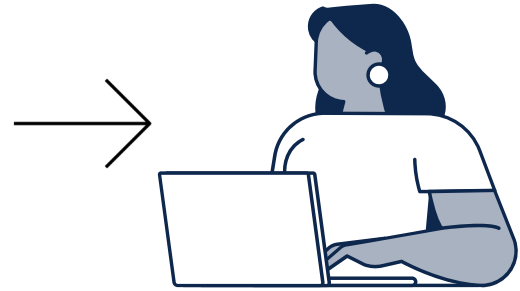
Jak vyzrát na problémy s Wi-Fi

Dominik Soukup
Jaroslav Čížek
20.9.2022



11b
Wi-Fi 1
11Mbps

more than 8hours

1999

11a, g
Wi-Fi 2/3
54Mbps

≈1.5hours

2003/2004

97% faster

11n
Wi-Fi 4
5GHz - 40MHz
MIMO
300Mbps

≈16min

2009

11ac
Wi-Fi 5
256QAM
400Mbps

≈12min

2013

48% faster

11ax
Wi-Fi 6
1024QAM
573Mbps

≈9min

2019

58% faster

11ax
Wi-Fi 6E
6 GHz – 80MHz
960Mbps

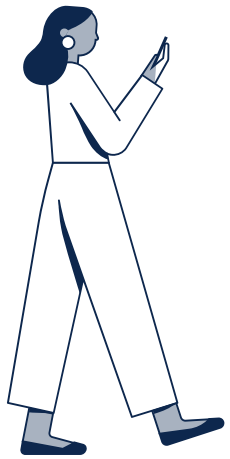
≈4min

2021

based on 2x2 6GHz Laptop // 60% in 2.4GHz, 70% in 5GHz and 80% in 6GHz efficiency // 4K 110min Movie = 25GB

The typical user ticket if a Wi-Fi device is involved…

Wi-Fi does not work…



Does not work…permanent or transient?

Wi-Fi symbol shows connection?

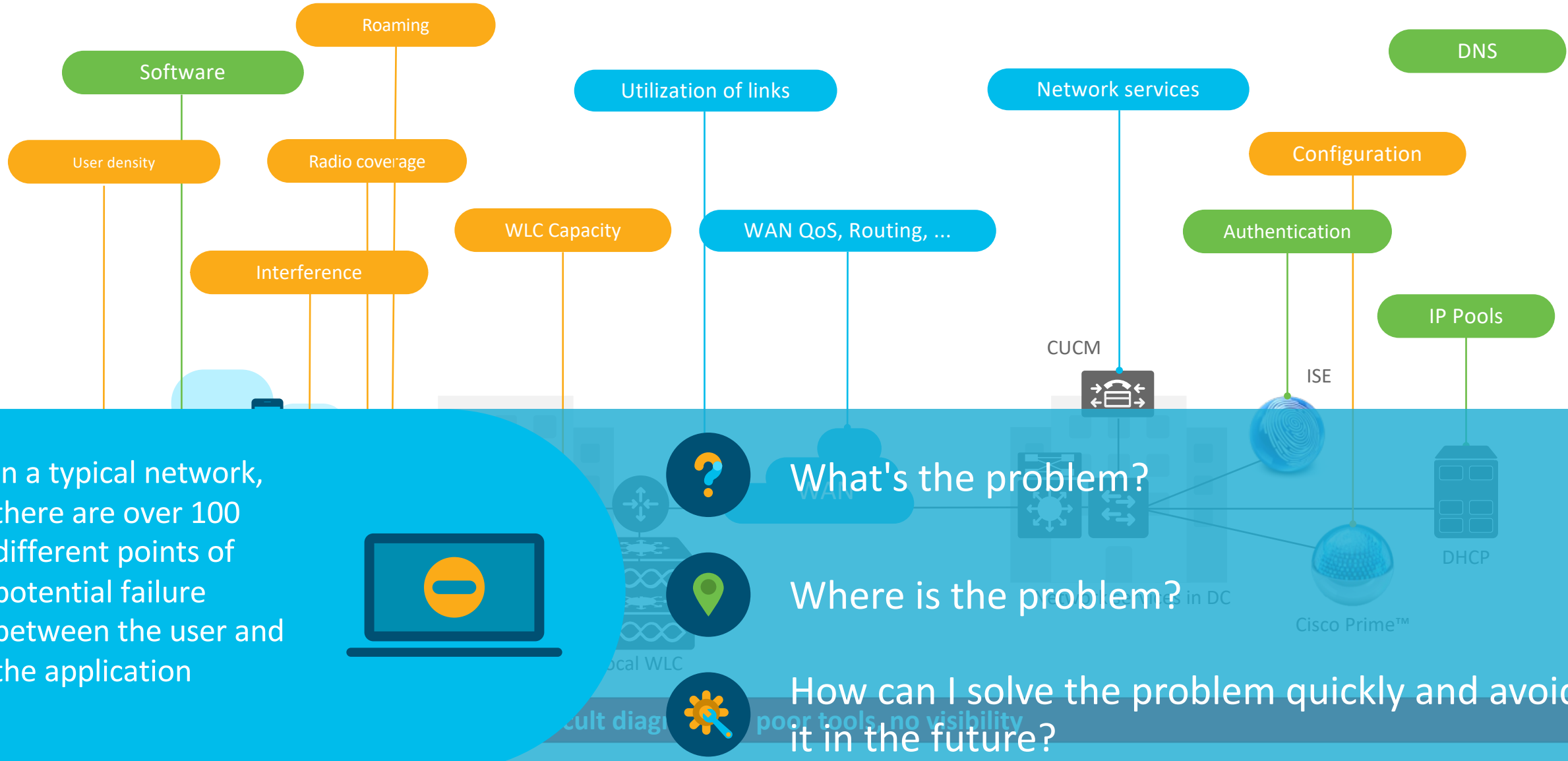
Which device?

Do you have an IP Address?

Can you reach the Internet?

Is it all or a specific application?

Network monitoring and diagnostics are difficult and complex



In a typical network, there are over 100 different points of potential failure between the user and the application

What's the problem?

Where is the problem?

How can I solve the problem quickly and avoid it in the future?

Challenge for IT departments: An IT specialist spends 43% of the time on average on diagnostics

"I don't have time to think"

Maintenance teams spend 4 times more time collecting diagnostic data than analyzing and concluding it

"Everything works fine for me"

The maintenance teams cannot reproduce the problem quickly and easily or are unable to diagnose it in real time. They also do not have access to the history of the network, user and application work.

"Is it slow? I don't know where the problem is. "

Problems with the quality of the user's work (user experience) are very difficult to diagnose due to the "blurring" of responsibilities, the number of points where problems may appear and the lack of measures to assess the quality of the service

Elements of diagnostics and monitoring of WiFi networks

1.

Client, AP or application diagnostics (Client, Device, Application Health)

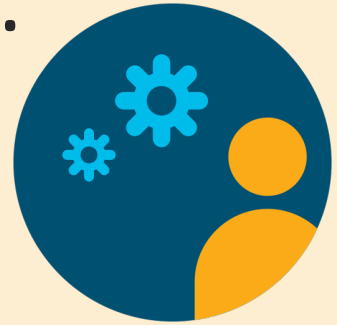
Identifying the problem and providing the administrator with information and diagnostic tools embedded in the context of the problem being solved. Hints. Analyzes. Conclusions.

2.

Wireless network performance parameters (Network Health)

Basic and intuitive (easy to understand) measures of the performance quality and efficiency of WiFi networks and network services (AAA / DHCP). Real-time reporting with trend observation.

3.



Visualization of the wireless network (Maps & Topology)

Visualization of the physical layer of the network as well as clients and disturbances operating in the network. Wireless network layer (What and where does it work and what is it connected with?)

4.

Proactive network diagnostics (WiFi Sensors& Notifications)

The use of wireless sensors for proactive network monitoring. Reduce the diagnostic time from days to minutes. Detecting the problem before it occurs (prevention).

5.

Observation of trends in the wireless network (WiFi Trends)

Forecasting the state of network operation in the future and indicating in advance trends and problems that will affect its operation in the future.

A modern monitoring and diagnostic system should help people work faster, smarter and more efficiently

Demonstrations

Cisco Catalyst 9800

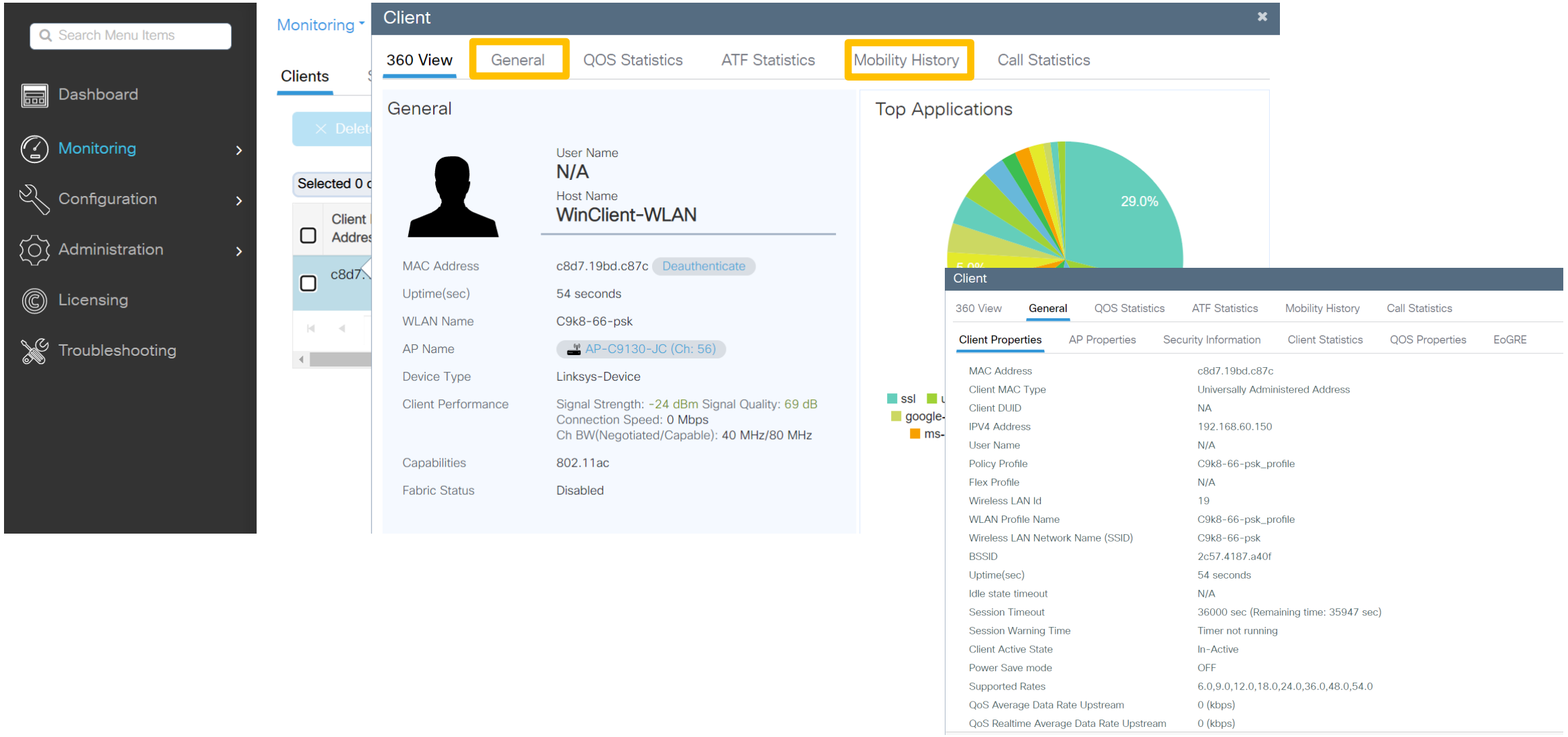
Cisco DNA Center

Client, AP or Application Diagnostics

Wireless client cannot connect

- Client with mac address <MAC1> is not able to join the wireless network
- Clients dropped from the wireless network earlier today at 10AM and recovered
- Some clients fail to connect after a failover

C9800 Client State Verification (WebUI)



C9800 Client State Verification (CLI)

show wireless client mac-address <CLIENT_MAC> detailed

```
Client MAC Address : <CLIENT_MAC>
Client MAC Type : Locally Administered Address
Client DUID: NA
Client IPv4 Address : <CLIENT_IPv4>
Client IPv6 Addresses : <CLIENT_IPV6>
Client Username: N/A
AP MAC Address : <AP_RADIO_MAC>
AP Name: 9120
AP slot : 1
Client State : Associated
Policy Profile : ppcentral150
Flex Profile : N/A
Wireless LAN Id: 11
WLAN Profile Name: 9800psk
Wireless LAN Network Name (SSID): 9800psk
BSSID : <AP_BSSID>
Connected For : 71 seconds
Protocol : 802.11ax - 5 GHz
Channel : 100
Client IIF-ID : 0xa0000001
Association Id : 1
…
```

```
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/06/2022 08:59:36
Central
Client Join Time:
  Join Time Of Client : 06/06/2022 08:59:36 Central
…
Policy Manager State: Run
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 71 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : FT-PSK
…
EAP Type : Not Applicable
VLAN Override after Webauth : No
VLAN : 150
Multicast VLAN : 0
…
```

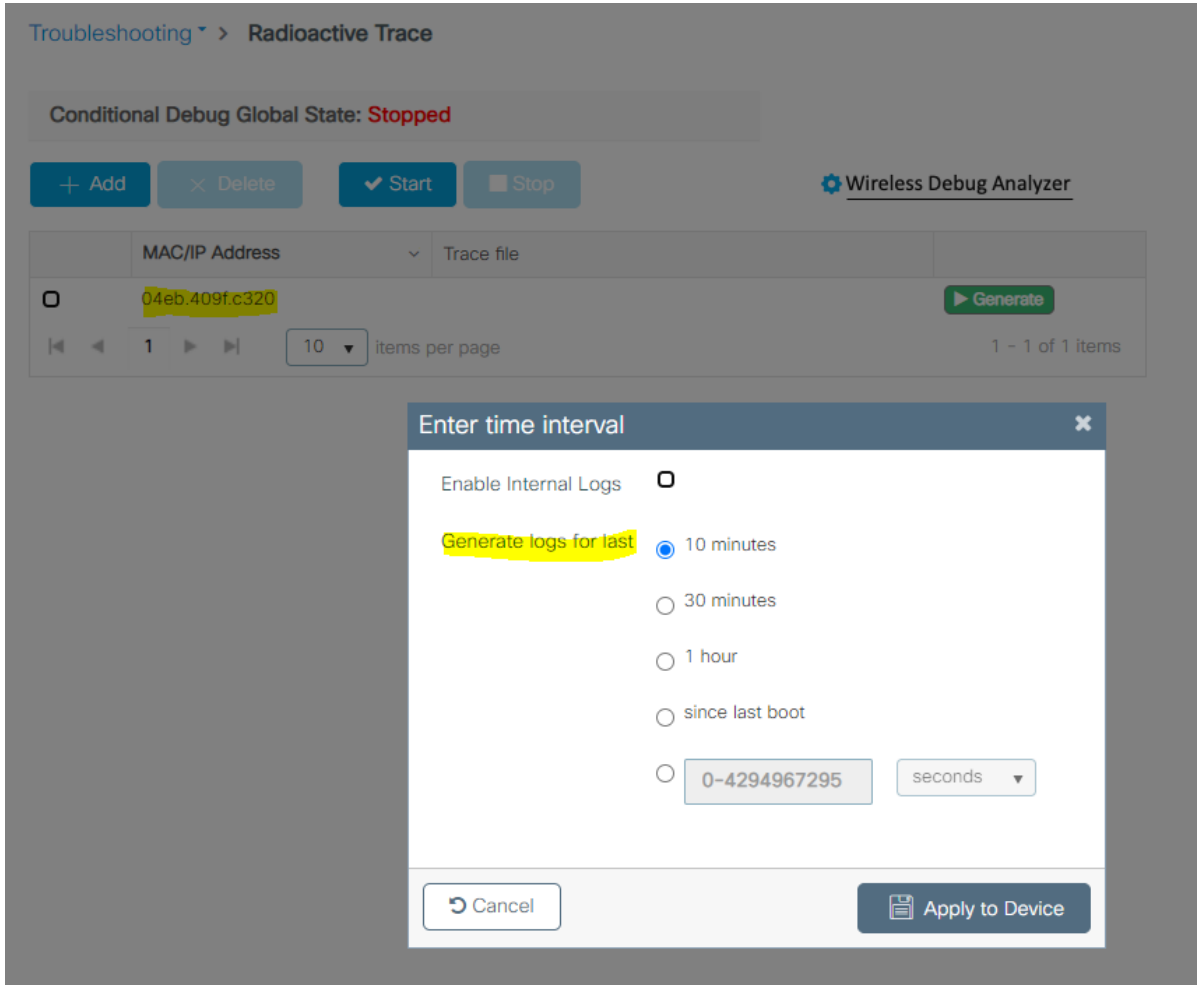
```
Session Manager:
…
  Resultant Policies:
            VLAN Name         : VLAN0150
            VLAN              : 150
            Absolute-Timer    : 1800

…
FlexConnect Data Switching : N/A
FlexConnect Dhcp Status : N/A
FlexConnect Authentication : N/A
Client Statistics:
  Number of Bytes Received from Client : 0
  Number of Bytes Sent to Client : 0
  Number of Packets Received from Client : 0
  Number of Packets Sent to Client : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -61 dBm
  Signal to Noise Ratio : 35 dB
```

show tech-support wireless client mac <CLIENT_MAC>

…. *for details across components*

Always-on Tracing



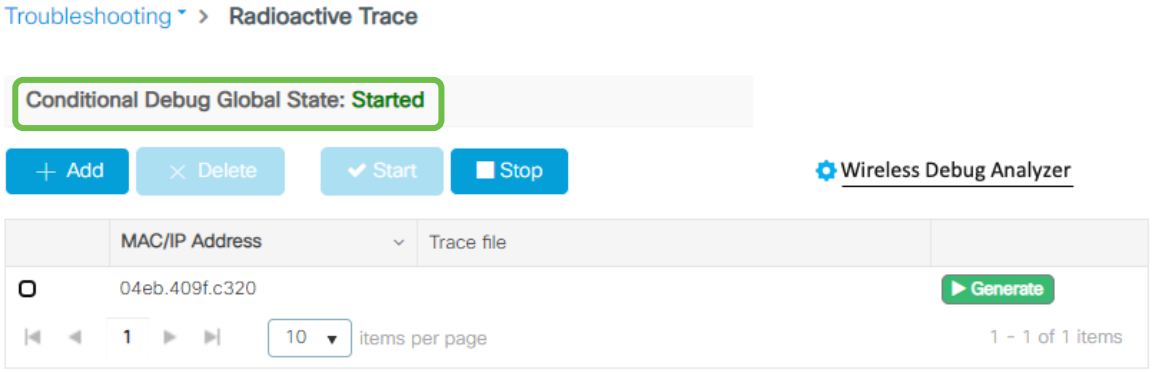
- Always-on traces and show help identify misconfigurations, errors and such
- GUI allows only conditional always-on traces
- CLI:
  show logging profile wireless to-file <>
  OR
  show logging process wncd
- By default, always-on traces from last 10 minutes are collected.
- You can choose duration over which to generate

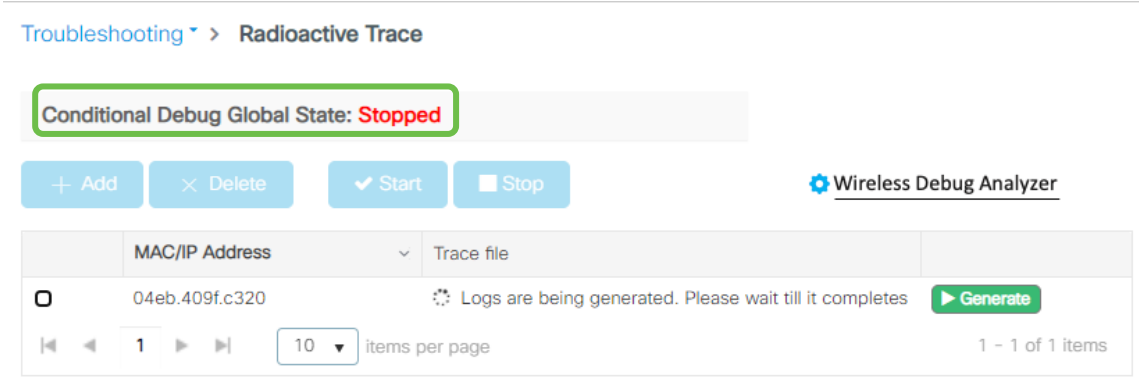
Always On: Failed Client Connection

show log profile wireless start last 10 minutes filter mac <CLIENT_MAC> to-file <FILENAME>.txt

```
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Association received. BSSID c064.e423.c64d, WLAN 9800psk, Slot 1 AP
c064.e423.c640, 9120
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
[dot11] [23554]: (note): MAC: c23f.ba14.984a  Association success. AID 1, Roaming = False, WGB = False, 11r = True, 11w = False Fast
roam = False
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
[client-auth] [23554]: (note): MAC: c23f.ba14.984a  L2 Authentication initiated. method PSK, Policy VLAN 150, AAA override = 0, NAC =
0
[ewlc-infra-evq] [23554]: (note): Authentication Success. Resolved Policy bitmap:11 for client c23f.ba14.984a
[client-auth] [23554]: (note): MAC: c23f.ba14.984a  ADD MOBILE sent. Client state flags: 0x71  BSSID: MAC: c064.e423.c64d capwap
IFID: 0x90000004, Add mobiles sent: 1
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [23554]: (ERR): MAC: c23f.ba14.984a  Keymgmt: Failed to eapol key m1 retransmit failure. Max retries for M1 over
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_EXCLUDE_WRONG_PSK,
details: , fsm-state transition 00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|07|15|1e|27|
[client-orch-sm] [23554]: (note): MAC: c23f.ba14.984a  Delete mobile payload sent for BSSID: c064.e423.c64d WTP mac: c064.e423.c640
slot id: 1
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_L2_AUTH_IN_PROGRESS ->
S_CO_DELETE_IN_PROGRESS
[errmsg] [23060]: (note): %CLIENT_EXCLUSION_SERVER-5-ADD_TO_EXCLUSIONLIST_REASON_DYNAMIC: R0/0: wncmgrd: Client MAC: c23f.ba14.984a
was added to exclusion list associated with AP Name:9120, BSSID:MAC: c064.e423.c64d, reason:Wrong PSK
[sanet-shim-translate] [23554]: (note): MAC: c23f.ba14.984a  Session manager disconnect event called, session label: 0x2b000002
[client-orch-state] [23554]: (note): MAC: c23f.ba14.984a  Client state transition: S_CO_DELETE_IN_PROGRESS -> S_CO_DELETED
```

RadioActive (RA) Tracing





- More detailed logs than always-on
- User has to intentionally enable debug level logs.
- Also called condition debugging as debug is enabled per context
- CLI equivalent

debug wireless {mac | ip}
Reproduce problem
no debug wireless {mac | ip}

RadioActive Trace – Association Failures

- Client sends disassociate

```
[client-orch-sm] [20370]: (info): MAC: <CLIENT_MAC>  Deleting the client, reason: 2,
CO_CLIENT_DELETE_REASON_DEAUTH_OR_DISASSOC_REQ, Client state S_CO_RUN
[client-orch-sm] [20370]: (note): MAC: <CLIENT_MAC>  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_DEAUTH_OR_DISASSOC_REQ, fsm-state transition
00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|07|13|17|18|28|33|42|44|46|48|4d|5c|5e|7f|a4|
```

- Data Rate Mismatch in Client Association Request

```
[dot11-validate] [23406]: (ERR): MAC: <CLIENT_MAC>  Dot11 validate radio rates. Missing Supported Rate for
index = 5, encode value: 12, radio type: DOT11_RADIO_TYPE_BG
```

- AP has max clients connected

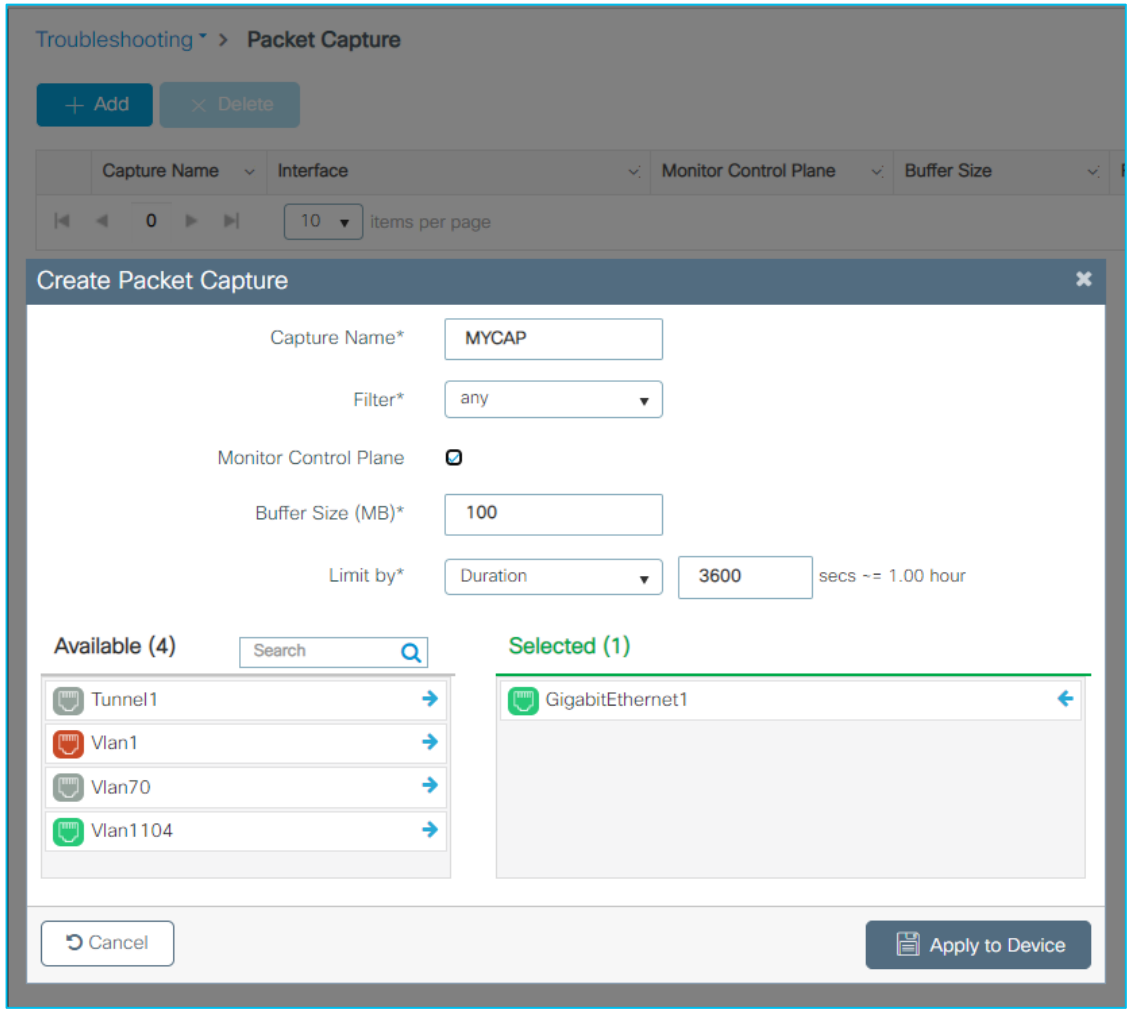
```
[ewlc-infra-evq] [17707]: (ERR): <CLIENT_MAC> CLIENT_ASSOC_FAIL Failure = IE_POST_VALIDATION_FAILURE
Validation Failure Type = 17, WLAN profile = WLAN1, Policy profile = POLICY1
[dot11] [17707]: (ERR): MAC: <CLIENT_MAC> Dot11 update co assoc fail. Sent assoc failure to CO. delete
reason: 41, CO_CLIENT_DELETE_REASON_DOT11_MAX_STA
[client-orch-sm] [17707]: (note): MAC: <CLIENT_MAC>  Client delete initiated. Reason:
CO_CLIENT_DELETE_REASON_DOT11_MAX_STA, fsm-state transition
00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|08|10|
```

