25,000	40,000	100,000
Number of transient endpoints (over 14-day period)	75,000	120,000	250,000
Ratio of endpoints: Wired	Any	Any	40,000
Wireless	Any	Any	60,000
Number of ports	48,000	192,000	480,000
Number of site elements	500	1,000	2,000
Number of wireless controllers	500	1,000	2,000
API rate limit	50 APIs/min	50 APIs/min	50 APIs/min

• How do I manage legacy Cisco devices‘

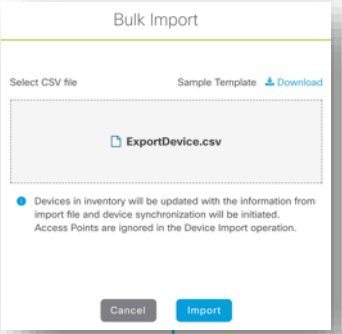
- Well, let me tell you a secret..



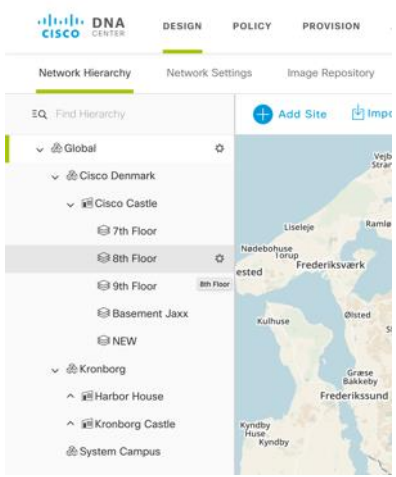
Getting started with Design

How to create your design : Site Hierarchy

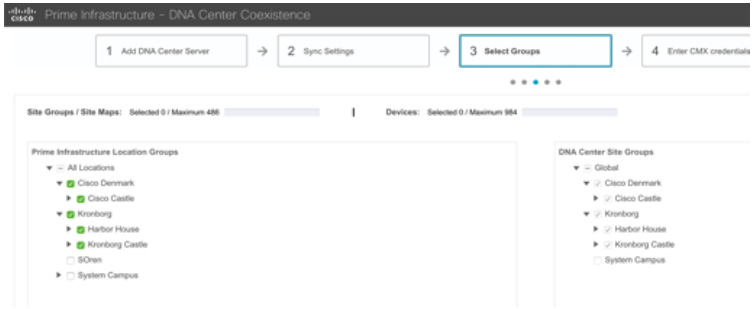
2) Manually Export /Import from Prime



1) Manually



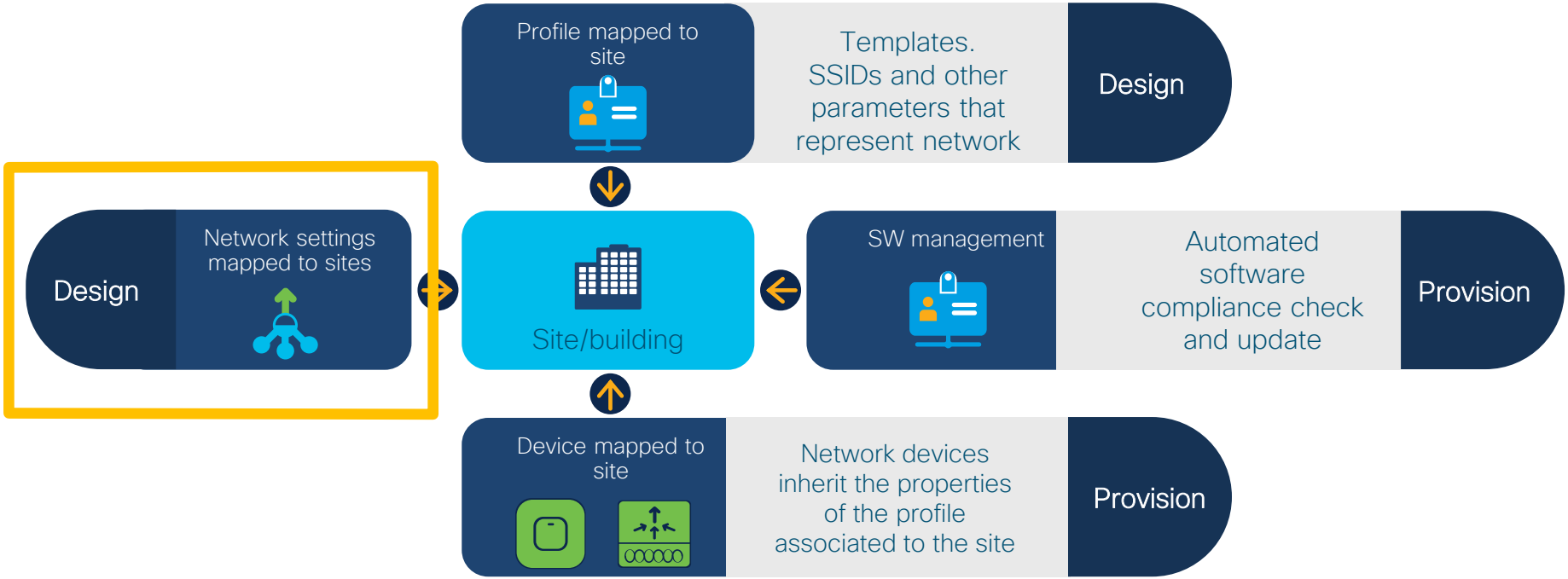
3) Prime 3.5 Co-existence Tool



DNA Center

PARADIGM SHIFT

Network settings



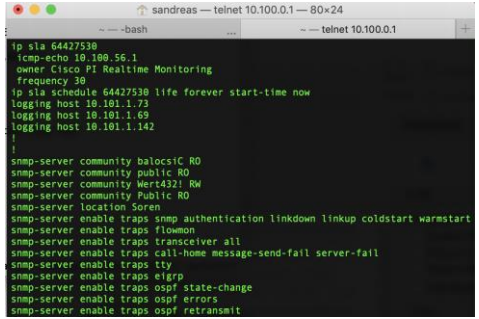
Intent-based workflows

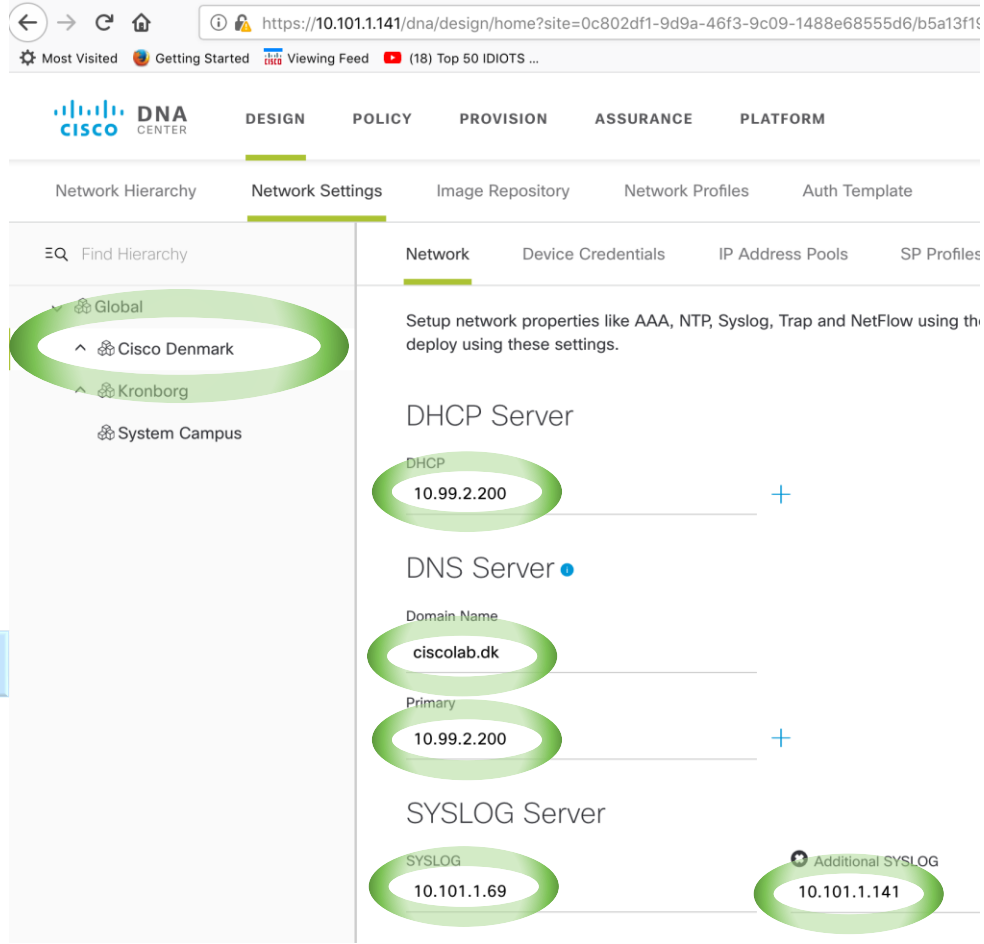
Automated deployment

Cisco best practices

Design -> Network Settings

Be carefull! Cisco DNA-Center will configure these settings instantly on all devices based on location etc.

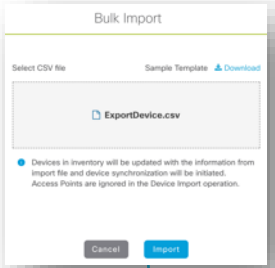




Getting devices into Cisco DNA-Center

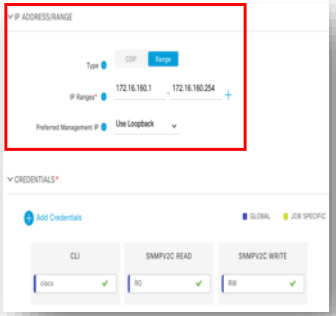
2) Manual add into Inventory

3) Bulk Import via CSV

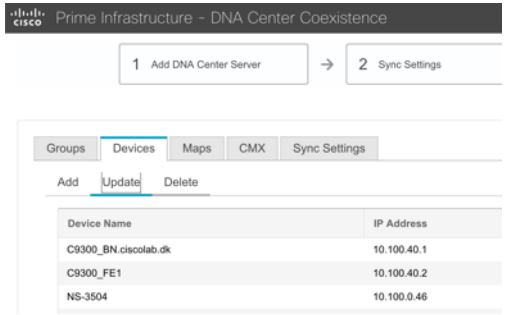


4) Plug and Play

1) Discovery Job



5) Prime ->Co-Existence



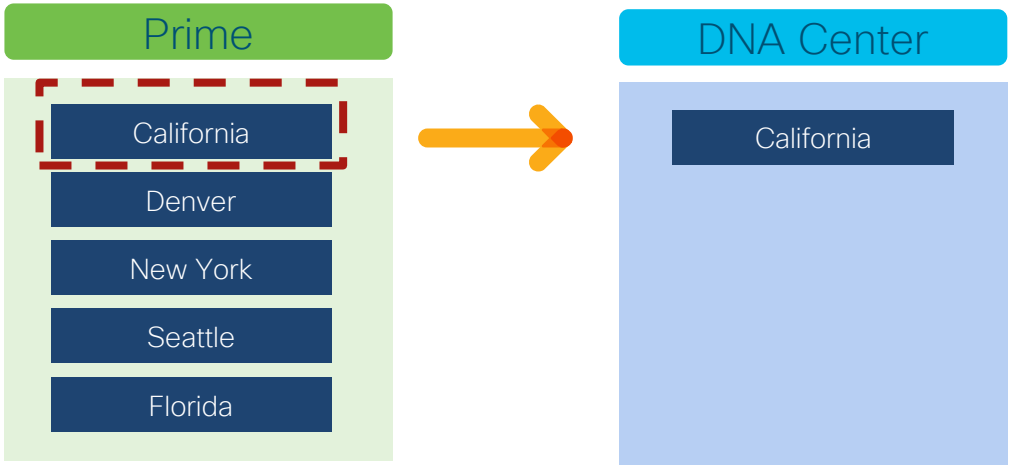
DNA Center

Co-Existence Tool to assist with Migration

Co-existence Objectives

1. Start using Cisco DNA Center with minimal efforts for Prime Infrastructure customers
2. Migrate Devices, Location Groups, Maps and CMX Servers from Prime Infrastructure to Cisco DNA Center seamlessly using the workflow
3. Allow Incremental updates to the migrated dynamically
4. Make it easy to run Prime Infrastructure and Cisco DNA-Center in parallel

Co-existence Overview



- Site
- Buildings
- Floors along with floor plan
- Routers
- Switches
- WLC
- AP's
- AP Position on the floor maps
- Floor Elements like Exclusion/Inclusion Regions, Obstacles etc
- CMX Servers

Jump start with DNA Center with a readily available site layout

Start the Cisco DNA-Center Co-existence tool

For Your Reference

https://10.101.1.69/webacs/loginAction.do?action=login&product=wcs&selectedCategory=en#pageId=system_setting_page

Most Visited | Getting Started | Viewing Feed | (18) Top 50 IDIOTS ...

Prime Infrastructure

Administration / Settings / System Settings

Search Menu

- Dashboard
- Monitor
- Configuration
- Inventory
- Maps
- Services
- Reports
- Administration

System Settings

Search All

- General
  - Account Settings
  - Data Retention
  - Guest Account
  - Help Us Improve
  - Job Approval
  - Proxy
  - Login Disclaimer
  - Report
  - Server
  - Software Update
  - Support Request
  - DNA Center coexistence

General

DNA Cen

DNA C

Yo

Network Architecture Center ... networking solution for managing application user experience in the enterprise.

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. To know more about DNA Center, visit http://cisco.com/go/dna

You can migrate devices, site groups, associated site maps and CMX data from Prime Infrastructure to DNA Center and manage your enterprise network over a centralized dashboard.

