You make **possible**

Cisco DNA Wireless Assurance

Isolate critical wireless problems for faster troubleshooting using the power of data

Prem Chandran, Technical Marketing Engineer
Paul Lysander, Technical Marketing Engineer

cisco Live!
Barcelona | January 27-31, 2020

BRKEWN-2034

Session Abstract

In this session you will get see various examples and workflow of Cisco DNA Assurance from a Wireless Use-cases perspective. It will cover all of the necessary steps to collect and correlate Wireless network operation information.

This session focuses on:

- Wireless Network SLA Management using Health and Sensor Dashboards
- Wireless Client Troubleshooting – through Intelligent Capture
- Wireless Anomaly detection, Root cause and Trend Analysis - Cisco AI Network Analytics
- Network Device remediation - Cisco Machine Reasoning Engine

Agenda

- Introducing Cisco DNA Assurance
- Key Use Cases for Wireless Network Troubleshooting
- New Innovations in Cisco DNA Assurance
- Cisco DNA Center Under the Hood
- Cisco DNA Center Assurance Deployment Best Practices
- Q&A

Introducing Cisco DNA Assurance

Unlock the power of data using contextual analytics architecture

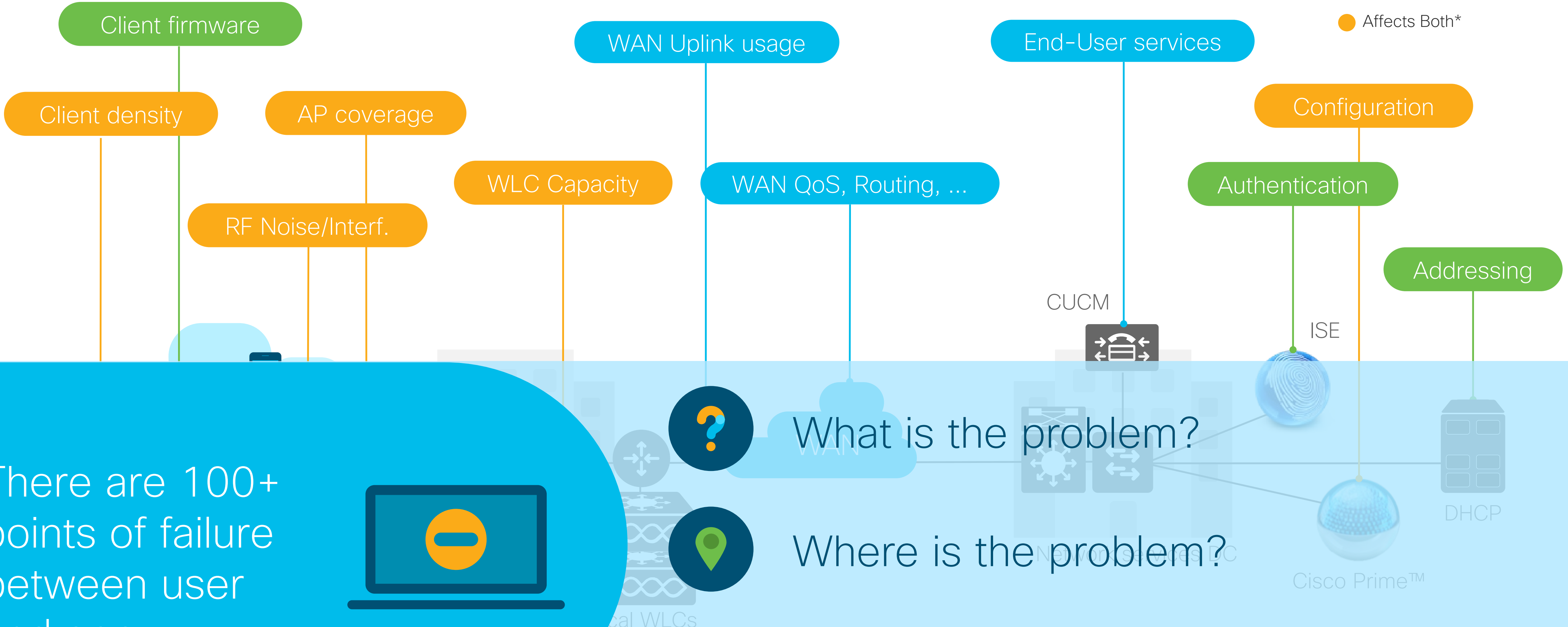
Network Assurance is a complex, end-to-end problem

"Re: Wi-Fi is Slow" – What's the root cause?

● Affects Join/Roam

● Affects Quality/Throughput

● Affects Both*



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?

* Both = Join/roam and quality/throughput

Humans Need Help

The Power of Mass Production

The Industrial Revolution liberated humans from the limits of their physical capabilities

The Power of Big Data

The Digital Revolution liberates humans from the limits of their mental capabilities

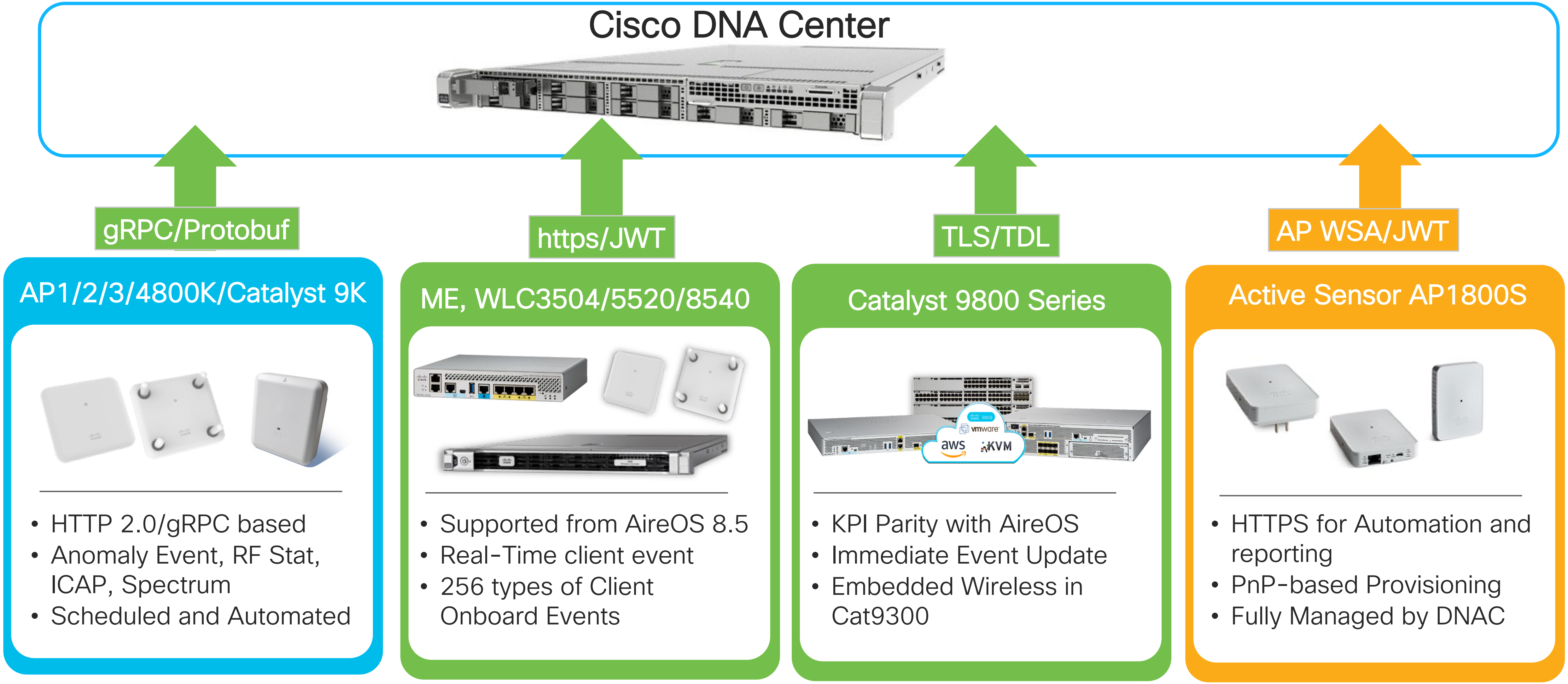
- **AI and ML**
- Contextualized Analytics
- Real-time Processing

Intent-Based Networking

Streaming Telemetry from Network Infrastructure provides right data with the right context

Traditional Telemetry		Streaming Telemetry
SNMP based Legacy data pull methods		Intent-based Wireless Infrastructure Streaming Telemetry
Pull based data import	→	Push based data export
CPU overhead with data crawlers	→	Low CPU overhead
Data intensive without optimizations	→	Optimized for Data export (KPI, Events)
No real time notification and false alarms	→	Notification send seconds after change
Min polling has too many black holes	→	Reduced delay in management data

Wireless Streaming Telemetry Architecture Purpose-Built for Cisco DNA Center Assurance



Cisco DNA Center

gRPC/Protobuf

https/JWT

TLS/TDL

AP WSA/JWT

AP1/2/3/4800K/Catalyst 9K

- HTTP 2.0/gRPC based
- Anomaly Event, RF Stat, ICAP, Spectrum
- Scheduled and Automated

ME, WLC3504/5520/8540

- Supported from AireOS 8.5
- Real-Time client event
- 256 types of Client Onboard Events

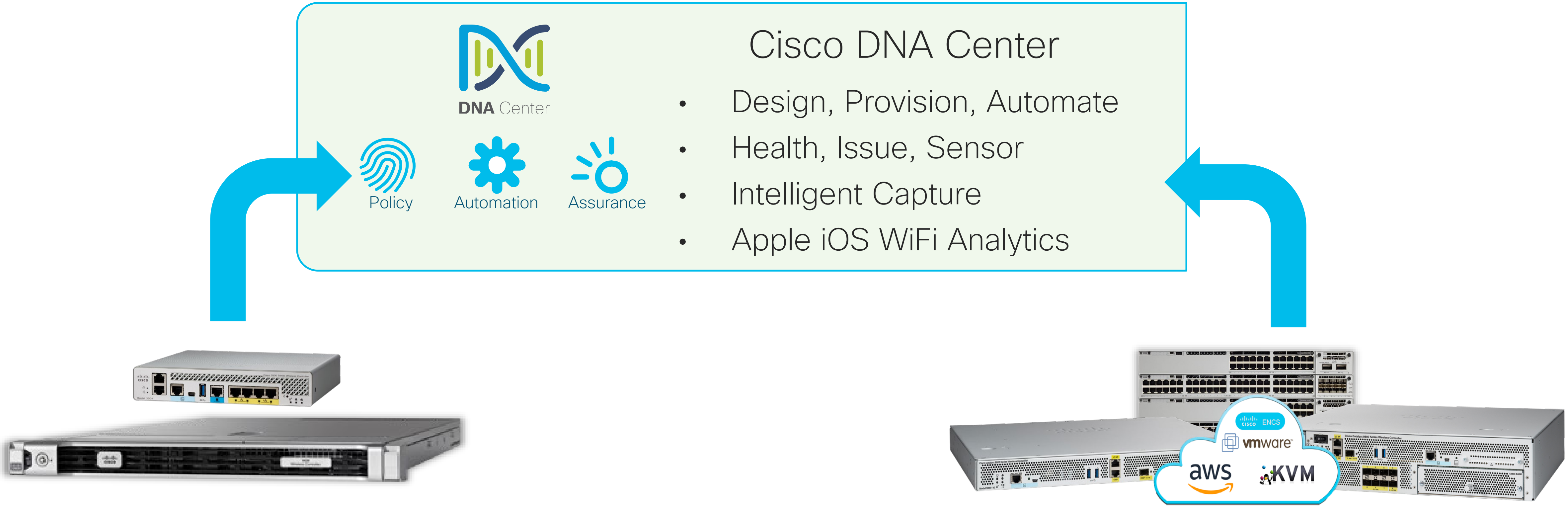
Catalyst 9800 Series

- KPI Parity with AireOS
- Immediate Event Update
- Embedded Wireless in Cat9300

Active Sensor AP1800S

- HTTPS for Automation and reporting
- PnP-based Provisioning
- Fully Managed by DNAC

Wireless Assurance provide feature Parity between AireOS and IOS-XE based Controller



Cisco DNA Center

- Design, Provision, Automate
- Health, Issue, Sensor
- Intelligent Capture
- Apple iOS WiFi Analytics

AireOS 8.5 or 8.8+

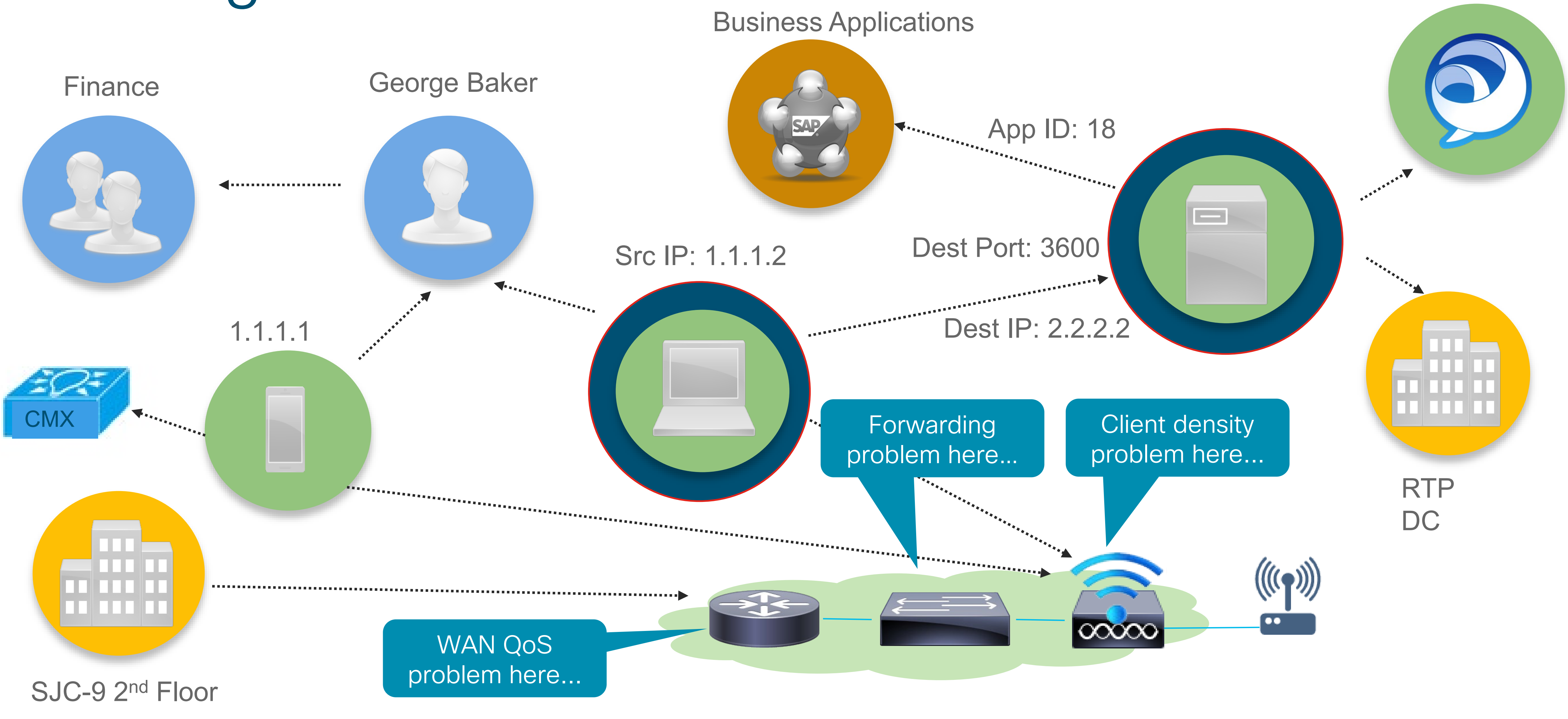
Use JWT – JSON Web Token

Catalyst 16.10.1 or later

Use TDL – Binary encoded, model-based JSON

Putting all this data into context....

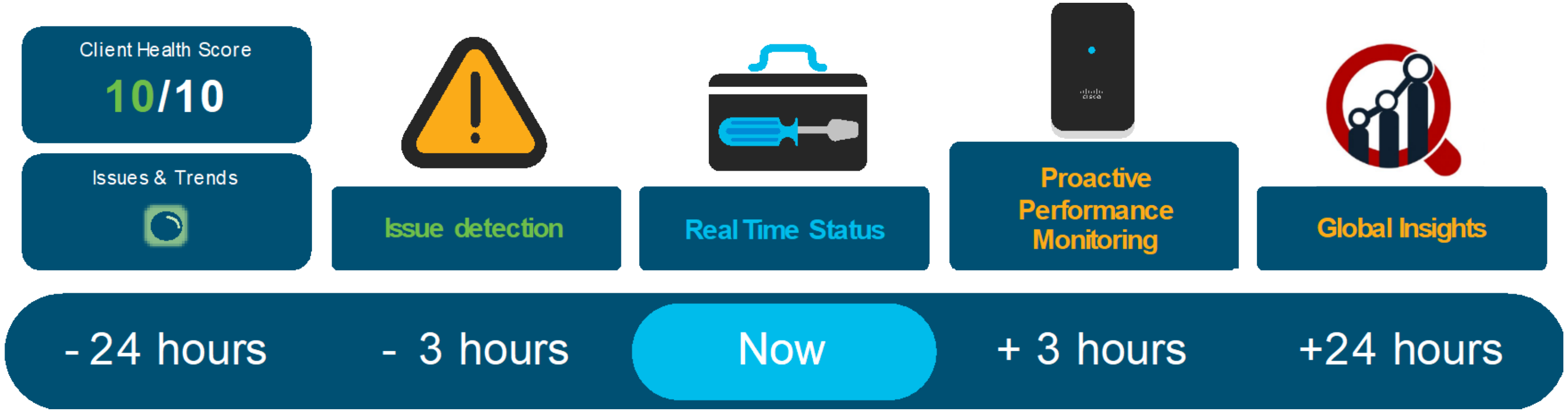
Big Data Processing



Netflow | AVC | DDI | ISE/Radius | Topology | CMX, DNAC | Device | Sensors

Network Time Travel

Big Data Processing



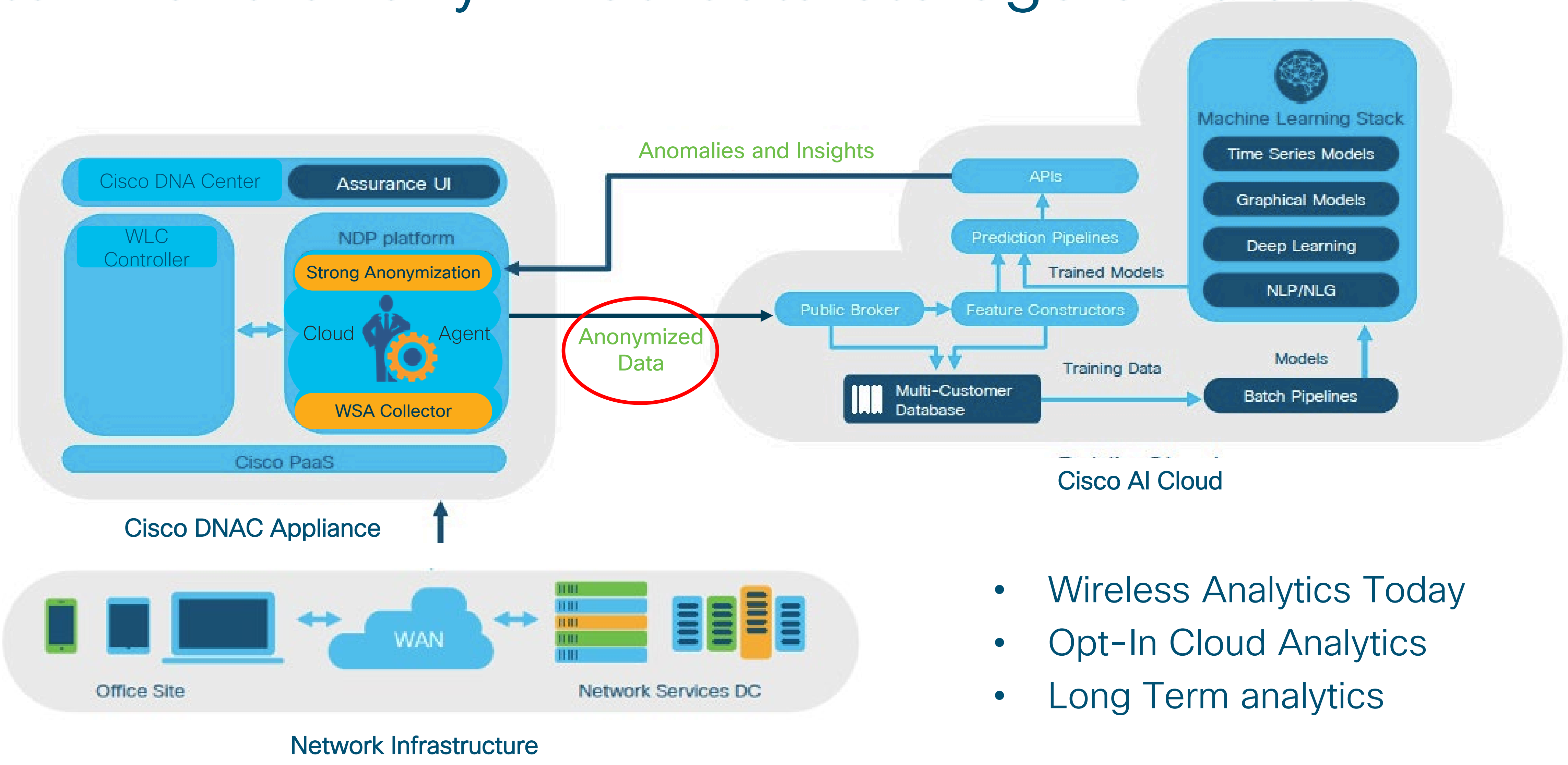
Unique Temporal Graph Technology captures network state information

Full contextual state stored for 14 days to allow time travel and recreate problem in data

5.4B+ context aware search graph entries created every 24 hours

Lowers Mean Time to Resolution and Increases end user productivity and experience

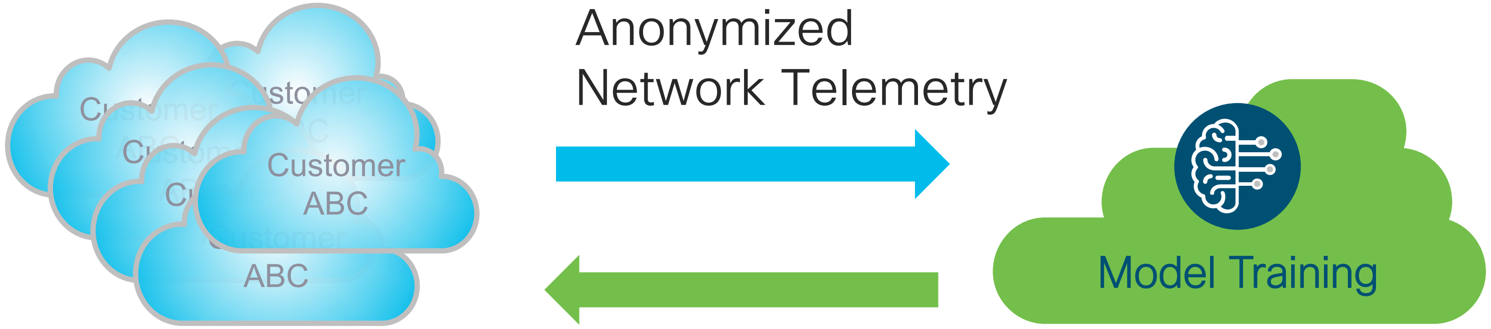
Cisco AI Network Analytics powered by Long-term and anonymized data storage on cloud



- Wireless Analytics Today
- Opt-In Cloud Analytics
- Long Term analytics

Closed-loop Cloud-based AI/ML model

- Send Network Telemetry in anonymized, encrypted, compressed way

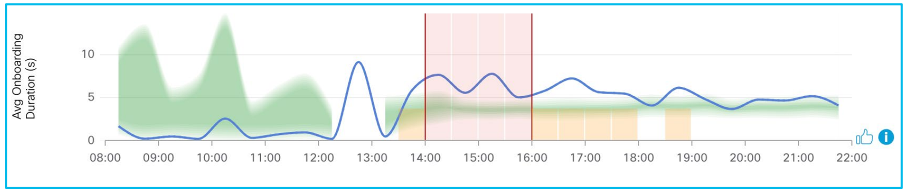


Anonymized Network Telemetry

Anomalies And Insight

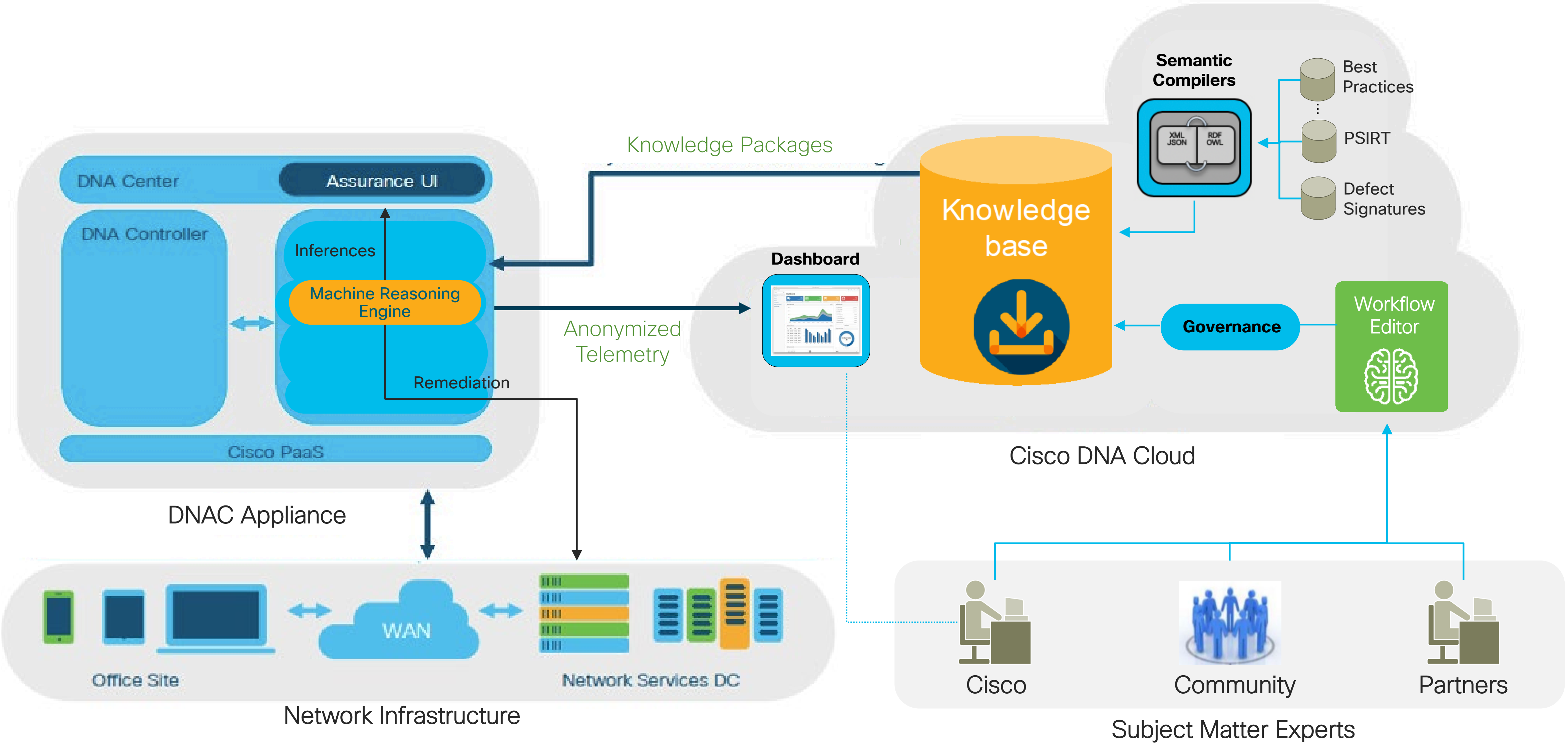
OnPrem Cisco DNA Center

Cisco AI Network Analytics Cloud

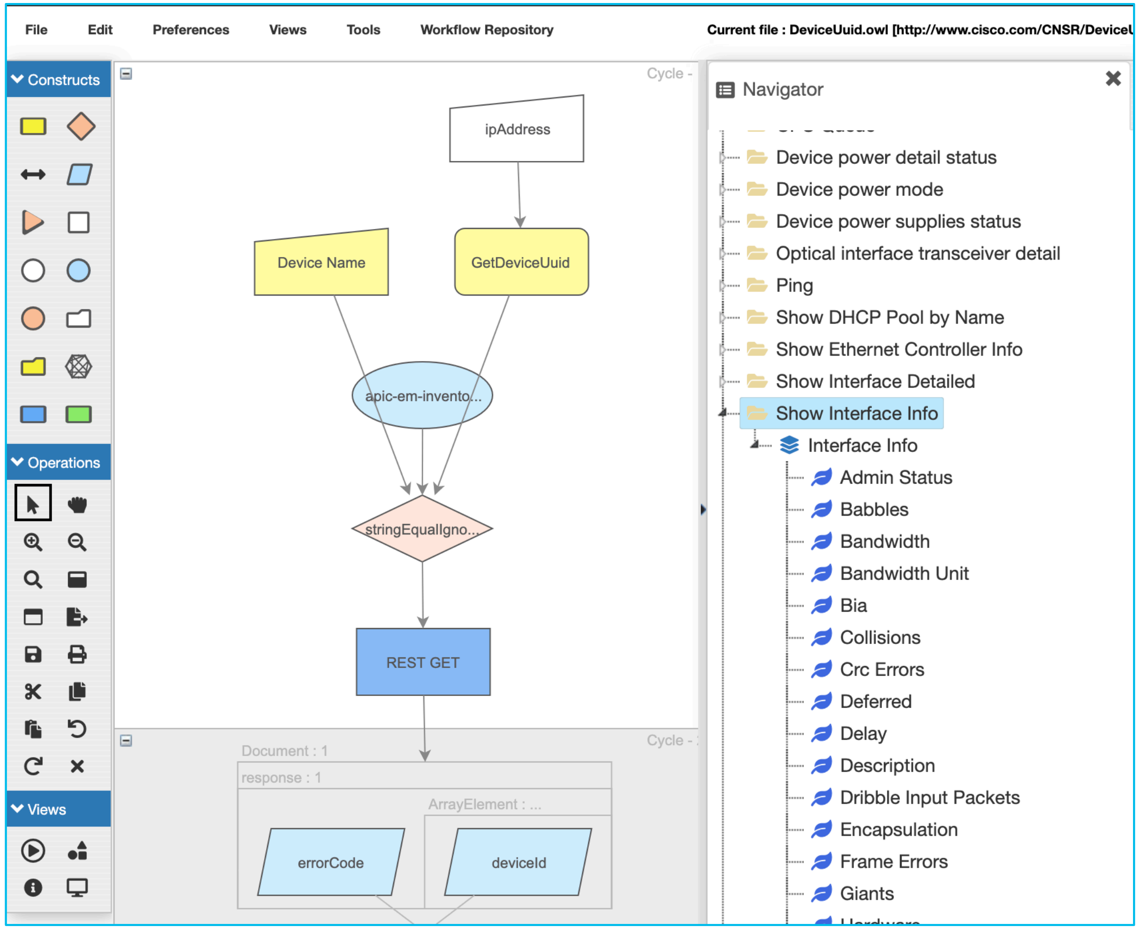


- Use Millions KPIs Stats to train Prediction model
- Get re-trained every week

Machine Reasoning Engine Architecture



Extensible knowledge-based model for capturing experts knowledge and propagate across organization



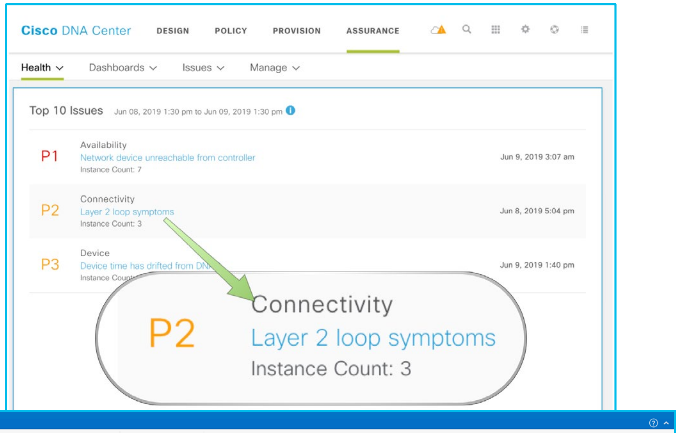
Machine Reasoning Workflow Editor

- Expert can create/contribute new network troubleshooting workflow
- Knowledge Based workflow
- Cisco DNA Center can get additional knowledge-base through Cisco Cloud
- Flow Chart Editor become Network Troubleshooting tool
- Extensible per PSIRT/CX/TAC DB

Machine Reasoning Process

1 Detect & Notification

DNA Dashboard



Top 10 Issues Jun 08, 2019 1:30 pm to Jun 09, 2019 1:30 pm

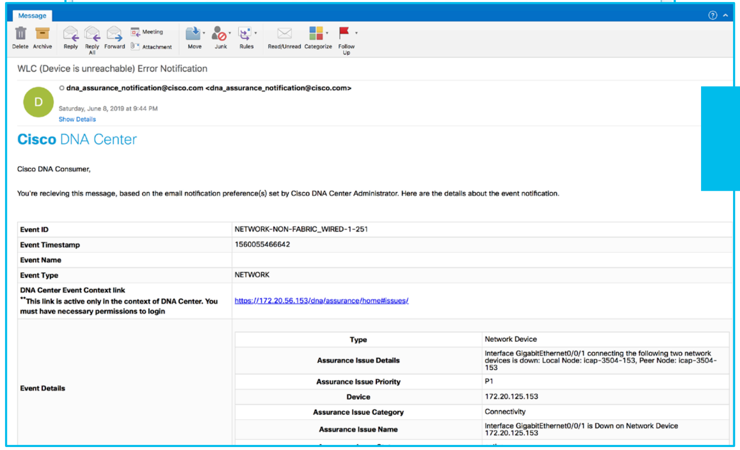
P1 Availability
Network device unreachable from controller
Instance Count: 7
Jun 9, 2019 3:07 am

P2 Connectivity
Layer 2 loop symptoms
Instance Count: 3
Jun 8, 2019 5:04 pm

P3 Device
Device time has drifted from DN
Instance Count
Jun 9, 2019 1:40 pm

P2 Connectivity
Layer 2 loop symptoms
Instance Count: 3

Email Notification



WLC (Device is unreachable) Error Notification

dna_assurance_notification@cisco.com <dna_assurance_notification@cisco.com>
Saturday, June 8, 2019 at 9:44 PM
Show Details

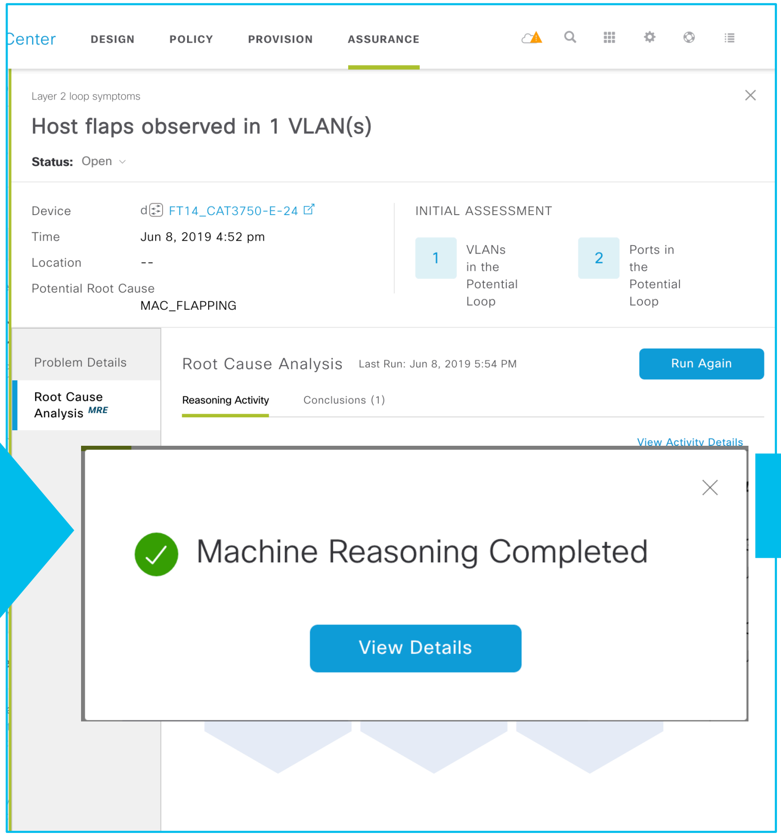
Cisco DNA Center

Cisco DNA Consumer,

You're recieving this message, based on the email notification preference(s) set by Cisco DNA Center Administrator. Here are the details about the event notification.

