cisco Connect

Simplifying Operations with Cisco's Unified Platform

Jason Clark

February 5, 2026

AI-Ready Data Centers

Future-Proofed Workplaces

Secure Global Connectivity

Digital Resilience

<<<<<< Accelerated by Cisco AI >>>>>>

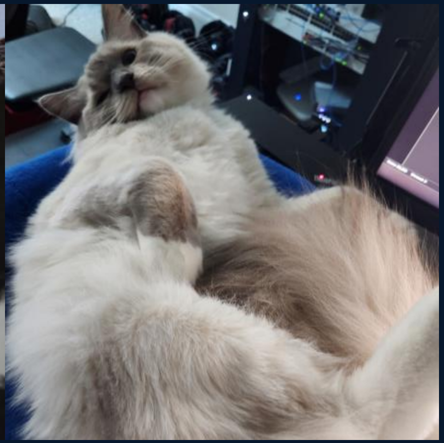
Agenda

1. Introduction
2. Unification
3. Methodology
4. Platform Tools
5. AI Powered Assurance
6. Agentic Ops
7. Summary

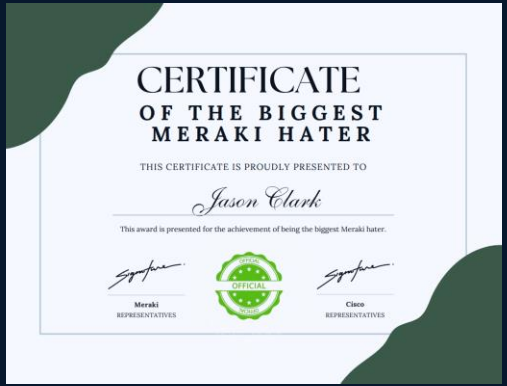
Introduction

Who Am I?

jasoncl2@cisco.com



- Father of ~~four~~ one, do cats count?
- Texas born and raised
- Customer Network Architect for 15 years
- Joined Cisco in 2020 right before the pandemic
- Previously a **Certified Meraki Hater**



CERTIFICATE

OF THE BIGGEST MERAKI HATER

THIS CERTIFICATE IS PROUDLY PRESENTED TO

Jason Clark

This award is presented for the achievement of being the biggest Meraki hater.

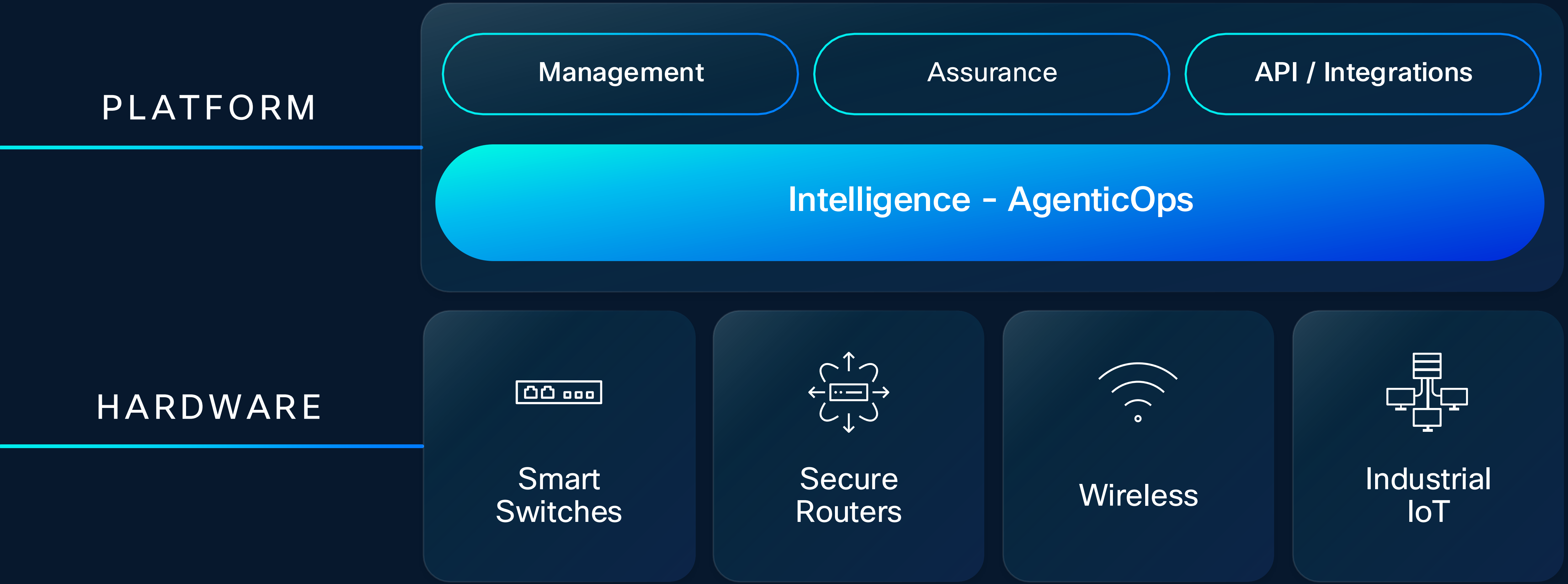
Meraki REPRESENTATIVES

OFFICIAL

Cisco REPRESENTATIVES

Cisco Unification

Our Unified Platform



PLATFORM

Management

Assurance

API / Integrations

Intelligence - AgenticOps

HARDWARE

Smart Switches

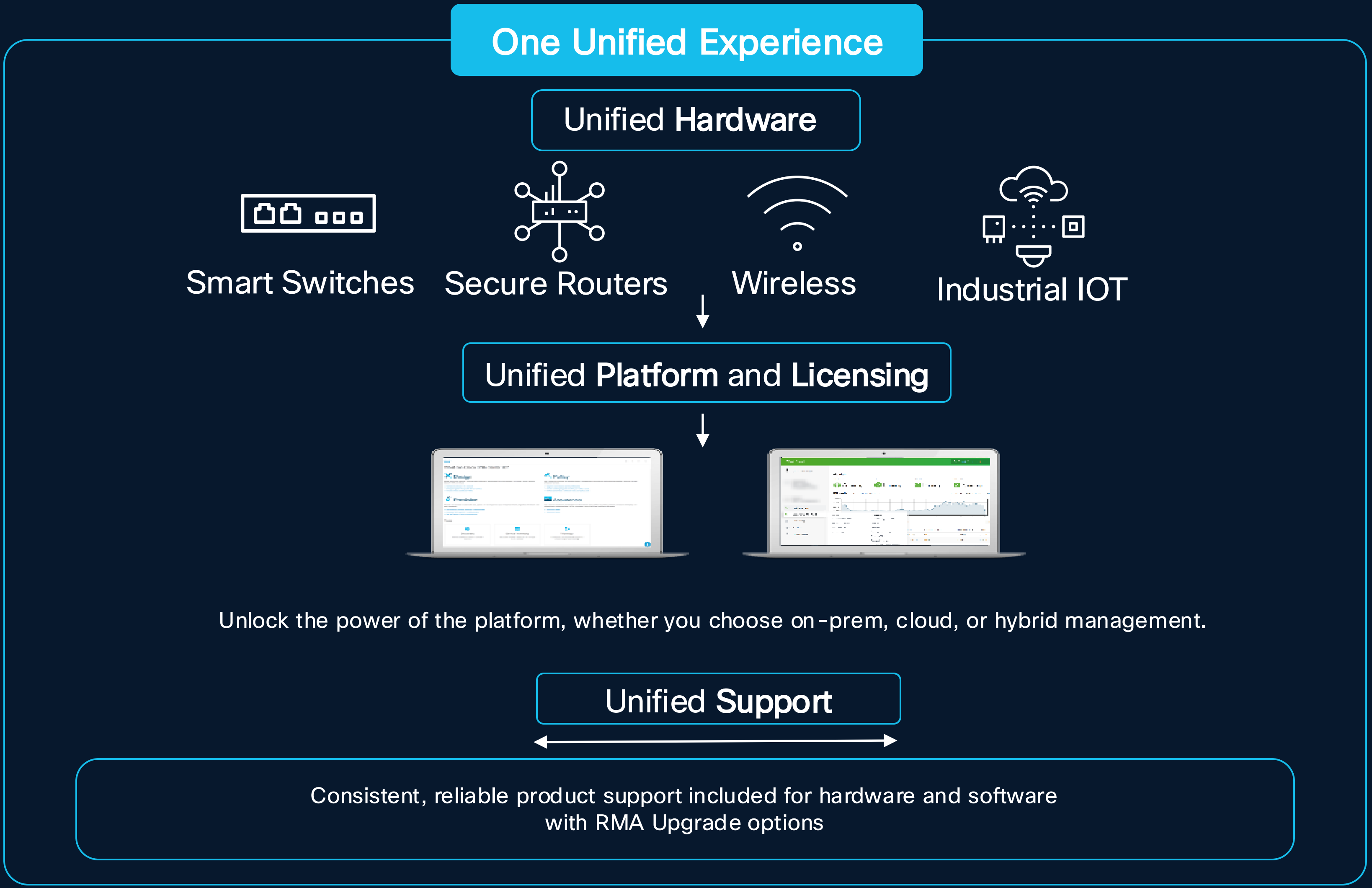
Secure Routers

Wireless

Industrial IoT

Simplifying the Cisco Networking Portfolio

With a New Unified Network Experience



One Unified Experience

Unified **Hardware**

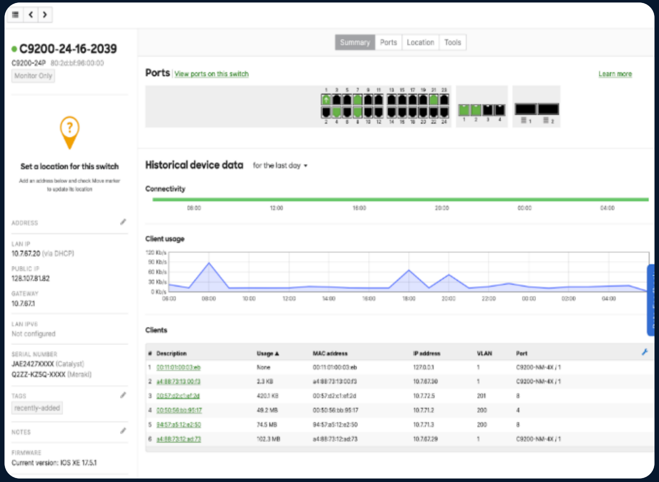
Unified **Platform** and **Licensing**

Unlock the power of the platform, whether you choose on-prem, cloud, or hybrid management.

Unified **Support**

Consistent, reliable product support included for hardware and software
with RMA Upgrade options

We are now making it simpler to choose how you experience our platform



C9200-24-16-2039
C9200-24P 80:2d:bf:96:00:00
Monitor Only

Set a location for this switch
Add an address below and check Move marker to update its location

ADDRESS

LAN IP
10.7.67.20 (via DHCP)

PUBLIC IP
128.107.81.82

GATEWAY
10.7.67.1

LAN IPV6
Not configured

SERIAL NUMBER
JAE2427XXXX (Catalyst)
Q2ZZ-KZ5Q-XXXX (Meraki)

TAGS
recently-added

NOTES

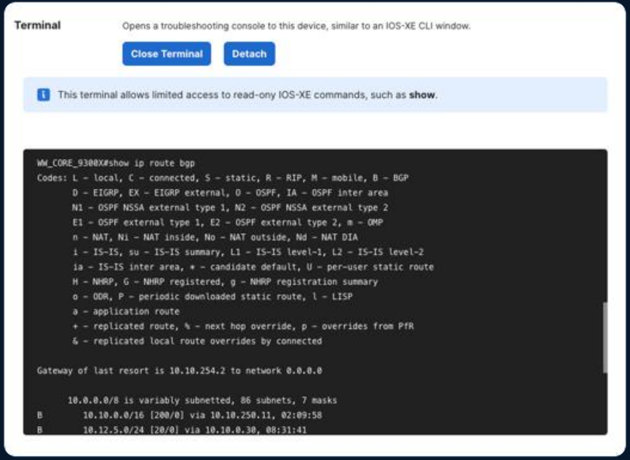
FIRMWARE
Current version: IOS XE 17.5.1

Ports | View ports on this switch

Historical device data for the last day

Clients

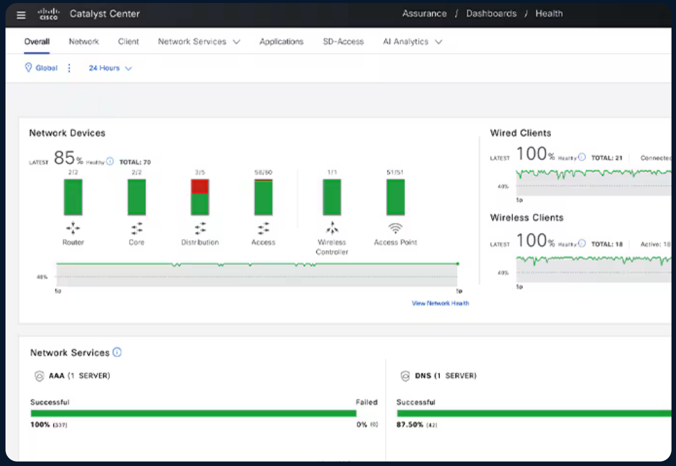
#	Description	Usage ▲	MAC address	IP address	VLAN	Port
1	00:11:01:00:03:eb	None	00:11:01:00:03:eb	127.0.0.1	1	C9200-NM-4X / 1
2	a4:88:73:13:00:f3	2.3 KB	a4:88:73:13:00:f3	10.7.67.30	1	C9200-NM-4X / 1
3	00:57:d2:c1:ef:2d	420.1 KB	00:57:d2:c1:ef:2d	10.7.72.5	201	8
4	00:50:56:bb:95:17	49.2 MB	00:50:56:bb:95:17	10.7.71.2	200	4
5	94:57:a5:12:e2:50	74.5 MB	94:57:a5:12:e2:50	10.7.71.3	200	8
6	a4:88:73:12:ad:73	102.3 MB	a4:88:73:12:ad:73	10.7.67.29	1	C9200-NM-4X / 1



Terminal — Opens a troubleshooting console to this device, similar to an IOS-XE CLI window.

This terminal allows limited access to read-ony IOS-XE commands, such as **show**.

```
WW_CORE_9300X#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.10.254.2 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 86 subnets, 7 masks
B        10.10.0.0/16 [200/0] via 10.10.250.11, 02:09:58
B        10.12.5.0/24 [20/0] via 10.10.0.30, 08:31:41
```



Network Devices
LATEST 85% Healthy TOTAL: 70

Wired Clients
LATEST 100% Healthy TOTAL: 21 Connected

Wireless Clients
LATEST 100% Healthy TOTAL: 18 Active: 18

Network Services
AAA (1 SERVER)
Successful 100% (337)
Failed 0% (0)

DNS (1 SERVER)
Successful 87.50% (42)

Configuration: Cloud

Configuration: Device

On-Premise Management

One Device, One License, One OS, Multiple Ways to Manage

Smart Switches

Secure Routers

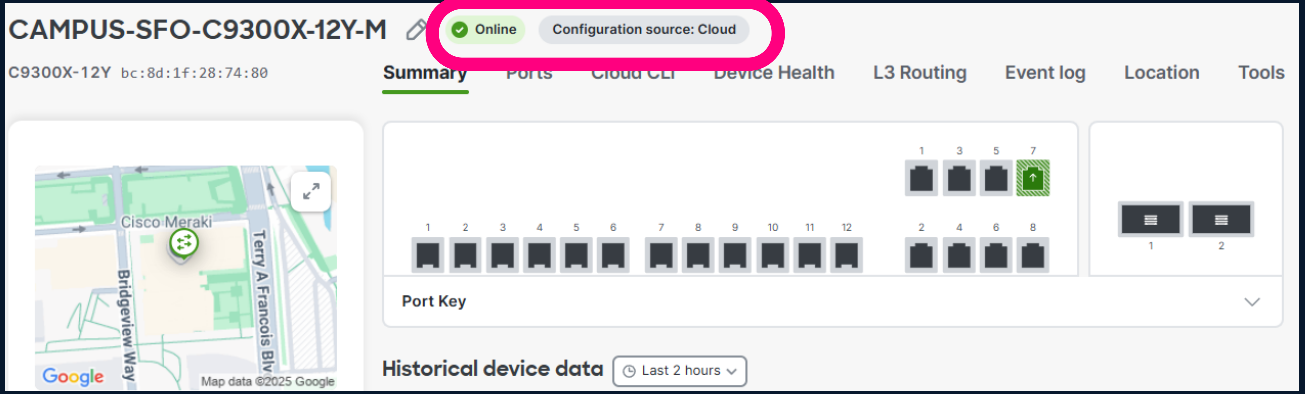
Wireless

Industrial IOT

Configuration: Cloud

Full Cloud-Managed Experience

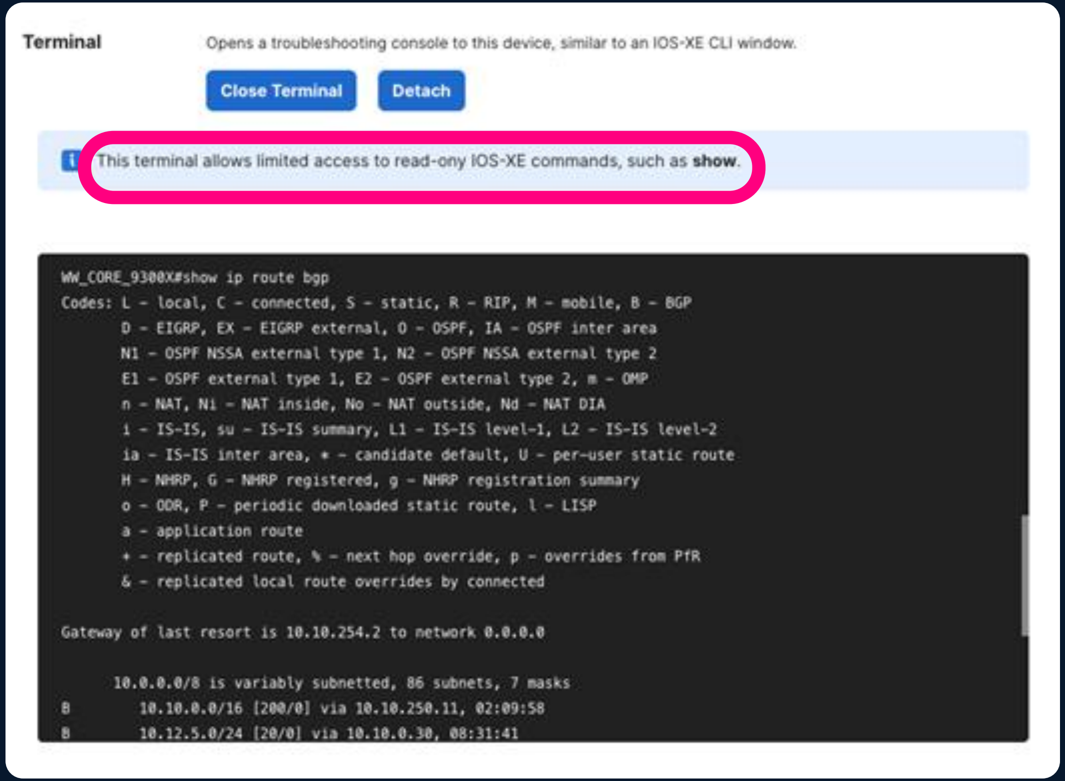
- Same look and feel as traditional Meraki
- Existing C9000 devices can be migrated to Cloud Configuration
- Migration = configuration ‘wipe’
- Rich telemetry and assurance
- Cloud CLI – Limited Write*
- Cloud-based configuration, ZTP, and firmware management


CAMPUS-SFO-C9300X-12Y-M

Online

Configuration source: Cloud

C9300X-12Y bc:8d:1f:28:74:80

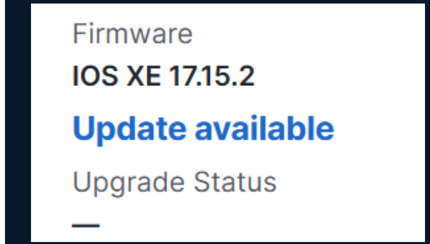

Terminal

Opens a troubleshooting console to this device, similar to an IOS-XE CLI window.

