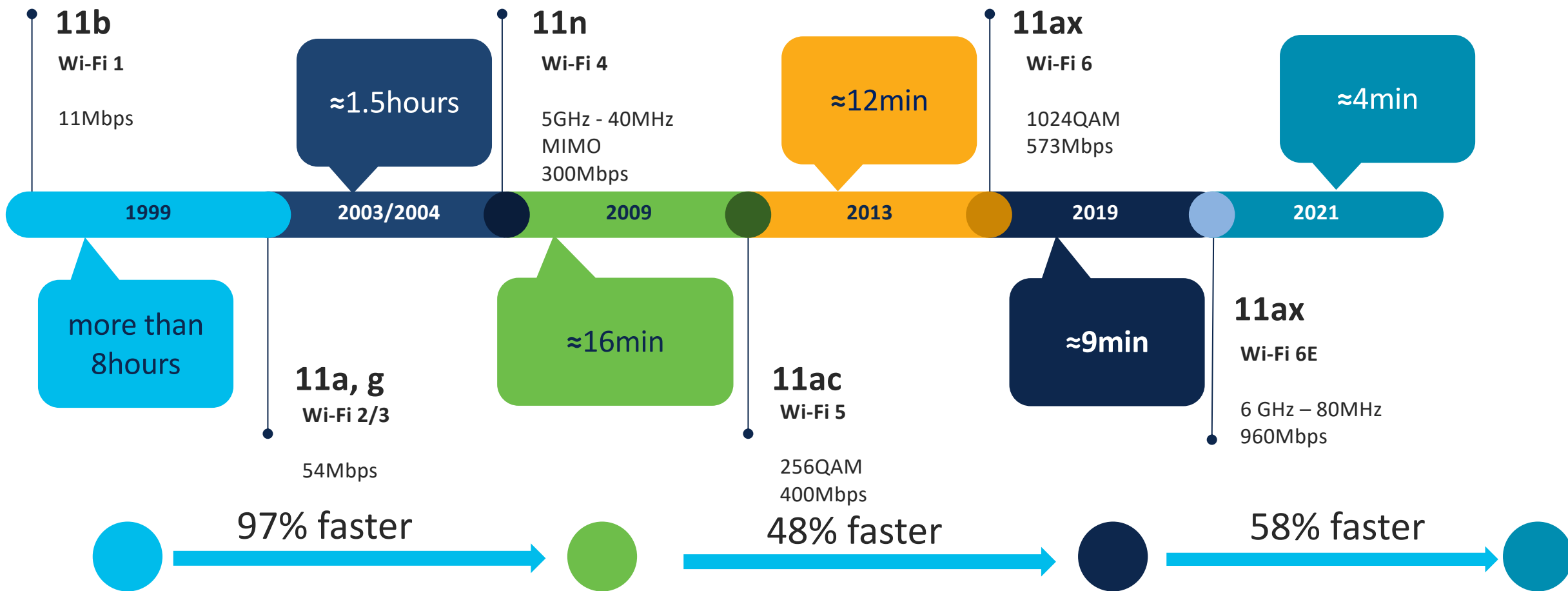
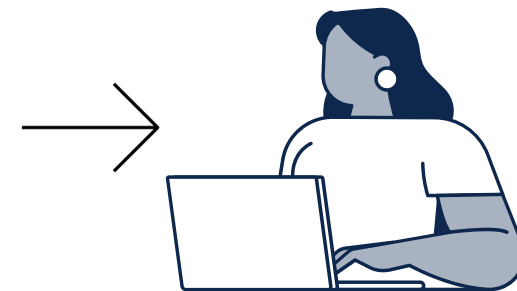


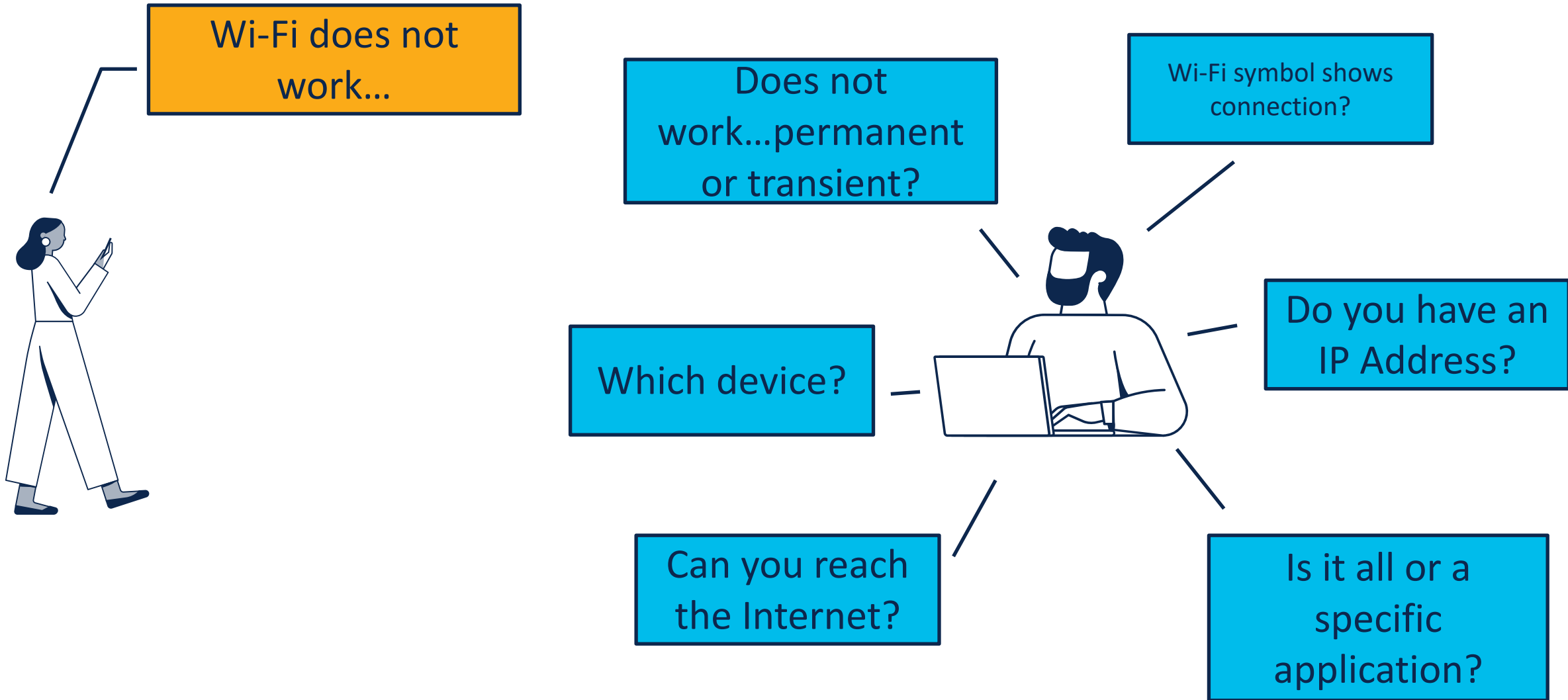


Jak vyzrát na problémy s Wi-Fi

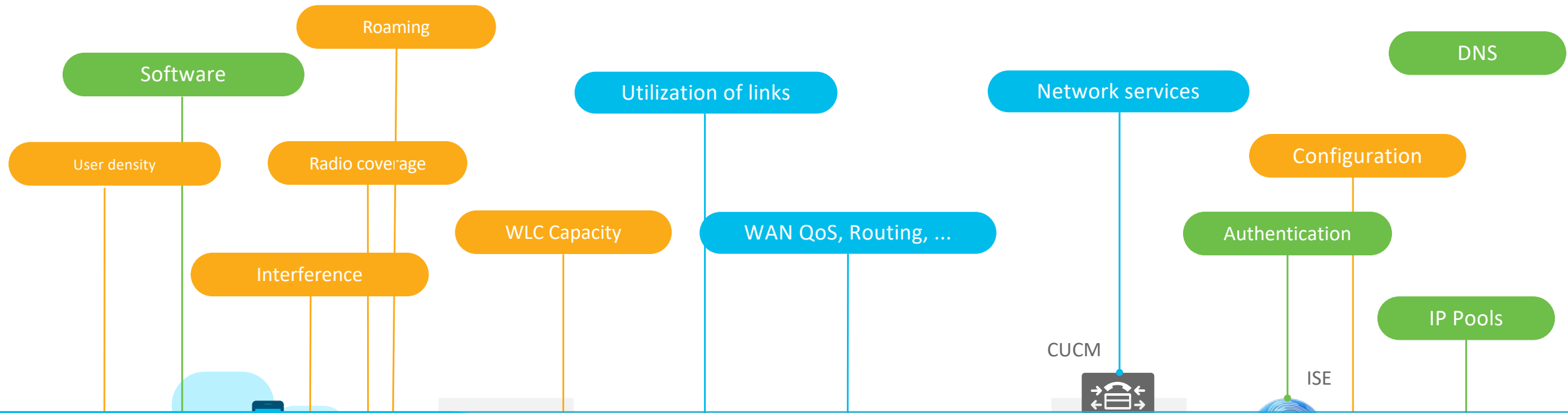
Dominik Soukup
Jaroslav Čížek
20.9.2022



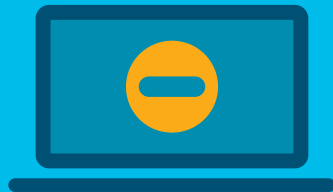
The typical user ticket if a Wi-Fi device is involved...



Network monitoring and diagnostics are difficult and complex



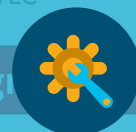
In a typical network, there are over 100 different points of potential failure between the user and the application



What's the problem?



Where is the problem?



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

difficult diagnosis, poor tools, no visibility

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.

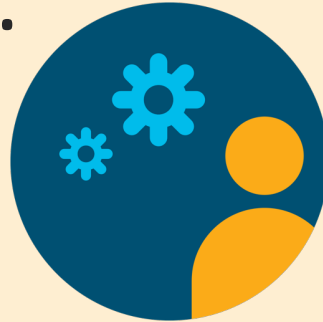
2.



**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.

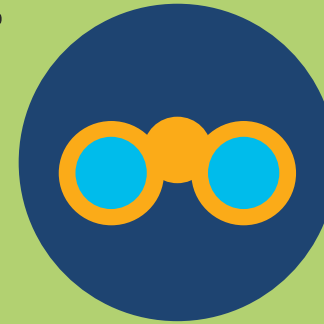
3.



**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)

Search Menu Items

- Dashboard
- Monitoring
- Configuration
- Administration
- Licensing
- Troubleshooting

Monitoring > Client

360 View **General** QoS Statistics ATF Statistics **Mobility History** Call Statistics

Clients

Selected 0 c

Client Address

c8d7...

General

User Name: N/A
Host Name: WinClient-WLAN

MAC Address: c8d7.19bd.c87c [Deauthenticate](#)

Uptime(sec): 54 seconds

WLAN Name: C9k8-66-psk

AP Name: [AP-C9130-JC \(Ch: 56\)](#)

Device Type: Linksys-Device

Client Performance: Signal Strength: -24 dBm Signal Quality: 69 dB
Connection Speed: 0 Mbps
Ch BW(Negotiated/Capable): 40 MHz/80 MHz

Capabilities: 802.11ac

Fabric Status: Disabled

Top Applications

Client

360 View **General** QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

MAC Address	c8d7.19bd.c87c
Client MAC Type	Universally Administered Address
Client DUID	NA
IPv4 Address	192.168.60.150
User Name	N/A
Policy Profile	C9k8-66-psk_profile
Flex Profile	N/A
Wireless LAN Id	19
WLAN Profile Name	C9k8-66-psk_profile
Wireless LAN Network Name (SSID)	C9k8-66-psk
BSSID	2c57.4187.a40f
Uptime(sec)	54 seconds
Idle state timeout	N/A
Session Timeout	36000 sec (Remaining time: 35947 sec)
Session Warning Time	Timer not running
Client Active State	In-Active
Power Save mode	OFF
Supported Rates	6,0,9,0,12,0,18,0,24,0,36,0,48,0,54,0
QoS Average Data Rate Upstream	0 (kbps)
QoS Realtime Average Data Rate Upstream	0 (kbps)

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

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add × Delete ✓ Start ■ Stop [Wireless Debug Analyzer](#)

	MAC/IP Address	Trace file
<input type="checkbox"/>	04eb.409f.c320	<input type="button" value="Generate"/>

1 10 items per page 1 - 1 of 1 items

Enter time interval

Enable Internal Logs

Generate logs for last 10 minutes

30 minutes

1 hour

since last boot

0-4294967295 seconds

- 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|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

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Started**

+ Add × Delete ✓ Start ■ Stop

Wireless Debug Analyzer

	MAC/IP Address	Trace file	
<input type="checkbox"/>	04eb.409f.c320		<input type="button" value="Generate"/>

10 items per page 1 - 1 of 1 items

Troubleshooting > Radioactive Trace

Conditional Debug Global State: **Stopped**

+ Add × Delete ✓ Start ■ Stop

Wireless Debug Analyzer

	MAC/IP Address	Trace file	
<input type="checkbox"/>	04eb.409f.c320	Logs are being generated. Please wait till it completes	<input type="button" value="Generate"/>

10 items per page 1 - 1 of 1 items

- 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}`

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)

Troubleshooting > Packet Capture

+ Add - Delete

Capture Name Interface Monitor Control Plane Buffer Size

10 items per page

Create Packet Capture

Capture Name* MYCAP

Filter* any

Monitor Control Plane

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ~ = 1.00 hour

Available (4) Search

- Tunnel1
- Vlan1
- Vlan70
- Vlan1104

Selected (1)

- GigabitEthernet1

Cancel Apply to Device

- 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

Troubleshooting > Packet Capture

+ Add - Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> MYCAP	GigabitEthernet1	Yes	0%	any	3600 secs	Inactive	<input type="button" value="Start"/> <input type="button" value="Export"/>

1 - 1 of 1 items

C9800 Client/AP troubleshooting –DEMO

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

The screenshot displays the Cisco Catalyst 9800-CL Wireless Controller GUI. The top navigation bar includes the Cisco logo, the title "Cisco Catalyst 9800-CL Wireless Controller 17.9.1", and a "Welcome admin" message. A search bar for "Search APs and Clients" and a "Feedback" button are also present. The left sidebar contains a "Search Menu Items" field and a list of navigation options: Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting (which is highlighted in blue). The main content area is titled "Troubleshooting" and features a grid of six troubleshooting tools: Logs, Core Dump and System Report, Debug Bundle, Packet Capture, Ping and Trace Route, and Radioactive Trace. Each tool has a brief description of its function. A help banner at the top right asks "Need help on what logs to collect for various scenarios?".

The screenshot shows an interactive help dialog titled "How can we assist you?". It features a search bar and a list of troubleshooting tasks. The "Troubleshooting AP Join" section is expanded, showing several diagnostic tasks:

- Are the expected number of APs connected?
- Are there any patterns in AP failure?
- Check for disconnections and discovery failures.
- Let's troubleshoot by a single AP
- Check for wncd issues.
- Check for DTLS Errors
- RadioActive trace with GUI
- Radioactive Trace with CLI

DNAC - Client 360 View

The screenshot displays the Cisco DNA Center interface for a client named Grace.Smith. The interface is divided into several sections:

- Connection details:** A line graph showing health metrics over a 24-hour period.
- CLIENT DETAILS:** Metadata including Device (Samsung Galaxy S10), OS (Android 10), MAC, IP, and SSID.
- Issues (0):** A section for reporting client problems.
- Onboarding:** A section for client onboarding events.
- Event Viewer:** A detailed log of events, such as 'Re-Authentication'.
- Path Trace:** A tool for tracing network paths between source and destination nodes.
- Application Experience:** A section for monitoring application performance.
- Detail Information:** A comprehensive table of client and network data.

Callouts and annotations include:

- Launch Intelligent Capture:** Points to the 'Intelligent Capture' button.
- Path Trace Tool for troubleshooting:** Points to the 'Path Trace' section.
- Individual client issues:** Points to the 'Issues (0)' section.
- Onboarding event viewer:** Points to the 'Event Viewer' section.
- User application experience:** Points to the 'Application Experience' section.
- Apple/Intel client analytics:** Points to the 'Device Info' tab in the detail information table.
- User connectivity details:** Points to the 'Connectivity' tab in the detail information table.
- RF as experienced by the user:** Points to the 'RF' and 'User Defined Network' tabs in the detail information table.

Device Info	Connectivity	RF	User Defined Network
Information			Connection Information
Device Type	Samsung Galaxy S10		Band
Operating System	Android 10		5 GHz
User Name	Grace.Smith		Spatial Streams
Host Name	Grace.Smith-Galaxy-S10		2
MAC Address	A8:B5:27:36:70:09		Channel Width
IPv4 Address	10.30.100.30		20 MHz
IPv6 Address	fe80::7e46:85ff:fe20:3ab1		WMM
			Supported
			U-APSD

DNAC - AP Device 360 View

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Health Dashboards Issues Manage Insights

Device 360

1/10 AP AP4800.8DAC
 Device Model: AIR-AP4800-B-K9 IP Address: 10.13.5.114 Location: Global / San Francisco / One Bush St / Flr13 Software Version: 8.8.120.6 Mode: FlexConnect

Jul 15, 2019 6:35 am
Device Health: 10
 *Device Health is the minimum of all KPI Health Scores.