Launch DNA Center coexistence

1

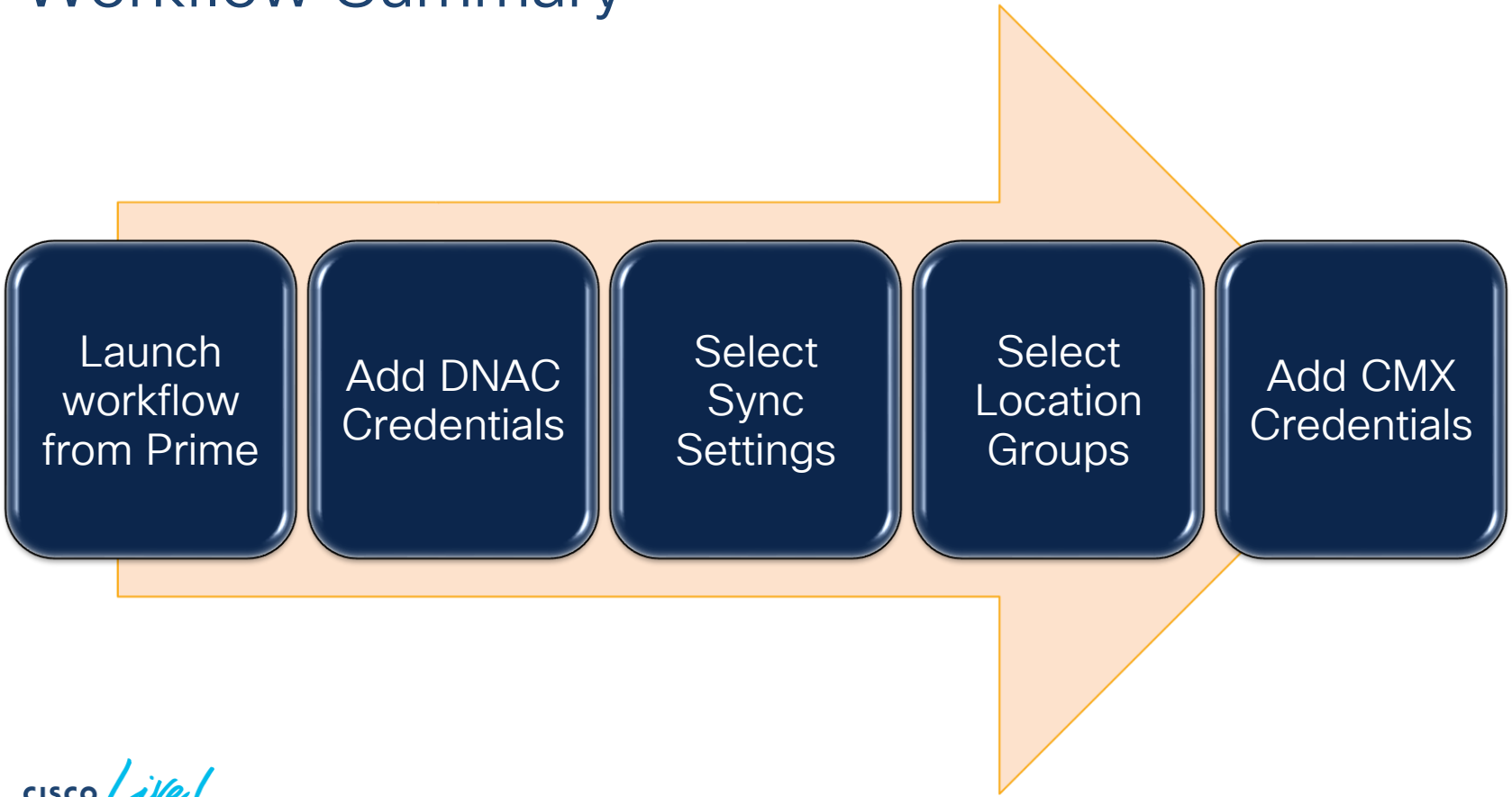
2

3

Note : First time you click the link the tool itself has to start, this typically takes 3-5 minutes

Demo,
Prime Co-existence

Workflow Summary



Sync Behavior

For Your Reference

Force Sync

- Force sync essentially pushes all data, based on selection of groups, irrespective of the previous data push from PI to DNA Center
- For any setting change to come into effect, a force sync has to be done
- Initial sync from PI to DNAC will always be a force sync

Auto Sync

- Auto Sync is an incremental, dynamic synchronization of the data from PI to DNAC based on the earlier selection
- Any changes to groups association and device credentials will be synced
- CMX and Maps are not in scope of auto sync and need to triggered via the Force Sync option
- Auto sync has 2 modes of operation :
  - ✓ Changes to the already synced groups and devices only are pushed to DNAC
  - ✓ Any new groups added as a sub-group to the already selected location groups and its device association are pushed to DNAC

Some comments on Cisco DNA-Center co-existence tool (1/4)

For Your Reference

Supported Prime Infrastructure versus Cisco DNA-Center versions can be found in the Cisco Prime Infrastructure 3.X Administrator Guide (see upcoming slide)

For Catalyst 9800 WLC you will need to manually add Netconf “port” and SSH credentials

10.5.0 and above versions of CMX is supported

SNMPv1 not supported in DNA-Center

PI user credentials has to be Root

Area/Site/floor names has to have be less then 32 characters and not contain ”/”

What happens behind the scenes: API calls between the Co-exist tool and Prime Infrastructure and between Co-exist tool and Cisco DNA-Center

Some comments on Cisco DNA-Center co-existence tool (2/4)

For Your Reference

Migration of 500 groups + 1000 devices using force sync will take between 20-30 minutes

Removal of many groups/devices/maps takes more time(hours)

Tip : If you are having issues, try and do it manually to see the error messages. You can also have a look in the logfile on Prime "/opt/CSCOlumos/logs/process_dnac_migration.log"

Adding an AP or moving and AP on a MAP requires a manual "force sync" from the Co-exist tool

Some comments on Cisco DNA-Center co-existence tool (3/4) Prime Infrastructure 3.7

For Your Reference

Appliance Type	Site Groups/Site Maps	Devices
DN1-HW-APL DN2-HW-APL	500	1000
DN2-HW-APL-L	1000	4000
DN2-HW-APL-XL	2000	5000

Cisco DNA Center Version	Supported/Recommended
1.2.1	Supported
1.2.2	Supported
1.2.3	Supported
1.2.4	Supported
1.2.5	Supported
1.2.6	Supported & Recommended
1.2.8	Supported & Recommended
1.2.10	Supported & Recommended
1.2.10.4	Supported & Recommended
1.2.11	Supported & Recommended
1.2.12	Supported & Recommended
1.3.0	Supported & Recommended
1.3.0.1	Supported
1.3.0.2	Supported
1.3.0.3	Supported & Recommended
1.3.1	Supported & Recommended

Some comments on Cisco DNA-Center co-existence tool (4/4)

For Your Reference

- If your WLC('s) is not assigned to a site(unassigned) or its assigned to the "System Campus", then it will not be exported to DNA-Center
- Sensor(s) will be deleted from maps if already added in DNA-Center

Upcoming enhancements in PI 3.7.1/3.8

For Your Reference

Error Message enhancement: On failure of DNAC Server integration, error messages have been changed to adhere to exact reason of failure like “Certificate Error, Credential error, unsupported version and Server not reachable

UI Enhancements:

Allow to select more than 500 records in Group selection screen

Provided “Progress Bar” widget in summary screen tab while the operation is in progress

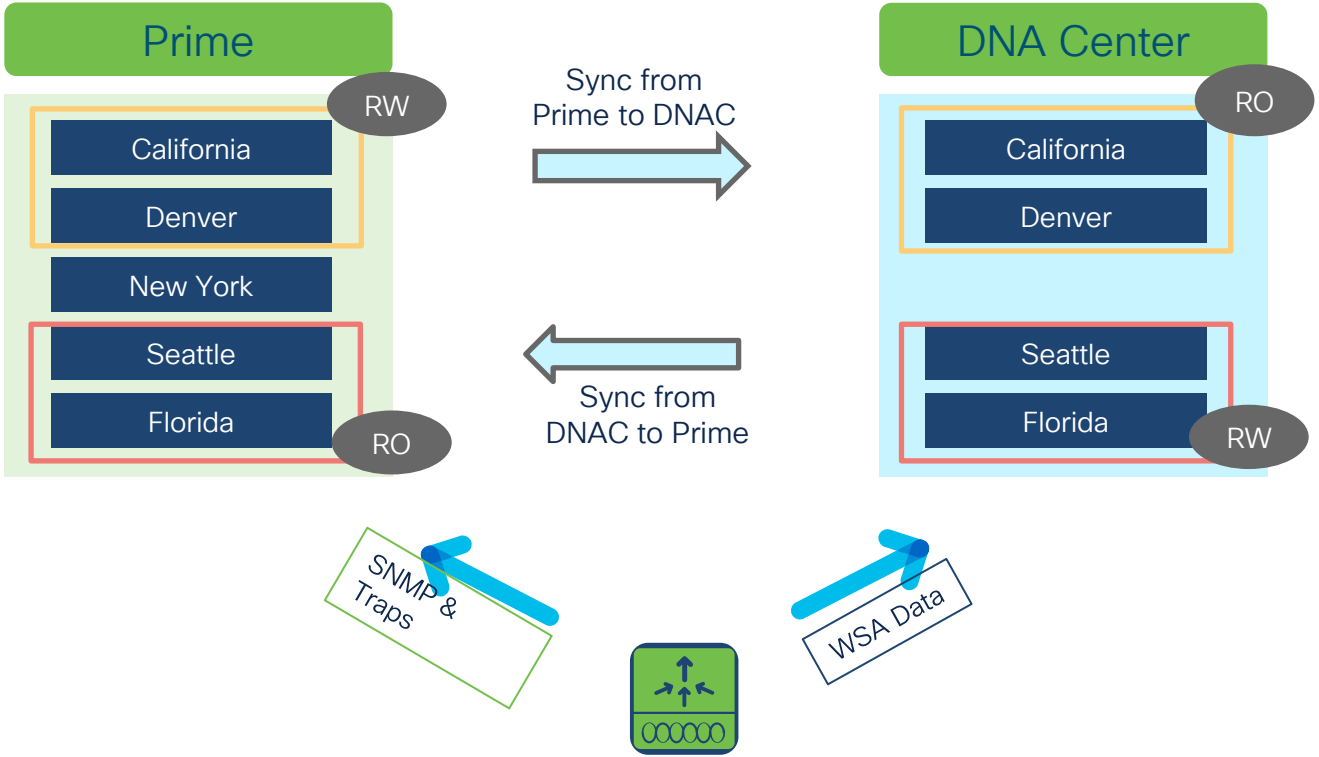
Ability to guess Country based on Civic address or Geo location

Avoiding stale entries of “Site” from being migrated to DNAC and displaying the stale groups as strike through

Avoid database issues by blocing dynamic updates when Cisco DNA Center is upgraded to unsupported version

Future

Where do we go next?



RMA tool

Device Replacement – RMA

Eliminate manual interventions for device replacements

Unified Workflows

- Common workflows to replace Switch, Router, Access Points*, Sensors*, C9800 WLC*
- Restores Image, Configuration, License
- Like to like device replacement

RMA Operations

- Replace device in ISE
- Replace device in Cert server
- Copy license from old device to new device
- Replace device in DNAC inventory
- Preserve KPI trends for old device

Single workflow for Wired and Wireless hardware replacement

* Roadmap

Why RMA in Cisco DNA Center?

Request RMA
↓
Unpack box
↓
Find blue console cable
↓
Download correct image, partly configure device
↓
Remove License from old device
↓
Install License on new device
↓
Find latest config
↓
Download latest config from Prime
↓
Download new Certificate
↓
Resync inventory in Prime or DNA-Center
↓
Update ISE with new device serial#
↓
Shutdown device (did you save the config?)
↓
Replace Device

Prime Infrastructure

Why RMA in Cisco DNA Center?

Cisco DNA-Center

Request RMA and note down Serial number of new device

Mark device for replacement

Follow device replacement workflow

Unpack and Replace device

Wifi AP refresh

Coming soon to a cinema near you..

Demo,
RMA tool

Key Points for RMA from 1.3.1

For Your Reference

- Exact PID to PID (C9300L-48UXG-2Q to C9300L-48UXG-2Q)
- Supports SD-Access
- RMA Methods:
  - **Zero-Touch RMA** - Replacement device is connected to Cisco DNA Center via PnP. No manual configuration on device required. (For SD-Access, DHCP should be configured on the "upstream" device)
  - **One-Touch RMA** - Replacement device is manually configured via console with basic IP and mgmt. credentials first so it can be discovered by Cisco DNA Center
- Unclaimed state
  - -Device did PnP and was redirected to DNA-Center
  - -Device was added to DNA-Center manually
  - -Device was learned from Smart Account PnP portal

Prerequisites for RMA in 1.3.1

For Your Reference

- Any device can be marked for replacement, but replacement workflow can only be done for a device that is unreachable
- Only “Managed” and “Not Provisioned” devices in Inventory and “Unclaimed” devices in Plug and Play are eligible as replacement devices for RMA.
- For Zero-Touch RMA, faulty device should be assigned to site before failure.
  - If it is not assigned to site before failure, it can be recovered only by One-Touch RMA method (via discovery).
- Software image of faulty device should be in repository of Software Image Management (SWIM).
- Replacement device should be connected to neighbor devices on the same port(s) as faulty device in topology. (Well,, Same vlan/subnet is enough)

Limitations for RMA in 1.3.1

For Your Reference

Not Supported:

- Stack Switch, StackWise Virtual (SVL), SUP(s) in Modular Switches, Nexus Switches
- Access Points, Wireless Sensors and Wireless Controllers (AireOS, C9800 or C9800 Embedded).
- Routers with network modules such as UCS-E*, SM-X-ES3*, NIM-SSD, SSD-MSATA-200G
- SDA: Extended node and Fabric-in-a-Box.

License:

- Support only restoring of DNA/Network Essential and DNA/Network Advantage licenses.
- Restoration of legacy switching licenses (e.g. LAN base, IP base and IP service) and routing licenses (IP base, security and etc.) is not supported. Note that License Manager does not show license info if switches with legacy license are running image prior to 16.8.
  - Workaround: Configure legacy licenses manually before triggering replacement in RMA workflow

Limitations for RMA in 1.3.1

For Your Reference

Configuration:

- The running config is archived only at initial discovery of device and at 23:00 daily.
- vlan.dat on switch is archived same way as the running config.

Zero-Touch RMA via PnP

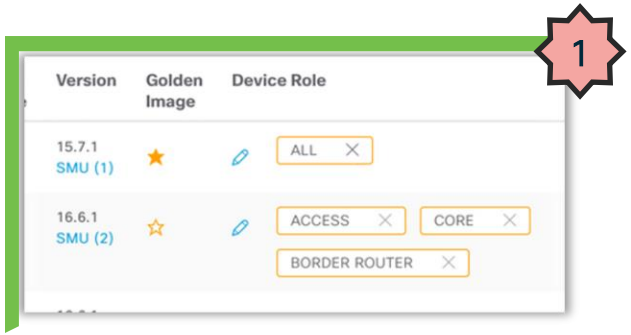
- When new device is claimed via PnP for RMA, if it is reloaded 1st time for image activation, DHCP IP on new device may change, which could cause image validation failure in RMA.

Certificate

- Support revocation of device certificate on faulty device if it is issued by Cisco DNA Center PKI, but does not support request and installation of device certificate by same CA on new device yet.
- Do not support revocation, request and installation of device certificate if it is issued by any CA outside Cisco DNA Center, e.g. auth certificate on router for DMVPN not issued by Cisco DNA Center PKI.

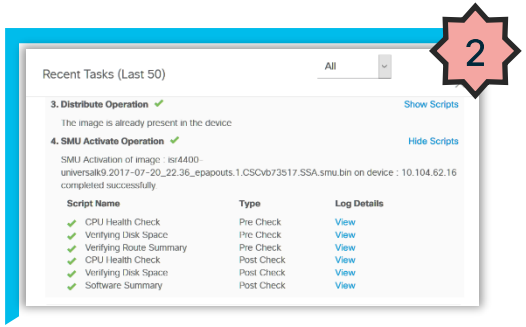
SWIM

Core Principles of Software Upgrade with DNA Center



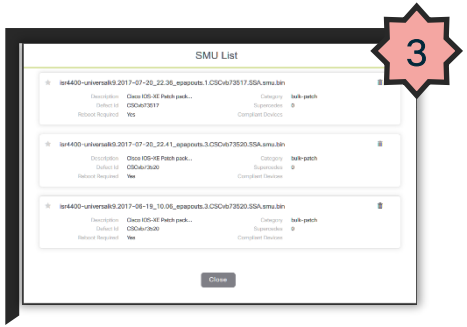
Intent based Network Upgrades

Standardization of Software by Network device role, device type and location



Seamless Upgrades

Pre/Post check validations with rollback provide confidence for upgrades



Reduce Downtime with Patching

Upgrade only what is needed with minimal to zero downtime

Software Image Management with DNA-Center

Note: Marking a software version as Golden does not update the device automatically

What can SWIM do for you:

- Upgrade software on switches, routers, WLC's (show recommended image)
- SMU support (patching)
- Rommon upgrade with software upgrade(requires Cisco.com access/credentials)
- Image Update Readiness Check (enough space, enough ram etc)
- Use an approval workflow
- Schedule upgrade and activation

Software images can be uploaded to DNA-Center:

- Manually using browser or ftp/http
- Directly from Cisco.com (needs cisco.com credentials)

Software can be marked golden based on:

- Device family type (9300, 9400 etc)
- Role (access, core etc)
- Site (area, building, floor)

Software Image Management

Intent Based Network Upgrades

Captures your upgrade intent to automate process and drive consistency

Streamlined Upgrade Process

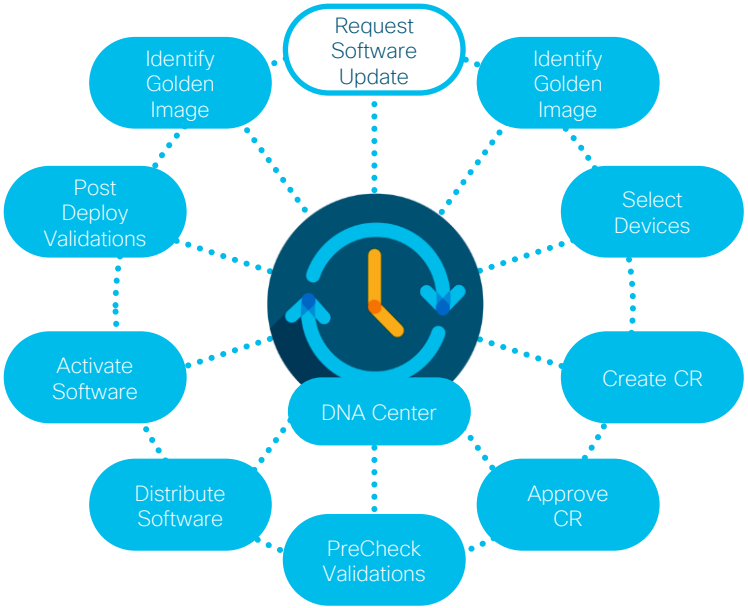
Upgrade base image, patches, and other add-ons in one single flow

Trustworthiness Integration

Assures that device images are not compromised in any way.