This terminal allows limited access to read-ony IOS-XE commands, such as **show**.

```
WW_CORE_9300X#show ip route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.10.254.2 to network 0.0.0.0

      10.0.0.0/8 is variably subnetted, 86 subnets, 7 masks
B        10.10.0.0/16 [200/0] via 10.10.250.11, 02:09:58
B        10.12.5.0/24 [20/0] via 10.10.0.30, 08:31:41
```

Cloud Native IOS XE


Firmware

IOS XE 17.15.2

Update available

Upgrade Status

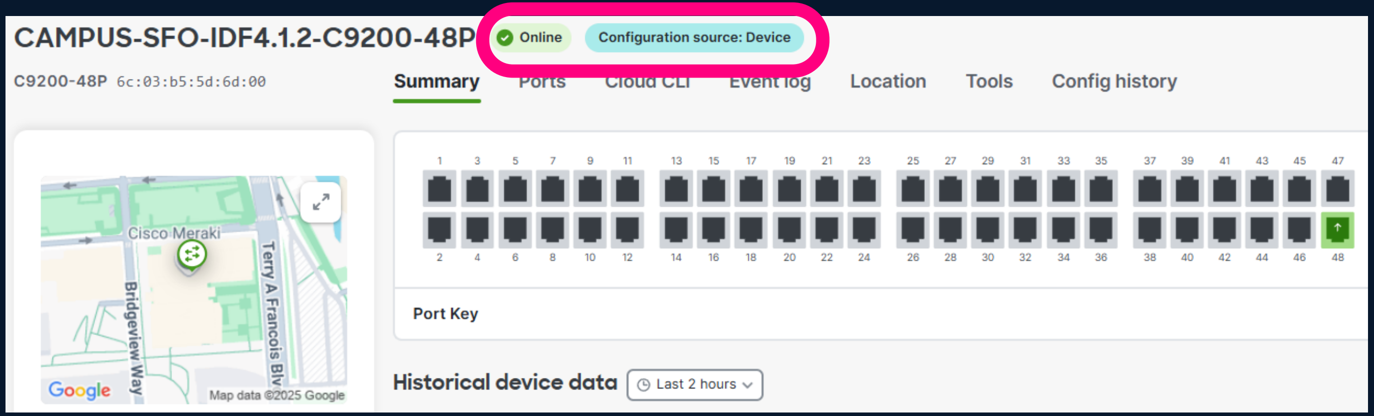
—

*Limited config override with guardrails

Configuration: Device

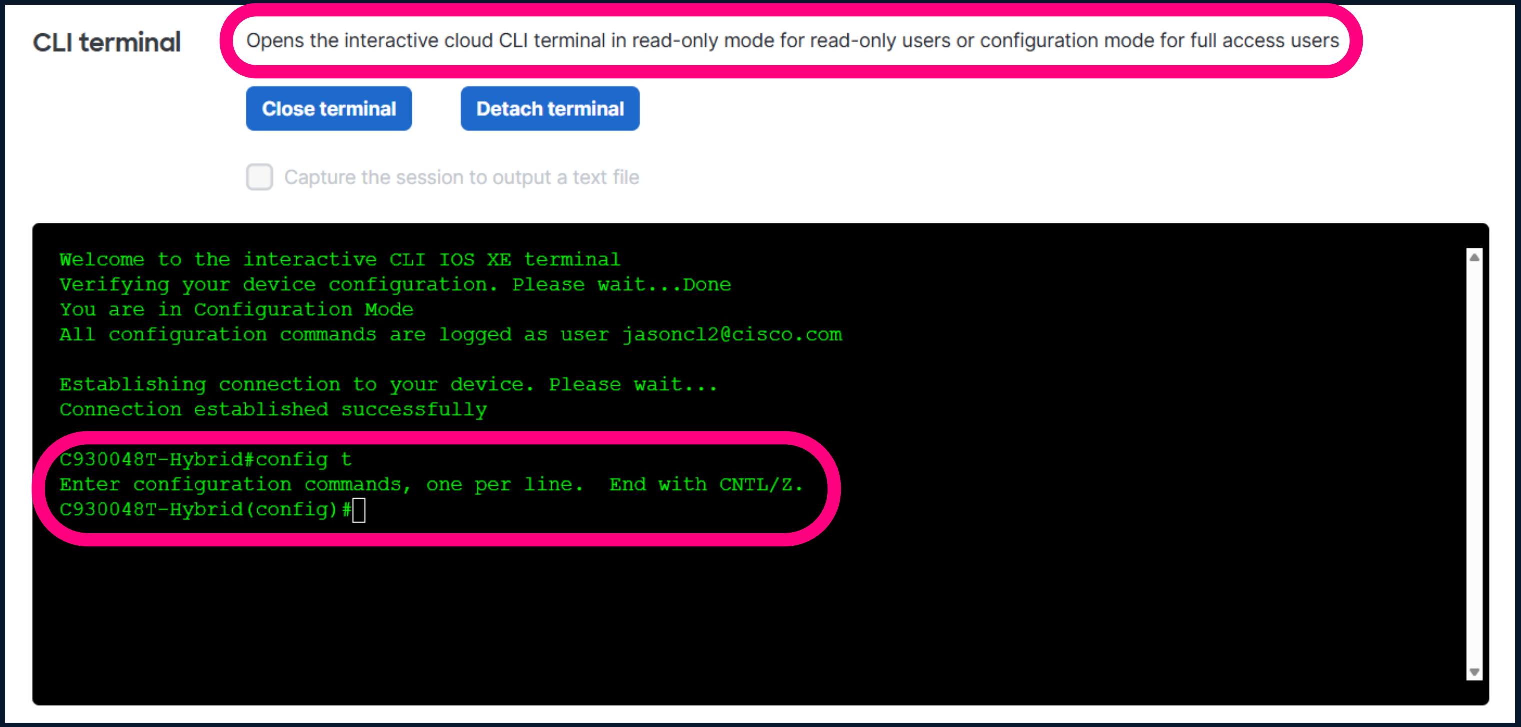
Bringing Assurance to Brownfield

- Uses existing DNA Licensing
- Ideal for brownfield deployments – no data-plane configuration changes
- Troubleshooting telemetry and alerting
- Cloud CLI – Read or config mode
- Configuration local on the device
- Cloud stored configuration history and diff
- Firmware management is road-mapped



CAMPUS-SFO-IDF4.1.2-C9200-48P Online Configuration source: Device

C9200-48P 6c:03:b5:5d:6d:00



CLI terminal

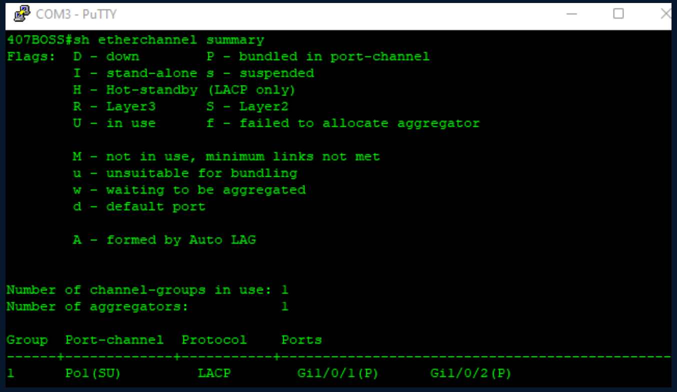
Opens the interactive cloud CLI terminal in read-only mode for read-only users or configuration mode for full access users

```
Welcome to the interactive CLI IOS XE terminal
Verifying your device configuration. Please wait...Done
You are in Configuration Mode
All configuration commands are logged as user jasoncl2@cisco.com

Establishing connection to your device. Please wait...
Connection established successfully

C930048T-Hybrid#config t
Enter configuration commands, one per line.  End with CNTL/Z.
C930048T-Hybrid(config)#
```

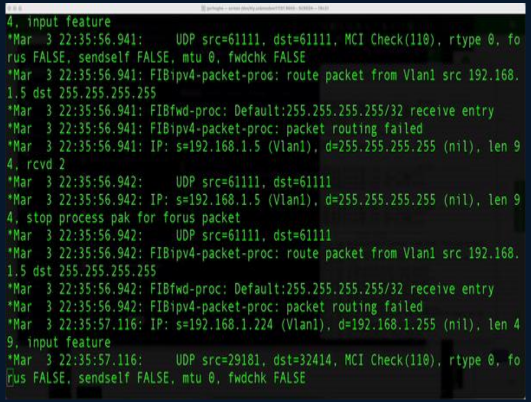
Troubleshooting Methodology

Non-Platform IOS XE CLI Troubleshooting

A Difference in Philosophy



```
407BOSS#sh etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP        Gi1/0/1(P)      Gi1/0/2(P)
```



```
4, input feature
*Mar  3 22:35:56.941:     UDP src=61111, dst=61111, MCI Check(110), rtype 0, fo
rus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
*Mar  3 22:35:56.941: FIBipv4-packet-proc: route packet from Vlan1 src 192.168.
1.5 dst 255.255.255.255
*Mar  3 22:35:56.941: FIBfwd-proc: Default:255.255.255.255/32 receive entry
*Mar  3 22:35:56.941: FIBipv4-packet-proc: packet routing failed
*Mar  3 22:35:56.941: IP: s=192.168.1.5 (Vlan1), d=255.255.255.255 (nil), len 9
4, rcvd 2
*Mar  3 22:35:56.942:     UDP src=61111, dst=61111
*Mar  3 22:35:56.942: IP: s=192.168.1.5 (Vlan1), d=255.255.255.255 (nil), len 9
4, stop process pak for forus packet
*Mar  3 22:35:56.942:     UDP src=61111, dst=61111
*Mar  3 22:35:56.942: FIBipv4-packet-proc: route packet from Vlan1 src 192.168.
1.5 dst 255.255.255.255
*Mar  3 22:35:56.942: FIBfwd-proc: Default:255.255.255.255/32 receive entry
*Mar  3 22:35:56.942: FIBipv4-packet-proc: packet routing failed
*Mar  3 22:35:57.116: IP: s=192.168.1.224 (Vlan1), d=192.168.1.255 (nil), len 4
9, input feature
*Mar  3 22:35:57.116:     UDP src=29181, dst=32414, MCI Check(110), rtype 0, fo
rus FALSE, sendself FALSE, mtu 0, fwdchk FALSE
```

Show Commands / Live Tools / Show Log

Debug Commands

Packet Capture

Cloud Management Troubleshooting

A Difference in Philosophy

Dashboard GUI
Live Tools
Event Logs

Assurance / Root Cause Analysis / Alerts

Intelligent PCAPs and Analysis

Meraki Platform APIs

Platform Intelligence

Contextual analysis of available network data in the right place, at the right time

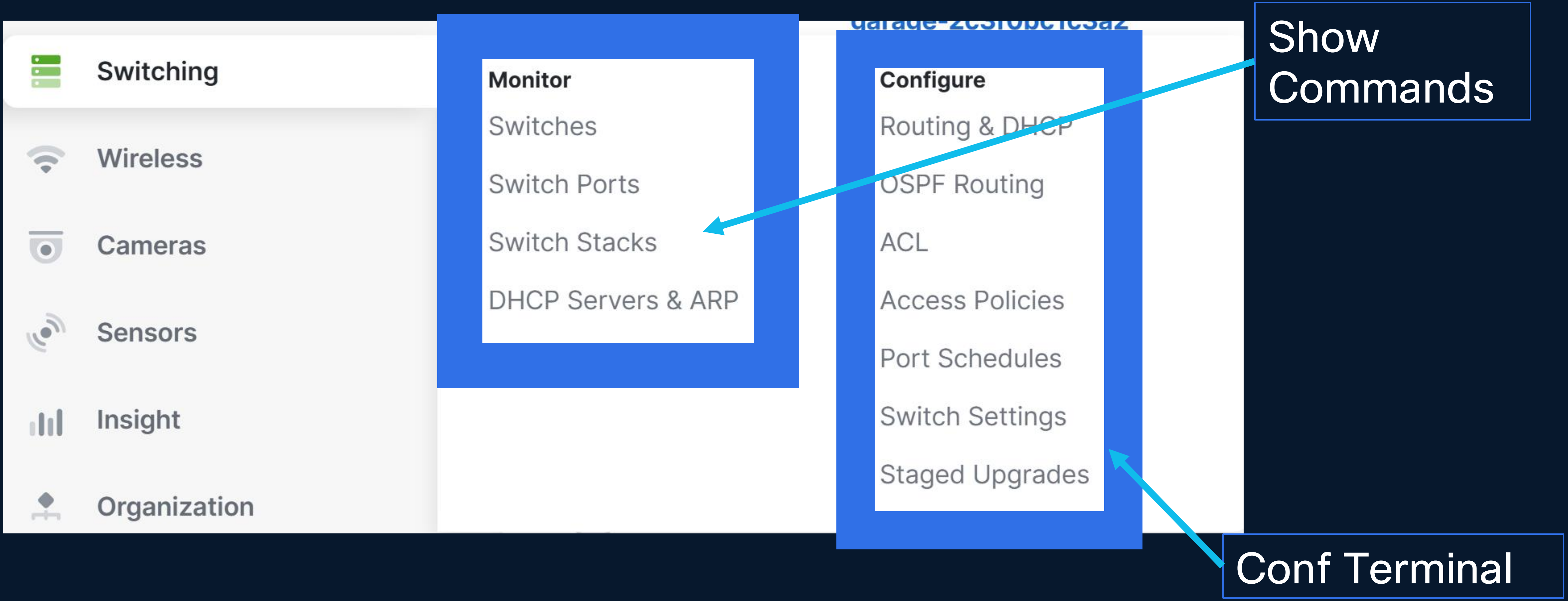
Machine Learning

Proactive response to changing conditions

Evergreen and no need to maintain management infrastructure

Meraki Monitor / Configure

Like IOS XE Show Commands and Configure Terminal



Switching

Wireless

Cameras

Sensors

Insight

Organization

Monitor

- Switches
- Switch Ports
- Switch Stacks
- DHCP Servers & ARP

Configure

- Routing & DHCP
- OSPF Routing
- ACL
- Access Policies
- Port Schedules
- Switch Settings
- Staged Upgrades

Show Commands

Conf Terminal

Platform Tools

Resilient Connectivity to the Cloud

Uplink Auto Config (UAC)

- Automated discovery for dashboard connectivity
- Automated failover / path discovery
- Tunable for primary interface
- Creates stack-ranked interface list

Safe Config Rollback

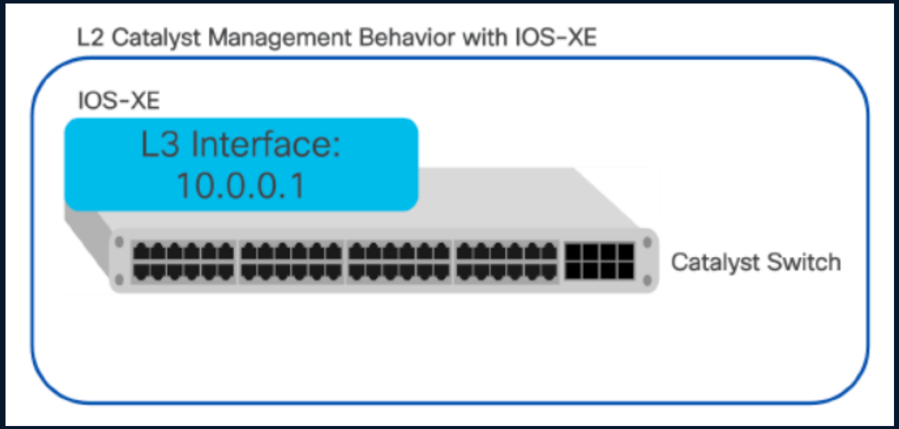
- Recovery mechanism for configuration error
- Marks configuration safe if dashboard connectivity is maintained after change
- Will roll-back to safe config if dashboard access is lost after configuration change

Uplink Auto Config (UAC)

- Uplink Auto Configuration facilitates automatic identification of uplink interfaces, eliminating the need for manual configuration of the switch.

- UAC supports new and existing deployments

- UAC selects the uplink interface, connects to dashboard, and maintains the uplink connectivity.