System Resources		Data Plane		Radio 0		Radio 1	
Memory Utilization	10	46%	Link Errors	10	--	Noise	10
CPU Utilization	10	5%	Air Quality	10	--	Air Quality	10
			Interference	10	--	Interference	10
			Radio Utilization	10	--	Radio Utilization	17

P3 AP Anomaly
 AP F4:DB:E6:86:F1:E0 missed during beacon scan. No immediate action required.
 Instance Count: 260

Radio 0 Channel and Width

Current Channel: 36
 Current Channel Width: 20 MHz
 Band: 5 GHz
 RF Profile: NA
 Mode: Monitor

Radio 0 Channel Utilization

Radio 0 Interference

Radio 1 Channel and Width

Current Channel: 52
 Current Channel Width: 80 MHz
 Band: 5 GHz
 RF Profile: NA
 Mode: Remote

Radio 1 Channel Utilization

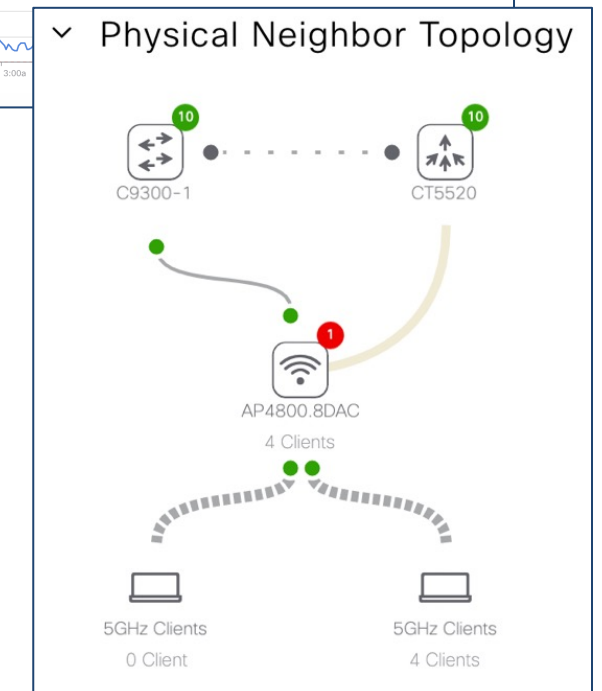
Radio 1 Interference

<input type="checkbox"/>	4C:71:0D:B5:C8:02	--	-59	6	Rogue	internet	--	--
<input type="checkbox"/>	4C:71:0D:B5:C8:03	--	-59	6	Rogue	blizzard-legacy	--	--

11 Records Show Records: 10

Access Points 2.4 GHz RSSI > -60 dBm

Legend: Neighbor (Colorful), Rogue (Purple), Current Channel (Blue)



DNAC - Intelligent Capture Client Dashboard

14 Day Time Travel

Anomaly Packet Capture

Client Statistics

Data Packet Capture

Live Packet Capture

Real-Time Client Location

Intelligent Capture: Grace.Smith

Run Data Packet Capture Download Start Live Capture

1 hour Nov 15 1:30p 1:35p 1:40p 1:45p 1:50p 1:55p 2:00p 2:05p 2:10p 2:15p 2:20p 2:25p 2:30p

Onboarding Events **LIVE**

All Anomaly PCAP Export PCAP

Nov 15, 2020	Time	Duration
● Authentication Start	2:07:23 pm	
● DHCP	2:07:23 pm	
● Broadcast Rekey PCAP	2:02:23 pm	< 1 ms
● Client Deauthenticated	2:02:23 pm	
● KeyExchange PCAP	2:02:23 pm	
● Broadcast Rekey	2:02:23 pm	
> ● Delete	1:57:23 pm	< 1 ms
● Onboarding	1:52:23 pm	< 1 ms
● Run	1:52:23 pm	
● DHCP	1:52:23 pm	
● DHCP	1:52:23 pm	
● Mobility	1:52:23 pm	
● KeyExchange	1:52:23 pm	

Client Location **LIVE**

Global/San Jose/SJC01/Floor 1 Client trail by RSSI

RF Statistics **LIVE**

RSSI, SNR, Rx Data Rate, Tx/Rx Packet, Tx Retry Count

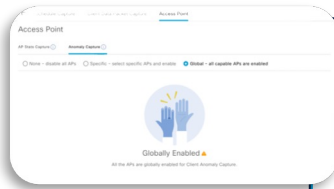
RSSI (dBm) SNR (dB)

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

Always-on Anomaly Capture

Discover and root case issues

1 Enable Anomaly Capture



Cisco DNA Center Assurance - Dashboards - Health - User 360

Intelligent Capture: Grace.Smit

1 hour

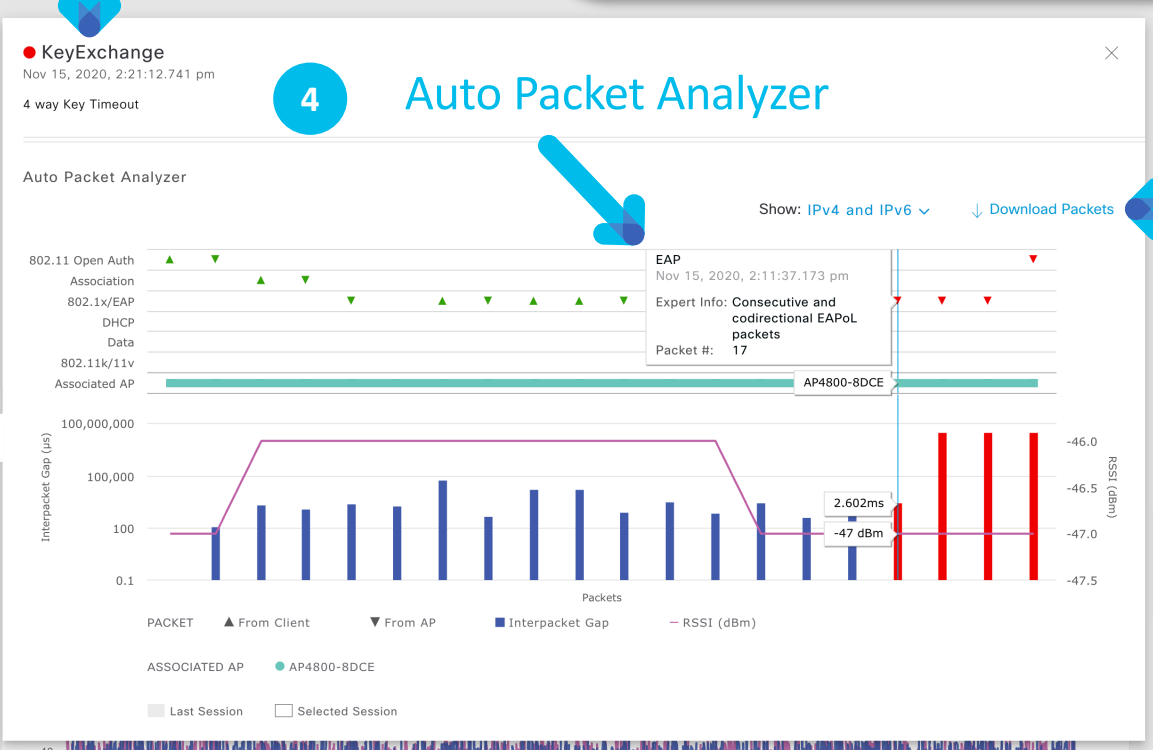
Nov 15 1:42p

3 Anomaly Type

2 Anomaly Event Packet Capture

Event Legend:
 Red = Anomaly event
 Green = Healthy event

Time	Duration
2:36:17 pm	< 1 ms
2:36:12 pm	< 1 ms
2:31:12 pm	< 1 ms
2:26:12 pm	< 1 ms
2:21:12 pm	< 1 ms
2:21:12 pm	< 1 ms
2:21:12 pm	< 1 ms
2:16:12 pm	< 1 ms
2:11:12 pm	< 1 ms
2:06:12 pm	< 1 ms
2:01:12 pm	< 1 ms
1:56:12 pm	< 1 ms



4 Auto Packet Analyzer

70695a631380_80211_1603980847905181.pcap

Apply a display filter ... <36/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_63:13:80	Cisco_9e:b1:c7	802.11	56	Authentication, SN=1695, FN=0, Flags=.....
2	0.003972	Cisco_9e:b1:c7	Cisco_63:13:80	802.11	56	Authentication, SN=0, FN=0, Flags=.....
3	0.004563	Cisco_63:13:80	Cisco_9e:b1:c7	802.11	161	Association Request, SN=1696, FN=0, Flags=.....
4	0.011495	Cisco_9e:b1:c7	Cisco_63:13:80	802.11	194	Association Response, SN=1, FN=0, Flags=.....
5	0.012977	Cisco_9e:b1:c7	Cisco_63:13:80	EAPOL	159	Key (Message 1 of 4)
6	1.105103	Cisco_9e:b1:c7	Cisco_63:13:80	EAPOL	159	Key (Message 1 of 4)
7	2.096703	Cisco_9e:b1:c7	Cisco_63:13:80	EAPOL	159	Key (Message 1 of 4)
8	3.088943	Cisco_9e:b1:c7	Cisco_63:13:80	802.11	52	Deauthentication, SN=2, FN=0, Flags=.....

Frame 15: 52 bytes on wire (416 bits), 52 bytes captured (416 bits)

Radiotap Header v0, Length 26

802.11 radio information

IEEE 802.11 Deauthentication, Flags:

IEEE 802.11 Wireless Management

Fixed parameters (2 bytes)

Reason code: 4-Way Handshake timeout (0x000f)

6 Validate Issue

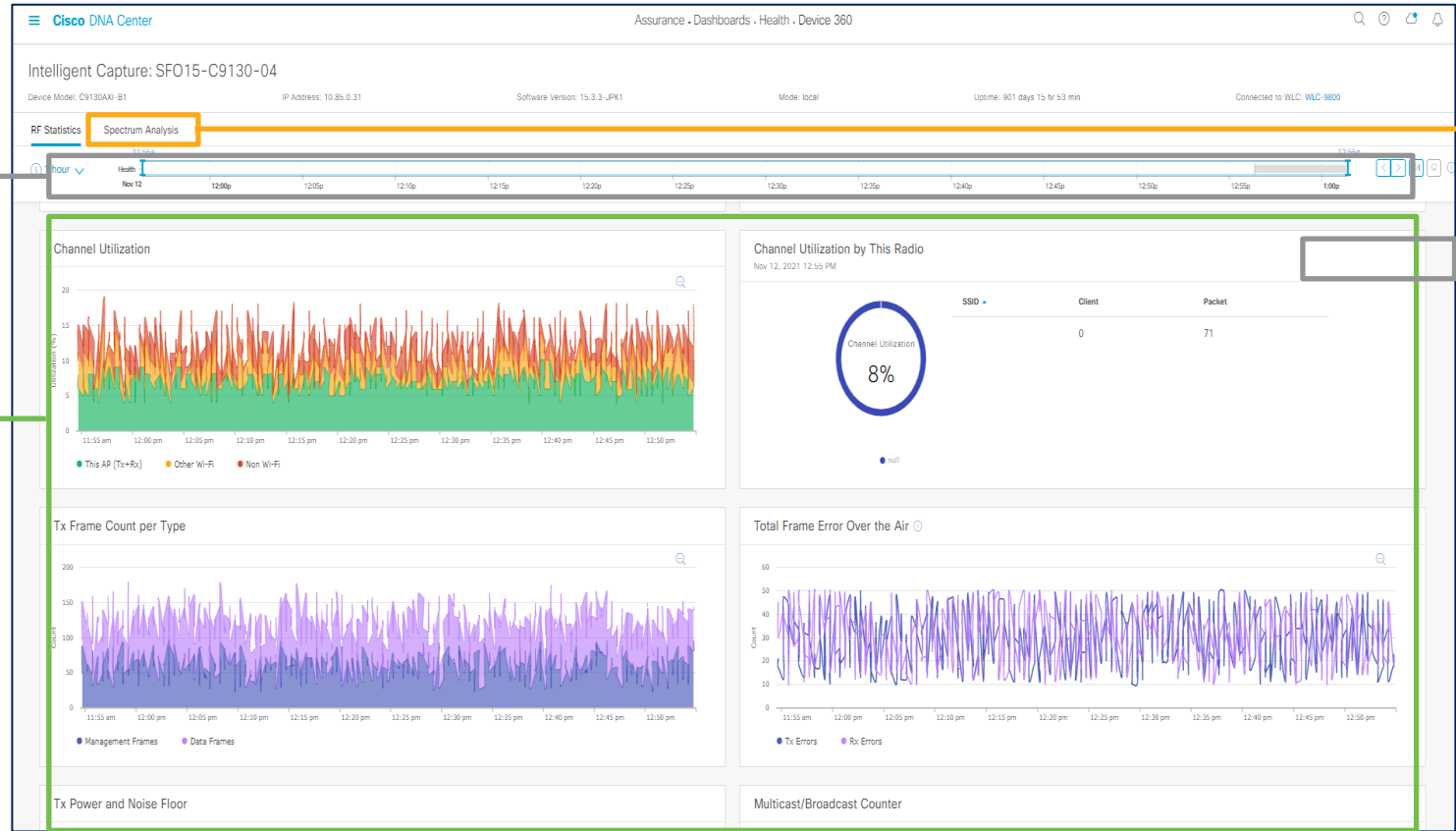
5 Download Packets

DNAC - Intelligent Capture AP Dashboard

14 Day
Time Travel

Always-on AP
RF Statistics

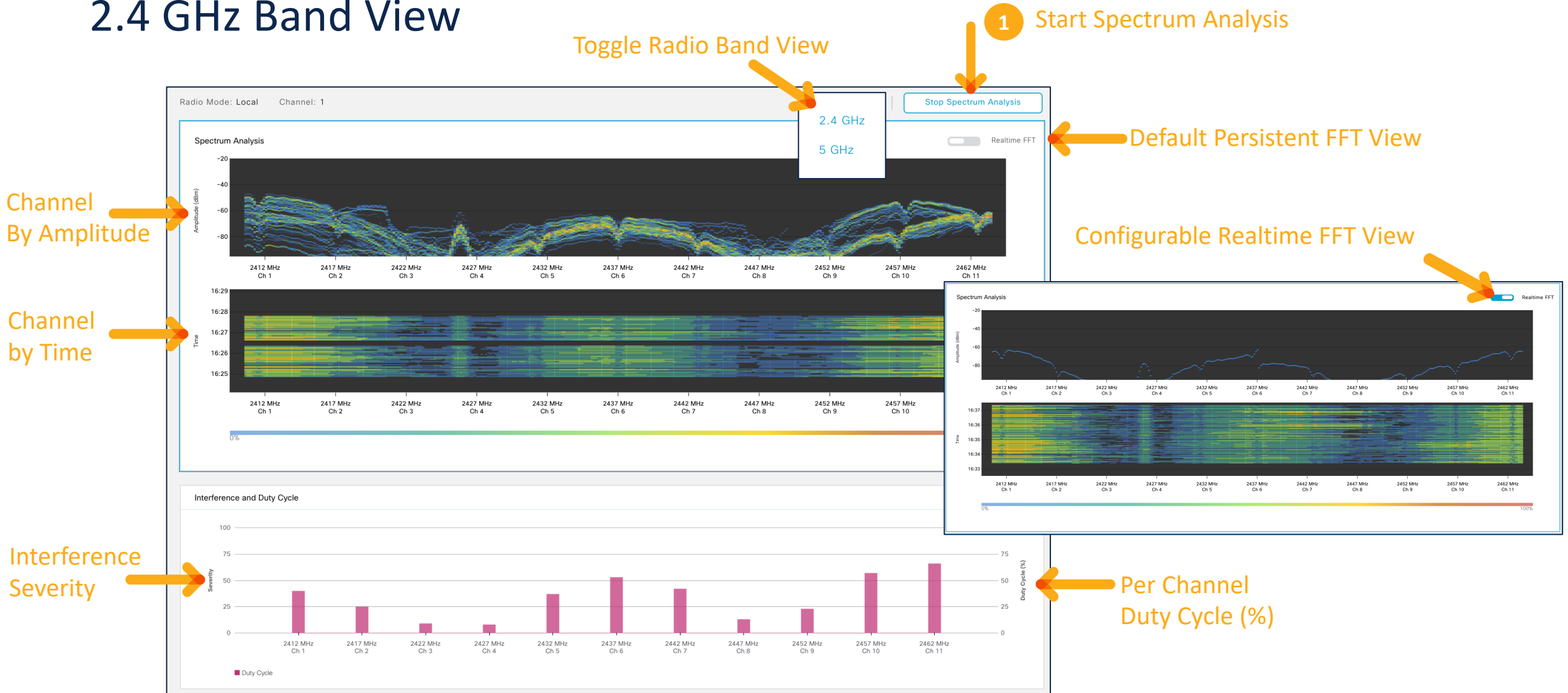
On-demand
Spectrum
Analysis



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

On-demand Spectrum Analysis

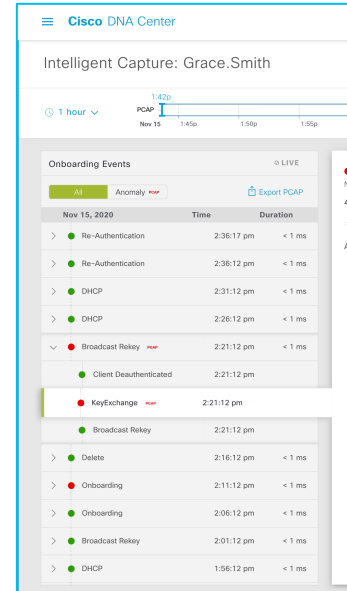
2.4 GHz Band View



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

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



SAMSUNG

intel®

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.