Troubleshooting on the AP side

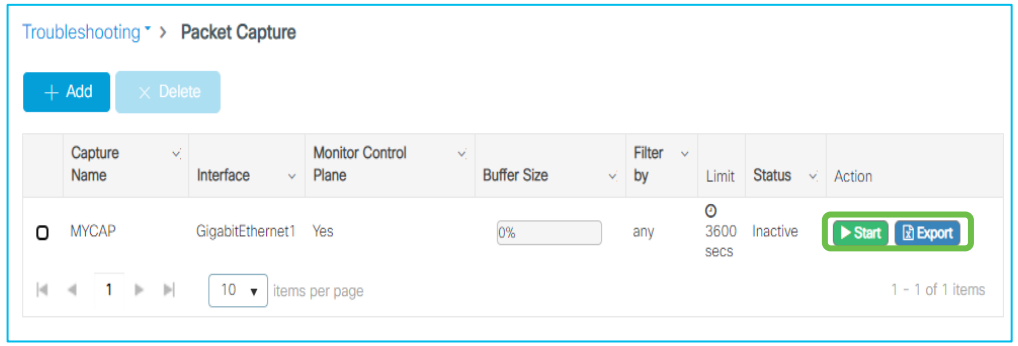
Debugs and Packet Traces on wave 2 / Wi-Fi6 APs

- Syslogs are stored in the flash even after reboot
- It is possible to export debugs to a syslog server
- **Debug client <mac>** is a macro that will trigger a control-plane sniffer capture. Various options exist to save as .pcap or export in hex
- Since 17.3, you can export an AP support bundle to the WLC
- **show client access-lists** allows to verify ACL and counters
- **Capture Packet Traces (Sniffer Traces)**
  - **Wired PCAP on AP Port**
  - **Radio Capture**
  - **Catalyst 91xx in Sniffer Mode**
- Much more at : https://www.cisco.com/c/en/us/support/docs/wireless/aironet-2800-series-access-points/214560-troubleshoot-wave-2-aps.html

Embedded Packet Capture (EPC)

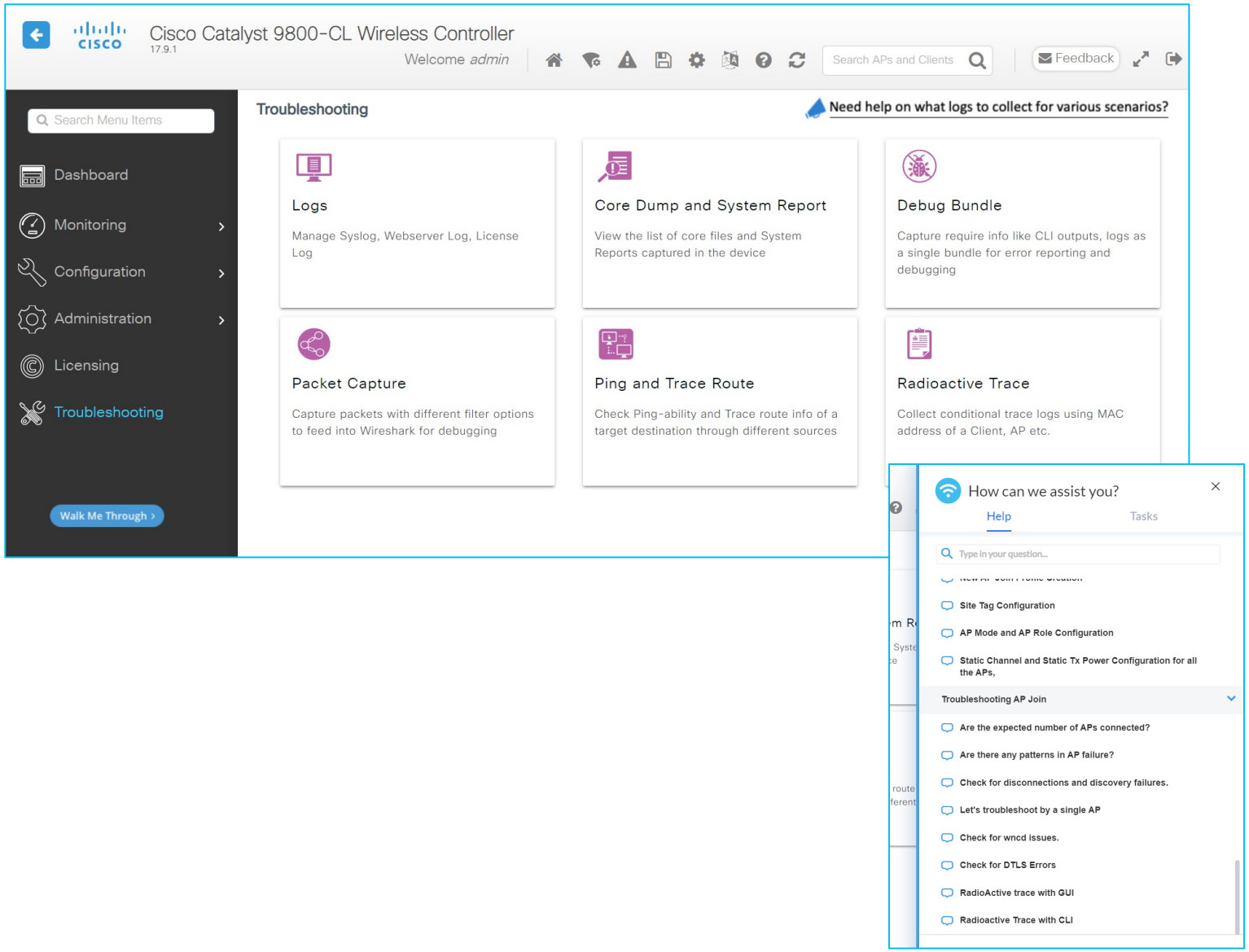


- Capture traffic from and to the C9800.
- Can be used to capture data traffic or control traffic or both
- Limited buffer = 100 MB (max)
- GUI incrementing adding filters already available in CLI

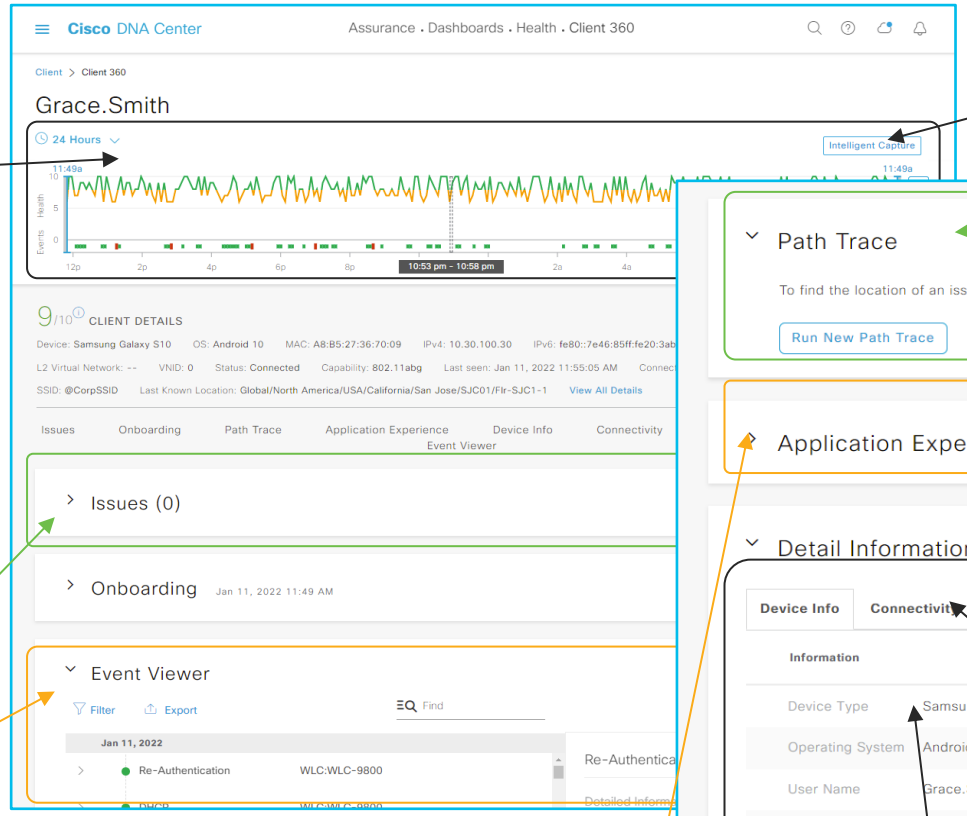


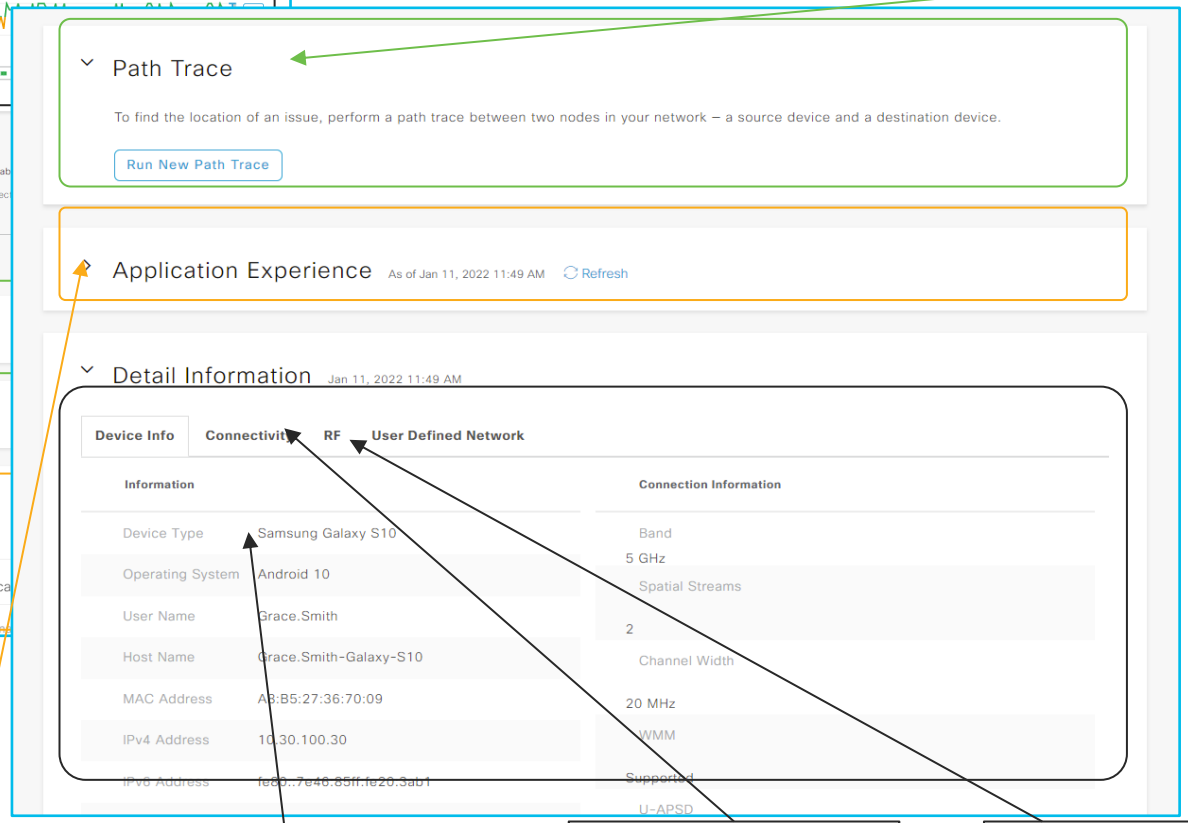
C9800 Client/AP troubleshooting –DEMO

- **C9800 GUI - Trobleshooting**
  - Client View
  - Radioactive Trace
  - Interactive help for AP troubleshooting



DNAC - Client 360 View





Connection details

Launch Intelligent Capture

Path Trace Tool for troubleshooting

Individual client issues

Onboarding event viewer

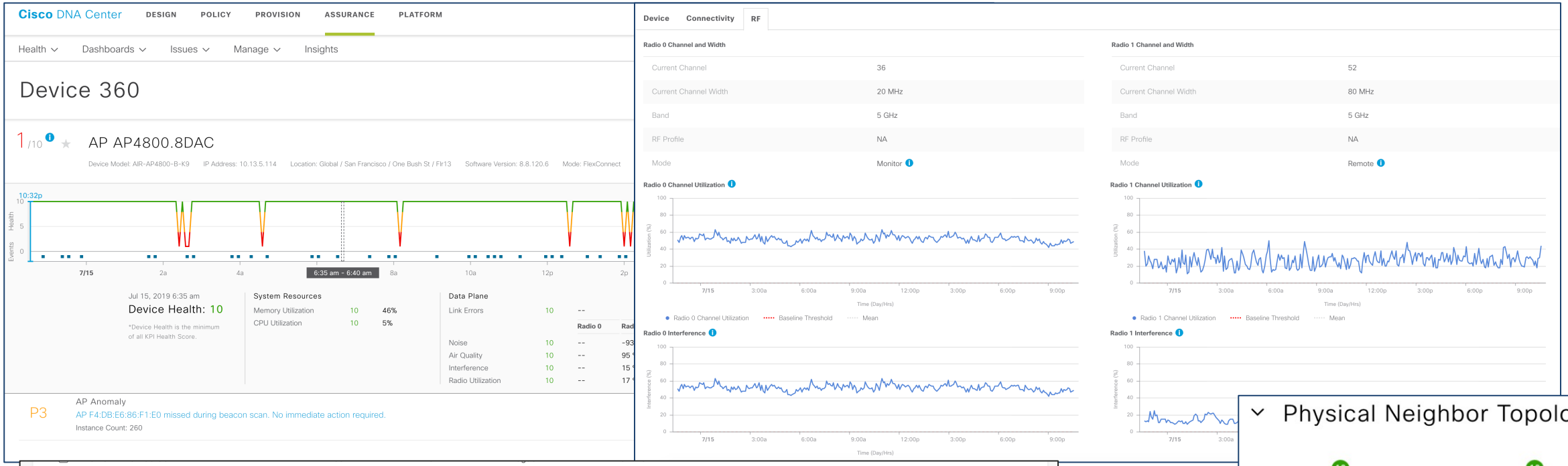
User application experience

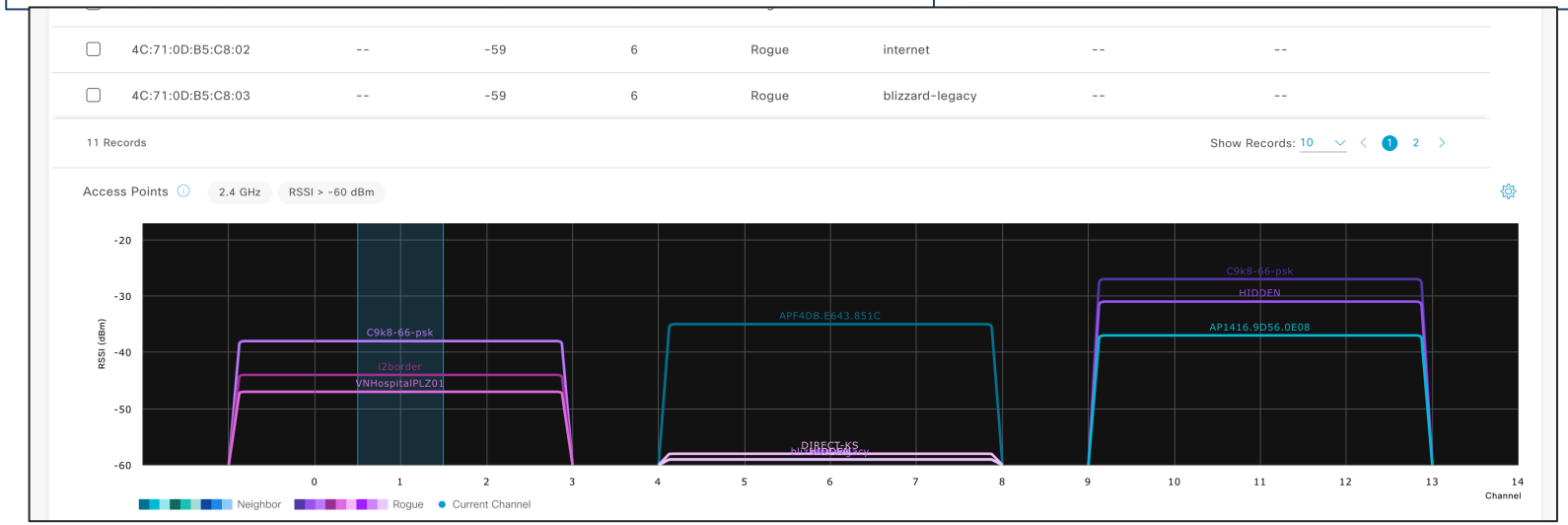
Apple/Intel client analytics

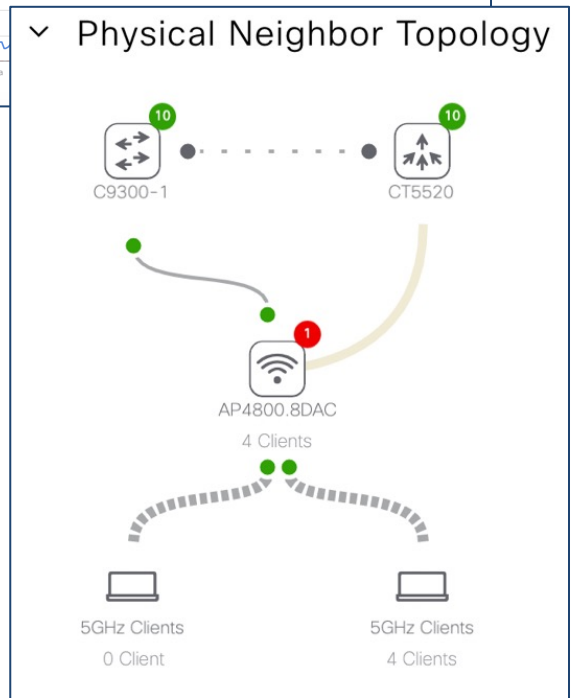
User connectivity details

RF as experienced by the user

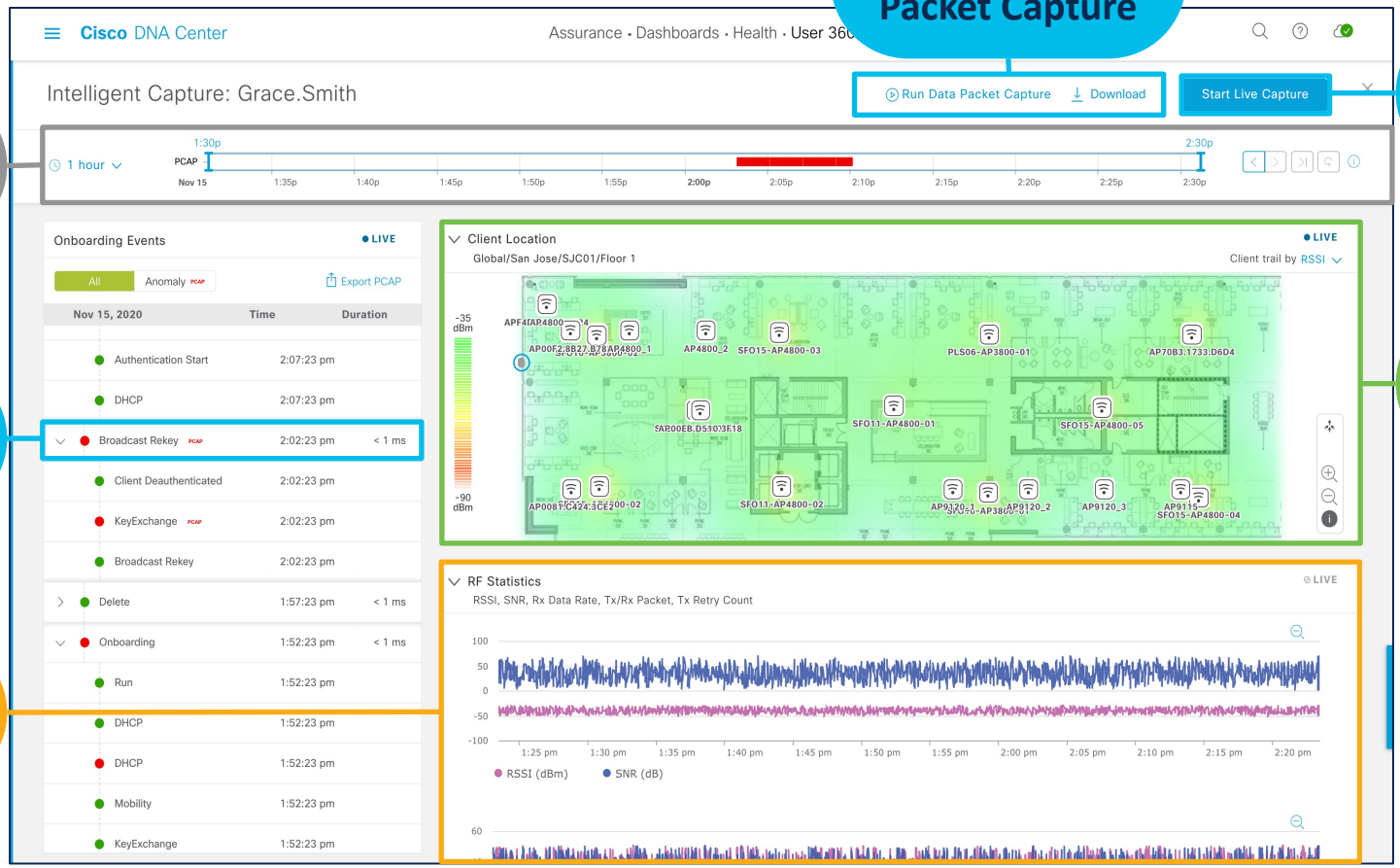
DNAC - AP Device 360 View







DNAC - Intelligent Capture
Client Dashboard



Data Packet Capture

Live Packet Capture

14 Day Time Travel

Anomaly Packet Capture

Client Statistics

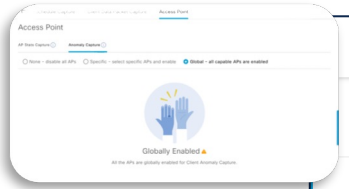
Real-Time Client Location

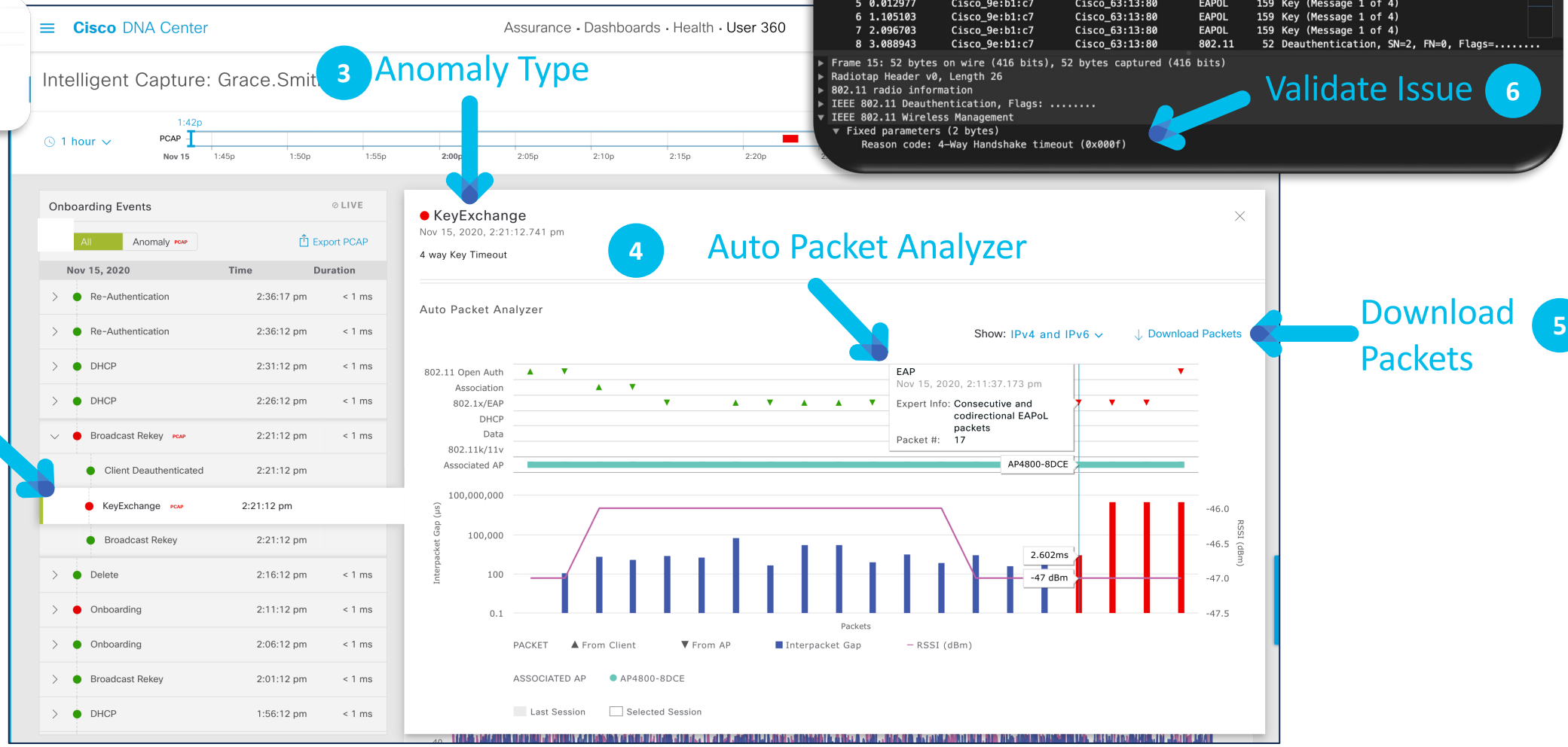
Navigation: [Open Menu] > Assurance > Health > Client > [Select Client] > Intelligent Capture

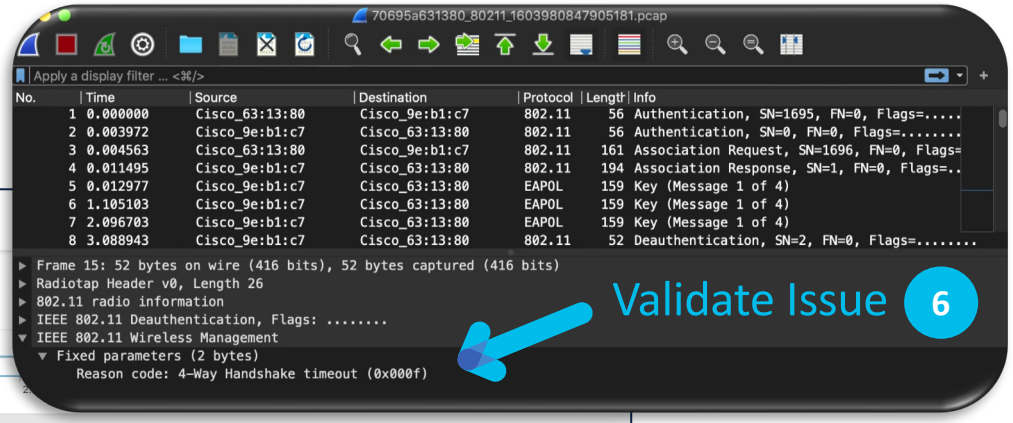
Always-on Anomaly Capture

Discover and root case issues

1 Enable Anomaly Capture







2 Anomaly Event Packet Capture

Download Packets 5

Event Legend:

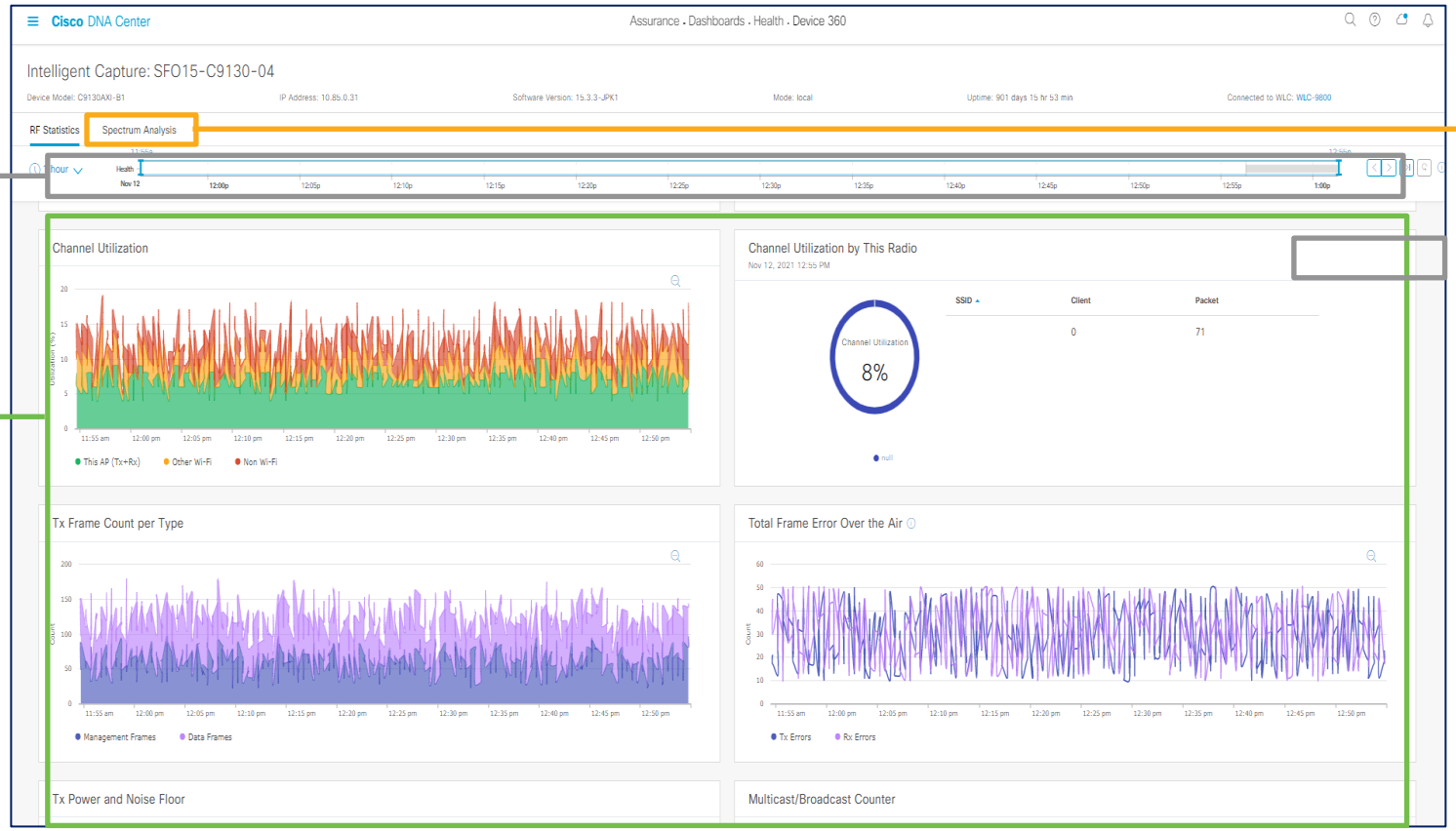
Red = Anomaly event

Green = Healthy event

DNAC - Intelligent Capture
AP Dashboard

14 Day Time Travel

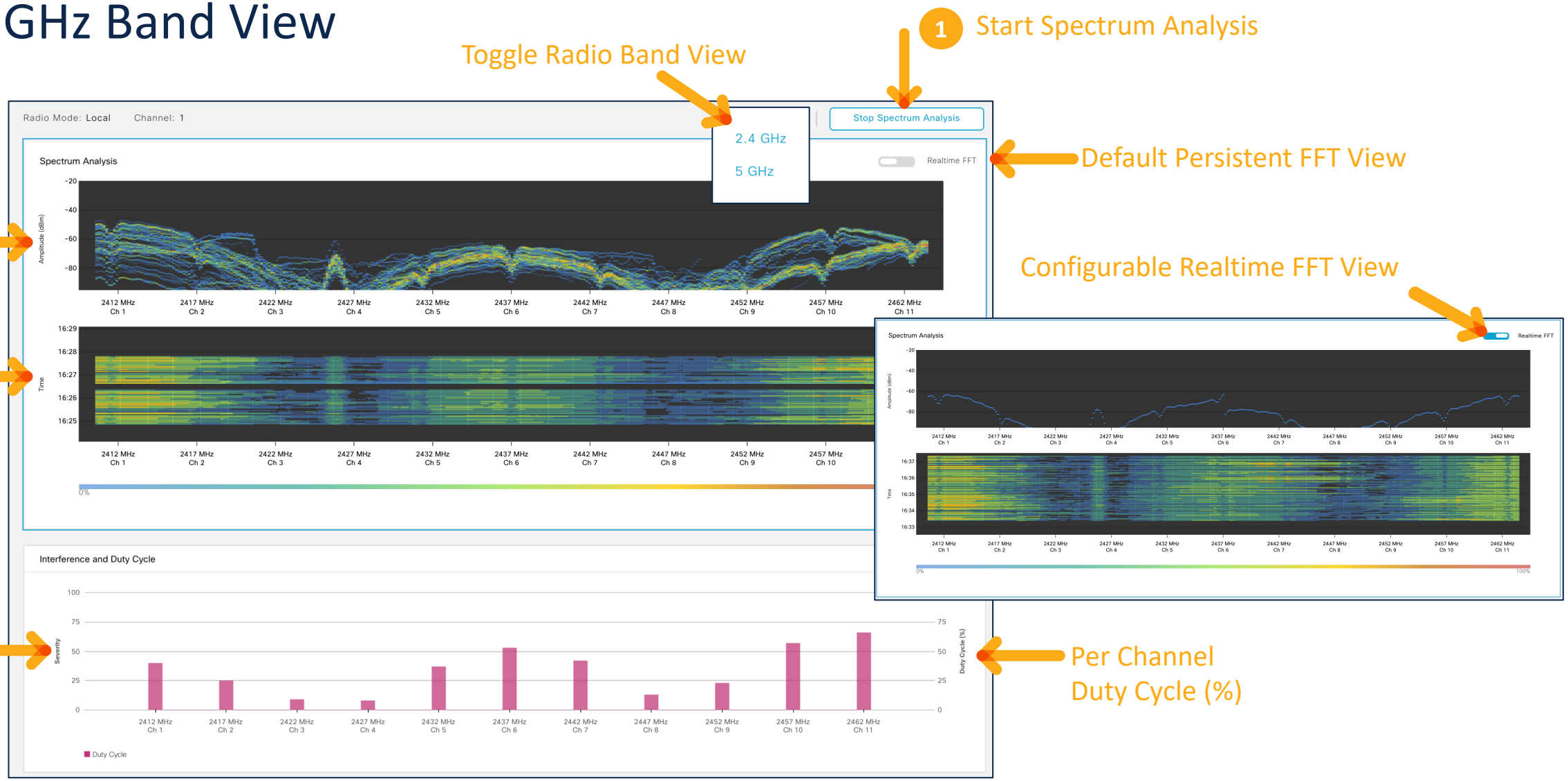
Always-on AP RF Statistics



On-demand Spectrum Analysis

Navigation: [Open Menu] > Assurance > Health > Access Points > [Select AP] > Intelligent Capture

On-demand Spectrum Analysis
2.4 GHz Band View

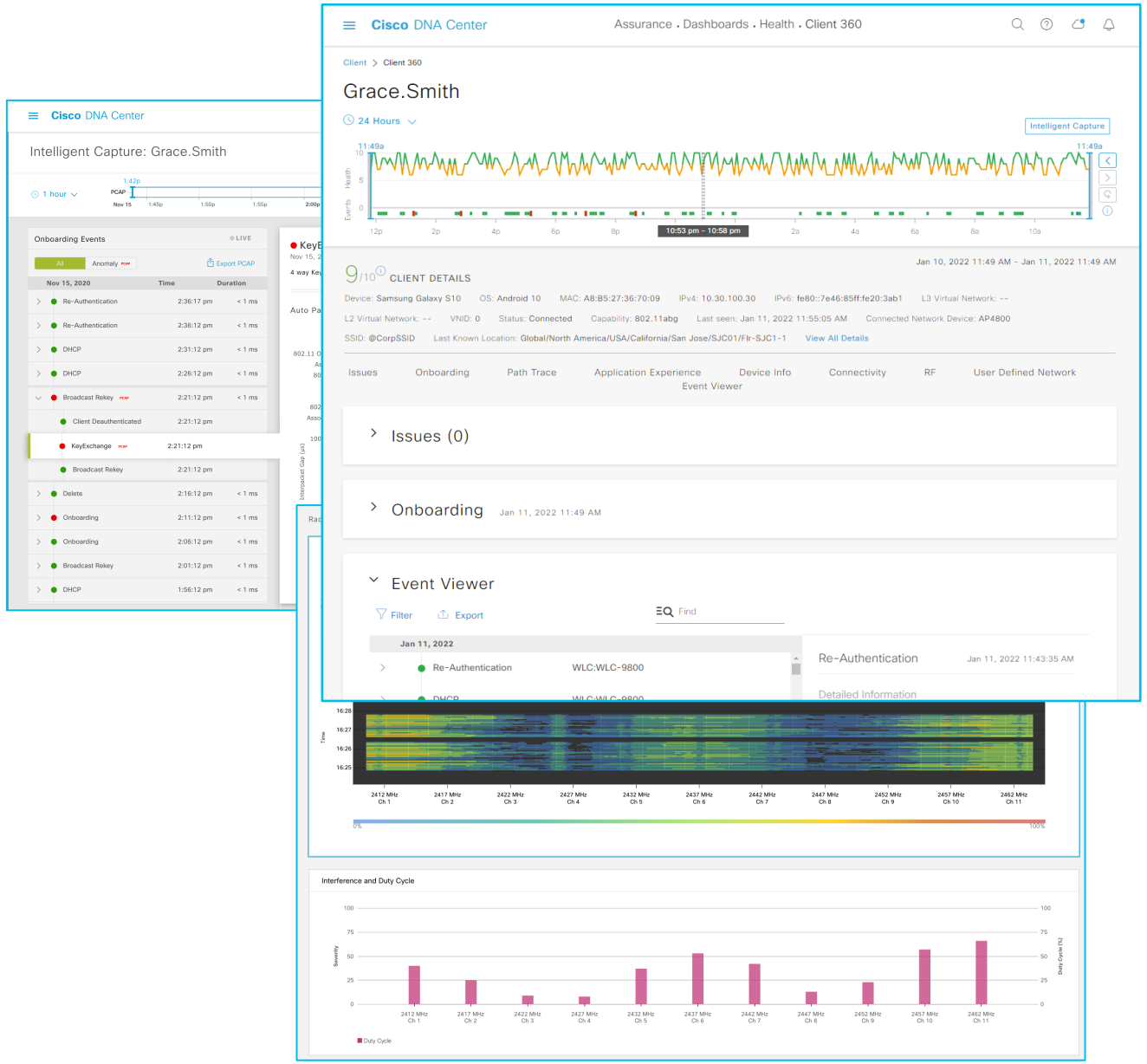


Navigation: [Open Menu] > Assurance > Health > Network > [Select AP] > Intelligent Capture > Spectrum Analysis

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

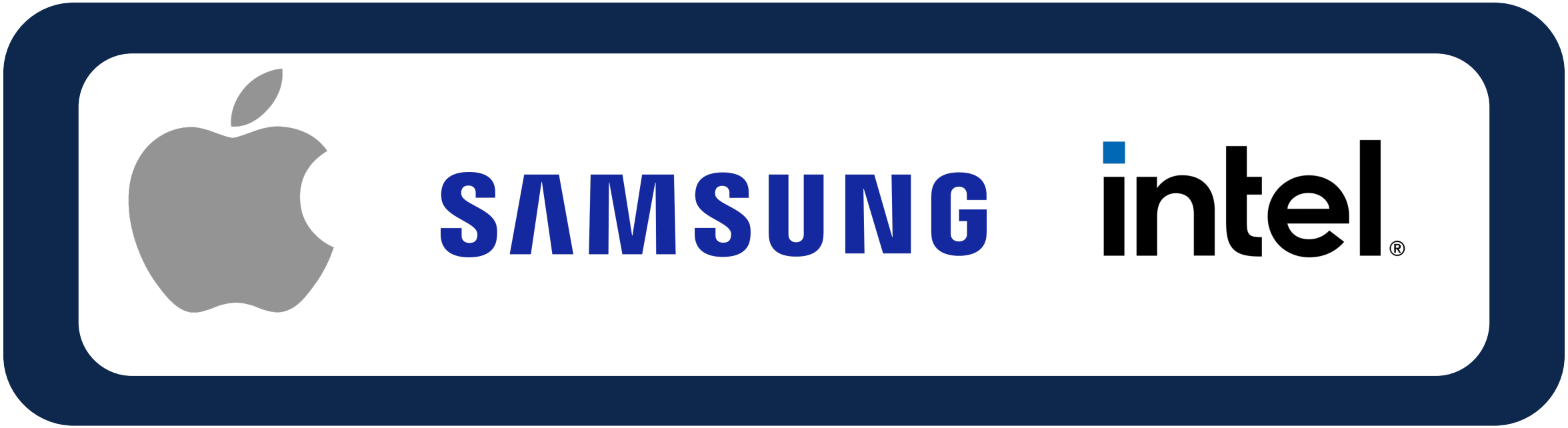
DNAC Client & Device 360 View, Intelligent Capture – DEMO

- **DNAC Client & AP Monitoring**
  - Client health charts
  - 360 Client and Device View
- **DNAC Intelligent Capture**
  - Always-on Anomaly Capture
  - Full Packet Capture
  - On-demand Spectrum Analysis



Cisco Device Ecosystem Partners

Client-side Benefits Only Available to Cisco Wireless Networks

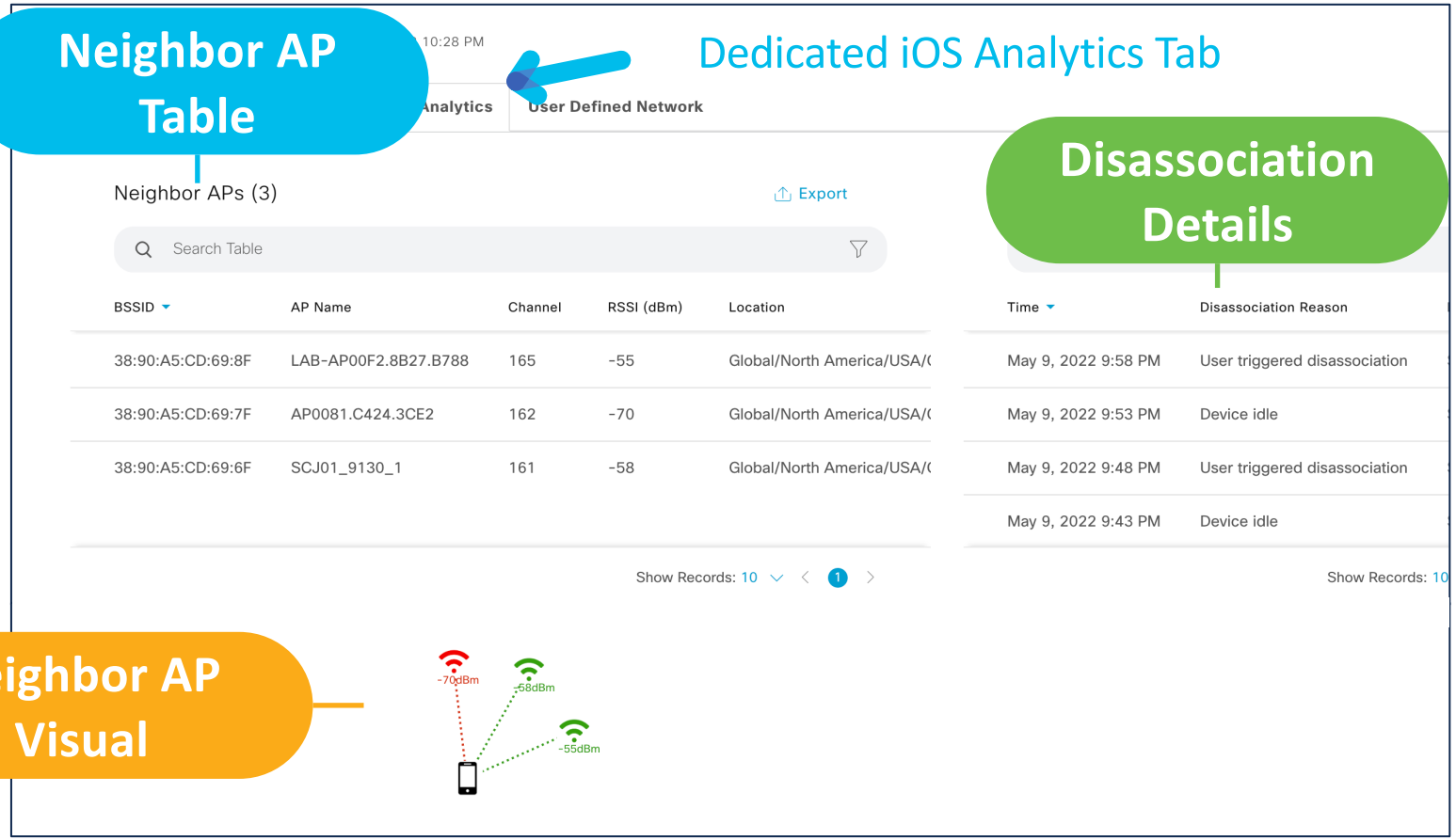


iOS Analytics, Fastlane, and Fastlane+ Overview

Recommended with Cisco DNA Center 2.2.1

iOS Analytics, Fastlane and Fastlane+

- iOS Analytics:
  - Detailed disassociate reasons
  - Neighboring APs, BSSID, RSSI
  - Enhanced device classification
- Fastlane & Fastlane+
  - Improved voice and video experience.

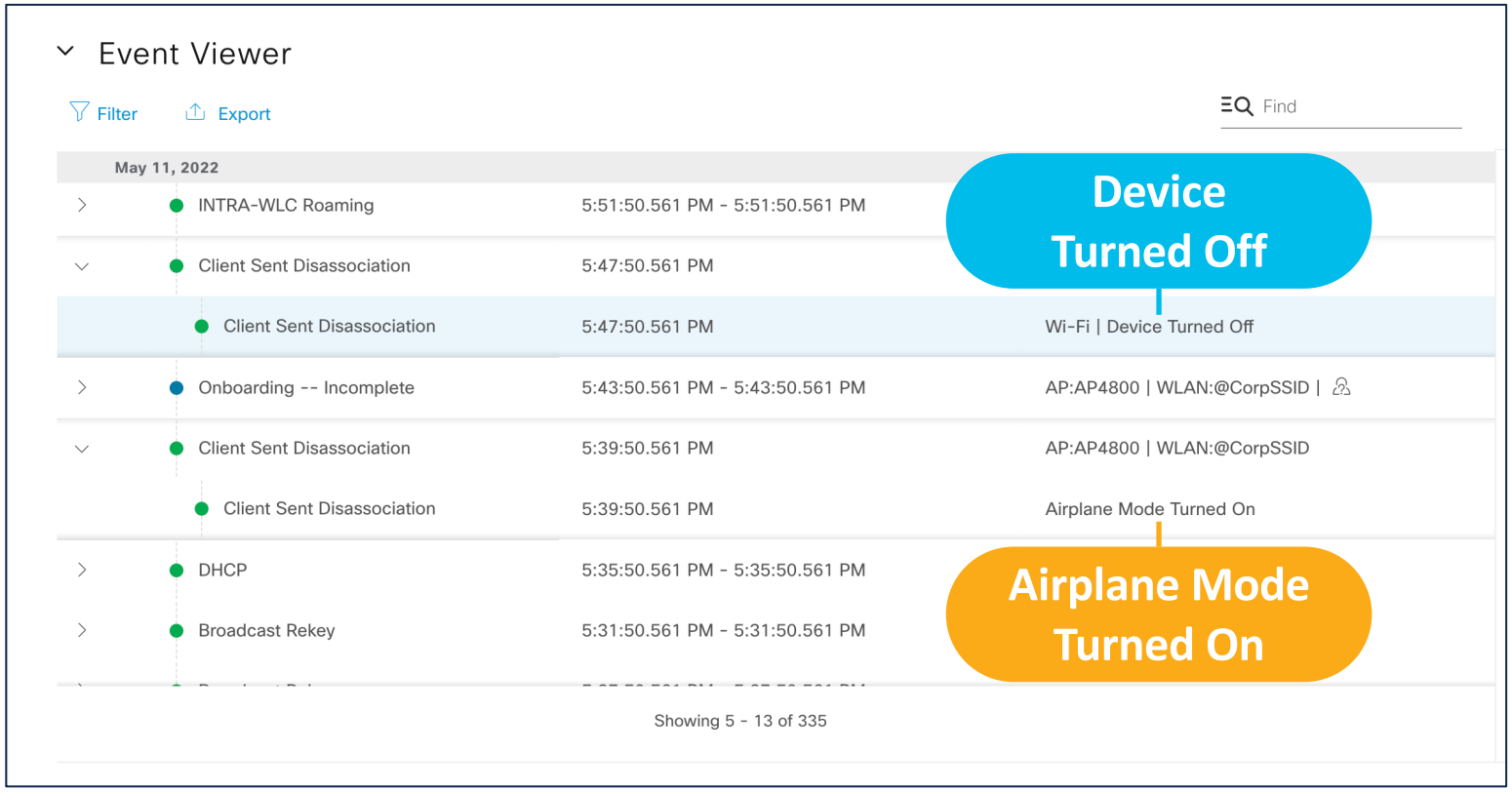


Samsung Analytics Overview

Recommended with Cisco DNA Center 2.2.1 and IOS XE 17.1.1

SAMSUNG Analytics

- Detailed disassociate reasons
- Enhanced device classification



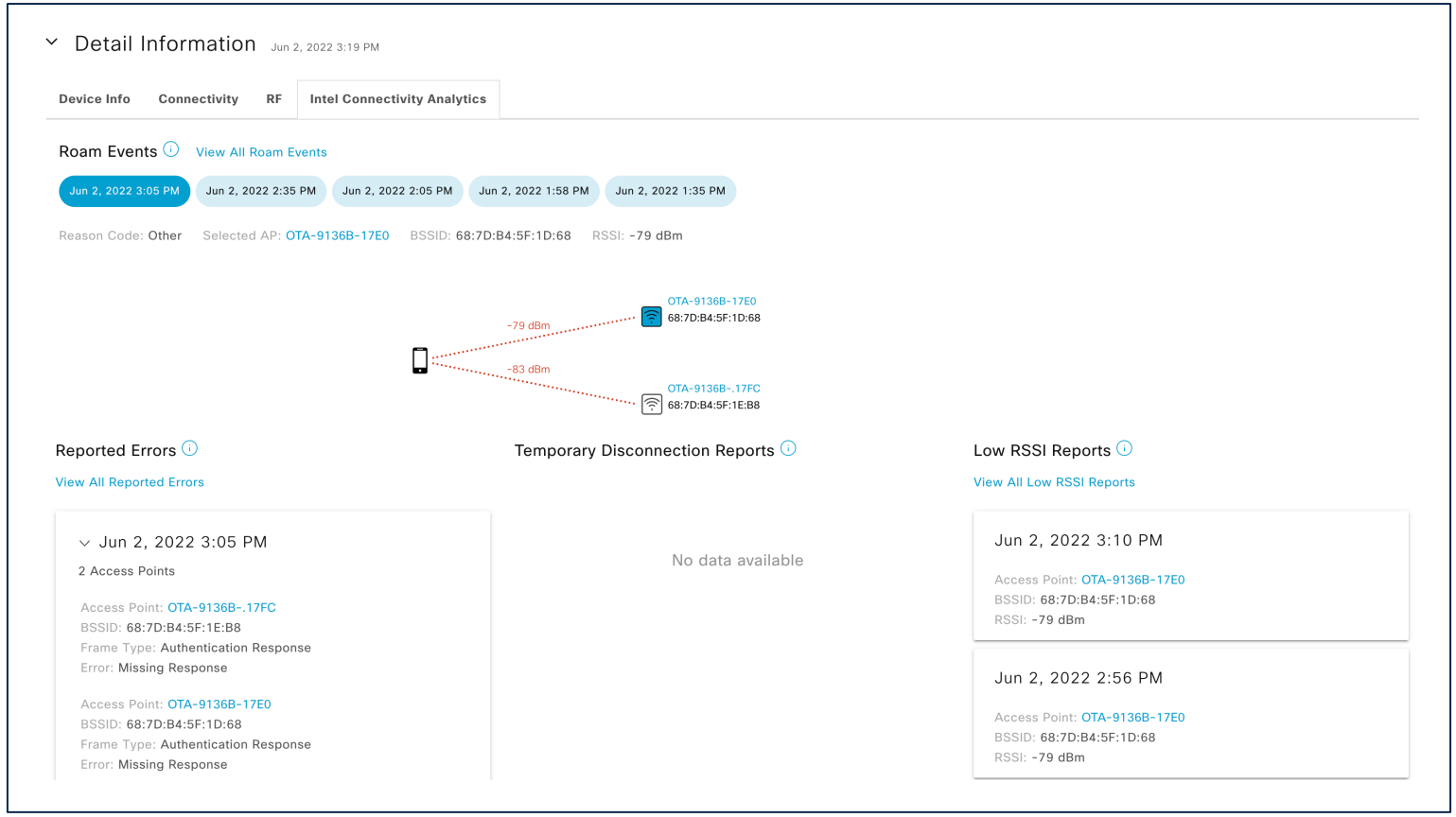
Intel Connectivity Analytics Overview

from Cisco DNA Center 2.3.3 and IOS XE 17.6.1

intel Connectivity Analytics

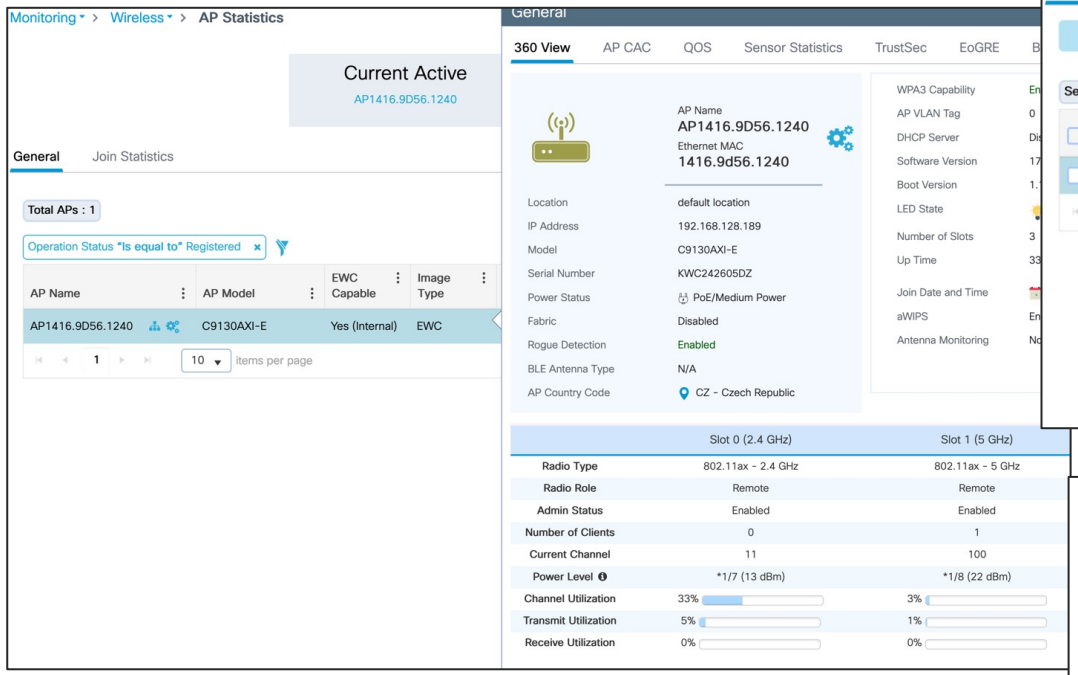
New in 2021!