Patching Support

Pre/Post check ensures updates do not have adverse effects on network



Automate your software upgrade cycle

Demo, SWIM

Rommon upgrade supported on

For Your Reference

Routers

PID	Standalone
ISR 4431	YES
ISR 4221	YES
ISR 4351	YES
ISR 4451-X	YES
ASR 1001-X	YES
ASR 1002-X	YES
ASR 1006-X (RP2)	YES
ASR 1006-X (RP3)	YES
ASR 1009-X (RP2)	YES
ASR 1009-X (RP3)	YES
ASR 1001-HX	YES
ASR 1002-HX	YES

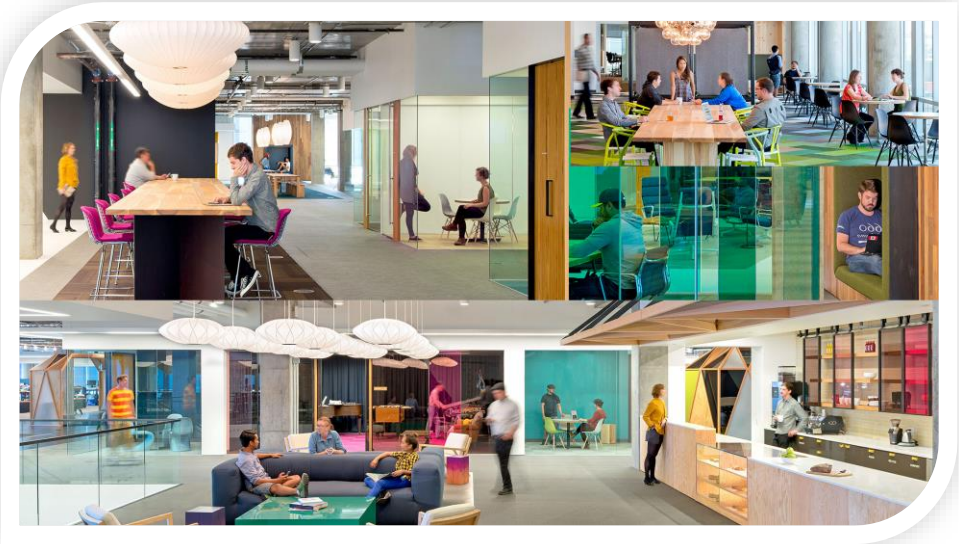
Switches

PID
C4500-E/X (SUP 7E|7LE|8LE)
C4500-X (SUP 7E|7LE|8LE
C4507R+E (SUP 7E|7LE|8LE)
C4503/6E (Sup 8E | 9E)
C4507R+E (Sup 8E | 9E)
C4510R+E (Sup 8E | 9E)
C4500X Fixed Chassis
C6503/4/6/9E (Sup 2T|6T)
C6513E (Sup 2T|6T)
C6807-XL (Sup 2T|6T)
C6840-X and C6880-X

Device Controllability is your friend ;-) How can I see that a software image is downloaded already?

Cisco DNA Service for Bonjour

Bonjour Services Use Cases



Bonjour enabled devices on the rise!

Current Limitations for Service Discovery

Technology

- Residential-class Technology
- Single network segment discovery
- Integration in Enterprise networks

Solution

- Fragmented Gateway Solutions
- Local System Bonjour Solution
- Not end-to-end solution

Boundary

- Single Device solution
- Unable to scale beyond single system
- Limited network discovery boundary

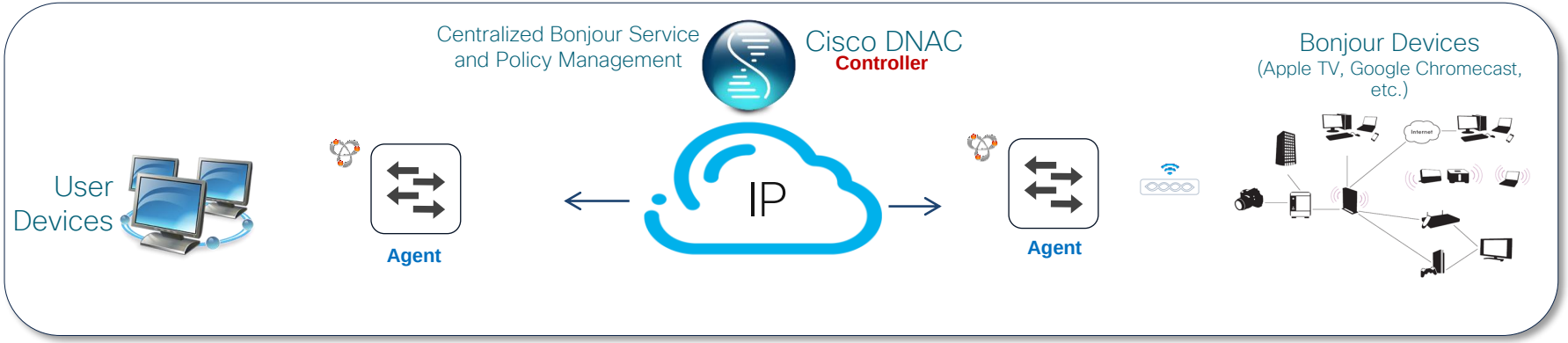
Scale

Performance

Scale

- Limited scale and performance
- Centralized architecture impact performance
- Sub-optimal mobility with scale

Bonjour Service Discovery Without Boundaries



Traditional Bonjour

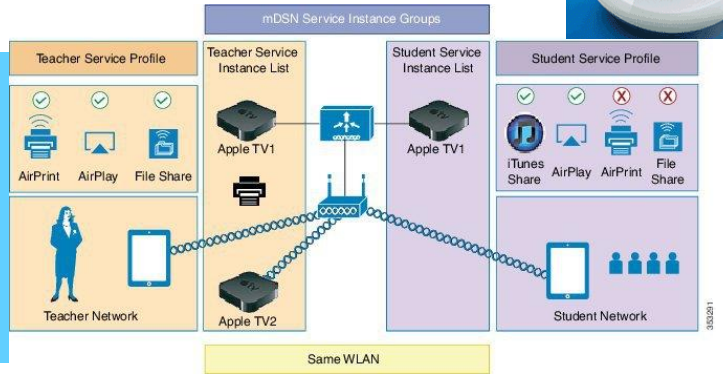
- Single Gateway solution, cannot scale across enterprise
- No access control
- Limited Management capabilities

Cisco DNA Service for Bonjour

- **Enables** Discovery and service distribution across LAN and WLAN networks
- **Access Controlled**
- **Simplified** Intuitive Controller Based Management

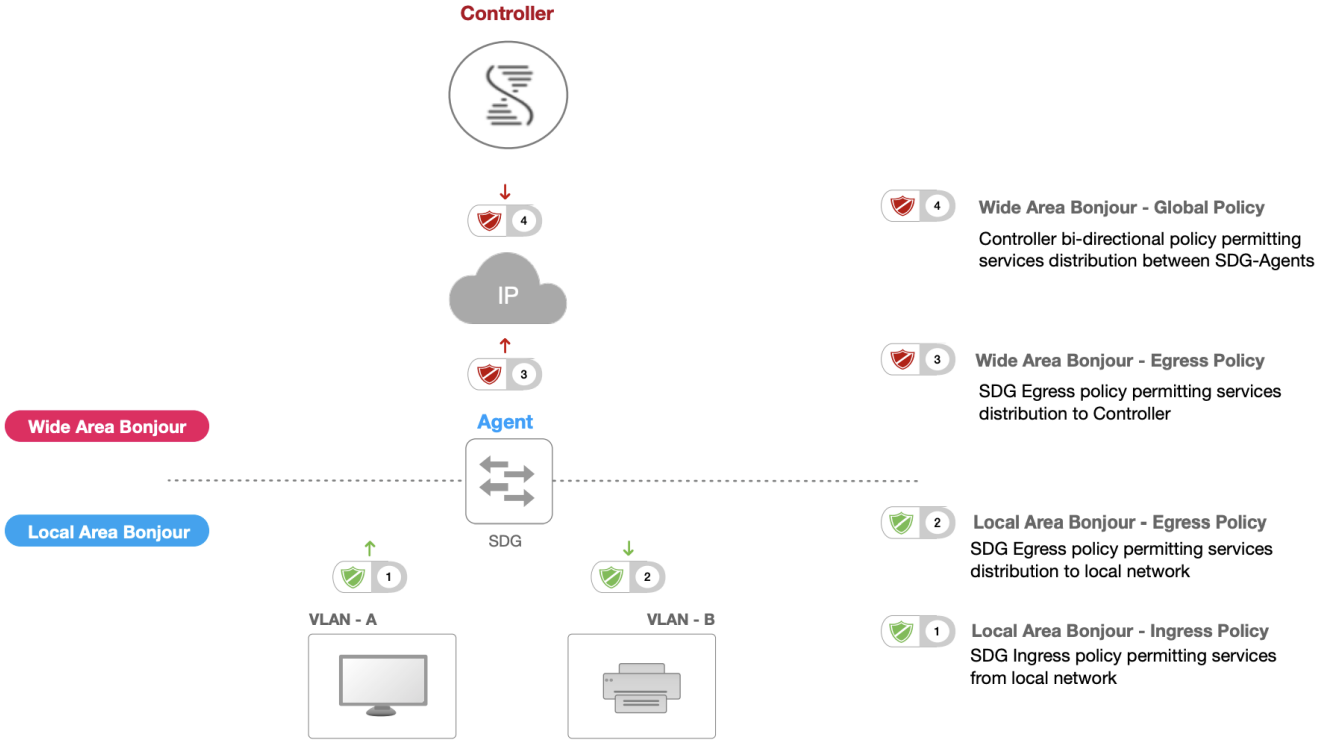
Bonjour with Prime Infrastructure

Option 1: Manual
mDNS config via CLI templates on WLC
- all manual work
- only on WLC
- only local Area Network



Option 2: Manual
Service Discovery Gateway config via CLI templates on WLC
- all manual work
- WLC & Switches & ISR
- Limited support of IOS-XE

Bonjour Service Policy Type



Demo, Bonjour

Agent – Local Area Bonjour Policy (CLI)

For Your Reference

Local Area Bonjour Policy – LAN and WLAN


```
!
Agent(config)# mdns-sd gateway
!
```

```
!
Agent(config)# mdns-sd service-list <NAME> < IN | OUT >
Agent(config-mdns-sl-in))# match airplay
!
```

```
!
Agent(config)# mdns-sd service-policy <NAME>
Agent(config-mdns-sl-in))# service-list <NAME> < IN | OUT >
!
```

```
!
Agent(config)# interface Vlan <ID>
Agent(config-if))# mdns-sd gateway
Agent(config-if-mdns-sd)# service-policy <NAME>
!
```

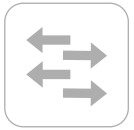
*** - Optional.** For Inter-VLAN Local Proxy

Notes – Built-In Bonjour Services Support

SD-Access Network Product Matrix

For Your Reference

Cisco DNA-Center



Catalyst

WLC *

Supported Controller	Hardware	Software
Cisco DNA-Center	DN2-HW-APL-L and DN2-HW-APL-L DN2-HW-APL-XL	v1.3.1.0

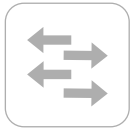
Supported SDG Agent	Local Area SDG	Wide Area SDG	Software
Catalyst 9200	DNA Essentials	⊗	17.1.1 *
Catalyst 9300	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9400	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9500 / 9500-H	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9600	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9800 WLC	DNA Essentials	DNA Advantage	Pass-Thru
Cisco 5520/8540 WLC	DNA Essentials	DNA Advantage	Pass-Thru
Catalyst Embedded WLC	DNA Essentials	DNA Advantage	16.11.1

* Roadmap

Traditional Network Product Matrix

For Your Reference

Cisco DNA-Center



Catalyst

ISR

WLC *

* Pass-Thru

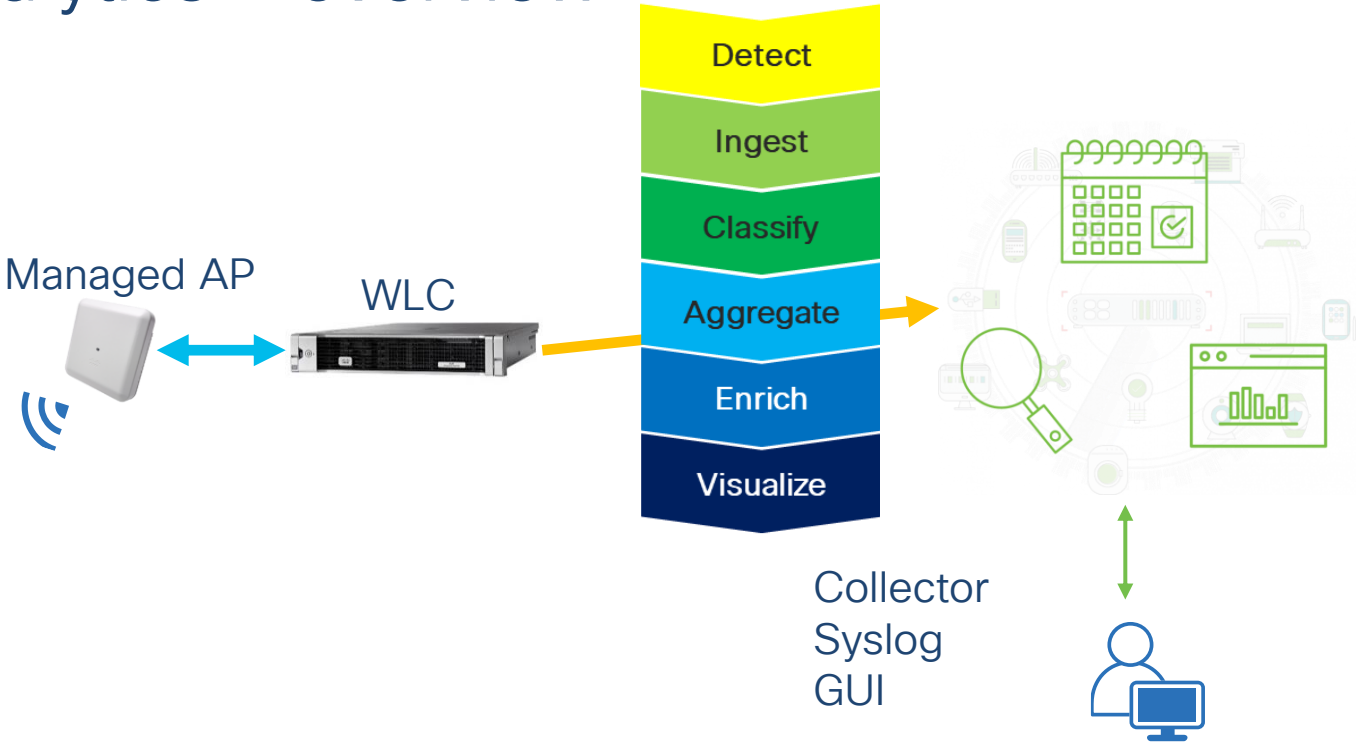
Supported Controller	Hardware	Software
Cisco DNA-Center	DN2-HW-APL-L and DN2-HW-APL-L DN2-HW-APL-XL	v1.3.1.0