Neighbor AP Table

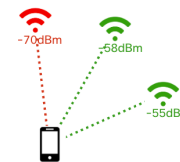
Neighbor APs (3)

Search Table

BSSID	AP Name	Channel	RSSI (dBm)	Location
38:90:A5:CD:69:8F	LAB-AP00F2.8B27.B788	165	-55	Global/North America/USA/(
38:90:A5:CD:69:7F	AP0081.C424.3CE2	162	-70	Global/North America/USA/(
38:90:A5:CD:69:6F	SCJ01_9130_1	161	-58	Global/North America/USA/(

Show Records: 10

Neighbor AP Visual



Dedicated iOS Analytics Tab

Disassociation Details

Time

Disassociation Reason

May 9, 2022 9:58 PM	User triggered disassociation
May 9, 2022 9:53 PM	Device idle
May 9, 2022 9:48 PM	User triggered disassociation
May 9, 2022 9:43 PM	Device idle

Show Records: 10

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

Event Viewer

Filter Export Find

May 11, 2022

>	● INTRA-WLC Roaming	5:51:50.561 PM - 5:51:50.561 PM	
∨	● Client Sent Disassociation	5:47:50.561 PM	
	● Client Sent Disassociation	5:47:50.561 PM	Wi-Fi Device Turned Off
>	● Onboarding -- Incomplete	5:43:50.561 PM - 5:43:50.561 PM	AP:AP4800 WLAN:@CorpSSID 🗑️
∨	● Client Sent Disassociation	5:39:50.561 PM	AP:AP4800 WLAN:@CorpSSID
	● Client Sent Disassociation	5:39:50.561 PM	Airplane Mode Turned On
>	● DHCP	5:35:50.561 PM - 5:35:50.561 PM	
>	● Broadcast Rekey	5:31:50.561 PM - 5:31:50.561 PM	

Showing 5 - 13 of 335

Device Turned Off

Airplane Mode Turned On

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

Detail Information Jun 2, 2022 3:19 PM

Device Info Connectivity RF Intel Connectivity Analytics

Roam Events [View All Roam Events](#)

Jun 2, 2022 3:05 PM Jun 2, 2022 2:35 PM Jun 2, 2022 2:05 PM Jun 2, 2022 1:58 PM Jun 2, 2022 1:35 PM

Reason Code: Other Selected AP: OTA-9136B-17E0 BSSID: 68:7D:B4:5F:1D:68 RSSI: -79 dBm

Reported Errors [View All Reported Errors](#)

Temporary Disconnection Reports [View All Temporary Disconnection Reports](#)

Low RSSI Reports [View All Low RSSI Reports](#)

Jun 2, 2022 3:05 PM
2 Access Points

Access Point: OTA-9136B-17FC
BSSID: 68:7D:B4:5F:1E:B8
Frame Type: Authentication Response
Error: Missing Response

Access Point: OTA-9136B-17E0
BSSID: 68:7D:B4:5F:1D:68
Frame Type: Authentication Response
Error: Missing Response

No data available

Jun 2, 2022 3:10 PM
Access Point: OTA-9136B-17E0
BSSID: 68:7D:B4:5F:1D:68
RSSI: -79 dBm

Jun 2, 2022 2:56 PM
Access Point: OTA-9136B-17E0
BSSID: 68:7D:B4:5F:1D:68
RSSI: -79 dBm

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

Monitoring > Wireless > Clients

360 View AP CAC QOS Sensor Statistics TrustSec EoGRE

General

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

	Slot 0 (2.4 GHz)	Slot 1 (5 GHz)
Radio Type	802.11ax - 2.4 GHz	802.11ax - 5 GHz
Radio Role	Remote	Remote
Admin Status	Enabled	Enabled
Number of Clients	0	1
Current Channel	11	100
Power Level	*1/7 (13 dBm)	*1/8 (22 dBm)
Channel Utilization	33%	3%
Transmit Utilization	5%	1%
Receive Utilization	0%	0%

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

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	AP1416.9D56.1240

Client

360 View General QOS Statistics ATF Statistics Mobility History Call Statistics

General

User Name: N/A

MAC Address: 8866.5a46.6e7d

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

Monitoring > Wireless > AP Statistics

General Join Statistics

Current Active
AP1416.9D56.1240

Clear ClearAll

Total APs : 1

AP Name	AP Model	Status	IP Address
AP1416.9D56.1240	C9130AXI-E	+	192.168.128.189

Monitoring > Wireless > AP 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



So anyway, I started blasting

Wireless Troubleshooting - Automation

Why?	What?
<p data-bbox="366 297 917 334">Efficient Client Troubleshooting</p> <p data-bbox="45 348 1243 515">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.</p>	<ul data-bbox="1284 297 2474 491" style="list-style-type: none">▪ 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
<p data-bbox="315 546 968 584">Uninterrupted Embedded Packet Capture</p> <p data-bbox="56 598 1230 765">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.</p>	<ul data-bbox="1284 546 2397 791" style="list-style-type: none">▪ 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
<p data-bbox="290 825 993 862">Automated Archive request and export</p> <p data-bbox="56 876 1230 1001">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.</p>	<ul data-bbox="1284 825 2346 962" style="list-style-type: none">▪ Configure & Export Archive traces from 9800 using EEM▪ Periodical & timed log capture for efficient troubleshooting▪ MRE Workflow integration work in progress
<p data-bbox="529 1082 754 1119">KPI Collector</p> <p data-bbox="45 1133 1243 1208">This tool will help to automate data collection (KPI or Action Plan), ensures we have the right data collected</p>	<ul data-bbox="1284 1082 2430 1326" style="list-style-type: none">▪ 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

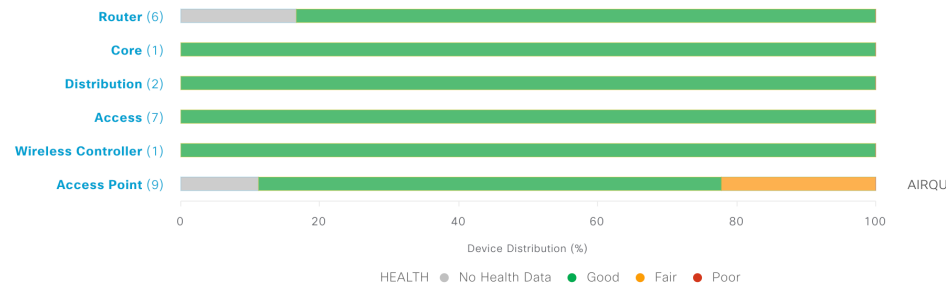
LATEST TREND

Network Devices

85% [ⓘ]

Healthy Network Devices

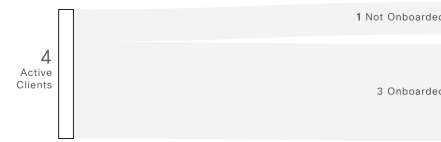
TOTAL DEVICES	26
Good Health	22
Fair Health	2
Poor Health	--
No Health Data	2



Wireless Clients

75% [ⓘ]
Healthy

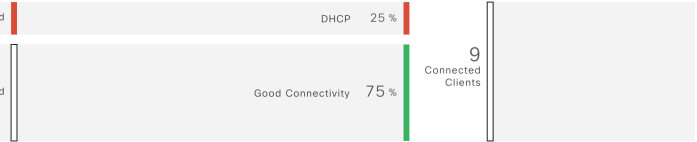
TOTAL: 4
Active: 4 | Inactive: 0 | New: 0 [ⓘ]



Wired Clients

100% [ⓘ]
Healthy

TOTAL: 9
Connected: 9 | No L

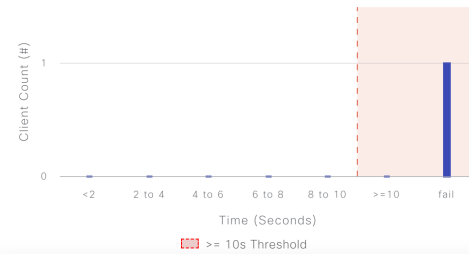


[View Details](#)

Client Onboarding Times

LATEST TREND

0% clients with onboarding times < 10 s

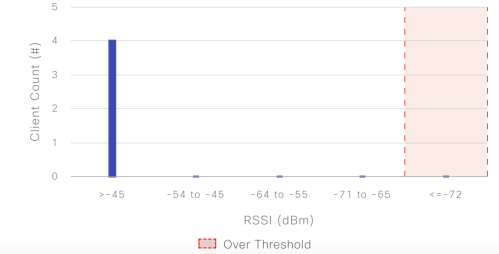


[View Details](#)

Connectivity RSSI

LATEST TREND

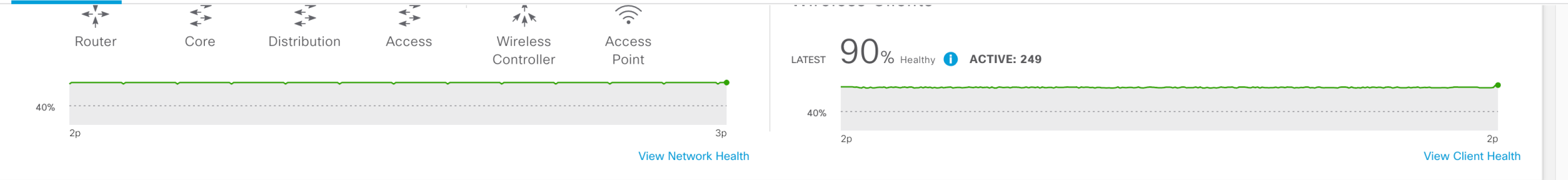
100% clients with RSSI > -72 dBm



[View Details](#)

Issues and Guided Remediations

Dashboards ▾ Trends And Insights ▾ Manage ▾



Top 10 Issue Types

Priority ▾	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P1	Fabric Devices Connectivity - ISE Server	BORDER ROUTER	Connected	7	1	1	May 15, 2020 7:34 am
P1	TCAM Utilization High Issues	BORDER ROUTER	Device	6	1	1	May 15, 2020 7:04 am
P1	Interface Connecting Network Devices is Down	ACCESS	Connectivity	7	1	1	May 15, 2020 6:52 am
P2	Layer 2 loop symptoms	DISTRIBUTION	Connectivity	14	1	2	May 15, 2020 6:50 am
P3	Wireless clients failed to connect - AAA Server Rejected Clients	WIRELESS	Onboarding	14	2	2	May 15, 2020 8:00 am
P3	Wireless clients failed to connect - Failed to authenticate due to Client Timeouts	WIRELESS	Onboarding	45	3	7	May 15, 2020 7:58 am
P3	Wireless clients failed to connect - Security Parameter Mismatch	WIRELESS	Onboarding	17	2	3	May 15, 2020 7:56 am

[View All Open Issues](#)

Global Event Viewer

Network Devices

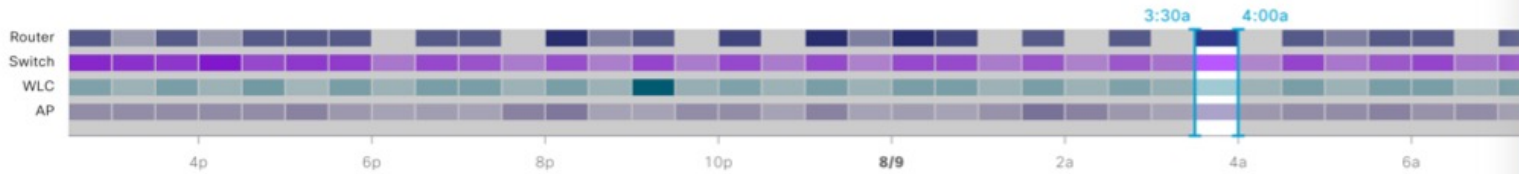
☰ Cisco DNA Center

Assurance / Dashboards / Issues & Events



Issues ▾ **Events**

📍 Global ⋮ ⌚ 24 Hours ▾



Tx Power Change

Aug 9, 2022 3:50 AM	Info
Event Type	Device Event
Reason	System Driven : Tx Power change due to OpenRRM.
Device Name	📶 APF4DB.E643.851C
Device IP	192.168.138.4
Location	Global/Prague/PRG07/PRG07-5
WLC Name	WLC-9800-SDA.enprglab.local
AP Mac	F4:DB:E6:44:46:60
Radio	0
Frequency	2.4GHz
Current Power Level	12 dBm
Previous Power Level	15 dBm

Events (103) ⓘ

Device Family **Router: 17** **Switch: 70** **WLC: 6** **AP: 10**

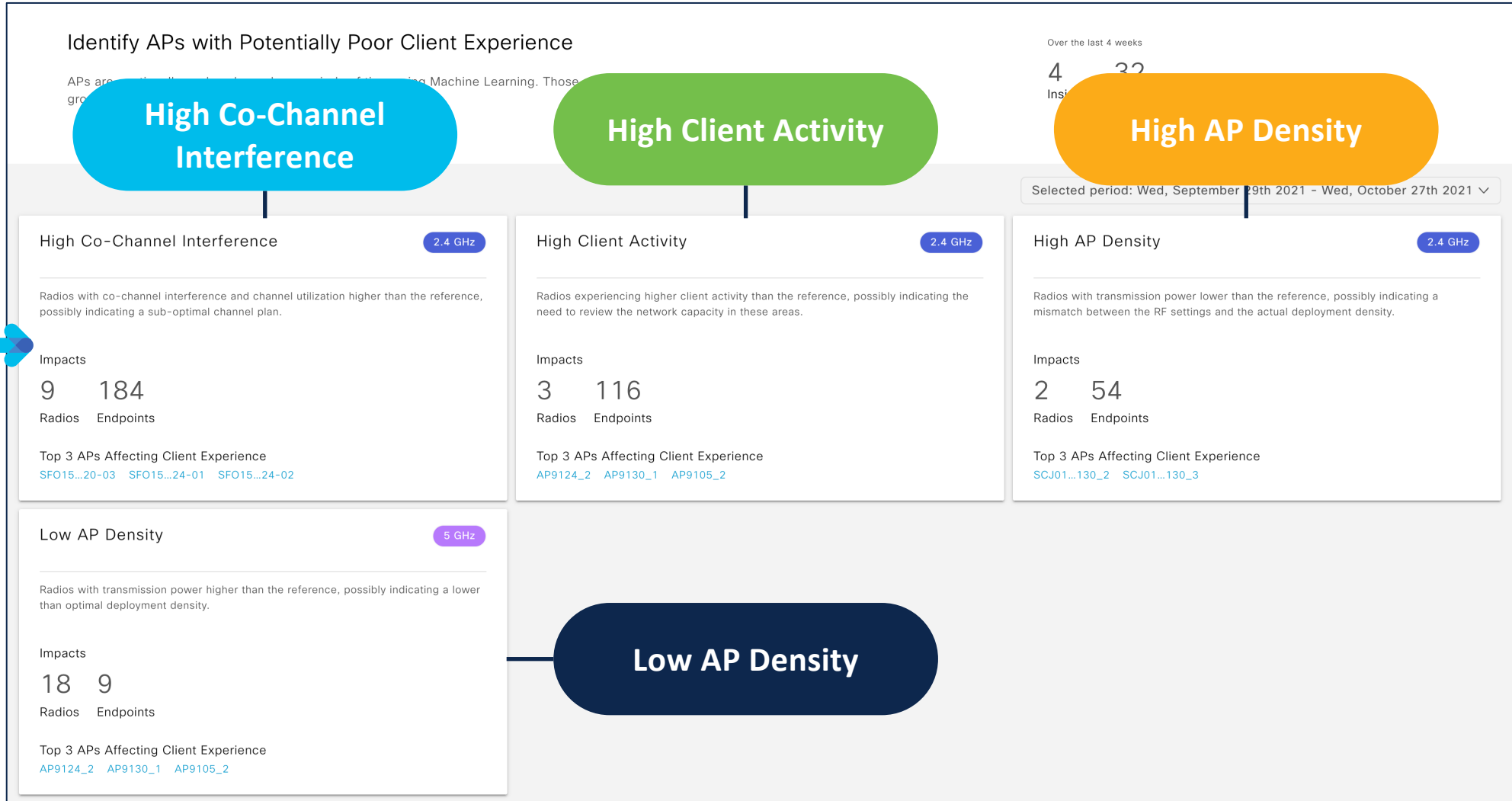
🔍 Severity × Event Name ×

0 Selected

<input type="checkbox"/>	Event Name	Status	Severity	Timestamp ▾	Device Name
<input type="checkbox"/>	Tx Power Change	●	Info	Aug 9, 2022 3:50 AM	📶 APF4DB.E643.851C

1 Records

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.

Reality** about Wi-Fi



Nature of RF

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

- 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.

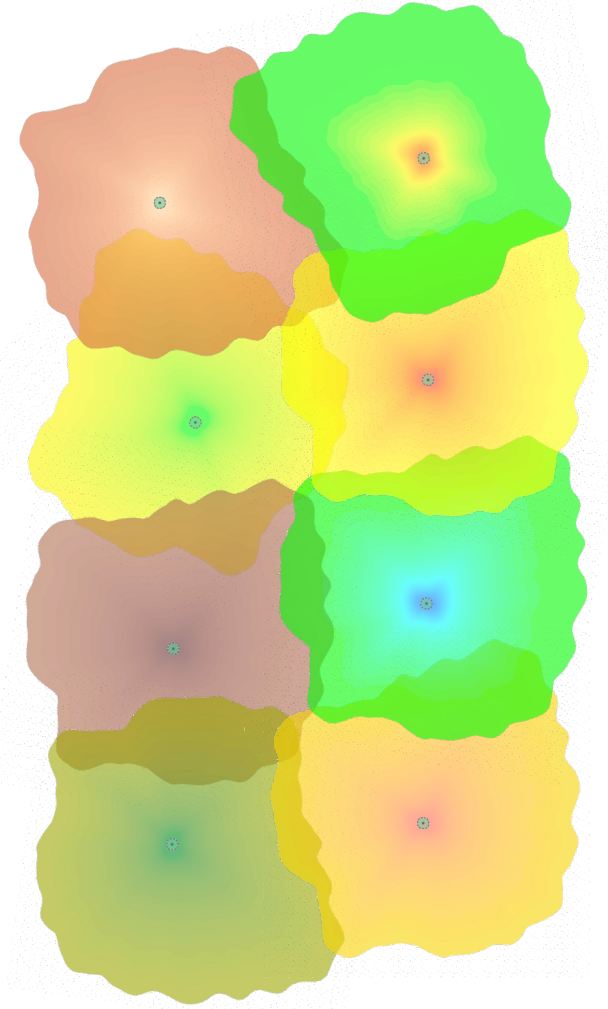
Some Examples:

Flexible
Radio Assignment

Transmit
Power Control

Dynamic
Channel Assignment

Dynamic
Band Selection



AI Radio Frequency Profile

Edit AI Radio Frequency Profile

Profile Name
RRM_RF_PROFILE

Basic Settings

Radio Frequency Settings

2.4 GHz 5 GHz

Busy Hours ⓘ

Start time: 17:00 | End time: 23:00 | Busy Hour Sensitivity ⓘ: Low Medium High

Enable RF Settings

	2.4 GHz	5 GHz
Flexible Radio Assignment ⓘ	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Channel Assignment ⓘ	<input type="checkbox"/>	<input type="checkbox"/>
Transmit Power Control ⓘ	<input type="checkbox"/>	<input type="checkbox"/>
Dynamic Bandwidth Selection ⓘ	<input type="checkbox"/>	<input type="checkbox"/>

AI-Enhanced RRM Control Center

24 Hours | Band: 5GHz | 2.4GHz | AI RF Profile: RRM_RF_PROFILE | Next RRM Run: 13 m 18 s | Jun 1, 2022 9:05 PM - Jun 2, 2022 9:05 PM

Enhanced RRM supports 2.4 GHz and 5 GHz bands for AI RF Profiles. 6 GHz support is coming soon.