Requirements:

- Underlying network has connectivity to Dashboard

- DHCP or static IP

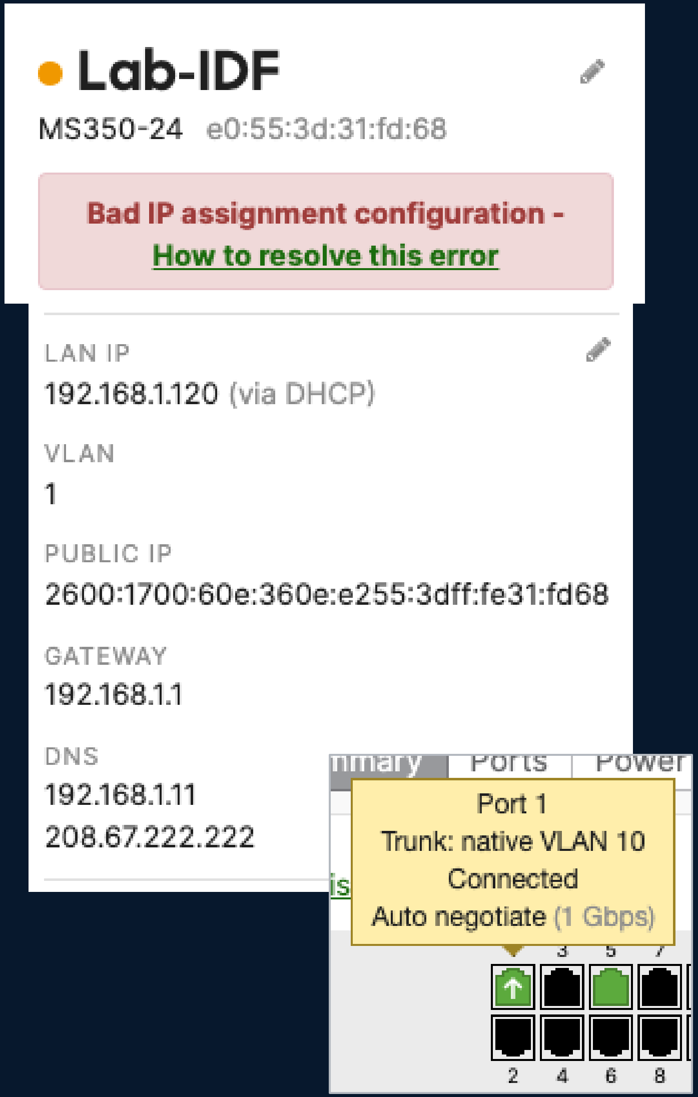
- DNS

- Minimum 60 packets per 2 minutes

- Preference is uplink port in Trunk Allowed All

Automatic Rollback of Bad Uplink / IP Config

Safe Config Rollback



● Lab-IDF

MS350-24 e0:55:3d:31:fd:68

Bad IP assignment configuration - How to resolve this error

LAN IP
192.168.1.120 (via DHCP)

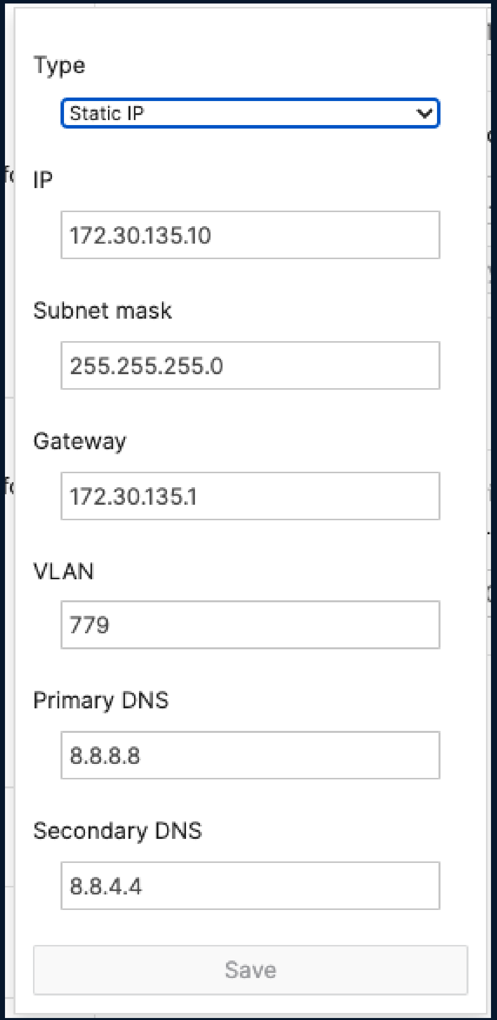
VLAN
1

PUBLIC IP
2600:1700:60e:360e:e255:3dff:fe31:fd68

GATEWAY
192.168.1.1

DNS
192.168.1.11
208.67.222.222

Port 1
Trunk: native VLAN 10
Connected
Auto negotiate (1 Gbps)



Type: Static IP

IP: 172.30.135.10

Subnet mask: 255.255.255.0

Gateway: 172.30.135.1

VLAN: 779

Primary DNS: 8.8.8.8

Secondary DNS: 8.8.4.4

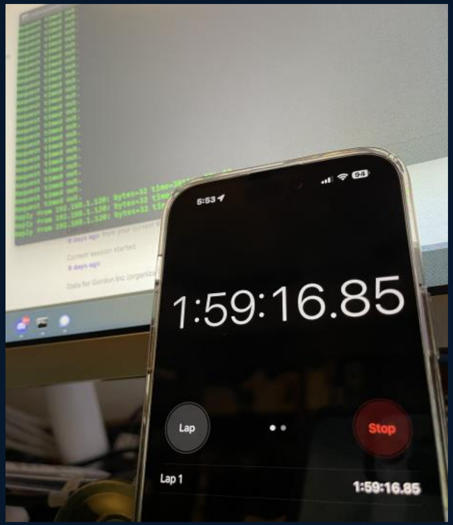
1. Change made in dashboard config
2. Synchronize config to device
3. Determine Impact to Management Tunnel
4. Rollback configuration Change
5. Update Dashboard with config error/alert

Note: Uplinks are extra resilient
Uplink config is tracked on node

Config Safe Mechanic

Safe Config Rollback

- Configuration changes are marked safe 30 minutes after a configuration change
- Configuration changes are marked safe 2 hours after firmware upgrades



If the configuration is **not** safe (loss of connectivity)

- Device will try to obtain an IP address on an alternate VLAN
- Device will revert to previous safe configuration after 2 hours
- After reverting to a safe configuration, the former configuration will be marked bad

1. Change made in dashboard config

2. Synchronize config to device

3. Device starts 30-minute timer to ensure configuration is safe

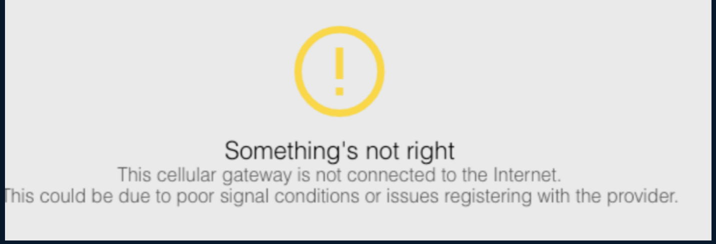
Config

4. After 2 hours of lost connectivity the config will roll back

Note: Power cycle during 2-hour outage window will force rollback to last known good configuration

Break Glass Option

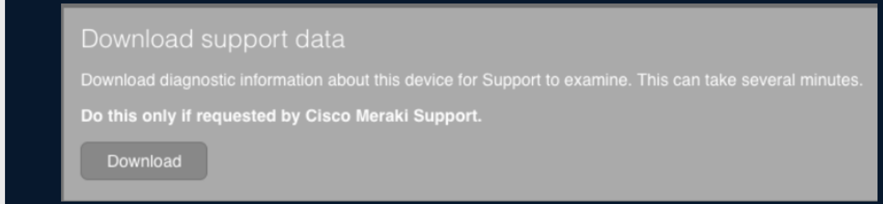
Local Status Page for Cloud Mode



Something's not right

This cellular gateway is not connected to the Internet.

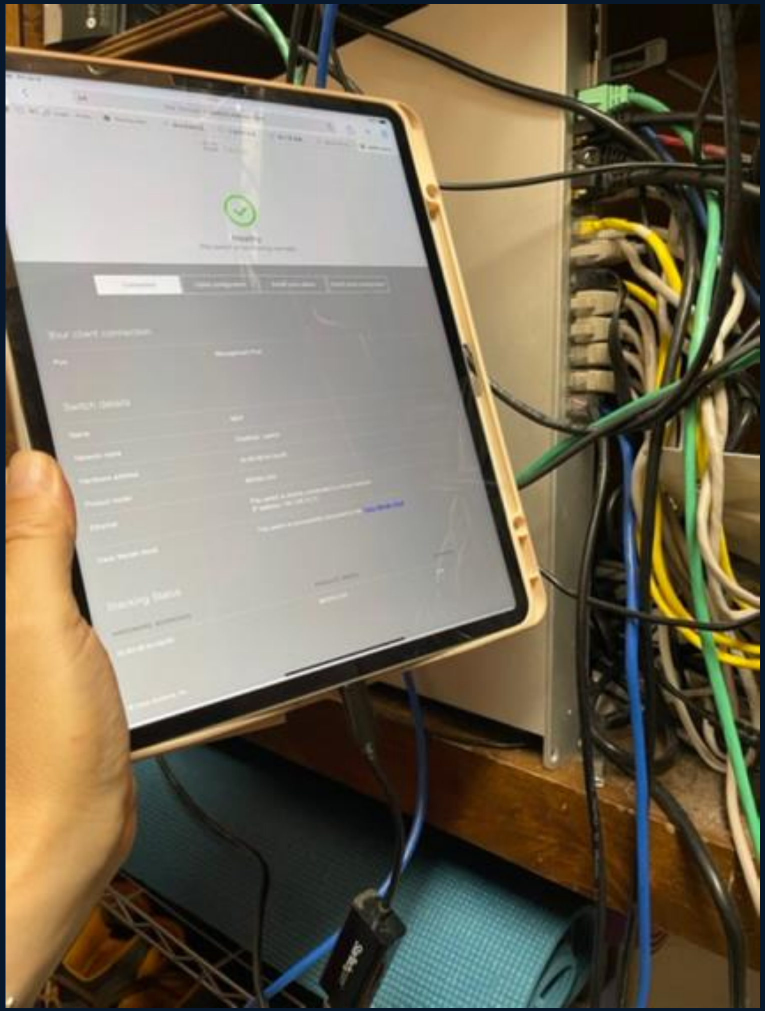
This could be due to poor signal conditions or issues registering with the provider.



Download support data

Download diagnostic information about this device for Support to examine. This can take several minutes.

Do this only if requested by Cisco Meraki Support.



Verify or restore cloud connectivity:

- View or edit
  - Static IP assignments and DNS servers
  - Port type, speed, and duplex
  - VLAN assignments

Methods to access:

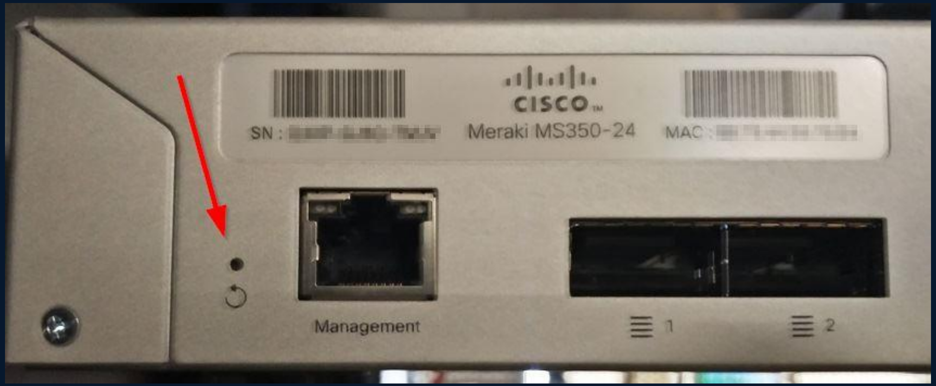
- Connect directly to mgmt. port or any LAN port
- All modern smart phones / tablets support USB-C style NIC
- Can be remotely accessed (Security!)

Tip: The LSP is intended to restore cloud connectivity, not to make configuration changes

Factory Reset

Force Config Reset and Pull Config

If configuration is in a state that cannot recover you can reset factory and force re-download. This also resets the firmware.



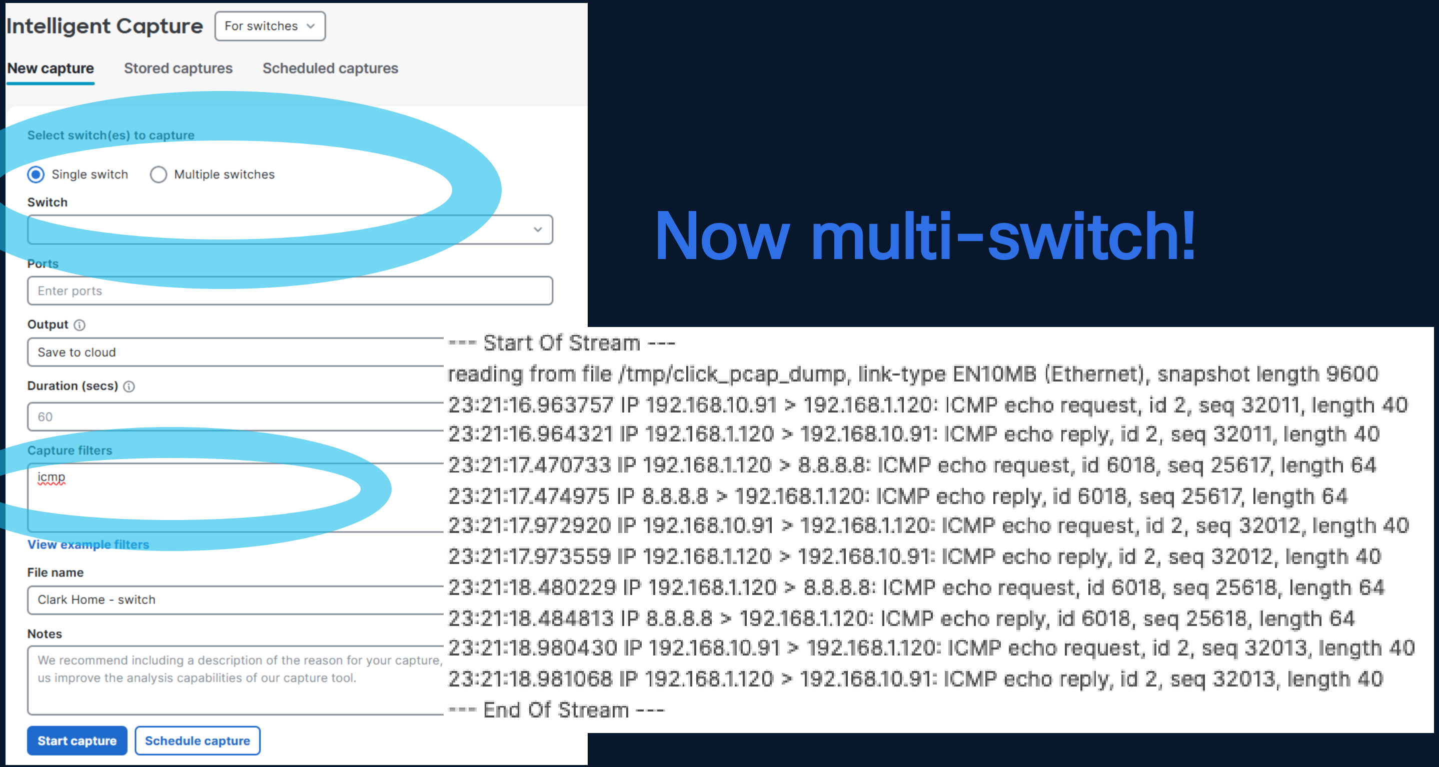
Hold reset button for 10-15 seconds

1. Wipe configuration with reset

2. Synchronize config to device

Factory Reset in a platform world is not a defeat! Configuration, logs, and analytics are stored in the cloud

~~Packet Capture~~ Intelligent Capture



Intelligent Capture [For switches]

New capture | Stored captures | Scheduled captures

Select switch(es) to capture

● Single switch ○ Multiple switches

Switch

Ports: Enter ports

Output: Save to cloud

Duration (secs): 60

Capture filters: icmp

View example filters

File name: Clark Home - switch

Notes: We recommend including a description of the reason for your capture,
us improve the analysis capabilities of our capture tool.

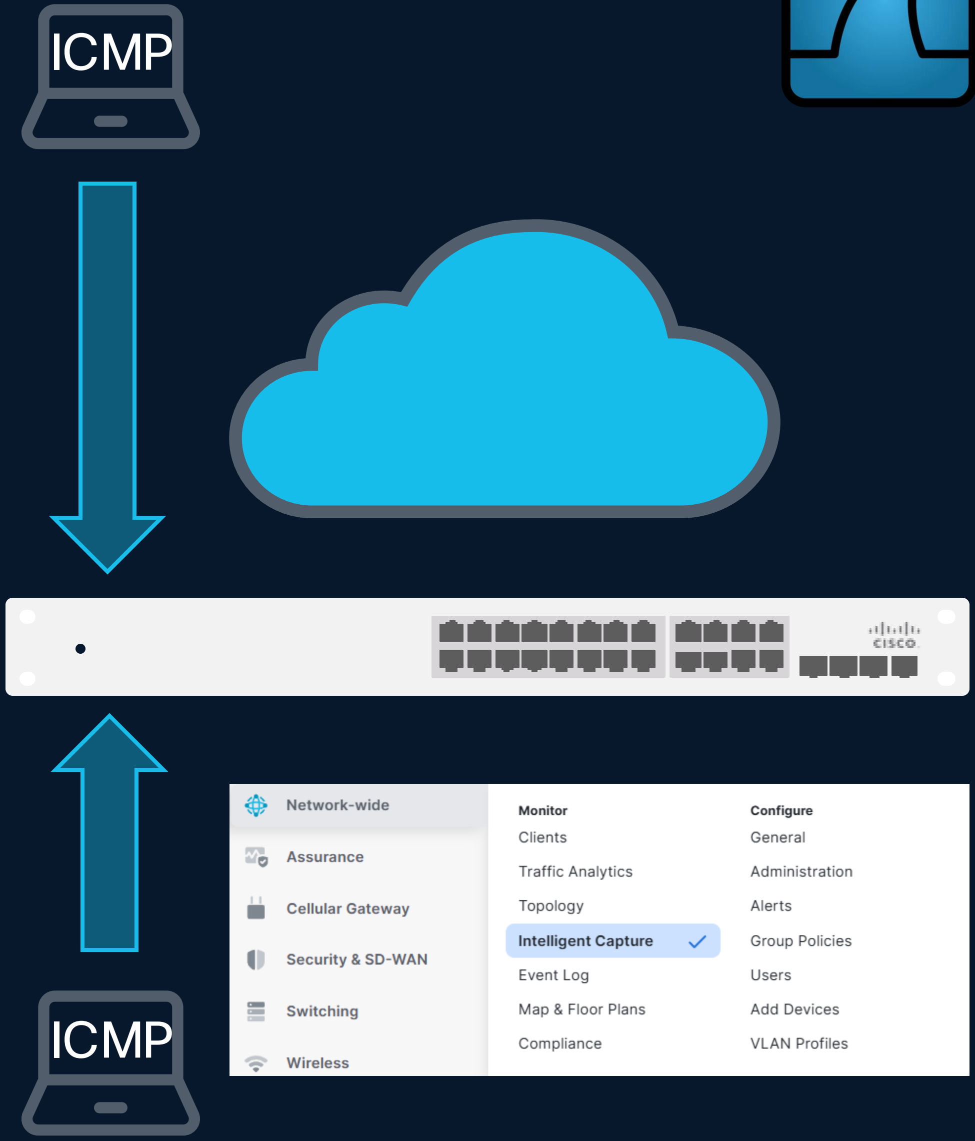
Start capture | Schedule capture

```
--- Start Of Stream ---
reading from file /tmp/click_pcap_dump, link-type EN10MB (Ethernet), snapshot length 9600
23:21:16.963757 IP 192.168.10.91 > 192.168.1.120: ICMP echo request, id 2, seq 32011, length 40
23:21:16.964321 IP 192.168.1.120 > 192.168.10.91: ICMP echo reply, id 2, seq 32011, length 40
23:21:17.470733 IP 192.168.1.120 > 8.8.8.8: ICMP echo request, id 6018, seq 25617, length 64
23:21:17.474975 IP 8.8.8.8 > 192.168.1.120: ICMP echo reply, id 6018, seq 25617, length 64
23:21:17.972920 IP 192.168.10.91 > 192.168.1.120: ICMP echo request, id 2, seq 32012, length 40
23:21:17.973559 IP 192.168.1.120 > 192.168.10.91: ICMP echo reply, id 2, seq 32012, length 40
23:21:18.480229 IP 192.168.1.120 > 8.8.8.8: ICMP echo request, id 6018, seq 25618, length 64
23:21:18.484813 IP 8.8.8.8 > 192.168.1.120: ICMP echo reply, id 6018, seq 25618, length 64
23:21:18.980430 IP 192.168.10.91 > 192.168.1.120: ICMP echo request, id 2, seq 32013, length 40
23:21:18.981068 IP 192.168.1.120 > 192.168.10.91: ICMP echo reply, id 2, seq 32013, length 40
--- End Of Stream ---
```

Now multi-switch!