Event ID	NETWORK-NON-FABRIC_WIRED-1-251	
Event Timestamp	1560055466642	
Event Name		
Event Type	NETWORK	
DNA Center Event Context link **This link is active only in the context of DNA Center. You must have necessary permissions to login**	https://172.20.56.153/dna/assurance/home#issues/	
Event Details	**Type**	Network Device
	Assurance Issue Details	Interface GigabitEthernet0/0/1 connecting the following two network devices is down: Local Node: icap-3504-153, Peer Node: icap-3504-153
	Assurance Issue Priority	P1
	Device	172.20.125.153
	Assurance Issue Category	Connectivity
	Assurance Issue Name	Interface GigabitEthernet0/0/1 is Down on Network Device 172.20.125.153

2 Machine Reasoning



Layer 2 loop symptoms

Host flaps observed in 1 VLAN(s)

Status: Open

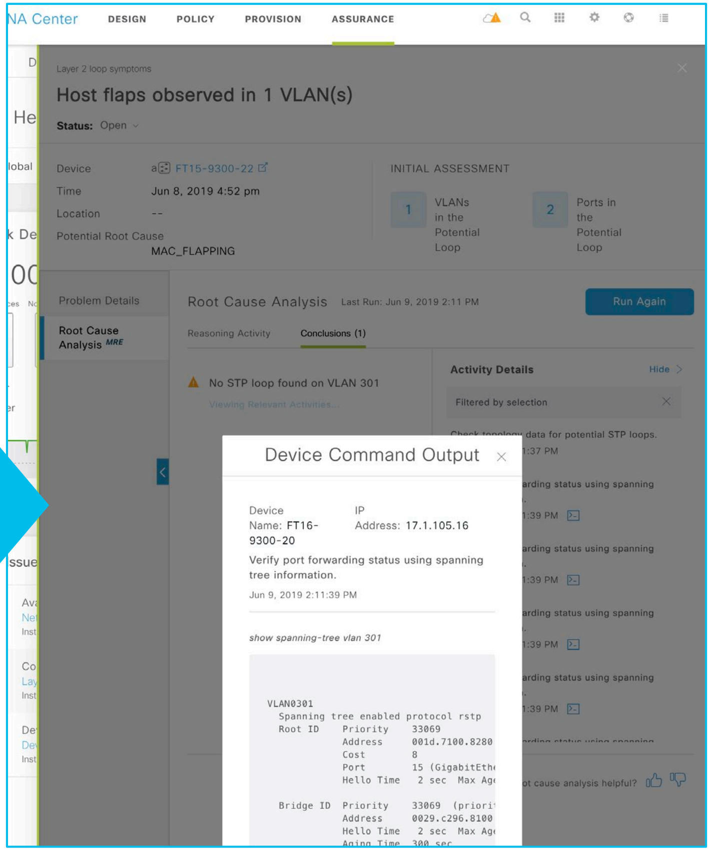
Device d FT14_CAT3750-E-24
Time Jun 8, 2019 4:52 pm
Location --
Potential Root Cause MAC_FLAPPING

INITIAL ASSESSMENT
1 VLANs in the Potential Loop
2 Ports in the Potential Loop

Root Cause Analysis Last Run: Jun 8, 2019 5:54 PM

Machine Reasoning Completed

3 Conclusion



Layer 2 loop symptoms

Host flaps observed in 1 VLAN(s)

Status: Open

Device a FT15-9300-22
Time Jun 8, 2019 4:52 pm
Location --
Potential Root Cause MAC_FLAPPING

INITIAL ASSESSMENT
1 VLANs in the Potential Loop
2 Ports in the Potential Loop

Root Cause Analysis Last Run: Jun 9, 2019 2:11 PM

No STP loop found on VLAN 301

Check topology data for potential STP loops.
1:37 PM
arding status using spanning
1:39 PM
arding status using spanning
1:39 PM
arding status using spanning
1:39 PM
arding status using spanning
1:39 PM

ot cause analysis helpful?

Device Command Output

Device Name: FT16-9300-20
IP Address: 17.1.105.16

Verify port forwarding status using spanning tree information.

Jun 9, 2019 2:11:39 PM

show spanning-tree vlan 301

```
VLAN0301
  Spanning tree enabled protocol rstp
  Root ID    Priority    33069
             Address     001d.7100.8280
             Cost        8
             Port        15 (GigabitEthe
             Hello Time   2 sec  Max Age

  Bridge ID  Priority    33069  (priori
             Address     0029.c296.8100
             Hello Time   2 sec  Max Age
             Aging Time  300 sec
```

Key Use Cases for Network Operators

Troubleshooting Wireless Networks

Troubleshooting Tool-kits for a Network operator

Cisco DNA Center Assurance

AI

Streaming Telemetry

Intelligent Capture Auto PCAPs

Active Sensor Testing

iOS and Samsung Analytics

AI Anomaly Baselining

AI Network Insight

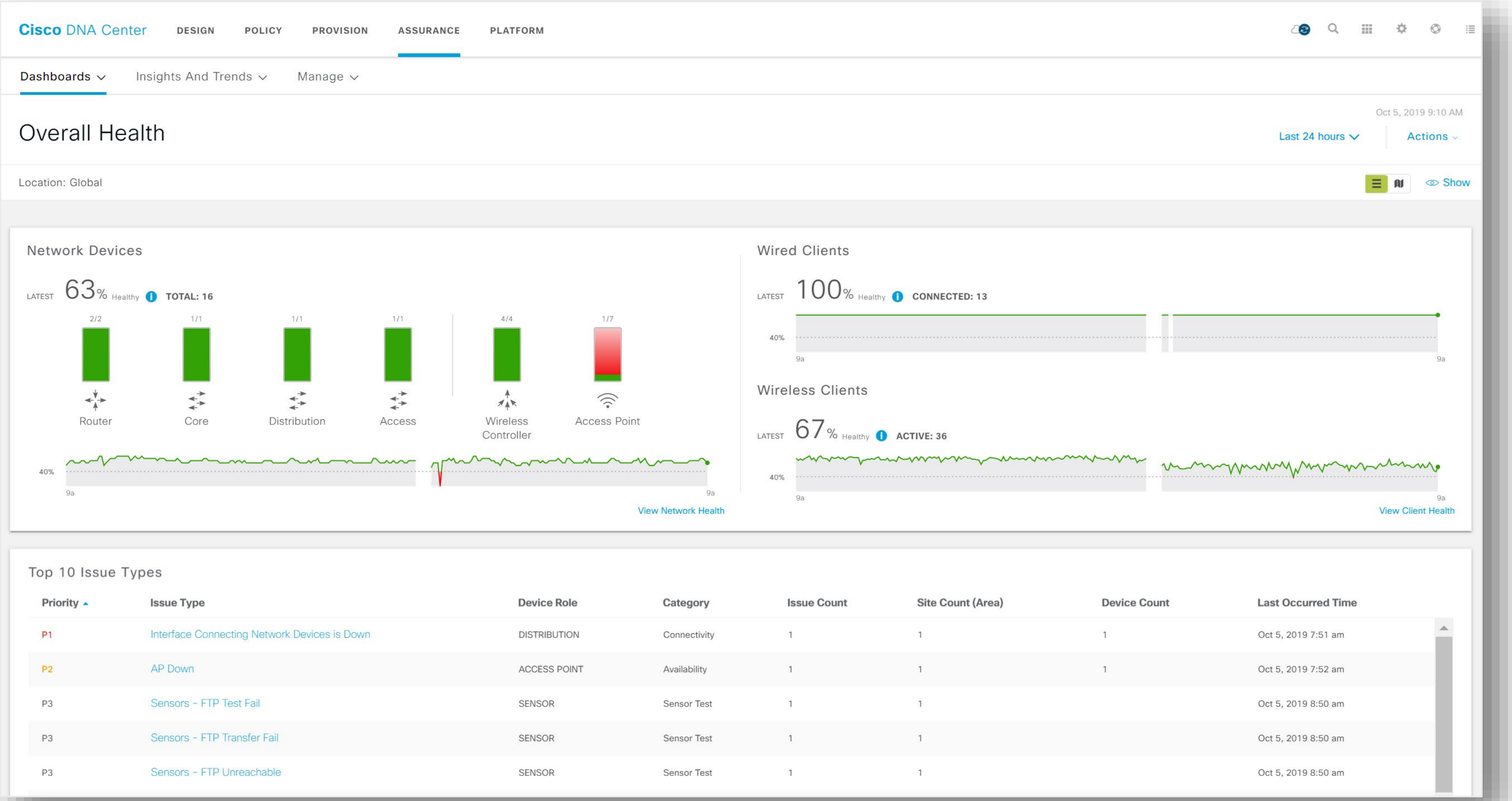
Machine Reasoning

Active Sensor for Wireless Network SLA assessment

Cisco APs with Intelligent Capture

Use case 1: Health State of my Network What is in my network and how is it doing?

Overall Health Dashboard for summary view



Overall Health

Oct 5, 2019 9:10 AM

Location: Global

Network Devices

LATEST 63% Healthy TOTAL: 16

Wired Clients

LATEST 100% Healthy CONNECTED: 13

Wireless Clients

LATEST 67% Healthy ACTIVE: 36

Top 10 Issue Types

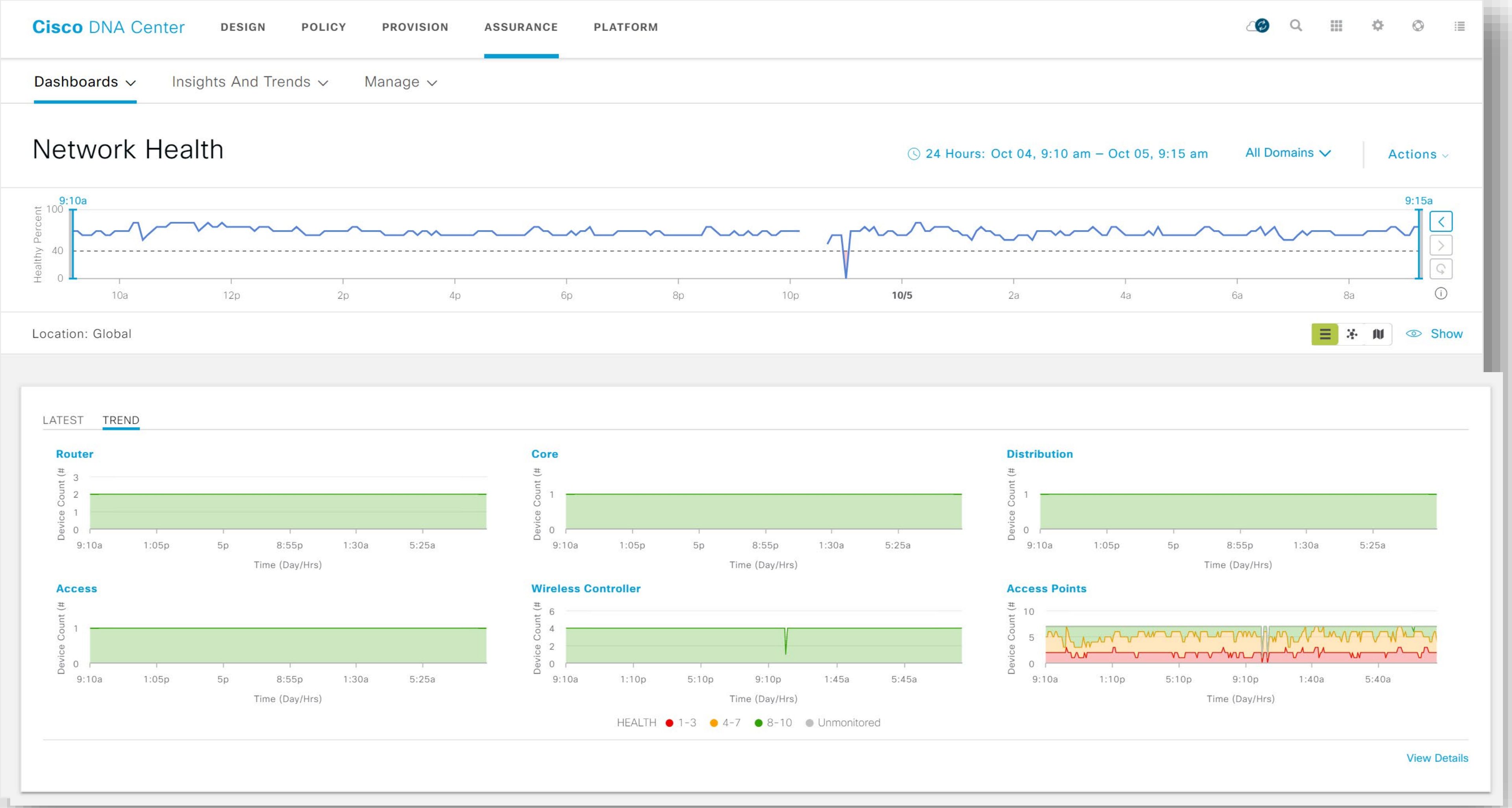
Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	Interface Connecting Network Devices is Down	DISTRIBUTION	Connectivity	1	1	1	Oct 5, 2019 7:51 am
P2	AP Down	ACCESS POINT	Availability	1	1	1	Oct 5, 2019 7:52 am
P3	Sensors - FTP Test Fail	SENSOR	Sensor Test	1	1		Oct 5, 2019 8:50 am
P3	Sensors - FTP Transfer Fail	SENSOR	Sensor Test	1	1		Oct 5, 2019 8:50 am
P3	Sensors - FTP Unreachable	SENSOR	Sensor Test	1	1		Oct 5, 2019 8:50 am

What is in my network and where are the hotspots?

What are the top issues affecting my network?

Use case 1: Network Visibility
How is my Network Infrastructure doing?

Network Health Dashboard for Top Reasons Impacting Network Health



Network Health

24 Hours: Oct 04, 9:10 am – Oct 05, 9:15 am

Location: Global

HEALTH ● 1-3 ● 4-7 ● 8-10 ● Unmonitored

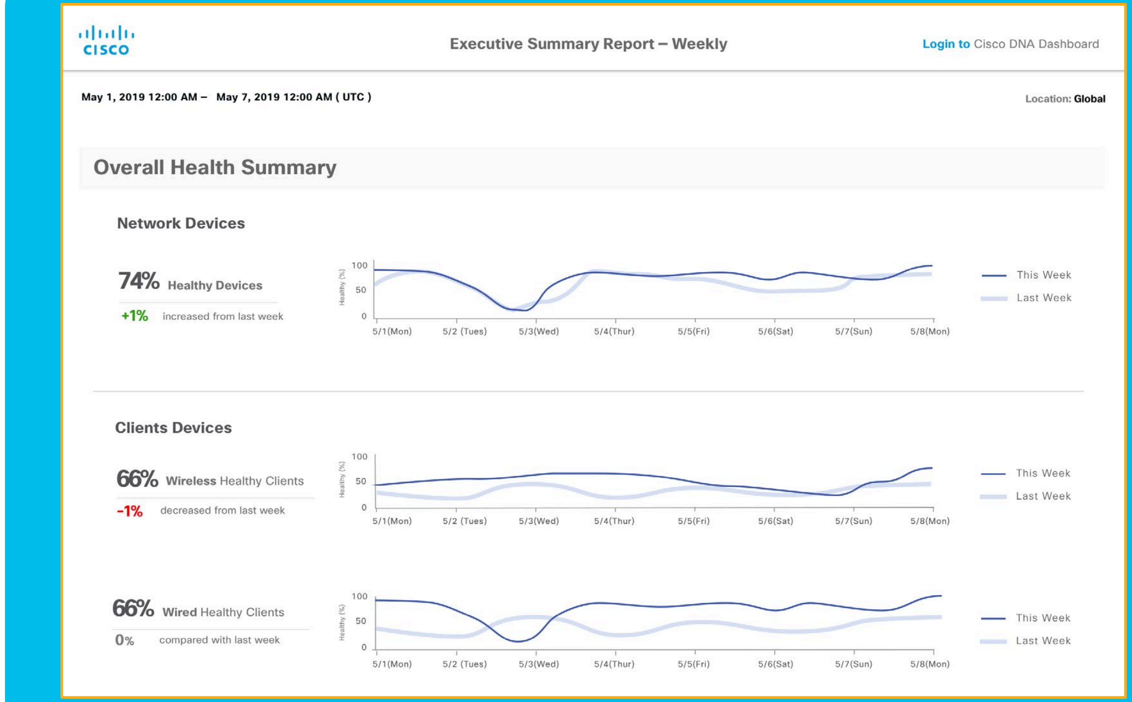
Did it change recently?

How many devices have fair/poor health and why?

New

Use case 1: Network Visibility Executive Summary Report

- Single Assurance Report captures Network/Client Health, Inventory and Issue summary
- 7 Days + 7 Days, Emphasize *delta* from last period


Executive Summary Report – Weekly

Login to Cisco DNA Dashboard

May 1, 2019 12:00 AM – May 7, 2019 12:00 AM (UTC)

Location: Global

Overall Health Summary

Network Devices

74% Healthy Devices

+1% increased from last week

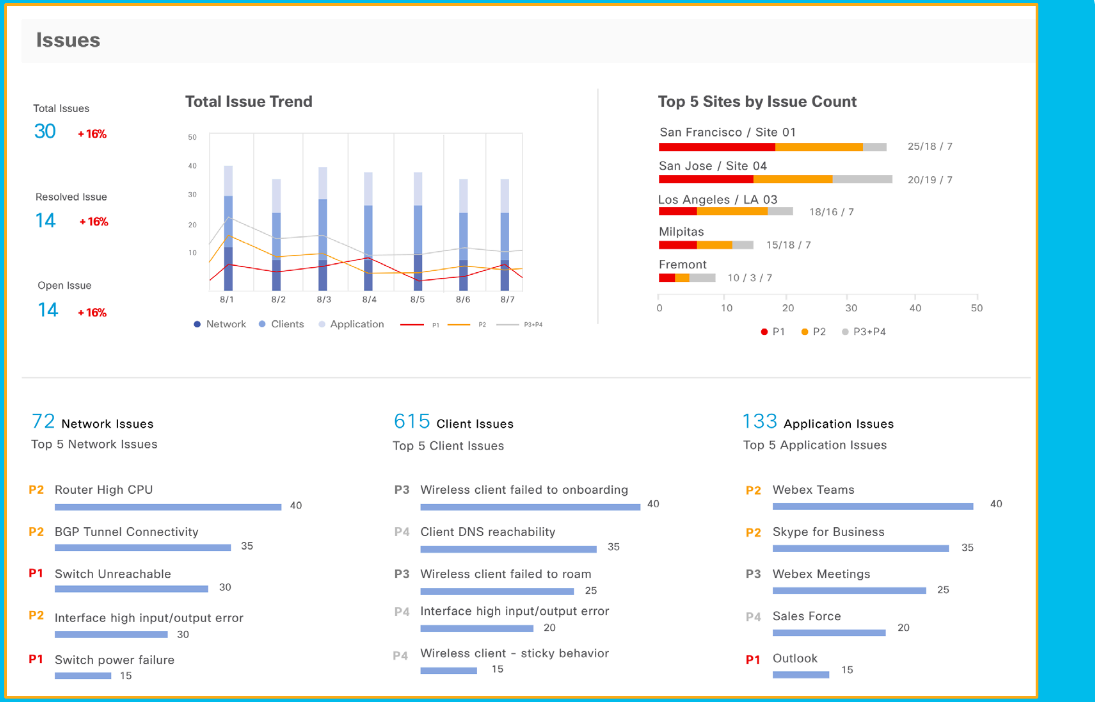
Clients Devices

66% Wireless Healthy Clients

-1% decreased from last week

66% Wired Healthy Clients

0% compared with last week


Issues

Total Issues 30 +16%

Resolved Issue 14 +16%

Open Issue 14 +16%

Total Issue Trend

Top 5 Sites by Issue Count

Site	P1/P2/P3+P4
San Francisco / Site 01	25/18 / 7
San Jose / Site 04	20/19 / 7
Los Angeles / LA 03	18/16 / 7
Milpitas	15/18 / 7
Fremont	10 / 3 / 7

72 Network Issues

Top 5 Network Issues

P2	Router High CPU	40
P2	BGP Tunnel Connectivity	35
P1	Switch Unreachable	30
P2	Interface high input/output error	30
P1	Switch power failure	15

615 Client Issues

Top 5 Client Issues

P3	Wireless client failed to onboarding	40
P4	Client DNS reachability	35
P3	Wireless client failed to roam	25
P4	Interface high input/output error	20
P4	Wireless client - sticky behavior	15

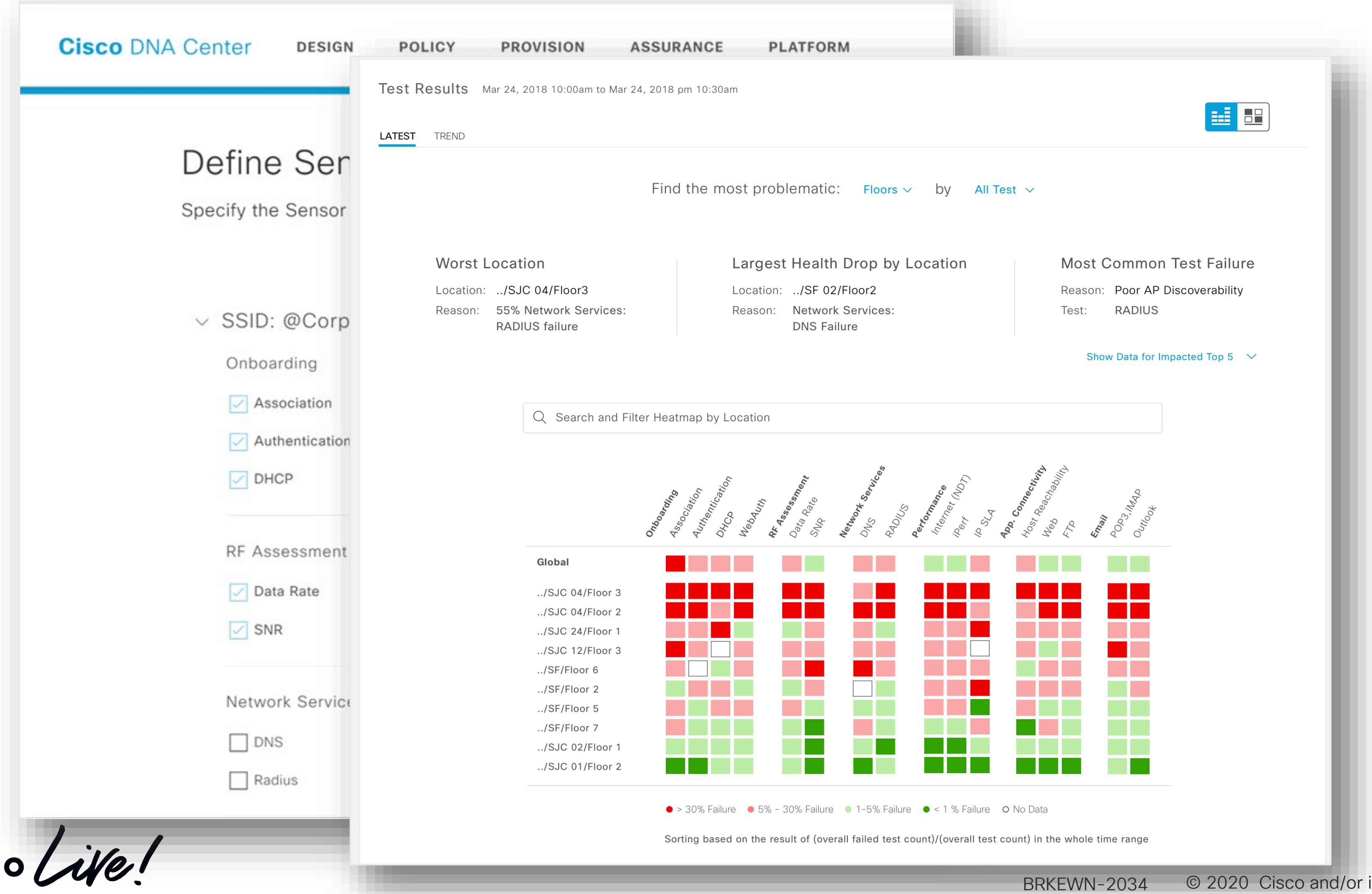
133 Application Issues

Top 5 Application Issues

P2	Webex Teams	40
P2	Skype for Business	35
P3	Webex Meetings	25
P4	Sales Force	20
P1	Outlook	15

Use case 2: Managing Network SLAs
How does my Wireless Network assessment look like?