SUMMARY		RF PERFORMANCE SUMMARY		RF COVERAGE SUMMARY	
Total AP Count	22	RRM Performance	99 / 100	AP Density	High
Total Clients	37	APs with High CCI ⓘ	0 %	Connectivity	High (35 dB)
		RRM Changes	16		

Insights

- Consider changing the configured Busy Hours for RRM to be more effective.

RF Performance

RRM Changes ⓘ

LATEST TREND

Total APs Optimized: 2

View Details

RRM Performance ⓘ

LATEST TREND

Total Access Points: 22

View Details

Co-Channel Interference ⓘ

LATEST TREND

Total Access Points: 22

View Details

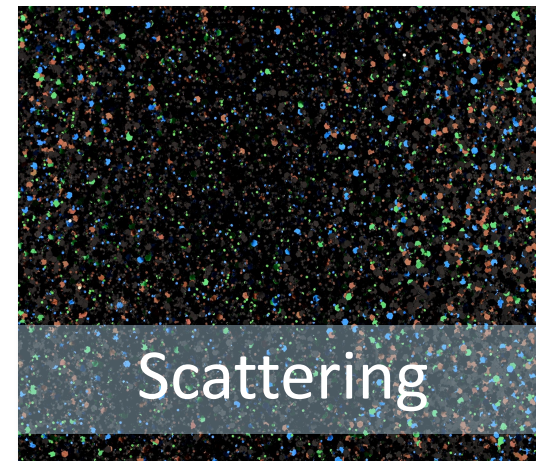
AI-Enhanced RRM

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

Visualization of the wireless network



What else happens in the air?



Cat9800 RF Visualization

Radio Statistics

Cisco Catalyst 9800-L Wireless Controller 17.8.1

Welcome dnac

Search APs and Clients

Feedback

Monitoring > Wireless > Radio Statistics

6 GHz Radios 5 GHz Radios 2.4 GHz Radios Dual-Band Radios

Total 5 GHz radios : 14

AP Name	AP Model	Slot No	Base Radio MAC	IP Address	Admin Status	Operation Status	Uptime	Radio Role (Radio MAC)
AP687D.B45C.A2A0	C9136I-E	1	00df.1ddb.9ec0	192.168.138.8	✓	➕	31 days 20 hrs 32 mins 29 secs	Automatic
AP687D.B45C.A2A0	C9136I-E	2	00df.1ddb.9ec0	192.168.138.8	⊘	➖	31 days 20 hrs 32 mins 29 secs	Automatic
AP488B.0A77.5F6C	C9124AXD-E	1	2c1a.0584.f0e0	192.168.138.6	✓	➕	41 days 19 hrs 52 mins 10 secs	Automatic
AP1416.9D56.070C	C9130AXI-E	1	548a.ba21.55c0	192.168.138.2	✓	➕	41 days 2 hrs 9 mins 4 secs	Automatic
AP1416.9D56.070C	C9130AXI-E	2	548a.ba21.55c0	192.168.138.2	✓	➕	41 days 2 hrs 9 mins 4 secs	Automatic
AP1416.9D56.0E08	C9130AXI-E	1	548a.ba26.ac40	192.168.138.11	✓	➕	41 days 12 hrs 41 mins 37 secs	Automatic
AP1416.9D56.0E08	C9130AXI-E	2	548a.ba26.ac40	192.168.138.11	✓	➕	41 days 12 hrs 41 mins 37 secs	Automatic (Monitor)
AP1416.9D56.0EB4	C9130AXI-E	1	548a.ba26.b1a0	192.168.138.1	✓	➕	41 days 12 hrs 42 mins 4 secs	Automatic
AP1416.9D56.0EB4	C9130AXI-E	2	548a.ba26.b1a0	192.168.138.1	✓	➕	41 days 12 hrs 42 mins 4 secs	Automatic
AP1416.9D56.123C	C9130AXI-E	1	548a.ba26.cde0	192.168.138.3	✓	➕	41 days 12 hrs 47 mins 33 secs	Automatic

1 2 10



Cat9800 RF Visualization

CleanAir Statistics

Cisco Catalyst 9800-L Wireless Controller 17.8.1

Welcome *dnac*

Search APs and Clients

Feedback

Monitoring > Wireless > CleanAir Statistics

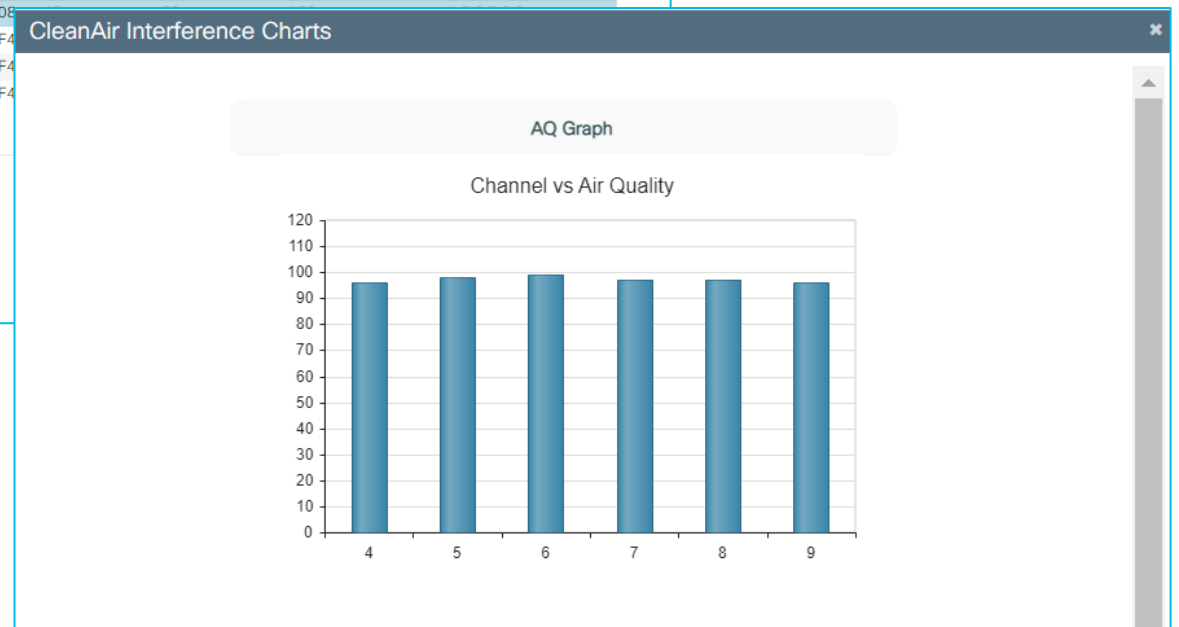
5 GHz Band **2.4 GHz Band**

CleanAir Interference Devices SI Interference Devices Air Quality Report Worst Air Quality Report

Cluster ID	MAC Address	Device ID	Interferer Type	AP Name	Severity	RSSI (dBm)	Duty Cycle (%)	Affected Channel
7f00.0000.ccf9	ba21.55c0.6bce	0x6bce	BT Link	AP1416.9D56.070C	2	-84	1	1,2,3
7f00.0000.cd07	ba21.55c0.6bd7	0x6bd7	BT Link	AP1416.9D56.070C	--	-88	1	
7f00.0000.cd09	ba21.55c0.6bd8	0x6bd8	BT Discovery	AP1416.9D56.070C	--	-88	1	
7f00.0000.cd0a	ba26.ac40.cc27	0xcc27	Continuous TX	AP1416.9D56.0E08				
7f00.0000.ccf7	ba26.d3a0.b7bf	0xb7bf	BT Link	AP1416.9D56.12F4				
7f00.0000.cd06	ba26.d3a0.b7c9	0xb7c9	BT Discovery	AP1416.9D56.12F4				
7f00.0000.cd08	ba26.d3a0.b7ca	0xb7ca	BT Link	AP1416.9D56.12F4				

1 10

Walk Me Through >



C9800 Wireless IPS Rogue Detection

Cisco Catalyst 9800-L Wireless Controller 17.B.1

Welcome dnac

Search APs and Clients

Feedback

Monitoring > Wireless > Rogues

Unclassified Friendly Malicious Custom Ignore List Rogue Clients Adhoc Rogues

× Delete

Total APs : 343

<input type="checkbox"/>	MAC Address	#Detecting Radios	Number of Clients	Status	Last Heard	Last Heard SSID	Last Channel	PMF Required
<input type="checkbox"/>	0023.6926.1717	1	2	Alert	09/16/2022 10:14:03	CTC_IT	1	No
<input type="checkbox"/>	0025.00ff.9473	4	0	Alert	09/16/2022 10:06:51	(*****HIDDEN*****)	6	No
<input type="checkbox"/>	00df.1ddb.cd10	4	0	Alert	09/16/2022 10:14:20	VNHospitalPLZ01	1	No
<input type="checkbox"/>	00df.1ddb.cd1f	1	0	Alert	09/16/2022 10:14:11	VNHospitalPLZ01	48	No
<input type="checkbox"/>	02ec.dafa.4667	3	0	Alert	09/16/2022 10:14:19	CMW	11	No
<input type="checkbox"/>	02ec.dafa.46b2	6	3	Alert	09/16/2022 10:14:21	CMW		
<input type="checkbox"/>	02ec.dafa.5183	1	2	Alert	09/16/2022 10:14:03	CMW		
<input type="checkbox"/>	02ec.dafb.4667	5	0	Alert	09/16/2022 10:14:19	CMW Guest		
<input type="checkbox"/>	02ec.dafb.46b2	3	0	Alert	09/16/2022 10:14:11	CMW Guest		
<input type="checkbox"/>	02ec.dafb.5183	4	0	Alert	09/16/2022 10:14:11	CMW Guest		

1 2 3 4 5 6 7 8 9 10 ... 10

Rogue AP Detail

Rogue Classification

MAC Address: 00df.1ddb.cd1f

Is this radio on wired network? No

Class Type: Unclassified

Status: ALERT

Initiate RLDP:

Is Rogue an impersonator? No

Rogue History

First time Reported On: 08/21/2022 16:26:16

Last time Reported On: 09/16/2022 10:14:11

APs that detected this Rogue

Base Radio MAC	AP Name	SSID	Channel	Channel Width	Channel from DS	Radio	Security Policy	Short Preamble	RSSI (dBm)	SNR (dB)	Containment Type
548a.ba26.ac...	AP1416.9D56.0E...	VNHospitalPLZ01	48	40	Yes	dot11ax - 5 GHz	WPA2/FT/Dot...	Disabled	-67	18	INVALID

Clients associated to this Rogue AP

MAC Address: Last Heard On

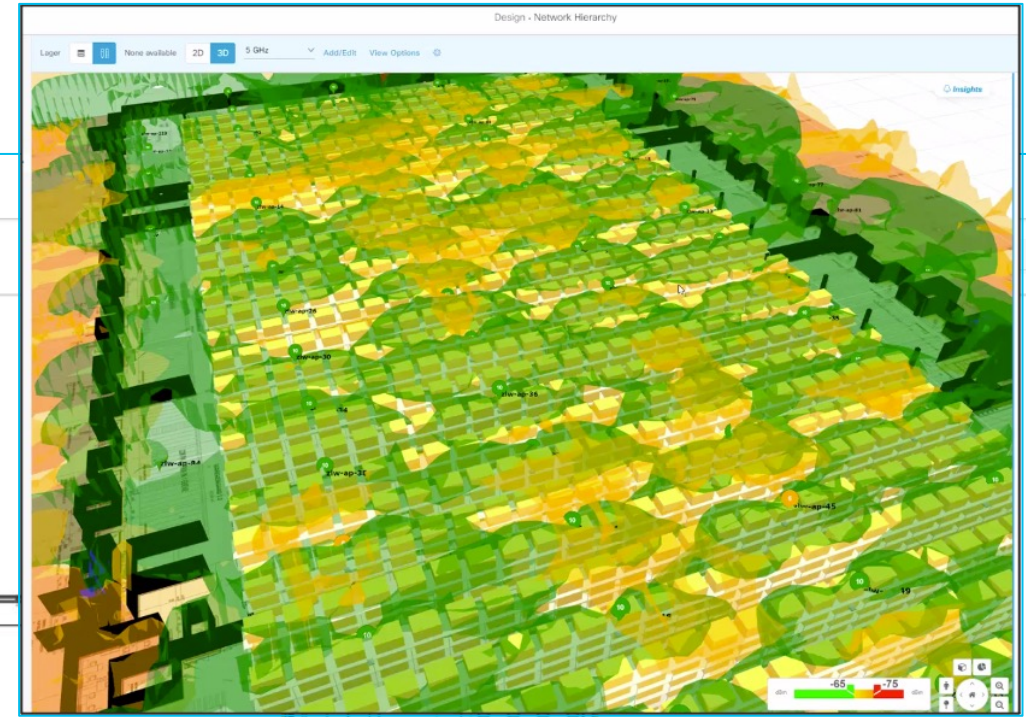
0 No items to display

2D & 3D Wireless Maps

Find Hierarchy

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

- 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



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

The screenshot displays the DNAC Wireless interface, showing a 3D map of a building floor plan. The map is overlaid with various APs and sensors, including C9130AP, SJC14-TME-AP1, SJC14-TM, SJC14-TME-AP10, SJC14-9136-AP-1, SJC14-T, Assurance_9130_3, SJC14-TME-AP8, Sensor10, SJC14-TME-AP7, SJC14-TME-AP5, SJC14-TME-AP4, SJC14-TME-AP2, and SJC14-TME-AP6. A color scale at the bottom right indicates signal strength from -65 dBm to -75 dBm. Below the main map, there is a detailed view of a specific area labeled '5th Floor' and an 'Interferers' panel.

The 'Interferers' panel shows a list of active interferers with the following data:

MAC Address	Interferer Type	Interferer Status	Band (GHz)	S
71:00:00:00:cd:1d	BLUETOOTH	Active	2.4	2
71:00:00:00:cd:3a	BLUETOOTH	Active	2.4	0
71:00:00:00:cd:3c	BLUETOOTH	Active	2.4	0
71:00:00:00:cd:3d	BLUETOOTH_PAGING_INQUIRY_DEVICE	Active	2.4	2
71:00:00:00:cd:3e	BLUETOOTH_PAGING_INQUIRY_DEVICE	Active	2.4	0
71:00:00:00:cd:0a	GENERIC_WAVEFORM	Active	2.4	3
71:00:00:00:cd:39	MICROWAVE_OVEN_1	Active	2.4	0

Configuring View Options in Wireless 3D Maps

Customize the Map's Visuals

1 Click View Options



2 To Open a Slide-in Pane

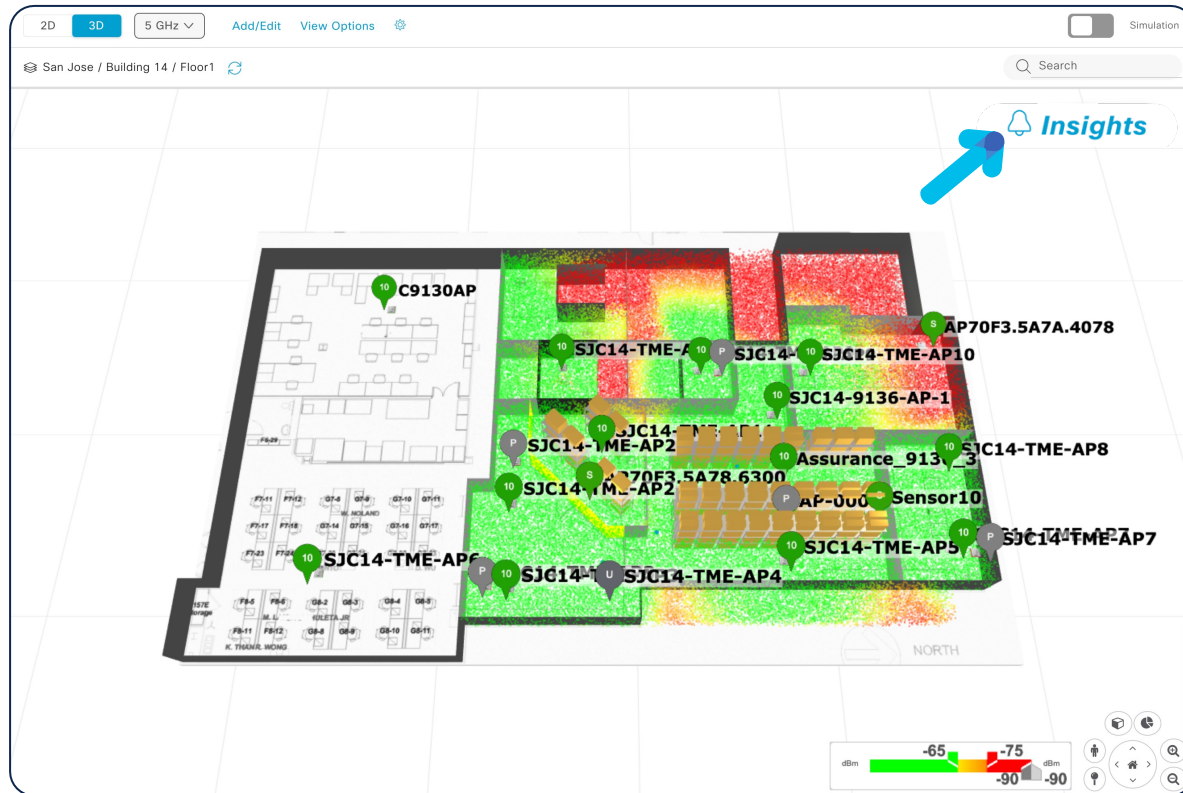
a RF Metric

b How it's Visualized

Monitoring SLAs With Visual Insights

Visibility Into Areas of Coverage That Need Attention

1 Click on the **Insights** icon 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

Cisco DNA Center Design / Network Hierarchy

2D 3D 2.4 GHz Add/Edit Data View Options

Prague / PRG07 / PRG07-5 Updated just now

Search Hierarchy Search Help

- Global
 - Bratislava
 - Jezeri
 - Kounov
 - mnt
 - Pardubice
 - Pizen
 - Prague
 - PRG07
 - PRG07-5
 - PRG07-DMZ
 - PRG07-Guest-ACC
 - PRG07-JC-PNP
 - Temp-PI-DNC-coexistence
 - TEST-DS
 - Warehouse-test
 - Zatec