- Issue reporting, roam and disassociate reasons
- Neighboring APs, BSSID, RSSI
- Enhanced device classification

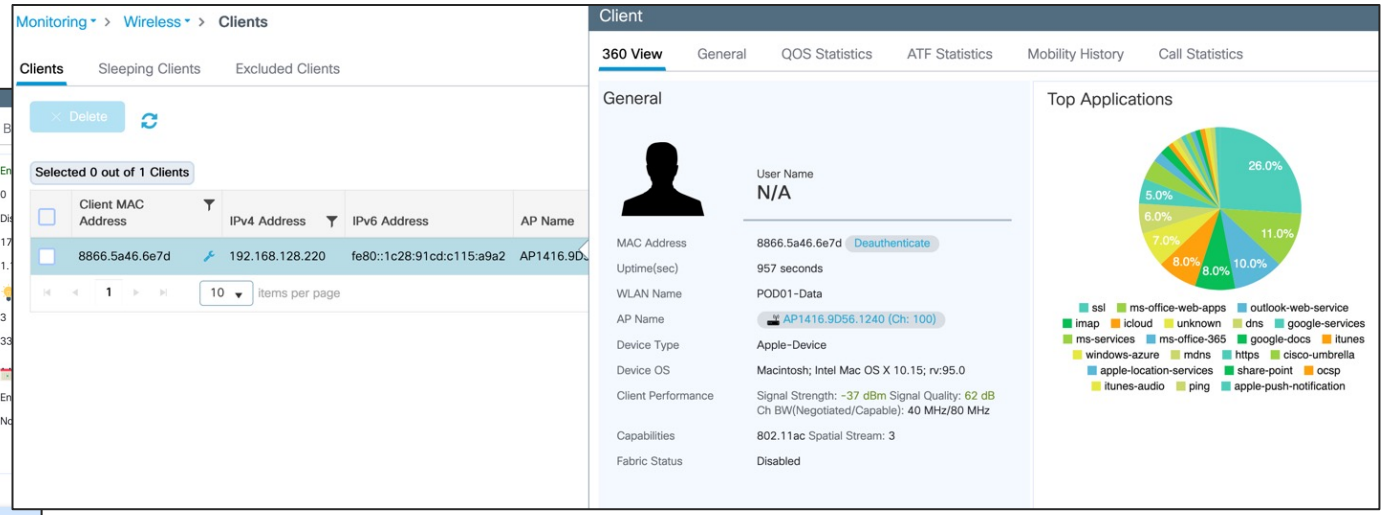


Wireless network performance parameters

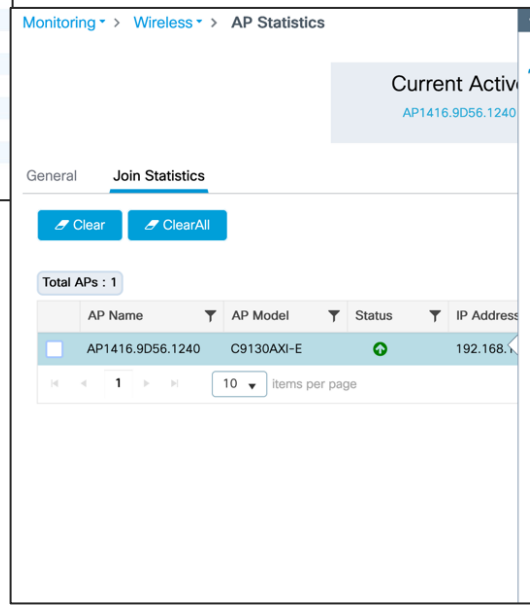
WLC Metrics

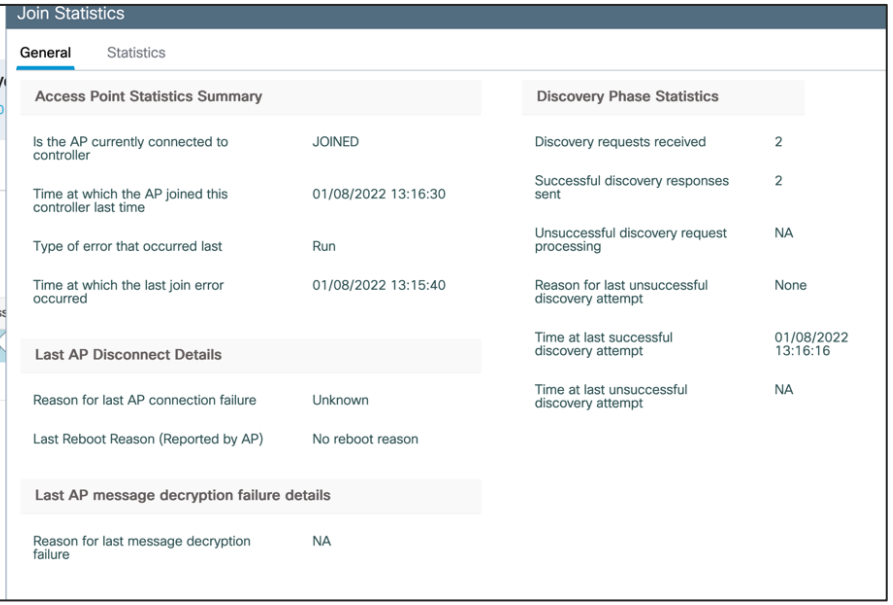

Monitoring > Wireless > AP Statistics
Current Active
AP1416.9D56.1240
General
Join Statistics
Total APs : 1
Operation Status "Is equal to" Registered
AP Name
AP Model
EWC Capable
Image Type
AP1416.9D56.1240
C9130AXI-E
Yes (Internal)
EWC
items per page

General
360 View
AP CAC
QOS
Sensor Statistics
TrustSec
EoGRE
AP Name
AP1416.9D56.1240
Ethernet MAC
1416.9d56.1240
Location
default location
IP Address
192.168.128.189
Model
C9130AXI-E
Serial Number
KWC242605DZ
Power Status
PoE/Medium Power
Fabric
Disabled
Rogue Detection
Enabled
BLE Antenna Type
N/A
AP Country Code
CZ - Czech Republic
WPA3 Capability
AP VLAN Tag
DHCP Server
Software Version
Boot Version
LED State
Number of Slots
Up Time
Join Date and Time
aWIPS
Antenna Monitoring
Slot 0 (2.4 GHz)
Slot 1 (5 GHz)
Radio Type
802.11ax - 2.4 GHz
802.11ax - 5 GHz
Radio Role
Remote
Admin Status
Enabled
Number of Clients
Current Channel
Power Level
Channel Utilization
Transmit Utilization
Receive Utilization


Monitoring > Wireless > Clients
Clients
Sleeping Clients
Excluded Clients
Delete
Selected 0 out of 1 Clients
Client MAC Address
IPv4 Address
IPv6 Address
AP Name
8866.5a46.6e7d
192.168.128.220
fe80::1c28:91cd:c115:a9a2
items per page

Client
360 View
General
QOS Statistics
ATF Statistics
Mobility History
Call Statistics
General
User Name
N/A
MAC Address
8866.5a46.6e7d
Deauthenticate
Uptime(sec)
957 seconds
WLAN Name
POD01-Data
AP Name
AP1416.9D56.1240 (Ch: 100)
Device Type
Apple-Device
Device OS
Macintosh; Intel Mac OS X 10.15; rv:95.0
Client Performance
Signal Strength: -37 dBm Signal Quality: 62 dB
Ch BW(Negotiated/Capable): 40 MHz/80 MHz
Capabilities
802.11ac Spatial Stream: 3
Fabric Status
Disabled
Top Applications
26.0%
11.0%
10.0%
8.0%
8.0%
7.0%
6.0%
5.0%
ssl
ms-office-web-apps
outlook-web-service
imap
icloud
unknown
dns
google-services
ms-services
ms-office-365
google-docs
itunes
windows-azure
mdns
https
cisco-umbrella
apple-location-services
share-point
ocsp
itunes-audio
ping
apple-push-notification


Monitoring > Wireless > AP Statistics
Current Activ
AP1416.9D56.1240
General
Join Statistics
Clear
ClearAll
Total APs : 1
AP Name
AP Model
Status
IP Address
AP1416.9D56.1240
C9130AXI-E
items per page


Join Statistics
General
Statistics
Access Point Statistics Summary
Is the AP currently connected to controller
JOINED
Time at which the AP joined this controller last time
01/08/2022 13:16:30
Type of error that occurred last
Run
Time at which the last join error occurred
01/08/2022 13:15:40
Last AP Disconnect Details
Reason for last AP connection failure
Unknown
Last Reboot Reason (Reported by AP)
No reboot reason
Last AP message decryption failure details
Reason for last message decryption failure
NA
Discovery Phase Statistics
Discovery requests received
2
Successful discovery responses sent
2
Unsuccessful discovery request processing
NA
Reason for last unsuccessful discovery attempt
None
Time at last successful discovery attempt
01/08/2022 13:16:16
Time at last unsuccessful discovery attempt
NA

IOS-XE Tracing Levels

- ERROR level represent abnormal situations. We want to raise the user attention to these
- WARNING represent an incident that could potentially lead to an error (or not…)
- NOTICE is the default logging level for binos daemons. It captures significant events if they are normal working conditions. (client connect, failover)
- INFO contains details about state machines and the communication flow
- DEBUG contains traces needed to root cause failure conditions

VERBOSE :

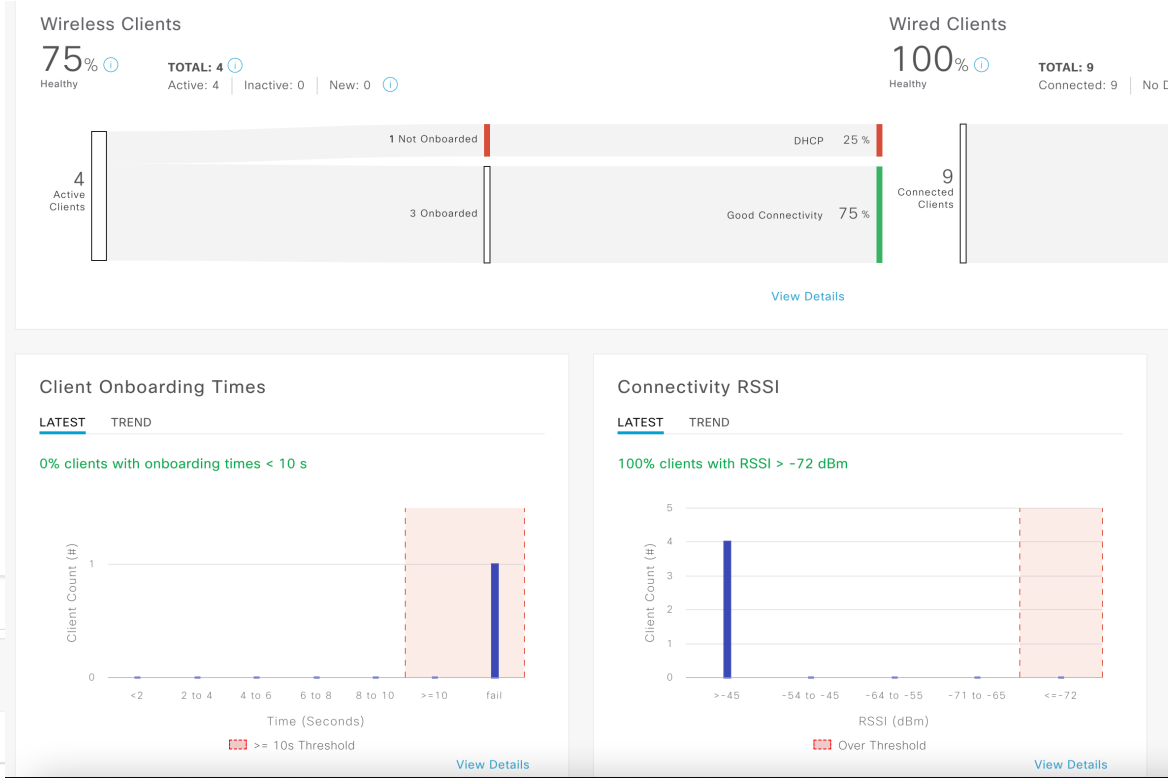
- INTERNAL is not a level but a flag on any log line when it is not meant to be understood by mere mortals but only by developers

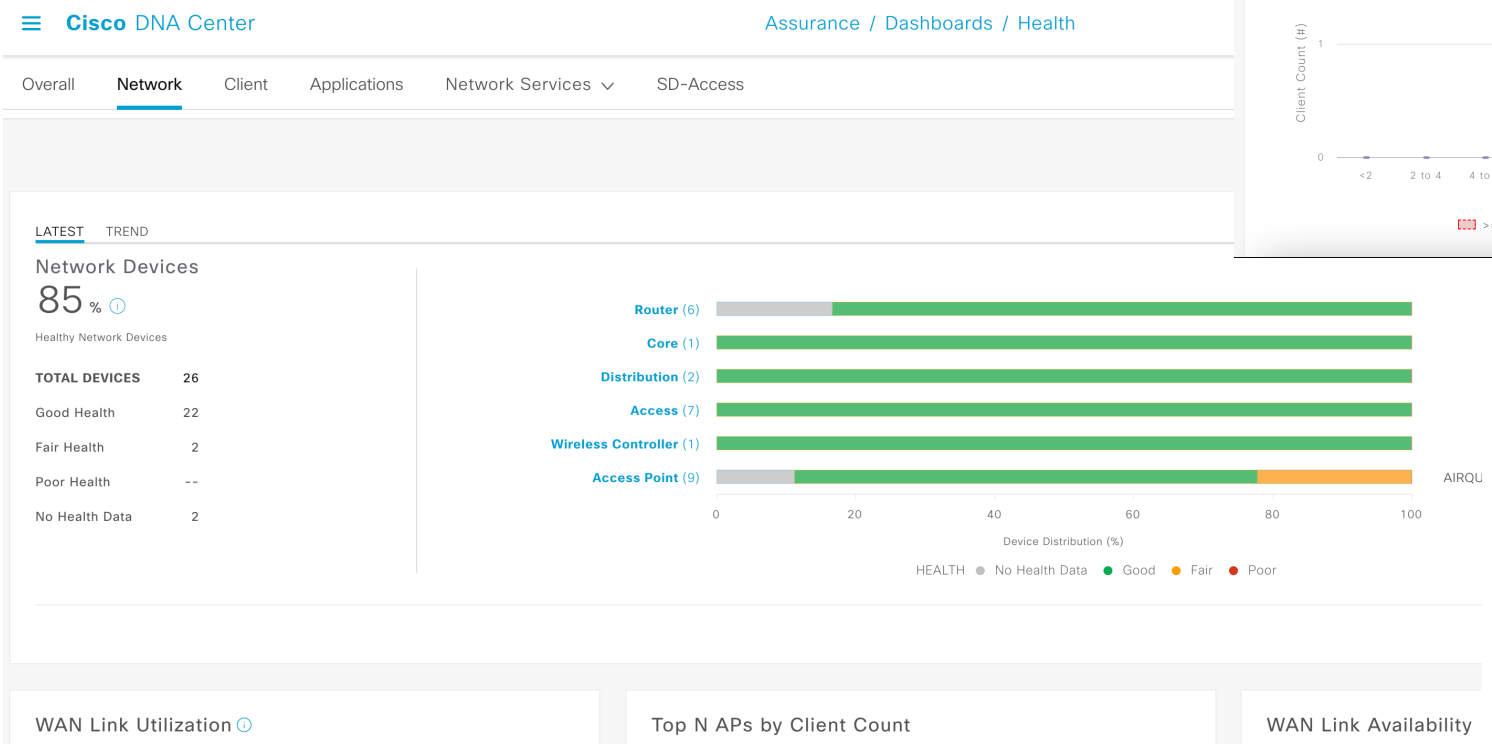
2-Critical
3-Error
4-Warning
5-Notice
6-Info
7-Debug
8-Verbose

Wireless Troubleshooting - Automation

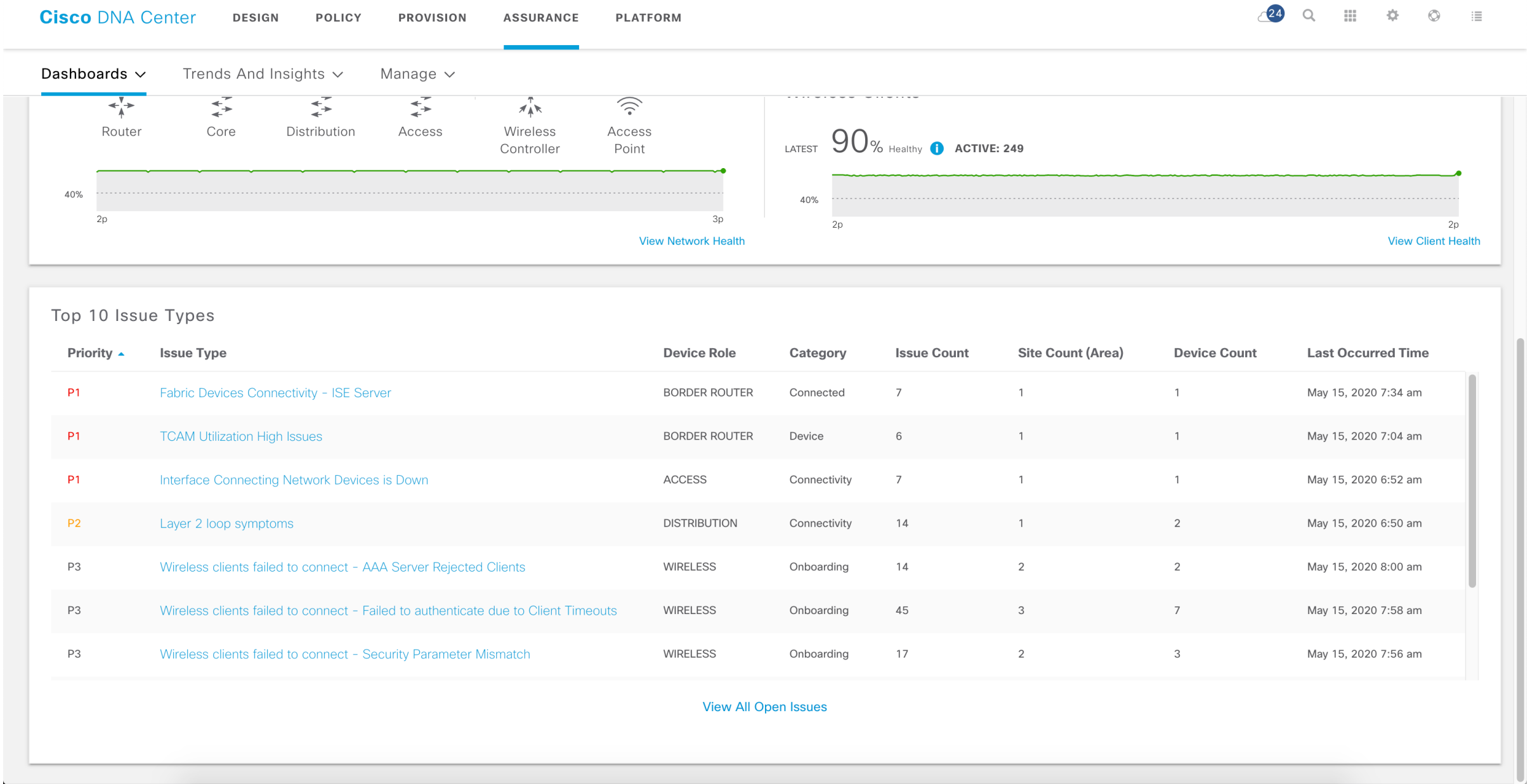
Why?	What?
Efficient Client Troubleshooting Wireless client troubleshooting requires lots of iterations to collect right information. This tool will help us to do all those steps in one shot, saving time and ensuring we get correlated logs and captures from 9800 WLC using Guestshell & Python Innovation.	▪ Automatic client RA traces, Packet Captures, & Summary of events using Guestshell python scripts ▪ Enabled on Multiple WLCs to capture IRCM ▪ DNAC : MRE workflow integration completed by Eng
Uninterrupted Embedded Packet Capture This tool will help to export packet capture buffer to a server without having to start and stop the capture, allowing to have continuous packet capture stored in server with different filenames to do forensic analysis with all the packets.	▪ Configure & Export rotatory packet capture on 9800 using Guestshell ▪ Continuous captures help when issue is random & Sporadic in nature ▪ MRE Workflow integration work in progress
Automated Archive request and export Based on recent learnings we need to enable verbose traces for complete 9800. This tool will help us to automate periodical archive traces and exports without requiring customer intervention.	▪ Configure & Export Archive traces from 9800 using EEM ▪ Periodical & timed log capture for efficient troubleshooting ▪ MRE Workflow integration work in progress
KPI Collector This tool will help to automate data collection (KPI or Action Plan), ensures we have the right data collected	▪ Run a set of commands and store info in the file using Python & Guestshell ▪ Tool will be able to collect outputs several times to monitor counter & Other KPI stats ▪ MRE Workflow integration work in progress

Network 360 View



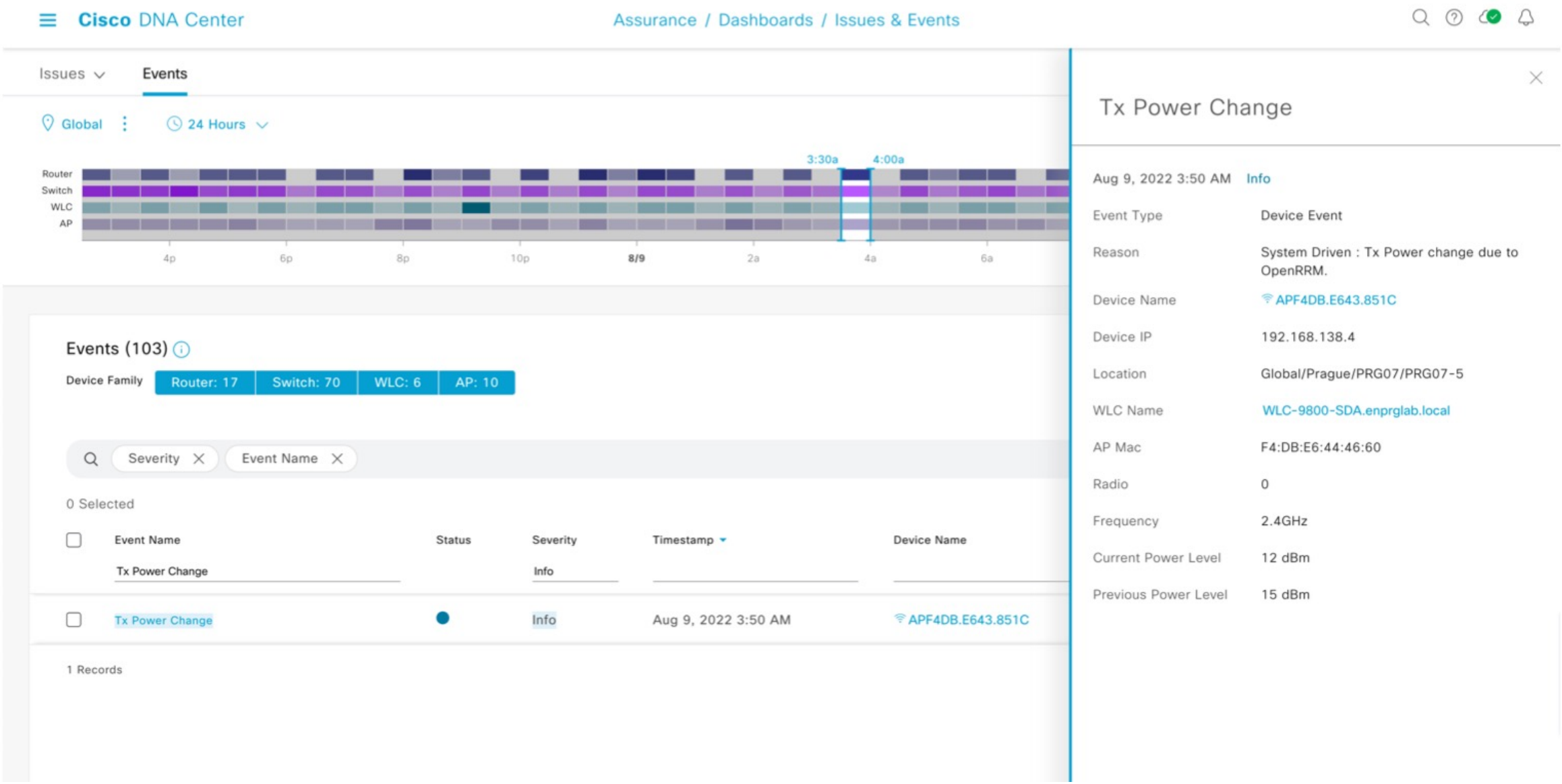


Issues and Guided Remediations

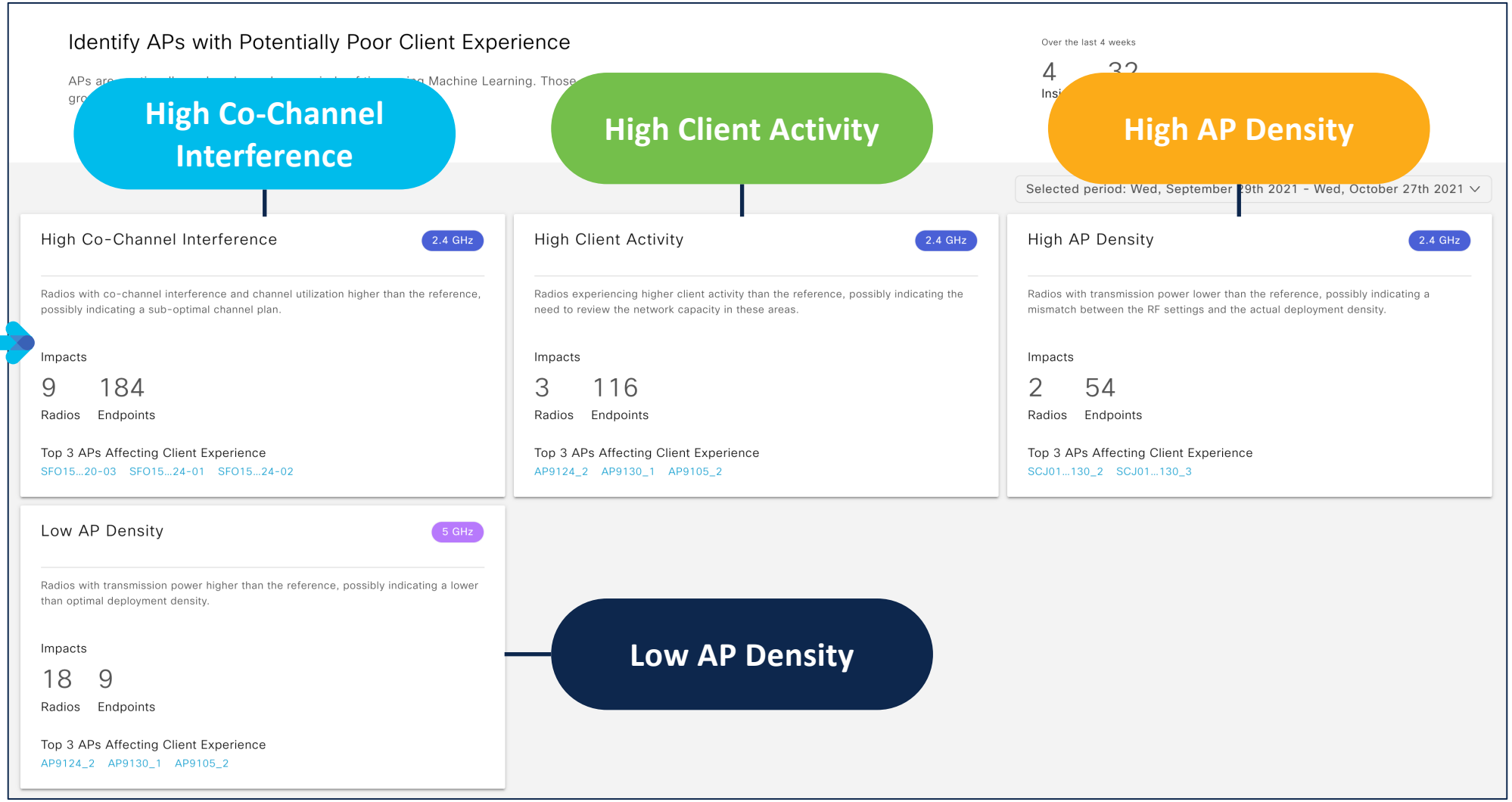


Global Event Viewer

Network Devices



AI-Driven AP Performance Advisories



Pain Points with Enterprise Wi-Fi: Expectations vs. Reality

Expectations* about Wi-Fi

- It's plug and play
- Gigabit speeds
- Always full bars
- Seamless experience

(*) Based on Marketing and Home Experience

VS.