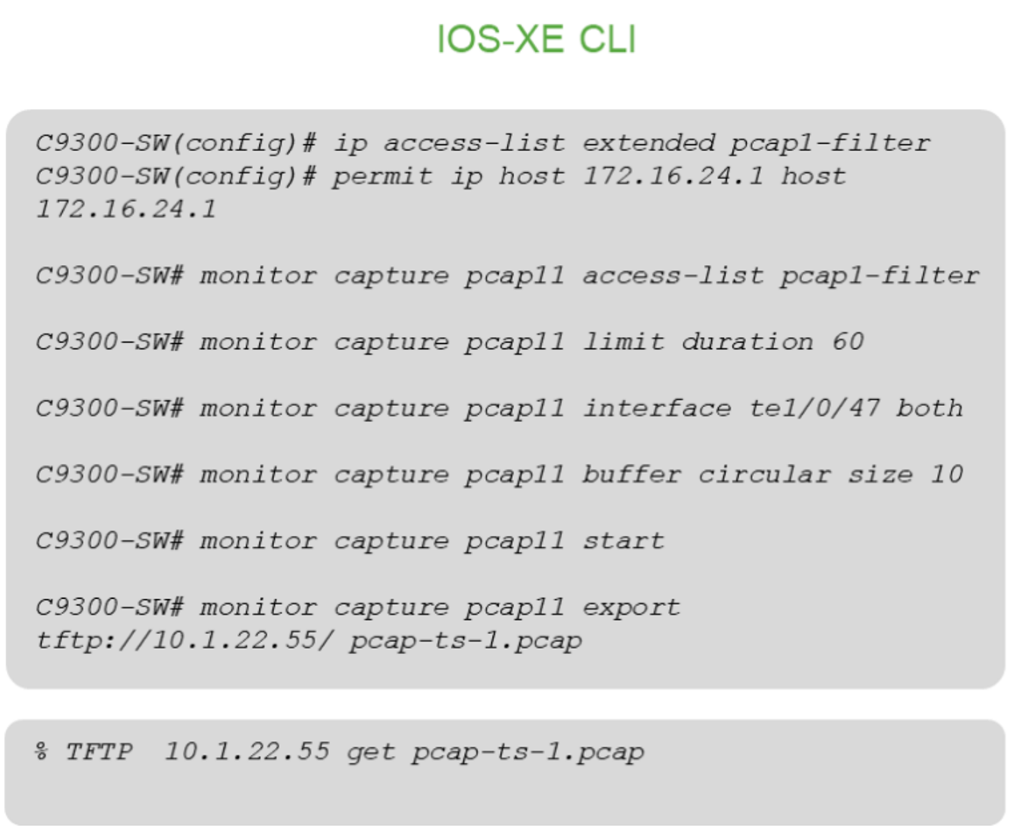
Example ICMP filter with real-time packet output

Tip: Run captures simultaneously on source/destination for troubleshooting



Packet Capture – Meraki Powered

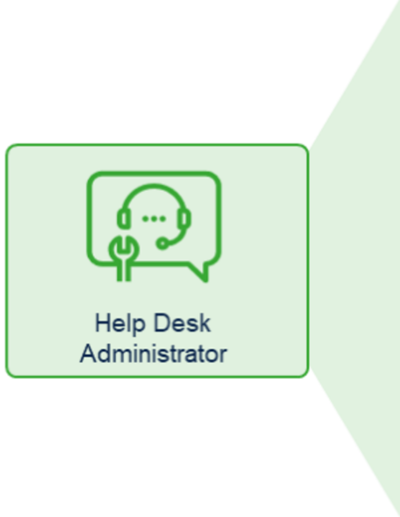
Simplified Troubleshooting for Tier 1 Support and Help Desk – No IOS XE CLI Experience Required

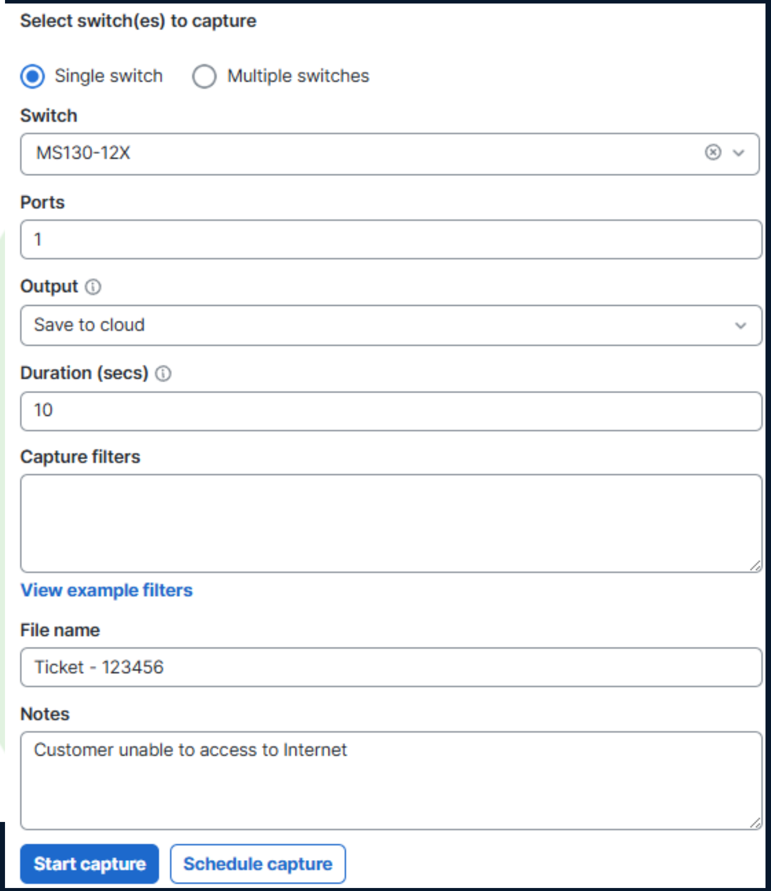


IOS-XE CLI

```
C9300-SW(config)# ip access-list extended pcap1-filter
C9300-SW(config)# permit ip host 172.16.24.1 host
172.16.24.1

C9300-SW# monitor capture pcap11 access-list pcap1-filter

C9300-SW# monitor capture pcap11 limit duration 60

C9300-SW# monitor capture pcap11 interface te1/0/47 both

C9300-SW# monitor capture pcap11 buffer circular size 10

C9300-SW# monitor capture pcap11 start

C9300-SW# monitor capture pcap11 export
tftp://10.1.22.55/ pcap-ts-1.pcap
```

```
% TFTP  10.1.22.55 get pcap-ts-1.pcap
```





Select switch(es) to capture

● Single switch ○ Multiple switches

Switch: MS130-12X

Ports: 1

Output: Save to cloud

Duration (secs): 10

Capture filters:

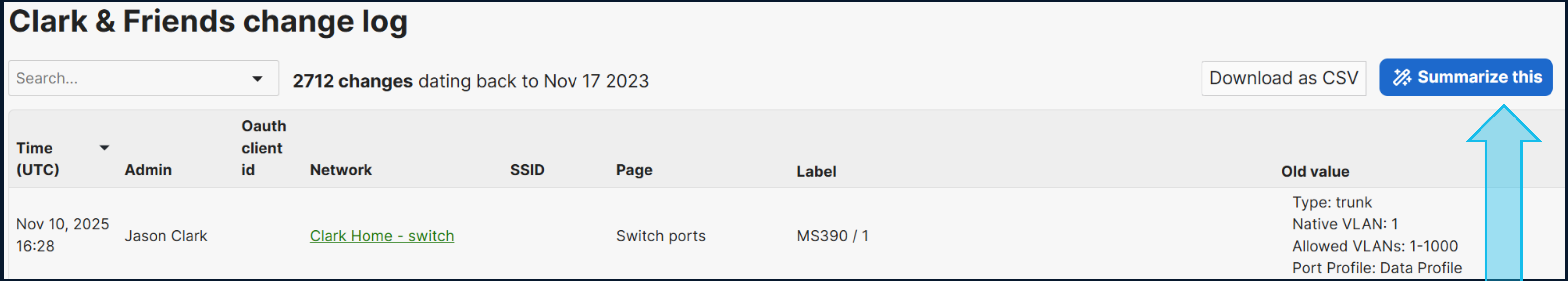
View example filters

File name: Ticket - 123456

Notes: Customer unable to access to Internet

Change Log and Event Log

Change Log



Clark & Friends change log

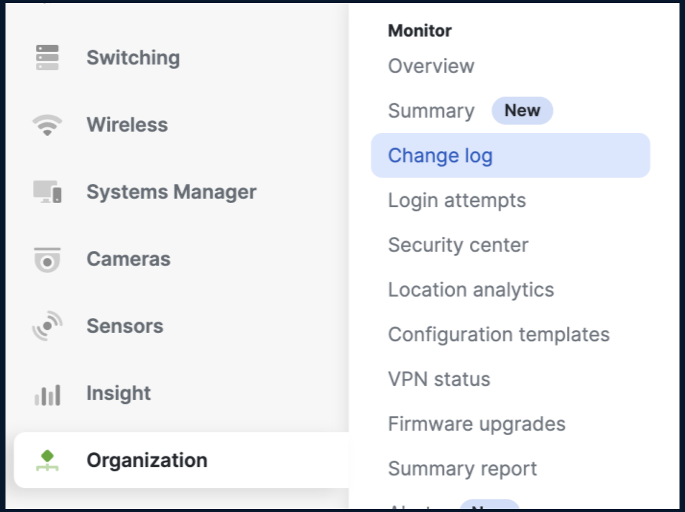
Search...

2712 changes dating back to Nov 17 2023

Download as CSV

Summarize this

Time (UTC)	Admin	Oauth client id	Network	SSID	Page	Label	Old value
Nov 10, 2025 16:28	Jason Clark		Clark Home - switch		Switch ports	MS390 / 1	Type: trunk Native VLAN: 1 Allowed VLANs: 1-1000 Port Profile: Data Profile



The fastest way to get your bearings during an outage is to look for what has changed

Searchable by Admin, Network, Tag, Time

Can be consumed by API, download-able as a CSV

Fulfills change-log compliance requirements such as PCI

AI Assistant can summarize changes and look for anomalies

Tip: Support usually starts here

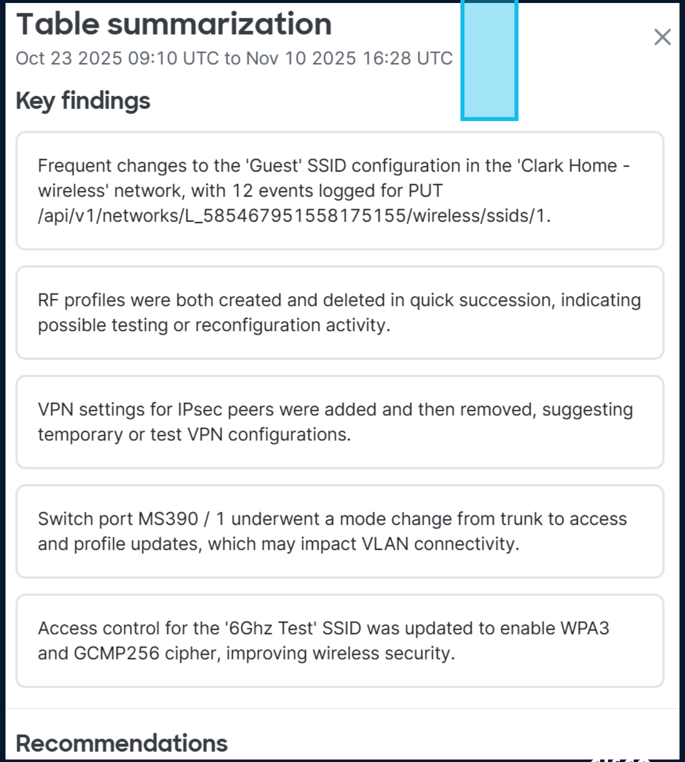


Table summarization

Oct 23 2025 09:10 UTC to Nov 10 2025 16:28 UTC

Key findings

Frequent changes to the 'Guest' SSID configuration in the 'Clark Home - wireless' network, with 12 events logged for PUT /api/v1/networks/L_585467951558175155/wireless/ssids/1.

RF profiles were both created and deleted in quick succession, indicating possible testing or reconfiguration activity.

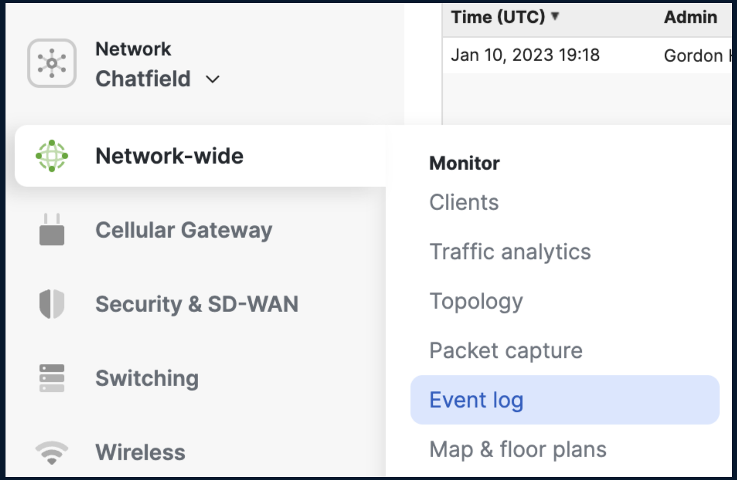
VPN settings for IPsec peers were added and then removed, suggesting temporary or test VPN configurations.

Switch port MS390 / 1 underwent a mode change from trunk to access and profile updates, which may impact VLAN connectivity.

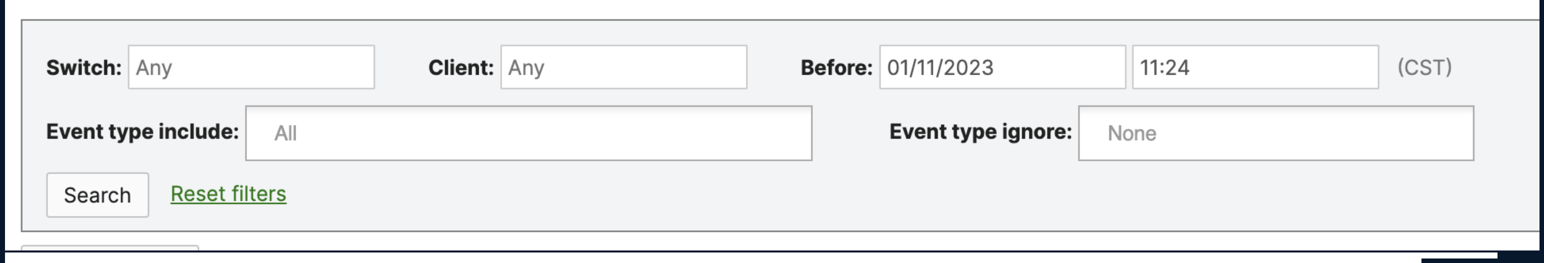
Access control for the '6Ghz Test' SSID was updated to enable WPA3 and GCMP256 cipher, improving wireless security.