5th Floor

AP locations: AP687D.B45C.A2A0, AP1416.9D56.12F4, AP-0001, AP-0002, APF4DB.E643.851, AP1416.9D56.123C, APF4DB.E643.851, 77.5F6C, AP-0003, AP1416.9D56.0E08, 9D56.0EB4, 416.9D56.070C

Interferers

AND +

None

Apply Filters to List Show Selected on Map Focus on selected

MAC Address	Interferer Type	Interferer Status	Band (GHz)	S
7f:00:00:00:cd:1d	BLUETOOTH	Active	2.4	2
7f:00:00:00:cd:3a	BLUETOOTH	Active	2.4	0
7f:00:00:00:cd:3c	BLUETOOTH	Active	2.4	0
7f:00:00:00:cd:3d	BLUETOOTH_PAGING_INQUIRY_DEVICE	Active	2.4	2
7f:00:00:00:cd:3e	BLUETOOTH_PAGING_INQUIRY_DEVICE	Active	2.4	0
7f:00:00:00:cd:0a	GENERIC_WAVEFORM	Active	2.4	3
7f:00:00:00:cd:39	MICROWAVE_OVEN_1	Active	2.4	0

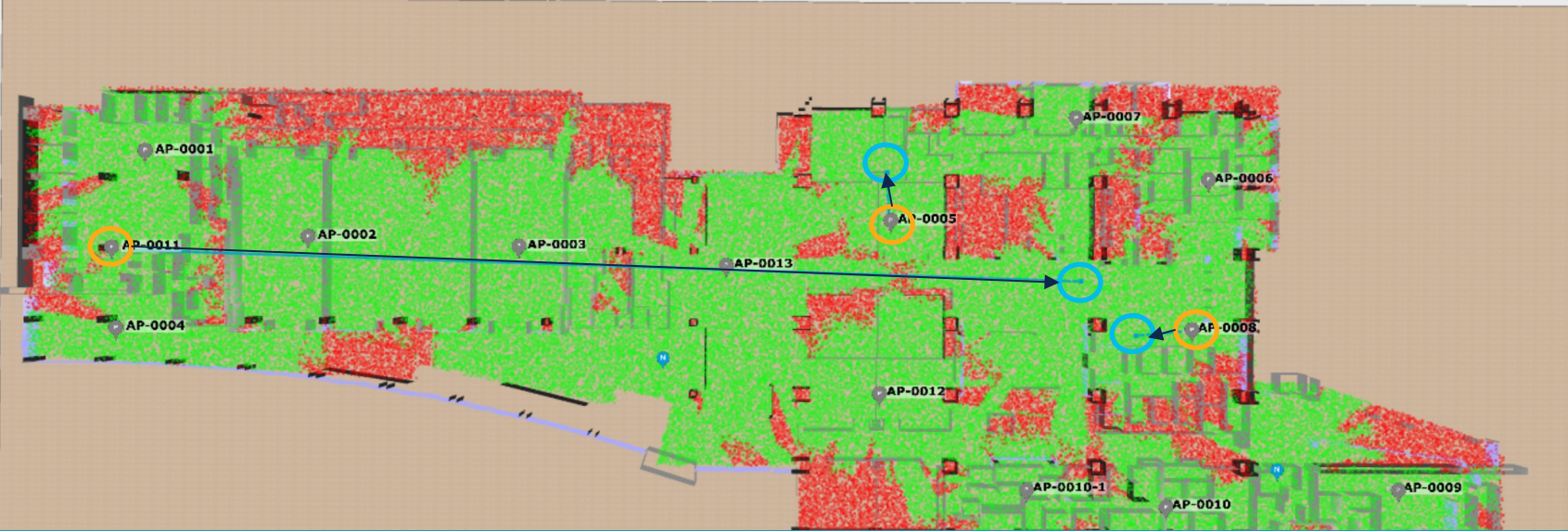
Showing 7 of 7

Leverage RF Optimizer for AP Redeployment Suggestions starting from 2.3.3!

2D 3D 5 GHz Add/Edit View Options Simulation

SJSU / B1 / F1 Search

Insights



Your floor coverage with RSSI of **-65** or more will be increased from **68 %** to **78%** by the optimizations below:

- Add 2 AP(s).
- Move 3 AP(s).

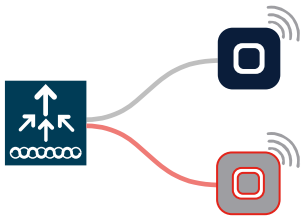
[Save as a plan](#)

Navigation icons: Home, Search, Refresh, Back, Forward, Zoom In, Zoom Out, User, Key.

WLAN has inherent vulnerabilities exposing it to various threats

On Wire Attacks

Rogue on Wire
Unknown | Malicious



✓ Switch-port Tracing

✓ RLDP

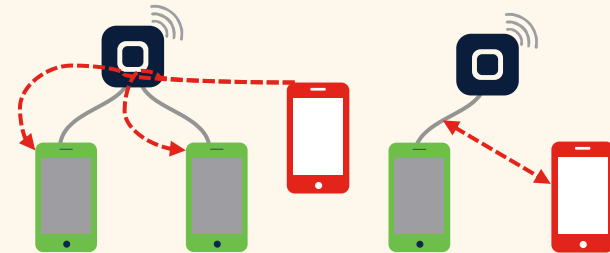
Over-the-Air Attacks

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



✓ Rogue Management
Basic Wireless Security

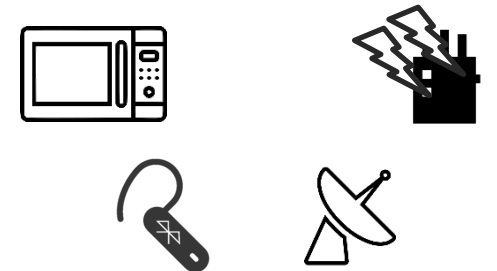
Denial of Service | Reconnaissance | Cracking Tools



✓ WIPS
Advanced Wireless Security

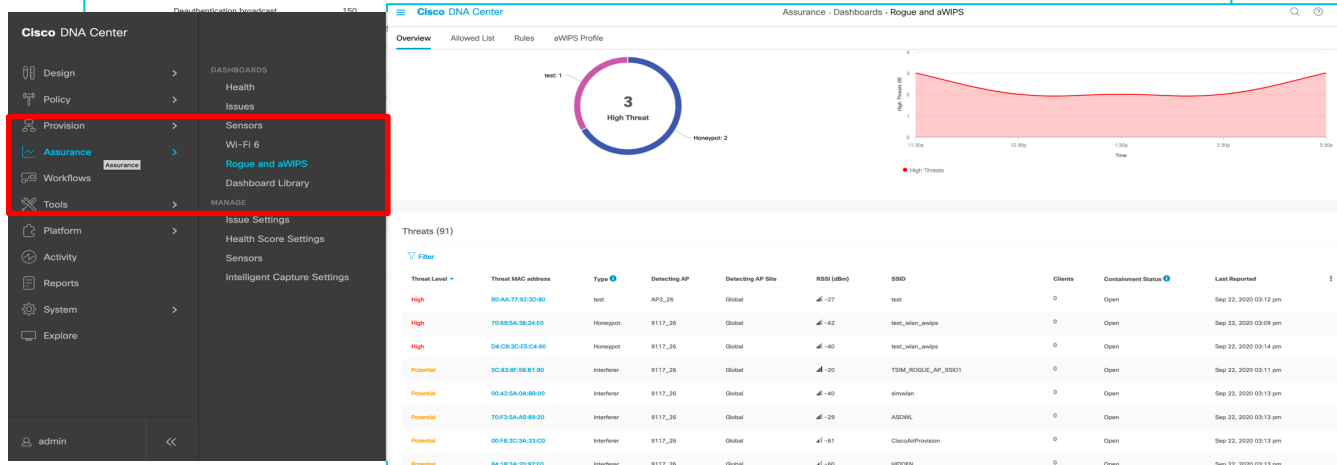
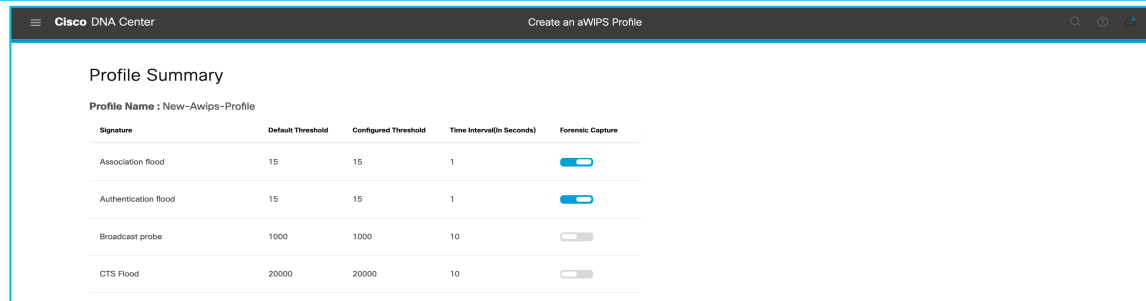
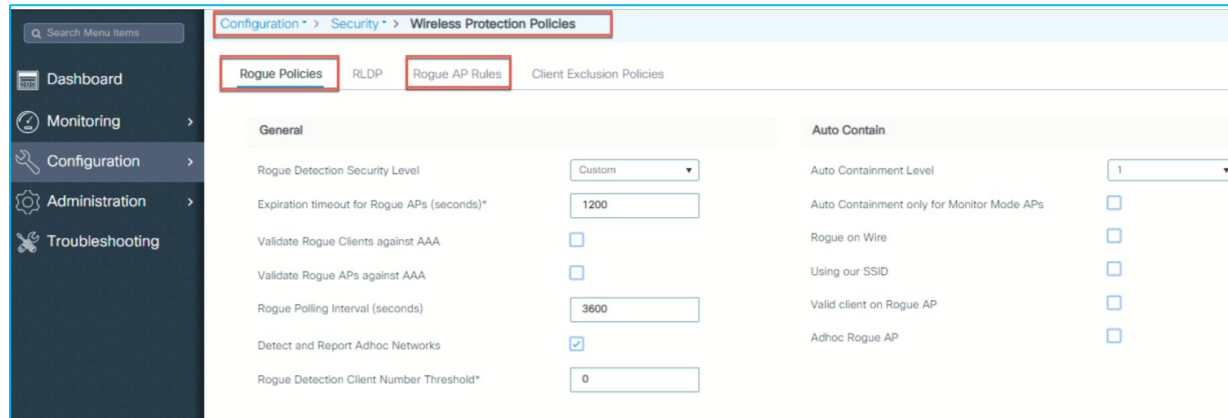
Non-802.11 Interferers

Microwave | Bluetooth
Radar | RF Jammers



✓ Cisco CleanAir
Visibility of non-WiFi interferers

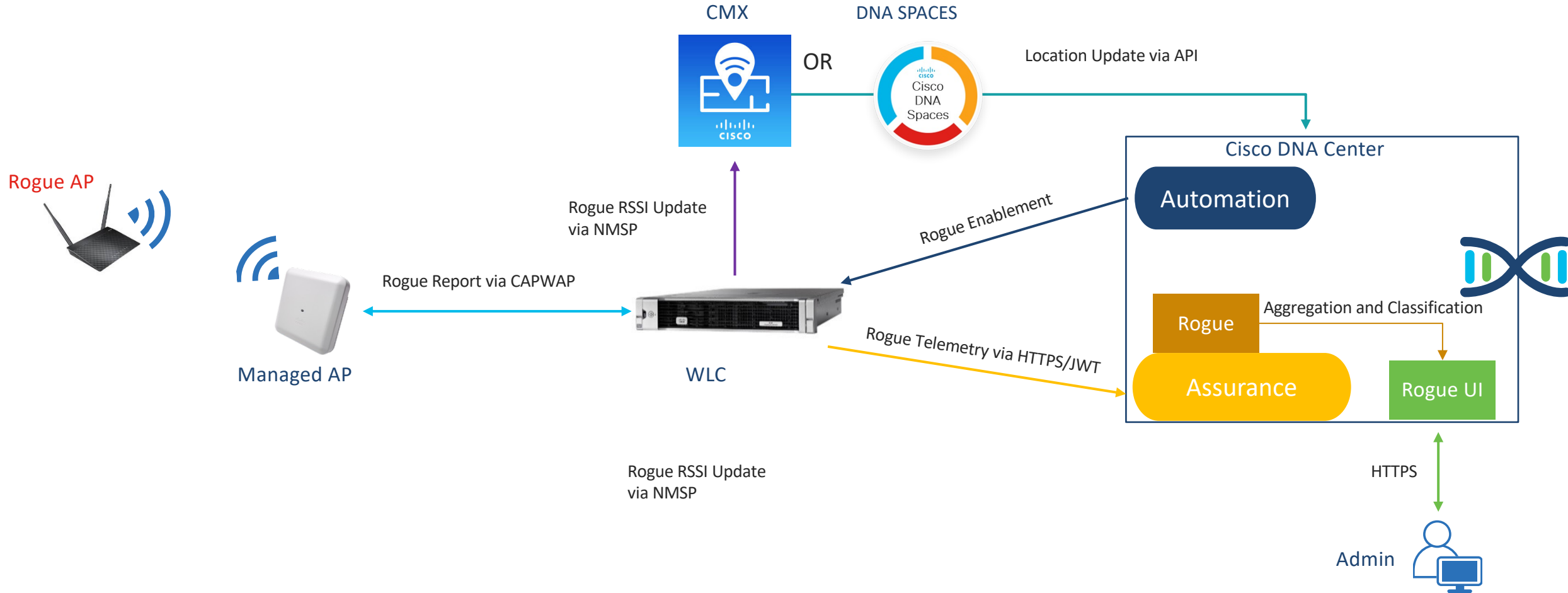
Cisco Rogue/WIPS Highlights



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

Overview Allowed List Rules aWIPS Profile

Sep 16, 2022 3:38 PM Refresh Show Map Last 7 days Actions



High Threat Summary

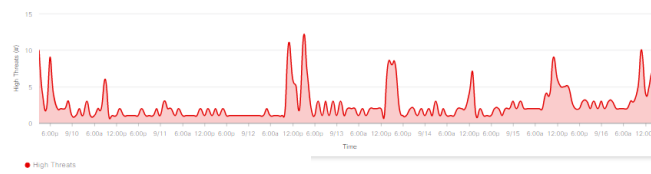
Active High Threats (110)

By threat type Top 10 All



- Airdrop Session (90)
- Fuzzed Probe Request (16)
- AP Impersonation (2)
- Honeyport (1)
- Authentication flood (1)

High Threats Over Time



Threats (316)

Search Table

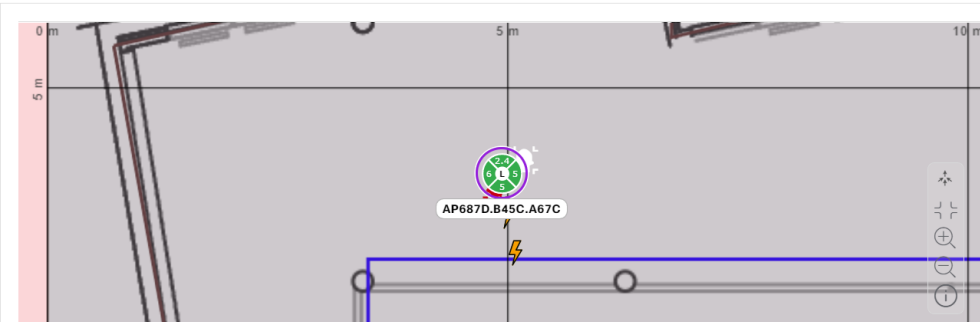
Threat Level	MAC Address	Type	Source/Target	Detecting AP
High	9EAE13562536	Airdrop Session	AP687D.B45C.A67C Global/Plzen/PLZ01/PLZ01-1	-
High	C6BA1775D4FA	Airdrop Session	AP687D.B45C.A67C Global/Plzen/PLZ01/PLZ01-1	-
High	9A93FF026E89	Airdrop Session	AP687D.B45C.A67C Global/Plzen/PLZ01/PLZ01-1	-
High	5A3F8838BE80	Airdrop Session	AP687D.B45C.A67C Global/Plzen/PLZ01/PLZ01-1	-
High	9A1C53CF0967	Airdrop Session	AP687D.B45C.A67C Global/Plzen/PLZ01/PLZ01-1	-

Threat 360: Mac 9A:93:FF:02:6E:B9

Threat Level	Threat Type	Vendor	Count	Last Reported
High	Airdrop Session	UNKNOWN	1	Sep 13, 2022 09:25 am

Location: Global/Plzen/PLZ01/PLZ01-1

Full Screen



Proactive network diagnostics

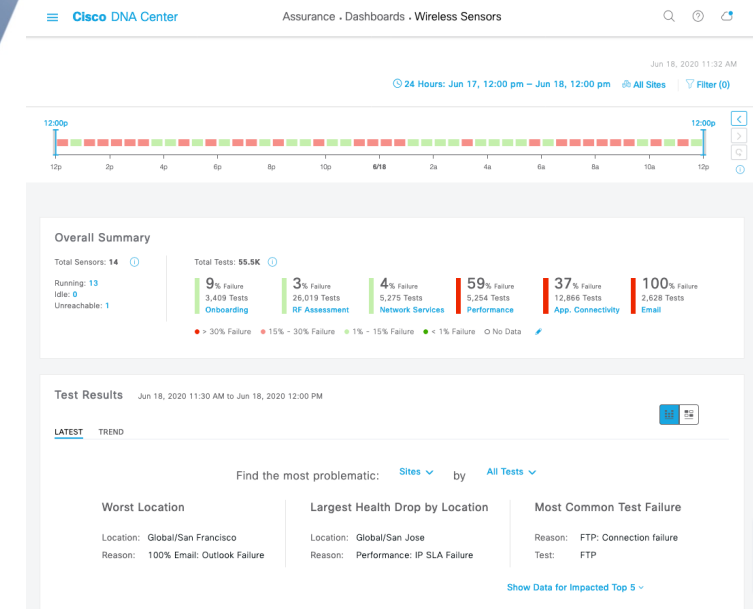


Aironet Active Sensor Use Cases

Test your network and report results to Cisco DNA Assurance!