Supported SDG Agent	Local Area SDG	Wide Area SDG	Software
Catalyst 9000 (C9300-C9600)	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9200	DNA Essentials	⊗	17.1.1
Catalyst 9200L	⊗	⊗	Pass-Thru
Catalyst 9800 WLC	DNA Essentials	⊗	Pass-Thru
Cisco 5520/8540 WLC	⊗	⊗	Pass-Thru
Catalyst 6800	IP Base	Adv Ent + DNA-Addon	15.5(1)SY4
Catalyst 4500E/X	IP Base	IP Services + DNA-Addon	3.11.0
Catalyst 3850/3650	DNA Essentials	DNA Advantage	16.11.1
Catalyst 2960 X	LAN Base	⊗	15.2.6E2
Catalyst 2960 XR	IPLite	⊗	15.2.6E2
Cisco ISR 4000 Series	IPBase	AppX	16.11.1

Cisco DNA Center

Rogue Management

Rogue analytics - overview



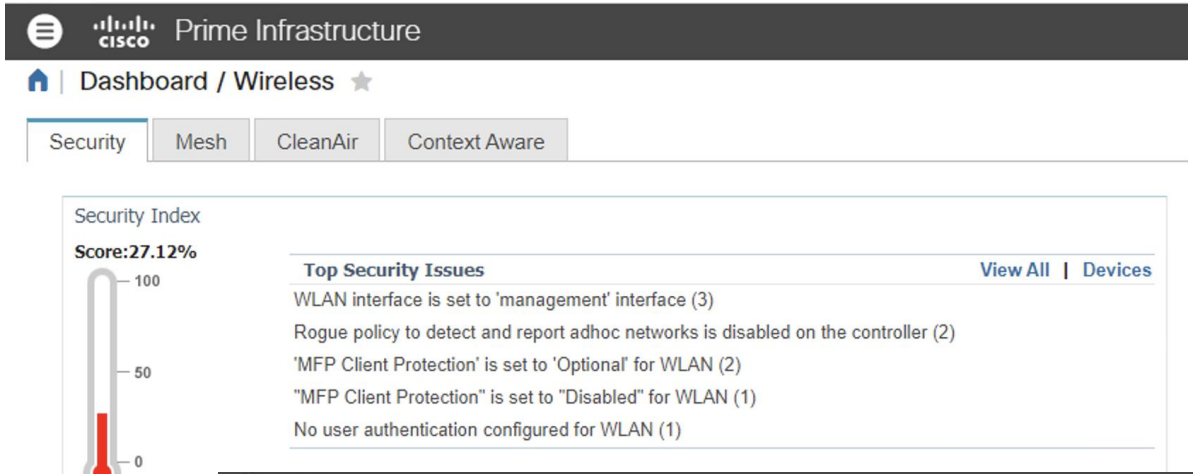
Rogue Classification

A **rogue access point is** a wireless **access point** that has been installed on a secure network, by well-**meaning** employee or by a malicious attacker.

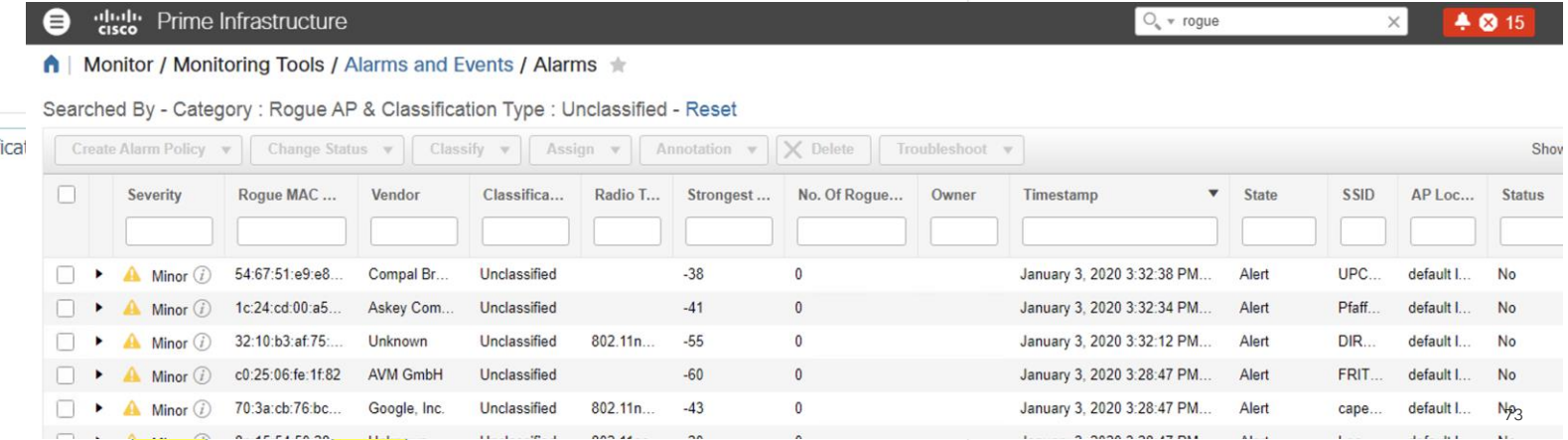
AP on Wire	Based on RSSI	Honeypod	Impersonate
Bridge Mode Rogue Client	Rogue AP (RSSI)	Honeypot Rogue 1 SSID : Blizzard	Impersonate AP-11 11:22:33:44:55:66

Informational → Potential → High

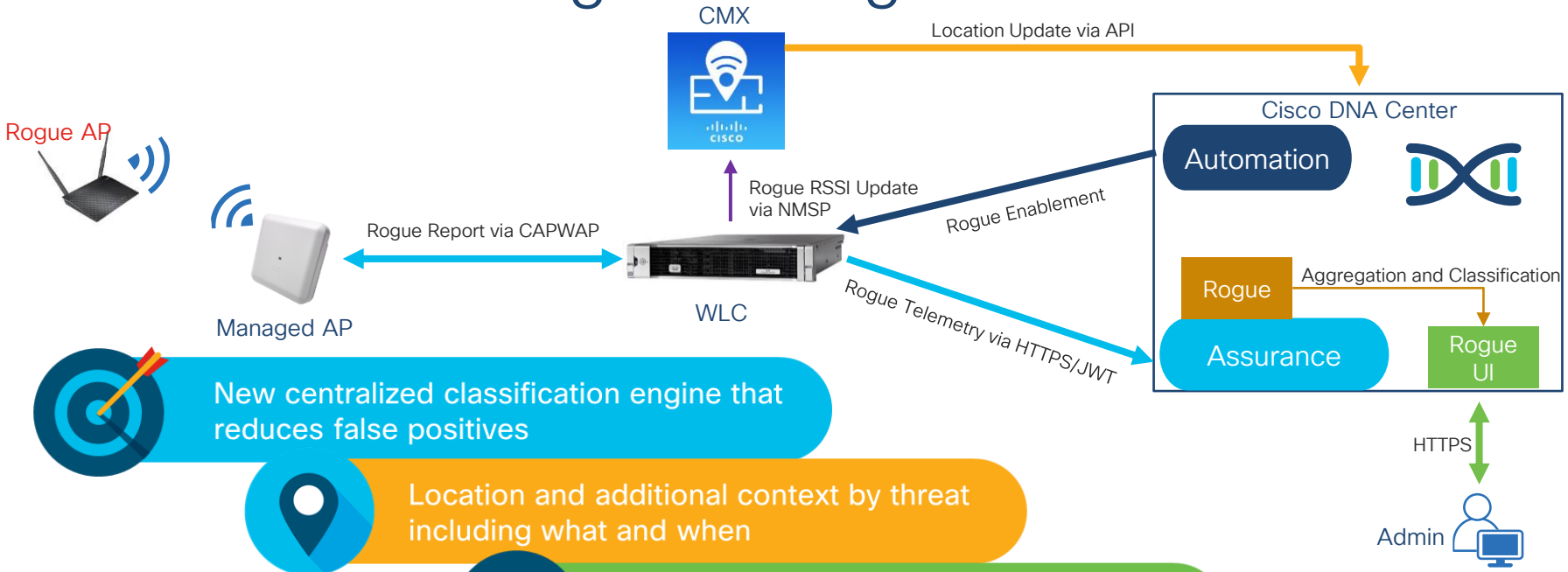
Rogue with Prime Infrastructure



Prime Infrastructure consolidates all of the controllers rogue access point data



Cisco DNAC - Rogue Management Architecture



New centralized classification engine that reduces false positives

Location and additional context by threat including what and when

Curated view to highlight most relevant data and reduce data overload

Automate action based on Rogue Enablement

Demo, Rogue

Rogue Management Dashboard - Overview

For Your Reference

Quick Time Filter

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Rogue Management

Nov 7, 2019 9:25 AM Refresh Show Map Last 3 hours

Time Slider

6:00a 7:00a 8:00a 9:00a

High Threats Over Time

High Threat Trend

No. of High Threat 1.2 1.0 0.8 0.6 0.4 0.2 0.0

6:00a 7:00a 8:00a 9:00a

Time

High Threat Level

1 High Threat

High Threat Count

Honeypot: 1

Threats (132) All Threats

Filter

Threat Level	Rogue AP MAC address	Type	Connection	Detecting AP	Detecting AP Site	RSSI	SSID	Last Reported
High	00:2A:10:4C:EB:A0	Honeypot	Wireless	SJC04-F1-AP3	...SJC/SJC04/SJC04-AFP-1	-76	lightning	Nov 07, 2019 09:23 am
Potential	70:79:B3:AD:51:E0	Interferer	Wireless	SJC04-F1-AP2	...SJC/SJC04/SJC04-AFP-1	-58	AS-B1-WLC-3504	Nov 07, 2019 09:23 am
Potential	08:4F:F9:2E:E0:AE	Interferer	Wireless	SJC04-F1-AP3	...SJC/SJC04/SJC04-AFP-1	-36	@CorpSSID	Nov 07, 2019 09:23 am
Potential	08:4F:F9:2F:25:6F	Interferer	Wireless	SJC04-F1-AP1	...SJC/SJC04/SJC04-AFP-1	-51	@CorpSSID_98	Nov 07, 2019 09:23 am

High Threat -Honeypot Rogue

For Your Reference

Threats (108)

Honeypot High Threat

Filter

Threat Level	Rogue AP MAC address	Type	Connection	Detecting AP	Detecting AP Site	RSSI	SSID	Last Reported
High	B0:26:80:D5:03:A0	Honeypot	Wireless	SJ-AP2	Global	-29	lightning	Apr 24, 2019 01:34 pm
High	00:F6:63:14:1D:A0	Honeypot	Wireless	SJ-AP2	Global	-56	lightning	Apr 24, 2019 01:34 pm
Potential	F4:DB:E6:46:28:E0	Interferer	Wireless	SJ-AP2	Global	-57	CiscoAirProvision	Apr 24, 2019 01:34 pm
Potential	EC:BD:1D:AB:0E:50	Interferer	Wireless	SJ-AP3	Global	-46	CiscoLive	Apr 24, 2019 01:34 pm
Potential	38:0E:4D:BB:81:90	Interferer	Wireless	SJ-AP1	Global	-53	jerry01	Apr 24, 2019 01:34 pm
Potential	EC:BD:1D:B1:DF:B0	Interferer	Wireless	SJ-AP2	Global	-34	MySsid001	Apr 24, 2019 01:34 pm
Potential	EC:C8:82:FB:32:A0	Interferer	Wireless	SJ-AP1	Global	-32	LA-Flex	Apr 24, 2019 01:34 pm
Potential	00:5D:73:9C:91:40	Interferer	Wireless	SJ-AP3	Global	-51	DNAC-WLC-02-SSID	Apr 24, 2019 01:34 pm
Potential	70:F3:5A:80:E3:80	Interferer	Wireless	SJ-AP1	Global	-43	MFG-5GTEST	Apr 24, 2019 01:34 pm

Show 100 entries

Showing 1 - 100 of 108

Previous 1 2 Next

High Threat - Honeypot 360 View

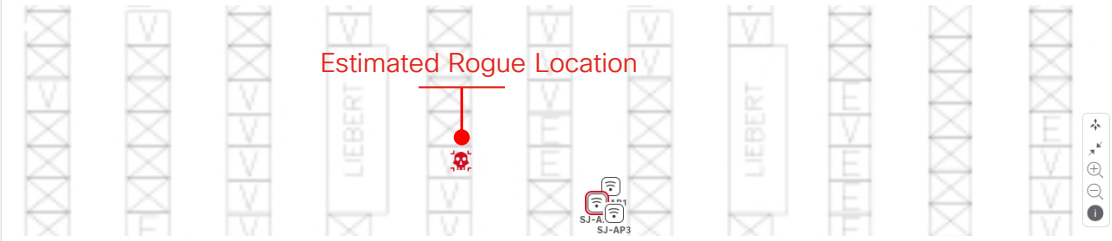
For Your Reference

Threat 360: Mac 00:F6:63:14:1D:A0

Threat Level	Threat Type	Status	Rogue Vendor	Last Reported
High	Honeypot	Active	Cisco Systems, Inc	Apr 24, 2019 04:49 pm

Location: ...San Jose/SJC04/Floor1

Full Screen



Without CMX, the estimated rogue location is shown based on the detecting AP with strongest RSSI only.

Detecting Access Points (4) Clients (0)

Detecting Access Points (4)

Export

Filter

Detecting AP	AP Domain	Rogue SSID	RSSI	Channels	Radio Type	SNR	State	Last Updated
SJ-AP2	...San Jose/SJC04/Floor1	lightning	-54	11	802.11n (2.4)	26	Active	Apr 24, 2019 04:49 pm
SJ-AP3	...San Jose/SJC04/Floor1	lightning	-60	132	802.11ac	35	Active	Apr 24, 2019 04:44 pm
SJ-AP1	...San Jose/SJC04/Floor1	lightning	-61	132	802.11ac	30	Active	Apr 24, 2019 04:44 pm

Detecting AP with strongest RSSI

Agenda

1. Introduction
2. Change in Paradigm in Network Management
3. Migration from Prime Infrastructure to Cisco DNA-Center
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

What is Assurance?