Sensor Test and Dashboard



Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Define Ser

Specify the Sensor

SSID: @Corp

Onboarding

☑ Association

☑ Authentication

☑ DHCP

RF Assessment

☑ Data Rate

☑ SNR

Network Servic

□ DNS

□ Radius

Test Results Mar 24, 2018 10:00am to Mar 24, 2018 pm 10:30am

LATEST TREND

Find the most problematic: Floors by All Test

Worst Location
Location: ../SJC 04/Floor3
Reason: 55% Network Services: RADIUS failure

Largest Health Drop by Location
Location: ../SF 02/Floor2
Reason: Network Services: DNS Failure

Most Common Test Failure
Reason: Poor AP Discoverability
Test: RADIUS

Show Data for Impacted Top 5

Search and Filter Heatmap by Location

	Onboarding				**RF Assessment**		**Network Services**		**Performance**			**App. Connectivity**			**Email**	
	Association	Authentication	DHCP	WebAuth	Data Rate	SNR	DNS	RADIUS	Internet (NDT)	iPerf	IP SLA	Host Reachability	Web	FTP	POP3,IMAP	Outlook
Global	🟥	🟧	🟧	🟧	🟧	🟨	🟧	🟧	🟨	🟨	🟧	🟧	🟨	🟨	🟨	🟨
../SJC 04/Floor 3	🟥	🟥	🟥	🟥	🟥	🟥	🟧	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
../SJC 04/Floor 2	🟥	🟥	🟧	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟧	🟧	🟥	🟥	🟥	🟥
../SJC 24/Floor 1	🟧	🟧	🟥	🟨	🟨	🟧	🟧	🟨	🟧	🟧	🟥	🟧	🟧	🟧	🟧	🟧
../SJC 12/Floor 3	🟥	🟧	□	🟧	🟧	🟧	🟧	🟧	🟧	🟧	□	🟧	🟨	🟧	🟥	🟧
../SF/Floor 6	🟧	□	🟨	🟧	🟧	🟥	🟥	🟧	🟧	🟧	🟧	🟨	🟧	🟧	🟧	🟧
../SF/Floor 2	🟨	🟧	🟧	🟨	🟨	🟧	□	🟨	🟧	🟧	🟥	🟧	🟧	🟧	🟨	🟧
../SF/Floor 5	🟧	🟨	🟧	🟧	🟧	🟨	🟨	🟨	🟧	🟧	🟩	🟧	🟨	🟨	🟨	🟨
../SF/Floor 7	🟧	🟨	🟨	🟨	🟨	🟩	🟧	🟨	🟨	🟨	🟧	🟩	🟧	🟨	🟨	🟨
../SJC 02/Floor 1	🟨	🟨	🟨	🟨	🟨	🟩	🟨	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟨	🟨
../SJC 01/Floor 2	🟩	🟩	🟨	🟨	🟨	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟩

🟥 > 30% Failure 🟧 5% - 30% Failure 🟨 1-5% Failure 🟩 < 1 % Failure □ No Data

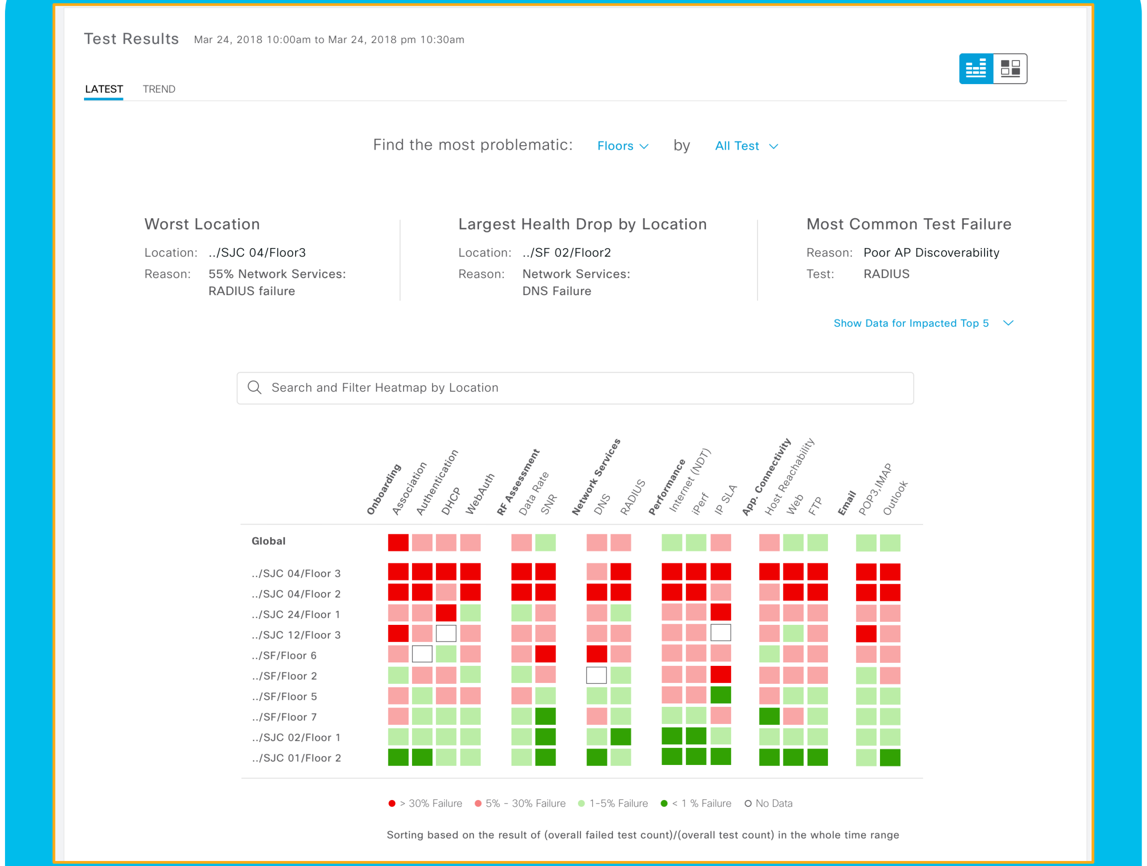
Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

Automate tests across multiple sites

Proactively monitor problematic sites from Sensor Dashboards

New

Sensor Dashboard Heatmap-based Navigation



Test Results Mar 24, 2018 10:00am to Mar 24, 2018 pm 10:30am

Find the most problematic: Floors by All Test

Worst Location
Location: ../SJC 04/Floor3
Reason: 55% Network Services: RADIUS failure

Largest Health Drop by Location
Location: ../SF 02/Floor2
Reason: Network Services: DNS Failure

Most Common Test Failure
Reason: Poor AP Discoverability
Test: RADIUS

Show Data for Impacted Top 5

Search and Filter Heatmap by Location

	Onboarding				RF Assessment		Network Services		Performance			App. Connectivity			Email	
	Association	Authentication	DHCP	WebAuth	Data Rate	SNR	DNS	RADIUS	Internet (NDT)	iPerf	IP SLA	Host Reachability	Web	FTP	POP3,IMAP	Outlook
Global	🟥	▨	▨	▨	▨	░	▨	▨	░	░	▨	▨	░	░	░	░
../SJC 04/Floor 3	🟥	🟥	🟥	🟥	🟥	🟥	▨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
../SJC 04/Floor 2	🟥	🟥	▨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	🟥	🟥	🟥	🟥
../SJC 24/Floor 1	▨	▨	🟥	░	░	▨	▨	░	▨	▨	🟥	▨	▨	▨	▨	▨
../SJC 12/Floor 3	🟥	▨	□	▨	▨	▨	▨	▨	▨	▨	□	▨	░	▨	🟥	▨
../SF/Floor 6	▨	□	░	▨	▨	🟥	🟥	▨	▨	▨	▨	░	▨	▨	▨	▨
../SF/Floor 2	░	▨	▨	░	░	▨	□	░	▨	▨	🟥	▨	▨	▨	░	▨
../SF/Floor 5	▨	░	▨	▨	▨	░	░	░	▨	▨	🟩	▨	░	░	░	░
../SF/Floor 7	▨	░	░	░	░	🟩	▨	░	░	░	▨	🟩	▨	░	░	░
../SJC 02/Floor 1	░	░	░	░	░	🟩	░	🟩	🟩	🟩	░	░	░	░	░	░
../SJC 01/Floor 2	🟩	🟩	░	░	░	🟩	🟩	░	🟩	🟩	🟩	🟩	🟩	🟩	░	🟩

🟥 > 30% Failure ▨ 5% - 30% Failure ░ 1-5% Failure 🟩 < 1 % Failure □ No Data

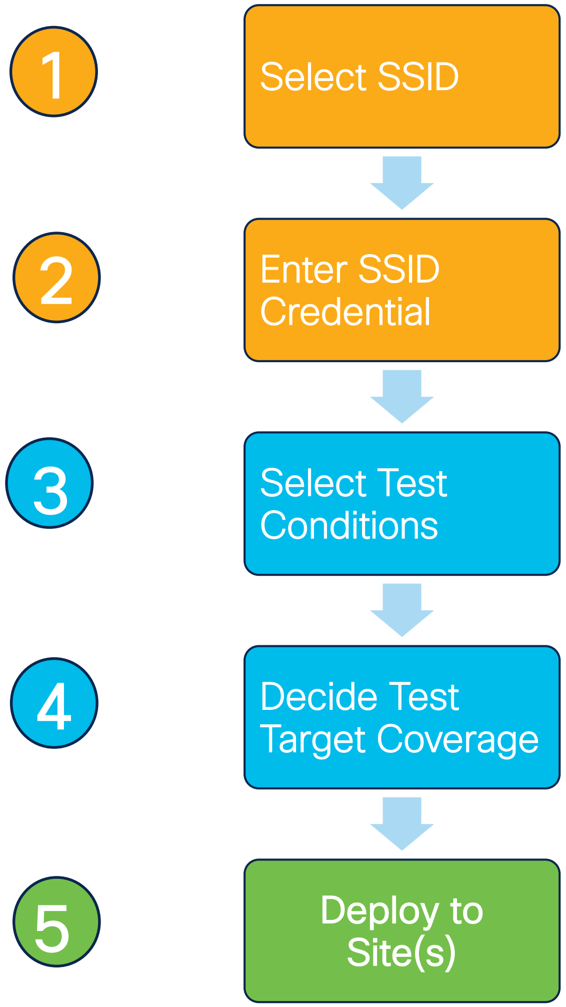
Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

- 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
- Search Bar to find any location/site
- Insight page for Actionable, Location-based insight
- Familiar Assurance Workflow – Network Time Travel, LATEST/TREND
- Drill-Down View to Test Result Detail

cisco Live!

New

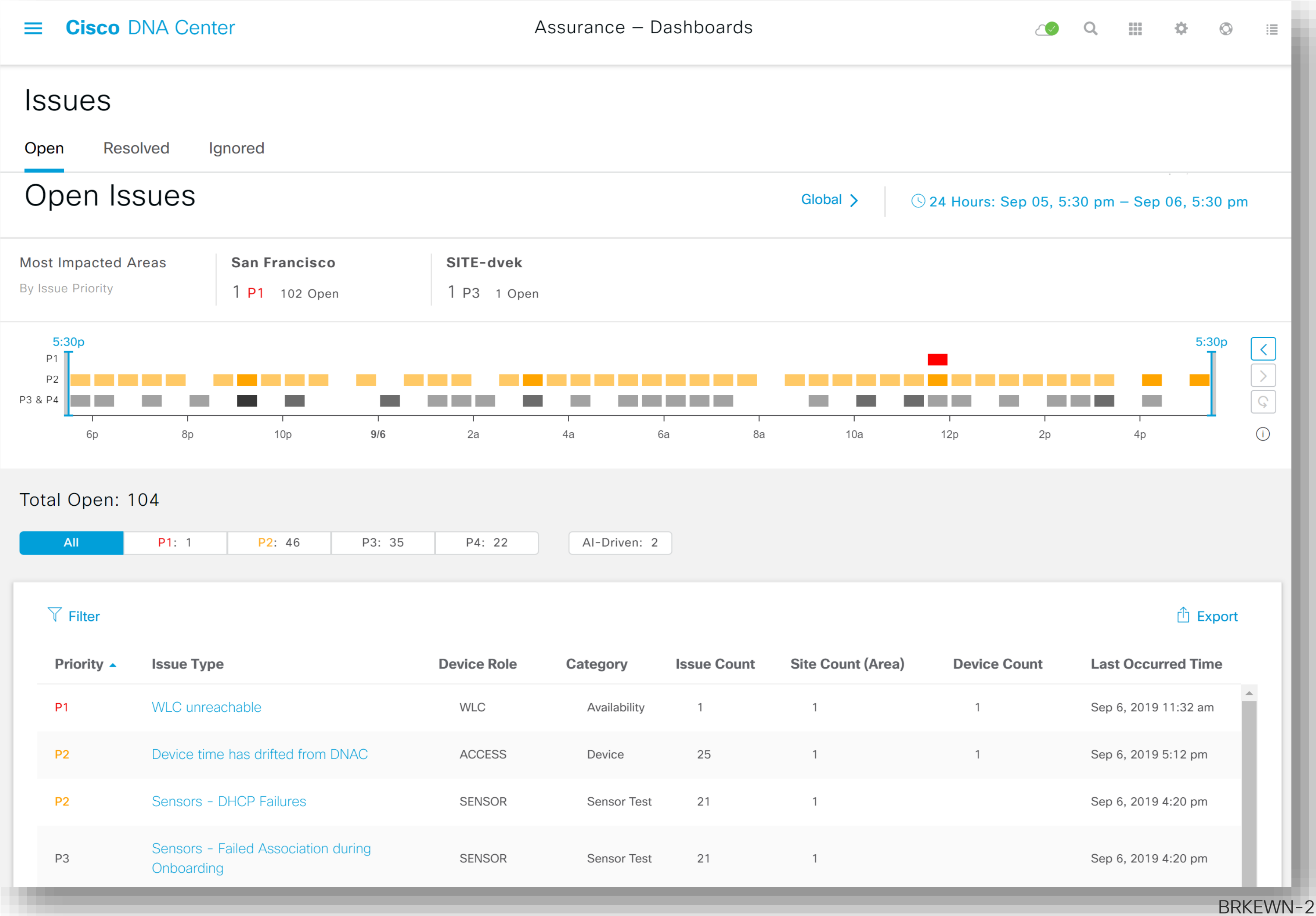
5 Easy Steps to Define a Sensor Test Template



- Create Once, Unlimited Reuse - Location-based Template (Global/Site/Building/Floor level control)
- Per-Site or or per-Sensor assignment
- Intuitive, Easy to use, DNAC Workflow 2.0 based automation flow.
- Single Test Template per Sensor
- Easy Template Edit
- Unique Sensor Test Case scenario per SSID
- Band-specific Test Coverage Control
- Resource Protection based on Sensor Test Estimation
- New Scheduling option – 7 min./ 15min Interval, Time of day, Continuous

Use case 3: Network Infrastructure is Unreachable
How can I get visibility into issues impacting my Network?

Issue Dashboard to analyze high priority issues and top sites having issues



Issues

Open Resolved Ignored

Open Issues

Global > 24 Hours: Sep 05, 5:30 pm – Sep 06, 5:30 pm

Most Impacted Areas
By Issue Priority

San Francisco
1 P1 102 Open

SITE-dvek
1 P3 1 Open

Total Open: 104

All | P1: 1 | P2: 46 | P3: 35 | P4: 22 | AI-Driven: 2

Filter Export

Priority ▲	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	WLC unreachable	WLC	Availability	1	1	1	Sep 6, 2019 11:32 am
P2	Device time has drifted from DNAC	ACCESS	Device	25	1	1	Sep 6, 2019 5:12 pm
P2	Sensors - DHCP Failures	SENSOR	Sensor Test	21	1		Sep 6, 2019 4:20 pm
P3	Sensors - Failed Association during Onboarding	SENSOR	Sensor Test	21	1		Sep 6, 2019 4:20 pm

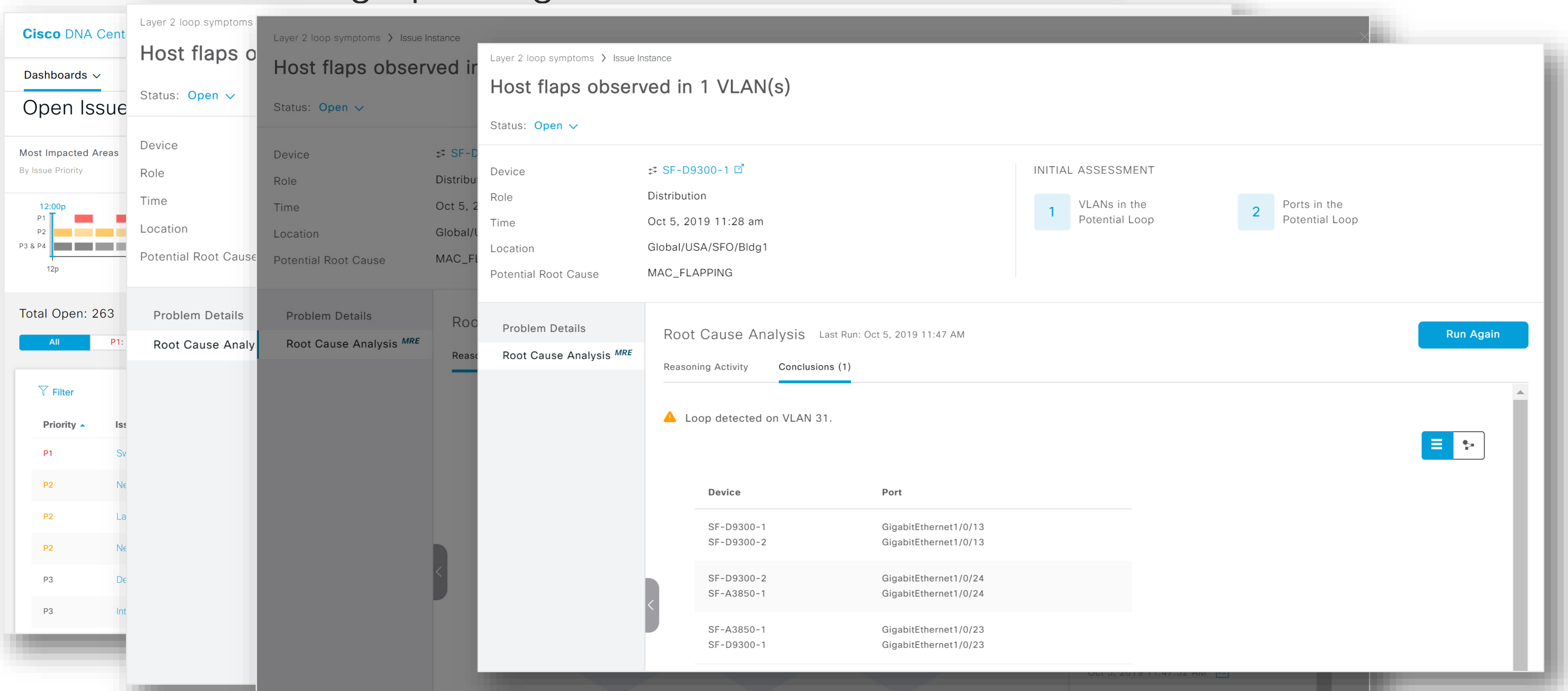
1 What are the top sites that need attention?

2 When did the problem happen?

3 How can I quickly get to the issue?

Use case 3: Network Infrastructure is Unreachable
How can I get visibility into issues impacting my Network?

Troubleshooting Spanning Tree



Layer 2 loop symptoms > Issue Instance

Host flaps observed in 1 VLAN(s)

Status: Open

Device	SF-D9300-1
Role	Distribution
Time	Oct 5, 2019 11:28 am
Location	Global/USA/SFO/Bldg1
Potential Root Cause	MAC_FLAPPING

INITIAL ASSESSMENT

1 VLANs in the Potential Loop

2 Ports in the Potential Loop

Problem Details

Root Cause Analysis MRE

Root Cause Analysis Last Run: Oct 5, 2019 11:47 AM

Run Again

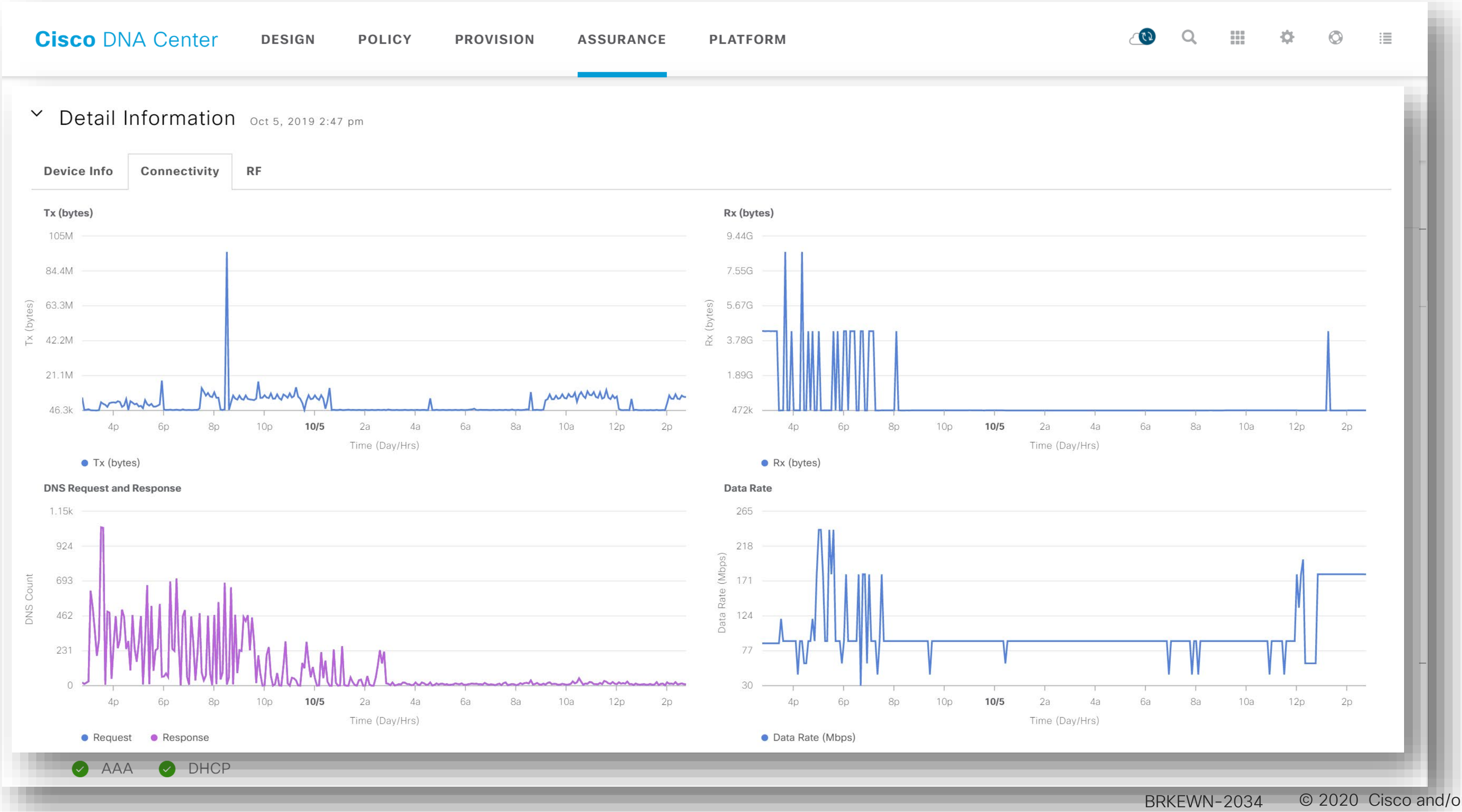
Reasoning Activity   Conclusions (1)

Loop detected on VLAN 31.

Device	Port
SF-D9300-1 SF-D9300-2	GigabitEthernet1/0/13 GigabitEthernet1/0/13
SF-D9300-2 SF-A3850-1	GigabitEthernet1/0/24 GigabitEthernet1/0/24
SF-A3850-1 SF-D9300-1	GigabitEthernet1/0/23 GigabitEthernet1/0/23

Use case 4: Clients failing to onboard to Wi-Fi Network How can I troubleshoot a client problem quickly?

Client 360 for contextual troubleshooting of client problems



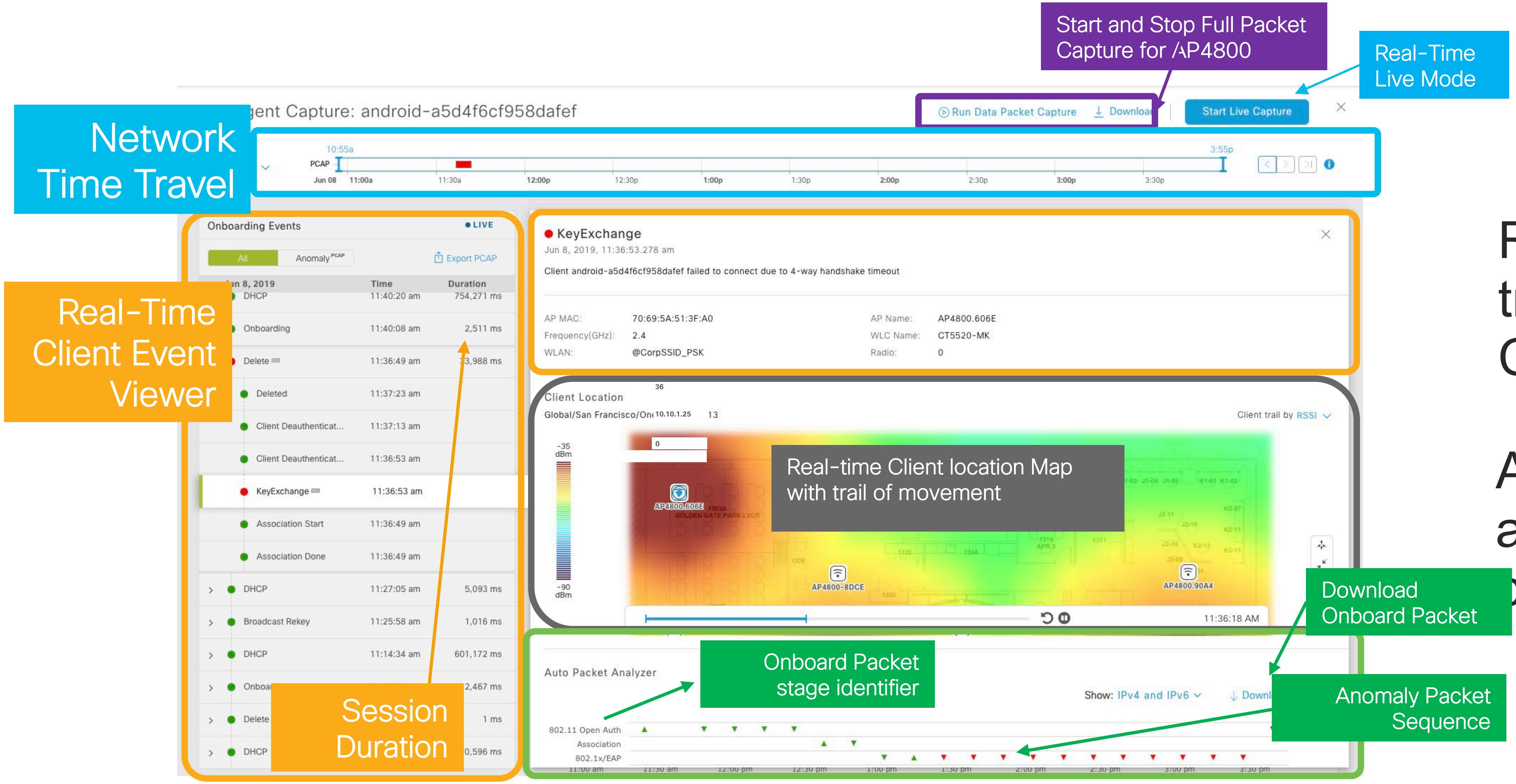
Event Viewer for Onboarding and Roaming Troubleshooting

Network time travel for troubleshooting issues in the past

Detailed Trending of Connectivity and KPIs

Use case 4: Clients failing to onboard to Wi-Fi Network How can I troubleshoot a client problem quickly?

Advanced Troubleshooting with Intelligent Capture



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

Download Onboard Packet

Onboard Packet stage identifier

Anomaly Packet Sequence

gent Capture: android-a5d4f6cf958dafef

Run Data Packet Capture | Download | Start Live Capture

Onboarding Events ● LIVE

All | Anomaly PCAP | Export PCAP

un 8, 2019	Time	Duration
DHCP	11:40:20 am	754,271 ms
Onboarding	11:40:08 am	2,511 ms
Delete	11:36:49 am	3,988 ms
Deleted	11:37:23 am	
Client Deauthenticat...	11:37:13 am	
Client Deauthenticat...	11:36:53 am	
KeyExchange	11:36:53 am	
Association Start	11:36:49 am	
Association Done	11:36:49 am	
DHCP	11:27:05 am	5,093 ms
Broadcast Rekey	11:25:58 am	1,016 ms
DHCP	11:14:34 am	601,172 ms
Onboa		2,467 ms
Delete		1 ms
DHCP		0,596 ms

● KeyExchange

Jun 8, 2019, 11:36:53.278 am

Client android-a5d4f6cf958dafef failed to connect due to 4-way handshake timeout

AP MAC:	70:69:5A:51:3F:A0	AP Name:	AP4800.606E
Frequency(GHz):	2.4	WLC Name:	CT5520-MK
WLAN:	@CorpSSID_PSK	Radio:	0

Client Location

Global/San Francisco/On 10.10.1.25

Client trail by RSSI

Auto Packet Analyzer

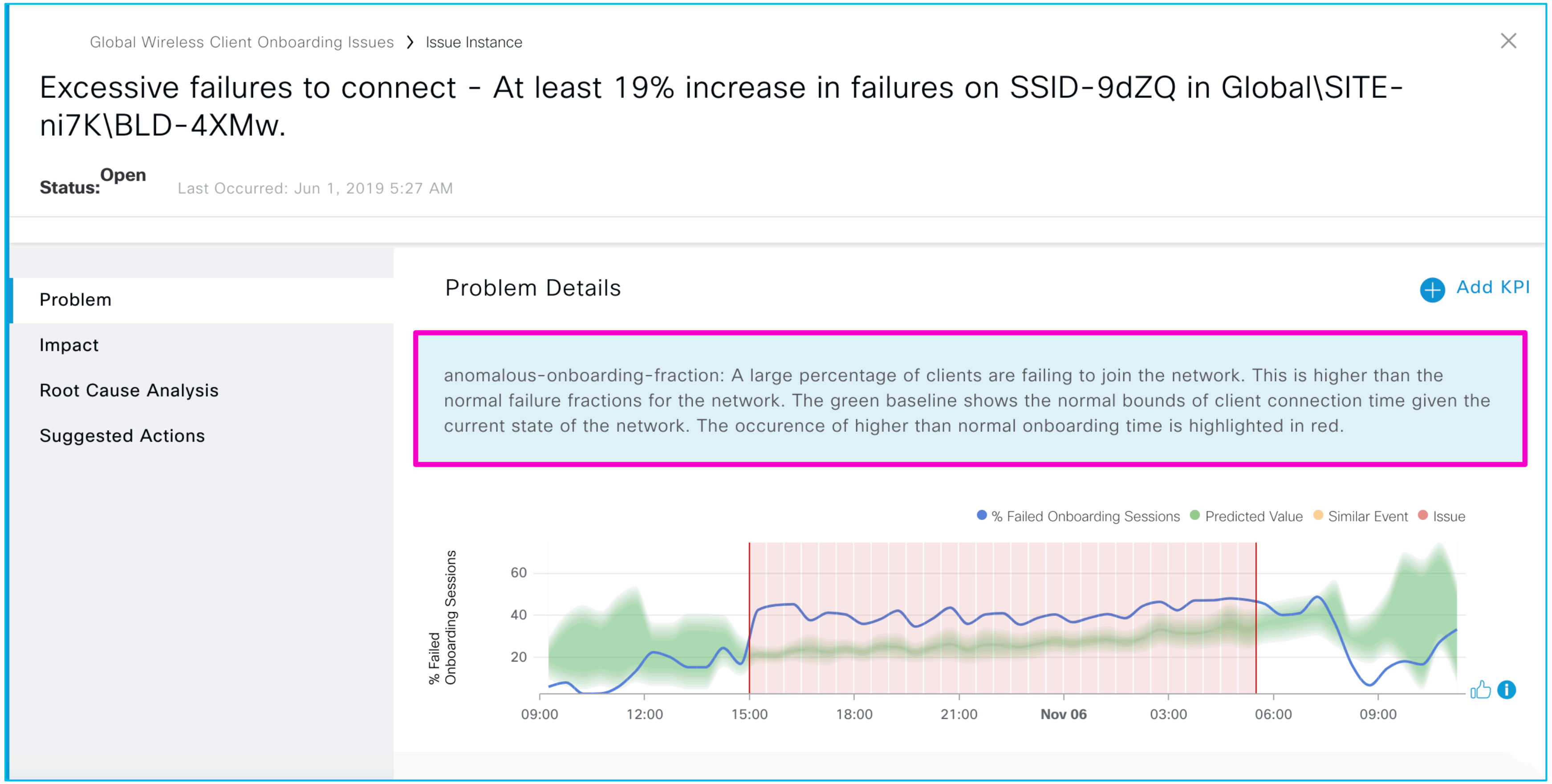
Show: IPv4 and IPv6 | Downl

Realtime troubleshooting of Client

Automated anomaly packet capture

Use case 5: Identify locations with slow Wi-Fi
How can I spot connectivity issues due to coverage hole?

AI-Driven Client Issues call out deviations from normal along with probable cause



Global Wireless Client Onboarding Issues › Issue Instance

Excessive failures to connect - At least 19% increase in failures on SSID-9dZQ in Global\SITE-ni7K\BLD-4XMw.

Status: **Open** Last Occurred: Jun 1, 2019 5:27 AM

Problem Details

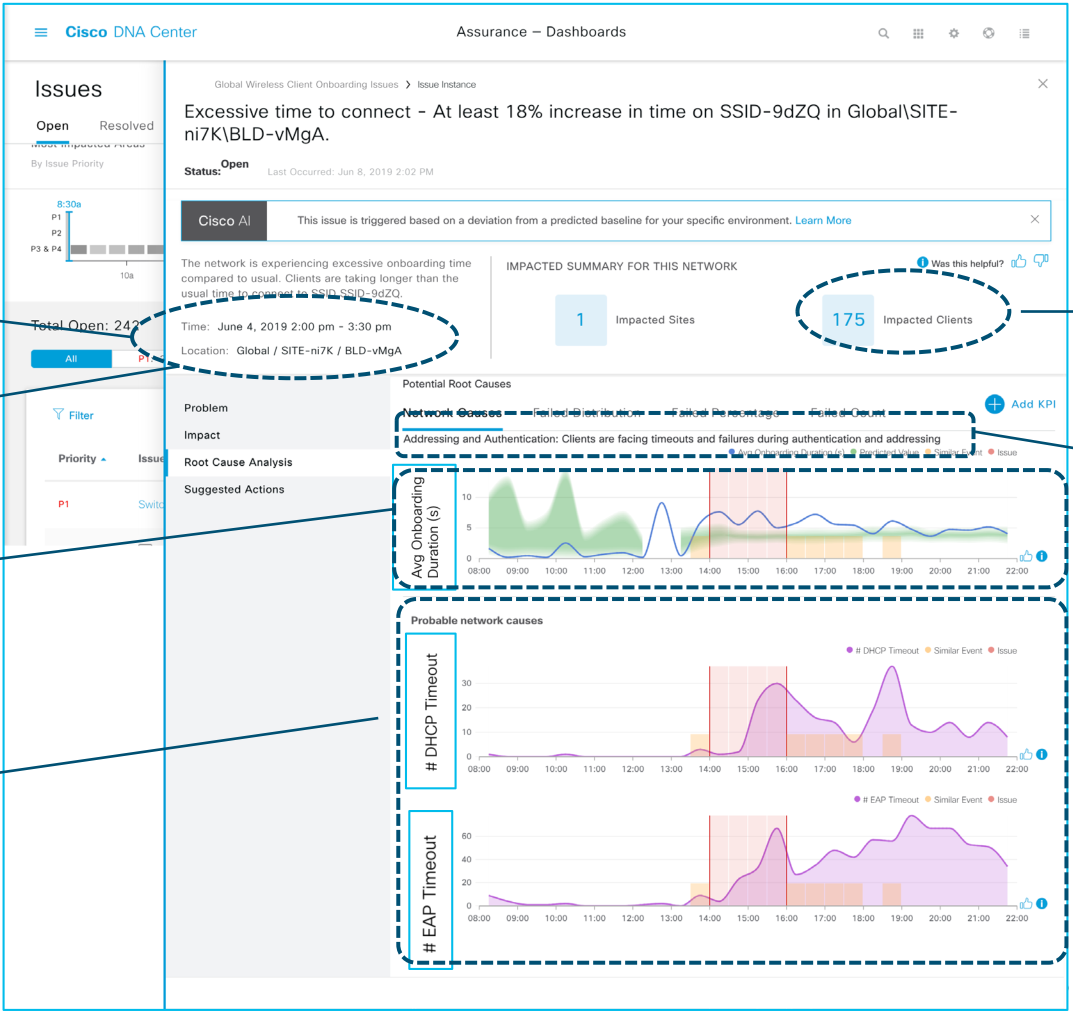
anomalous-onboarding-fraction: A large percentage of clients are failing to join the network. This is higher than the normal failure fractions for the network. The green baseline shows the normal bounds of client connection time given the current state of the network. The occurence of higher than normal onboarding time is highlighted in red.