Nature of RF

- **Dynamic**
- **Interferences**
- **Noise**
- **Lots of users**
- **…**

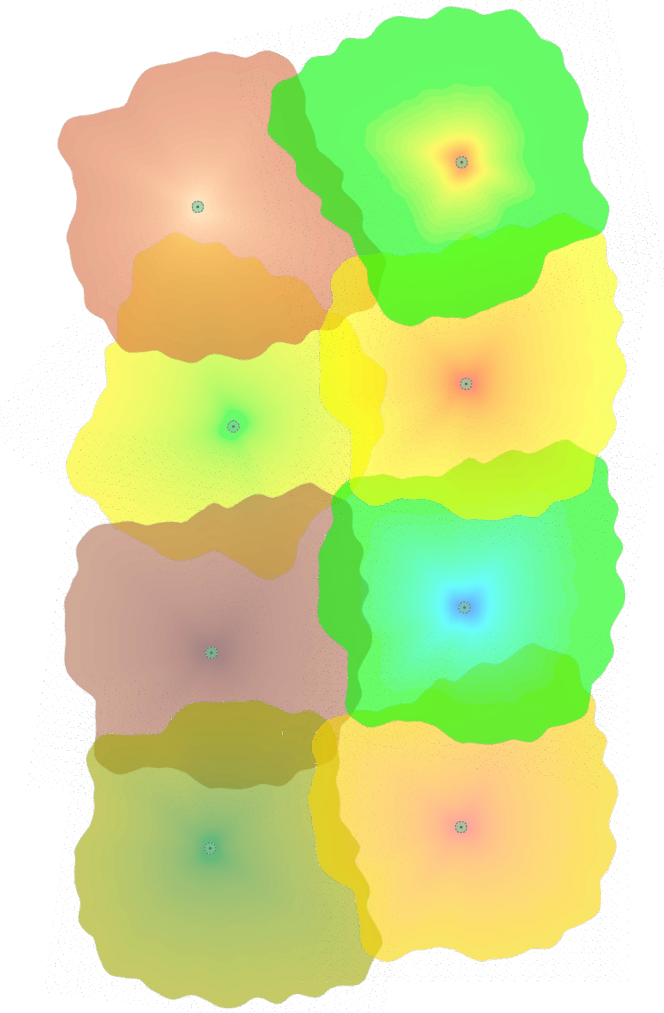
Reality** about Wi-Fi

- RF tuning required for optimal performances
- 10 Mbps? Lucky you!
- Sticky clients
- Bad client drivers
- Random disconnects

(**) Enterprise Network Experience

What is Radio Resource Management (RRM)?

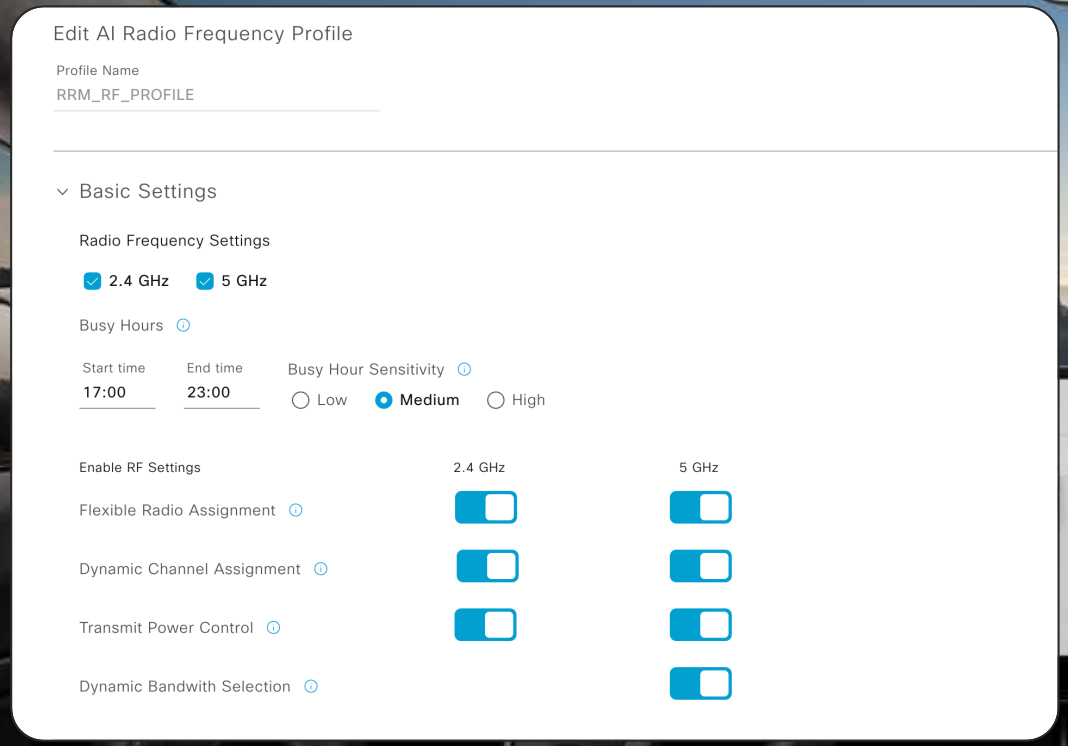
RRM is a WLC feature that automatically optimizes wireless configurations to improve wireless performance.



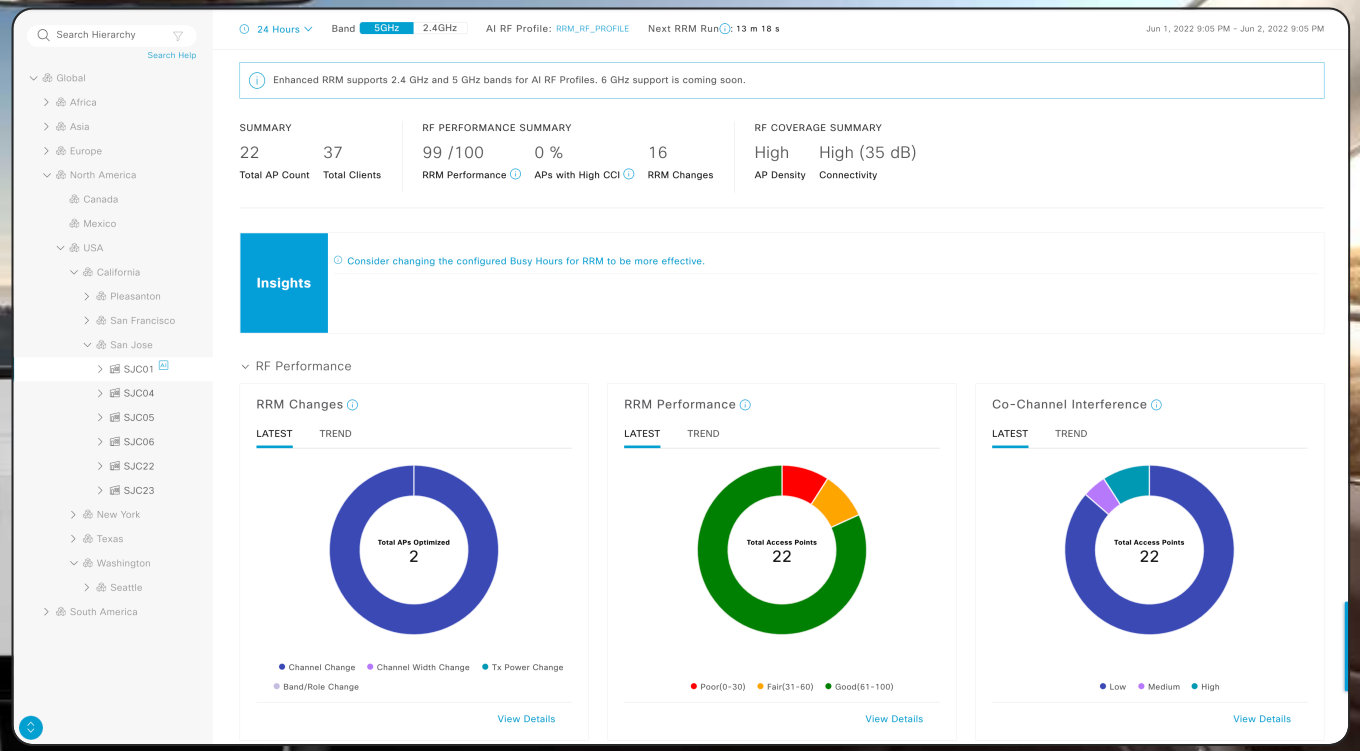
Some Examples:

- Flexible Radio Assignment
- Transmit Power Control
- Dynamic Channel Assignment
- Dynamic Band Selection

AI Radio Frequency Profile



AI-Enhanced RRM Control Center

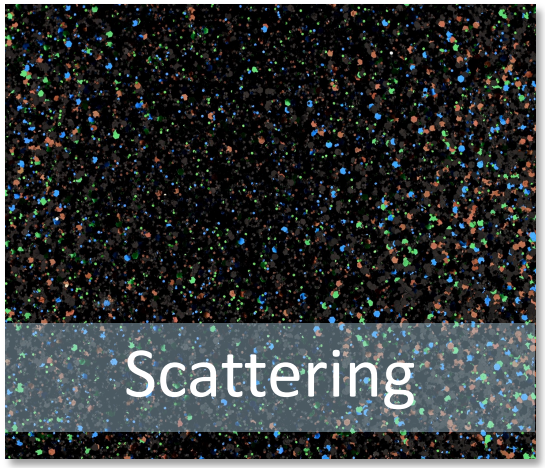


AI-Enhanced RRM

Policy-driven Configurations, Complete Visibility & Serviceability, Proactive Optimizations

Visualization of the wireless network

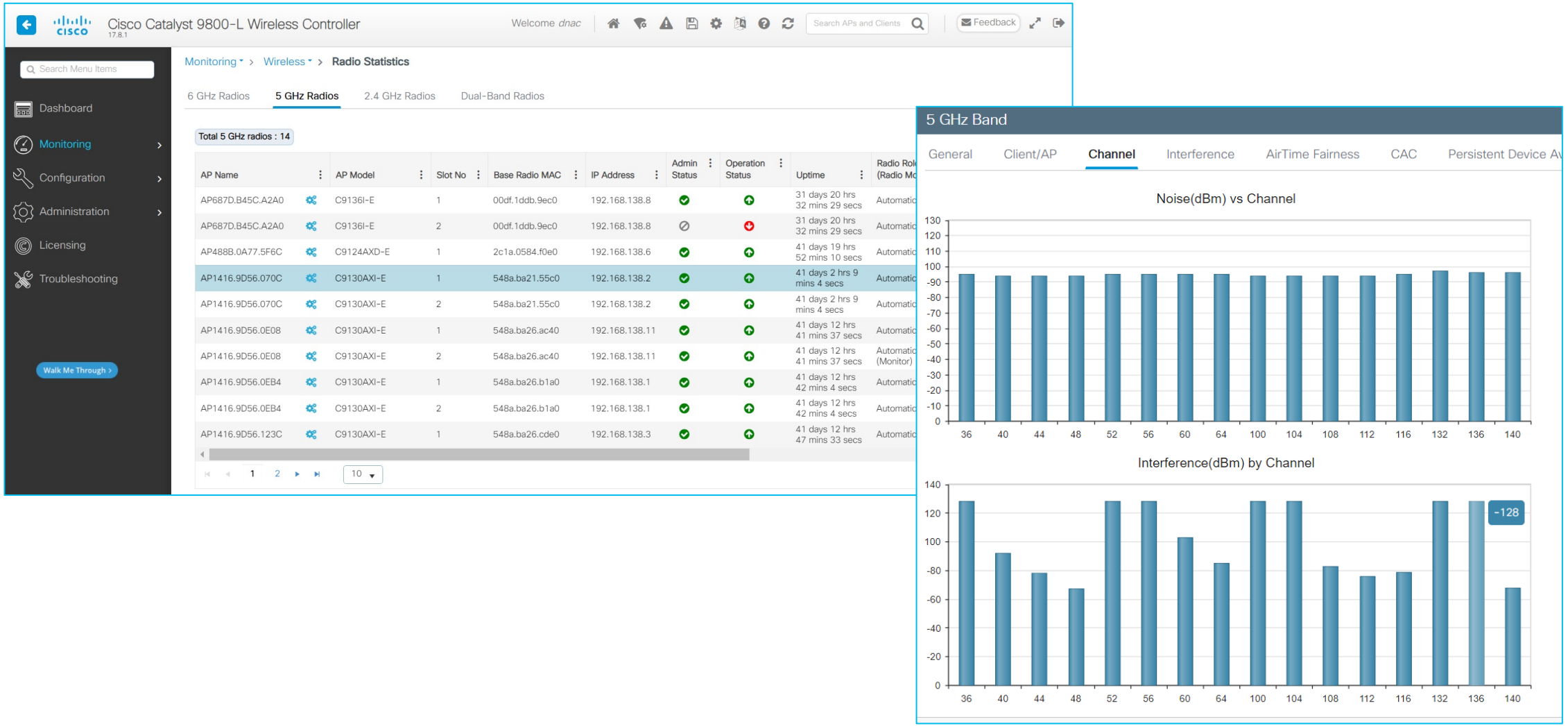
What else happens in the air?



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

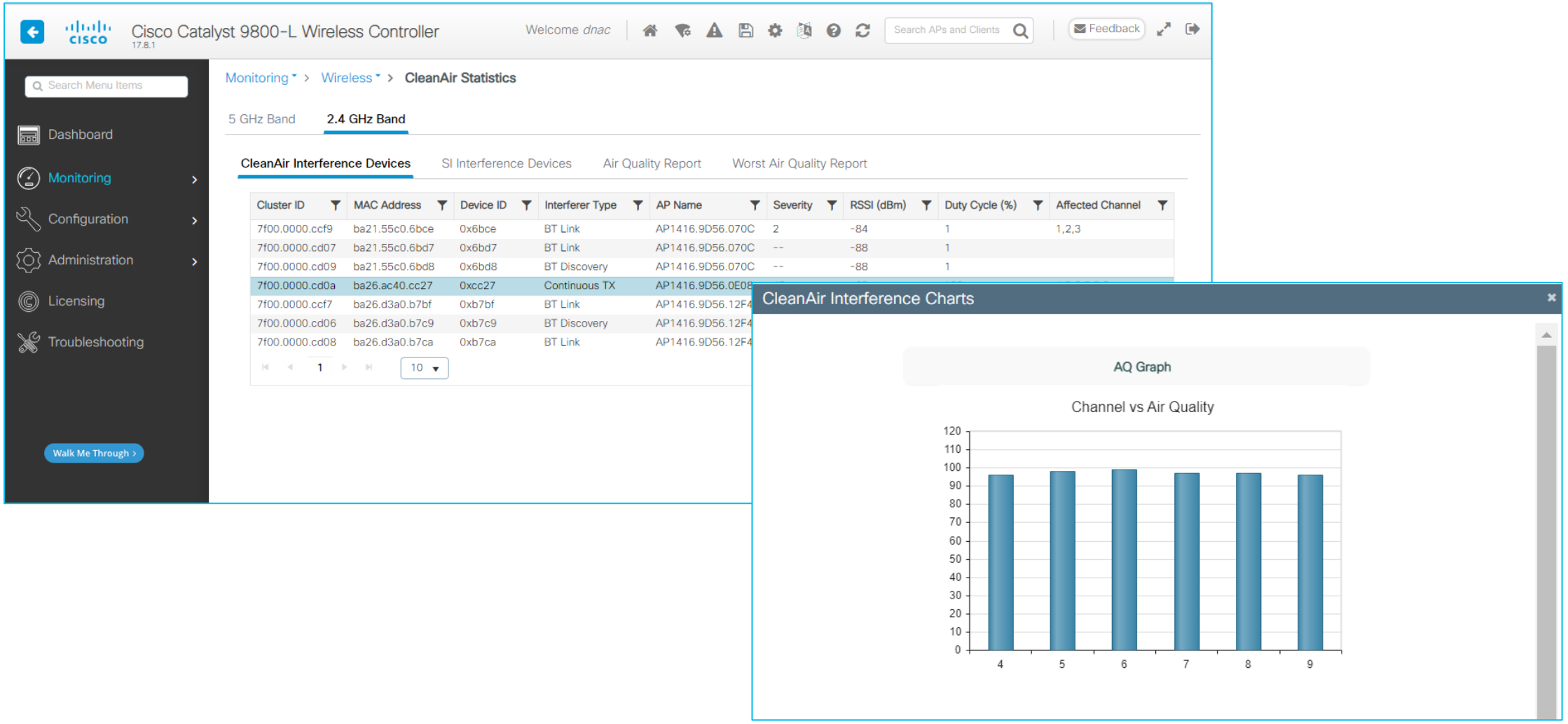
Cat9800 RF Visualization

Radio Statistics



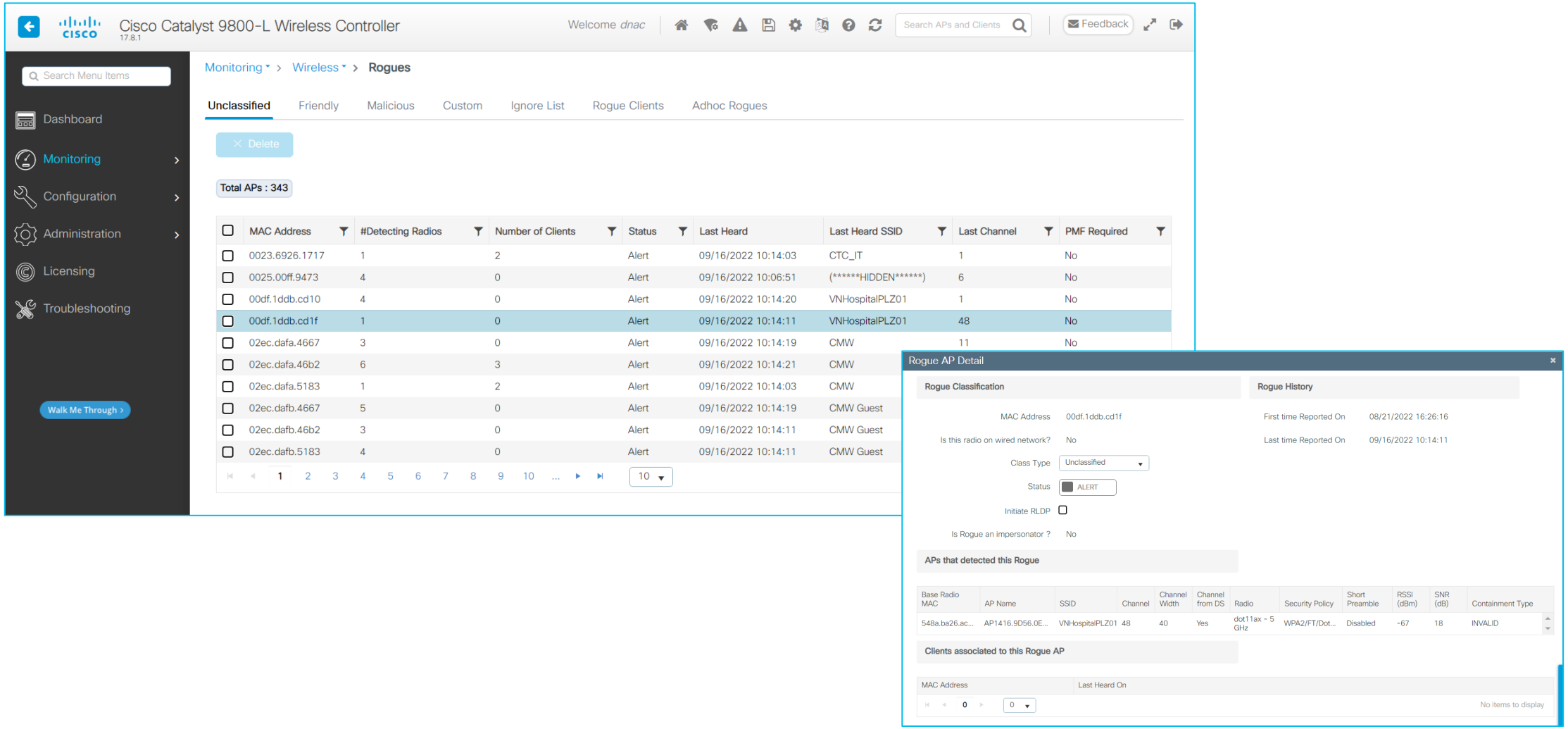
Cat9800 RF Visualization

CleanAir Statistics

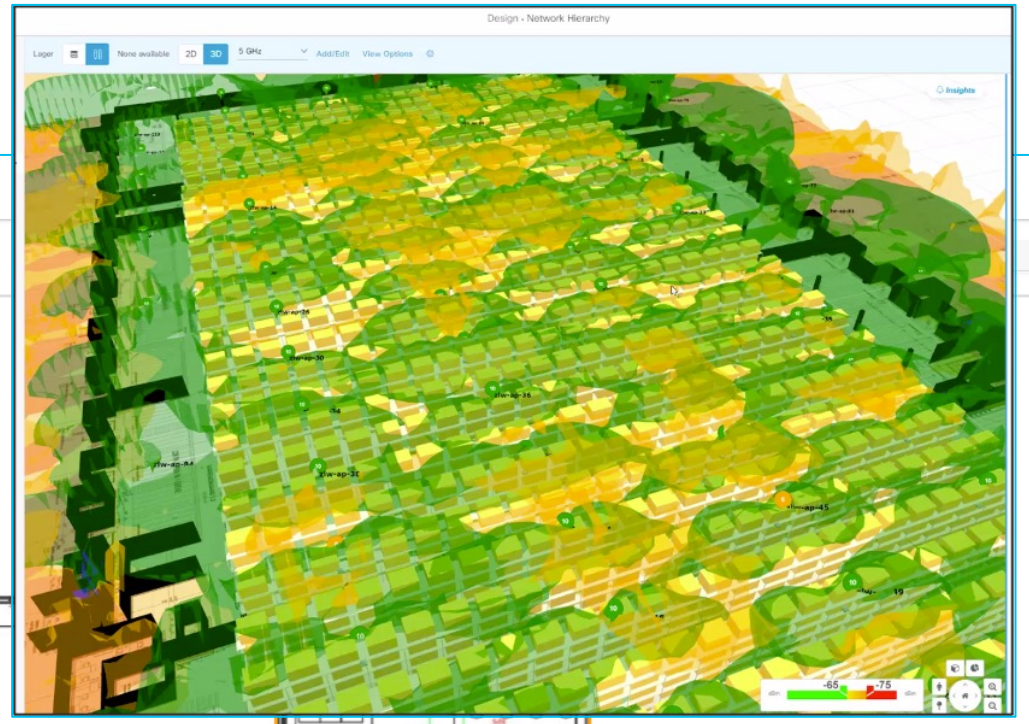


C9800 Wireless IPS

Rogue Detection



2D & 3D Wireless Maps



Cisco DNA Center

Design • Network Hierarchy

Find Hierarchy

- Global
  - Bratislava
  - Jezeri
  - Kounov
  - Pardubice
  - Plzen
    - PLZ01
      - PLZ01-1
  - Prague
    - PRG07
      - PRG07-5
      - PRG07-ATXDemo
      - PRG07-DMZ
      - PRG07-Guest-ACC
      - PRG07-JC-PNP
  - Temp-PI-DNC-coexistence
  - TEST-DS
  - Warehouse-test
  - Zatec

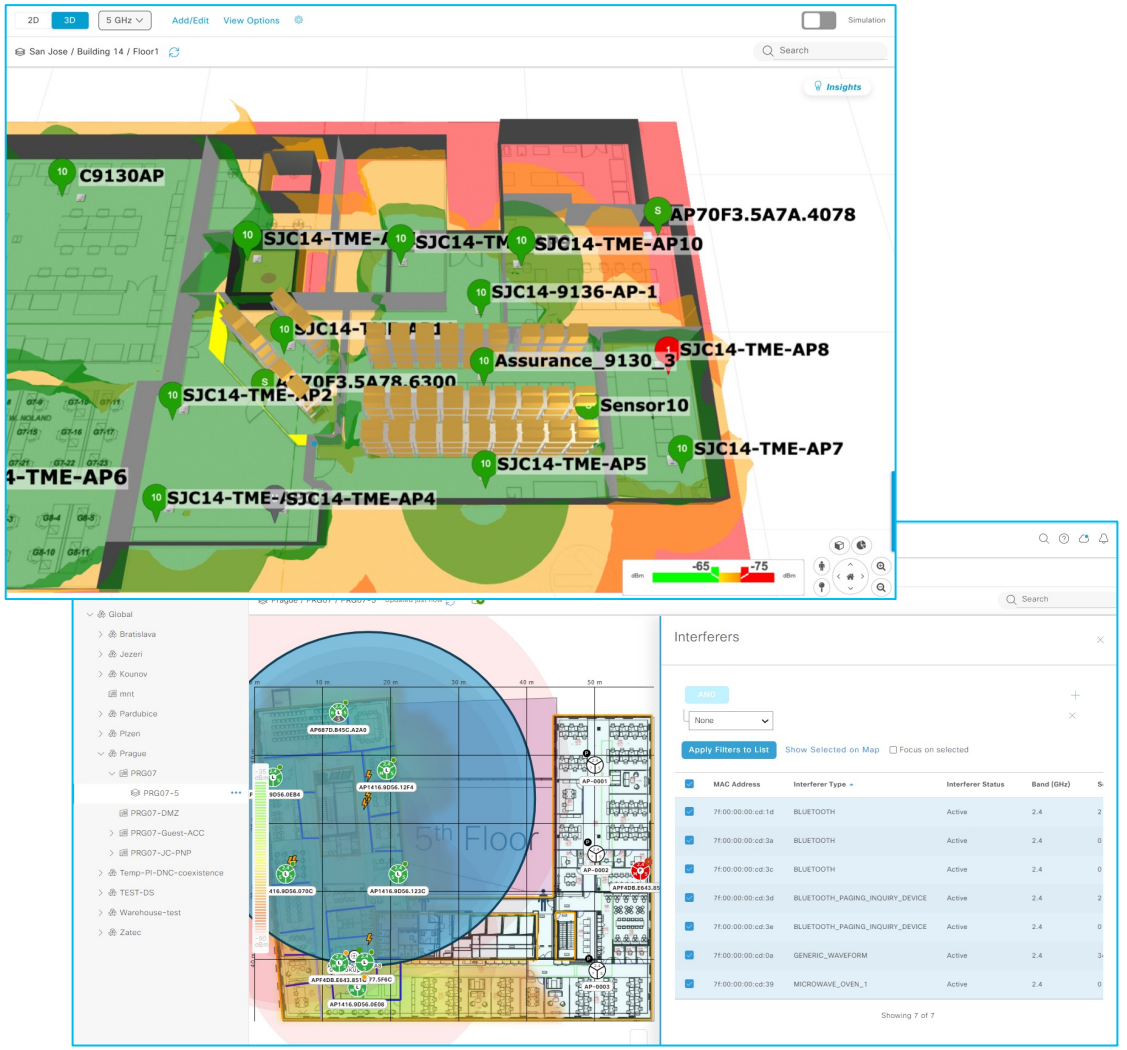
PRG07-5 | 2D | 3D | 5 GHz | Add/Edit | Data | View Options