The guarantee that the infrastructure is doing what you intended it to do

PARADIGM SHIFT

Continuous Verification

Monitor and alert on operational impact to network after every Configuration Changes

Successful Rollouts, Operational Continuity

Insights & Visibility

Visibility, Context, Historical Insights, Prediction

Minimize Downtime, User Productivity

Corrective Actions

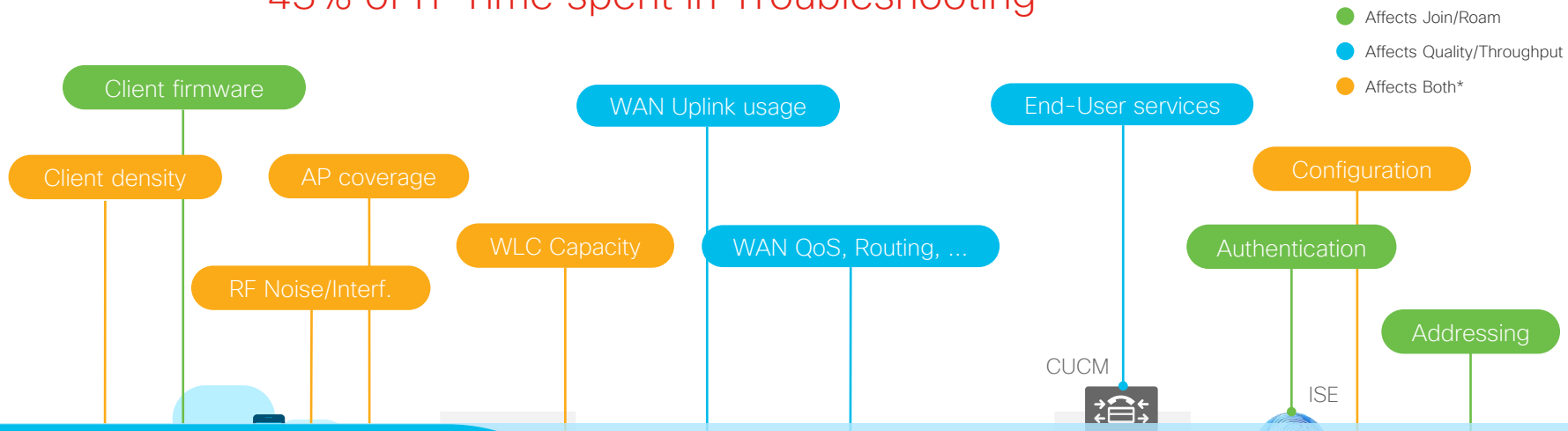
Guided Remediation, Automated Updates, System optimization

IT Productivity

Network Quality is a Complex, End-to-End Problem

PARADIGM SHIFT

43% of IT Time spent in Troubleshooting



There are 100+ points of failure between user and app

What is the problem?

Where is the problem?

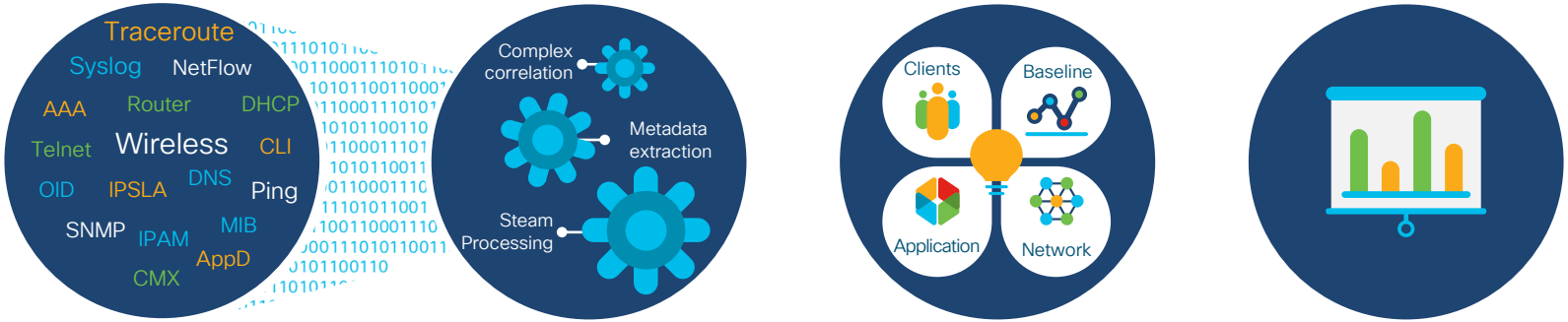
How can I fix the problem fast?

Cisco DNA Assurance

PARADIGM SHIFT

- From network data to business insights

Network telemetry contextual data	Complex event processing	Correlated insights	Suggested remediation

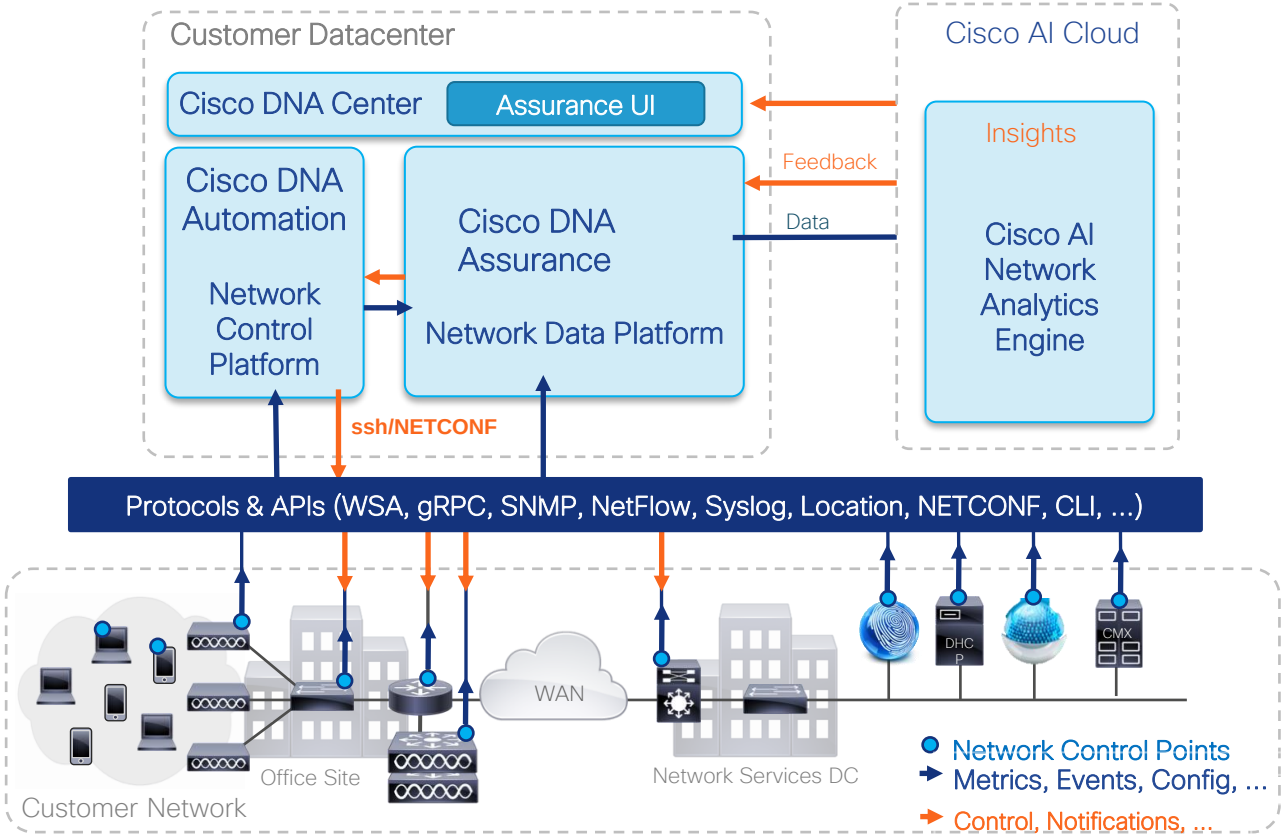


Everything as a sensor

Over 150 actionable insights

Clients | Applications | Wireless | Switching | Routing

Cisco DNA Assurance Architecture



Client / Network / Application 360 views

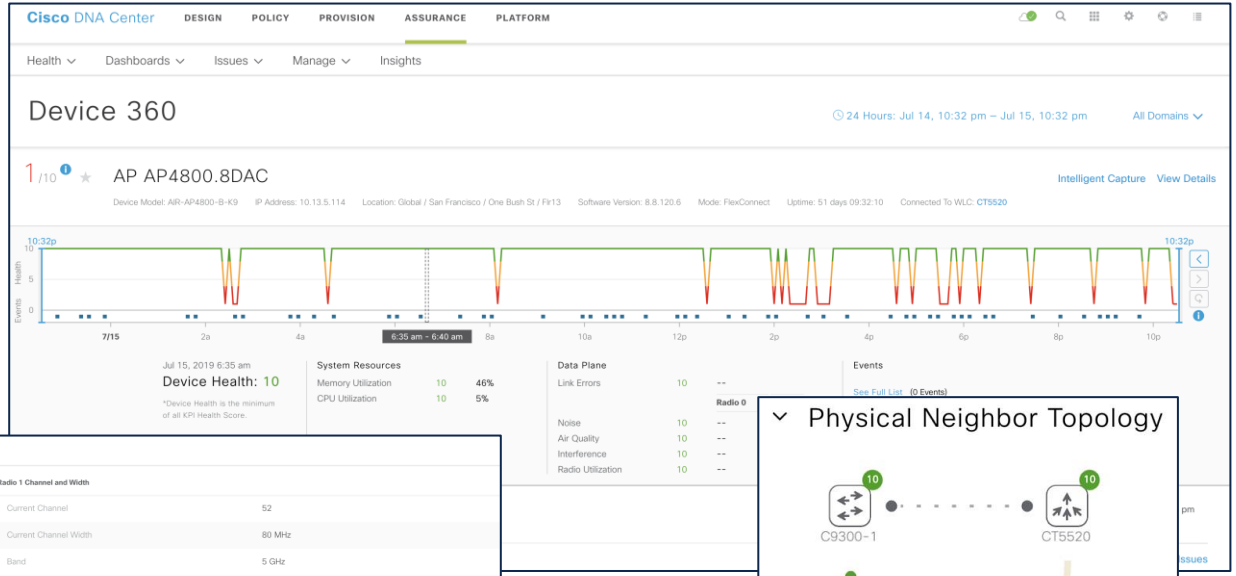
Demo, 360 Views

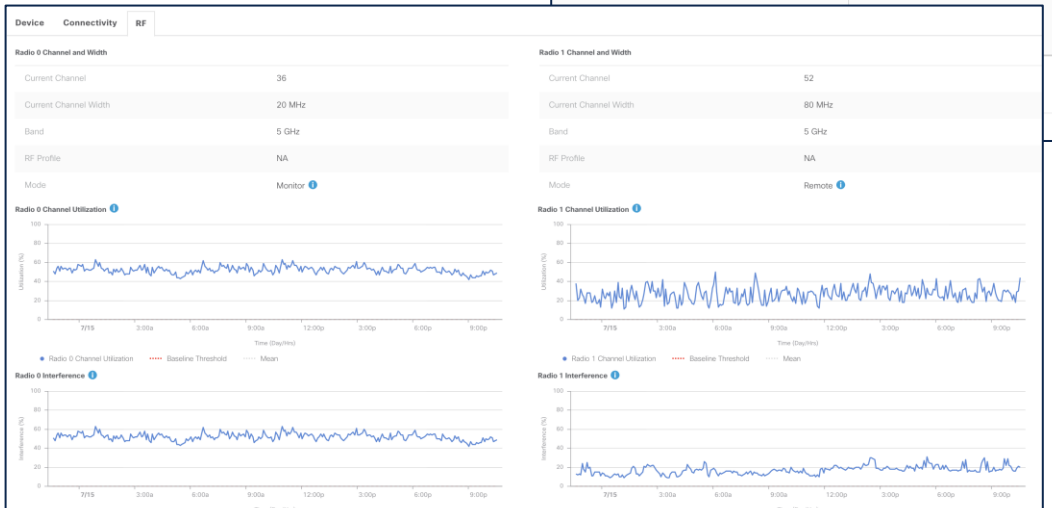
360^0 Visibility– Network Device

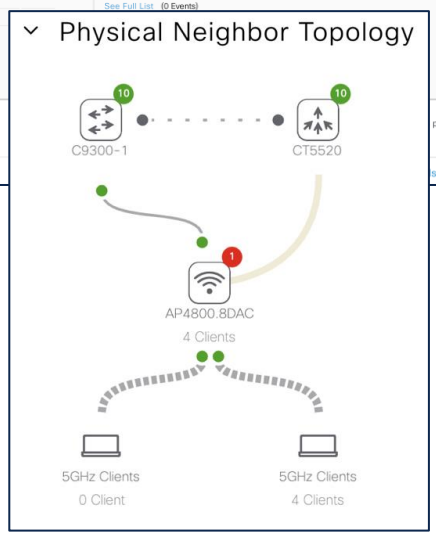
Network device Health history, Proactively identify any Issues

Detailed Device health information

Physical Neighbor Topology







360⁰ Visibility–Client Device

Network Client Health history, Proactively identify any Issues

Detailed Client health information

Client Onboarding Details

Cisco DNA Center | DESIGN | POLICY | PROVISION | ASSURANCE | PLATFORM

Health | Dashboards | Issues | Manage | Insights

Client 360

24 Hours: Jul 14, 10:43 pm – Jul 15, 10:43 pm | All Domains | Intelligent Capture

7/10 User4

Device: Android-Motorola | OS: android-dhcp-7.1.1 | MAC: 7C:46:85:20:7B:27 | IPv4: 10.13.4.186 | IPv6: fe80::7e46:85ff:fe20:7b27 | VLAN ID: 140 | Status: Connected | Last seen: Jul 15, 2019 10:42:00 pm | Connected Network Device: AP4800.922C

SSID: @CorpSSID | Last Known Location: San Francisco/One Bush St/Flr13

Issues | Onboarding | Event Viewer | Path Trace | Application Experience | Detail Information

Issues (3)

P3 Onboarding — Wireless client failed to connect (SSID: @CorpSSID, AP: AP4800.606E, Band: 2.4 GHz, Site: Global/San Francisco/One Bush St/Flr13) - Failed to authenticate due to Client Timeout — Jul 15, 2019 8:10 pm — Instance Count: 13

P3 Onboarding — Wireless client failed to connect (SSID: @CorpSSID, AP: AP4800.922C, Band: 2.4 GHz, WLC : CT5520) - AAA Server Rejected Client — Jul 15, 2019 7:07 pm — Instance Count: 2

P3 Onboarding — Wireless client failed to roam (SSID: @CorpSSID, AP: AP4800.606E, Band: 2.4 GHz, WLC : CT5520) - AAA Server Rejected — Instance Count: 1

Detail Information Jul 15, 2019 10:43 pm

Device Info | Connectivity | RF

Information		Connection Information	
User Name	User4	Band	2.4 GHz
Host Name	android-2ccc07873cebb1f0	Spatial Streams	0
MAC Address	7C:46:85:20:7B:27	Channel Width	20 MHz
IPv4 Address	10.13.4.186	WMM	Supported
IPv6 Address	fe80::7e46:85ff:fe20:7b27	U-APSD	Disabled

Onboarding Jul 15, 2019 10:43 PM

AAA | DHCP

andro...7873cebb1f0 — @CorpSSID — AP4800.922C (1 Client) — CT5520 (34 Clients)

Application Experience

Client level Application usage visibility per Business relevance category

Per-Application Health Score along with historical trending

Detailed Application level flow metrics – Throughput, Packet loss, Latency, Delay

Application Experience Jan 25, 2018 1:14 pm Refresh

Business Relevant | Business Irrelevant | Default

Application (5) Export

Filter Find

Name	Domain Name	Health		Destination	Average Throughput (Mbps)	Average Bandwidth Utilization (%)	Traffic Class	Packet Loss (%)		Latency (ms)		Application Delay (ms)	
		Most Recent	Last 24 Hours					Max	Average	Max	Average	Max	Average
All Applications				Multiple	2	2							
cifs	--	1	View	USA/Data Center	1	1	bulk-data	100	2	45944	2292	106	0
ssh	--	2	View	USA/Data Center	0.49	0.69	ops-admin-mgmt	100	8	184793	2350	3961	6
citrix-static	--		--	USA/Data Center	0.08	0.11	multimedia-streaming	0	0	0	0	0	0
ntp	--		--	USA/Data Center	0	0	ops-admin-mgmt	0	0	0	0	0	0