Recommendations

Event Log

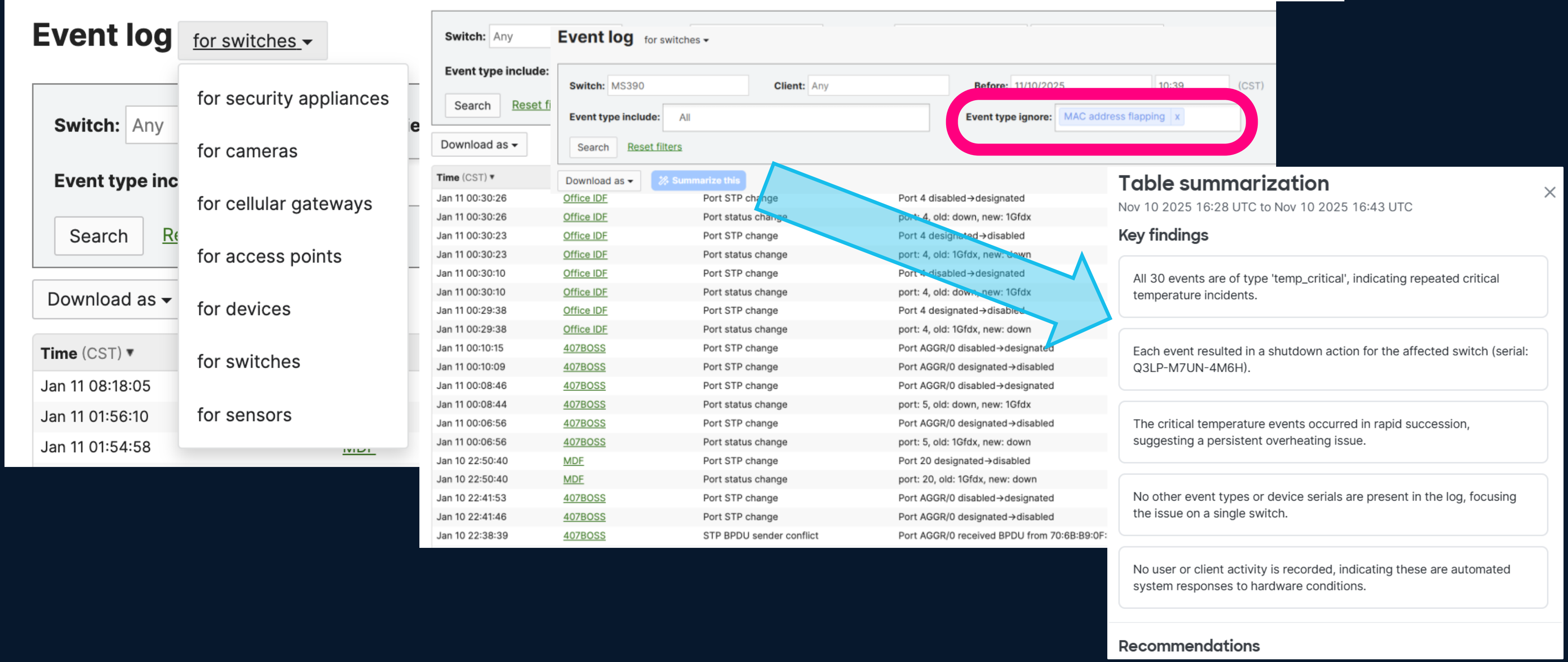


Time (UTC) ▾	Admin
Jan 10, 2023 19:18	Gordon



Switch: Any Client: Any Before: 01/11/2023 11:24 (CST)

Event type include: All Event type ignore: None



Switch: Any

Event type include:

Time (CST) ▾
Jan 11 08:18:05
Jan 11 01:56:10
Jan 11 01:54:58

Event log for switches

Switch: MS390 Client: Any Before: 11/10/2025 10:39 (CST)

Event type include: All Event type ignore: MAC address flapping x

Time (CST) ▾			
Jan 11 00:30:26	Office IDF	Port STP change	Port 4 disabled→designated
Jan 11 00:30:26	Office IDF	Port status change	port: 4, old: down, new: 1Gfdx
Jan 11 00:30:23	Office IDF	Port STP change	Port 4 designated→disabled
Jan 11 00:30:23	Office IDF	Port status change	port: 4, old: 1Gfdx, new: down
Jan 11 00:30:10	Office IDF	Port STP change	Port 4 disabled→designated
Jan 11 00:30:10	Office IDF	Port status change	port: 4, old: down, new: 1Gfdx
Jan 11 00:29:38	Office IDF	Port STP change	Port 4 designated→disabled
Jan 11 00:29:38	Office IDF	Port status change	port: 4, old: 1Gfdx, new: down
Jan 11 00:10:15	407BOSS	Port STP change	Port AGGR/0 disabled→designated
Jan 11 00:10:09	407BOSS	Port STP change	Port AGGR/0 designated→disabled
Jan 11 00:08:46	407BOSS	Port STP change	Port AGGR/0 disabled→designated
Jan 11 00:08:44	407BOSS	Port status change	port: 5, old: down, new: 1Gfdx
Jan 11 00:06:56	407BOSS	Port STP change	Port AGGR/0 designated→disabled
Jan 11 00:06:56	407BOSS	Port status change	port: 5, old: 1Gfdx, new: down
Jan 10 22:50:40	MDF	Port STP change	Port 20 designated→disabled
Jan 10 22:50:40	MDF	Port status change	port: 20, old: 1Gfdx, new: down
Jan 10 22:41:53	407BOSS	Port STP change	Port AGGR/0 disabled→designated
Jan 10 22:41:46	407BOSS	Port STP change	Port AGGR/0 designated→disabled
Jan 10 22:38:39	407BOSS	STP BPDU sender conflict	Port AGGR/0 received BPDU from 70:6B:B9:0F:

Table summarization

Nov 10 2025 16:28 UTC to Nov 10 2025 16:43 UTC

Key findings

All 30 events are of type 'temp_critical', indicating repeated critical temperature incidents.

Each event resulted in a shutdown action for the affected switch (serial: Q3LP-M7UN-4M6H).

The critical temperature events occurred in rapid succession, suggesting a persistent overheating issue.

No other event types or device serials are present in the log, focusing the issue on a single switch.

No user or client activity is recorded, indicating these are automated system responses to hardware conditions.

Recommendations

Logs can be exported to syslog servers

AI Assistant can now summarize and make recommendations

Tip: When trying to find issues leverage the ‘event type ignore’ option (remove the hay to find the needle)

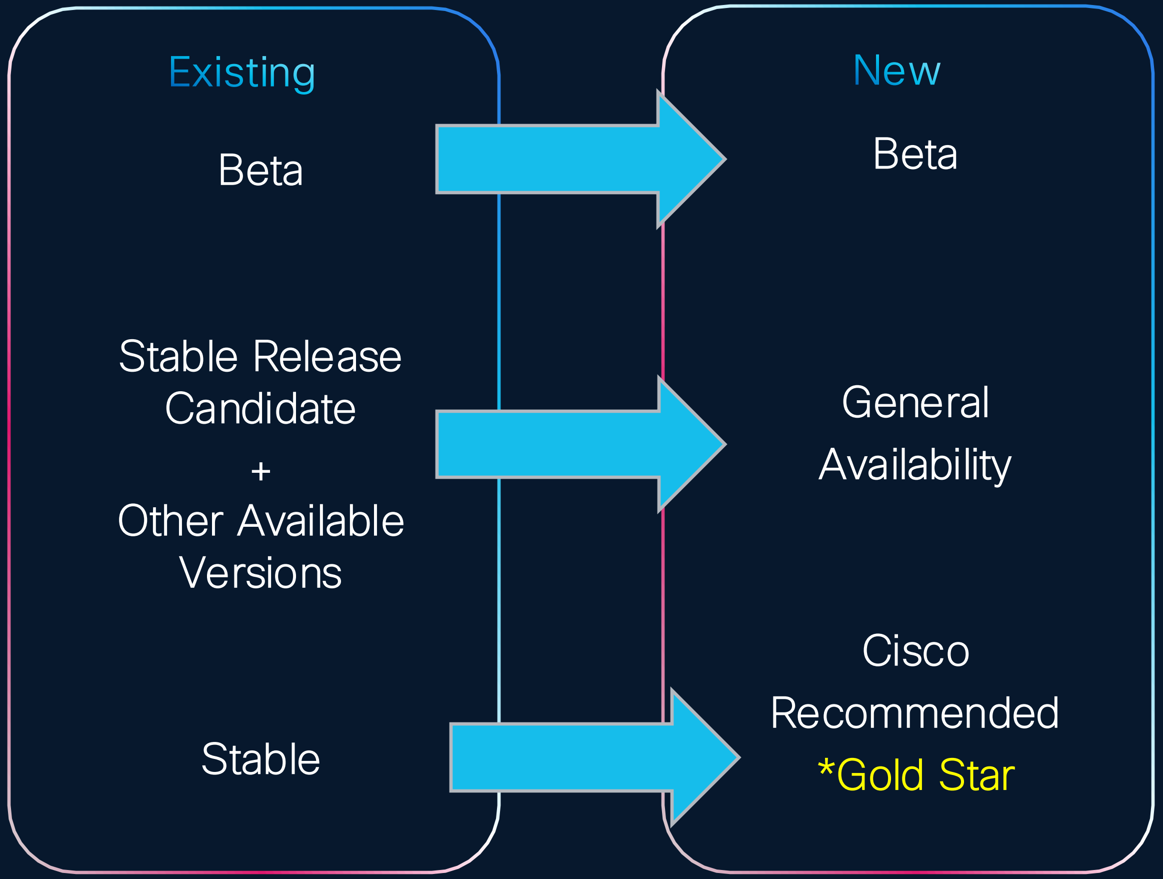
Firmware

Firmware = Troubleshooting?

Firmware is Absolutely Part of the Troubleshooting Methodology

- Recent firmware changes may be impacting the network
- Firmware bugs do exist
- Firmware features may change packet flow behavior
- When comparing, check Firmware differences
- Good excuse to reboot

20.X → 26.X [year].[feature release]



Existing

Beta

Stable Release Candidate + Other Available Versions

Stable

New

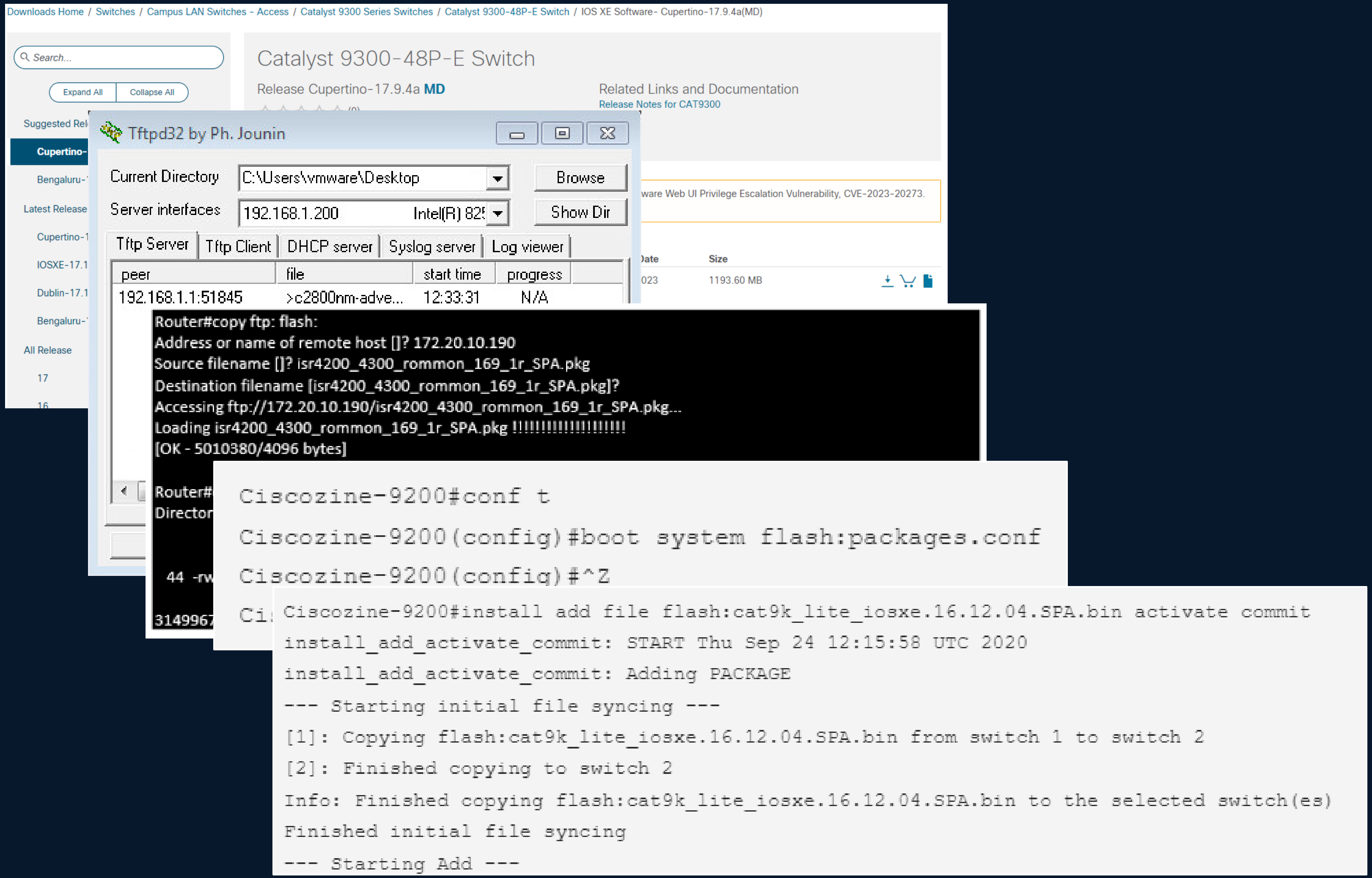
Beta

General Availability

Cisco Recommended *Gold Star

Firmware Management – Traditional Approach

1. Obtain the Firmware
2. Copy to device
3. Set Boot Variable
4. Run install command
5. Reload
6. Clean up



Downloads Home / Switches / Campus LAN Switches - Access / Catalyst 9300 Series Switches / Catalyst 9300-48P-E Switch / IOS XE Software- Cupertino-17.9.4a(MD)

Catalyst 9300-48P-E Switch

Release Cupertino-17.9.4a **MD**

Related Links and Documentation

Release Notes for CAT9300

ware Web UI Privilege Escalation Vulnerability, CVE-2023-20273.

Tftpd32 by Ph. Jounin

Current Directory: C:\Users\vmware\Desktop

Server interfaces: 192.168.1.200 Intel(R) 82!

```
peer                 file            start time   progress
192.168.1.1:51845    >c2800nm-adve...  12:33:31    N/A
```

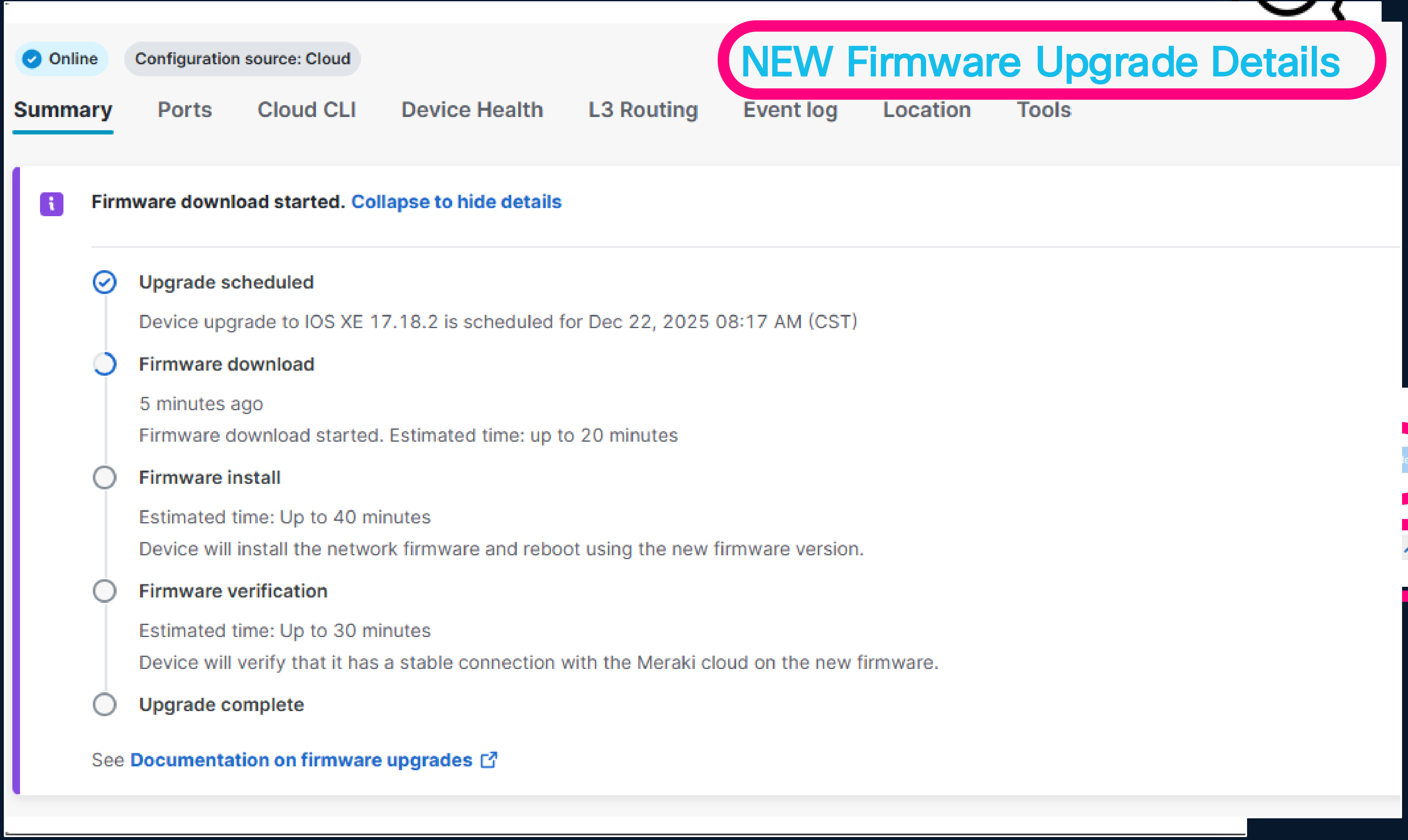
```
Router#copy ftp: flash:
Address or name of remote host []? 172.20.10.190
Source filename []? isr4200_4300_rommon_169_1r_SPA.pkg
Destination filename [isr4200_4300_rommon_169_1r_SPA.pkg]?
Accessing ftp://172.20.10.190/isr4200_4300_rommon_169_1r_SPA.pkg...
Loading isr4200_4300_rommon_169_1r_SPA.pkg !!!!!!!!!!!!!!!!!!!!
[OK - 5010380/4096 bytes]

Router#
Director

 44 -rw

3149967
```

```
Ciscozine-9200#conf t
Ciscozine-9200(config)#boot system flash:packages.conf
Ciscozine-9200(config)#^Z
Ci
```

```
Ciscozine-9200#install add file flash:cat9k_lite_iosxe.16.12.04.SPA.bin activate commit
install_add_activate_commit: START Thu Sep 24 12:15:58 UTC 2020
install_add_activate_commit: Adding PACKAGE
--- Starting initial file syncing ---
[1]: Copying flash:cat9k_lite_iosxe.16.12.04.SPA.bin from switch 1 to switch 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_lite_iosxe.16.12.04.SPA.bin to the selected switch(es)
Finished initial file syncing
--- Starting Add ---
```

Firmware Management – Platform Approach

1. Select your Firmware
2. Schedule your Upgrade
3. Take a break – you earned it!



NEW Firmware Upgrade Details

Firmware download started. Collapse to hide details

Upgrade scheduled

Device upgrade to IOS XE 17.18.2 is scheduled for Dec 22, 2025 08:17 AM (CST)

Firmware download

5 minutes ago

Firmware download started. Estimated time: up to 20 minutes

Firmware install

Estimated time: Up to 40 minutes

Device will install the network firmware and reboot using the new firmware version.

Firmware verification

Estimated time: Up to 30 minutes

Device will verify that it has a stable connection with the Meraki cloud on the new firmware.