Machine learning algorithms catch deviations from normal behavior of network

Probable Causes help narrow down the problem

Use case 5: Identify locations with slow Wi-Fi
How can I spot connectivity issues?

Root Cause Analysis
Who / What / When / Where / Why / How



Cisco DNA Center — Assurance – Dashboards

Issues

Open — Resolved

Global Wireless Client Onboarding Issues › Issue Instance

Excessive time to connect - At least 18% increase in time on SSID-9dZQ in Global\SITE-ni7K\BLD-vMgA.

Status: Open — Last Occurred: Jun 8, 2019 2:02 PM

Cisco AI — This issue is triggered based on a deviation from a predicted baseline for your specific environment. Learn More

The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to SSID SSID-9dZQ.

Time: June 4, 2019 2:00 pm - 3:30 pm

Location: Global / SITE-ni7K / BLD-vMgA

IMPACTED SUMMARY FOR THIS NETWORK

Was this helpful?

1 Impacted Sites

175 Impacted Clients

Potential Root Causes

Network Causes — Failed Distribution — Failed Percentage — Failed Count

Addressing and Authentication: Clients are facing timeouts and failures during authentication and addressing

Probable network causes

3 When

4 Where

6 How

5 Why

1 Who

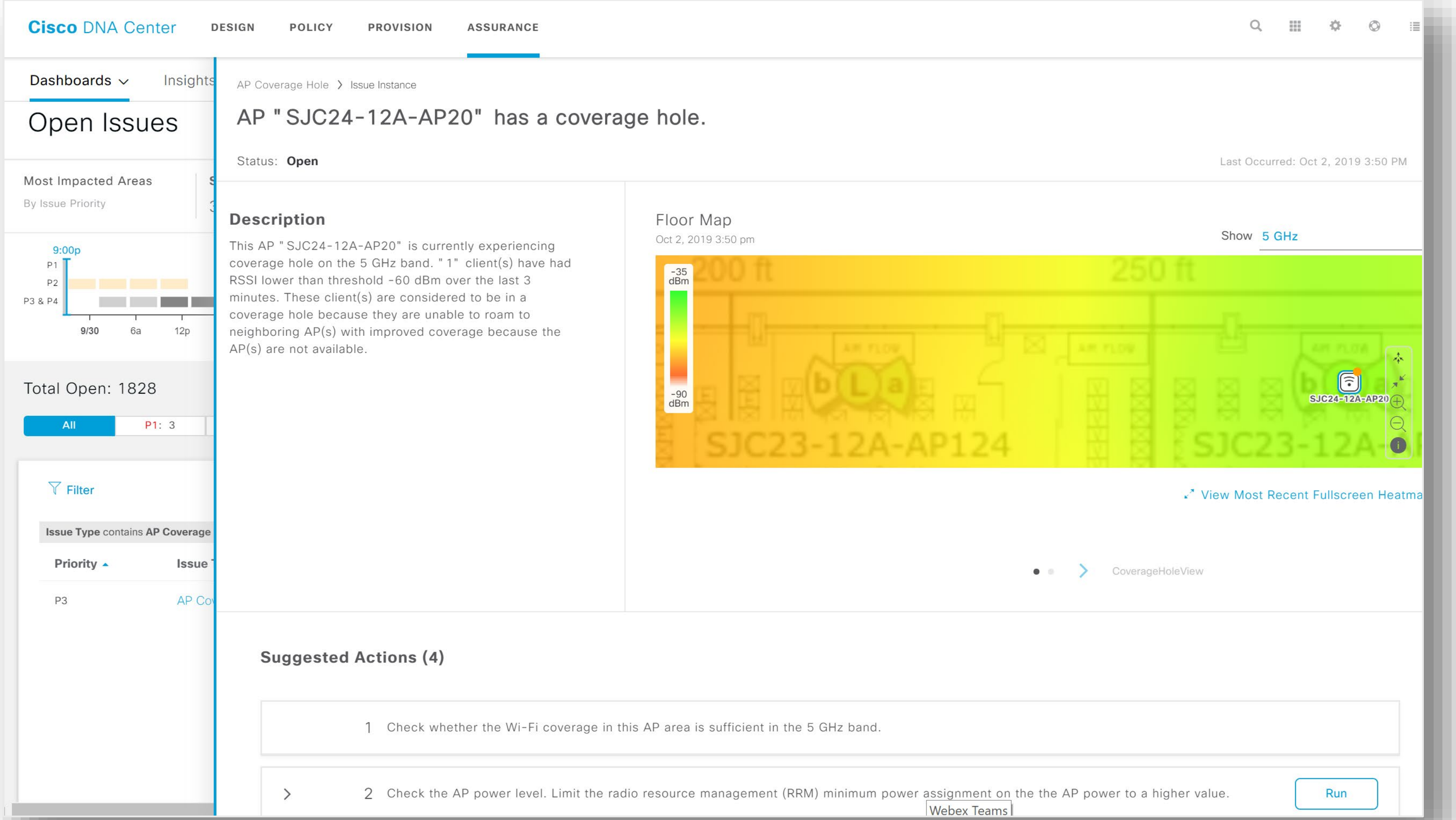
2 What

"Clients are facing timeouts and failures during authentication and addressing"

cisco Live!

Use case 5: Identify locations with poor RF coverage How can I spot connectivity issues due to coverage hole?

Coverage Hole Problems



AP " SJC24-12A-AP20" has a coverage hole.

Status: Open

Last Occurred: Oct 2, 2019 3:50 PM

Description

This AP " SJC24-12A-AP20" is currently experiencing coverage hole on the 5 GHz band. " 1" client(s) have had RSSI lower than threshold -60 dBm over the last 3 minutes. These client(s) are considered to be in a coverage hole because they are unable to roam to neighboring AP(s) with improved coverage because the AP(s) are not available.

Floor Map

Oct 2, 2019 3:50 pm

Show 5 GHz

Suggested Actions (4)

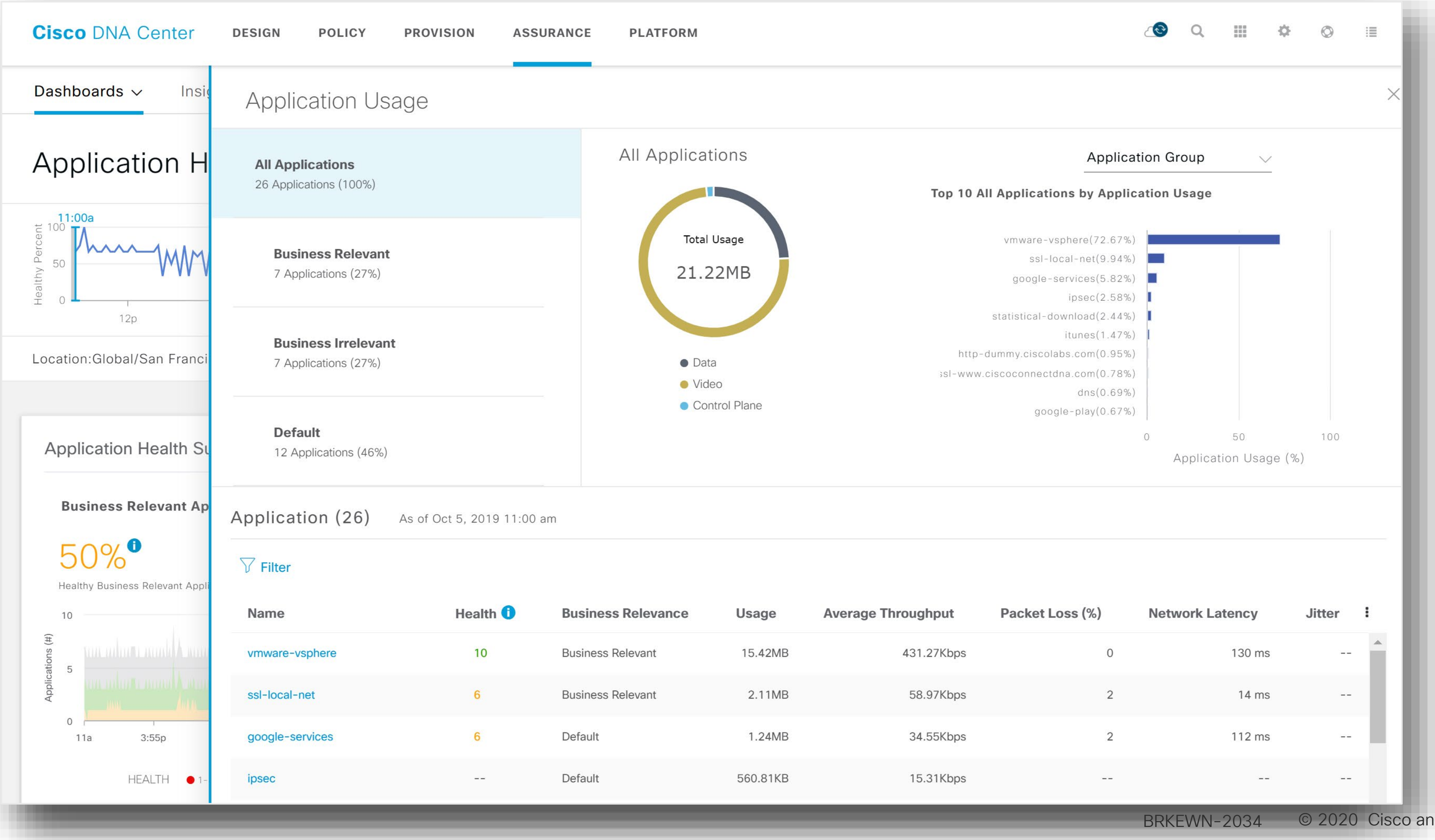
1 Check whether the Wi-Fi coverage in this AP area is sufficient in the 5 GHz band.

2 Check the AP power level. Limit the radio resource management (RRM) minimum power assignment on the the AP power to a higher value. Run

Get visibility of coverage holes in your floor based on real client data

Use case 6: Application Visibility
What applications are flowing through in my Network?

Application Health Dashboard for monitoring Top Applications by Usage



Application Usage

All Applications
26 Applications (100%)

Business Relevant
7 Applications (27%)

Business Irrelevant
7 Applications (27%)

Default
12 Applications (46%)

All Applications

Top 10 All Applications by Application Usage

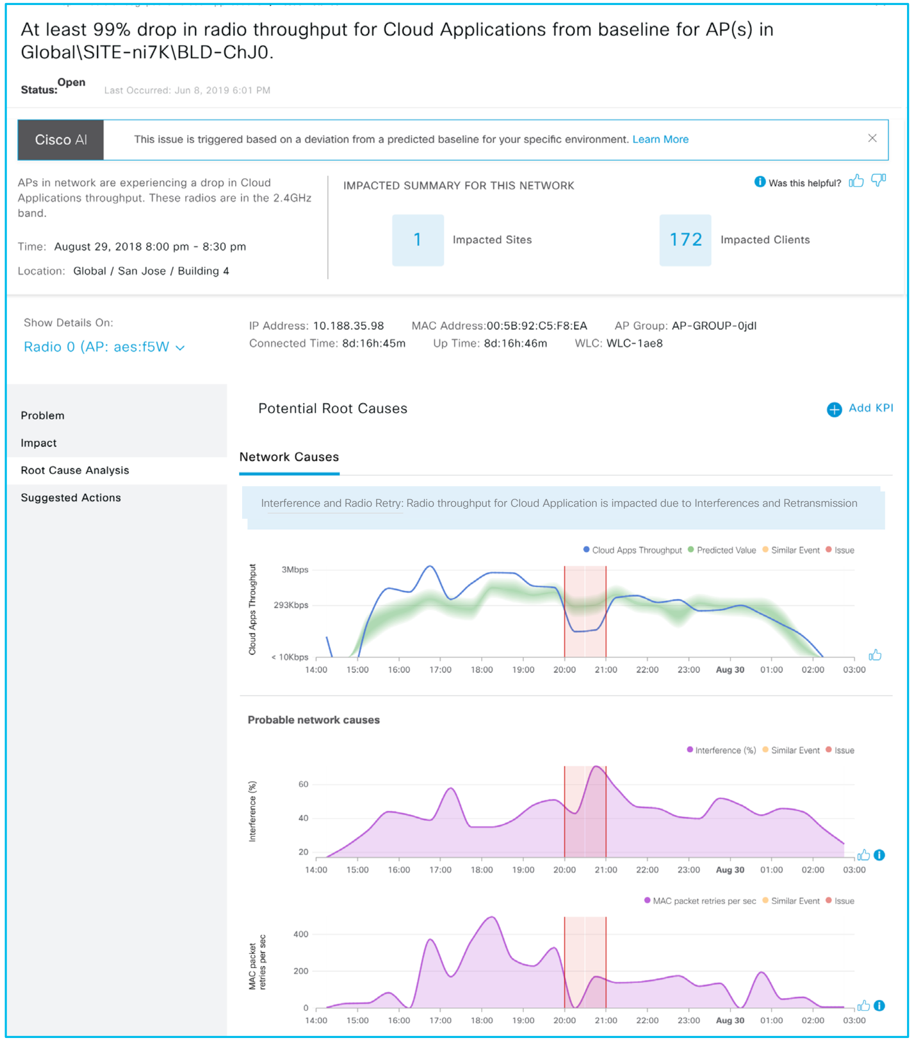
Application (26) As of Oct 5, 2019 11:00 am

Name	Health	Business Relevance	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter
vmware-vsphere	10	Business Relevant	15.42MB	431.27Kbps	0	130 ms	--
ssl-local-net	6	Business Relevant	2.11MB	58.97Kbps	2	14 ms	--
google-services	6	Default	1.24MB	34.55Kbps	2	112 ms	--
ipsec	--	Default	560.81KB	15.31Kbps	--	--	--

Application Distribution by Group or Traffic Class

What are the Top Application Traffic seen in my Network?

Use case 7: Clients having poor Application experience How can I troubleshoot an application problem quickly?



At least 99% drop in radio throughput for Cloud Applications from baseline for AP(s) in Global\SITE-ni7K\BLD-ChJ0.

Status: **Open** Last Occurred: Jun 8, 2019 6:01 PM

Cisco AI — This issue is triggered based on a deviation from a predicted baseline for your specific environment. Learn More

APs in network are experiencing a drop in Cloud Applications throughput. These radios are in the 2.4GHz band.

Time: August 29, 2018 8:00 pm - 8:30 pm

Location: Global / San Jose / Building 4

IMPACTED SUMMARY FOR THIS NETWORK — Was this helpful?

1 Impacted Sites

172 Impacted Clients

Show Details On: Radio 0 (AP: aes:f5W

IP Address: 10.188.35.98 MAC Address:00:5B:92:C5:F8:EA AP Group: AP-GROUP-0jdl
Connected Time: 8d:16h:45m Up Time: 8d:16h:46m WLC: WLC-1ae8

Problem
Impact
Root Cause Analysis
Suggested Actions

Potential Root Causes — Add KPI

Network Causes

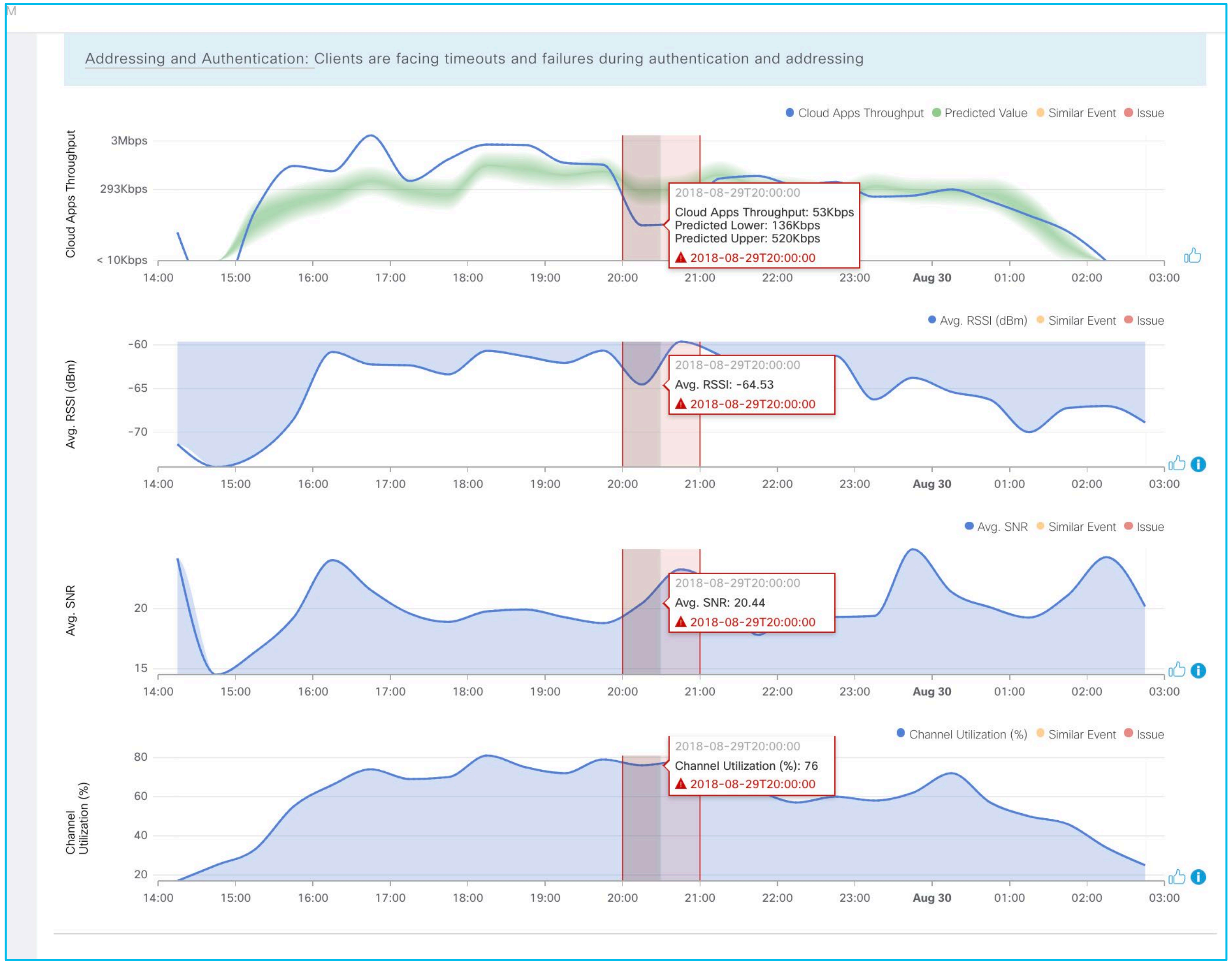
Interference and Radio Retry: Radio throughput for Cloud Application is impacted due to Interferences and Retransmission

● Cloud Apps Throughput ● Predicted Value ● Similar Event ● Issue
Cloud Apps Throughput
3Mbps
293Kbps
< 10Kbps
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

Probable network causes

● Interference (%) ● Similar Event ● Issue
Interference (%)
60
40
20
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00
● MAC packet retries per sec ● Similar Event ● Issue
MAC packet retries per sec
400
200
0
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

Add More KPI



Addressing and Authentication: Clients are facing timeouts and failures during authentication and addressing

● Cloud Apps Throughput ● Predicted Value ● Similar Event ● Issue
Cloud Apps Throughput
3Mbps
293Kbps
< 10Kbps
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

2018-08-29T20:00:00
Cloud Apps Throughput: 53Kbps
Predicted Lower: 136Kbps
Predicted Upper: 520Kbps
2018-08-29T20:00:00

● Avg. RSSI (dBm) ● Similar Event ● Issue
Avg. RSSI (dBm)
-60
-65
-70
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

2018-08-29T20:00:00
Avg. RSSI: -64.53
2018-08-29T20:00:00

● Avg. SNR ● Similar Event ● Issue
Avg. SNR
20
15
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

2018-08-29T20:00:00
Avg. SNR: 20.44
2018-08-29T20:00:00

● Channel Utilization (%) ● Similar Event ● Issue
Channel Utilization (%)
80
60
40
20
14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Aug 30 01:00 02:00 03:00

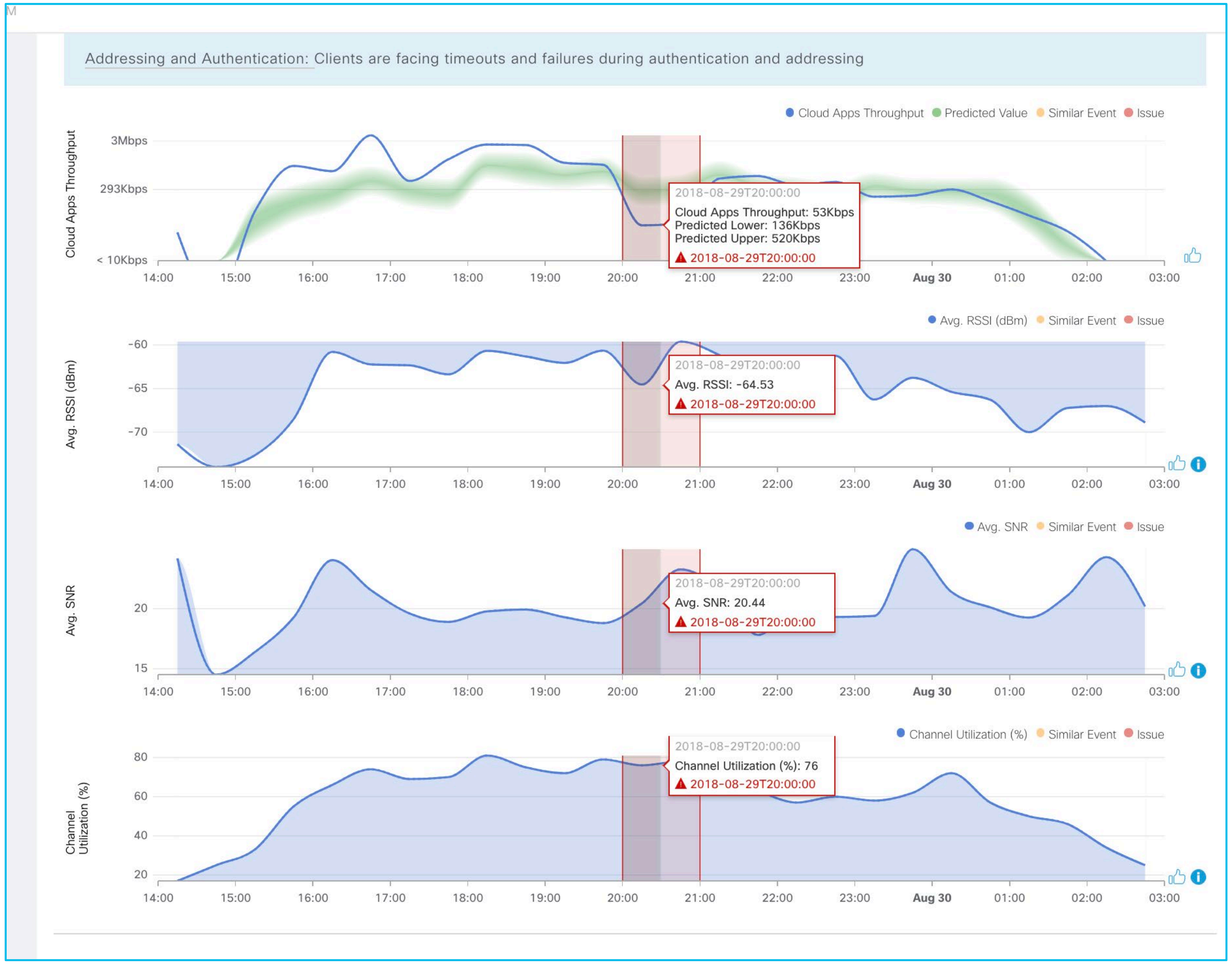
2018-08-29T20:00:00
Channel Utilization (%): 76
2018-08-29T20:00:00

Interference and Radio Retry is Probable Network cause

Use case 7: Clients having poor Application experience How can I troubleshoot an application problem quickly?

None of matrix are root cause of this issue because…

- RSSI is went down but still going strong (-60 ~ -70)
- SNR is Good (20 dB) means No strong noise source nearby
- High Utilization – consistently high



Addressing and Authentication: Clients are facing timeouts and failures during authentication and addressing

2018-08-29T20:00:00
Cloud Apps Throughput: 53Kbps
Predicted Lower: 136Kbps
Predicted Upper: 520Kbps
▲ 2018-08-29T20:00:00

2018-08-29T20:00:00
Avg. RSSI: -64.53
▲ 2018-08-29T20:00:00

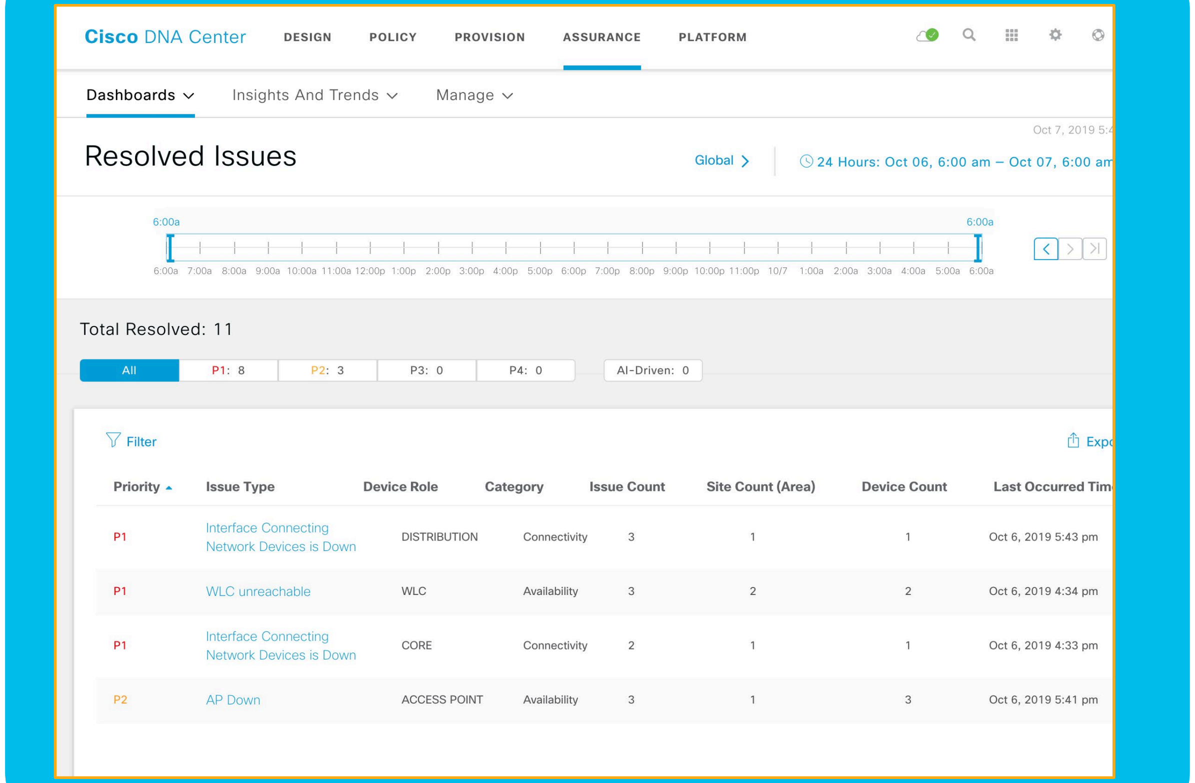
2018-08-29T20:00:00
Avg. SNR: 20.44
▲ 2018-08-29T20:00:00

2018-08-29T20:00:00
Channel Utilization (%): 76
▲ 2018-08-29T20:00:00

● Cloud Apps Throughput ● Predicted Value ● Similar Event ● Issue
Cloud Apps Throughput
3Mbps
293Kbps
< 10Kbps
● Avg. RSSI (dBm) ● Similar Event ● Issue
Avg. RSSI (dBm)
-60
-65
-70
● Avg. SNR ● Similar Event ● Issue
Avg. SNR
20
15
● Channel Utilization (%) ● Similar Event ● Issue
Channel Utilization (%)
80
60
40
20
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
Aug 30
01:00
02:00
03:00

New

Use case 8: Issue Lifecycle Management
How do I manage issues with ticket management solutions?


Cisco DNA Center
DESIGN
POLICY
PROVISION
ASSURANCE
PLATFORM
Dashboards
Insights And Trends
Manage
Oct 7, 2019 5:4
Global
6:00a
6:00a
6:00a 7:00a 8:00a 9:00a 10:00a 11:00a 12:00p 1:00p 2:00p 3:00p 4:00p 5:00p 6:00p 7:00p 8:00p 9:00p 10:00p 11:00p 10/7 1:00a 2:00a 3:00a 4:00a 5:00a 6:00a
Filter
Expo

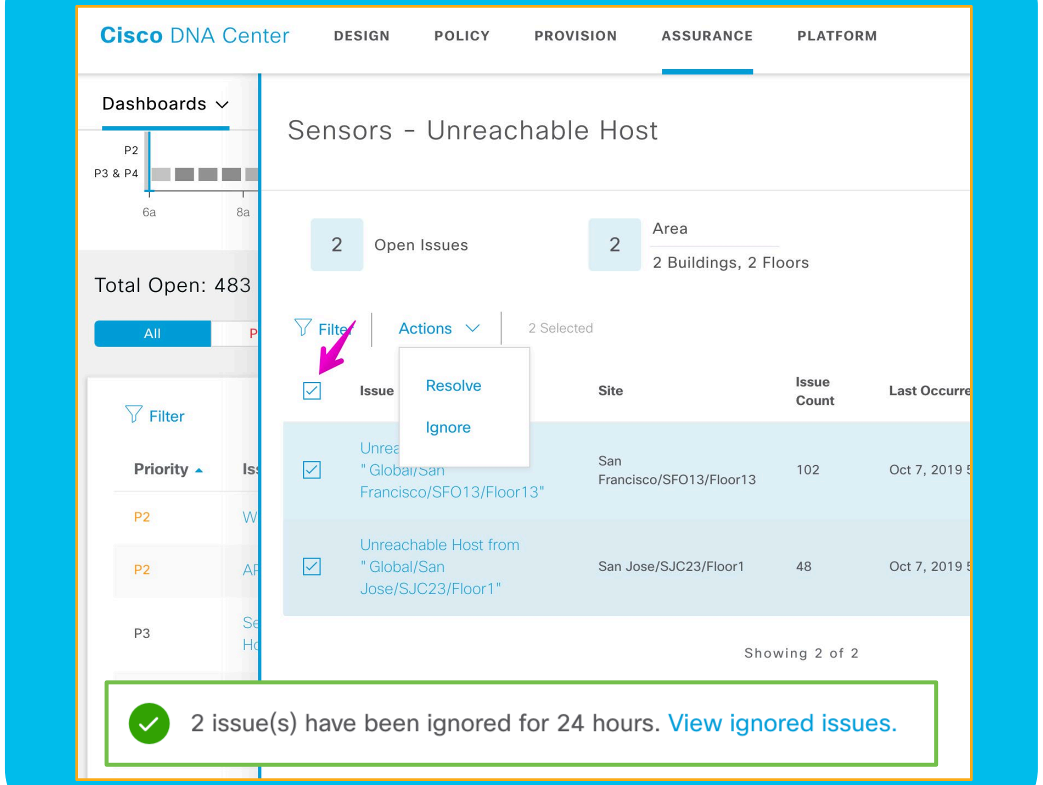
Resolved Issues

24 Hours: Oct 06, 6:00 am – Oct 07, 6:00 am

Total Resolved: 11

All | P1: 8 | P2: 3 | P3: 0 | P4: 0 | AI-Driven: 0

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Tim
P1	Interface Connecting Network Devices is Down	DISTRIBUTION	Connectivity	3	1	1	Oct 6, 2019 5:43 pm
P1	WLC unreachable	WLC	Availability	3	2	2	Oct 6, 2019 4:34 pm
P1	Interface Connecting Network Devices is Down	CORE	Connectivity	2	1	1	Oct 6, 2019 4:33 pm
P2	AP Down	ACCESS POINT	Availability	3	1	3	Oct 6, 2019 5:41 pm



Sensors - Unreachable Host

2 Open Issues

2 Area
2 Buildings, 2 Floors

Total Open: 483

☑	Issue	Site	Issue Count	Last Occurre
☑	Unrea " Global/San Francisco/SFO13/Floor13"	San Francisco/SFO13/Floor13	102	Oct 7, 2019 5
☑	Unreachable Host from " Global/San Jose/SJC23/Floor1"	San Jose/SJC23/Floor1	48	Oct 7, 2019 5

Showing 2 of 2

2 issue(s) have been ignored for 24 hours. View ignored issues.