Business Relevant | Business Irrelevant | Default

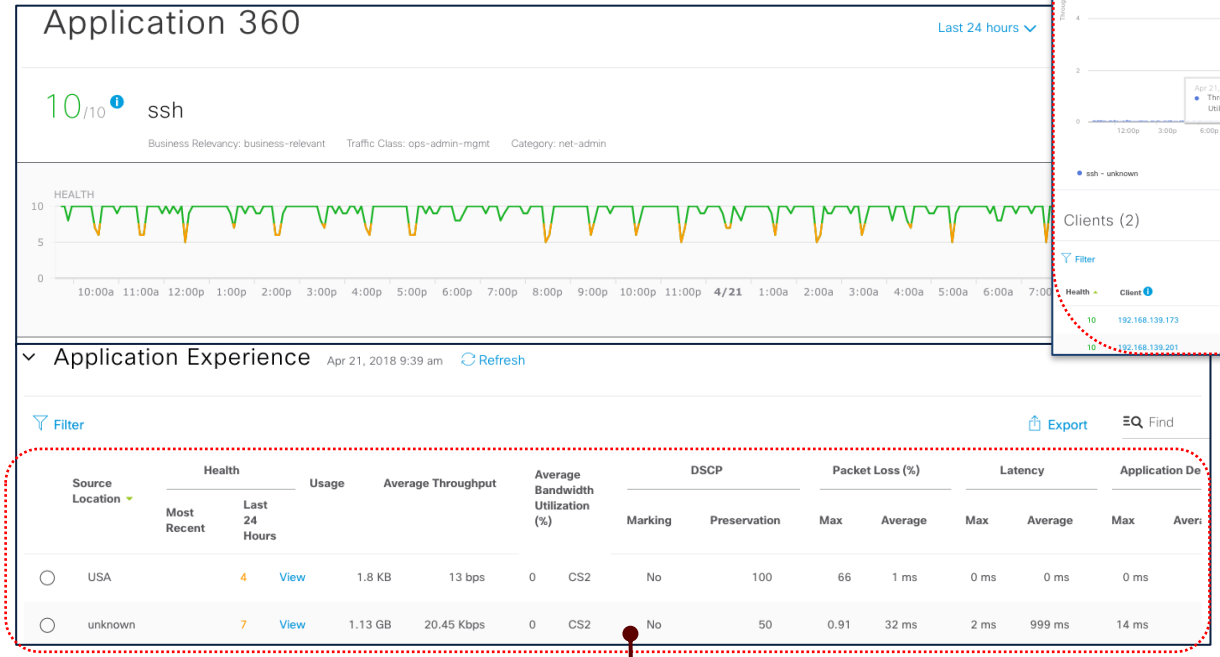
Application (3) Export

Filter Find

Name	Domain Name	Health		Destination	Average Throughput (Mbps)	Average Bandwidth Utilization (%)	Traffic Class	Packet Loss (%)		Latency (ms)		Application Delay (ms)	
		Most Recent	Last 24 Hours					Max	Average	Max	Average	Max	Average
All Applications				Multiple	0.13	0.18							
disney-web-portal	www.disney.com	7	View	USA/Data Center	0.09	0.13	transactional-data	100	7	21325	585	6222	40
espn-browsing	www.espn.com	4	View	USA/Data Center	0.03	0.04	transactional-data	100	2	50363	1700	5761	45
netflix	www.netflix.com:443	2	View	USA/Data Center	0.01	0.01	multimedia-streaming	100	4	93552	1383	6618	93

DNAC 1.2

Application Assurance – Per App 360 View

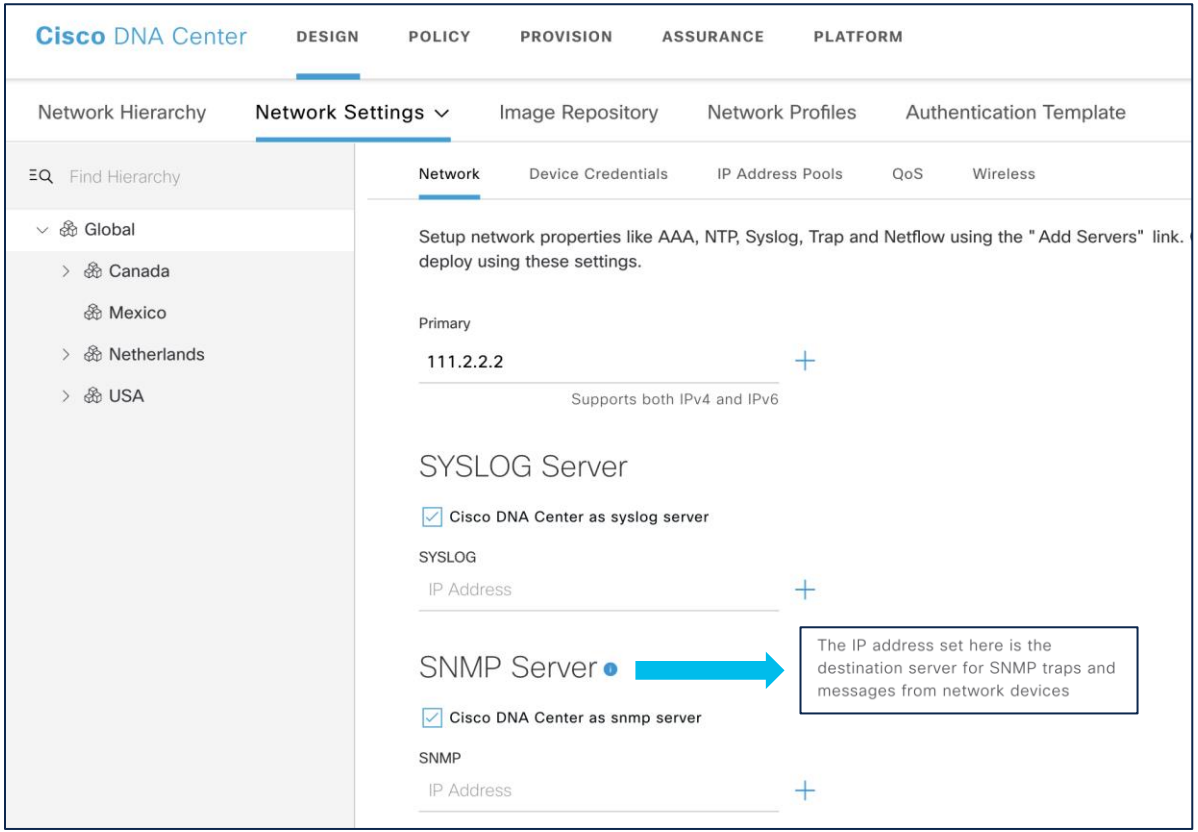


- Application Performance over last 24 hrs
- List of clients who used the App in the given timeframe

- Top N Flows between Sites

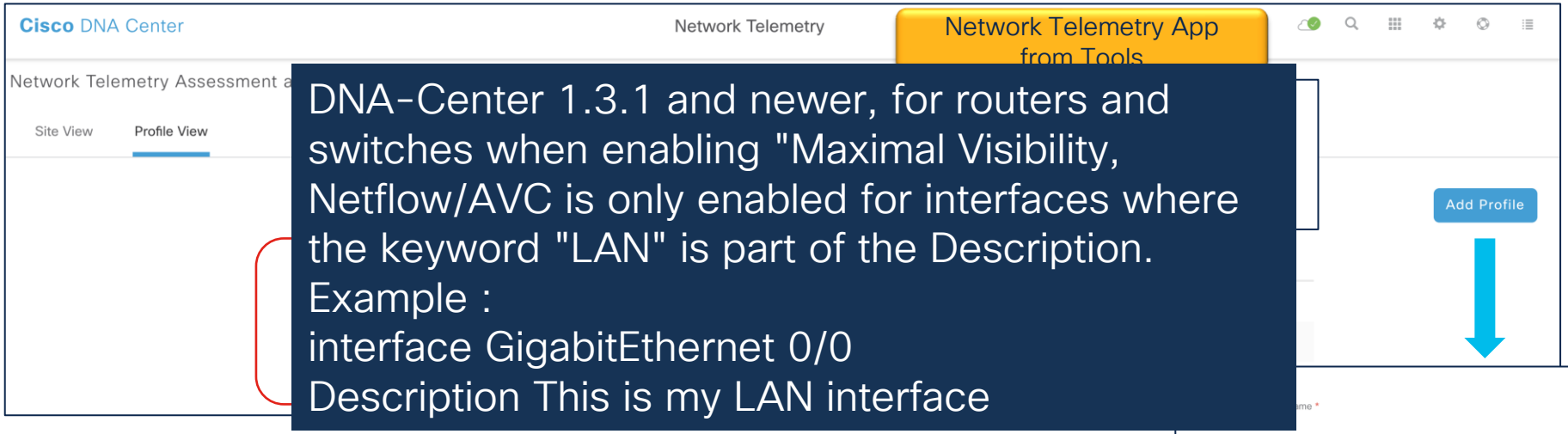
Setup Telemetry from Infrastructure to DNA-Center

Telemetry Configuration



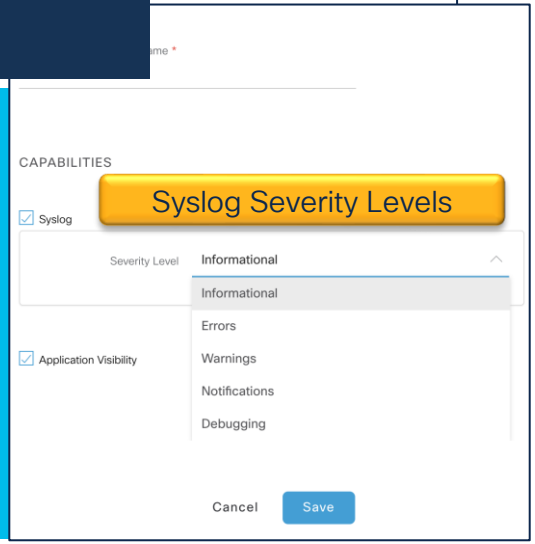
- Telemetry Configuration
  - SYSLOG Server
  - SNMP Trap Server
  - SNMP Polling
- Cisco DNA Center is configured as Syslog and SNMP Trap Server by default
- Telemetry Configuration is pushed while assigning devices to sites
- Usage of Network Telemetry App is not mandatory and used only to create custom telemetry profile

Network Telemetry App



DNA-Center 1.3.1 and newer, for routers and switches when enabling "Maximal Visibility, Netflow/AVC is only enabled for interfaces where the keyword "LAN" is part of the Description.
Example :
interface GigabitEthernet 0/0
Description This is my LAN interface

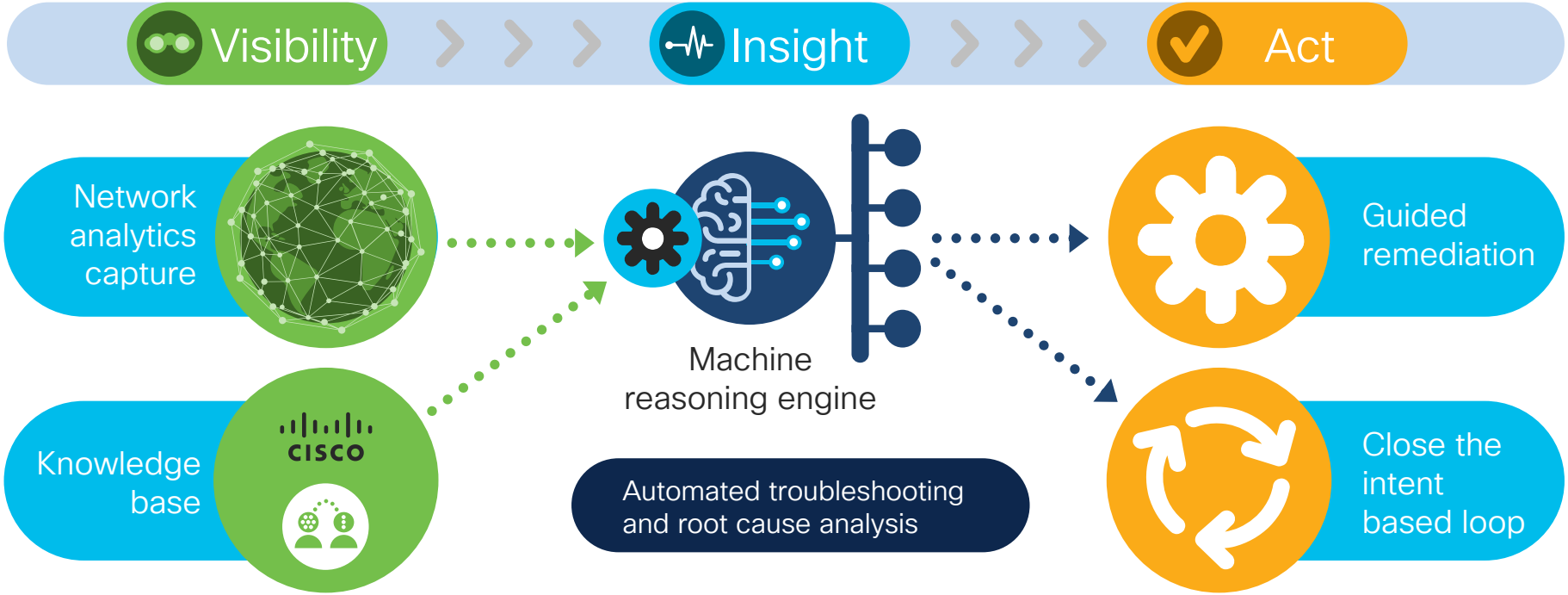
- Maximal Visibility
  - Syslog with severity level “Informational”
  - Application Visibility, **NetFlow support on switches, routers and WLC**
- Optimal Visibility
  - Syslog with severity level “Informational”
  - **No Application Visibility**
- Create Custom Telemetry Profile with different Syslog Severity Level if desired