-35 dBm

-90 dBm

DNAC Wireless
2D & 3D Maps –DEMO

- **DNAC Wireless maps**
  - View Options
  - Monitoring SLAs With Visual Insights
  - RF Optimizer for AP Redeployment Suggestions
  - DNAC Interferer Visualization

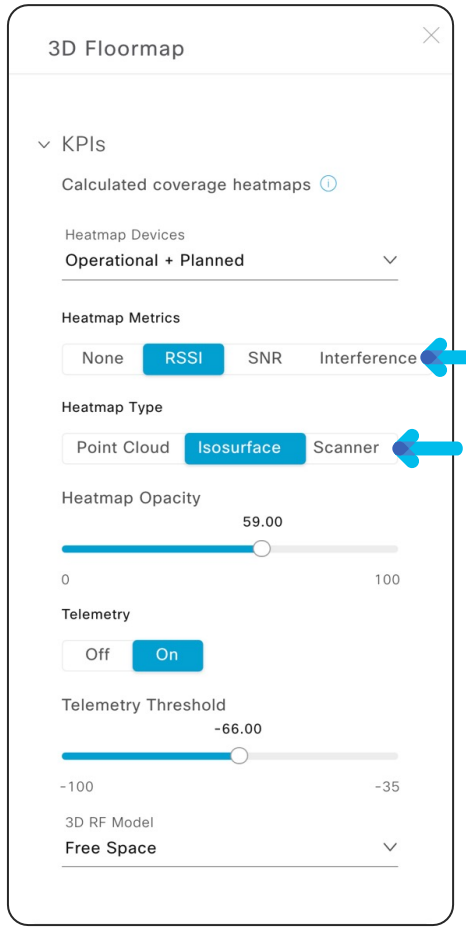


Configuring View Options in Wireless 3D Maps

Customize the Map's Visuals

1 Click View Options

2 To Open a Slide-in Pane



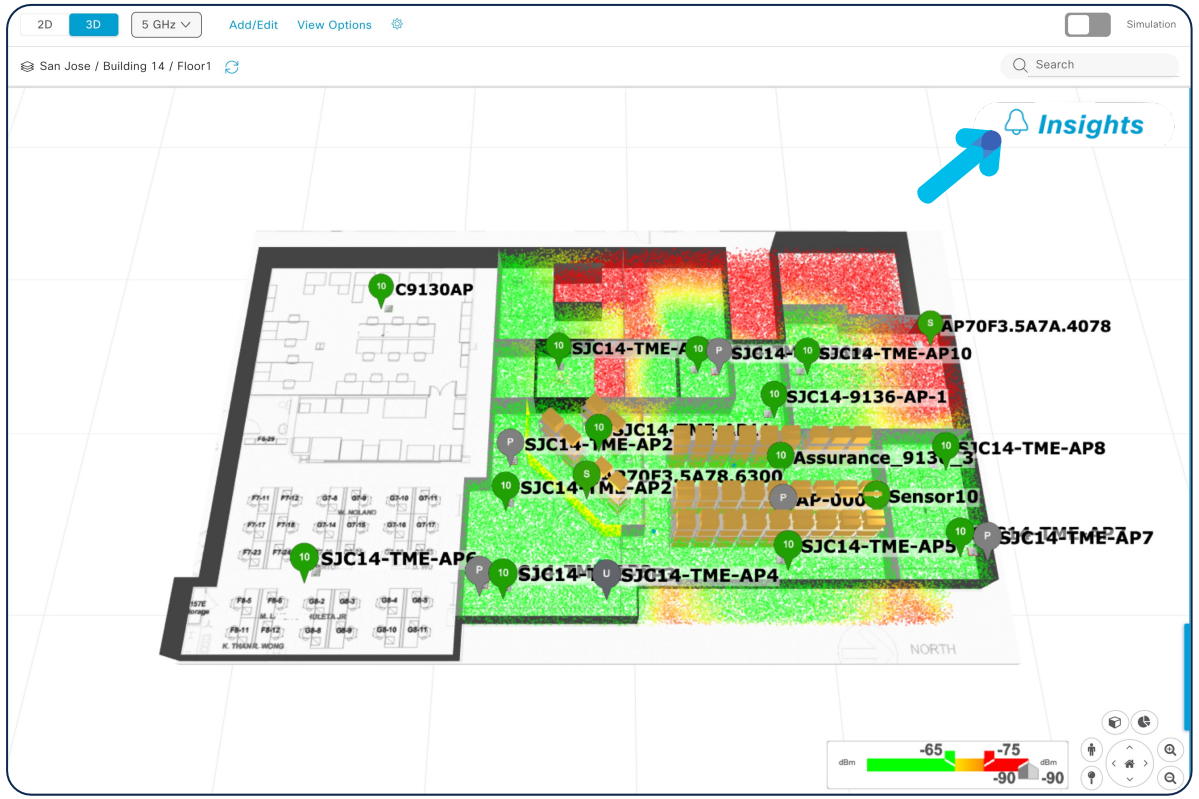
a RF Metric

b How it's Visualized

Monitoring SLAs With Visual Insights

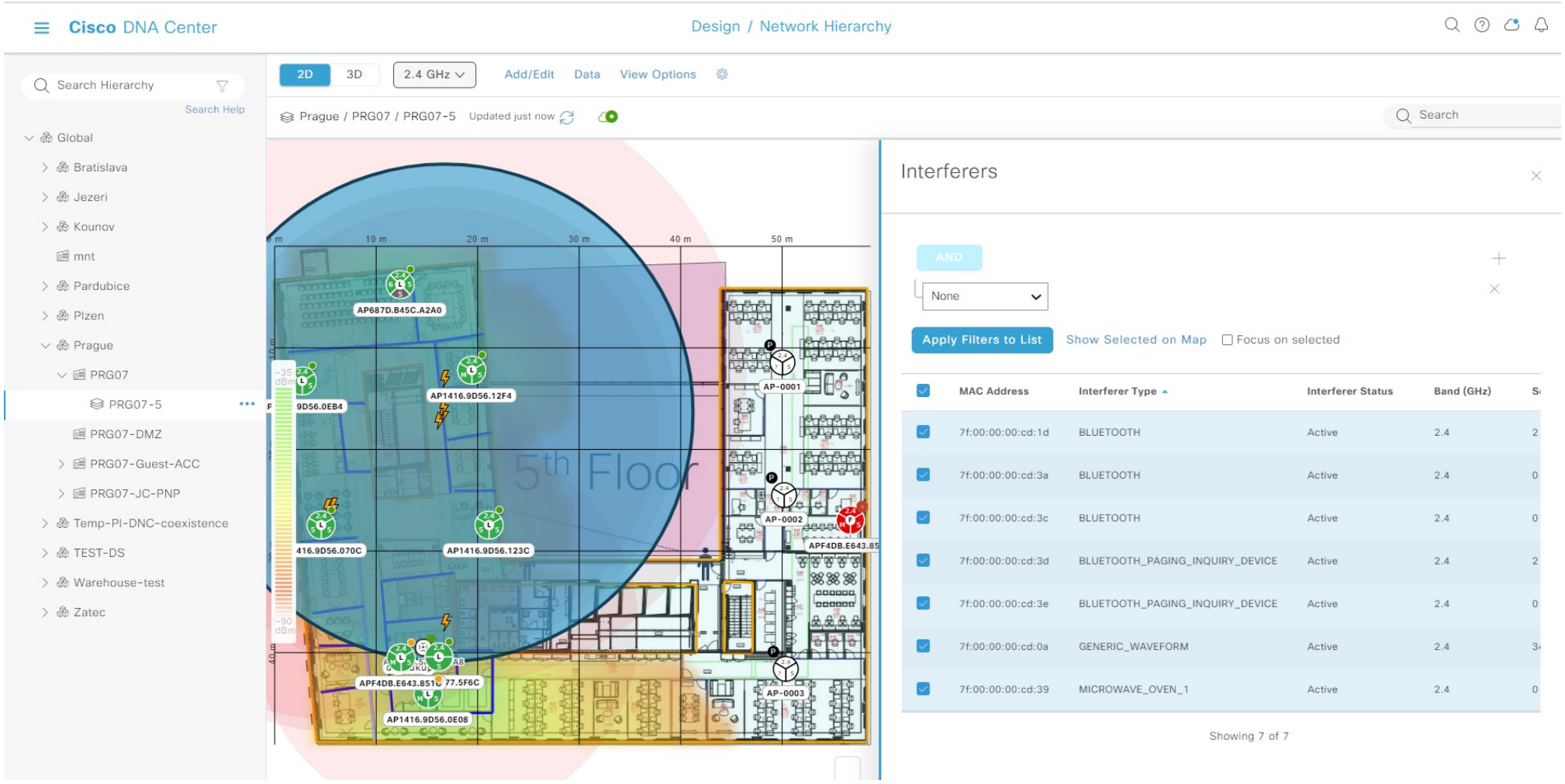
Visibility Into Areas of Coverage That Need Attention

1 Click on the Insights n to view SLAs that meet or miss the configured threshold.

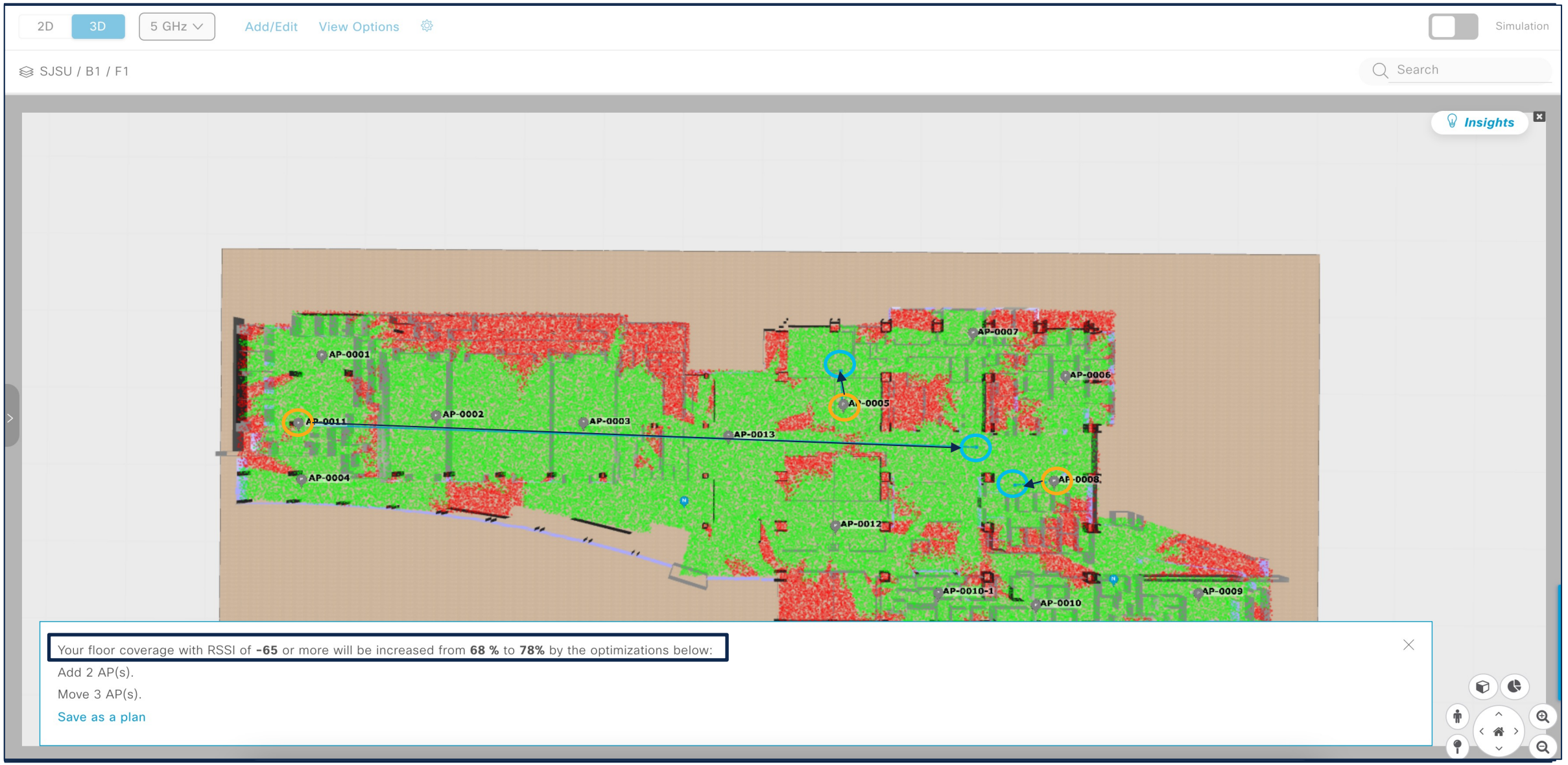


2 A banner appears with a list of insights. Clicking on **Click** adjusts the map for you to view insight details.

DNAC Interferer Visualization



Leverage RF Optimizer for AP Redeployment Suggestions
starting from 2.3.3!

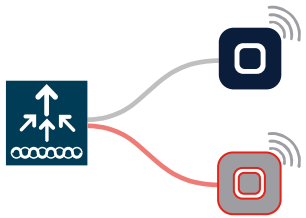


WLAN has inherent vulnerabilities exposing it to various threats

On Wire Attacks

Rogue on Wire

Unknown | Malicious



- Switch-port Tracing
- RLDP

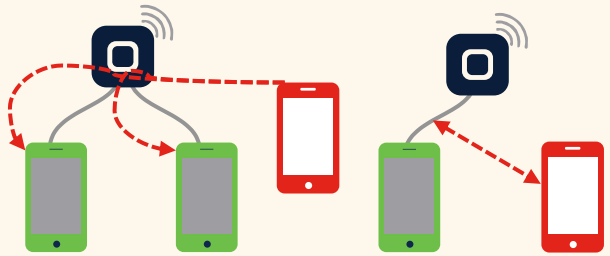
Over-the-Air Attacks

Rogue Access Points | Honeypot or Evil Twin | AP MAC Spoofing

- Rogue Management

Basic Wireless Security

Denial of Service | Reconnaissance | Cracking Tools



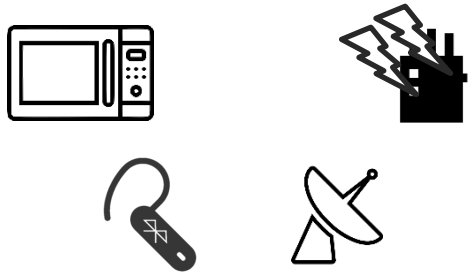
- WIPS

Advanced Wireless Security

Non-802.11 Interferers

Microwave | Bluetooth

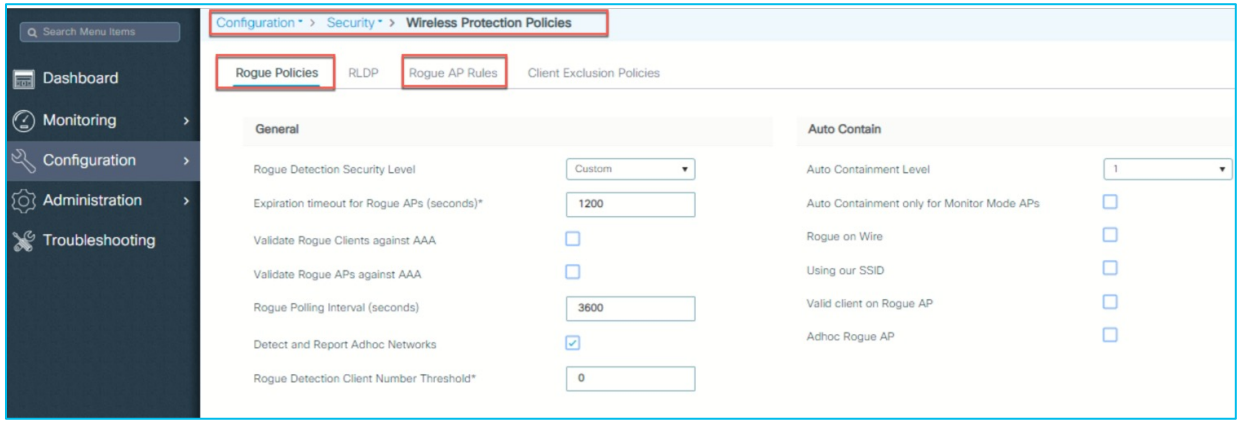
Radar | RF Jammers

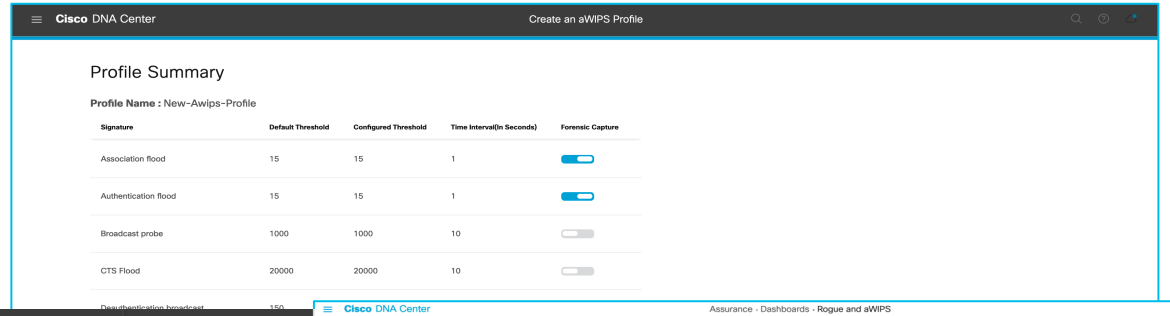


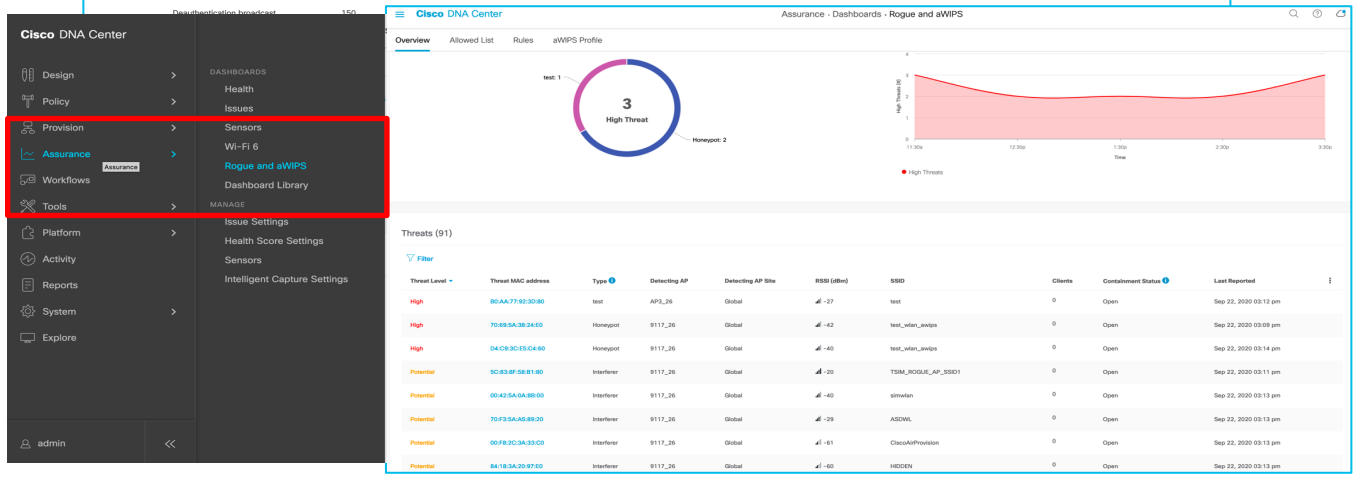
- Cisco CleanAir

Visibility of non-WiFi interferers

Cisco Rogue/WIPS Highlights



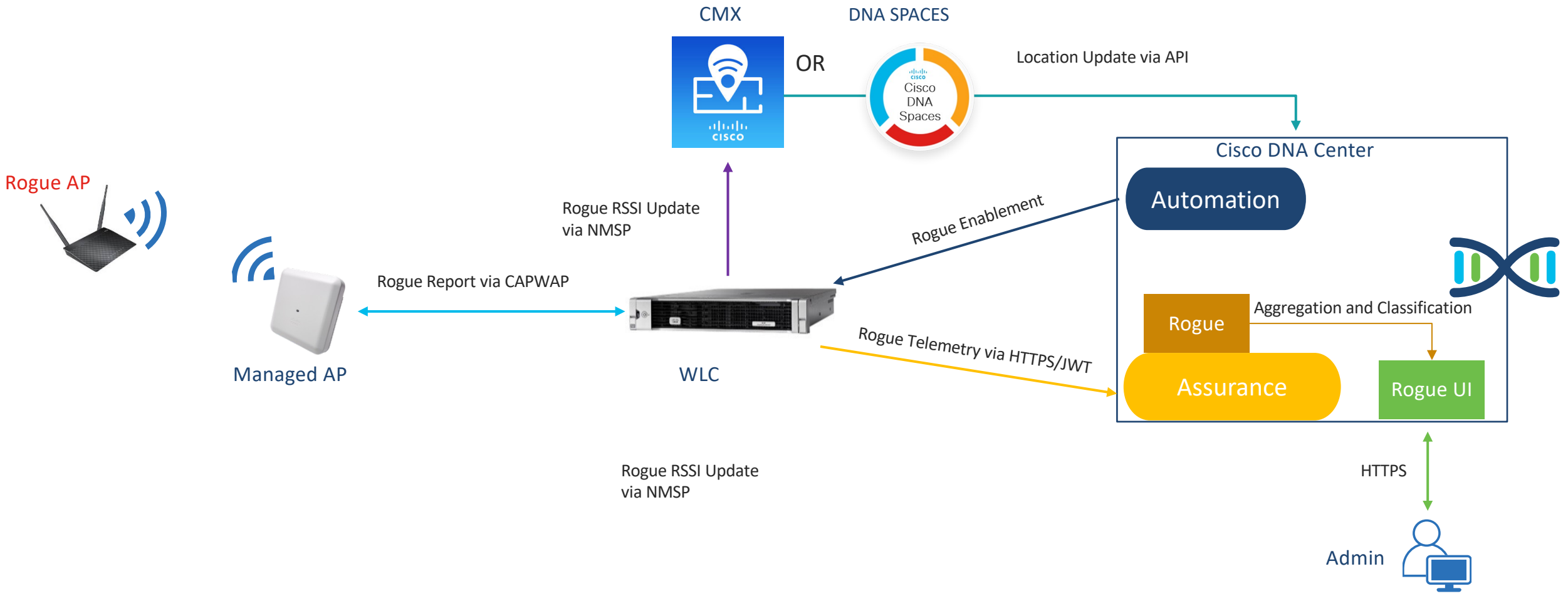




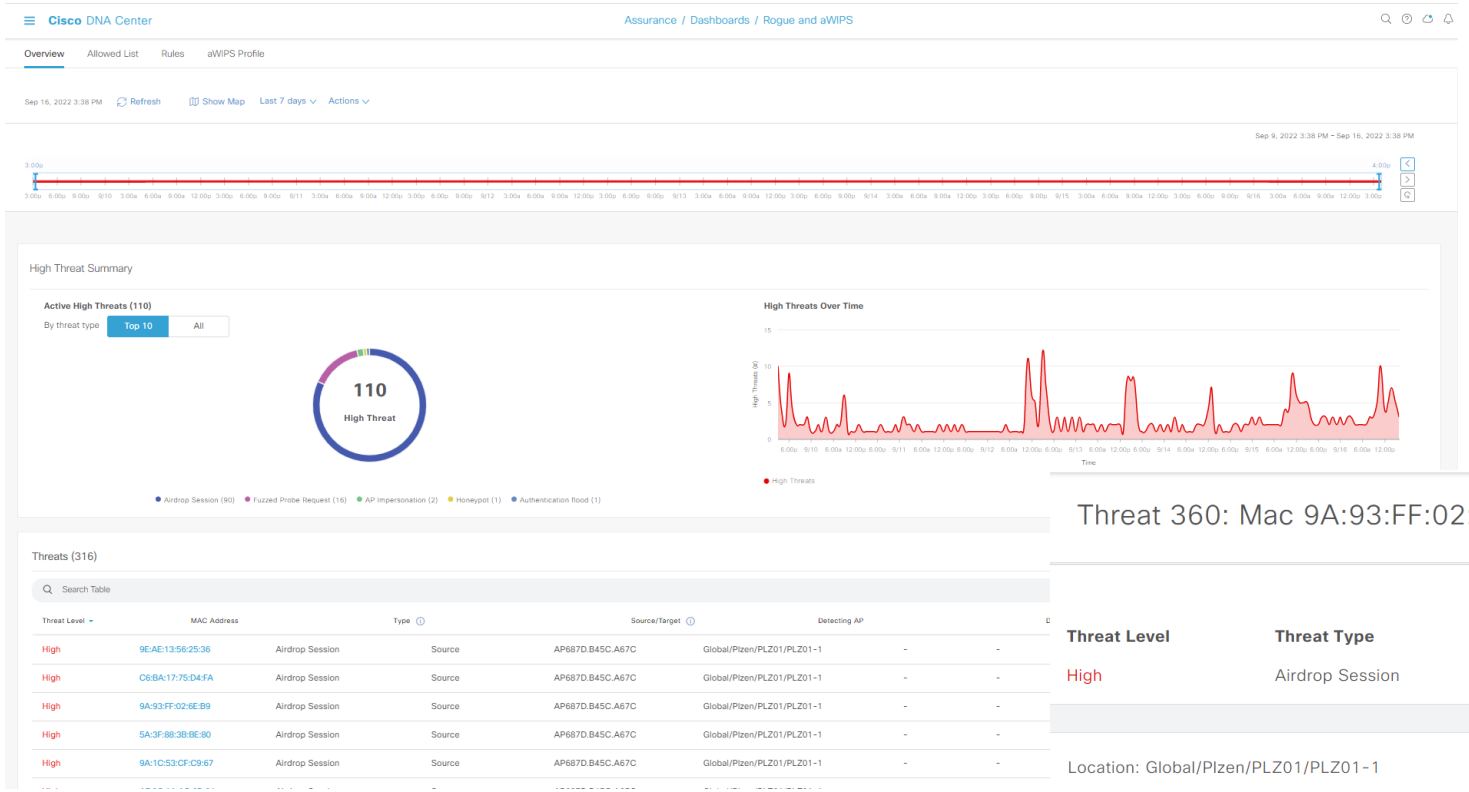
Highlights - Cisco Catalyst 9100, 9800 and Cisco DNA Center deliver state-of-the-art Rogue/WIPS Management:

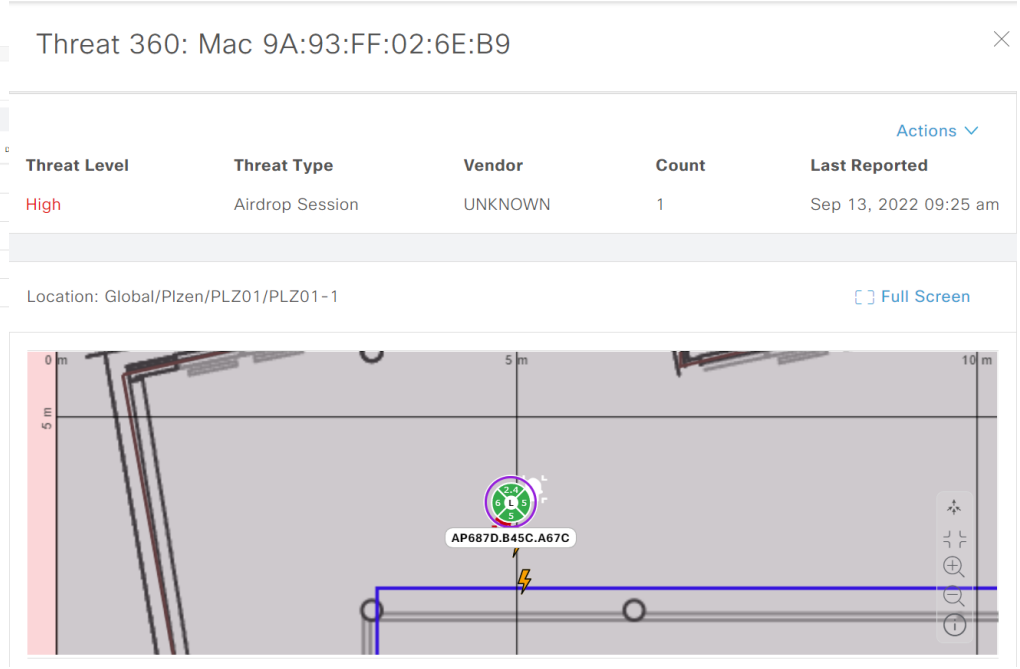
- Dedicated RF ASIC radio for Rogue/WIPS
- Rogue Auto-Classification techniques (proprietary)
- Rogue Rule creation on Cat 9800 WLC
- New Rogue/WIPS Signatures * (Future Updates)
- Rogue Containment (Manual in DNA Center)
- DNA Center aWIPS Dashboard Assurance
- DNA Center WIPS Workflow
- Threshold Configuration
- Forensic Captures
- Cisco DNA Spaces for Rogue AP & Client location

Rogue Management Architecture



DNAC Security Threat Summary & Map Location





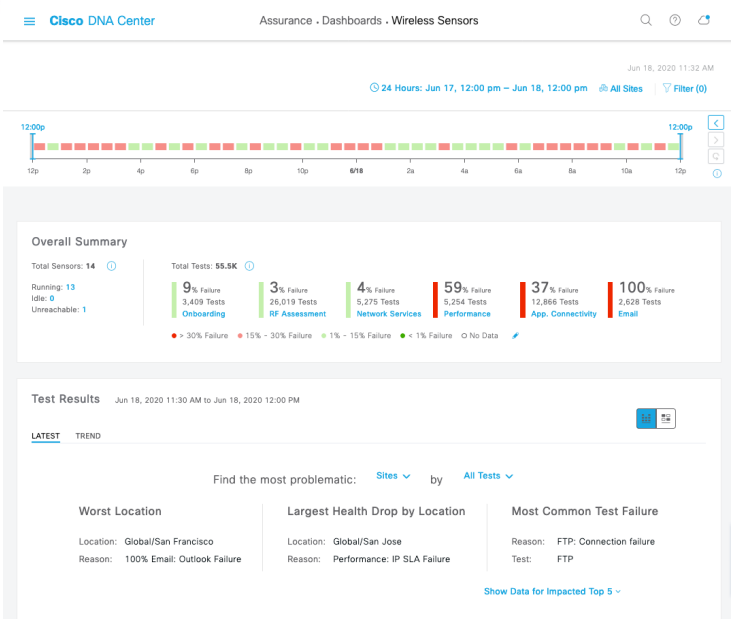
Proactive network diagnostics

Aironet Active Sensor Use Cases

Test your network and report results to Cisco DNA Assurance!

Performs the following Wireless Tests:

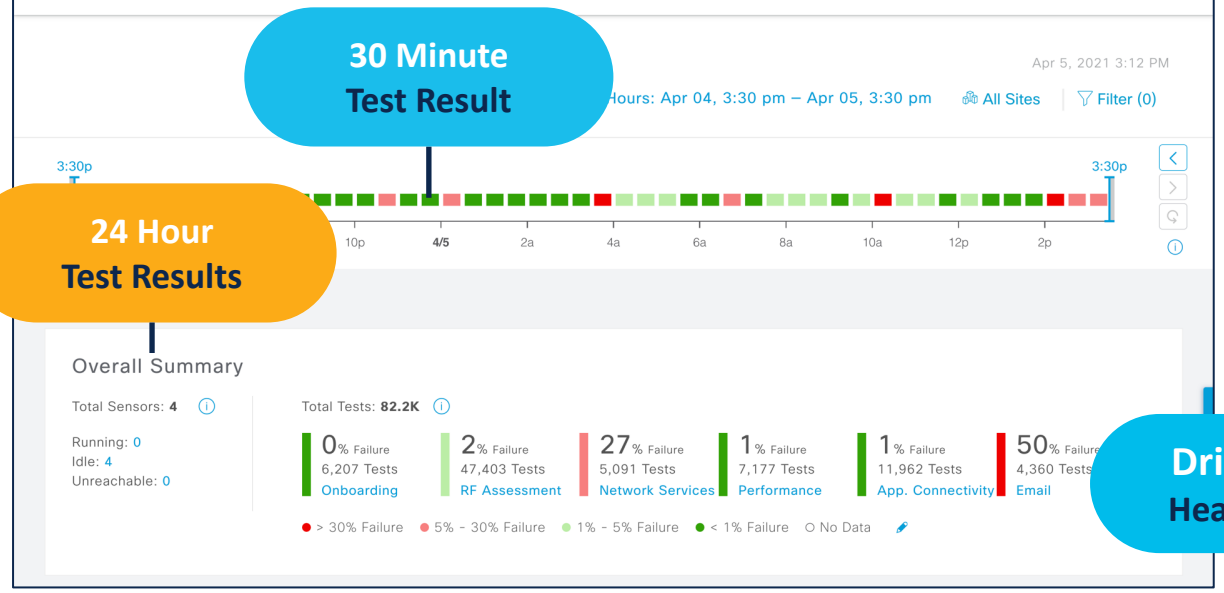
- Onboarding (Auth Types - 802.1x, MAB and Open Auth, DHCP)
- RF Assessment (Data rate, SNR)
- Network Services (DNS, RADIUS)
- Performance (iPerf3, NDT, IP SLA)
- Application (FTP, Web server, host reachability)
- Email (IMAP, POP3, OWA)



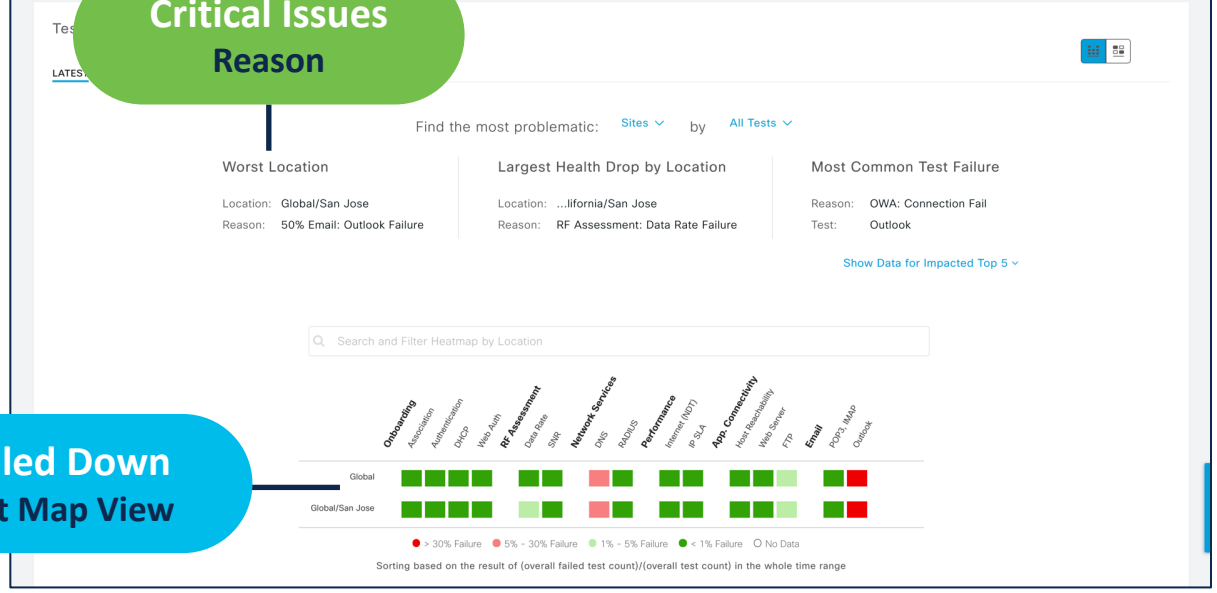
Wireless Sensor Global Dashboard

Overall Summary Trend View

24 Hour View

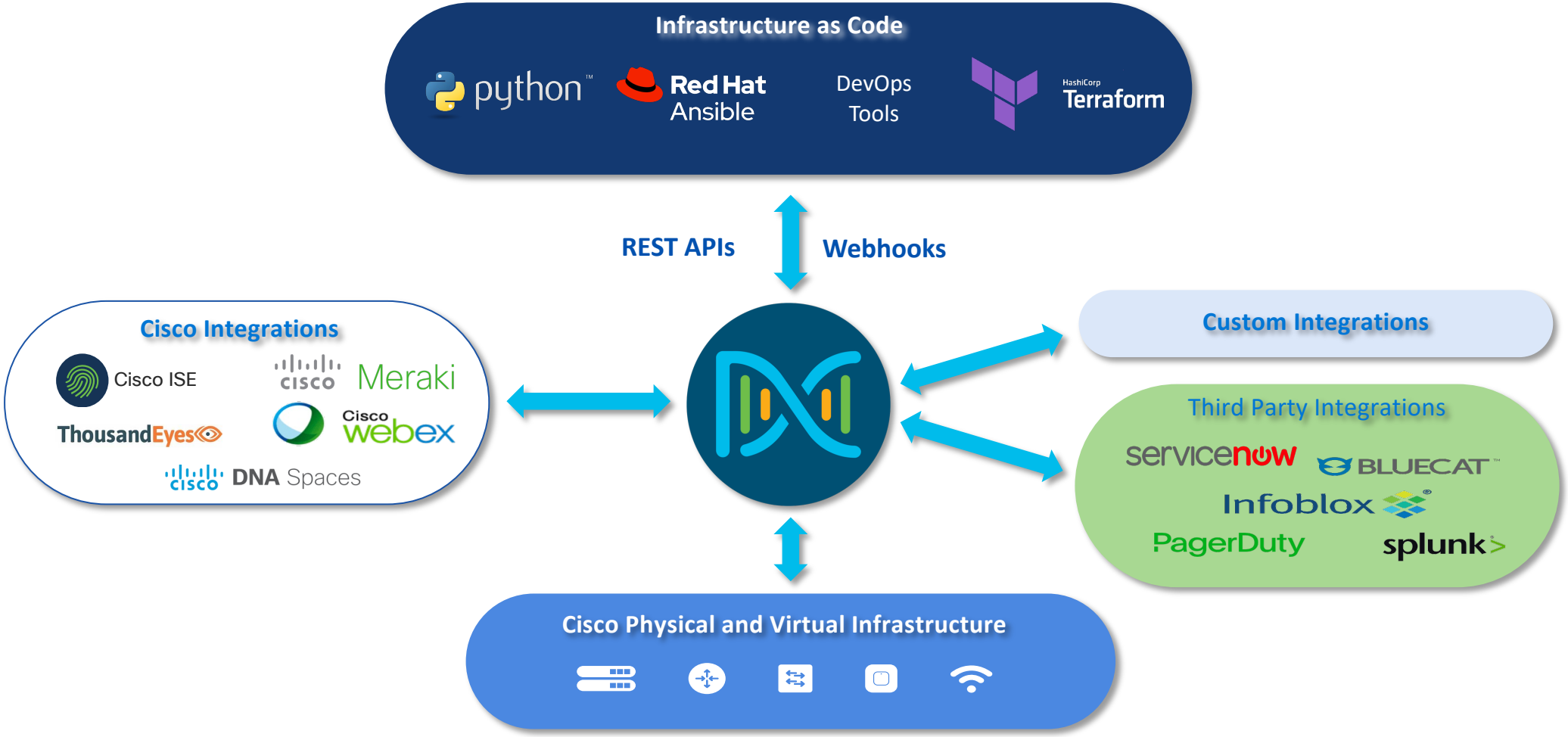


30 Minute View



- Global View of All Sensor Test Results
- SSID, Band, Site Filtering
- Network Time Travel up to 14 Days
- Per Site Per Test Category Result View

Cisco DNA Center Platform



Cisco DNA Center Platform Overview

Event Notifications

- Assurance Issues
- AI/ML Insights
- System Health
- Integration Connectivity
- License Management
- Webhooks
- **PagerDuty**
- **Webex**
- Syslog
- SNMP

Northbound REST APIs

- Network Inventory
- Network Topology
- Network Design
- Provisioning
- SWIM, PnP
- Path Trace
- Assurance
- SDA
- Templates
- RMA
- Config Archive
- Sensors

IT Ecosystem Integrations

- IT Service Management
- IP Address Management
- Reporting
- Wireless Planning
- Incident Response
- SIEM, **Splunk**

Developer Resources

- Sample Code, Videos
- Python SDK, Ansible, Terraform
- Cisco DevNet
  - Sandboxes, Learning Labs
  - Developer Guides
  - Sample Code

200 Events in different areas such as …

Backup/Restore

Fabric

AP Anomaly

Wired Connectivity

CPU and Memory Utilization

Onboarding

Software Image Management

Compliance

Device hardware and software

Application Experience

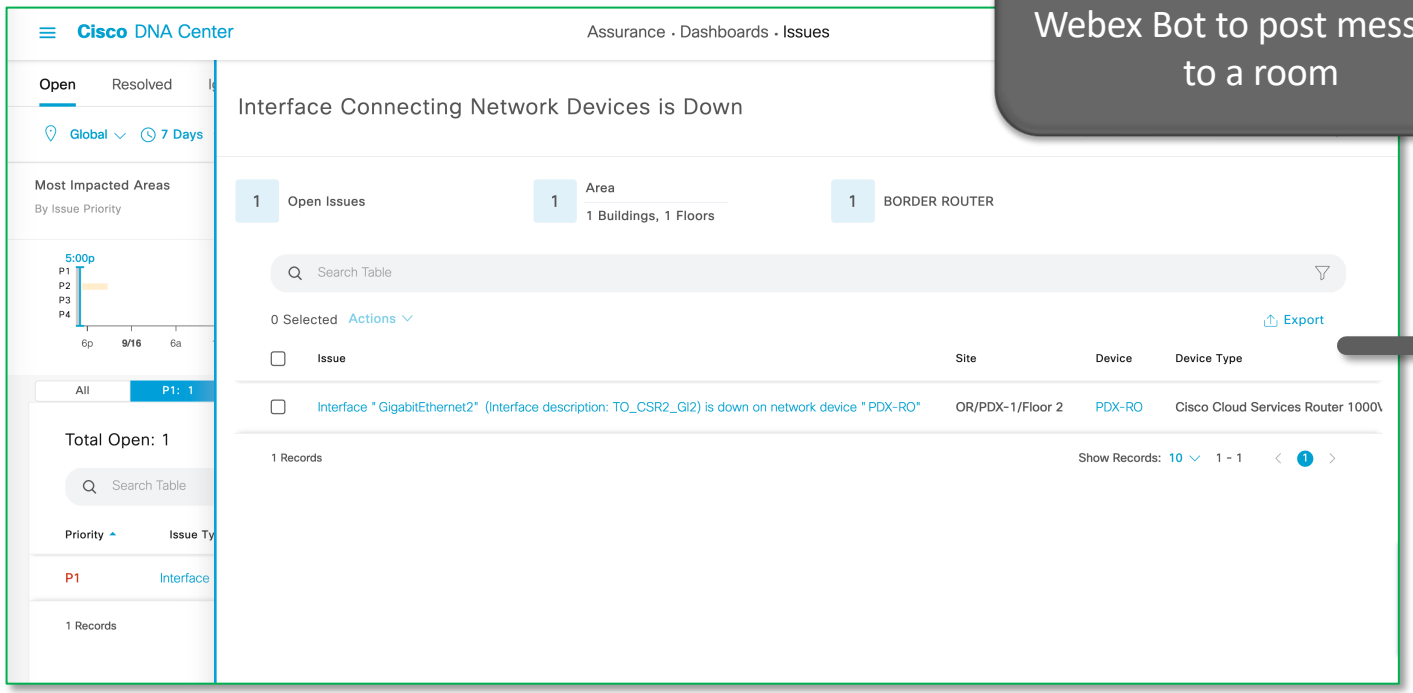
Device Availability

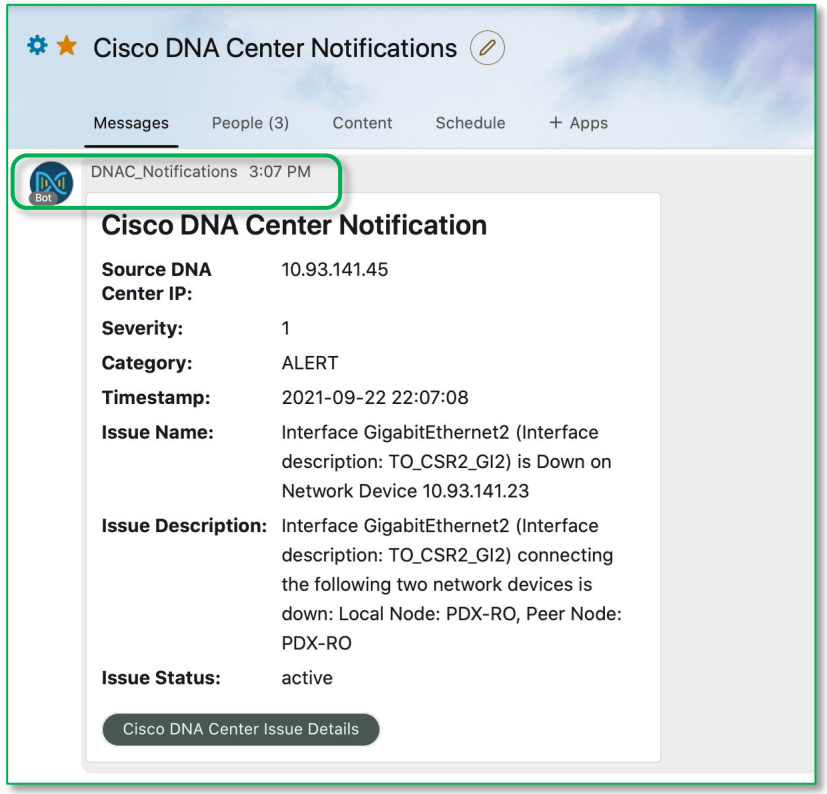
Wireless Connectivity

Sensor Test Troubleshooting

Events Notifications to Webex Message

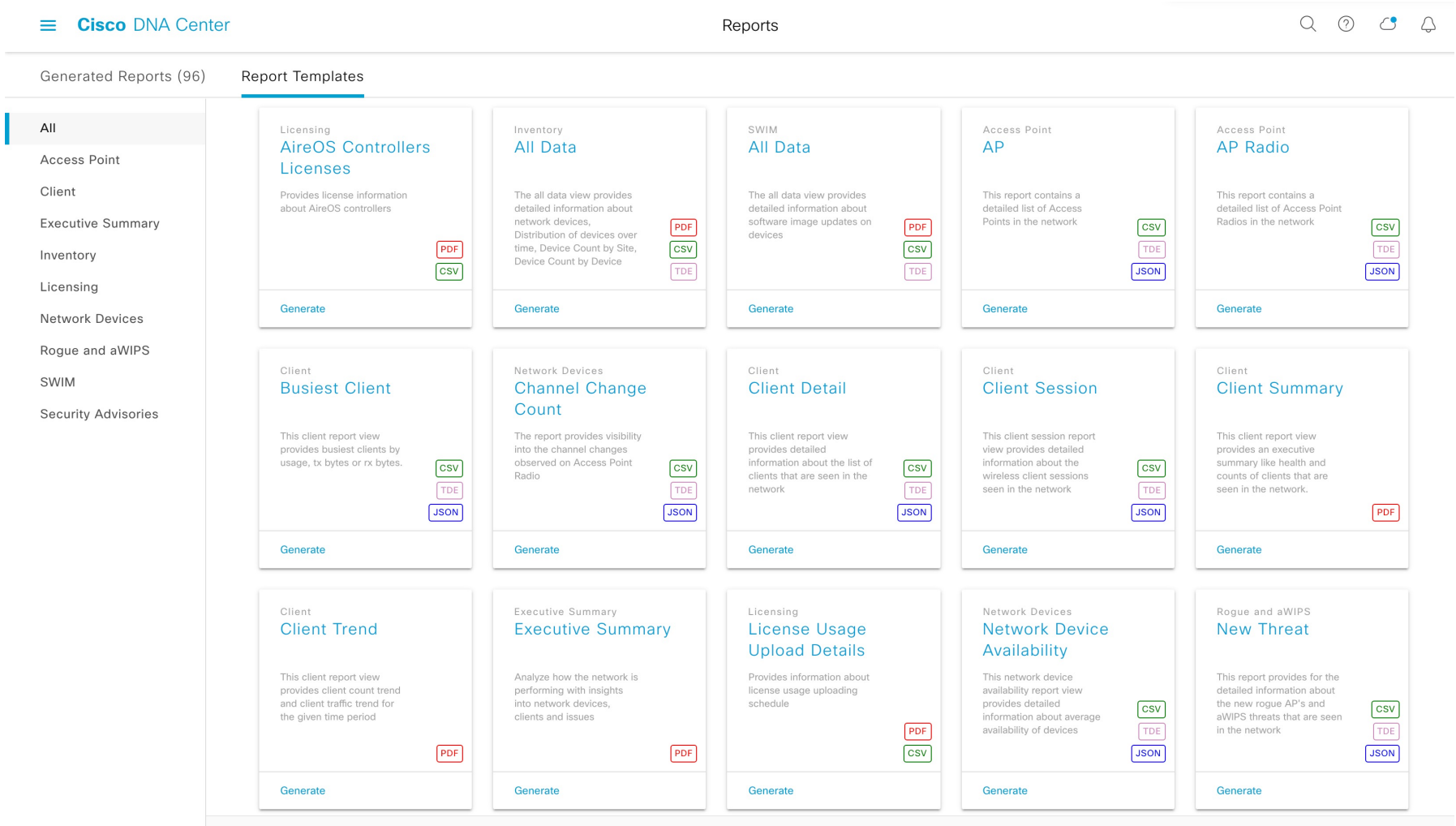
Cisco DNA Center will use a Webex Bot to post messages to a room





Note: *Starting with DNA Center version 2.2.3.x Multi Cisco DNA Center Clusters Support*

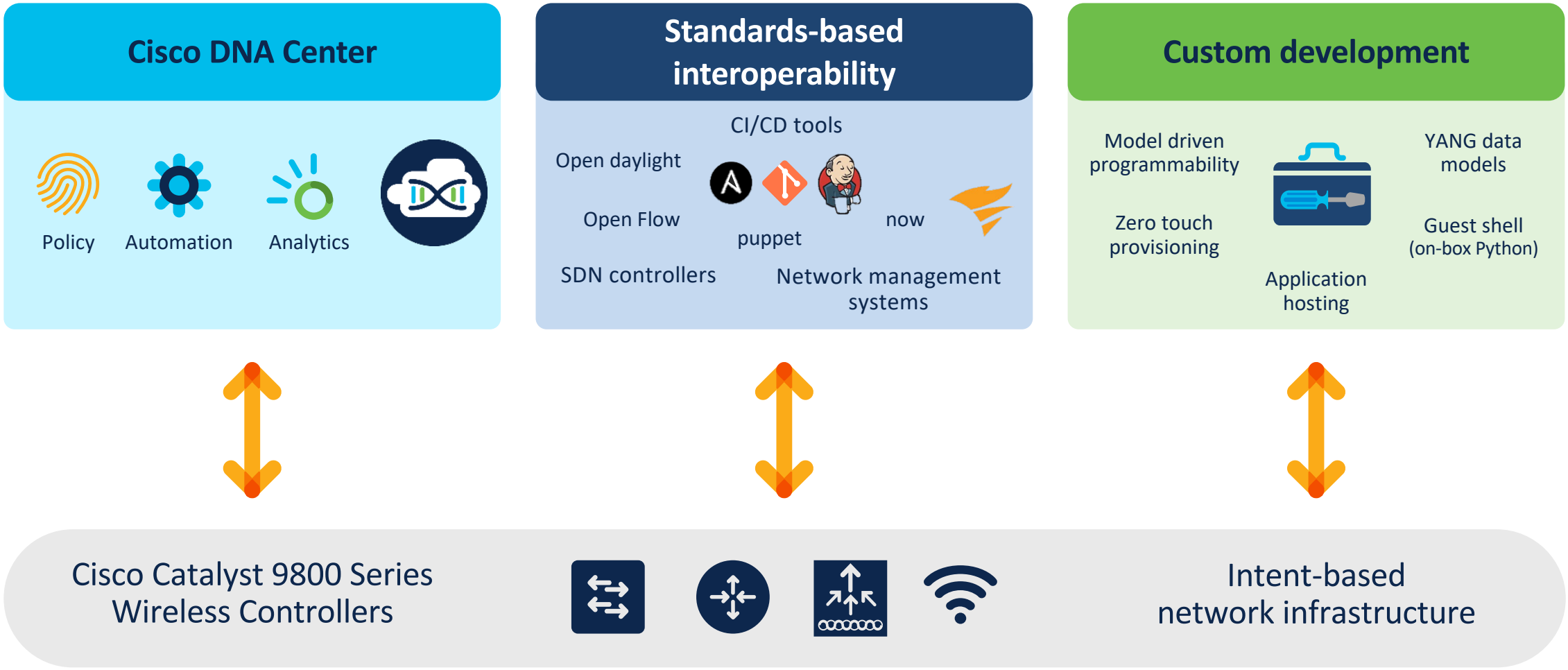
Report Templates



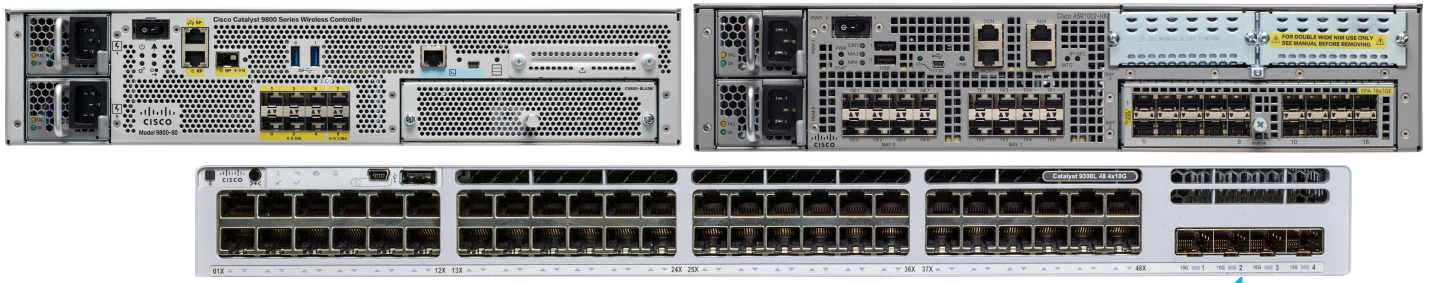
- 20+ reports
- Multiple export formats
- 90 days retention
- Easy workflow
- Multiple Filter options