Performs the following Wireless Tests:

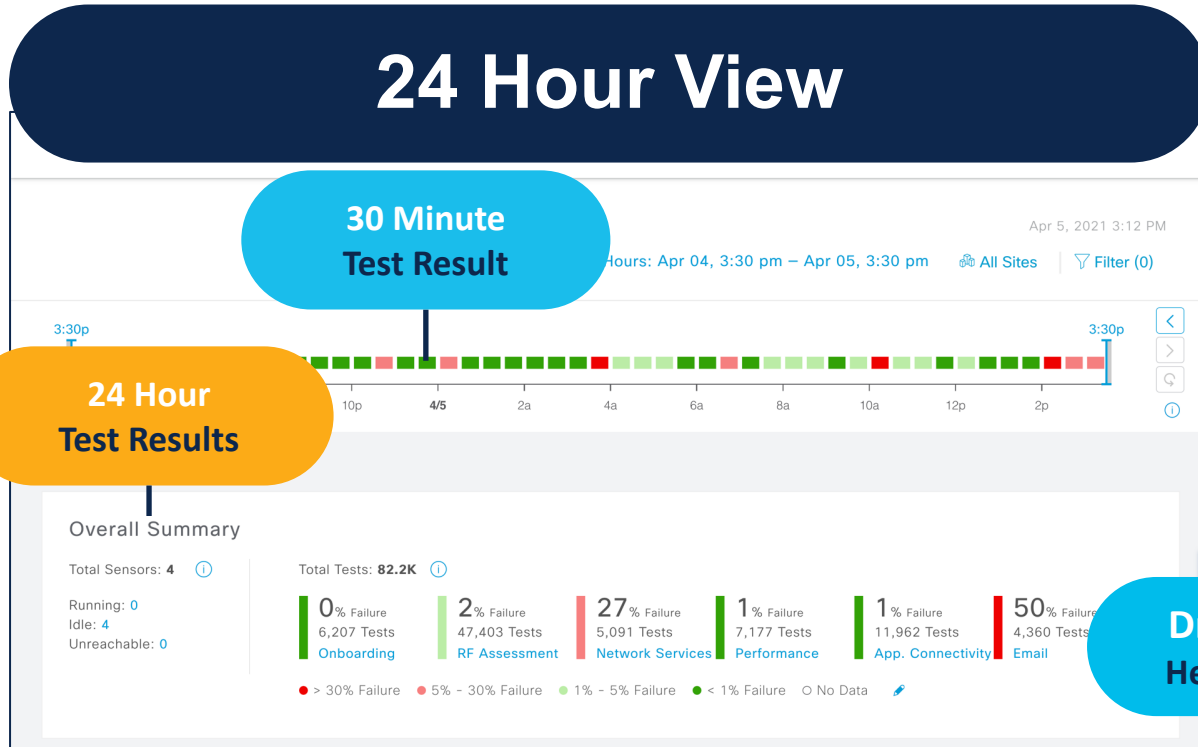
- ➔ Onboarding (Auth Types - 802.1x, MAB and Open Auth, DHCP)
- ➔ RF Assessment (Data rate, SNR)
- ➔ Network Services (DNS, RADIUS)
- ➔ Performance (iPerf3, NDT, IP SLA)
- ➔ Application (FTP, Web server, host reachability)
- ➔ Email (IMAP, POP3, OWA)



Wireless Sensor Global Dashboard

Overall Summary Trend View

24 Hour View

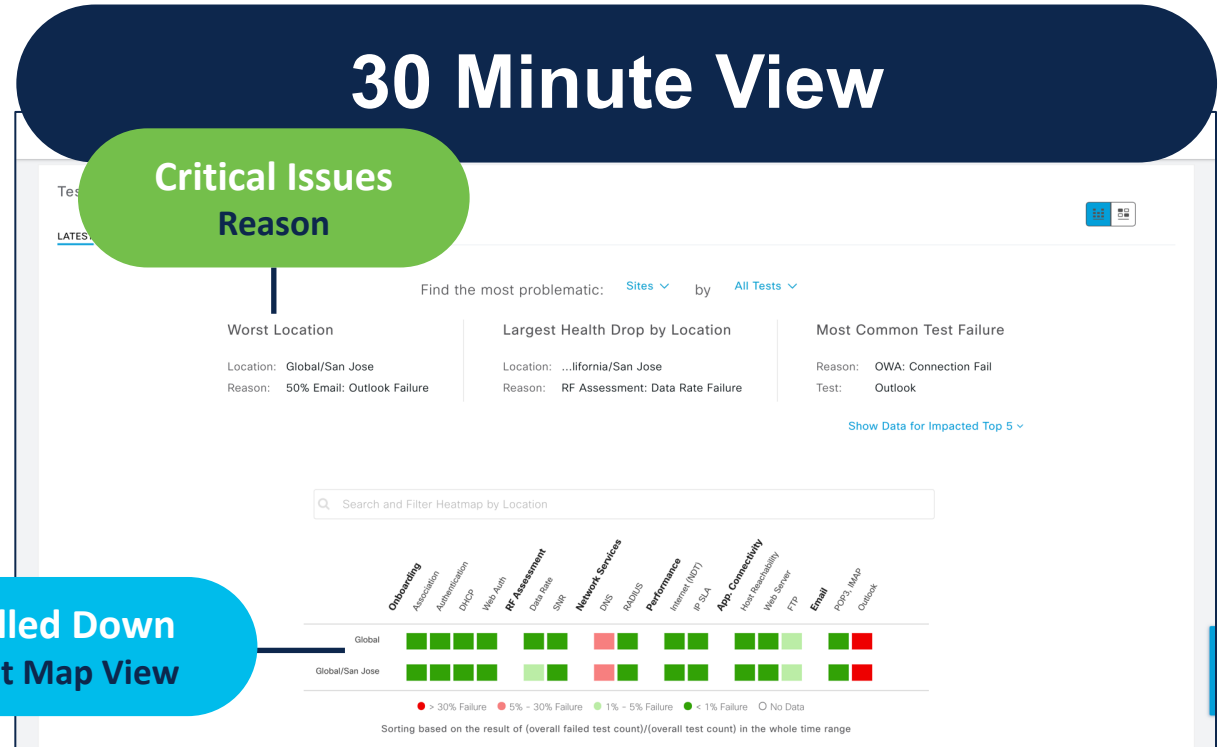


30 Minute Test Result

24 Hour Test Results

Drilled Down Heat Map View

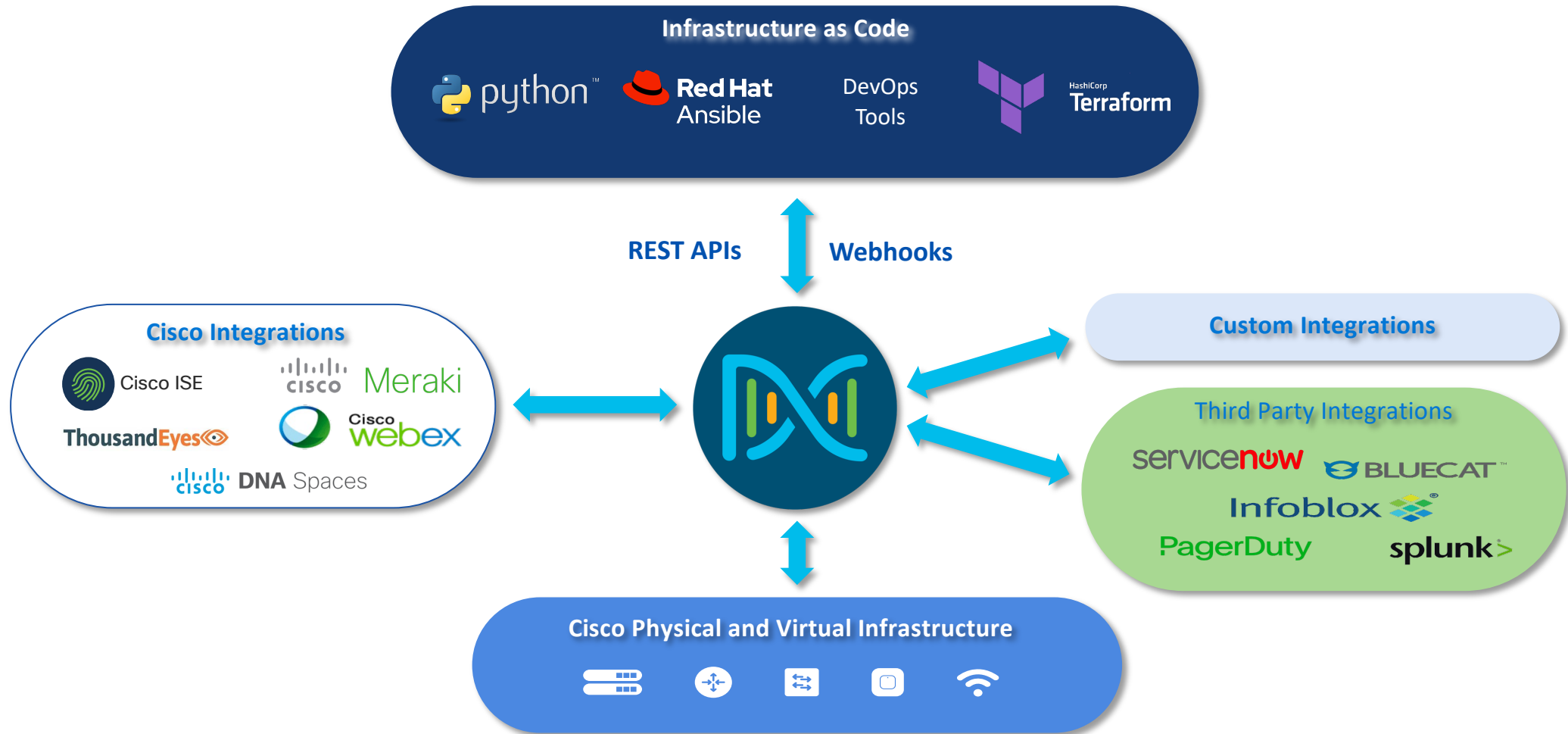
30 Minute View



- 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

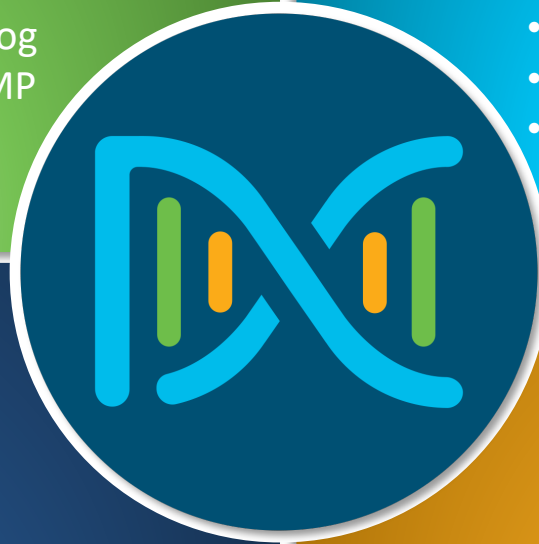
- Network Inventory
- Network Topology
- Network Design
- Provisioning
- SWIM, PnP
- Path Trace
- Assurance
- SDA
- Templates
- RMA
- Config Archive
- Sensors

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

The image shows two screenshots. The left screenshot is from the Cisco DNA Center 'Issues' dashboard. It displays a table with one issue: 'Interface *GigabitEthernet2* (Interface description: TO_CSR2_GI2) is down on network device *PDX-RO*'. The table columns are Issue, Site, Device, and Device Type. The right screenshot is from a Webex chat room titled 'Cisco DNA Center Notifications'. It shows a message from a bot with the following details:

- Source DNA Center IP:** 10.93.141.45
- Severity:** 1
- Category:** ALERT
- Timestamp:** 2021-09-22 22:07:08
- Issue Name:** Interface GigabitEthernet2 (Interface description: TO_CSR2_GI2) is Down on Network Device 10.93.141.23
- Issue Description:** Interface GigabitEthernet2 (Interface description: TO_CSR2_GI2) connecting the following two network devices is down: Local Node: PDX-RO, Peer Node: PDX-RO
- Issue Status:** active

Cisco DNA Center Issue Details

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

Report Templates

Generated Reports (96)

Report Templates

- All
- Access Point
- Client
- Executive Summary
- Inventory
- Licensing
- Network Devices
- Rogue and aWIPS
- SWIM
- Security Advisories

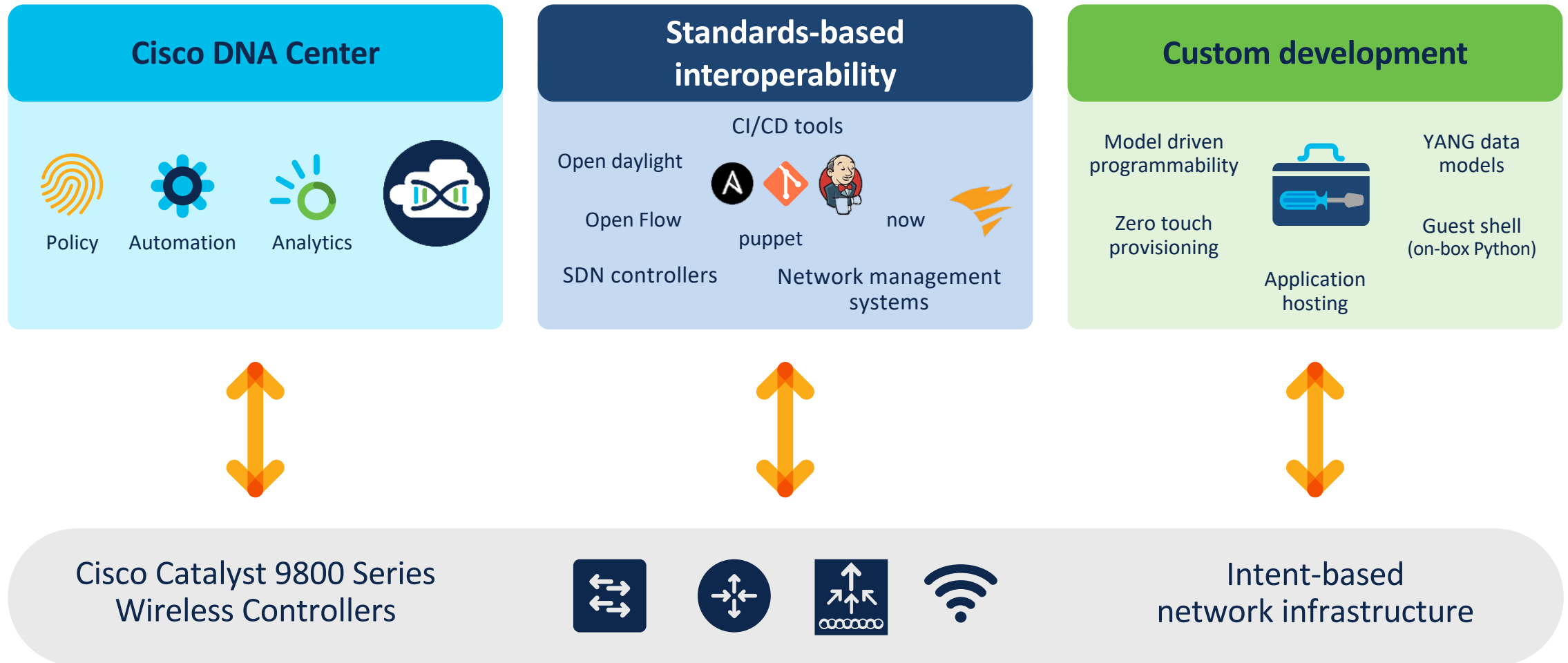
<p>Licensing AireOS Controllers Licenses</p> <p>Provides license information about AireOS controllers</p> <p>PDF, CSV, TDE</p> <p>Generate</p>	<p>Inventory All Data</p> <p>The all data view provides detailed information about network devices, Distribution of devices over time, Device Count by Site, Device Count by Device</p> <p>PDF, CSV, TDE</p> <p>Generate</p>	<p>SWIM All Data</p> <p>The all data view provides detailed information about software image updates on devices</p> <p>PDF, CSV, TDE</p> <p>Generate</p>	<p>Access Point AP</p> <p>This report contains a detailed list of Access Points in the network</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Access Point AP Radio</p> <p>This report contains a detailed list of Access Point Radios in the network</p> <p>CSV, TDE, JSON</p> <p>Generate</p>
<p>Client Busiest Client</p> <p>This client report view provides busiest clients by usage, tx bytes or rx bytes.</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Network Devices Channel Change Count</p> <p>The report provides visibility into the channel changes observed on Access Point Radio</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Client Client Detail</p> <p>This client report view provides detailed information about the list of clients that are seen in the network</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Client Client Session</p> <p>This client session report view provides detailed information about the wireless client sessions seen in the network</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Client Client Summary</p> <p>This client report view provides an executive summary like health and counts of clients that are seen in the network.</p> <p>PDF</p> <p>Generate</p>
<p>Client Client Trend</p> <p>This client report view provides client count trend and client traffic trend for the given time period</p> <p>PDF</p> <p>Generate</p>	<p>Executive Summary Executive Summary</p> <p>Analyze how the network is performing with insights into network devices, clients and issues</p> <p>PDF, CSV</p> <p>Generate</p>	<p>Licensing License Usage Upload Details</p> <p>Provides information about license usage uploading schedule</p> <p>PDF, CSV</p> <p>Generate</p>	<p>Network Devices Network Device Availability</p> <p>This network device availability report view provides detailed information about average availability of devices</p> <p>CSV, TDE, JSON</p> <p>Generate</p>	<p>Rogue and aWIPS New Threat</p> <p>This report provides for the detailed information about the new rogue AP's and aWIPS threats that are seen in the network</p> <p>CSV, TDE, JSON</p> <p>Generate</p>