Upgrade complete

See **Documentation on firmware upgrades**

Configuration Source: Device mode firmware upgrades road-mapped

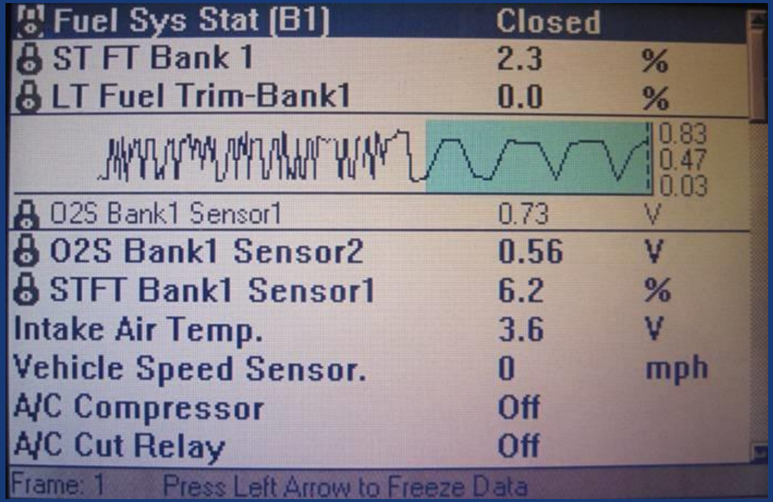
Just the Right Amount of Info at the Right Time

Just the Right Amount of Information at the Right Time

Elegant but too simple

Cisco Meraki

Just Right



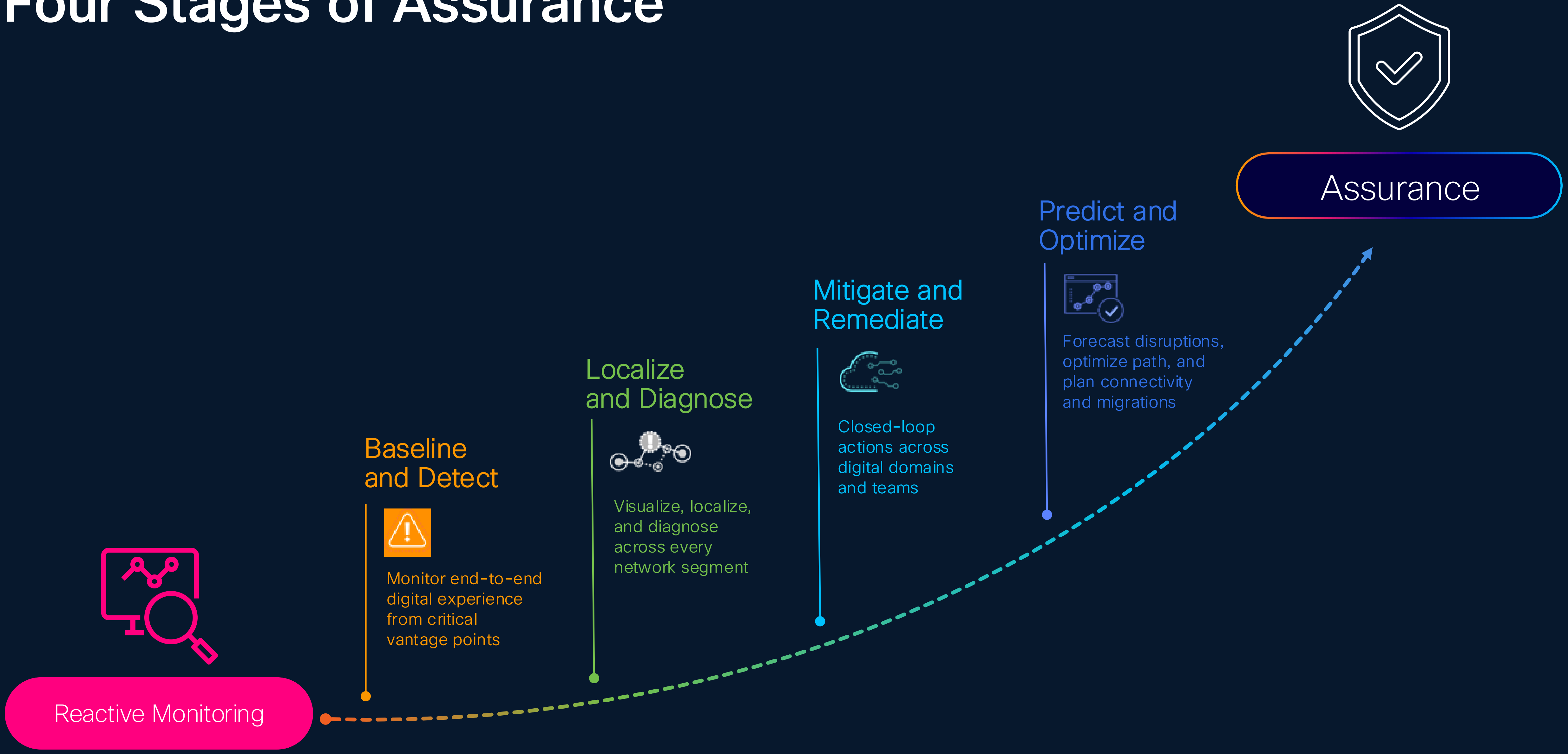
```
Fuel Sys Stat (B1)          Closed
ST FT Bank 1                2.3      %
LT Fuel Trim-Bank1          0.0      %
                                     0.83
                                     0.47
                                     0.03
O2S Bank1 Sensor1           0.73     V
O2S Bank1 Sensor2           0.56     V
STFT Bank1 Sensor1          6.2      %
Intake Air Temp.            3.6      V
Vehicle Speed Sensor.       0        mph
A/C Compressor              Off
A/C Cut Relay               Off
Frame: 1     Press Left Arrow to Freeze Data
```

OBD2 – Data Overload

AI Powered Assurance

Dashboard Intelligence,
Root Cause Analysis,
Intelligent Alerting

Four Stages of Assurance



Reactive Monitoring

Baseline and Detect

Monitor end-to-end digital experience from critical vantage points

Localize and Diagnose

Visualize, localize, and diagnose across every network segment

Mitigate and Remediate

Closed-loop actions across digital domains and teams

Predict and Optimize

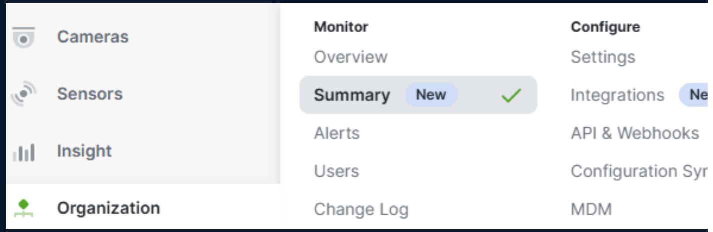
Forecast disruptions, optimize path, and plan connectivity and migrations

Assurance

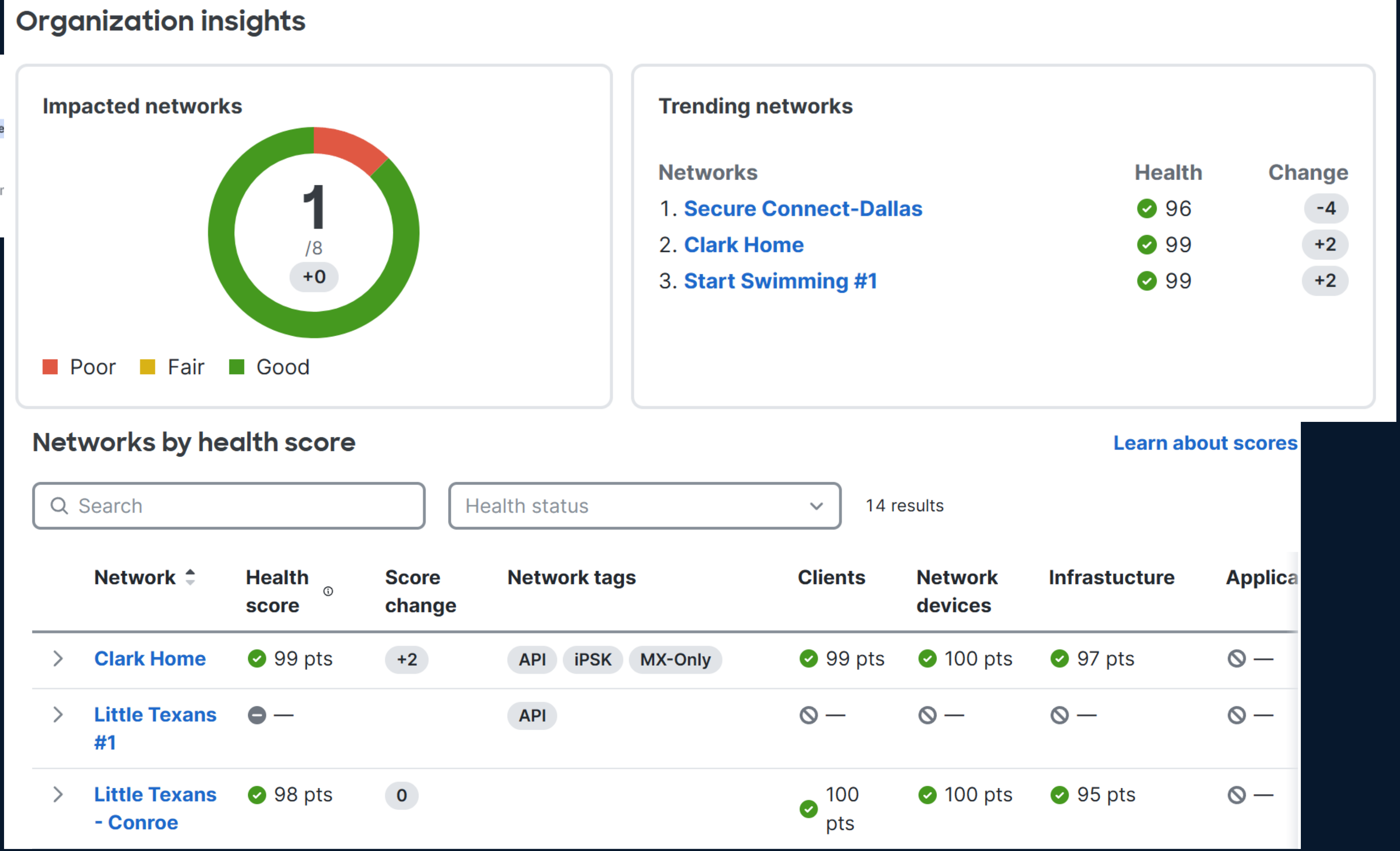
Operationalize and Day N NetOps

Introducing the Assurance Menu

Organization-wide



- Org-Wide summary
- Full stack network health
- Tools haven’t moved
- Health score and trends
- Cat Center integration



Organization insights

Impacted networks

🟥 Poor 🟨 Fair 🟩 Good

Trending networks

Networks	Health	Change
1. Secure Connect-Dallas	✓ 96	-4
2. Clark Home	✓ 99	+2
3. Start Swimming #1	✓ 99	+2

Networks by health score

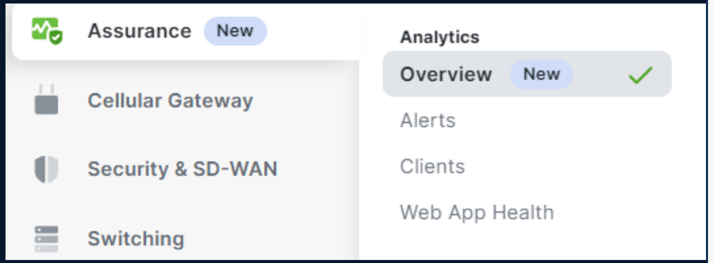
Learn about scores

14 results

Network	Health score	Score change	Network tags	Clients	Network devices	Infrastucture	Applica
Clark Home	✓ 99 pts	+2	API iPSK MX-Only	✓ 99 pts	✓ 100 pts	✓ 97 pts	⊘ —
Little Texans #1	⊖ —		API	⊘ —	⊘ —	⊘ —	⊘ —
Little Texans - Conroe	✓ 98 pts	0		✓ 100 pts	✓ 100 pts	✓ 95 pts	⊘ —

Operationalize and Day N NetOps

Network-specific

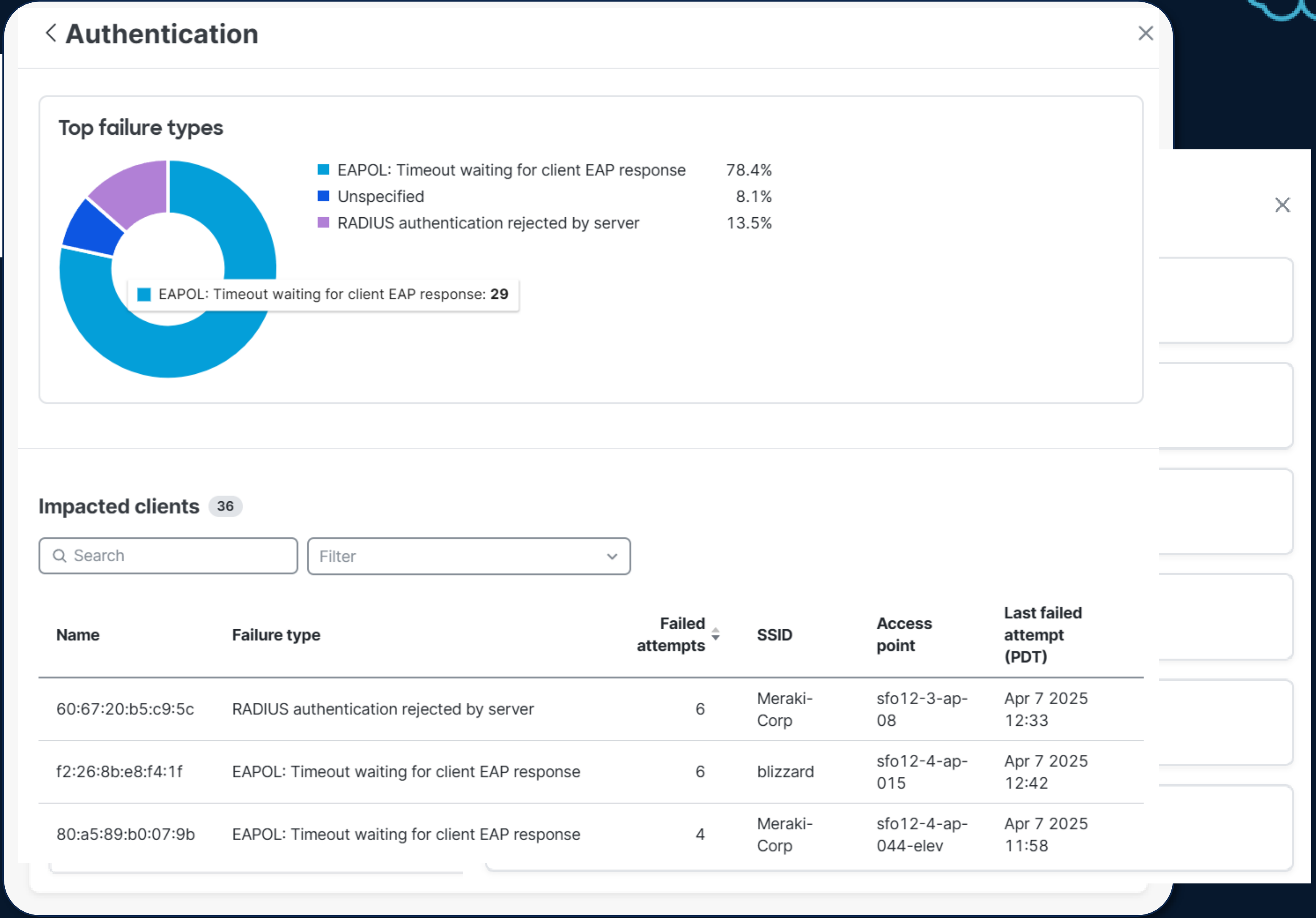


- Assurance New
- Cellular Gateway
- Security & SD-WAN
- Switching

Analytics

- Overview New ✓
- Alerts
- Clients
- Web App Health

- Client, device, apps, and infrastructure health
- Drill-down to detected issues
- See impacted clients
- Direct link to troubleshoot



Authentication

Top failure types

EAPOL: Timeout waiting for client EAP response	78.4%
Unspecified	8.1%
RADIUS authentication rejected by server	13.5%

EAPOL: Timeout waiting for client EAP response: **29**

Impacted clients 36

Search

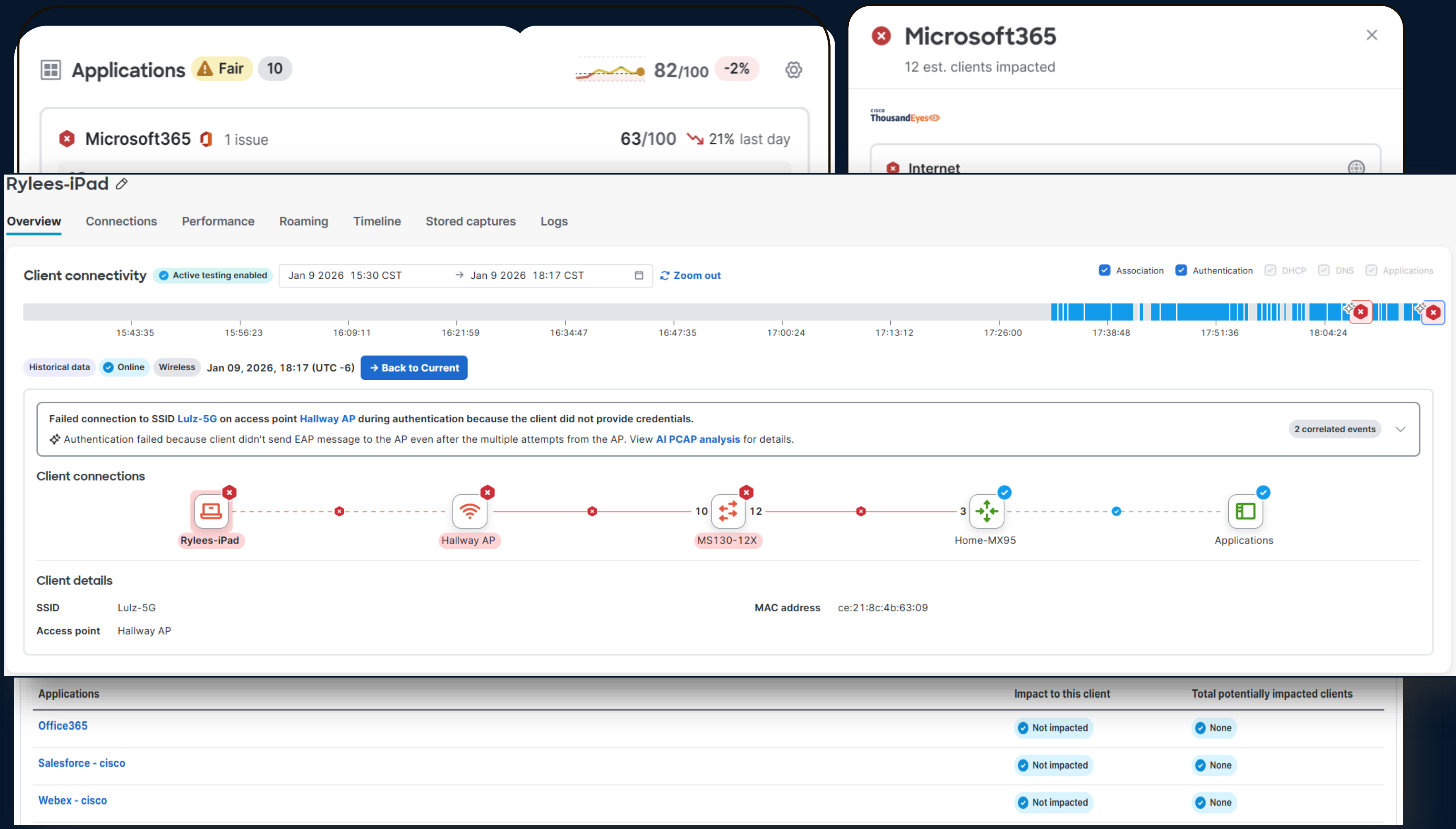
Filter

Name	Failure type	Failed attempts	SSID	Access point	Last failed attempt (PDT)
60:67:20:b5:c9:5c	RADIUS authentication rejected by server	6	Meraki-Corp	sfo12-3-ap-08	Apr 7 2025 12:33
f2:26:8b:e8:f4:1f	EAPOL: Timeout waiting for client EAP response	6	blizzard	sfo12-4-ap-015	Apr 7 2025 12:42
80:a5:89:b0:07:9b	EAPOL: Timeout waiting for client EAP response	4	Meraki-Corp	sfo12-4-ap-044-elev	Apr 7 2025 11:58

Operationalize and Day N NetOps

ThousandEyes Assurance Integration

- Per-application health
- Visibility beyond the WAN
- Differentiate internet and application issues
- Single-client topology
- ‘Time Travel’ to see the topology when an issue occurred



Applications ⚠ Fair 10 — 82/100 -2%

Microsoft365 1 issue — 63/100 ↘ 21% last day

Microsoft365 ✕

12 est. clients impacted

ThousandEyes

Internet

Rylees-iPad

Overview | Connections | Performance | Roaming | Timeline | Stored captures | Logs

Client connectivity ✓ Active testing enabled Jan 9 2026 15:30 CST → Jan 9 2026 18:17 CST Zoom out

☑ Association ☑ Authentication ☐ DHCP ☐ DNS ☐ Applications

Historical data ✓ Online Wireless Jan 09, 2026, 18:17 (UTC -6) → Back to Current

Failed connection to SSID Lulz-5G on access point Hallway AP during authentication because the client did not provide credentials.