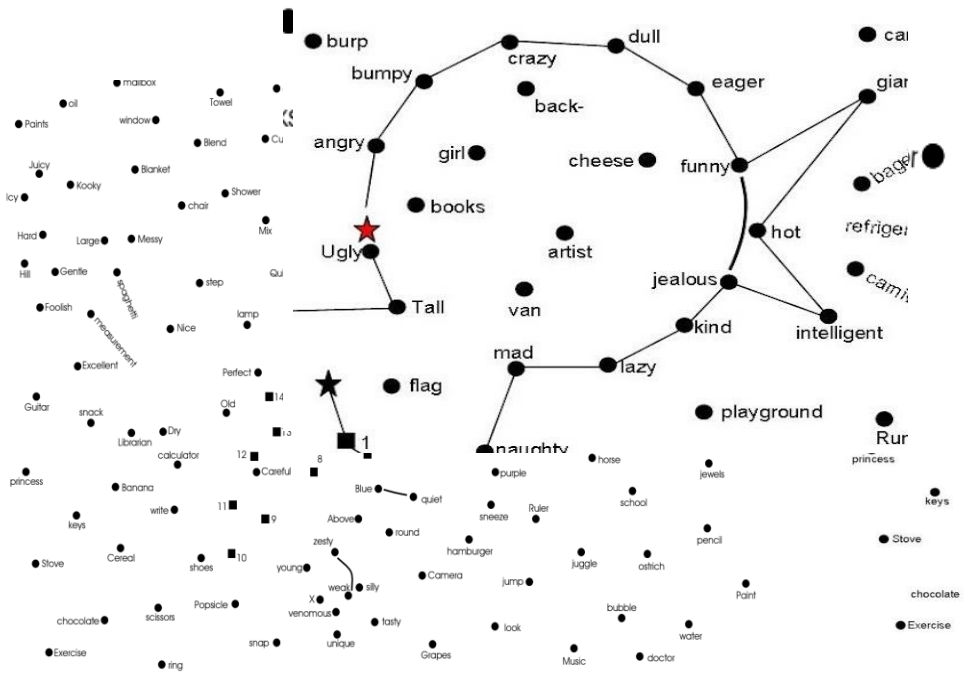
Cisco DNA Center

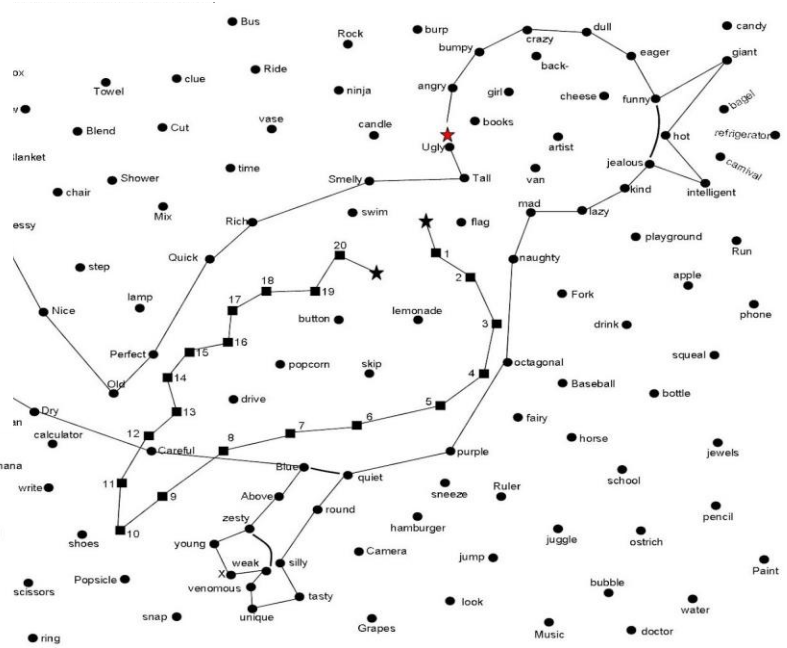
AI / ML Network Analytics

AI Network Analytics Architecture



Raw Data is Uninsightful and Overwhelming





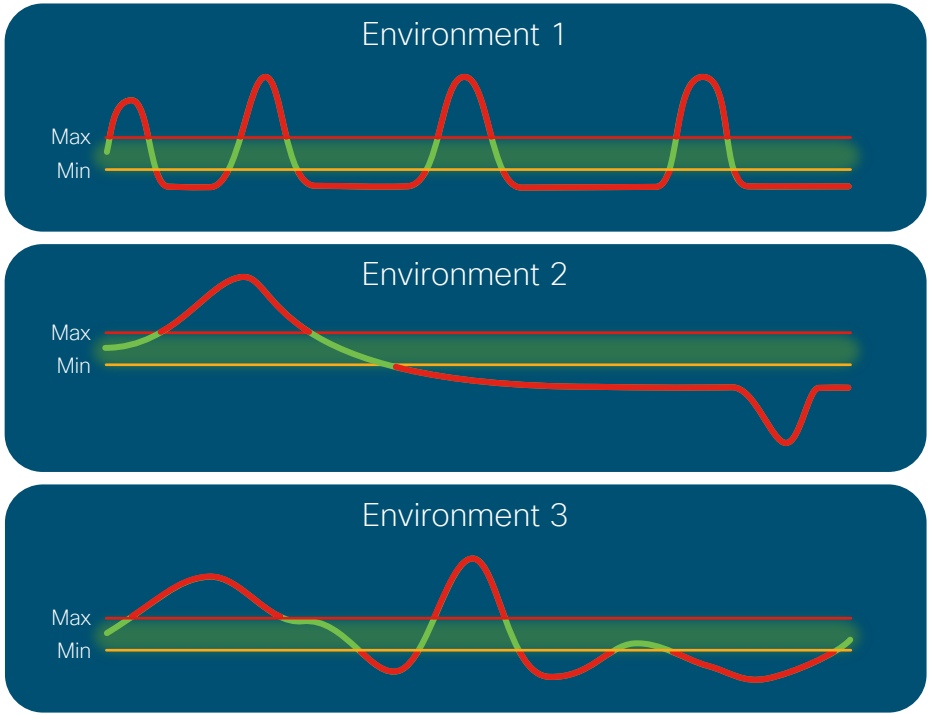
Relationships Between Data
Points Can Reveal hidden Insights

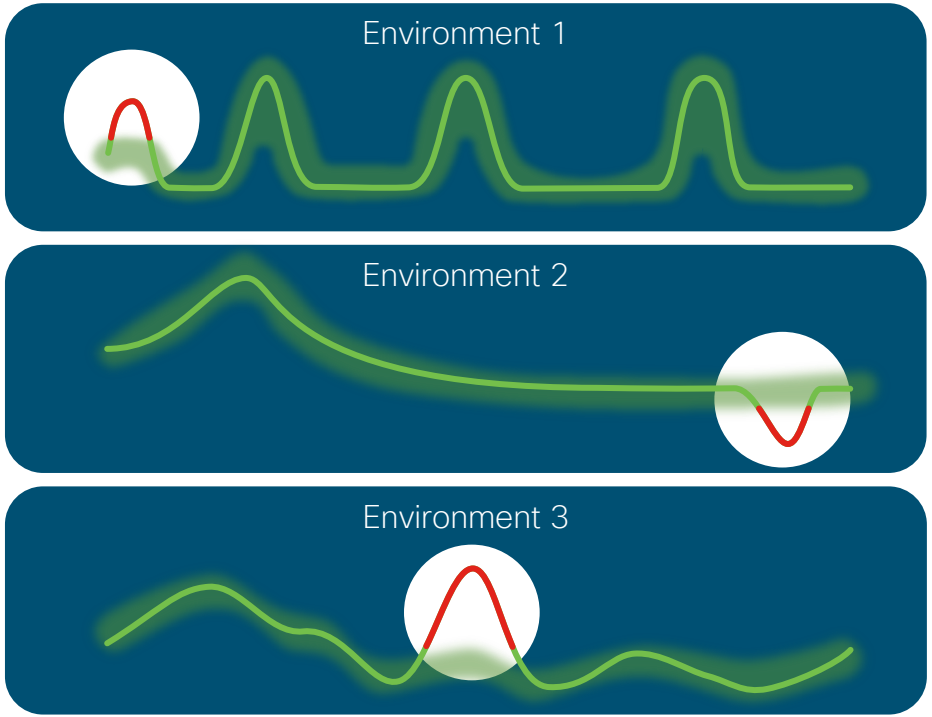
Use Case 1: Improve Incident Alert Fidelity

Personalized Baselining

Before: Custom thresholds = Alert overload

AI-driven: Dynamic baselines = relevant anomalies





Use Case 2: Proactive & Predictive Insights

Intelligent Analysis

Find Issues
Before Users Do

- Proactive Exploration
- System Generated Insights
- Peer-to-peer & Site-to-site Comparison

Demo, AI Network Analytics

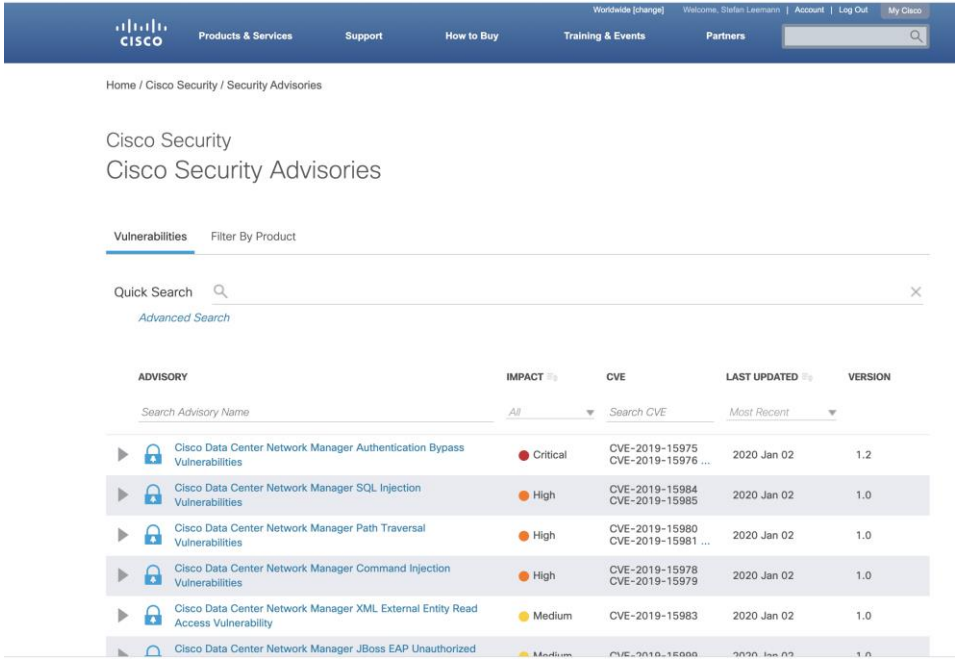
Cisco DNA Center

Security advisories

Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends Cisco Security Advisories and Alerts.

The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.



https://tools.cisco.com/security/center/publicationListing.x

Security advisories with Prime Infrastructure

Prime Infrastructure

Reports / Reports / PSIRT and EOX

Schedule Job | View Job Details | PAS

Device PSIRT | Device Hardware EOX | Device Software EOX | Module Hardware EOX | Field Notice

Updates with Maintenance Releases

Device PSIRT CSV | Go | Show All

Device Name	Device Type	IP Address	OS Type	OS Version	PSIRT Title	Vulnerable	Match Reason	Caveat
berlab6880.cisco.com	Cisco Catalyst 68xx Virtual Switch	10.49.232.151	IOS	15.2(1)SY3	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab3750x-rack2.cisco.com	Cisco 3750 Stackable Switches	10.100.10.145	IOS	15.2(4)E4	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab3750-tg1	Cisco 3750 Stackable Switches	10.100.80.22	IOS	12.2(55)SE12	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab6880.cisco.com	Cisco Catalyst 68xx Virtual Switch	10.49.232.151	IOS	15.2(1)SY3	Multiple Cisco Products OSPF LSA Manipulati...	Vulnerable	MATCH:OSTY...	Mapping logi...
berlab3750x-rack2.cisco.com	Cisco 3750 Stackable Switches	10.100.10.145	IOS	15.2(4)E4	Multiple Cisco Products OSPF LSA Manipulati...	Vulnerable	MATCH:OSTY...	Mapping logi...
berlab3750-tg1	Cisco 3750 Stackable Switches	10.100.80.22	IOS	12.2(55)SE12	Cisco IOS and IOS XE Software Cluster Man...	Vulnerable	MATCH:OSTY...	Automation d...

Security Advisories: Advisories View

Tools area, click **Security Advisories**

Cisco DNA Center — Security Advisories

Security Advisories — Focus: Advisories — Last scanned: Jan 3, 2020 4:54 PM — Scan

Advisories (84)

Filter

Advisory ID	Advisory Title	CVSS Score	Impact	CVE	Devices	Known Since (days)	Last Updated
cisco-sa-20190828-iosxe-rest-auth-bypass	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	10	CRITICAL	CVE-2019-12643	13	128	08/29/2019
cisco-sa-20180328-smi2	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0171	6	646	05/04/2018
cisco-sa-20170317-cmp	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2017-3881	2	1022	04/18/2019
cisco-sa-20180328-xesc	Cisco IOS XE Software Static Credential Vulnerability	9.8	CRITICAL	CVE-2018-0150	12	646	09/20/2018
cisco-sa-20180328-qos	Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0151	5	646	04/28/2018
cisco-sa-20180606-aaa	Cisco IOS XE Software Authentication, Authorization, and Accounting Login Authentication Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0315	2	576	06/08/2018
cisco-sa-20180328-lldp	Cisco IOS, IOS XE, and IOS XR Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities	8.8	HIGH	CVE-2018-0175,CVE-2018-0167	3	646	05/02/2018
cisco-sa-20190612-iosxe-csrf	Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	8.8	HIGH	CVE-2019-1904	1	205	07/17/2019

Security Advisories: Device view

Cisco DNA Center

Security Advisories

Security Advisories Focus: Devices

Find Hierarchy

- Global
  - Unassigned Devices
  - CANADA
  - Casa Central
  - USA

Devices (28)

Filter | Tag Device

Device Name
TO-ASR1001X-1.corp.loc
LA1-3850-CSW-2.corp.lo
LA1-ASR1001X-1.corp.lo
LA2-3850-ACC-1.corp.lo
LA2-3850-CSW-3.corp.lo
LA2-3850-ACC-2.corp.lo
LA1-ASR1001X-2.corp.lo
LA1-3850-CSW-1.corp.lo

LA1-3850-CSW-2.corp.local (10.30.255.101)

Reachable Uptime: 482 days 17 hours 32 minutes

Run Commands | View 360 | Last updated: 4:55 PM | Refresh

Details | Advisories | Configuration | Interfaces

Filter

Advisory ID	Advisory Title	CVSS Score	Impact	CVE	Known Since (days)	Last Updated
cisco-sa-20190828-iosxe-rest-auth-bypass	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	10	CRITICAL	CVE-2019-12643	128	08/29/2019
cisco-sa-20180328-qos	Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0151	646	04/28/2018
cisco-sa-20180328-xesc	Cisco IOS XE Software Static Credential Vulnerability	9.8	CRITICAL	CVE-2018-0150	646	09/20/2018
cisco-sa-20180328-smi2	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	9.8	CRITICAL	CVE-2018-0171	646	05/04/2018
cisco-sa-20180328-xepriv	Cisco IOS XE Software Web UI Remote Access Privilege Escalation Vulnerability	8.8	HIGH	CVE-2018-0152	646	03/29/2018

Security Advisories: Good to know

To use the Security Advisories tool, you must install the Machine Reasoning package

If you log in to Cisco DNA Center as an Observer, you cannot view the **Security Advisories** tool in the home page.

AUTO UPDATE: System Settings > Settings > Machine Reasoning.
Click Import Latest from Cisco, or download the latest available Knowledge Base, and then Import from local. AUTO UPDATE toggle button to subscribe to the automatic update.