Observation of trends in the wireless network

Flexible management options with Cisco Catalyst 9800 Series Wireless Controllers



gRPC Dial Out Configured Telemetry



CLI

...or with... + Ansible

YANG

Cisco IOS XE
16.10+

gRPC Dial-Out

Receiver
Decodes to text

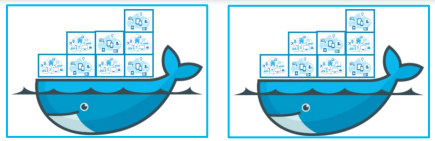
telegraf

Collector
Time Series Database

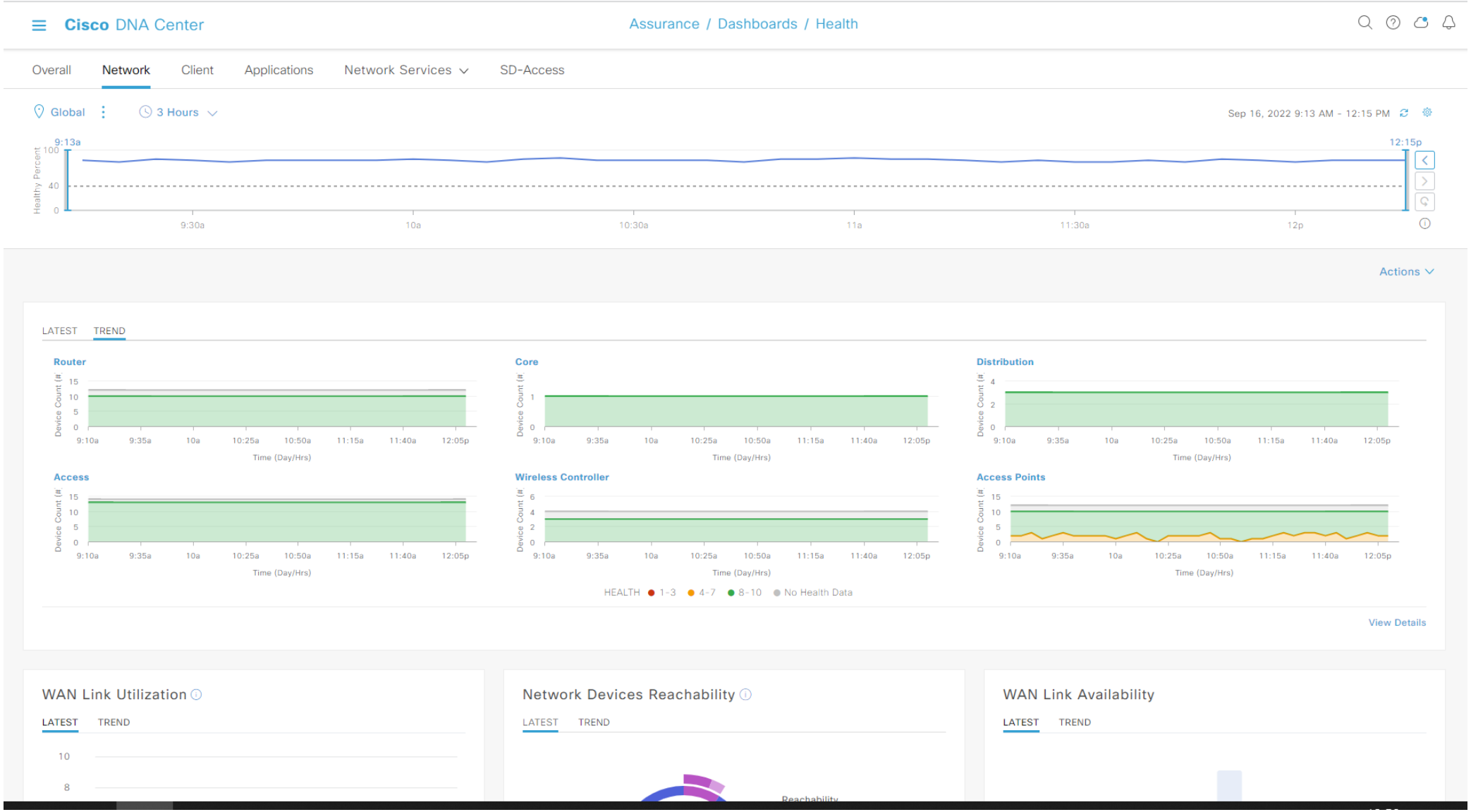
InfluxDB

Monitoring
and Visualizations

Grafana



DNAC Assurance – Timeline / Trend Dashboards



Cisco AI Network Analytics overview

Anonymized data

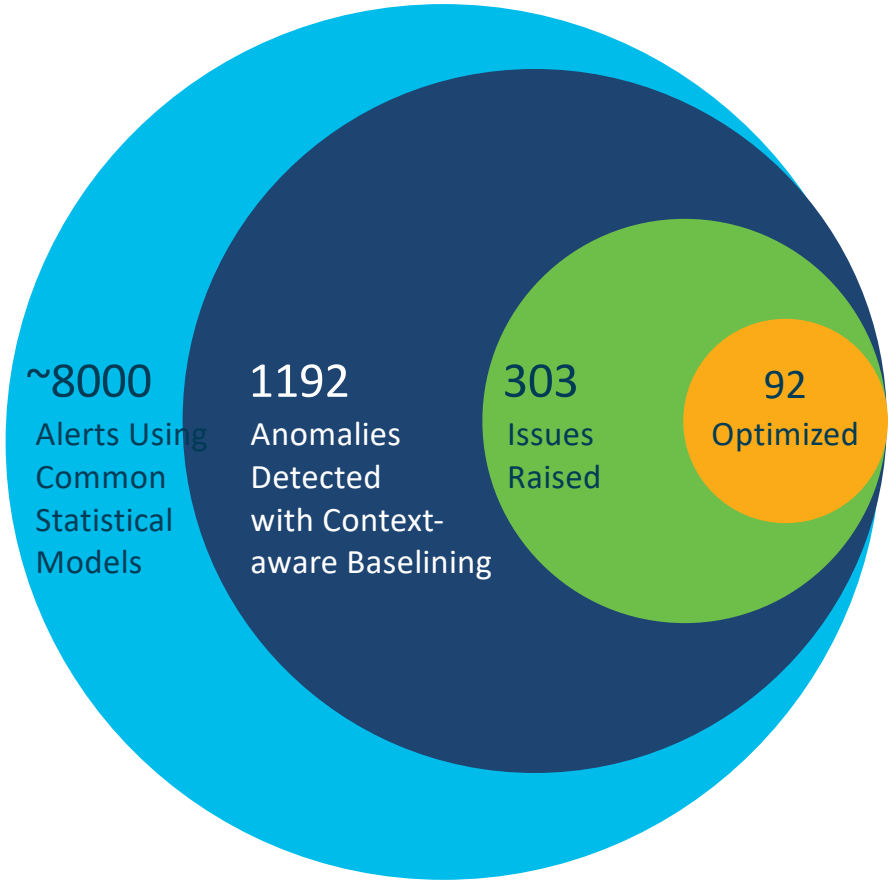
Anomalies and insights

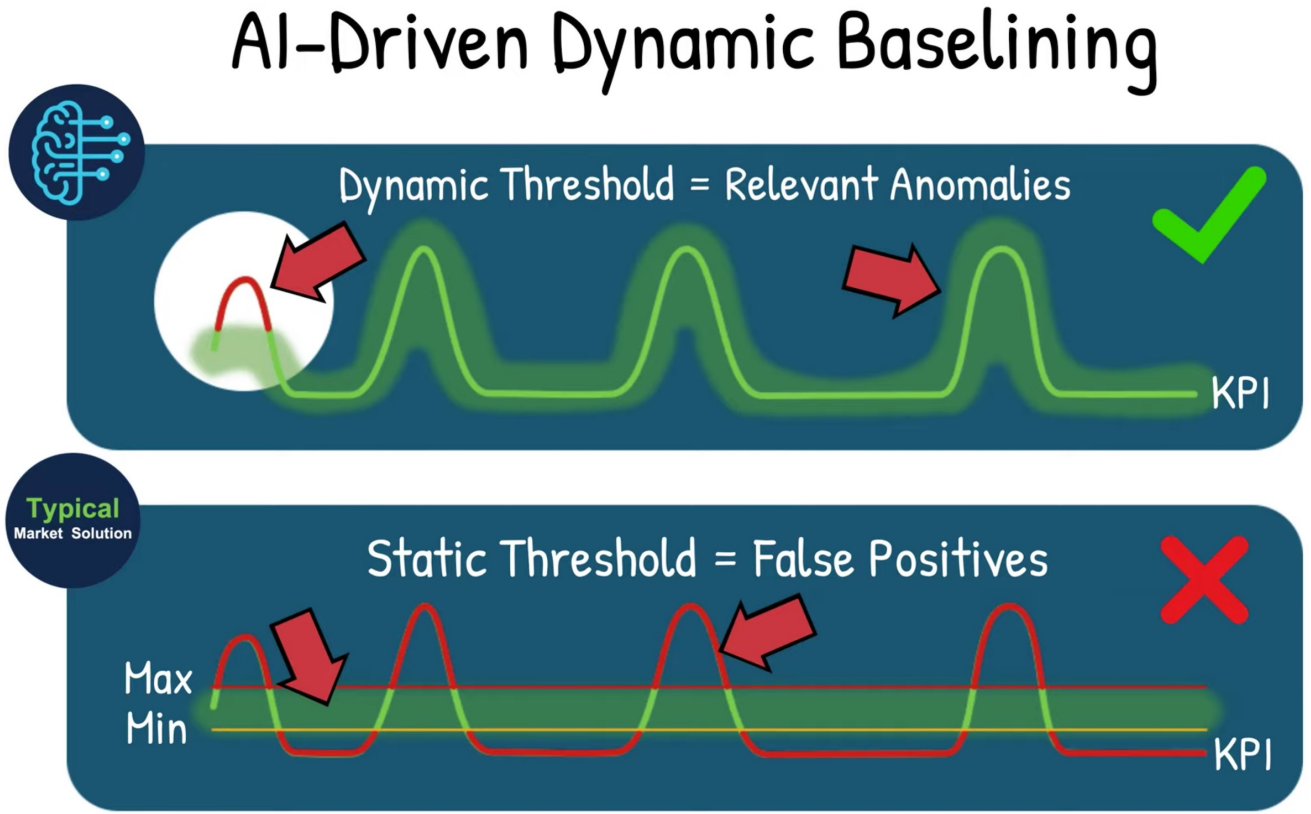
Improve Incident Alert Personalized Baseline

The Key for Success: Small Number of Relevant anomalies

98%

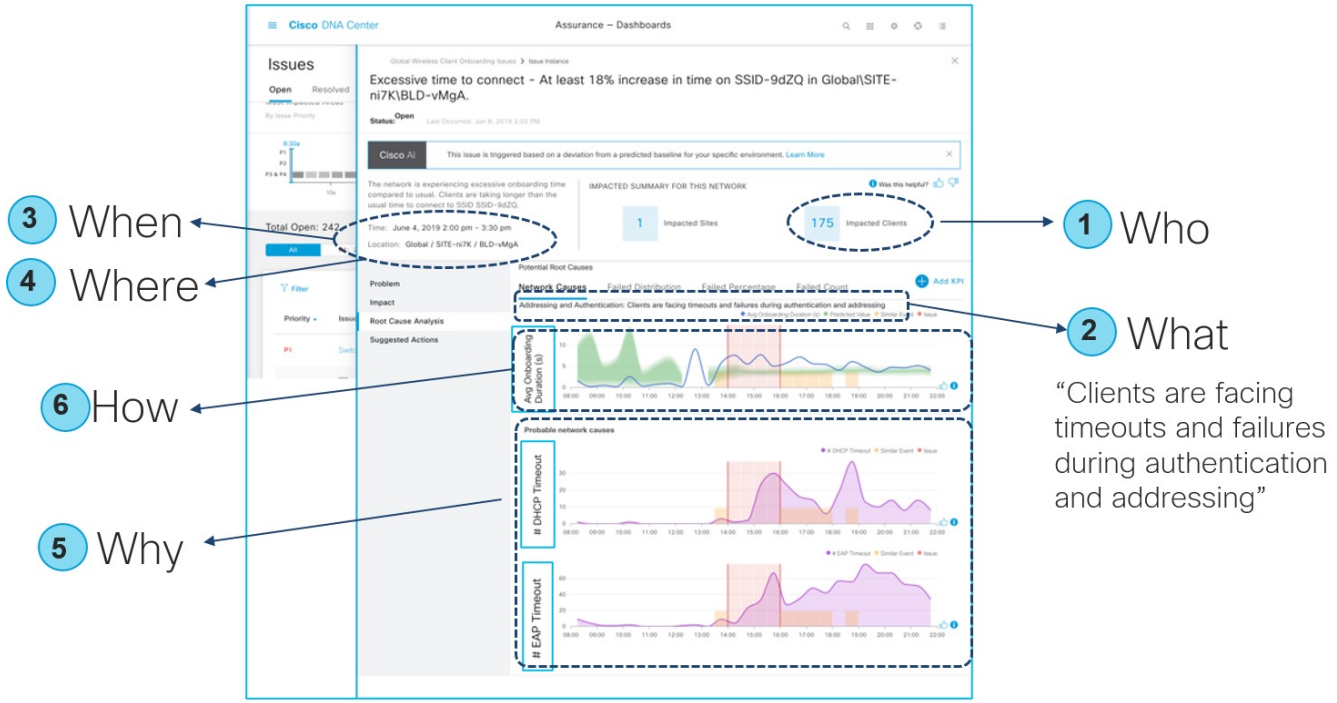
Reduction in Alerts





AI and machine learning insights
→ Root Cause Analysis

- Improve incident alert fidelity – personalized baselining
- Proactive and predictive insights – intelligent analysis
- Accelerated remediation– powered by machine reasoning algorithms
- Discovery of anomaly – long-term trending/behavior change
- Network heatmap and peer comparison



Cisco AI Network Analytics Feature Summary

AI Driven Issues

Discover and Root Cause network risks and anomalies from the **Machine Learning** generated baselines

13 KPIs: Onboarding & Throughput

Network Heatmaps

Optimize AP Performance across the network through visual exploration of performance KPIs

17 KPIs: RF & Application

Peer Comparison

Benchmark your network **Performance** against thousands of similar networks

6 KPIs: RF & Throughput

Network Insights

Mitigate network **risks** with long-term trend analysis across APs and Buildings

5 KPIs: Capacity & Throughput

Network Comparison

Identify improvement opportunities by **Comparing Performance KPIs** across Buildings, AP Models and Endpoint Types

22 KPIs: RF, Onboarding, Throughput

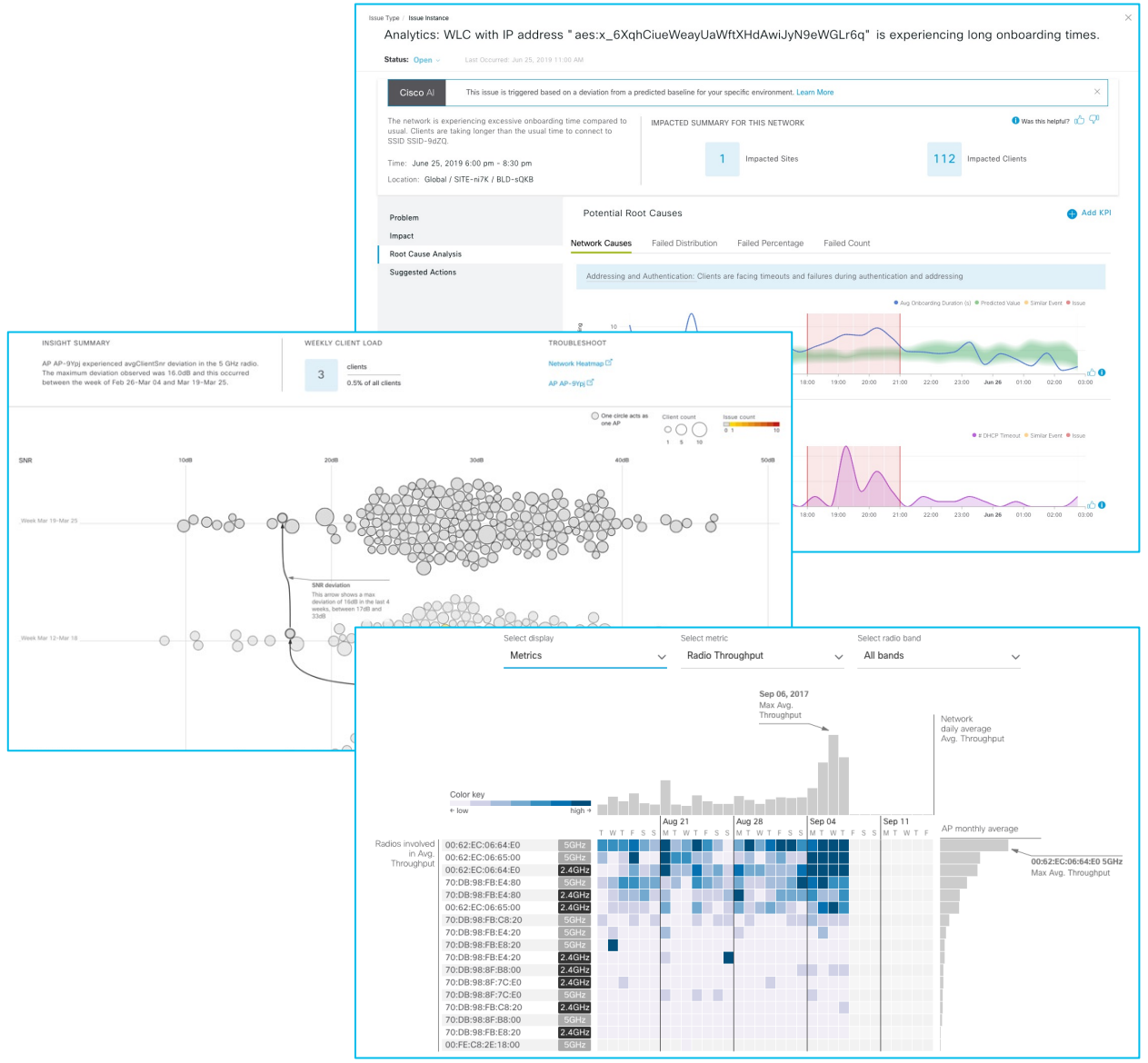
Baselines

Observe historical **Onboarding Behavior** with a **Machine Learning** generated baseline across buildings and SSIDs

5 KPIs: Onboarding

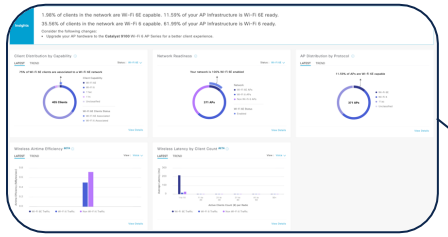
DNAC AI Network Analytics –DEMO

- **AI Network Analytics**
  - Trends and Insights
  - Network Heatmaps
  - Peer Comparison
  - Network Comparison
  - Baselines



Unleash the True Potential of Your Wireless with Cisco DNA Center's AIOps!

Wi-Fi 6E Integrations



Wireless 3D Analyzer

AI-Enhanced RRM

AI Network Analytics

AP Performance Advisories

Device Ecosystem Partnerships

SAMSUNG

intel

Recommended upgrade path (integrated Antenna)

Wireless Controller Transition

100-
150 APs

Distributed Branch, Small Campus

3504
Wireless Controller

C9800-L

C9800-CL
C9800 for cloud

150 to
1500 APs

Medium Campus

5508, 5520
Wireless Controller

C9800-40

C9800-CL
C9800 for cloud

1500 to
6000 APs

Large Campus

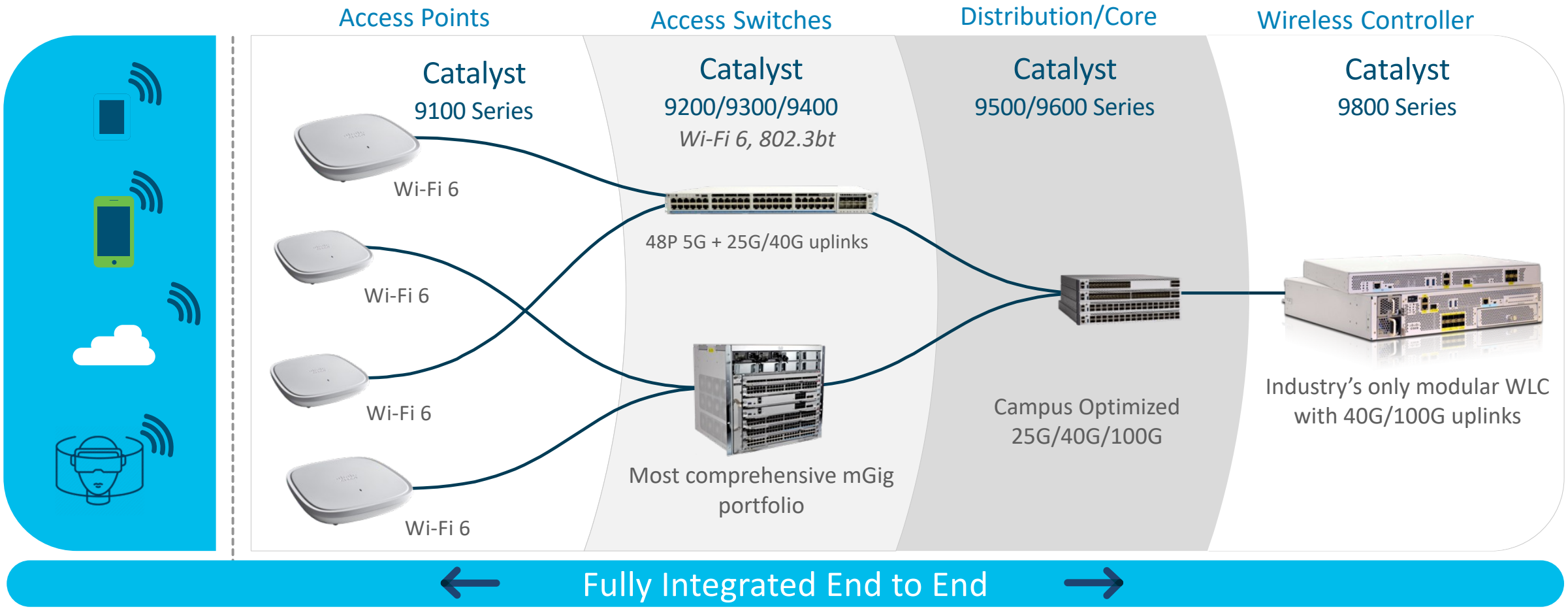
7510, 8510, 8540
Wireless Controller

C9800-80

C9800-CL
C9800 for cloud

Cisco Catalyst Access Network

Best Access Experience for IT and IoT



Fully Integrated End to End

Built for intent-based networking

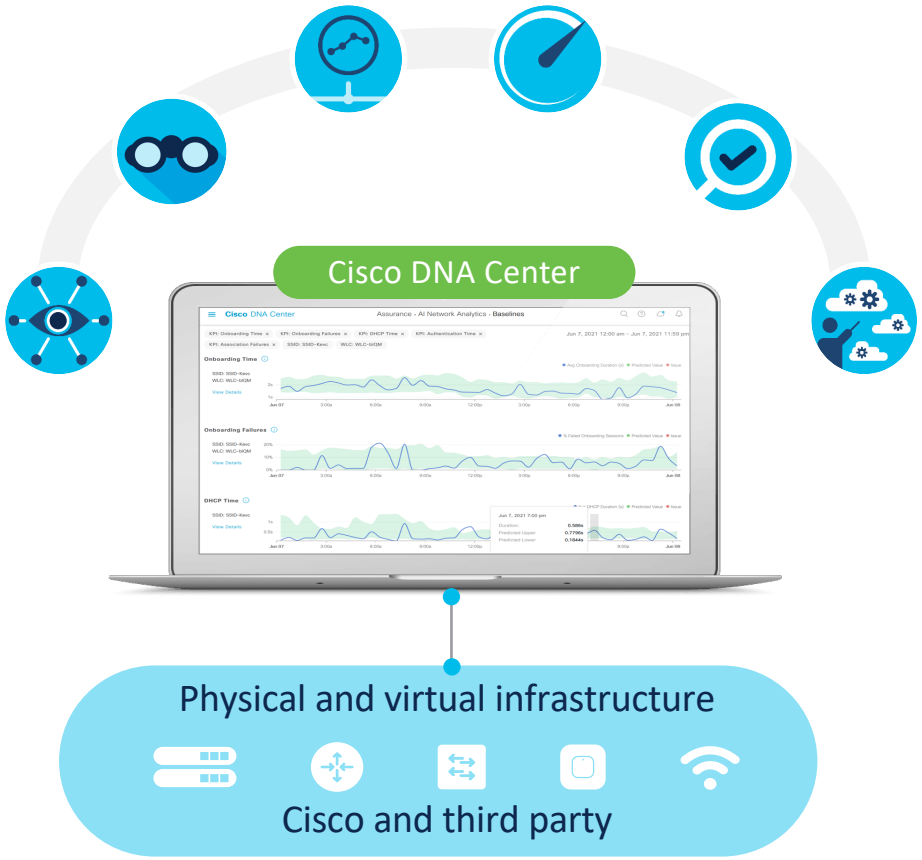
Automation

Security

Analytics

The Four Pillars of Cisco DNA Center

Driving network insights, automation, and security!



AIOps

AI-driven visibility, and troubleshooting to ensure a great user, application and network experience.

NetOps

Automation to simplify the creation and maintenance of your networks.

SecOps

AI-driven security to classify endpoints and enforce security policies.

DevOps

APIs, SDKs, and closed-loop integrations to simplify ecosystem integration.

Cisco DNA Center For Real Engineers

Zvolte jeden nebo více webinářů, kterých se chcete zúčastnit:

- Cisco DNA Center Demo Series - APJC Time Zone
  06:00-07:30 | 8. zář 2022 (UTC+02:00) Tyler Jeffries
- Cisco DNA Center Demo Series - Americas Time Zone
  19:00-20:30 | 8. zář 2022 (UTC+02:00) Tyler Jeffries
- Cisco DNA Center Demo Series - APJC Time Zone
  06:00-07:30 | 15. zář 2022 (UTC+02:00) Tyler Jeffries
- Cisco DNA Center Demo Series - EMEA Time Zone
  12:00-13:30 | 15. zář 2022 (UTC+02:00) Tyler Jeffries

Registrace zde

Vyzkoušejte si funkce DNAC

- Kontakt: dosoukup@cisco.com

- Registrační formulář

CISCO