- 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

Cisco IOS XE
16.10+



CLI
...or with... + Ansible
YANG

Receiver
Decodes to text



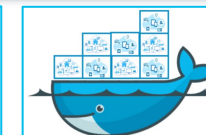
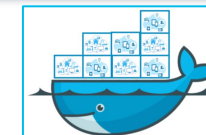
gRPC Dial-Out

telegraf

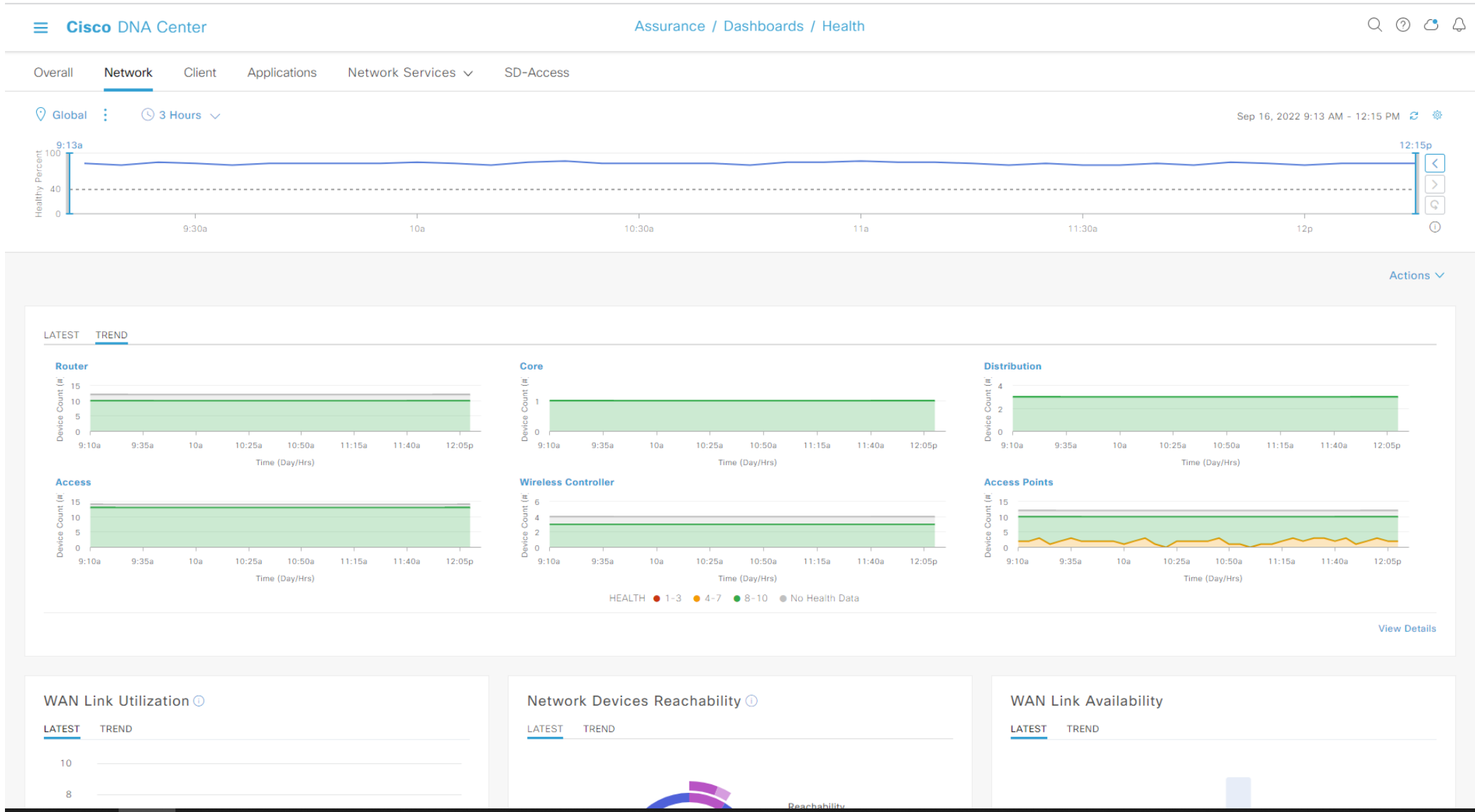
Collector
Time Series Database



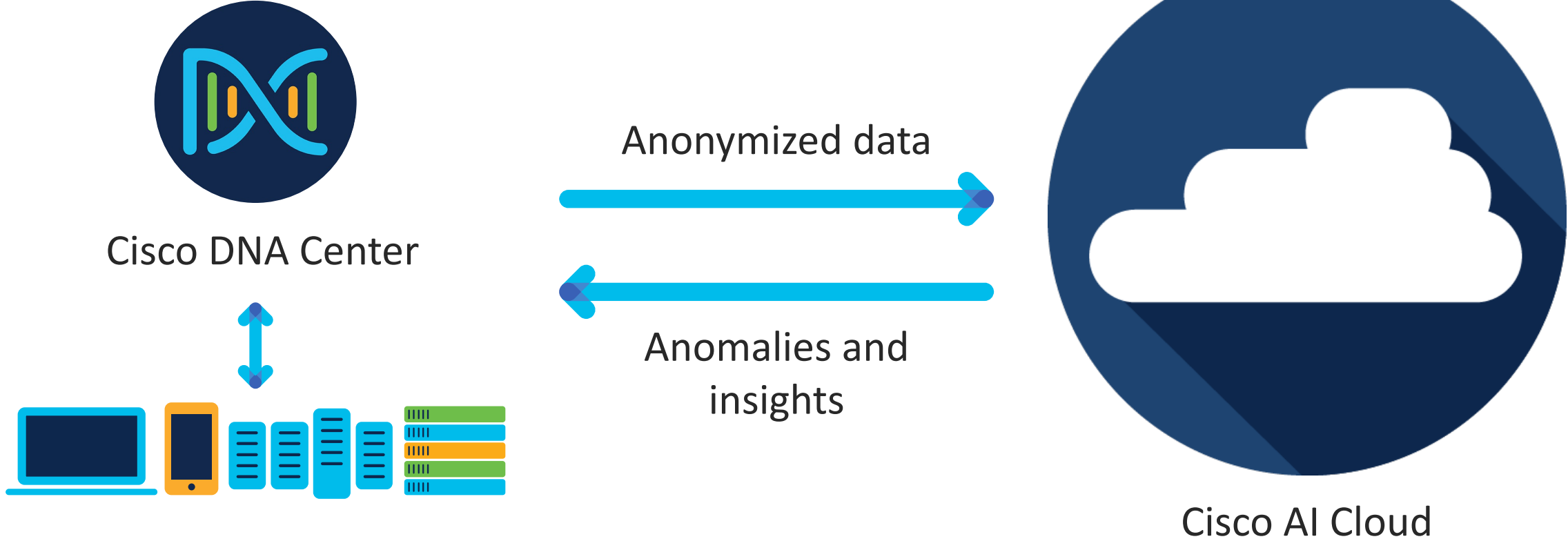
Monitoring
and Visualizations



DNAC Assurance – Timeline / Trend Dashboards



Cisco AI Network Analytics overview

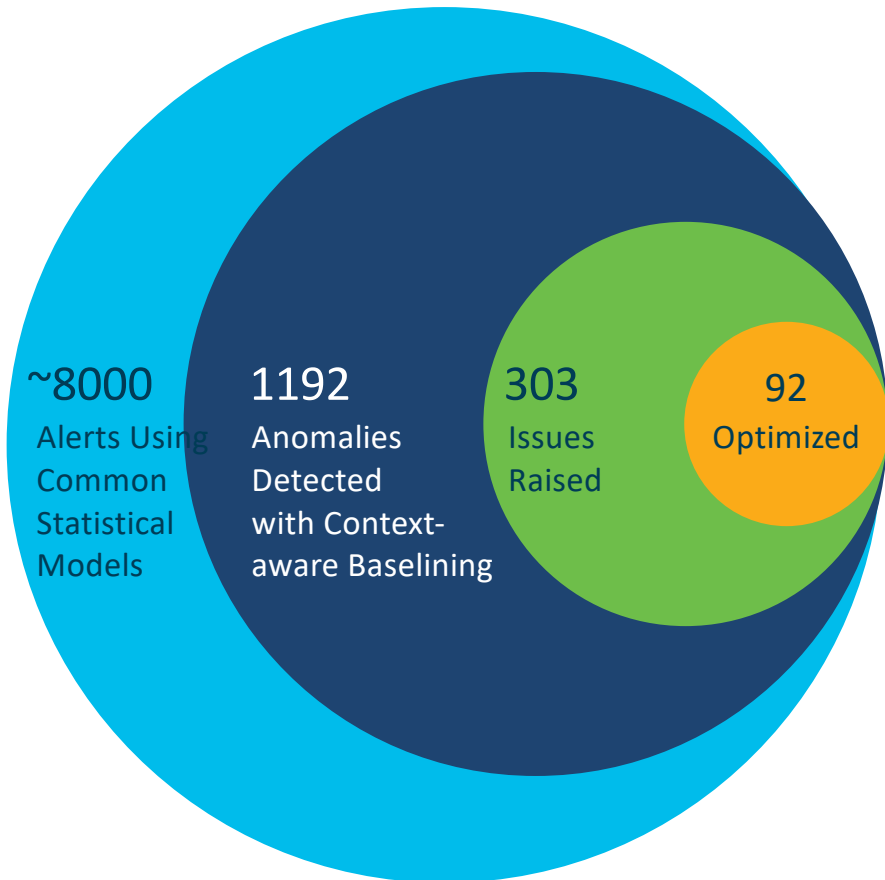


Improve Incident Alert Personalized Baseline

The Key for Success: Small Number of Relevant anomalies

98%

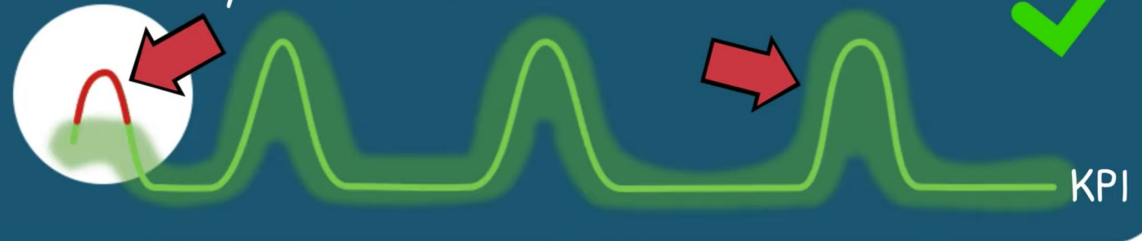
Reduction in Alerts



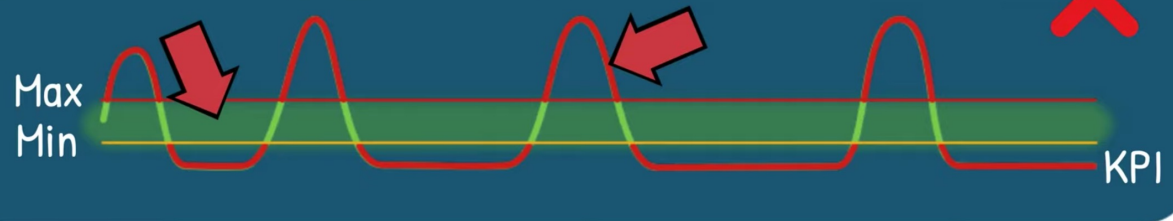
AI-Driven Dynamic Baselineing



Dynamic Threshold = Relevant Anomalies



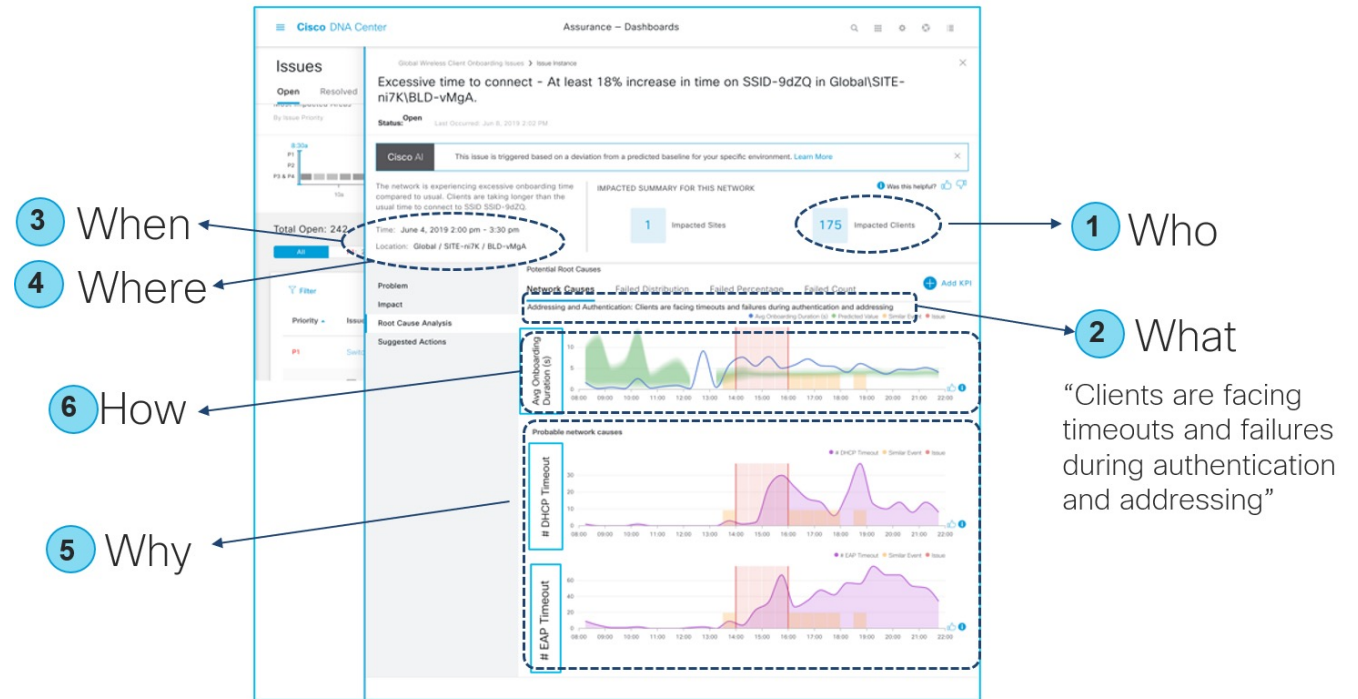
Static Threshold = False Positives



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



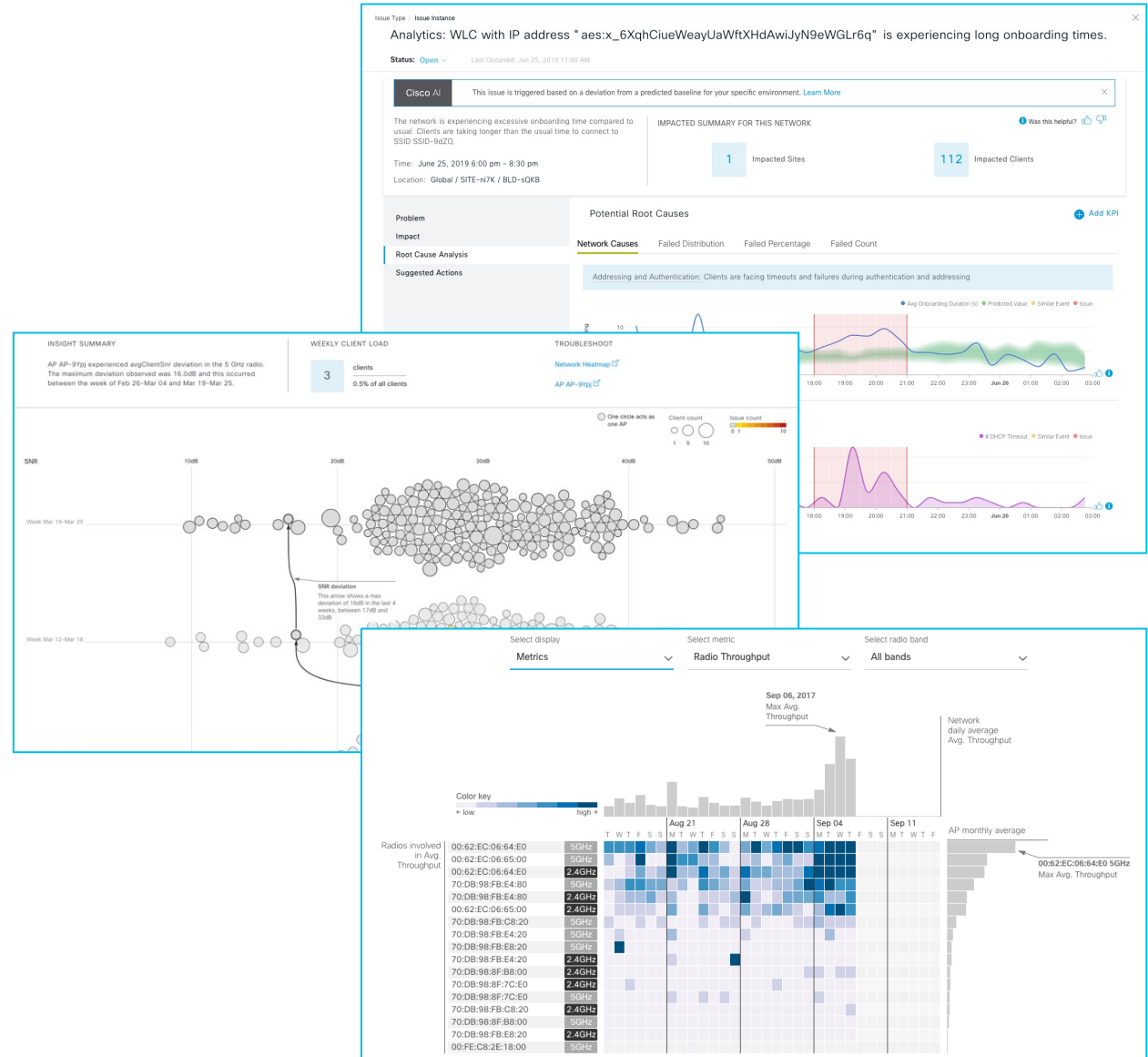
Baselines

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

5 KPIs: Onboarding

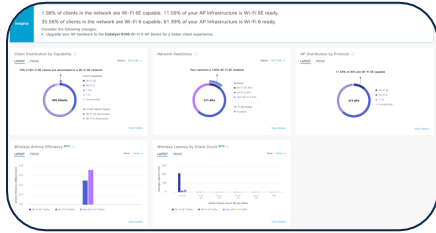
DNAC AI Network Analytics –DEMO