If you are launching the **Security Advisories** page for the first time, click **Scan**

No Hardware EoX in Cisco DNAC

No Software EoX in Cisco DNAC

Cisco DNA Center
Intelligent Capture

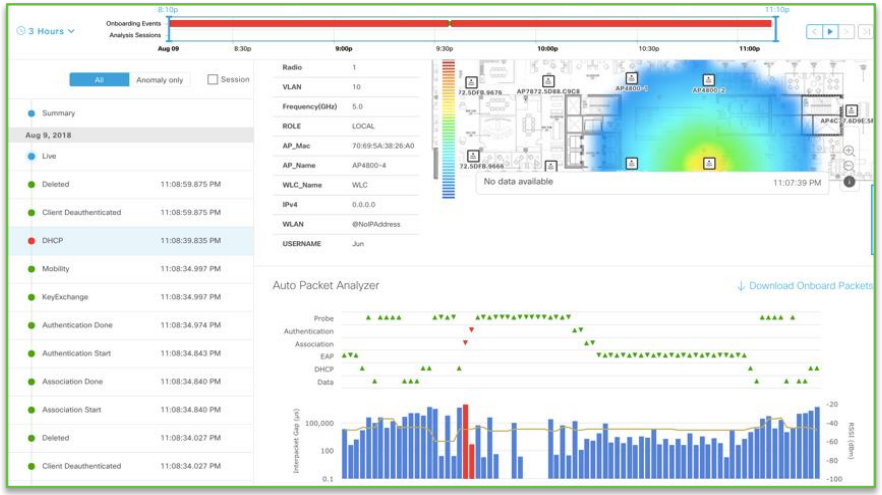
Intelligent Capture overcomes the challenge of replicating Wireless issues

Users assume the wireless network is the problem

Cross Stack Innovation
AP HW, AireOS, DNAC

Dramatic simplification via single PCAP across multiple APs with zero packet loss during roaming

Packet capture is a very difficult task over WiFi



~~72 hours~~
to minutes

Average Time to resolve user issues with Intelligent Capture

Live Client **Onboarding State** → Anomaly Triggered **PCAPs** → **On-Demand RF Scanning** → **Real-time Client Location** → **On-Demand Wi-Fi App Analytics**

Real Time Wireless Client Troubleshooting

Start and Stop Full Packet Capture for AP4800

Real-Time Live Mode

Network Time Travel

Real-Time Client Event Viewer

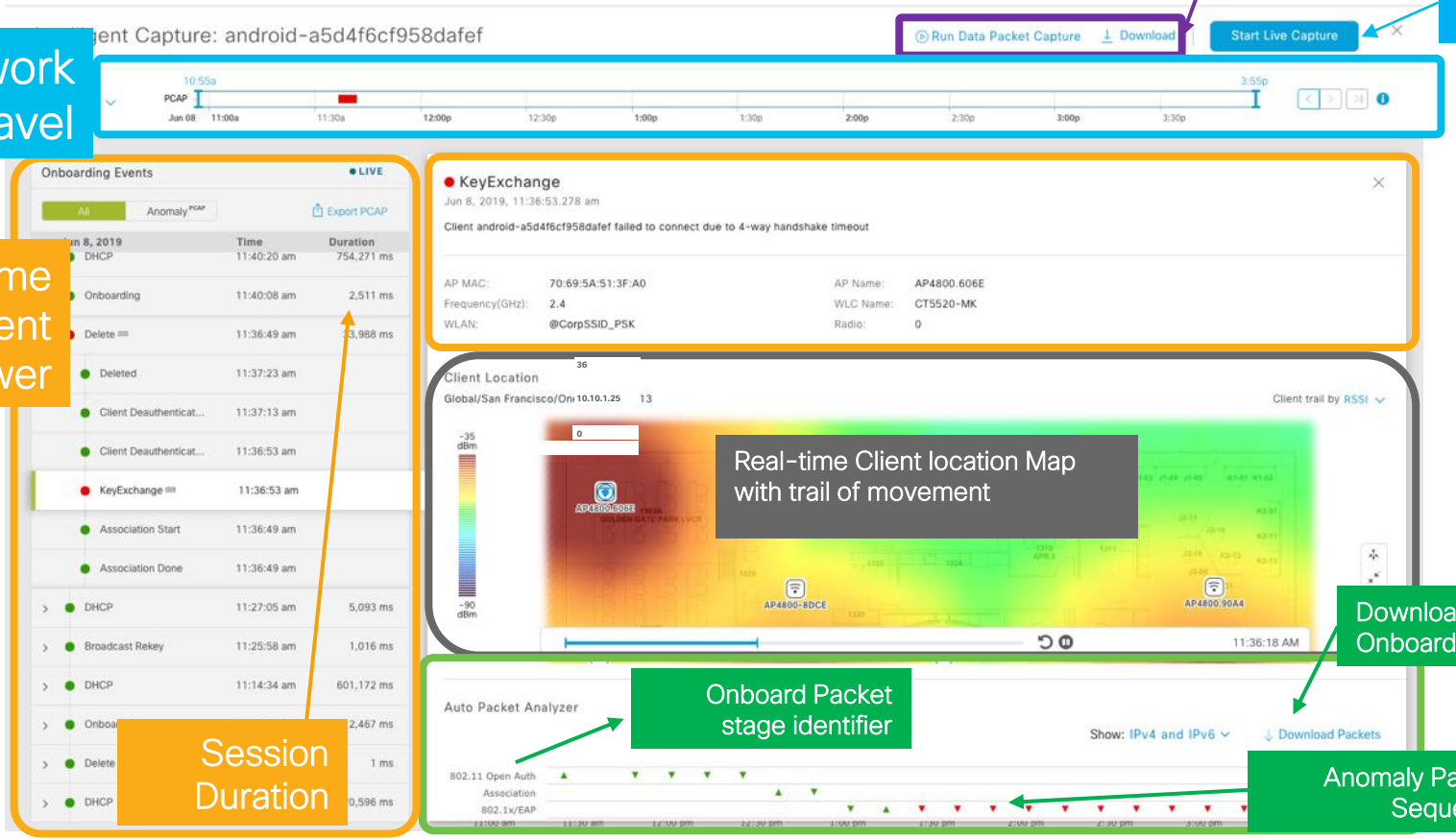
Session Duration

Real-time Client location Map with trail of movement

Onboard Packet stage identifier

Download Onboard Packet

Anomaly Packet Sequence



Real Time Spectrum Analyzers

- Persistent Fast Fourier Transform
- Swept Spectrogram

- Interferers with impacted BW
- Duty Cycle per Channel

- Available on WiFi5 und WiFi 6 APs
- Support Local/FlexConnect and Monitor mode AP

Intelligent Capture
Three Configuration Step

For Your Reference

Recommended Version

- DNAC 1.3.x
- AireOS 8.8.125/8.10
- IOS-XE 16.12.1s
- AP2800/3800/4800 AP9120/9130

Day-1 Config

1. Add WLC to DNAC (Discovery or Inventory)
2. (Optional) Hyperlocation
3. (Optional) Add CMX and vNAM to DNAC

Cisco DNAC automate all of necessary configs in WLC and AP

Intelligent Capture Operation and Scale

For Your Reference

Operation	Data Type	Concurrent Session
Global or per AP	Anomaly Packet Capture	All APs in the DNAC inventory
	Client RF stats (30 sec)	All Clients connected up to 1000 APs
	AP RF Stats	Up to 1000 APs
On-demand (Live mode) or Scheduled	Real Time Client RF stats (5sec)	Up to 16 Clients
	Real Time Client Onboarding Events from WLC (2sec. Interval)	
	OnBoard PCAP (Mgmt., DHCP/ICMP, EAP, etc.)	
On-Demand	Full Packet Capture	One Client Device
	Spectrogram View	Up to 20 APs

Cisco DNA Center
Wireless Sensor

Wireless Sensor

1

On-Boarding Tests

802.11 Association

802.11 Authentication & Key Exchange

IP Addressing DHCP (IPv4)

2

Network tests

DNS (IPv4)

RADIUS (IPv4)

First Hop Router/Default gateway (IPv4)

Intranet Host

External Host (IPv4)

3

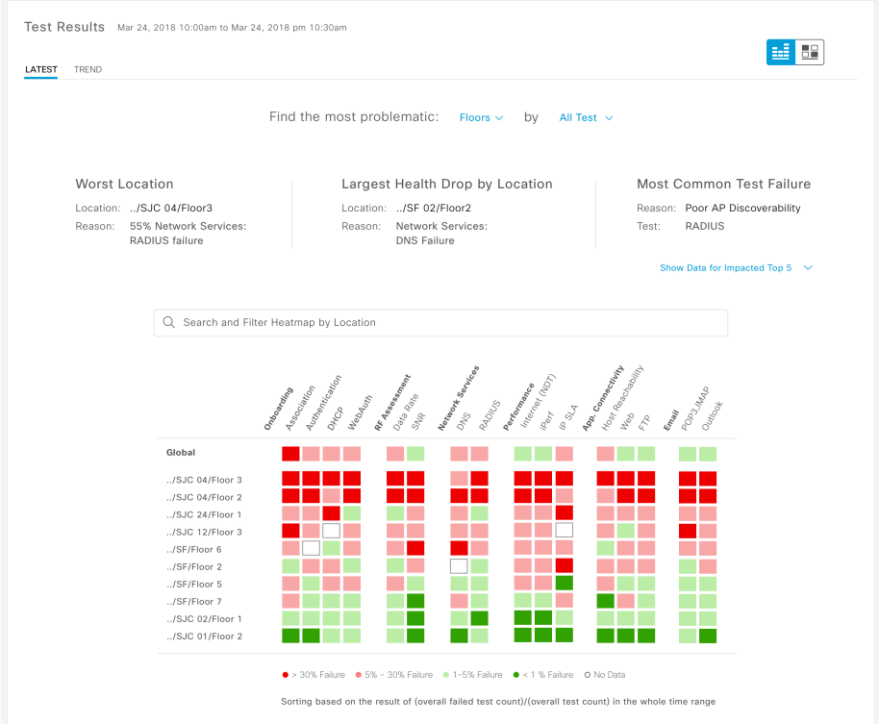
Application tests

Email: POP3, IMAP, Outlook Web Access (IPv4)

File Transfer: FTP (IPv4), iPerf Test

Web: HTTP & HTTPS (IPv4)

Wireless Sensor – Dashboard Heatmap



- Network Time Travel with Sensor Test Result
- Customizable Color grading threshold
- Insight View – Worst Location, Largest Health Drop by Location, Most Common Test Failure with reason code, expandable to top 5 on each category

Demo, Wireless Sensor

Wireless Sensor 360

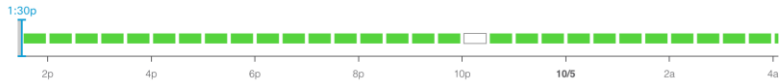
Network Time Travel

Sensor Dashboard

Sensor Sensor-0140

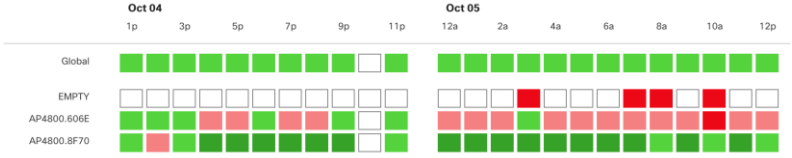
State: RUNNING Location: Global/San Francisco/SFO13/Floor13 Ethernet MAC: 70:f3:5a:78:01:40 Base Radio: 70:f3:5a:78:6b:6

IP Adress: 10.13.5.122 Type: Cisco Aironet 1800S Active Sensor Sensor Uptime: Sep 28, 2019 12:08 pm Template: ST-SFO



Target AP-based View

Test Type: All Tests



> 50% Failure 30% - 50% Failure 10% - 30% Failure < 10% Failure No Data

Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

Performance Trend w/ comparison

Sensor Performance Trend

Test Type: Association

Add Custom Location

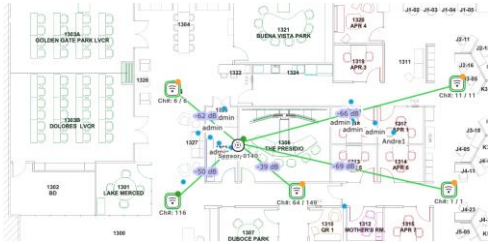
Visual Neighbor AP Map

Neighbor APs

Band 2.4 GHz 5 GHz

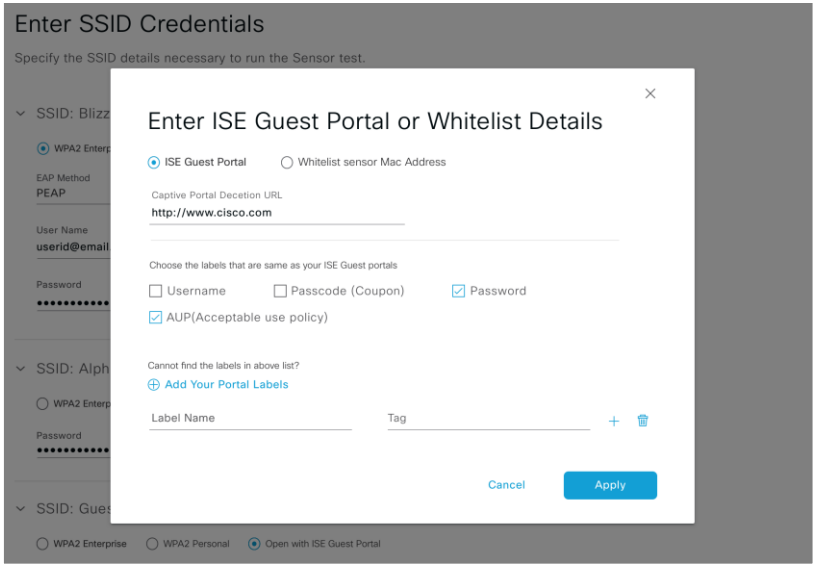
Neighbor APs	RSSI
AP4800.606E	-62 dBm
AP4800.8F70	-50 dBm
AP4800.90A4	-39 dBm
SJC.AP1F-1.8DAC	-66 dBm
SJC.AP1F-2.922C	-69 dBm

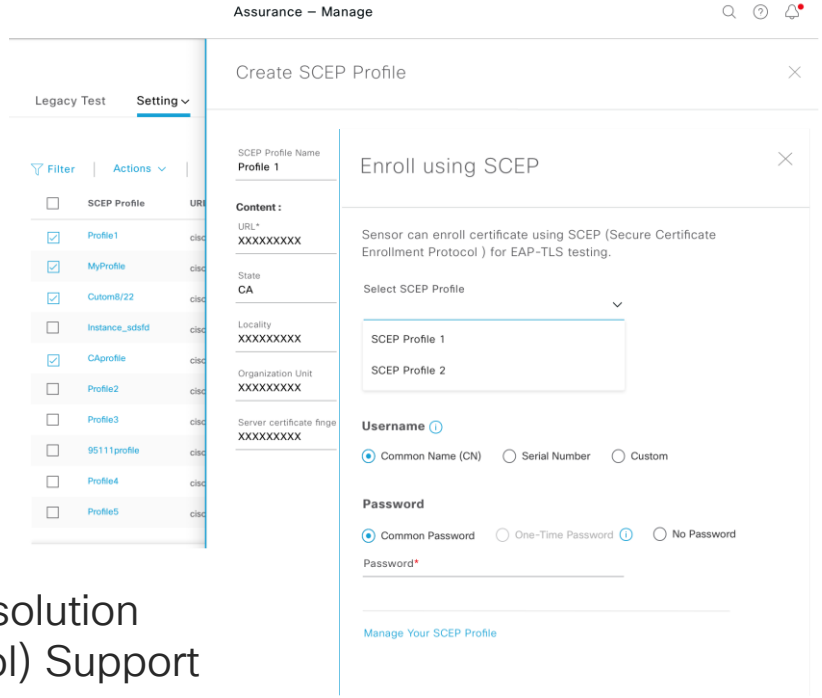
Showing 1 - 5 of 5 Previous 1 Next



Wireless Sensor – Guest Network

Guest Network Test
Sensor extended Guest SSID
Test to ISE and ClearPass





Enterprise-grade EAP-TLS provisioning solution
SCEP (Simple Certificate Enrollment Protocol) Support

Agenda

1. Introduction
2. Change in Paradigm in Network Management
3. Migration from Prime Infrastructure to Cisco DNA-Center
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

Key takeaways

Cisco DNA Assurance

Benefit from health scores and insights instead of analyzing events and alarms

Cisco DNA Center build to automate based on Cisco and Customer best practices

Cisco DNA Center Co-Existence ensures a smooth and successful migration from Prime Infrastructure

The impact of "Change in Paradigm of network management"

Mission statement :
Get all the benefits of Cisco DNA-Center with Co-Existence to Prime Infrastructure

Thank you

CISCO

Possibilities

#CiscoLive