Auto Resolve Issue

Device Reachability and Link Availability issues

Bulk Resolve/Ignore Issue

New Innovations in Cisco DNA Center Assurance

Solving the Most common Wireless problems through AI/ML - Focus on Client Experience

Wireless Onboarding

Wireless User Failed to Connect
Wireless User took too long to Connect

Excessive Time	Excessive Failures	Excessive DHCP Time
Excessive DHCP Failures	Excessive AAA Time	Excessive AAA Failures
Excessive Assoc. Time	Excessive Assoc. Failures	

Application Experience

Wireless User's Application throughput is declining

Total Radio	Media Application Throughput
Cloud Application	Social Application Throughput

Analytics and Outlier Detection on

- Wi-Fi Onboarding Analytics
- Wi-Fi Radio Performance Analytics
- App Perf. Analytics on Wi-Fi network

New

Active Sensor with Enterprise-Ready Features

- Dedicate Backhaul support
- Enhanced DNAC Discovery
- SCEP support
- Web-Auth support – ISE
- Sensor 360
- Sensor-Test Template – Location-based
- Sensor Dashboard – Top location-based Sensor test Heatmap
- Location-based Drill Down
- iPerf3 Test

New

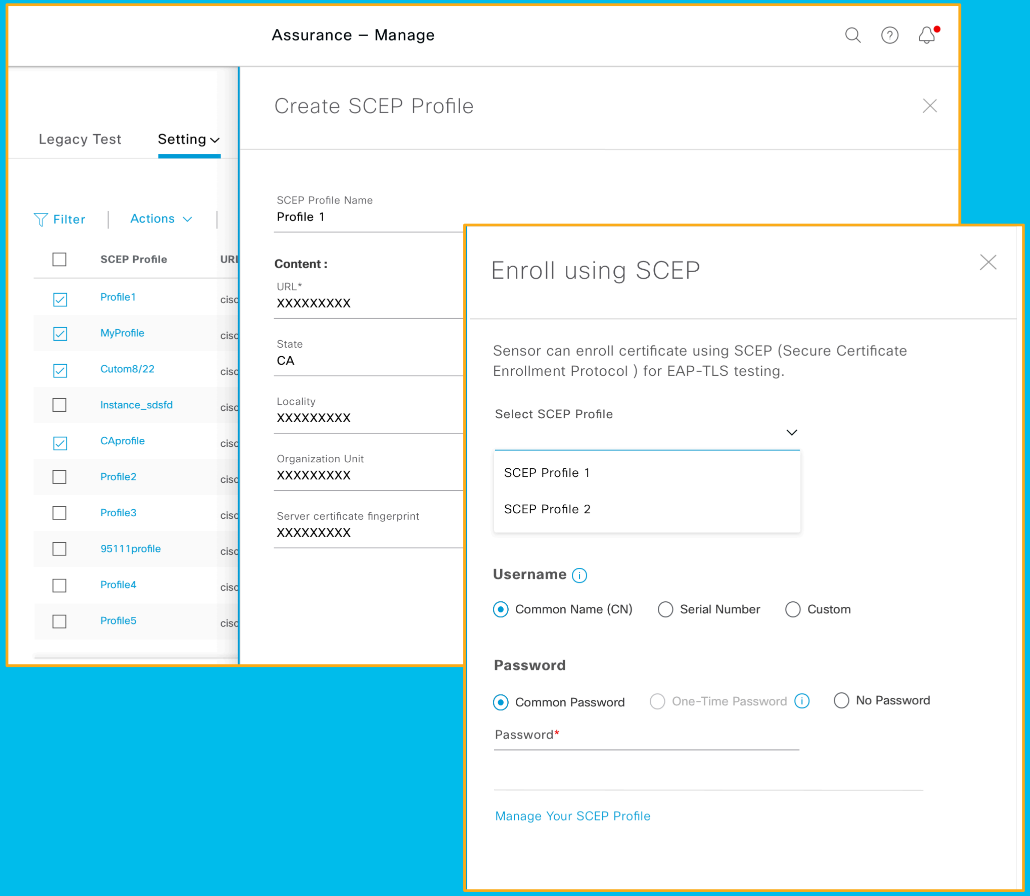
Day-0 Experience: Sensor Provisioning and Wireless Backhaul Enhancement

- Offering Day-0 SSH, allow Admin to remotely connect to Sensor and manual provision DNAC via SSH
- Use *CiscoSensorProvisioning* SSID as both Wireless Provisioning as well as Wireless backhaul purpose
- Provide Default, SensorProvisoning Backhaul Profile. Admin can skip creating separate Sensor profile.
- EAP-TLS support on Wireless Backhaul
- Extended Heartbeat Timeout (From 20min. → 8hrs since 8.8.263)
- Persistent Wireless Backhaul

New

Enterprise-Grade EAP-TLS Provisioning Solution SCEP (Secure Certificate Enrollment Protocol) Support

Assurance > Manage > Sensor > SCEP



Assurance – Manage

Legacy Test   Setting ⌄

Filter | Actions ⌄

☐	SCEP Profile	URI
☑	Profile1	cisc
☑	MyProfile	cisc
☑	Cutom8/22	cisc
☐	Instance_sdsfd	cisc
☑	CAprofile	cisc
☐	Profile2	cisc
☐	Profile3	cisc
☐	95111profile	cisc
☐	Profile4	cisc
☐	Profile5	cisc

Create SCEP Profile

SCEP Profile Name: Profile 1

Content :

URL*: XXXXXXXXX

State: CA

Locality: XXXXXXXXX

Organization Unit: XXXXXXXXX

Server certificate fingerprint: XXXXXXXXX

Enroll using SCEP

Sensor can enroll certificate using SCEP (Secure Certificate Enrollment Protocol) for EAP-TLS testing.

Select SCEP Profile ⌄

SCEP Profile 1

SCEP Profile 2

Username ⓘ

● Common Name (CN)   ○ Serial Number   ○ Custom

Password

● Common Password   ○ One-Time Password ⓘ   ○ No Password

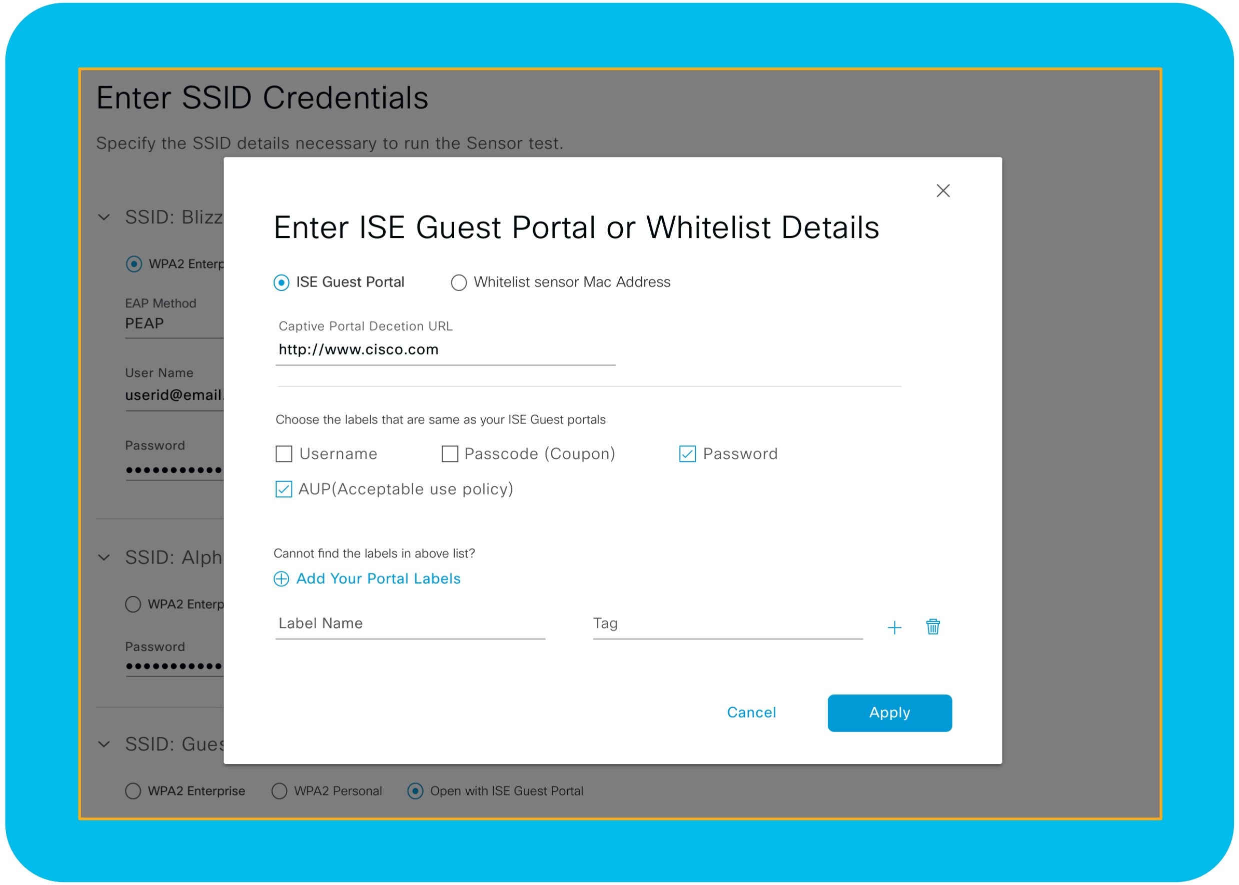
Password*

Manage Your SCEP Profile

- Secure Certificate Enrollment for EAP-TLS Test
- Admin can create and trigger SCEP processes through Sensor List page
- Support Microsoft and ISE SCEP Server
  - ISE SCEP uses IP-ACL for authentication
  - Microsoft SCEP server requires Username(CN) and SCEP Password to run SCEP
    - One Time Password, valid for 60min
    - Common Password
- Auto populate SAN Field using Sensor MAC Address

New

Guest Network Test
Sensor Extended Guest SSID Test to ISE



Enter SSID Credentials

Specify the SSID details necessary to run the Sensor test.

SSID: Blizz

● WPA2 Enterp

EAP Method
PEAP

User Name
userid@email

Password
•••••••••••

SSID: Alph

○ WPA2 Enterp

Password
•••••••••••

SSID: Gues

○ WPA2 Enterprise ○ WPA2 Personal ● Open with ISE Guest Portal

Enter ISE Guest Portal or Whitelist Details

● ISE Guest Portal ○ Whitelist sensor Mac Address

Captive Portal Decetion URL
http://www.cisco.com

Choose the labels that are same as your ISE Guest portals

□ Username □ Passcode (Coupon) ☑ Password

☑ AUP(Acceptable use policy)

Cannot find the labels in above list?

⊕ Add Your Portal Labels

Label Name Tag

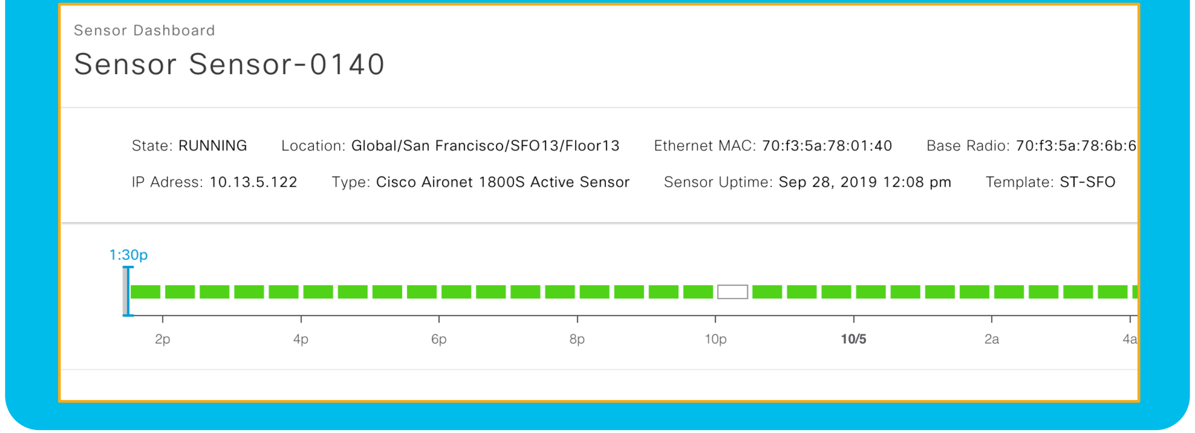
- ISE Guest Portal (CWA) Support
- ClearPass Captive Portal (under Cisco WLAN environment)
- Sensor will inspect the HTML elements on the Guest Portal:
    - Forms: Sensor looks for the action link for POST method
    - Controls: Sensor looks for the control names matching to the HTML tag names received from the DNAC
    - Sensor looks for the hidden token and Cookies to secure the time-bound temporary authentication access.

cisco Live!

New

Introducing Sensor 360

Network Time Travel



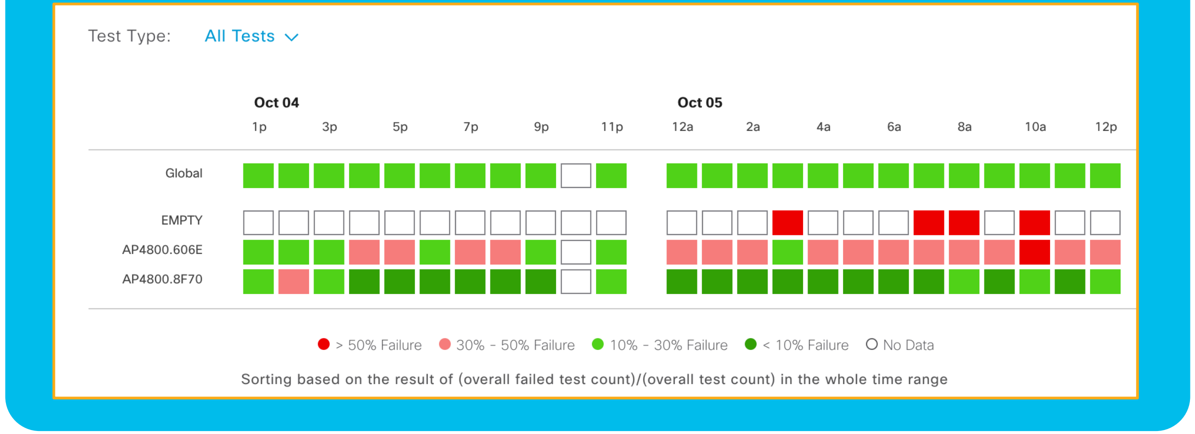
Sensor Dashboard

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



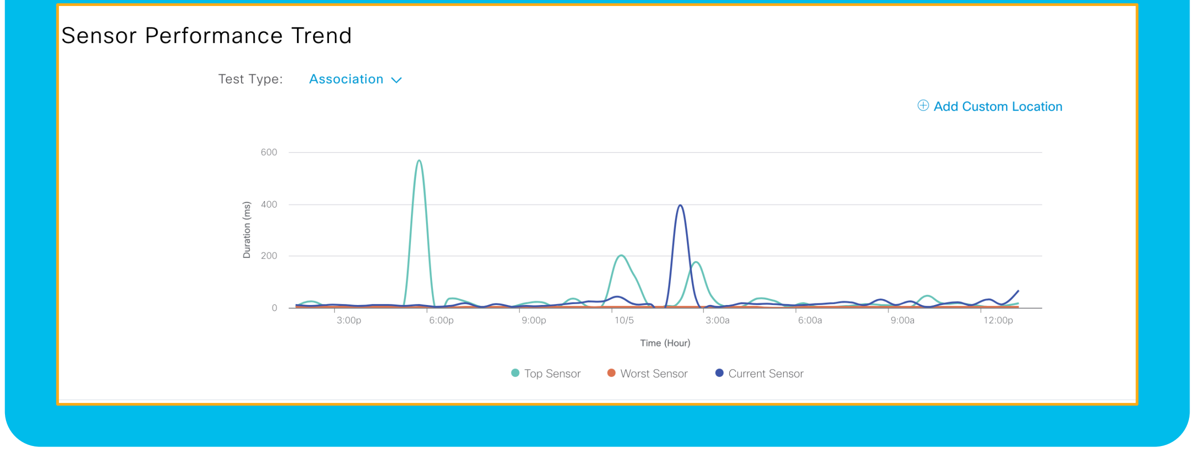
Test Type: All Tests ⌄

	Oct 04											Oct 05												
	1p		3p		5p		7p		9p		11p	12a		2a		4a		6a		8a		10a		12p
Global	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	□	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
EMPTY	□	□	□	□	□	□	□	□	□	□	□	□	□	□	🟥	□	□	□	🟥	🟥	□	🟥	□	□
AP4800.606E	🟩	🟩	🟩	▨	▨	🟩	▨	▨	🟩	□	🟩	▨	▨	▨	🟩	▨	▨	▨	▨	▨	▨	🟥	▨	▨
AP4800.8F70	🟩	▨	🟩	■	■	■	■	■	■	□	🟩	■	■	■	■	■	■	■	■	🟩	■	🟩	■	🟩

🟥 > 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

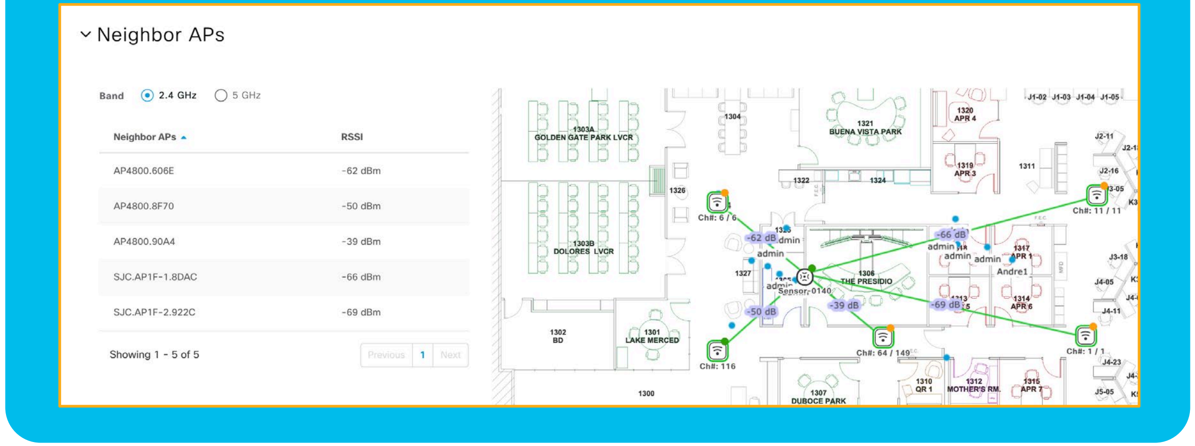
Performance Trend w/ comparison



Sensor Performance Trend

Test Type: Association ⌄

Visual Neighbor AP Map



⌄ Neighbor APs

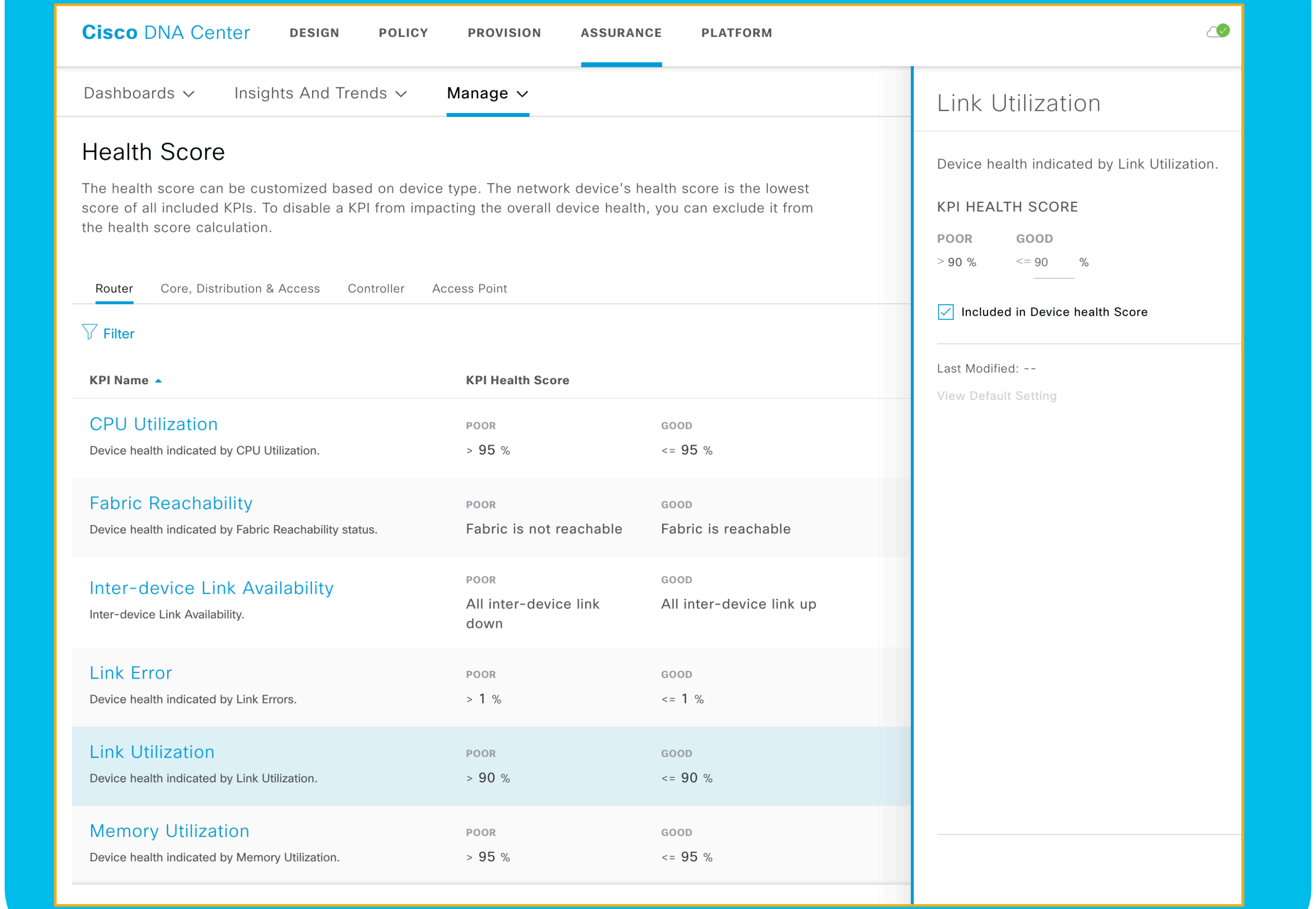
Band ◉ 2.4 GHz ○ 5 GHz

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

New

Health Score Customization



Health Score

The health score can be customized based on device type. The network device's health score is the lowest score of all included KPIs. To disable a KPI from impacting the overall device health, you can exclude it from the health score calculation.

Router | Core, Distribution & Access | Controller | Access Point

Filter

KPI Name	KPI Health Score	
	POOR	GOOD
CPU Utilization Device health indicated by CPU Utilization.	> 95 %	<= 95 %
Fabric Reachability Device health indicated by Fabric Reachability status.	Fabric is not reachable	Fabric is reachable
Inter-device Link Availability Inter-device Link Availability.	All inter-device link down	All inter-device link up
Link Error Device health indicated by Link Errors.	> 1 %	<= 1 %
Link Utilization Device health indicated by Link Utilization.	> 90 %	<= 90 %
Memory Utilization Device health indicated by Memory Utilization.	> 95 %	<= 95 %

Link Utilization

Device health indicated by Link Utilization.

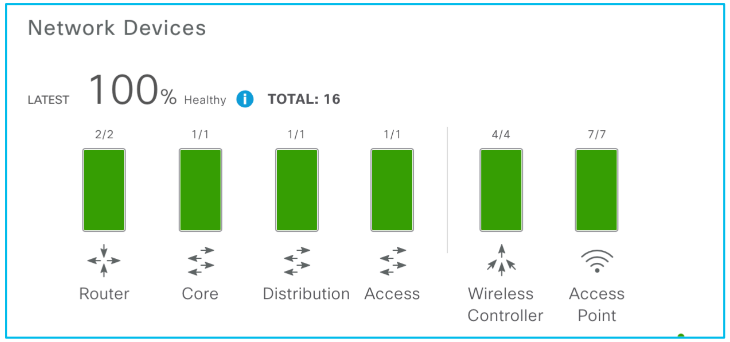
KPI HEALTH SCORE

POOR	GOOD
> 90 %	<= 90 %

☑ Included in Device health Score

Last Modified: --

View Default Setting



- Customize Network Health Score calculation formula
- **Customize** what **KPI** will be included in the network health score calculation
- Customize **Threshold** value of each KPI

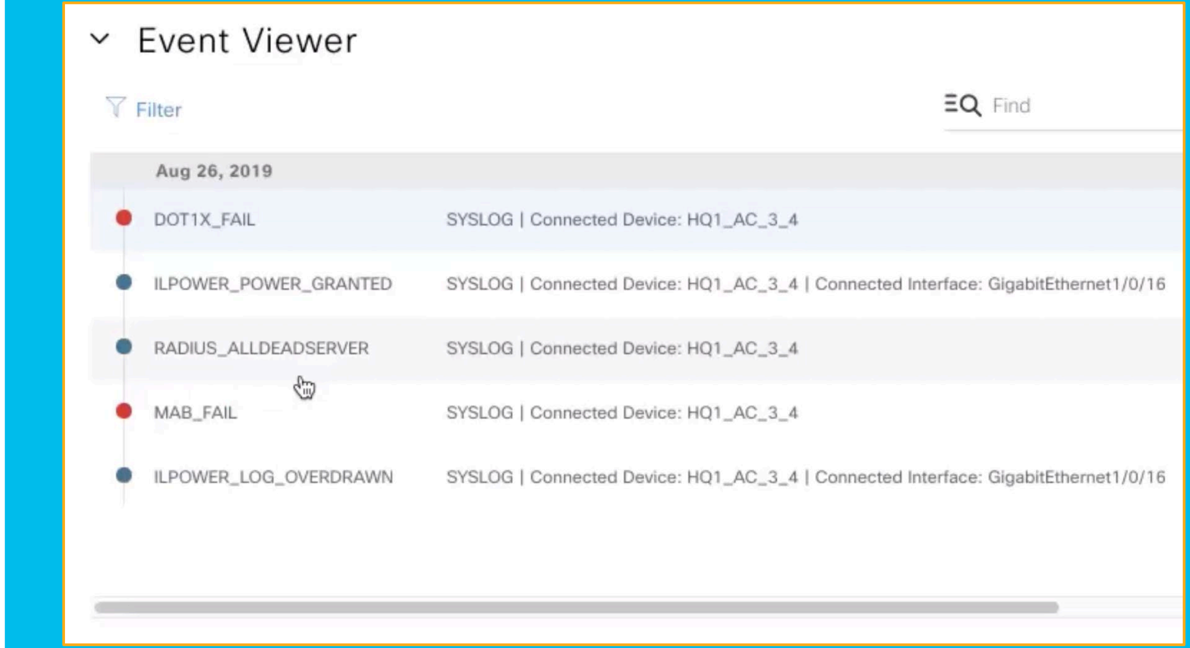
Fixed Formula

- Pick “Lowest” KPI among others

New

Event Viewer Enhancements

Wired Client Event Viewer



Event Viewer

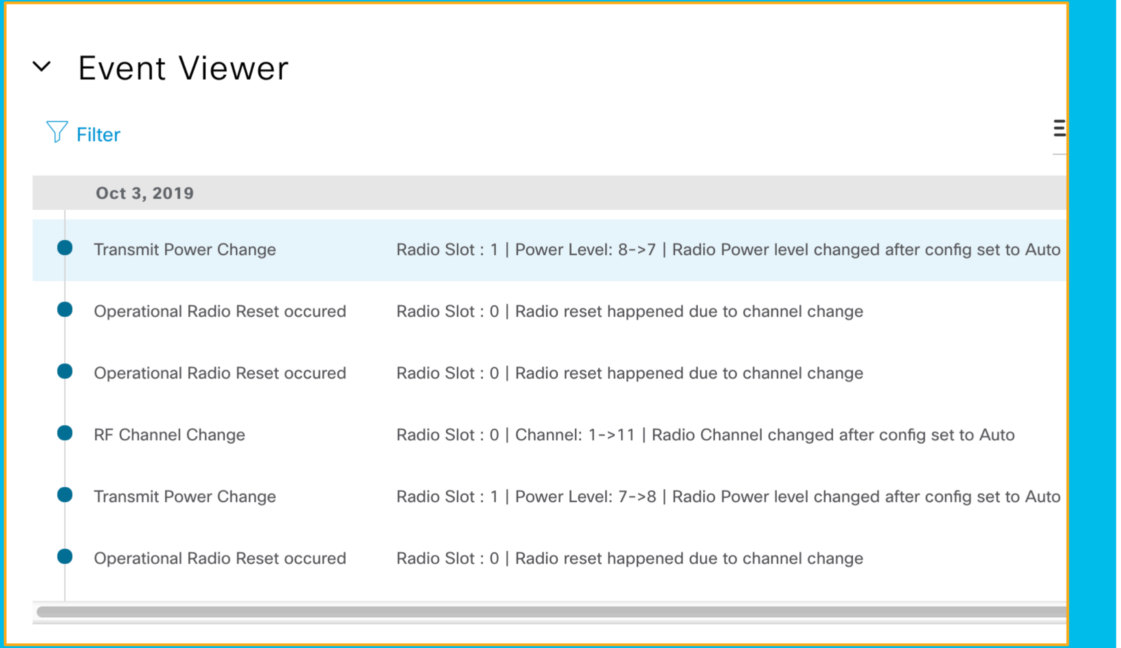
Filter

Find

Aug 26, 2019

●	DOT1X_FAIL	SYSLOG | Connected Device: HQ1_AC_3_4
●	ILPOWER_POWER_GRANTED	SYSLOG | Connected Device: HQ1_AC_3_4 | Connected Interface: GigabitEthernet1/0/16
●	RADIUS_ALLDEADSERVER	SYSLOG | Connected Device: HQ1_AC_3_4
●	MAB_FAIL	SYSLOG | Connected Device: HQ1_AC_3_4
●	ILPOWER_LOG_OVERDRAWN	SYSLOG | Connected Device: HQ1_AC_3_4 | Connected Interface: GigabitEthernet1/0/16

Enhanced AP Event Viewer



Event Viewer

Filter

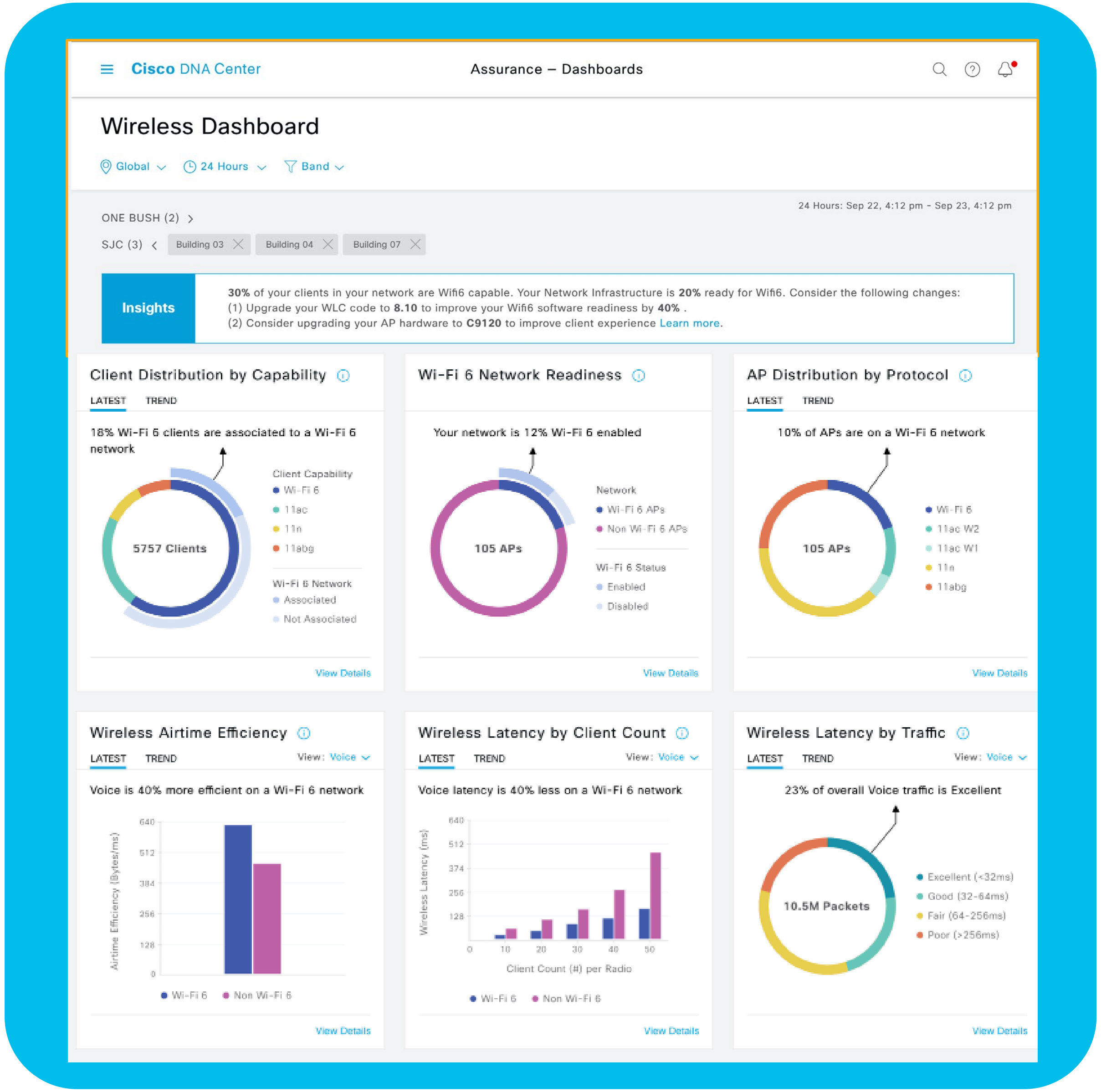
Oct 3, 2019

●	Transmit Power Change	Radio Slot : 1 | Power Level: 8->7 | Radio Power level changed after config set to Auto
●	Operational Radio Reset occured	Radio Slot : 0 | Radio reset happened due to channel change
●	Operational Radio Reset occured	Radio Slot : 0 | Radio reset happened due to channel change
●	RF Channel Change	Radio Slot : 0 | Channel: 1->11 | Radio Channel changed after config set to Auto
●	Transmit Power Change	Radio Slot : 1 | Power Level: 7->8 | Radio Power level changed after config set to Auto
●	Operational Radio Reset occured	Radio Slot : 0 | Radio reset happened due to channel change

- Event Viewer support for wired clients
- Expose Onboard failure reason to title
- Event header to show Event Reason, Changed Status

New

Wi-Fi 6 Dashboard



Cisco DNA Center Assurance – Dashboards

Wireless Dashboard

Global 24 Hours Band

24 Hours: Sep 22, 4:12 pm - Sep 23, 4:12 pm

ONE BUSH (2)

SJC (3) Building 03 Building 04 Building 07

Insights

30% of your clients in your network are Wifi6 capable. Your Network Infrastructure is **20%** ready for Wifi6. Consider the following changes:
(1) Upgrade your WLC code to **8.10** to improve your Wifi6 software readiness by **40%** .
(2) Consider upgrading your AP hardware to **C9120** to improve client experience Learn more.