Authentication failed because client didn't send EAP message to the AP even after the multiple attempts from the AP. View AI PCAP analysis for details.

2 correlated events

Client connections

Client details

SSID Lulz-5G

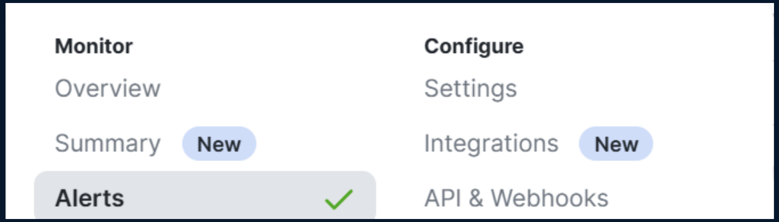
Access point Hallway AP

MAC address ce:21:8c:4b:63:09

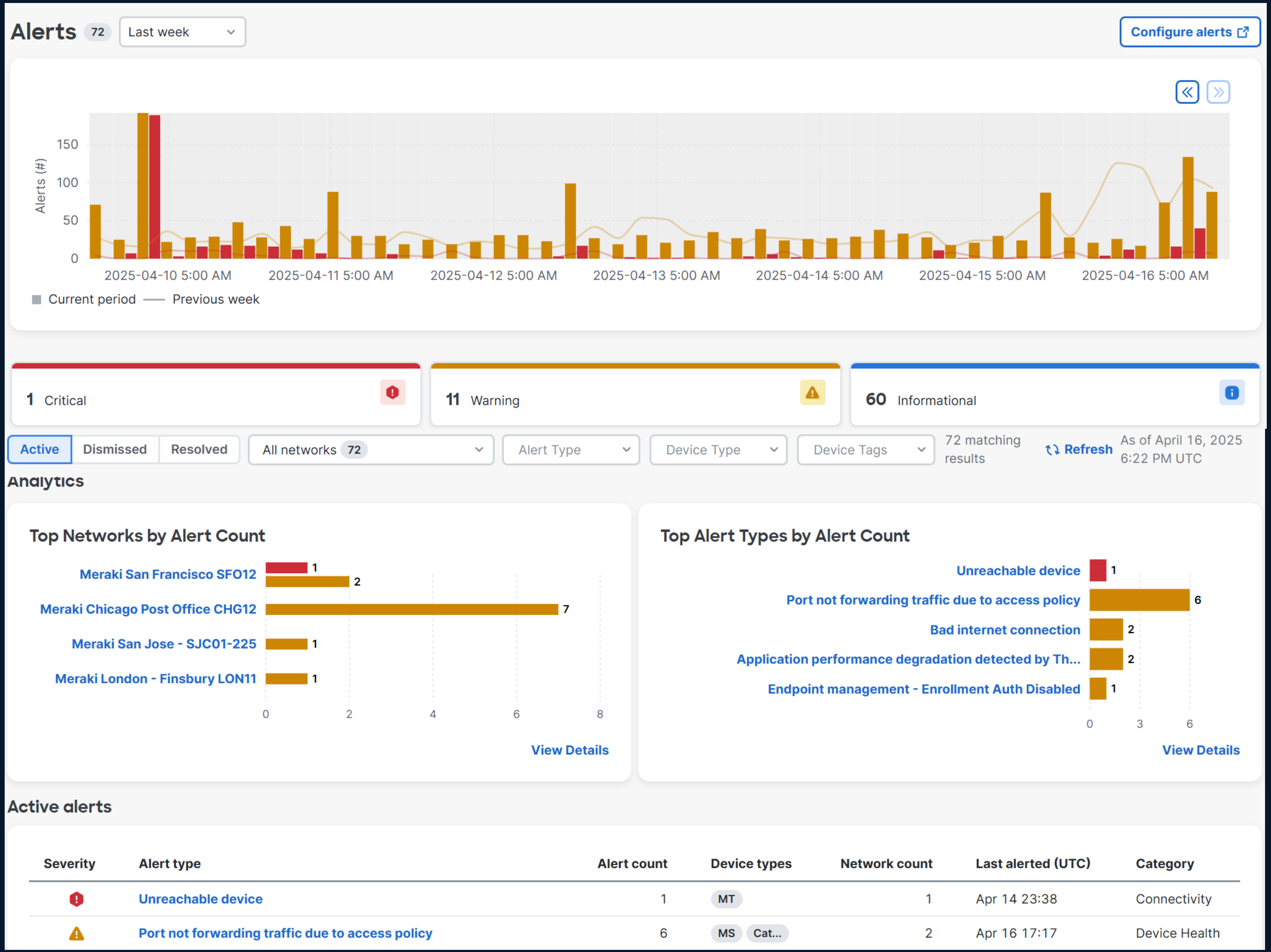
Applications	Impact to this client	Total potentially impacted clients
Office365	✓ Not impacted	✓ None
Salesforce - cisco	✓ Not impacted	✓ None
Webex - cisco	✓ Not impacted	✓ None

Organization Wide Intelligent Alerts

What’s Happening Across Your Network



- Start your day or NOC view
- Alert filtering
- Alert trends
- Dismiss acknowledged alerts
- View recently resolved alerts



Severity	Alert type	Alert count	Device types	Network count	Last alerted (UTC)	Category
●	Unreachable device	1	MT	1	Apr 14 23:38	Connectivity
⚠	Port not forwarding traffic due to access policy	6	MS Cat...	2	Apr 16 17:17	Device Health

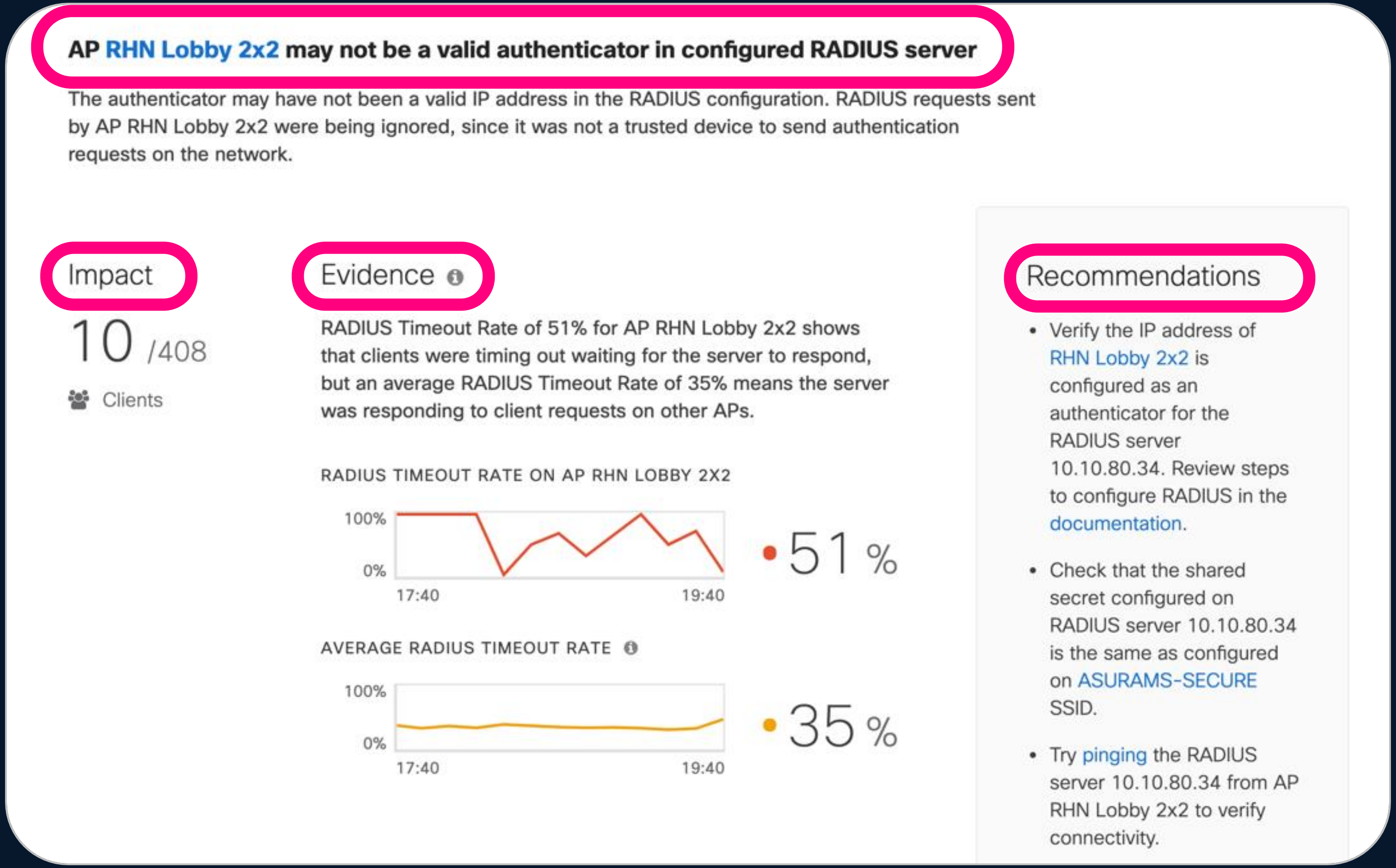
Root Cause Analysis

Impact, Evidence, and Data-Driven Recommendations to solve Complex Problems

Fast, contextual identification of the root cause of issues across the network

Clear recommendations to remediate detected problems

Natural-language description of client connection behavior



AP RHN Lobby 2x2 may not be a valid authenticator in configured RADIUS server

The authenticator may have not been a valid IP address in the RADIUS configuration. RADIUS requests sent by AP RHN Lobby 2x2 were being ignored, since it was not a trusted device to send authentication requests on the network.

Impact

10 /408

Clients

Evidence

RADIUS Timeout Rate of 51% for AP RHN Lobby 2x2 shows that clients were timing out waiting for the server to respond, but an average RADIUS Timeout Rate of 35% means the server was responding to client requests on other APs.

RADIUS TIMEOUT RATE ON AP RHN LOBBY 2X2

AVERAGE RADIUS TIMEOUT RATE

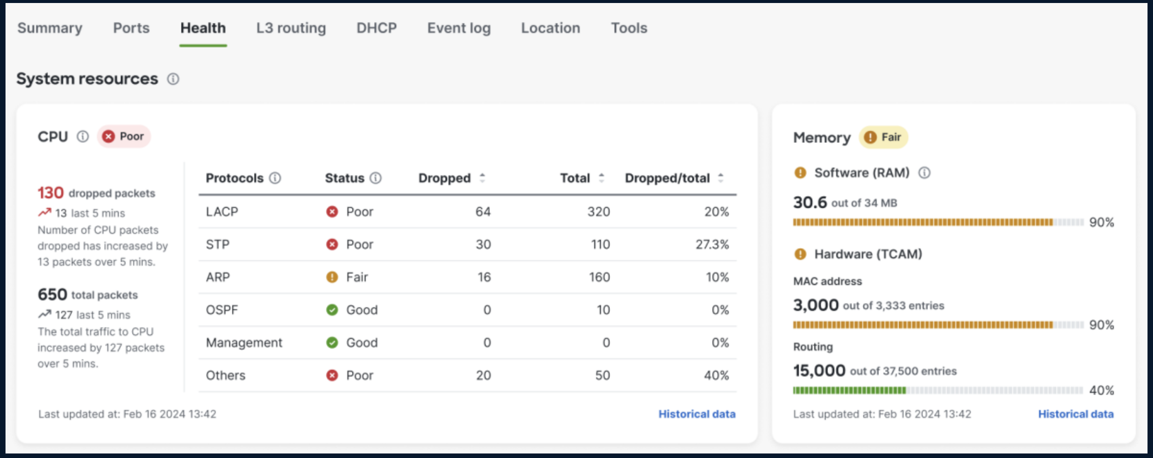
Recommendations

- Verify the IP address of RHN Lobby 2x2 is configured as an authenticator for the RADIUS server 10.10.80.34. Review steps to configure RADIUS in the documentation.
- Check that the shared secret configured on RADIUS server 10.10.80.34 is the same as configured on ASURAMS-SECURE SSID.
- Try pinging the RADIUS server 10.10.80.34 from AP RHN Lobby 2x2 to verify connectivity.

Device Health Tab

Providing Visibility Into Health Metrics for Switching and Wireless

- Track physical statistics
  - Power
  - Temperature
- Resource Metrics
  - CPU/Memory
  - TCAM
  - PoE



System resources

CPU Poor

130 dropped packets
13 last 5 mins
Number of CPU packets dropped has increased by 13 packets over 5 mins.

650 total packets
127 last 5 mins
The total traffic to CPU increased by 127 packets over 5 mins.

Protocols	Status	Dropped	Total	Dropped/total
LACP	Poor	64	320	20%
STP	Poor	30	110	27.3%
ARP	Fair	16	160	10%
OSPF	Good	0	10	0%
Management	Good	0	0	0%
Others	Poor	20	50	40%

Last updated at: Feb 16 2024 13:42 Historical data

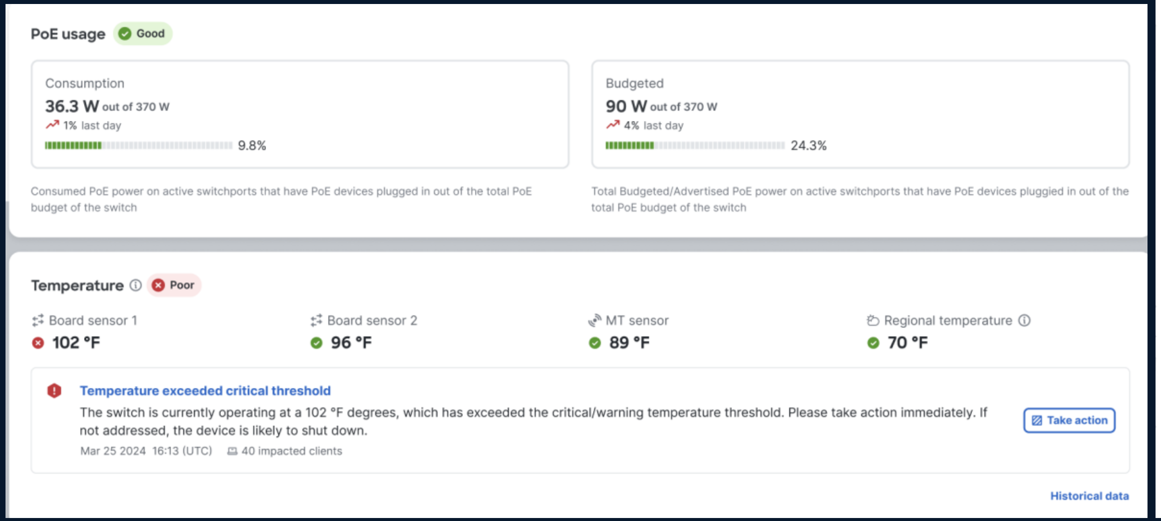
Memory Fair

Software (RAM)
30.6 out of 34 MB
90%

Hardware (TCAM)
MAC address
3,000 out of 3,333 entries
90%

Routing
15,000 out of 37,500 entries
40%

Last updated at: Feb 16 2024 13:42 Historical data


PoE usage Good

Consumption
36.3 W out of 370 W
1% last day
9.8%

Budgeted
90 W out of 370 W
4% last day
24.3%

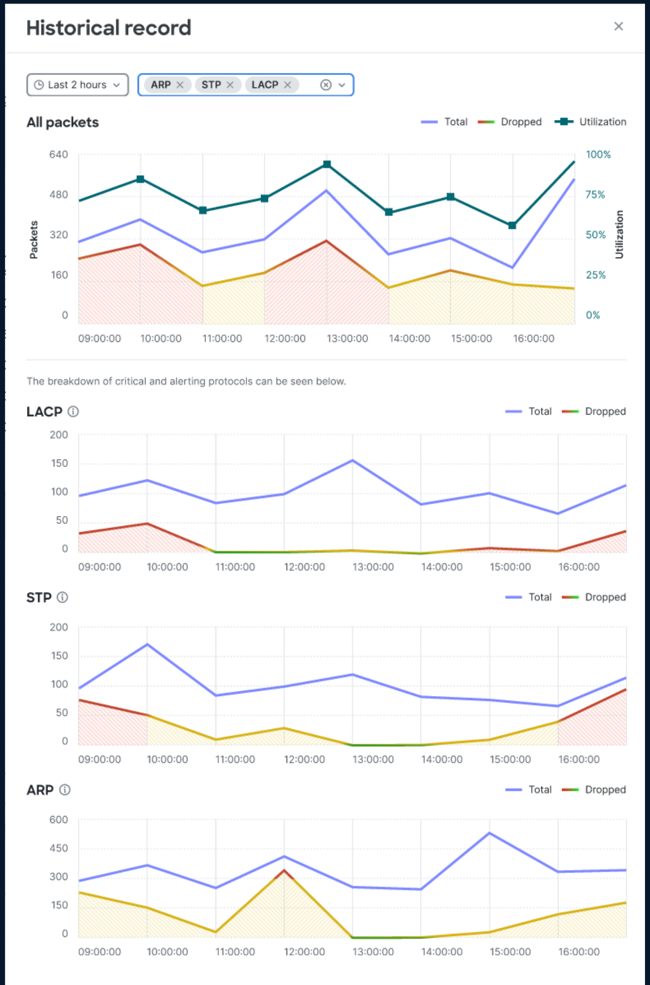
Consumed PoE power on active switchports that have PoE devices plugged in out of the total PoE budget of the switch