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

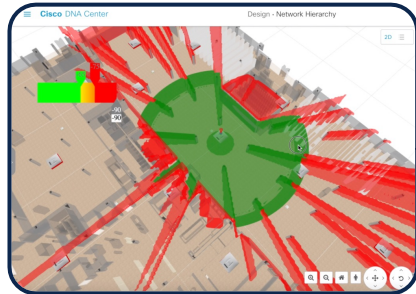


Unleash the True Potential of Your Wireless with Cisco DNA Center's AIOps!

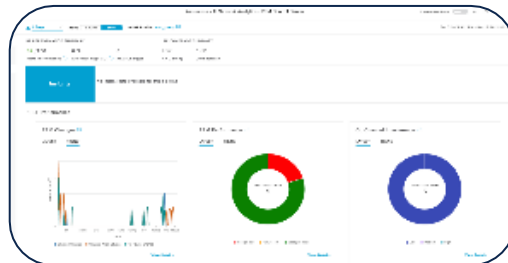
Wi-Fi 6E Integrations



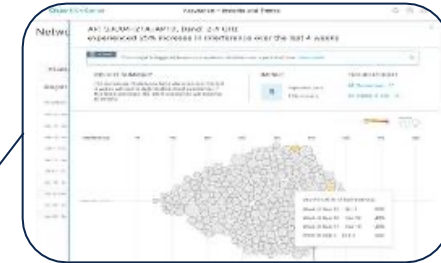
Wireless 3D Analyzer



AI-Enhanced RRM



AI Network Analytics



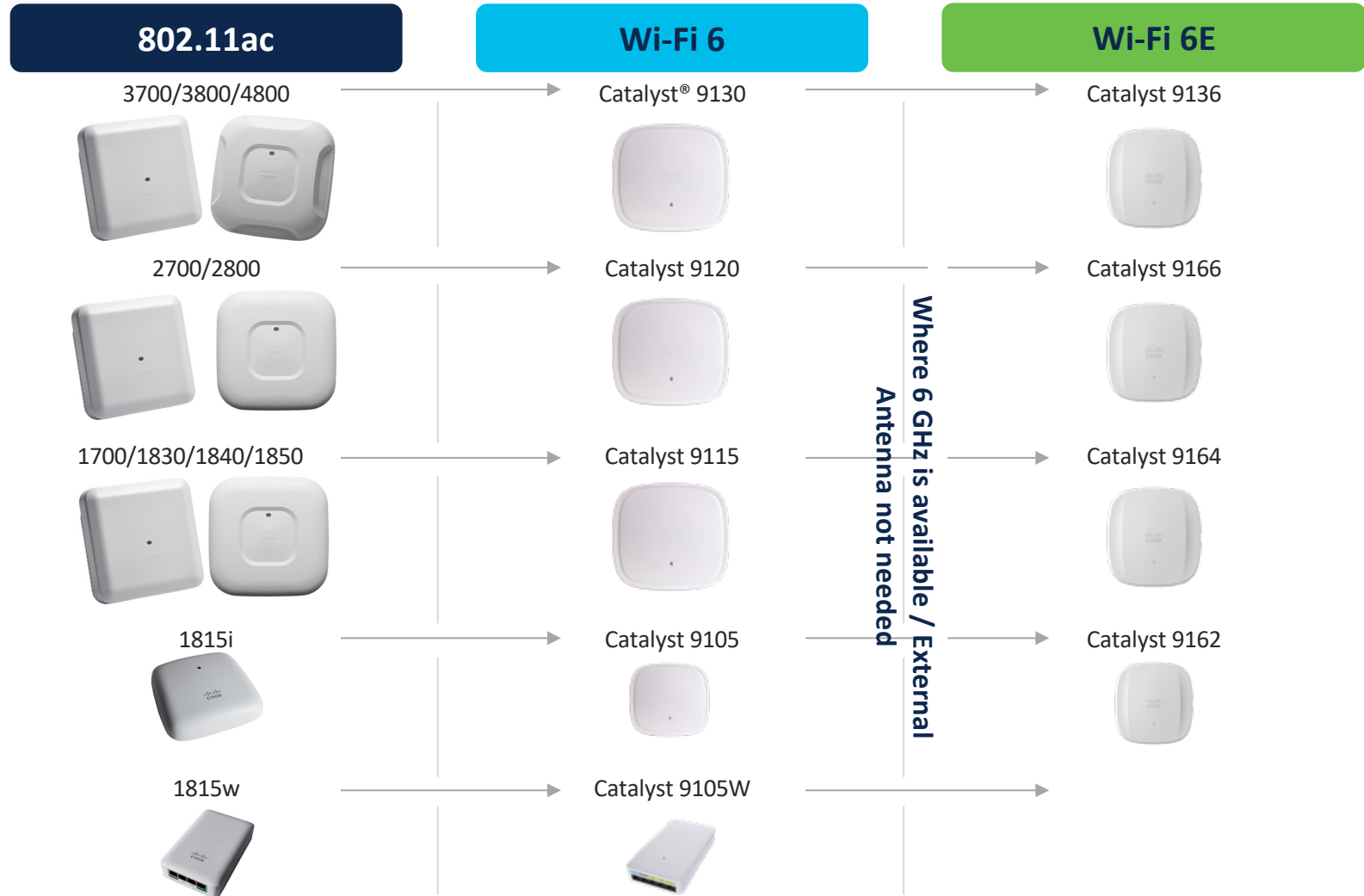
AP Performance Advisories



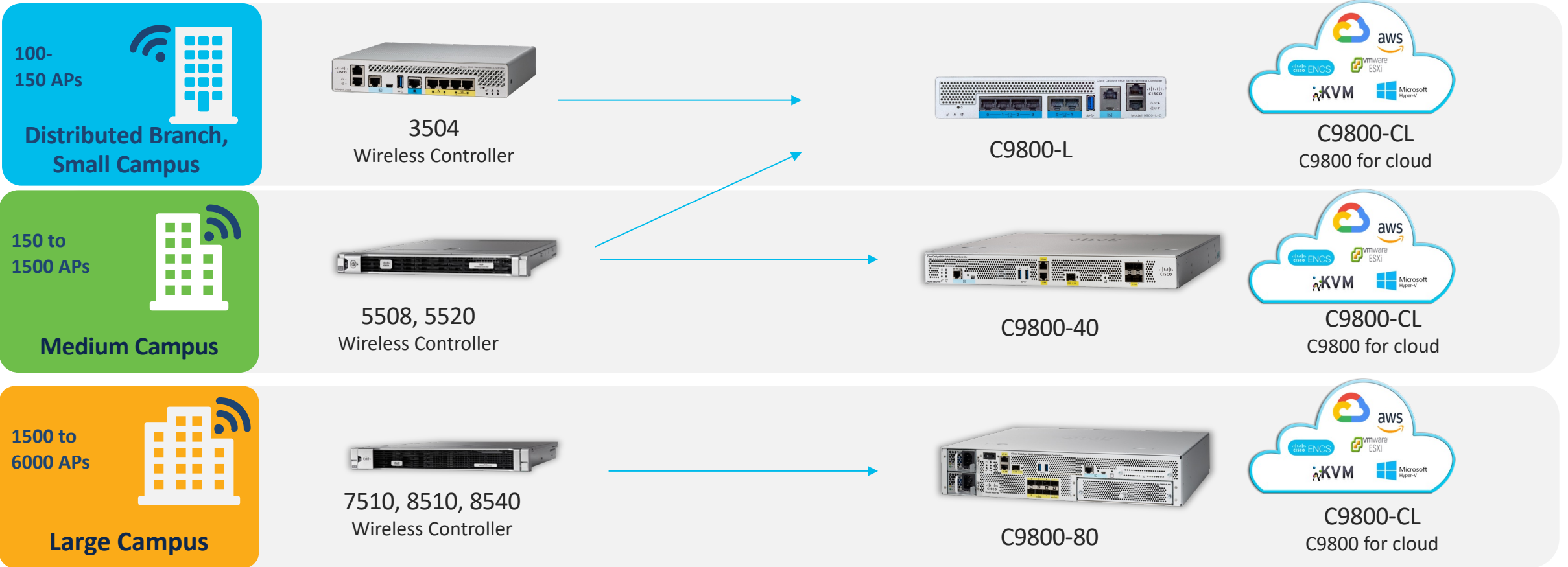
Device Ecosystem Partnerships



Recommended upgrade path (integrated Antenna)

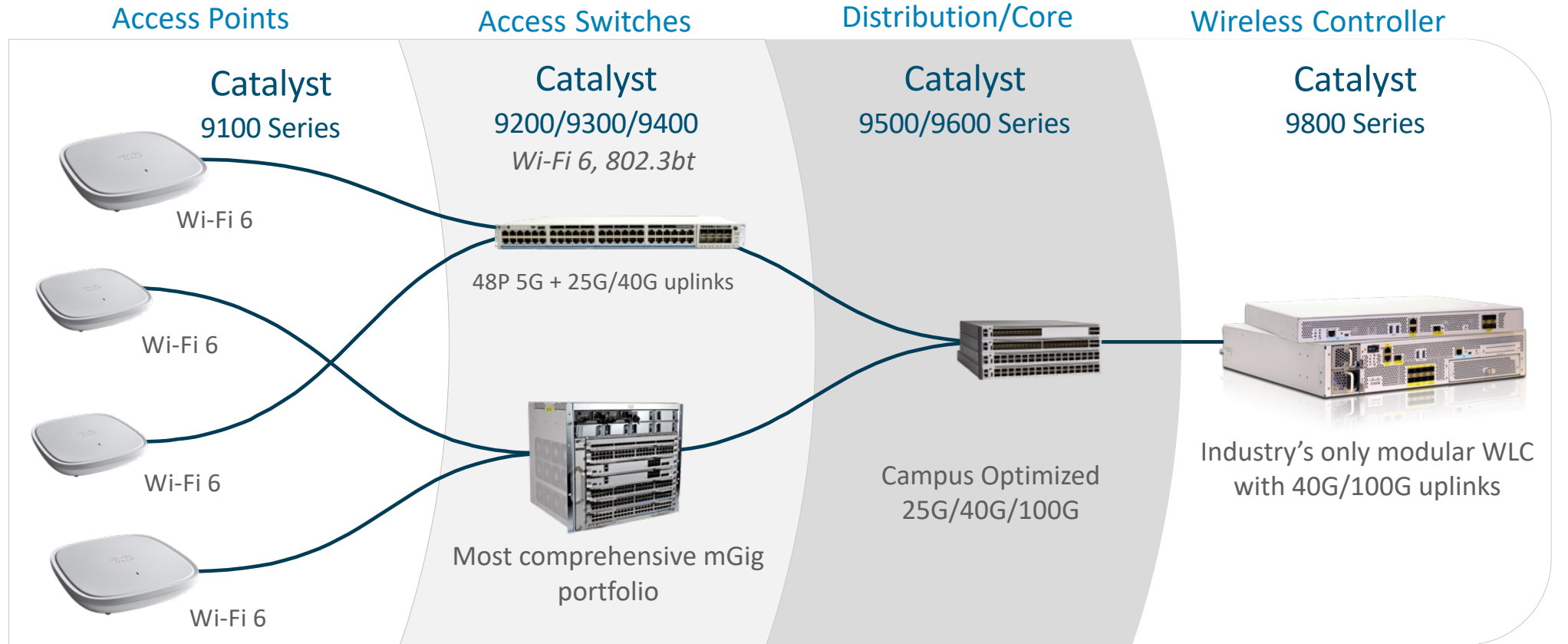
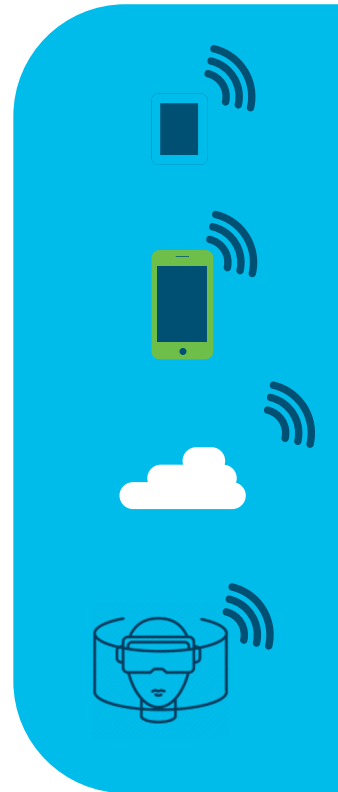


Wireless Controller Transition



Cisco Catalyst Access Network

Best Access Experience for IT and IoT



← Fully Integrated End to End →

Built for intent-based networking



Automation



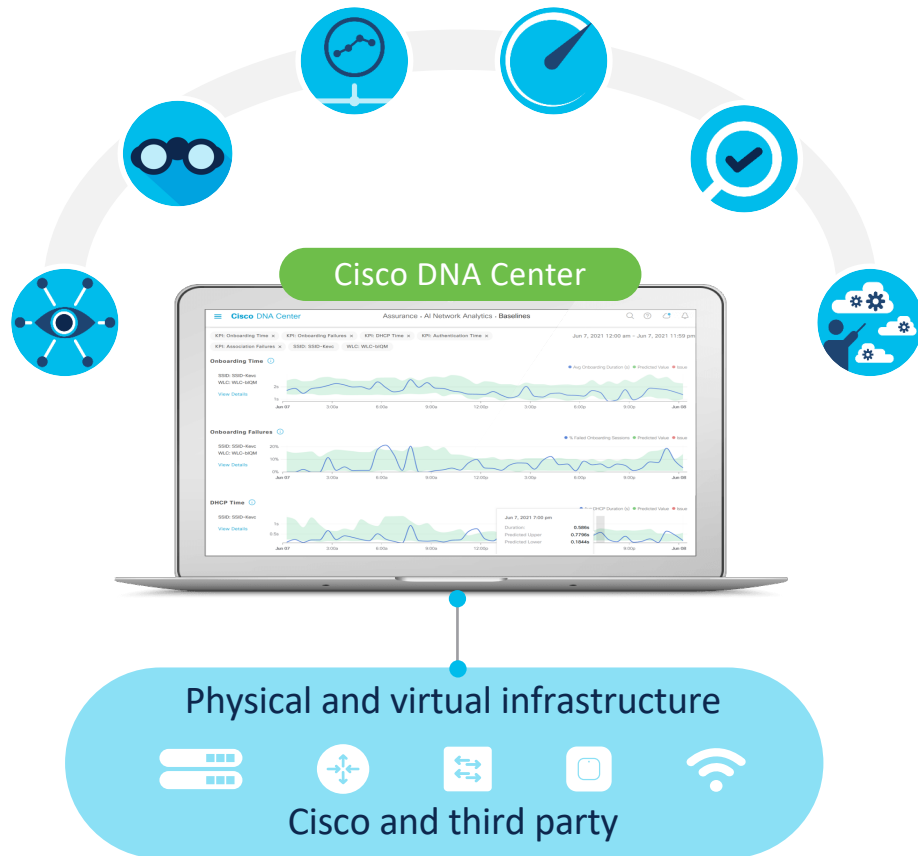
Security



Analytics

The Four Pillars of Cisco DNA Center

Driving network insights, automation, and security!



AI Ops

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



Net Ops

Automation to simplify the creation and maintenance of your networks.



Sec Ops

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](#)