Client Distribution by Capability

18% Wi-Fi 6 clients are associated to a Wi-Fi 6 network

Wi-Fi 6 Network Readiness

Your network is 12% Wi-Fi 6 enabled

AP Distribution by Protocol

10% of APs are on a Wi-Fi 6 network

Wireless Airtime Efficiency

Voice is 40% more efficient on a Wi-Fi 6 network

Wireless Latency by Client Count

Voice latency is 40% less on a Wi-Fi 6 network

Wireless Latency by Traffic

23% of overall Voice traffic is Excellent

- Identify Wi-Fi 6 Readiness for Client and AP
- Assess and Compare Wi-Fi 6 vs. Non Wi-Fi 6 network
- Wireless Latency by Traffic and Client Count
- Analysis of Connection Speeds (MCS) distribution per client type
- Traffic Class analysis

New

Samsung Analytics

SAMSUNG

- In addition to iOS Analytics, DNA Center Assurance extend support of client perspective to Samsung, starting 802.11ax
- Target Device: Samsung S10, Note9/10
- Cisco Adaptive 802.11r support
- Client-Side Disassociation Reason Code
- Samsung Device AP Neighbor list support
- Client 360 Integration
- Client Event Viewer Integration

... More Enhancements on DNA Center Assurance

Nested Site support for CMX integration

Enhanced Intelligent Capture Manage

Failure reason description on iCap

Client Data Rate Widget

NetFlow Collector Performance Improvement

Client Wi-Fi Standard KPI

Client List Export on Widget View Detail Page

AppVisibility on WLC

AppVisibility on Switch

Time Travel on Issue Dashboard

Network Reachability Icon

Bulk Sensor Profile Assignment

Rogue management

New Issue Dashboard

Spill-over Columns in Network Device List

New DNA Center Home Page

Client issues Optimization

Most impacted Site by issues

Device Cross launch from Issue Detail page

Real Time Event Notification

More than 180 issues

Issue filtering by Category and Priority

Ability to run Sensor test against specific target AP

..and MORE !

Cisco DNA Assurance Deployment Best Practices

How do we get started?

Cisco DNA Assurance Deployment Considerations

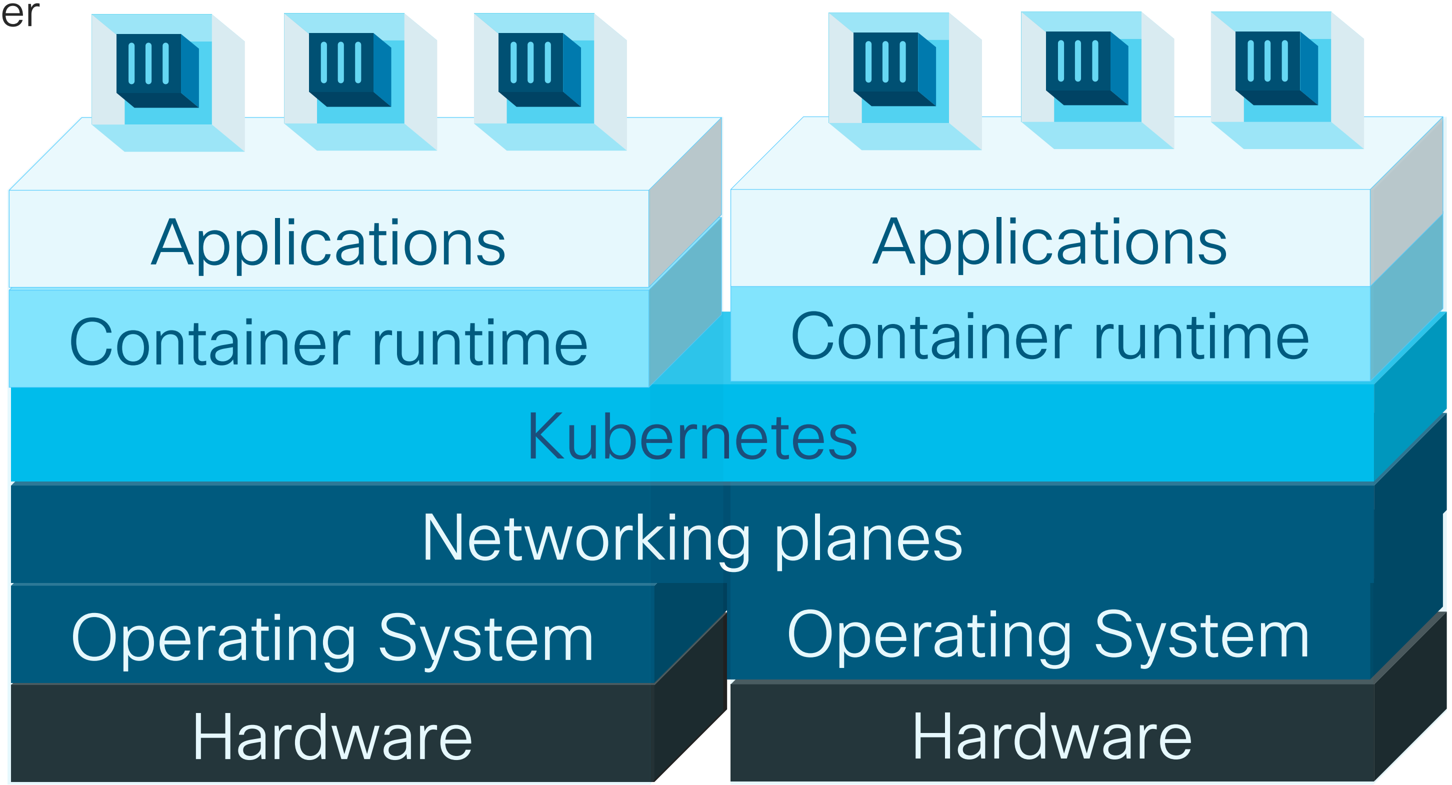
- Cisco DNA Center Under the Hood
  - How do you setup Cisco DNA Center? Caveats to keep mind and key ports to use
- Cisco DNA Assurance Deployment Best Practices
  - How do we check Streaming Telemetry on WLC is working?
  - How to turn on Application Experience on network devices(Router, Switch, WLC)?
  - What's the Bandwidth consumption on Cisco DNA Assurance?
  - How does Anomaly-Based Intelligent Capture works?
  - How to ensure Data Privacy of AI-Cloud?
  - How to start AI Network Analytics?

Cisco DNA Center
Under the hood

Cisco DNA Center Appliance

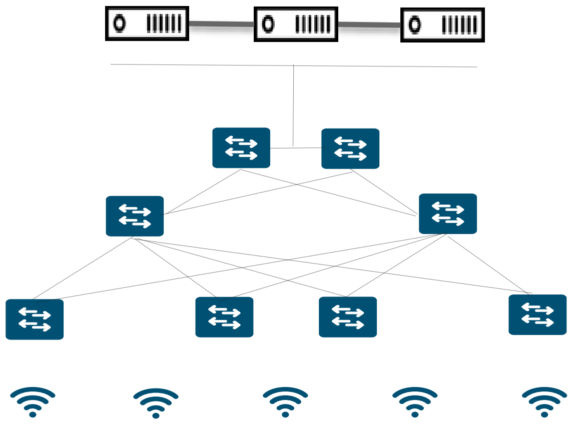
Overview of Infrastructure Software Stack of On-premise Deployments

- Form factor: Cisco UCS C-Series server
  - Multiple appliances are deployed as a cluster
- Containerized applications
- Microservices based platform
- Kubernetes for orchestration
- Platform provided services
  - Database, messaging, storage
- Applications expose REST API
-



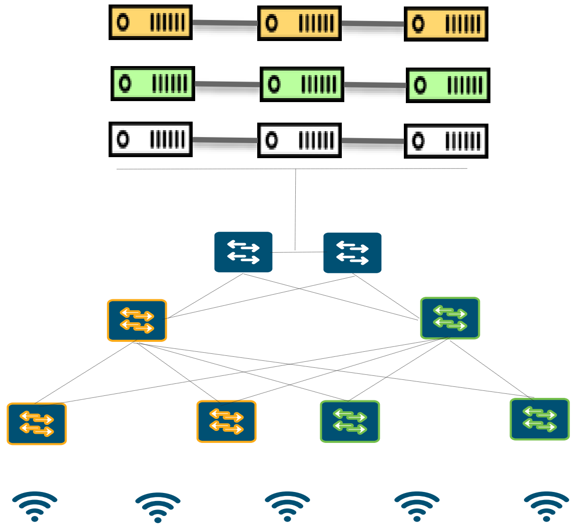
Multi Site Architecture

Same DC



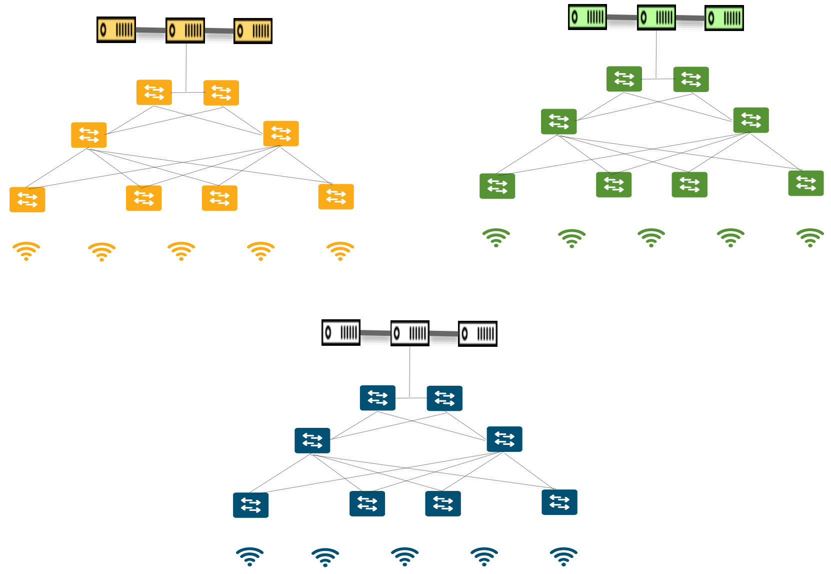
Centralized
One cluster for the entire network/admin domain

Same DC



Multiple cluster for a single network but different admin domains

Multiple DC



Region based admin domains/ Separate networks

Cisco DNA Center - Enterprise Scale readiness

Bigger Form Factor Appliances

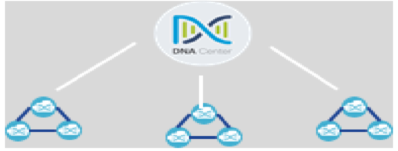
- DN2-HW-APL
- DN2-HW-Apl-L
- DN2-HW-APL-XL

- Available Now

Disaster Recovery

- **Disaster Recovery (DR)** for **3 node clusters across Data Centers**
- Witness support for split-brain scenarios
- Automatic Failover (Primary>Secondary)
- User initiated Failback (Secondary>Primary)
- **Available 1HCY20**

Cisco DNA Center Management System (DMS)



- **Simplified single pane of glass multi-cluster** management of distributed Cisco DNA Centers
- Centralized visibility and Monitoring of Network
- Search Support

- **Roadmapped for 2HCY20**

Cisco DNA Appliance – Scale and Hardware Spec

DN2-HW-APL

- ✓ 44 Core M5
- ✓ 5000 Network devices
- ✓ 1000 Switches and Routers
- ✓ 4000 APs
- ✓ 25000 endpoints (concurrent)

DN2-HW-APL-L

- ✓ 56 Core M5
- ✓ 8000 Network devices
- ✓ 6000 AP and 2000 Switches/Routers
- ✓ 40,000 end points (concurrent)

DN2 – HW-APL-XL

- ✓ 112 Core M5
- ✓ 18K devices
- ✓ 13K AP/5K switches and routers
- ✓ 100,000 end points (60K wireless/40K wired)

✓ Automation HA available with all models
Cluster members must be of the same appliance type

(stack is a single switch count)

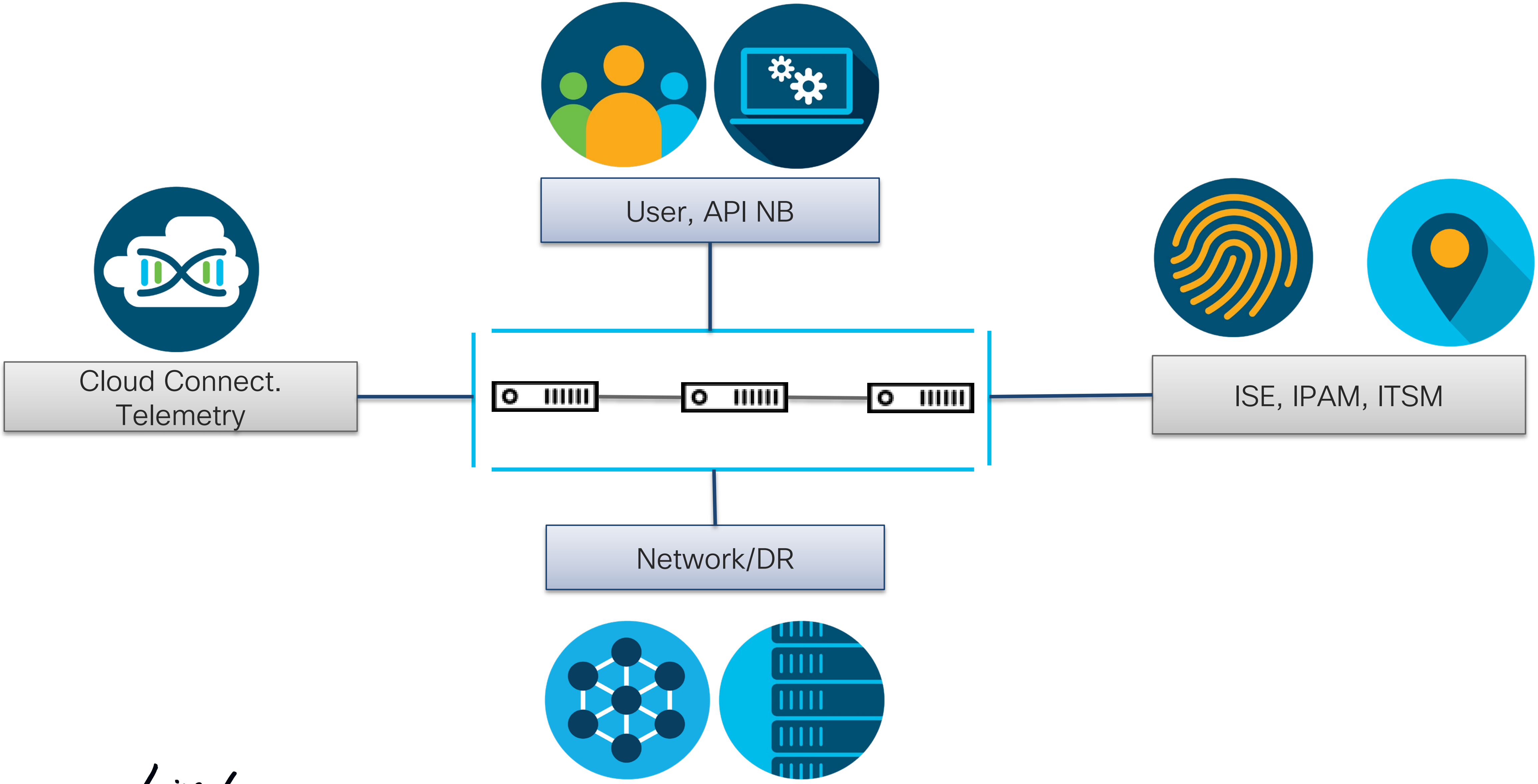
Cisco DNA Center System Scale Parameter – 1.3.x Release

Parameters	DN2-HW-APL	DN2-HW-APL-L	DN2-HW-APL-XL
No. of Endpoints (concurrent)	25K	40K	100K (40K Wired/60K Wireless)
No. of Devices (Switches/Routers/WLCs)	1000	2000	5000
Ports	48K	192K	480K
Total Interfaces (Physical and Logical)	1.2mil	1.2mil	1.2mil
No. of AP's	4000	6000	12000
No. of DNAC Sites	500	1000	2000
No. of Access Control Policies	25K	25K	25K
No. Access Contracts	500	500	500
Per Fabric Site Scale			
No. of Fabric Devices	500	600	1200
No. of VNs	64	64	256
No. of IP Pools	100	300	600

Latency from Cisco DNA Center to Devices: 200ms (RTT)

Setting Up Cisco DNA Center

Logical Connectivity

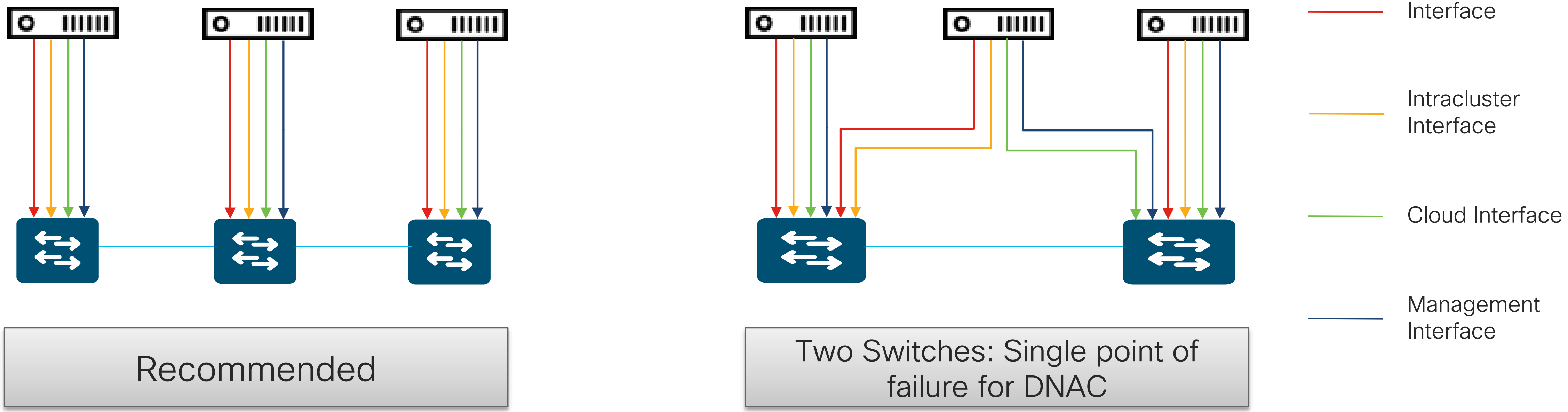


Cluster Installation Pre-requisite

- Plan the cluster design before installation
- Each network (e.g. Enterprise, cloud-connectivity, or management) requires
  - Individual node IP address
  - A virtual IP (external entities, e.g. devices or UI portal access the cluster by VIP)
- Isolated intra-cluster network
  - Nodes identify each other by intra-cluster link IP
  - A lot of state replication happens over the intra-cluster link (latency sensitive)
  - Loss of intra-cluster link leads to node’s isolation from cluster
- Reserve 2 subnets of at least /21 size for services to use

Deployment Scenarios

Cabling up Cisco DNA Center clusters to Top of Rack or Access Switches



Recommended

Two Switches: Single point of failure for DNAC

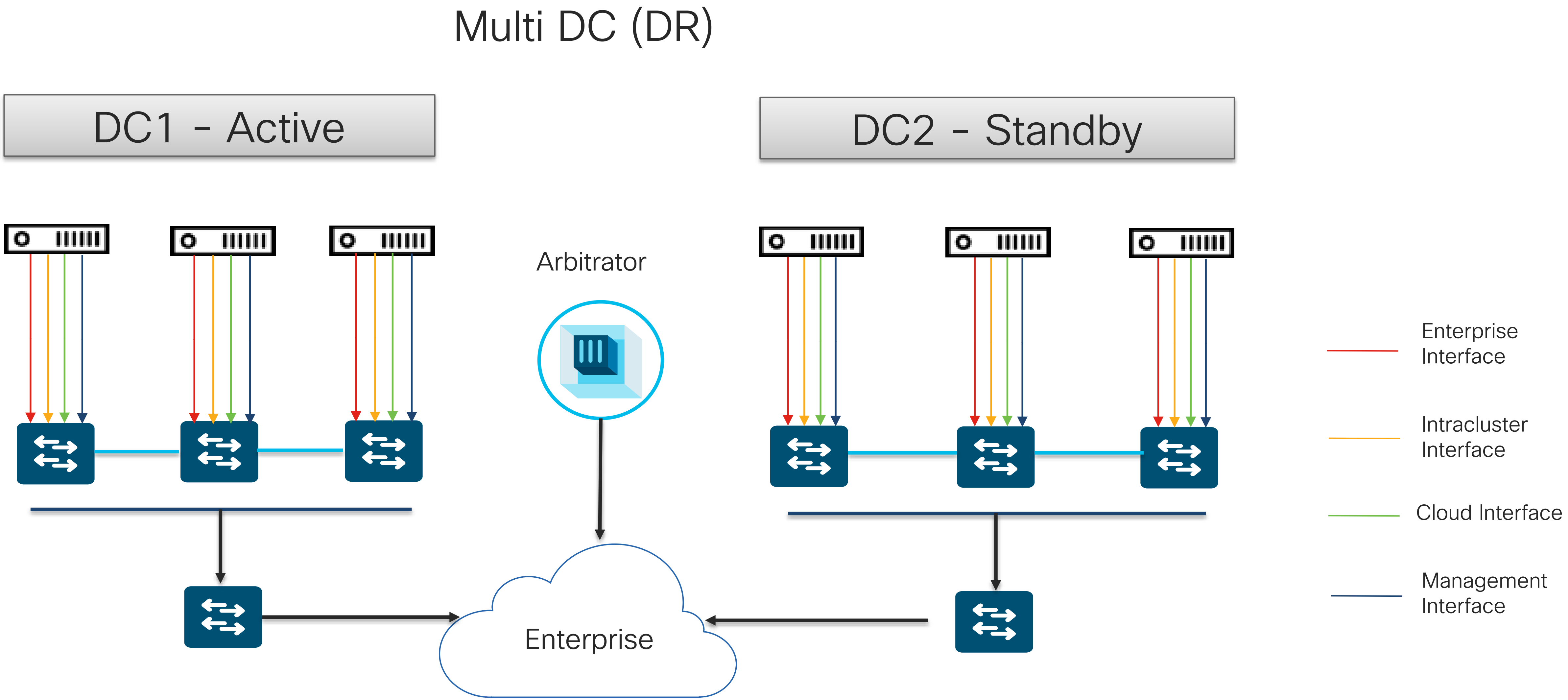
Enterprise Interface

Intracluster Interface

Cloud Interface

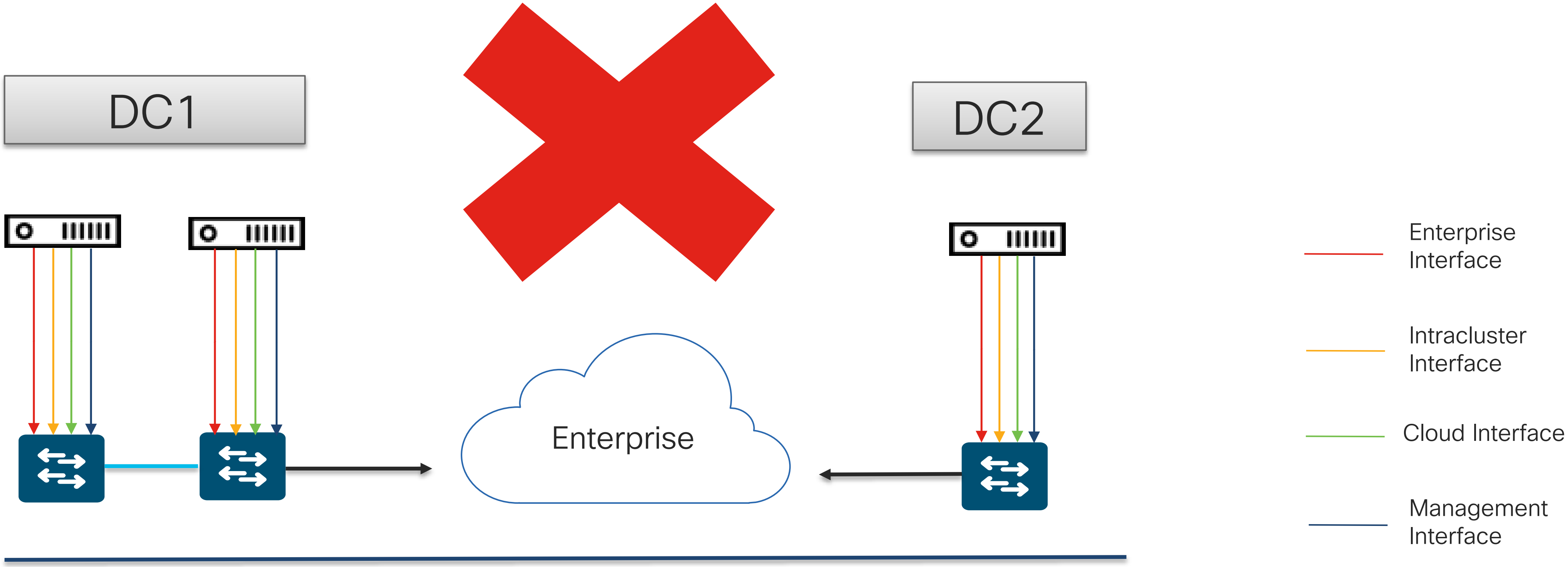
Management Interface

Multi-DC Deployment Scenario



Deployment Scenarios

Multi DC

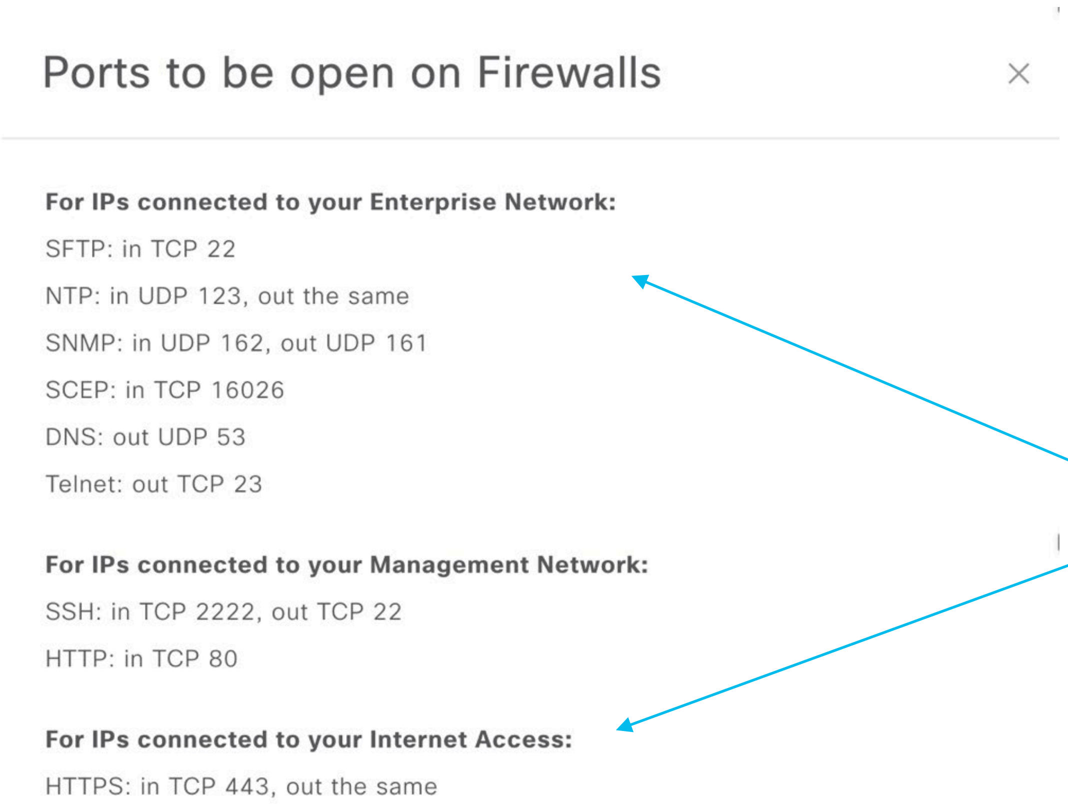


External Connectivity Requirements

The following URLs need to be accessible from the Cisco DNA Center for various operations

External Connections	URLs
Cisco DNA Center Update package downloads	https://*.ciscoconnectdna.com/*
Smart Account and SWIM Software Downloads	https://*.cisco.com/*
Rendering Geo-Maps on the Cisco DNA Center UI	https://*.tiles.mapbox.com/*
Meraki Integration	https://*.meraki.com/
IPAM Integration	URL for the IPAM-server
User feedback	https://dnacenter.uservoice.com/

Internal Connectivity Requirements



Ports to be open on Firewalls

For IPs connected to your Enterprise Network:

SFTP: in TCP 22

NTP: in UDP 123, out the same

SNMP: in UDP 162, out UDP 161

SCEP: in TCP 16026

DNS: out UDP 53

Telnet: out TCP 23

For IPs connected to your Management Network:

SSH: in TCP 2222, out TCP 22

HTTP: in TCP 80

For IPs connected to your Internet Access:

HTTPS: in TCP 443, out the same

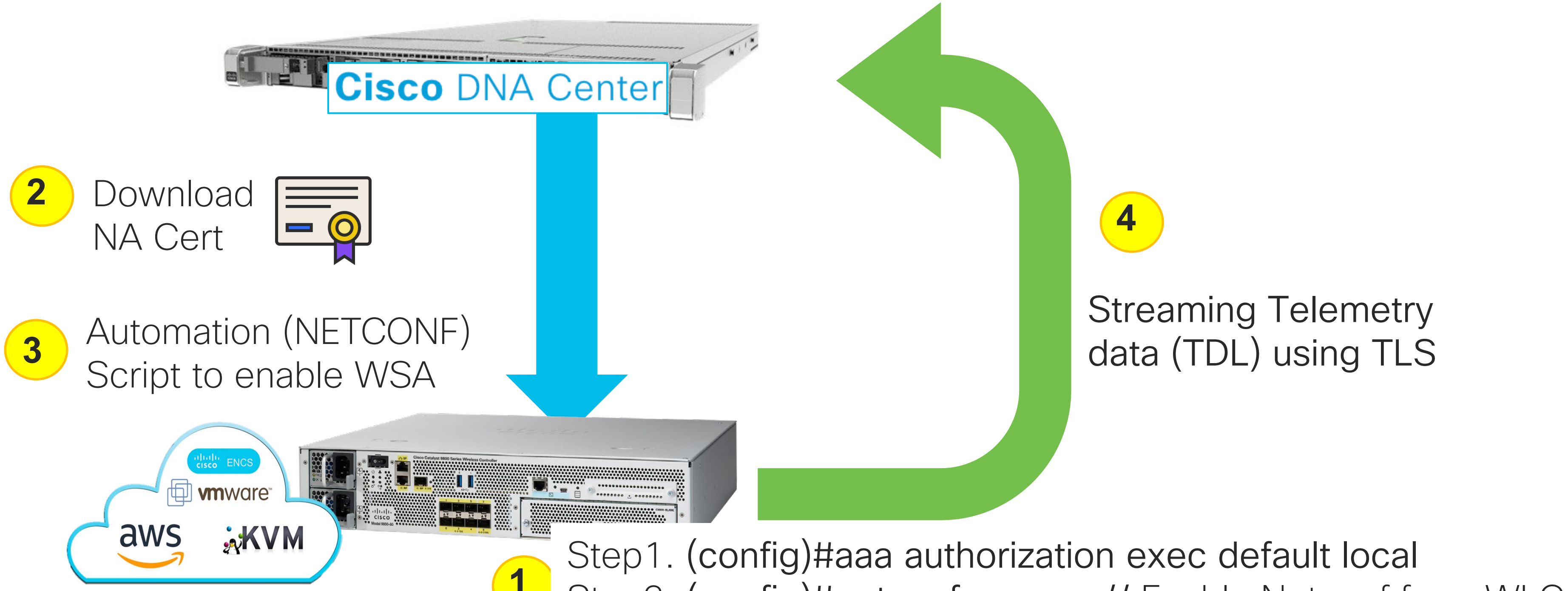
- Ensure that these ports are open for traffic flows to and from the appliances.
- Additional ports, protocols, and types of traffic must be accommodated if you are deploying the appliance in a network that employs SDA infrastructure.

Cisco DNA Assurance Setup

Key Considerations

Cisco DNA Center automatically turns on streaming telemetry when Catalyst 9800 is added to inventory

- Cisco DNAC pushes automated scripts to enable telemetry
  1. Prerequisite – Enable Netconf-yang from Cat9800 CLI
  2. Install DNAC Certificate for https setup with Cisco DNAC
  3. Configure and Enable streaming telemetry (TDL) using NETCONF to Cisco DNAC


Cisco DNA Center
2 Download NA Cert
3 Automation (NETCONF) Script to enable WSA
4 Streaming Telemetry data (TDL) using TLS
cisco ENCS
vmware
aws
KVM

1 Step1. (config)#aaa authorization exec default local
Step2. (config)#netconf-yang // Enable Netconf from WLC CLI

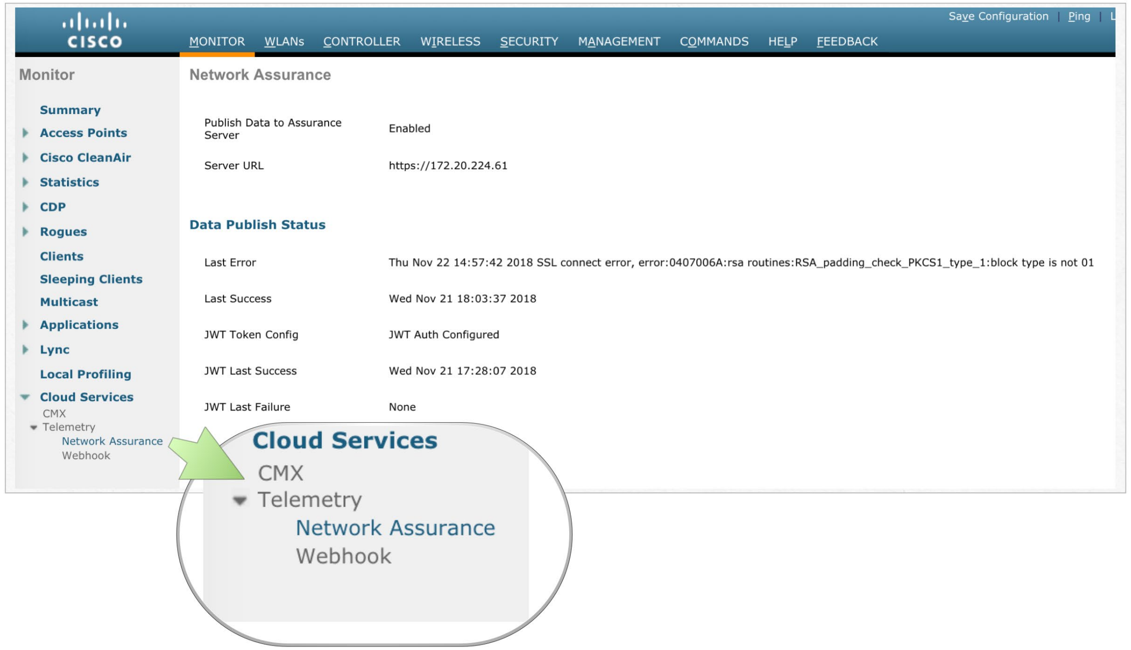
How to verify if DNAC-WLC streaming telemetry is properly configured

- CLI - “*show network assurance summary*”
  - Last Success Timestamp is newer than Last Error
  - New JWT Token updated every an hour

- GUI* –[Monitor][Cloud Services][Telemetry][Network Assurance]

```
(Cisco Controller) >show network assurance summary


    Server url............................ https://192.168.139.162
    Wsa Service........................... Enabled
    wsa Onchange Mode..................... Enabled
    wsa Sync Interval..................... Fixed
                                          NAC Data Publish Status:
      Last Error......................... Fri Feb 16 06:57:12 2018
      Last Success....................... Fri Feb 16 07:38:18 2018
      JWT Token Config................... JWT Auth Configured
      JWT Last Success................... Fri Feb 16 06:57:12 2018
      JWT Last Failure................... None
```



Network Assurance

Publish Data to Assurance Server Enabled

Server URL https://172.20.224.61

Data Publish Status

Last Error Thu Nov 22 14:57:42 2018 SSL connect error, error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01

Last Success Wed Nov 21 18:03:37 2018

JWT Token Config JWT Auth Configured

JWT Last Success Wed Nov 21 17:28:07 2018

JWT Last Failure None

AireOS WLC Provisioning troubleshooting

- Streaming Telemetry Failure -WLC shows “partial collection failure” in Last Sync Status
- Check following items,
  1. Check if WLC has right SNMP Read Only community name
  2. Check if Cisco DNAC has right WLC Credential
  3. Check if WLC Network Assurance is properly “Externalizing Data”
  4. Check if WLC has right time(NTP or manual)
  5. Check if WLC properly subscribed necessary channels from WLC GUI,

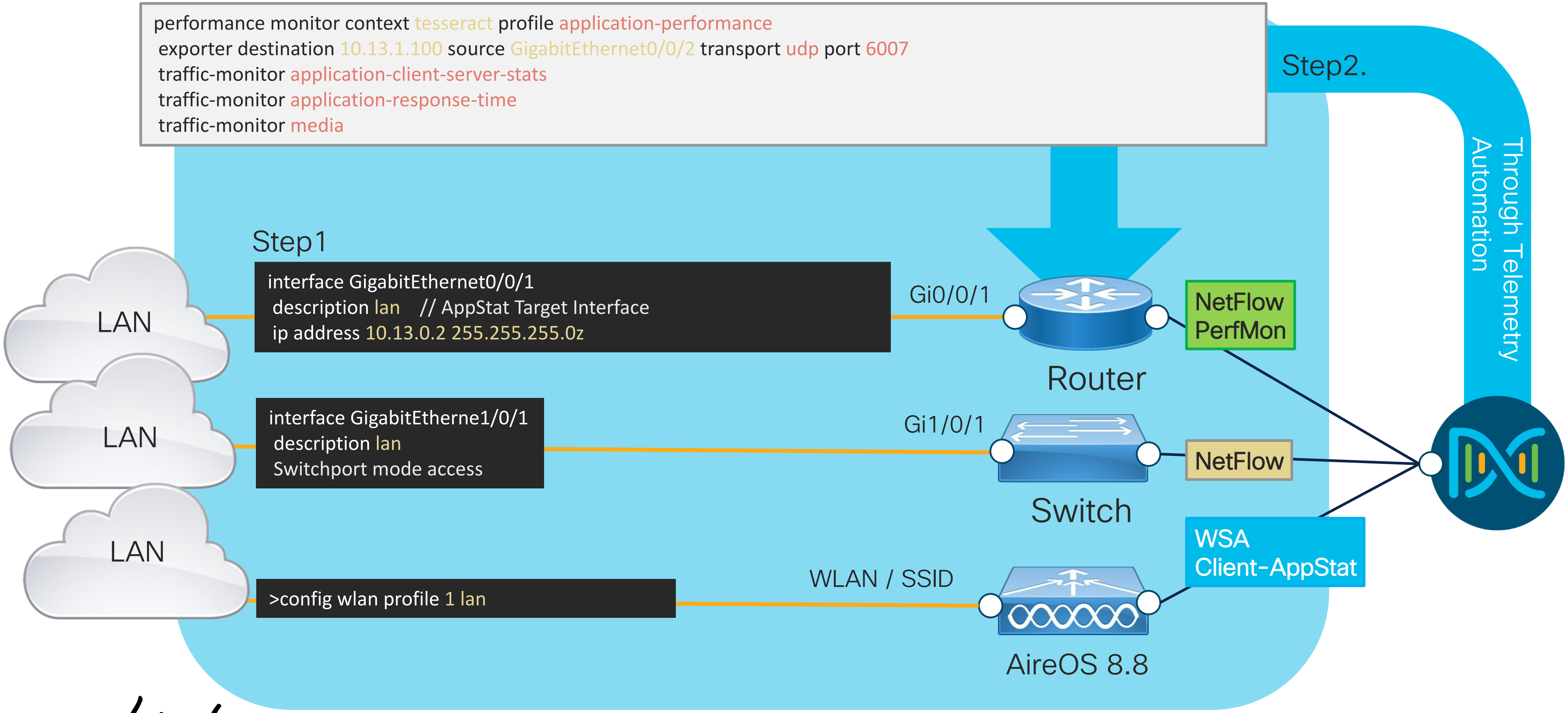
     [MANAGEMENT] [Cloud Services] [Telemetry] [Network Assurance] [Server] [Advanced Configuration]

Catalyst 9800 Provisioning troubleshooting

- Streaming Telemetry Failure -WLC shows “partial collection failure” in Last Sync Status
- Check following items,
  1. (config) #netconf-yang // Enable netconfig
  2. (config) #crypto pki trustpoint DNAC-CA. // Check DNAC-CA trust config
  3. (config) #aaa new-model
  4. (config)#aaa authorization exec default local
  5. Check if WLC properly subscribed necessary channels from WLC GUI,

     [MANAGEMENT] [Cloud Services] [Telemetry] [Network Assurance] [Server] [Advanced Configuration]

Application Visibility/Experience Enablement on Router / Switch / WLC



```
performance monitor context tesseract profile application-performance
 exporter destination 10.13.1.100 source GigabitEthernet0/0/2 transport udp port 6007
 traffic-monitor application-client-server-stats
 traffic-monitor application-response-time
 traffic-monitor media
```

Step2.

Through Telemetry Automation

Step1

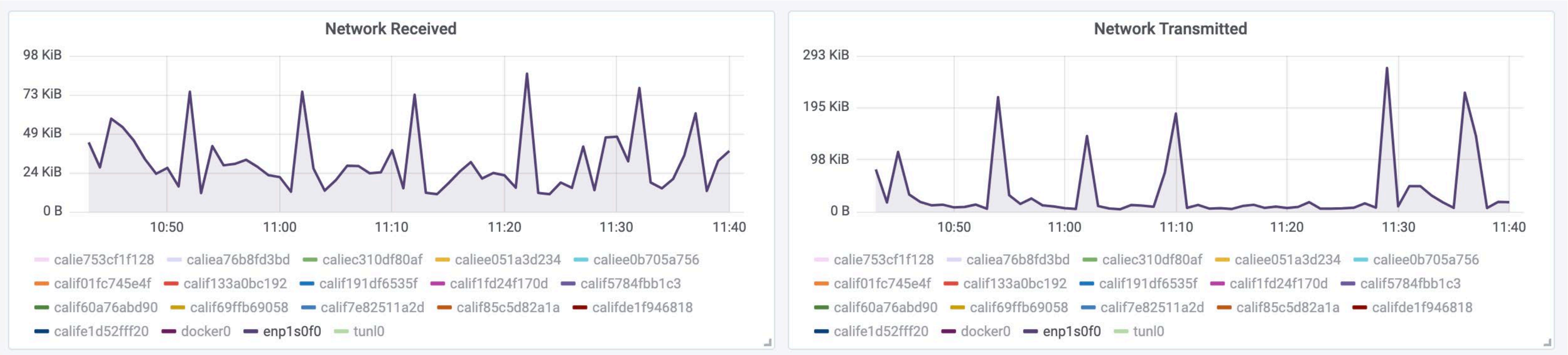
```
interface GigabitEthernet0/0/1
 description lan    // AppStat Target Interface
 ip address 10.13.0.2 255.255.255.0z
```

```
interface GigabitEtherne1/0/1
 description lan
 Switchport mode access
```

```
>config wlan profile 1 lan
```

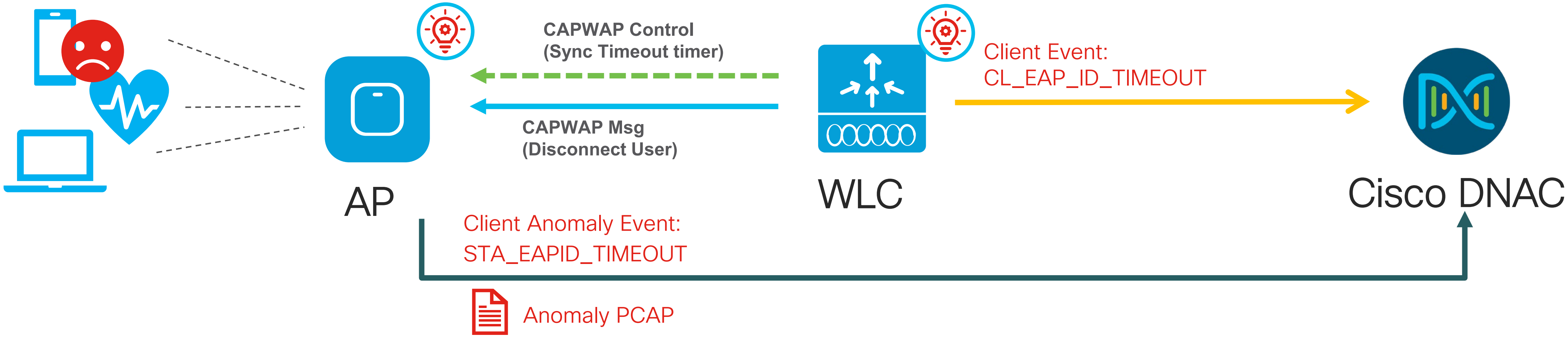
How to identify Telemetry Traffic consumption?

System Settings > Monitoring > Nodes > Select Network Interface name



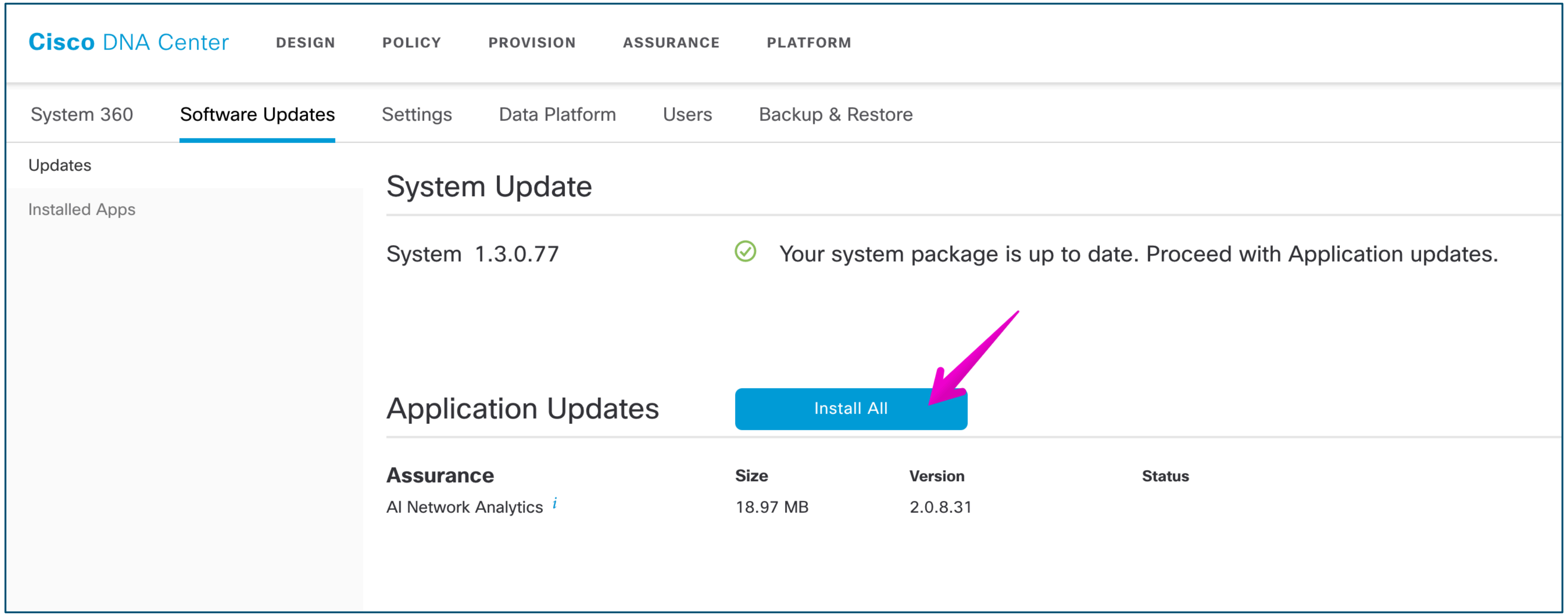
- Streaming Telemetry : Assurance - Wireless Collector, Assurance – gRPC
- Network BW consumption is not always linear to size of network but often decided by end-user behaviors and co-located environment
  - E.g. Client (Onboarding) Event, Rogue, Interferer

Intelligent Capture: Anomaly Packet Capture through AP-WLC-DNAC Correlation



- Client Onboarding State machine is located in WLC and generate Client Event
- AP is using Client onboarding policy (DHCP Timeout timer, 802.11 message etc) and generate Client Anomaly Event
  - DHCP Failure
  - 802.1x Failure
  - EAP Key Exchange Failure (4-way, GTK Failure, Invalid EAPOL Key MIC etc)
  - Protocol Mismatch (Invalid RSN IE, Supported Rate Mismatch, Mismatching Replay Counter, etc)

Cisco AI Network Analytics Agent Deployment Step1: Install Packages



System Update

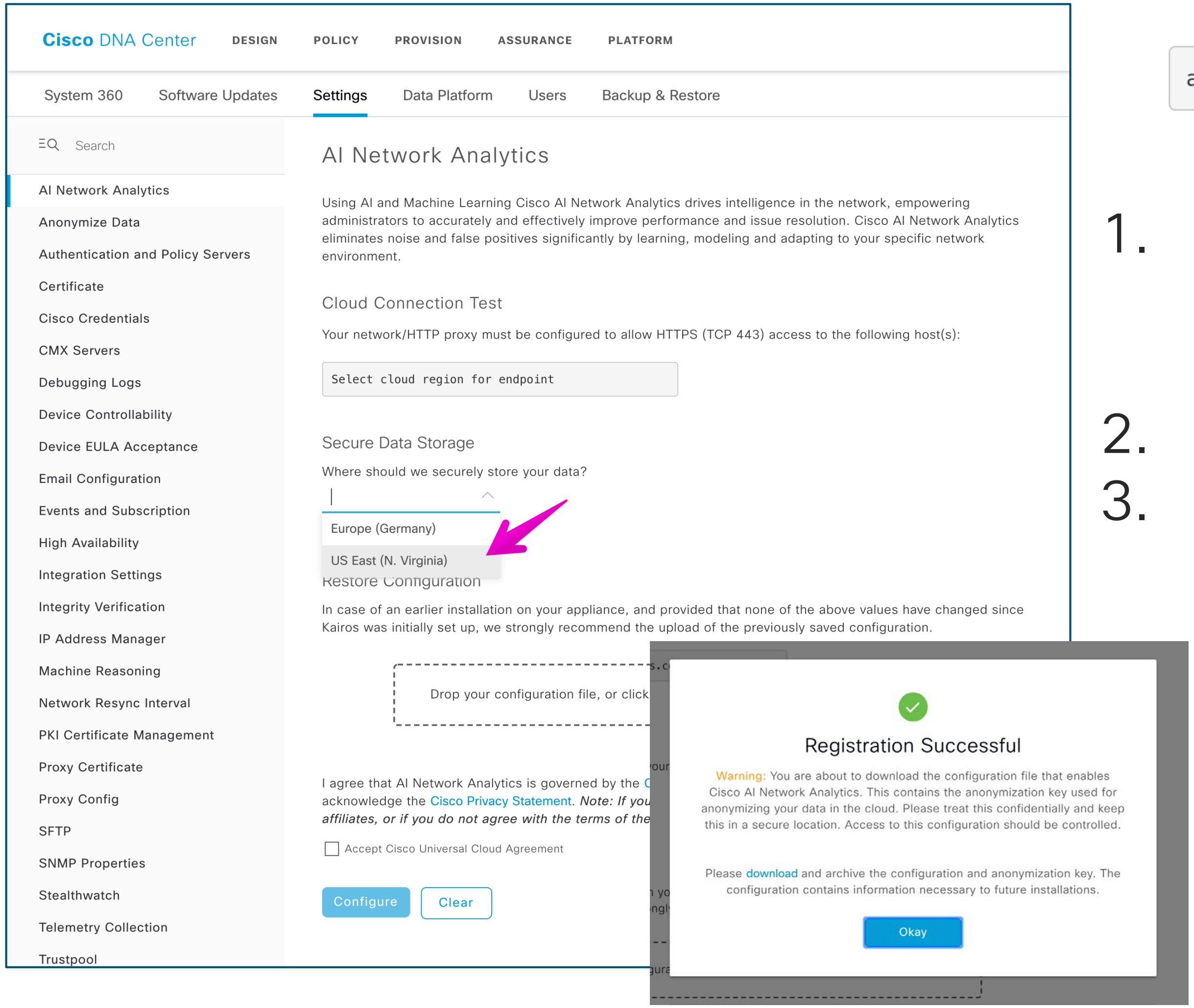
System 1.3.0.77 ✓ Your system package is up to date. Proceed with Application updates.

Application Updates

Assurance	Size	Version	Status
AI Network Analytics *i*	18.97 MB	2.0.8.31	

- Go to [Settings][Software Update]
- Install “AI Network Analytics” package

Agent Deployment
Step2: Cloud Analytics Onboard



AI Network Analytics

Using AI and Machine Learning Cisco AI Network Analytics drives intelligence in the network, empowering administrators to accurately and effectively improve performance and issue resolution. Cisco AI Network Analytics eliminates noise and false positives significantly by learning, modeling and adapting to your specific network environment.

Cloud Connection Test

Your network/HTTP proxy must be configured to allow HTTPS (TCP 443) access to the following host(s):

```
Select cloud region for endpoint
```

Secure Data Storage

Where should we securely store your data?

Europe (Germany)
US East (N. Virginia)

Restore Configuration

In case of an earlier installation on your appliance, and provided that none of the above values have changed since Kairos was initially set up, we strongly recommend the upload of the previously saved configuration.

Drop your configuration file, or click

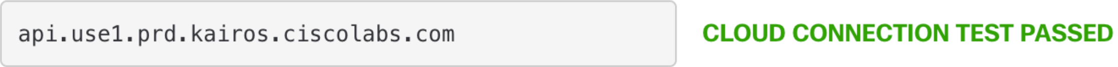
I agree that AI Network Analytics is governed by the C
acknowledge the Cisco Privacy Statement. *Note: If you*
affiliates, or if you do not agree with the terms of the

□ Accept Cisco Universal Cloud Agreement

Registration Successful

Warning: You are about to download the configuration file that enables Cisco AI Network Analytics. This contains the anonymization key used for anonymizing your data in the cloud. Please treat this confidentially and keep this in a secure location. Access to this configuration should be controlled.

Please download and archive the configuration and anonymization key. The configuration contains information necessary to future installations.



```
api.use1.prd.kairos.ciscolabs.com
```

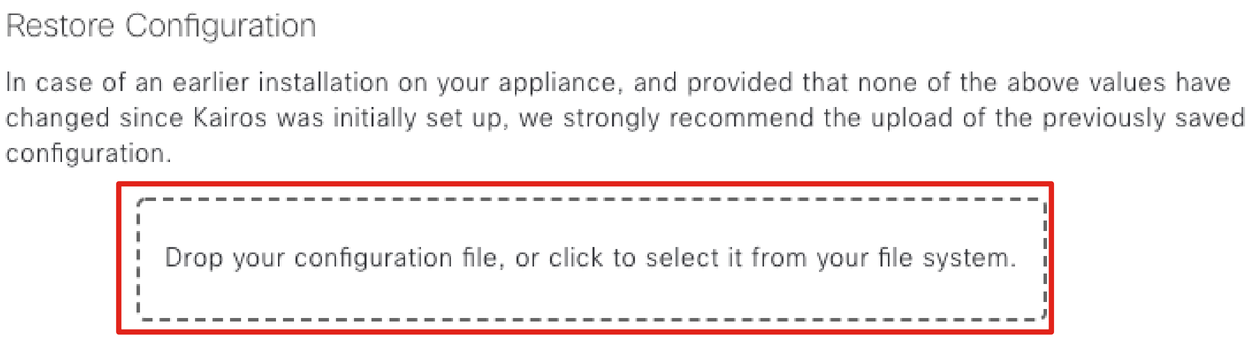
CLOUD CONNECTION TEST PASSED

1. Select Location of Cloud Data Center
   1. US (api.use1.prd.Kairos.ciscolabs.com)
   2. Europe (api.euc1.prd.kairos.ciscolabs.com)
2. Agreed on Term and Condition
3. Click [Configure] button

Agent Deployment
Step3: Save AI Network Analytics Config file

kairos-config.json

...after successful AI Network Onboarding,
DNAC Automatically download config backup file, Kairos-config.json
which includes anonymization-key, client cert., client-key.

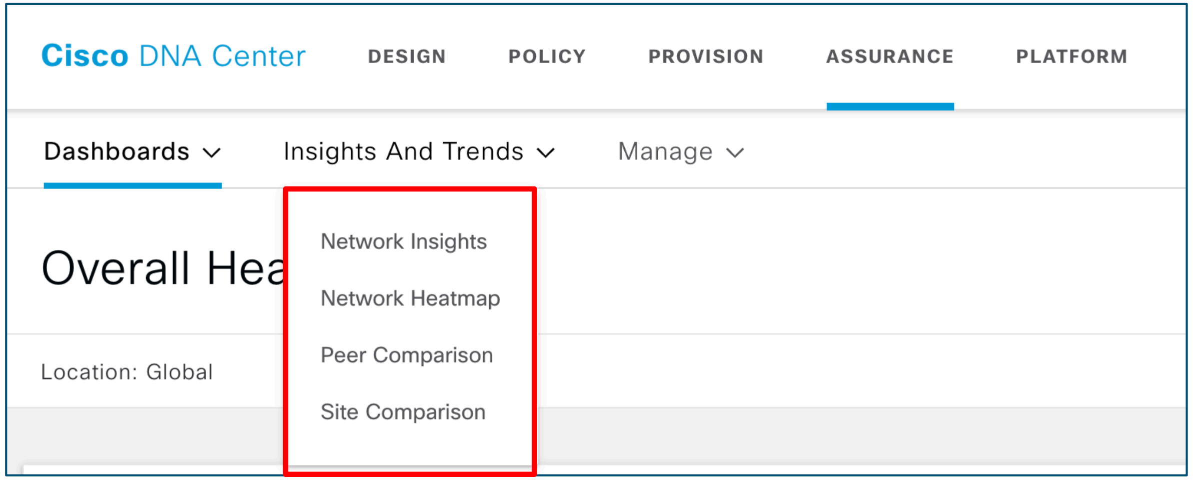


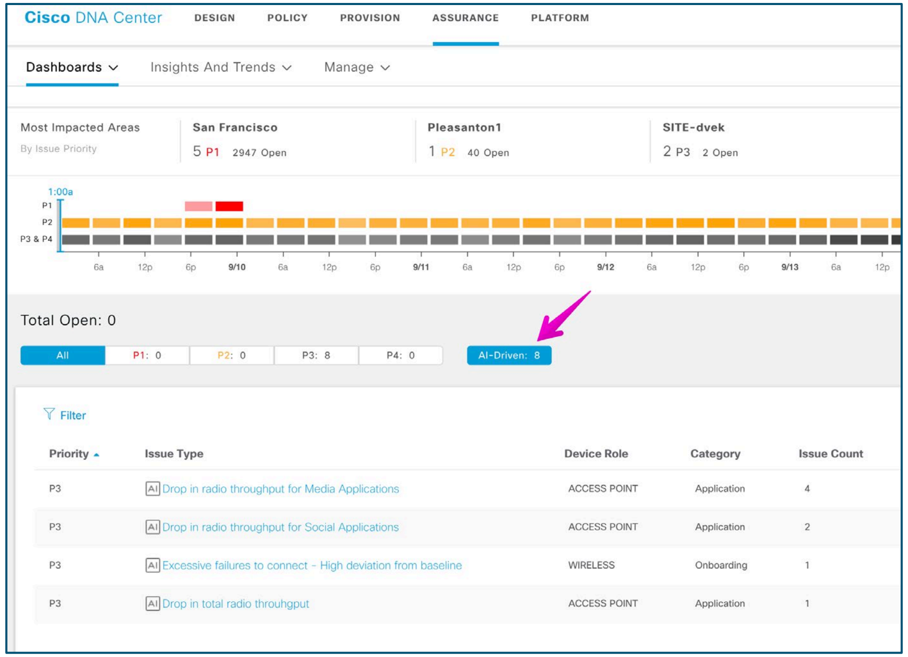
Restore Configuration

In case of an earlier installation on your appliance, and provided that none of the above values have changed since Kairos was initially set up, we strongly recommend the upload of the previously saved configuration.

Drop your configuration file, or click to select it from your file system.

Agent Setup: What’s next





Most Impacted Areas
By Issue Priority

San Francisco
5 P1 2947 Open

Pleasanton1
1 P2 40 Open

SITE-dvek
2 P3 2 Open

Total Open: 0

Priority	Issue Type	Device Role	Category	Issue Count
P3	AI Drop in radio throughput for Media Applications	ACCESS POINT	Application	4
P3	AI Drop in radio throughput for Social Applications	ACCESS POINT	Application	2
P3	AI Excessive failures to connect - High deviation from baseline	WIRELESS	Onboarding	1
P3	AI Drop in total radio throuhgput	ACCESS POINT	Application	1

- You can recognize that AI Network Analytics is installed, by looking at the Assurance UI, where the “Insights And Trends” tab is now present
- “Insights And Trends” gives Access to Network Insights, heatmaps, Smart dashboards and compare with others or building to building
- After 7 Days, new “AI-Driven Issues” will be pushed and available from new Issue Dashboard

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

- Demos in the Cisco Showcase
- Walk-In Labs
- Meet the Engineer 1:1 meetings
- Related sessions

Thank you

You make **possible**

Appendix

Feature Matrix

Wireless Telemetry Type

Type	Port	Telemetry Source	Feature	Recommended S/W Ver*
WSA (Wireless Service Assurance)	TCP 443	CT3504, 5520, 8540 Mobility Express	Channelized WSA DiffSync, Event or Stat. Filtered Channel	8.5.140.0 or 8.8.120.0
TDL	TCP 443	Catalyst 9800	Real Time Event TLS-based	16.10.1e
gRPC	TCP 32626	AP2/3/4800	Real Time Stat Binary telemetry	8.8.120.0
AP WSA	TCP 443	AP1815/30/50 AP1800s	Control and Report channel	8.5.140.0 or 8.8.120.0 8.8.261

*Based on Cisco DNA Center 1.3

Streaming Telemetry produces 3 times faster and more data

	I/O	Type	Cisco DNAC	Legacy NMS	Notes
Client and Network Health analysis	Input	AP & Client RF Stat Intervals	90 sec	300 sec (5 min)	x3 Faster
	Output	Update frequency on DNAC	300 sec (5 min; includes Health score computation)	900 sec (15 min)	x3 Faster
Client Onboarding analysis	Input	Onboarding Events Viewer Intervals	240+ Events coming at a rate of 30 sec	Assoc. & Disassoc. Events Only at 300 sec	x10 Faster
	Output	Update frequency on DNAC	300 sec (5 min)	300-900 sec (5-15 min)	Up to x3 Faster
Client and Network Troubleshooting using Intelligent Capture*	Input	AP RF Stat Intervals	30 sec	N.A	N.A
		Client RF Stat Intervals	5 sec	N.A	N.A
		On-Boarding Event Viewer Intervals	2 sec	N.A	N.A
		Spectrum Analyzer	5 sec	N.A	N.A
	Output	Update Interval on DNAC	30 sec	N.A	N.A

Wireless Assurance Feature by Deployment model

	Network Health	Client Health	Client360	Issue	Sensor	Intelligent Capture	Cisco AI Network Analytics
Local Mode	●	●	●	●	●	●	●
FlexConnect (Central Auth)	●	●	●	●	●	●	●
LocalAuth, LocalDHCP	●	●	○*	○*	●	●	○*
Mobility Express	●	●	●	●	●	●	●
Catalyst 9800	●	●	●	●	●	●	Roadmap

*In FlexConnect LocalAuth/DHCP/Assoc mode, Event Viewer and Onboarding Widget, Onboarding Issue has limited visibility

Wireless Assurance AP Feature Matrix

	Min. S/W AireOS	Min. S/W Cat9800	.11n / Wave-1 APs	AP1800/ C9115	C9120	AP2800 / 3800	AP4800
Health, Issue	8.5.120	16.10.1e	●	●	●	●	●
Rogue Management (DNAC 1.4)	8.8.111	16.12.x	●	●	●	●	●
DNS Widget	8.8.111	16.10.1e	X	●	●	●	●
IP SLA Responder	8.8.111	16.10.1e	X	●	●	●	●
Intelligent Capture (AP& Client RF Stat, Anomaly PCAP, Scheduled PCAP)	8.8.120	16.12.x	X	●*	●*	●	●
Intelligent Capture w/ Spectrum Analyzer	8.8.120	16.12.x	X	X	X	●	●
Intelligent Capture w/ Full Packet Capture	8.8.120	16.12.x	X	X	X	X	●

Intelligent Capture Operation and Scale

DataType	Operation	Scale
Full Packet Capture	On-Demand	Single Client Device (1 client at any point in time on DNA Assurance)
Client RF stats	Scheduled	Up to 16 Clients
Client Onboarding Events (WLC)	Always On	
Partial PCAP (Mgmt., DHCP/ICMP, EAP, etc.)	Scheduled	Up to 16 Clients
AP RF Stats, Other AP Stats	Via Config option (On/Off)	APs at any point in time on DNA Assurance for 4000 AP deployment
Client RF Stats	Scheduled	Up to 16 Client
Spectogram View	On-Demand	Only during client browser is opened
Client Location Update	Always On	For All Clients (using CMX)

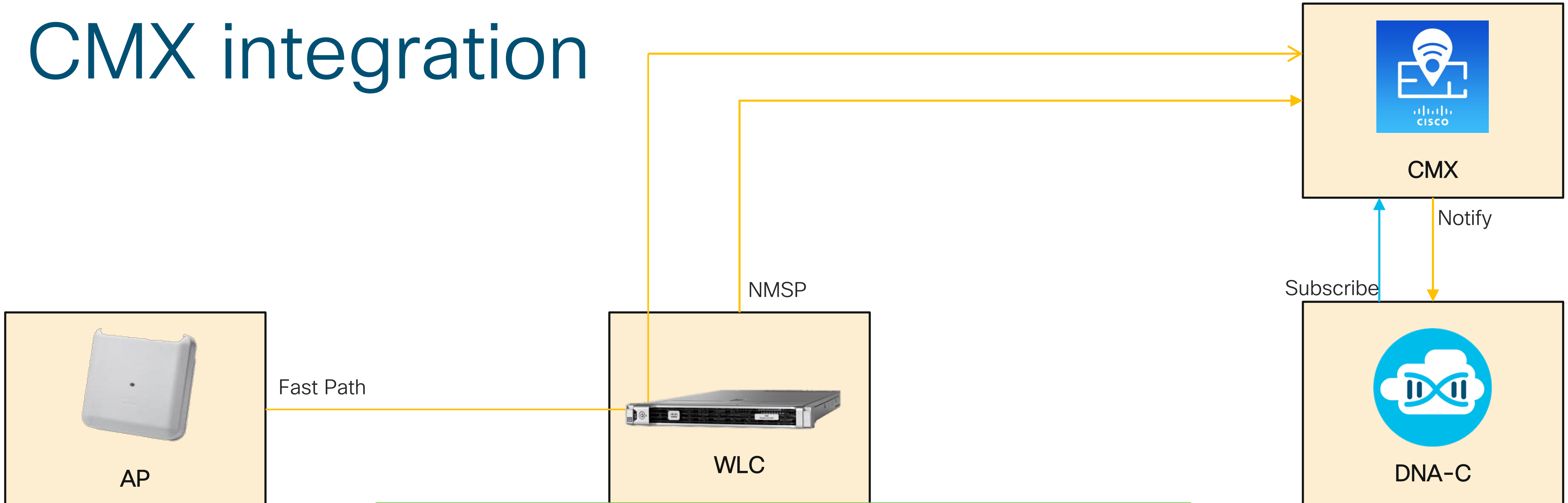
Available Packet Type per Capture mode

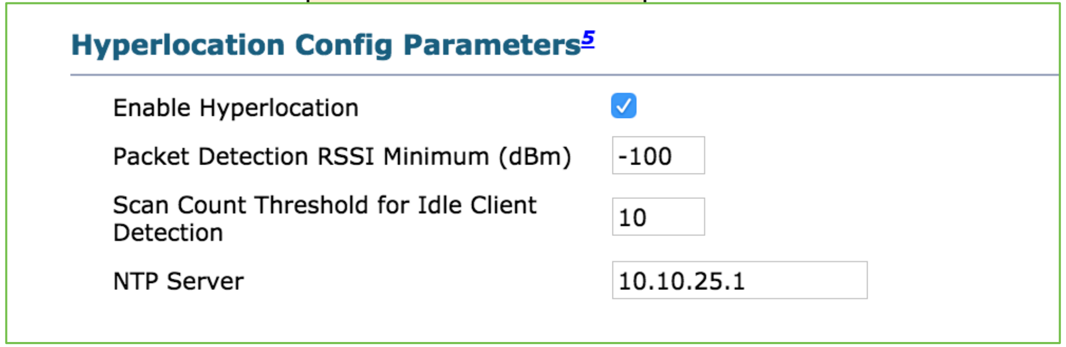
PCAP Type	How to trigger	Media Type	Captured Protocol	Features	Supported AP and capture method
Onboard PCAP	On-demand or Scheduled or automated	• Wireless PCAP	802.11 mgmt. (Auth, Assoc) Data – (802.1x/EAP, DHCP, DNS, ARP, ICMP), Roaming – 802.11k, 802.11v Block Ack	• Auto Packet Analyzer • Downloadable from anywhere using Web browser • Automated Onboard Failure PCAP up to 100 packet per session • Data Packet auto decryption	AP2800/3800/4800 – Inline-based Packet capture
Full PCAP	On-demand	• Wireless PCAP • Wired PCAP	• 802.11 with Radio Header (Mgmt, Control, Data Frame) • 802.3 with Ethernet Header	• Application Analyzer, • Wireless Delay, Wireless Packet Loss Chart • Jitter chart using RTP (Wired & Wireless) • Data Packet auto decryption	AP4800 – 3rd Radio w/ Self-Sniffing feature

Intelligent Capture FAQ

- Bandwidth Consumption modeling – Intelligent Capture is essentially On-demand, scheduling-based feature
- BW consumption only occurs when each feature get turned on
  - Partial Packet Capture
  - Spectrum
  - On-Demand Full Packet Capture : Client BW consumption x 2 (wired, wireless)
- Catalyst 9800 platform Intelligent Capture support – scheduled on 16.12.1

CMX integration





Hyperlocation Config Parameters[5]

Enable Hyperlocation	☑
Packet Detection RSSI Minimum (dBm)	-100
Scan Count Threshold for Idle Client Detection	10
NTP Server	10.10.25.1

- Client updates sent via existing methods using NMSP or Fast Path
- DNAC to subscribe/register for location updates for one or list of clients
- Push-based Client location update from CMX to DNAC
- Enable Hyperlocation support for NTP enforcement

How to setup Sensor

Sensor Workflow

Day-0 Sensor Provisioning

- Sensor Profile creation
- DNAC Discovery
- Claim
- Map Placement

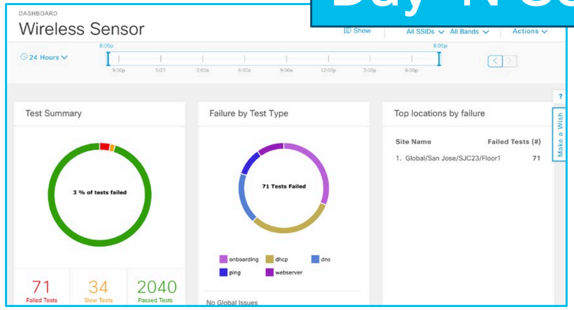
Day-1 Sensor Test Config

- Select Onboard SSID
- Network Test
- Performance Test (Speed Test, SLA)
- Application Connectivity

Day-2 Sensor Upgrade

- Upgrade using DNAC
- Upgrade using CLI

Day-N Sensor Dashboard



DASHBOARD

Wireless Sensor

Test Summary

3 % of tests failed

71 Failed Tests

34 Slow Tests

2040 Passed Tests

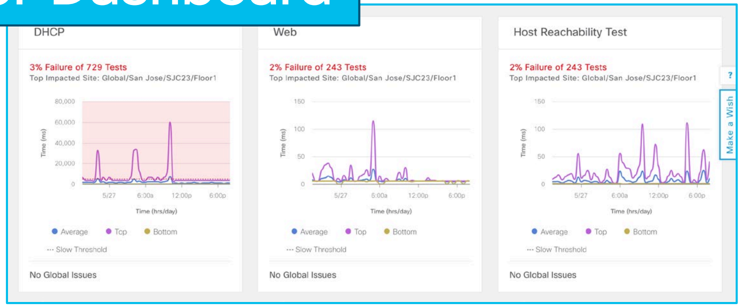
Failure by Test Type

71 Tests Failed

No Global Issues

Top locations by failure

Site Name	Failed Tests (#)
1. Global/San Jose/SJC23/Floor1	71



DHCP

3% Failure of 729 Tests
Top Impacted Site: Global/San Jose/SJC23/Floor1

No Global Issues

Web

2% Failure of 243 Tests
Top Impacted Site: Global/San Jose/SJC23/Floor1

No Global Issues

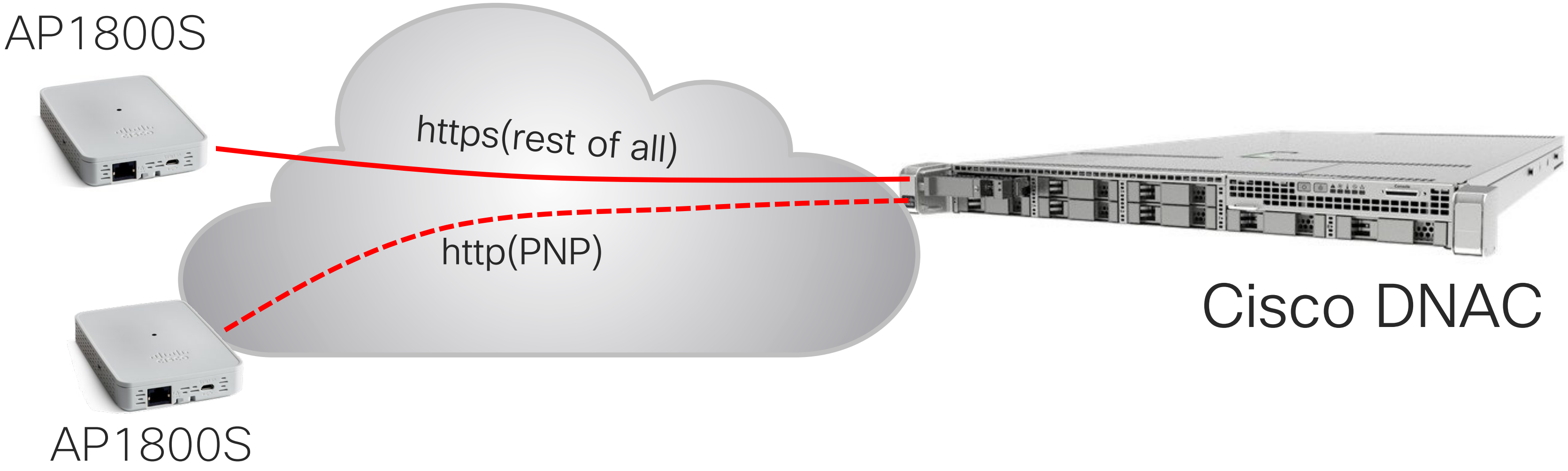
Host Reachability Test

2% Failure of 243 Tests
Top Impacted Site: Global/San Jose/SJC23/Floor1

No Global Issues

D-1, Before start sensor...

- Make sure you have network connectivity between Sensor and DNAC
  - http (TCP 80) – PNP protocol, essential to register sensor into DNAC
  - https (TCP 443) – Backhaul Channel
    - Heartbeat
    - Test config download & Test result upload
    - Image Upgrade – HTTPS (TCP 443)

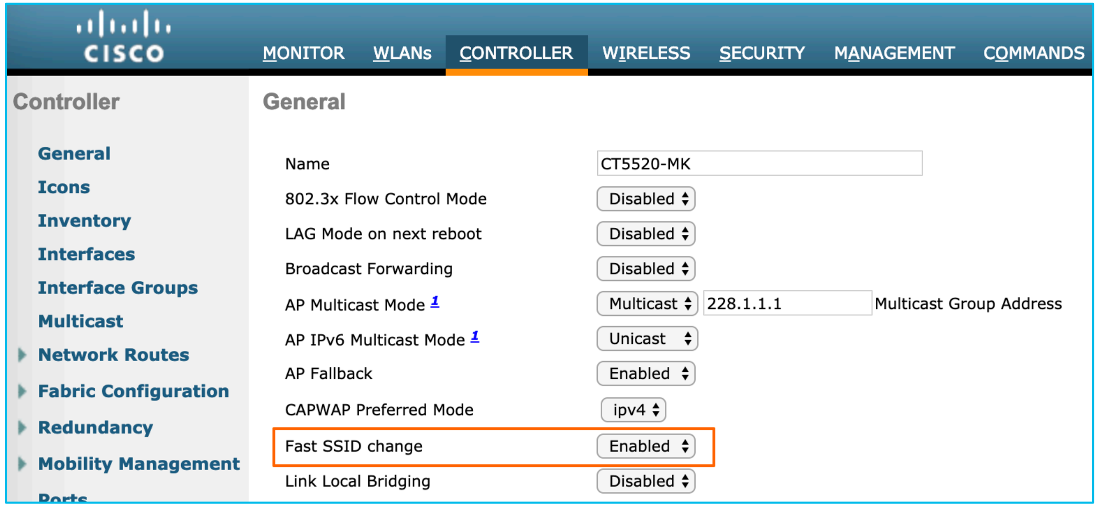


Sensor Test Target WLAN

- Sensor can onboard Cisco WLAN Network with following security config
  - OPEN
  - WPA2-PSK (AES)
  - WPA2-Enterprise
    - PEAP-MSCHAPv2
    - EAP-FAST
    - EAP-TLS
  - WLC Internal WebAuth
  - IPv4/DHCP Environment
  - Broadcast SSID
  - Hidden SSID (requires 8.8MR2 and AP1800s 8.8.260 SW)

- Sensor requires Cisco WLAN environment for its testing target network

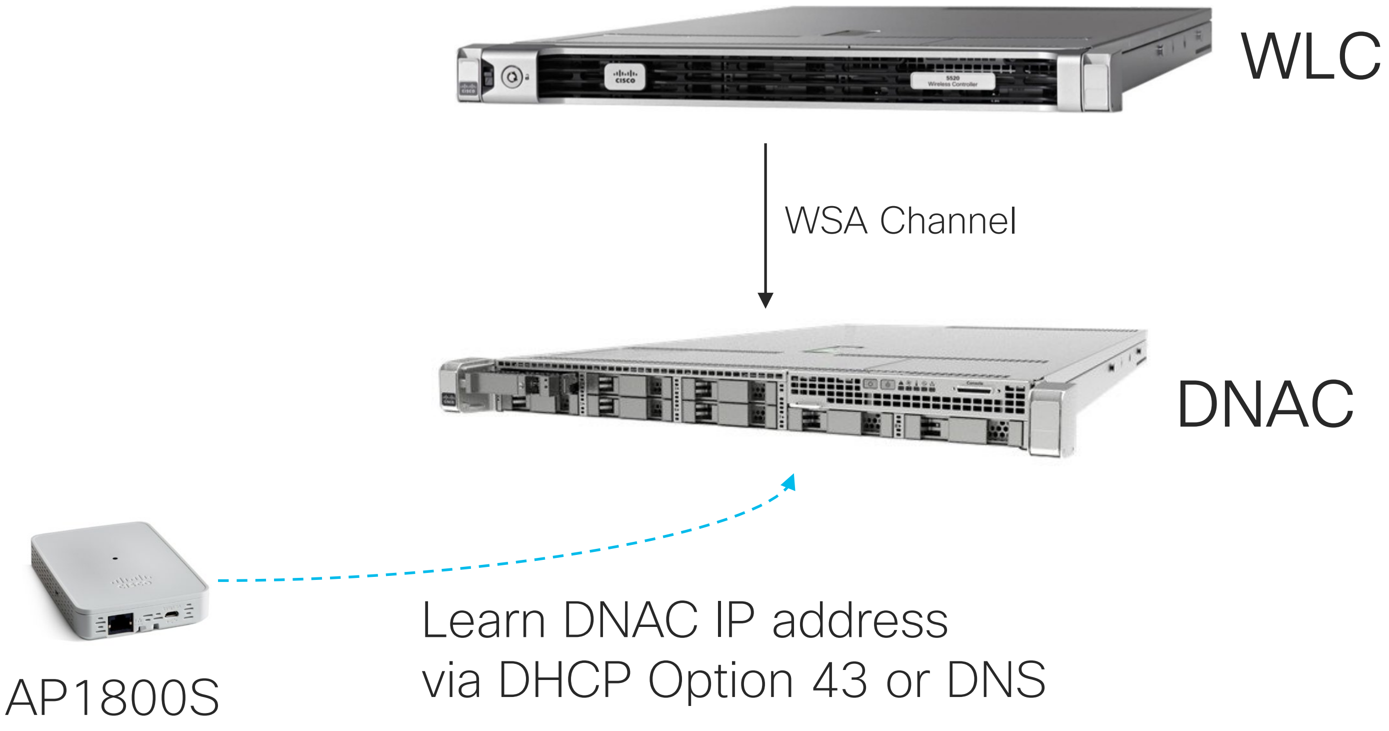
*Sensor can run testing across multiple SSIDs switching band and associating SSID.
This Sensor behavior cause Fast SSID Switching.
Enable Fast SSID Change option is recommended



General

Name	CT5520-MK	
802.3x Flow Control Mode	Disabled	
LAG Mode on next reboot	Disabled	
Broadcast Forwarding	Disabled	
AP Multicast Mode [1]	Multicast 228.1.1.1	Multicast Group Address
AP IPv6 Multicast Mode [1]	Unicast	
AP Fallback	Enabled	
CAPWAP Preferred Mode	ipv4	
Fast SSID change	Enabled	
Link Local Bridging	Disabled	

Types of discovery path to DNAC

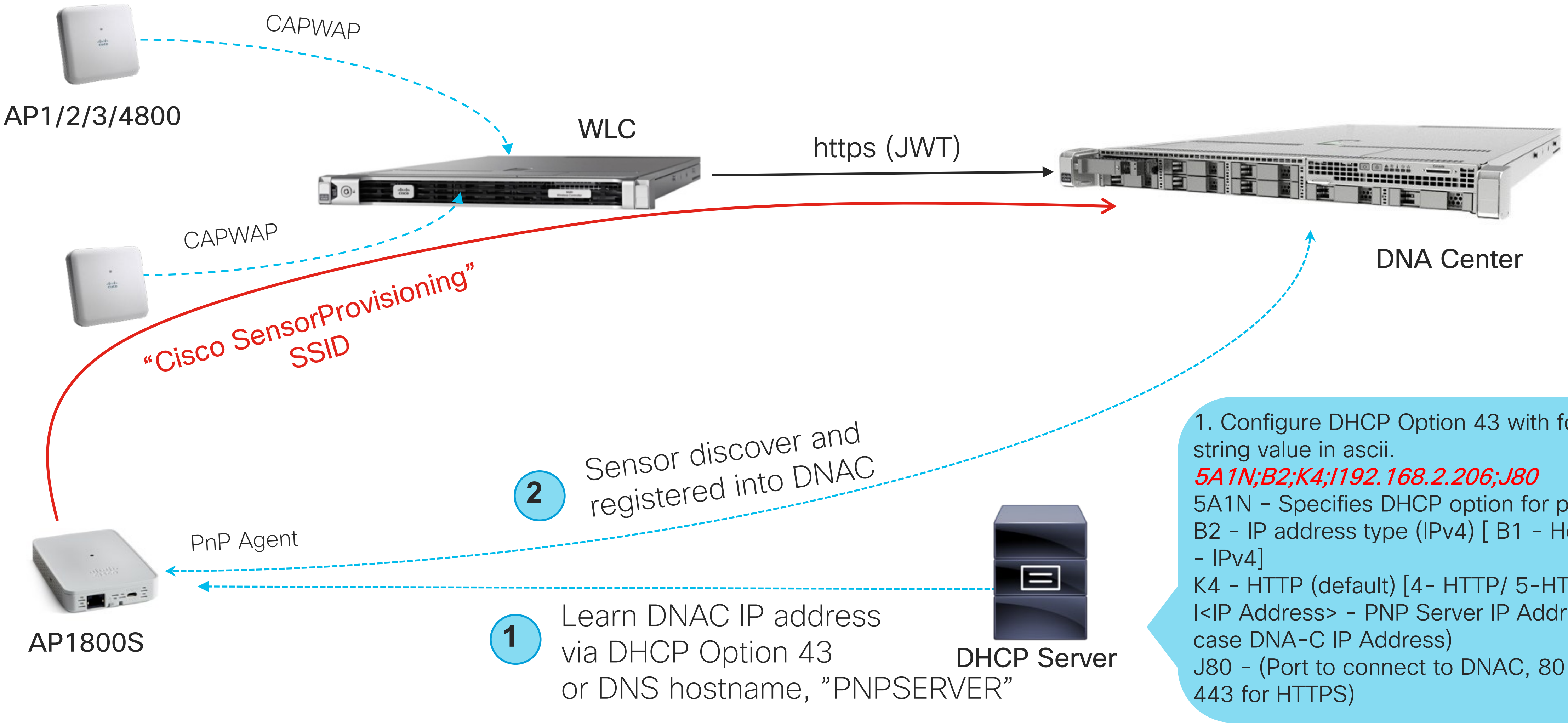


Learn DNAC IP address
via DHCP Option 43 or DNS

“CiscoSensorProvisioing” SSID

- Sensor Wireless Provisioning is done via well-known, fixed SSID
- Non-Broadcasting SSID
- Turned on from sensor provision enable command
- Must be broadcast to all APs in WLC using one of First 16 SSIDs index from WLC
- Authenticated by EAP-TLS, using WLC Local EAP
- Sensor uses MIC to get authenticated by WLC Local EAP Server

Dedicate Sensor discover DNA Center via DHCP Option 43 or DNS Hostname

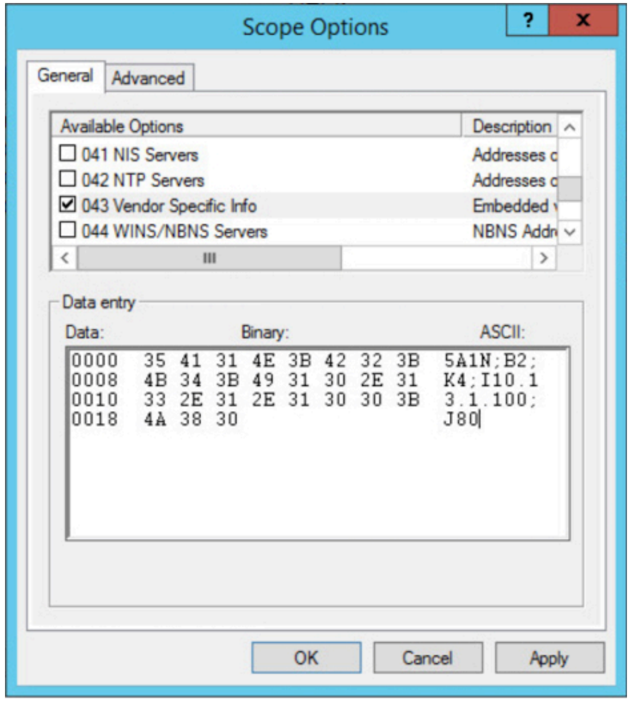


CAPWAP
AP1/2/3/4800
WLC
https (JWT)
DNA Center
CAPWAP
"Cisco SensorProvisioning" SSID
2
Sensor discover and registered into DNAC
PnP Agent
AP1800S
1
Learn DNAC IP address via DHCP Option 43 or DNS hostname, "PNPSERVER"
DHCP Server

1. Configure DHCP Option 43 with following string value in ascii.
5A1N;B2;K4;I192.168.2.206;J80
5A1N - Specifies DHCP option for plug and play
B2 - IP address type (IPv4) [B1 - Hostname / B2 - IPv4]
K4 - HTTP (default) [4- HTTP/ 5-HTTPS]
I<IP Address> - PNP Server IP Address (in this case DNA-C IP Address)
J80 - (Port to connect to DNAC, 80 for HTTP and 443 for HTTPS)

DNAC Discovery using DHCP/DNS Server

From DHCP Server



Scope Options

Available Options	Description
□ 041 NIS Servers	Addresses c
□ 042 NTP Servers	Addresses c
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr

Data entry

Data: Binary: ASCII:

```
0000  35 41 31 4E 3B 42 32 3B   5A1N;B2;
0008  4B 34 3B 49 31 30 2E 31   K4;I10.1
0010  33 2E 31 2E 31 30 30 3B   3.1.100;
0018  4A 38 30                  J80
```

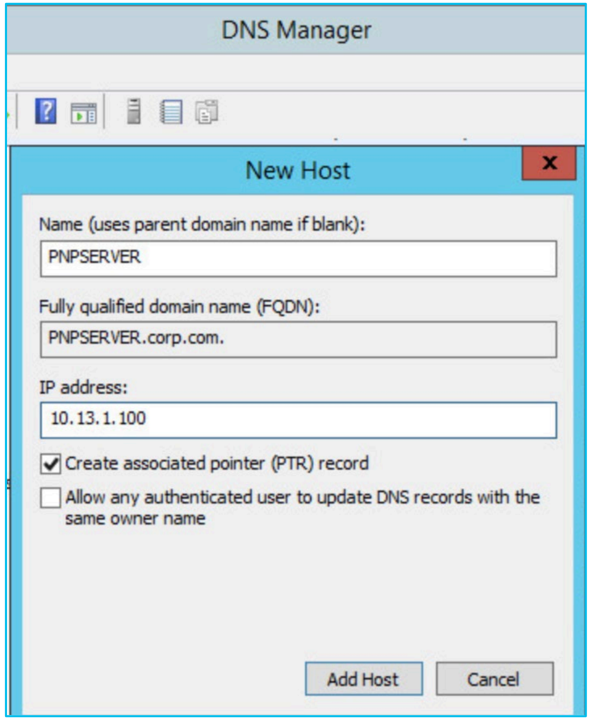
Create Option 43

“5A1N;B2;K4;I10.13.1.100;J80”

10.13.1.100 – DNAC IP Address

OR

From DNS Server



DNS Manager

New Host

Name (uses parent domain name if blank):

PNPSERVER

Fully qualified domain name (FQDN):

PNPSERVER.corp.com.

IP address:

10.13.1.100

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

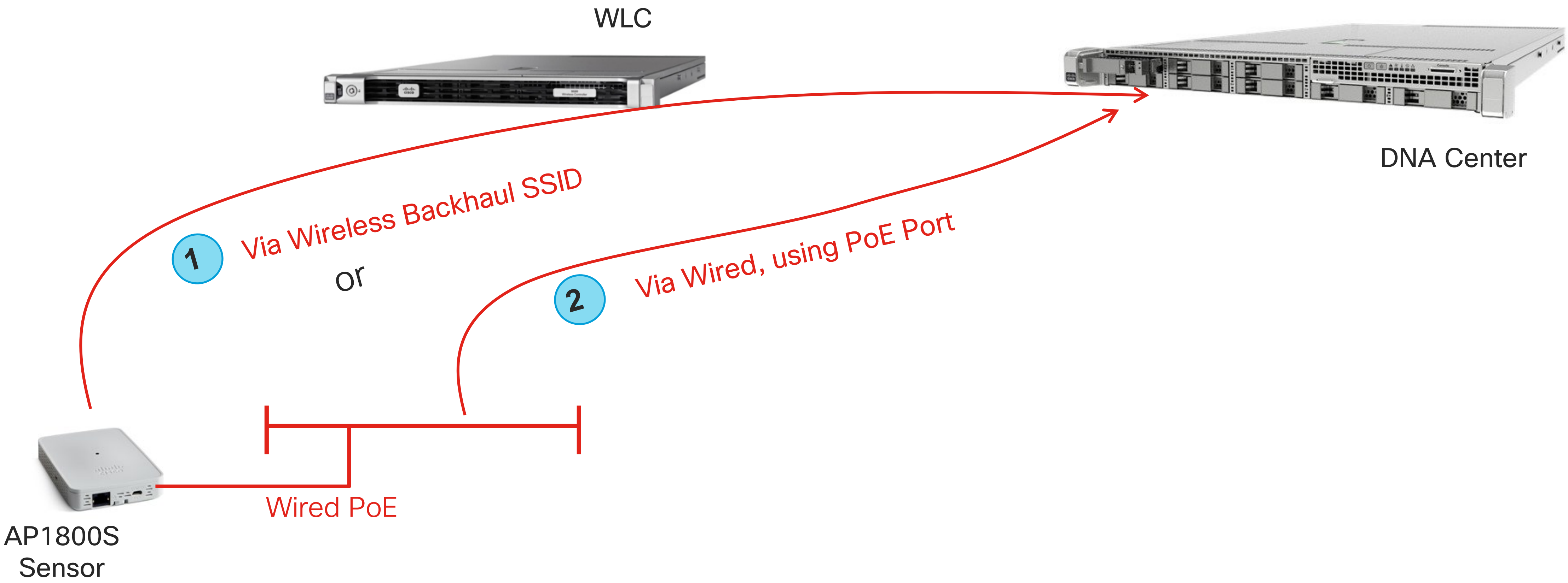
Create entry “PNPSERVER” and assign DNAC IP Address

- If Option 43 field is already used for other purpose, Use conditional Option 43 using VCI string. AP1800S’s VCI string is “Cisco AP c1800”

- Alternatively, DNAC IP Address can be manually provision from CLI Console (AIR-CONSADPT=)

```
# config dot11 sensor pnp ip
<xxx.xxx.xxx.xxx>
```

Sensor communicate directly to DNAC to report test result using designated Backhaul Interface



Sensor Test result is directly reported to DNAC using Wireless Backhaul SSID or Wired Backhaul. Make sure Sensor can directly communicate to DNAC

8 Step Sensor Image Upgrade through DNAC

Prep - Image Management

1* Download Image from CCO

2* Import image into DNAC ⊕ Import

3 Tag New sensor image as Golden Image ★

4 Click [Update Device] Update Devices

Upgrade from PROVISION

5 Select Upgrade Target Sensor

6 Action > Update OS Image

7 [Distribute] select “Now”

8 [OS Update] Select “Schedule Activation after Distribution is completed”

9 “Confirm” Upgrade

10 Wait for SWIM to complete upgrade

Or using Console cable or SSH

```
# archive download-sw /reload tftp://192.168.0.1/SW1800-SENSOR-K9-8-7-258-0.tar.gz
```