Total Budgeted/Advertised PoE power on active switchports that have PoE devices plugied in out of the total PoE budget of the switch

Temperature Poor

Board sensor 1	Board sensor 2	MT sensor	Regional temperature
102 °F	96 °F	89 °F	70 °F

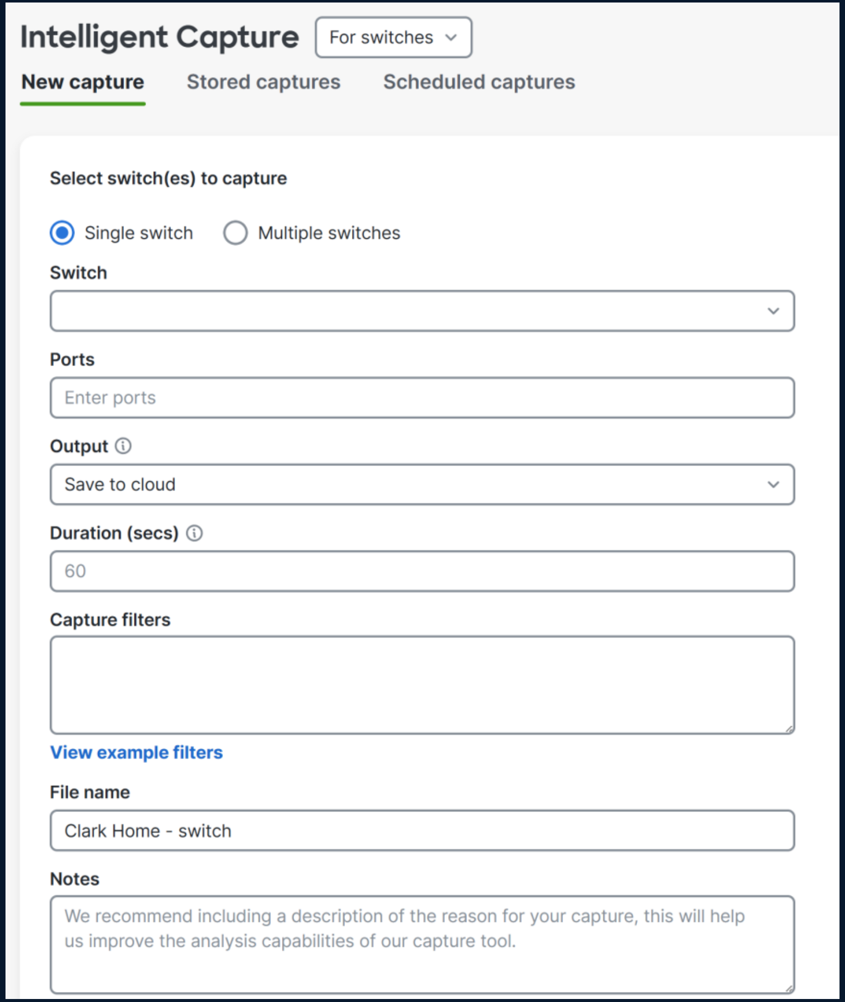
Temperature exceeded critical threshold
The switch is currently operating at a 102 °F degrees, which has exceeded the critical/warning temperature threshold. Please take action immediately. If not addressed, the device is likely to shut down.
Mar 25 2024 16:13 (UTC) 40 impacted clients


Historical record

The breakdown of critical and alerting protocols can be seen below.

Intelligent Capture

Streamline Troubleshooting - Schedule, Store, and Proactive Captures



Intelligent Capture

Select switch(es) to capture

● Single switch ○ Multiple switches

Switch

Ports: Enter ports

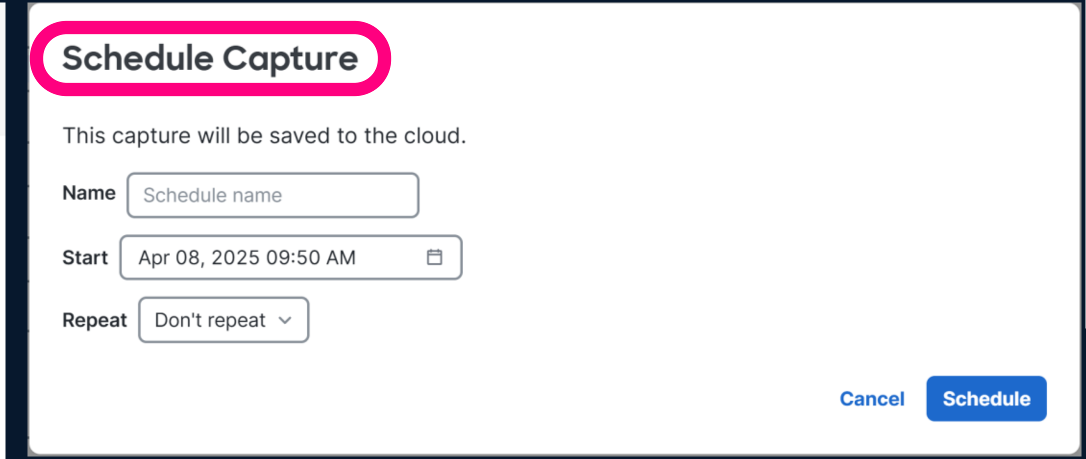
Output: Save to cloud

Duration (secs): 60

Capture filters

File name: Clark Home - switch

Notes: We recommend including a description of the reason for your capture, this will help us improve the analysis capabilities of our capture tool.



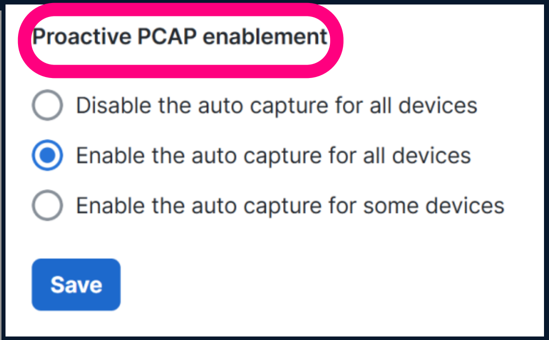
Schedule Capture

This capture will be saved to the cloud.

Name: Schedule name

Start: Apr 08, 2025 09:50 AM

Repeat: Don't repeat

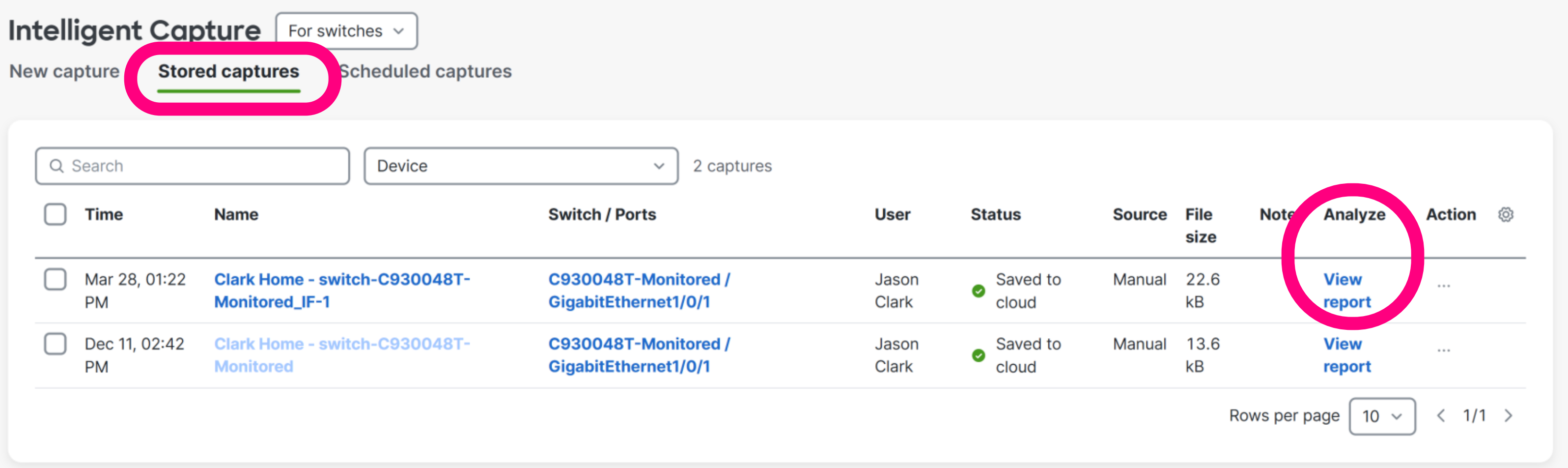


Proactive PCAP enablement

○ Disable the auto capture for all devices

● Enable the auto capture for all devices

○ Enable the auto capture for some devices



Intelligent Capture

2 captures

☐	Time	Name	Switch / Ports	User	Status	Source	File size	Note	Analyze	Action
☐	Mar 28, 01:22 PM	Clark Home - switch-C930048T-Monitored_IF-1	C930048T-Monitored / GigabitEthernet1/0/1	Jason Clark	✓ Saved to cloud	Manual	22.6 kB		View report	...
☐	Dec 11, 02:42 PM	Clark Home - switch-C930048T-Monitored	C930048T-Monitored / GigabitEthernet1/0/1	Jason Clark	✓ Saved to cloud	Manual	13.6 kB		View report	...

Rows per page 10 1/1

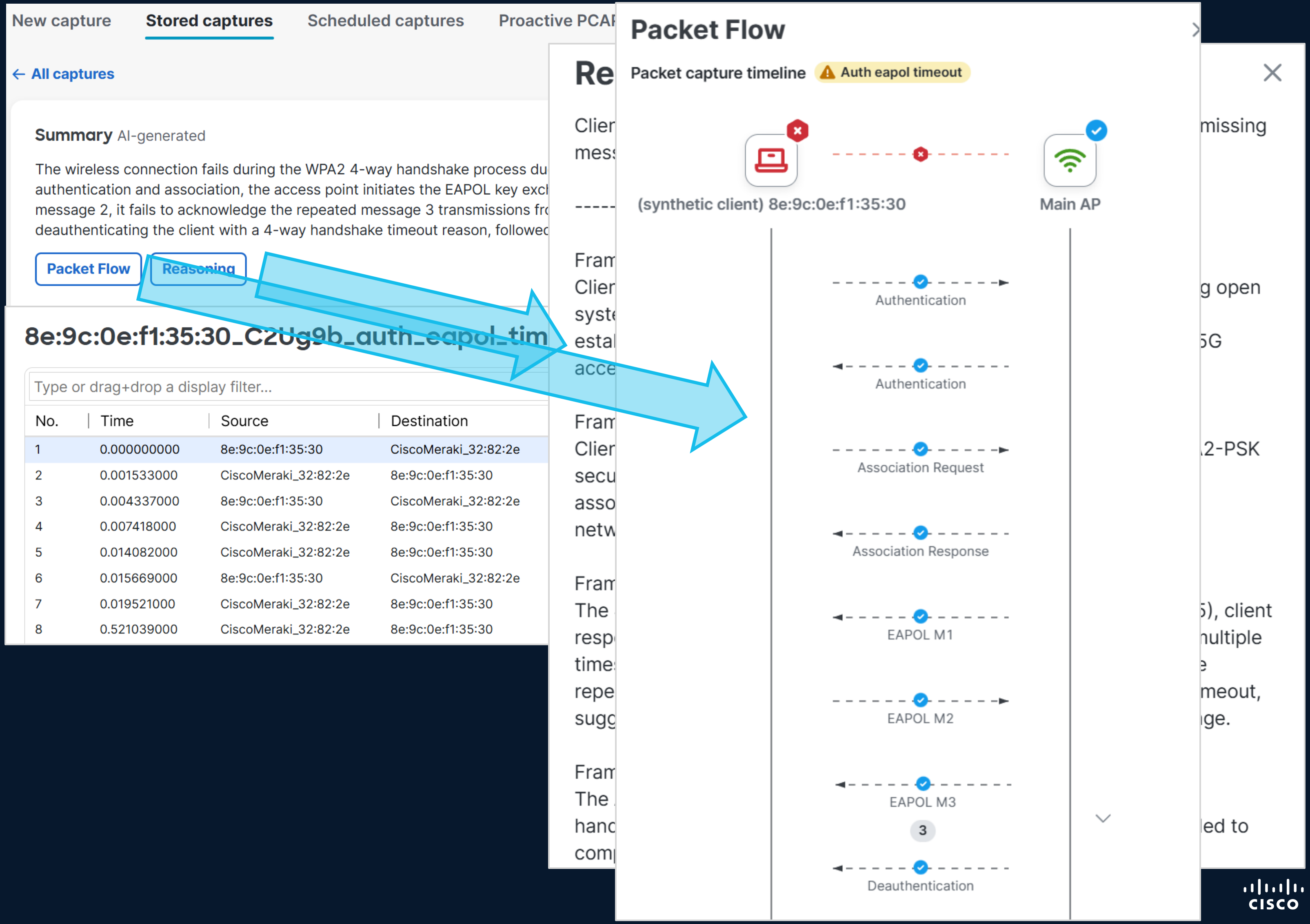
Intelligent Capture Analysis

Quick and Simple Identification of Issues at a Packet Level

Quickly detect common issues in DHCP, ARP, and ICMP packets

Analyze uploaded, scheduled, or ‘proactive’ captures

Review findings and evidence



Summary AI-generated

The wireless connection fails during the WPA2 4-way handshake process du
authentication and association, the access point initiates the EAPOL key excl
message 2, it fails to acknowledge the repeated message 3 transmissions fro
deauthenticating the client with a 4-way handshake timeout reason, followed

8e:9c:0e:f1:35:30_C2Ug9b_auth_eapol_tim

Type or drag+drop a display filter...

No.	Time	Source	Destination
1	0.000000000	8e:9c:0e:f1:35:30	CiscoMeraki_32:82:2e
2	0.001533000	CiscoMeraki_32:82:2e	8e:9c:0e:f1:35:30
3	0.004337000	8e:9c:0e:f1:35:30	CiscoMeraki_32:82:2e
4	0.007418000	CiscoMeraki_32:82:2e	8e:9c:0e:f1:35:30
5	0.014082000	CiscoMeraki_32:82:2e	8e:9c:0e:f1:35:30
6	0.015669000	8e:9c:0e:f1:35:30	CiscoMeraki_32:82:2e
7	0.019521000	CiscoMeraki_32:82:2e	8e:9c:0e:f1:35:30
8	0.521039000	CiscoMeraki_32:82:2e	8e:9c:0e:f1:35:30

Re

Clier
mess

Fram
Clier
syste
estal
acce

Fram
Clier
secu
asso
netw

Fram
The
resp
time
repe
sugg

Fram
The
hand
comp

missing

g open

5G

2-PSK

5), client
multiple
e
meout,
ge.

led to

Agentic Ops

AI Assistant for Networking

GA

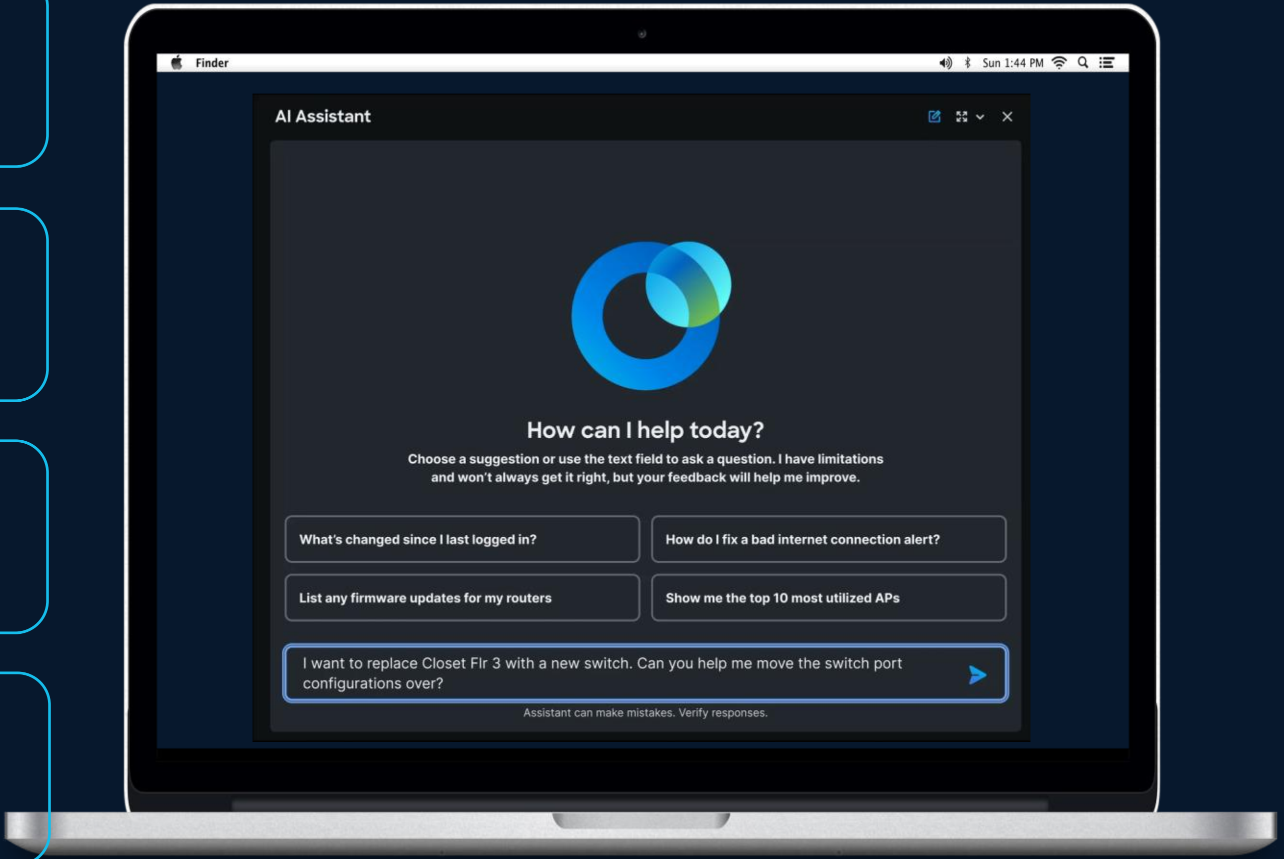
Accelerate Network Management through Gen-AI Conversational Interface

Client troubleshooting using unique partnership with Apple, Intel, Samsung

AI-driven RCA, end-to-end network correlation orchestrated through conversational interface

Conduct network change management by conversation

AI-generated summarization of Cisco document libraries and best practices



How can I help today?

Choose a suggestion or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

What's changed since I last logged in?

How do I fix a bad internet connection alert?

List any firmware updates for my routers

Show me the top 10 most utilized APs

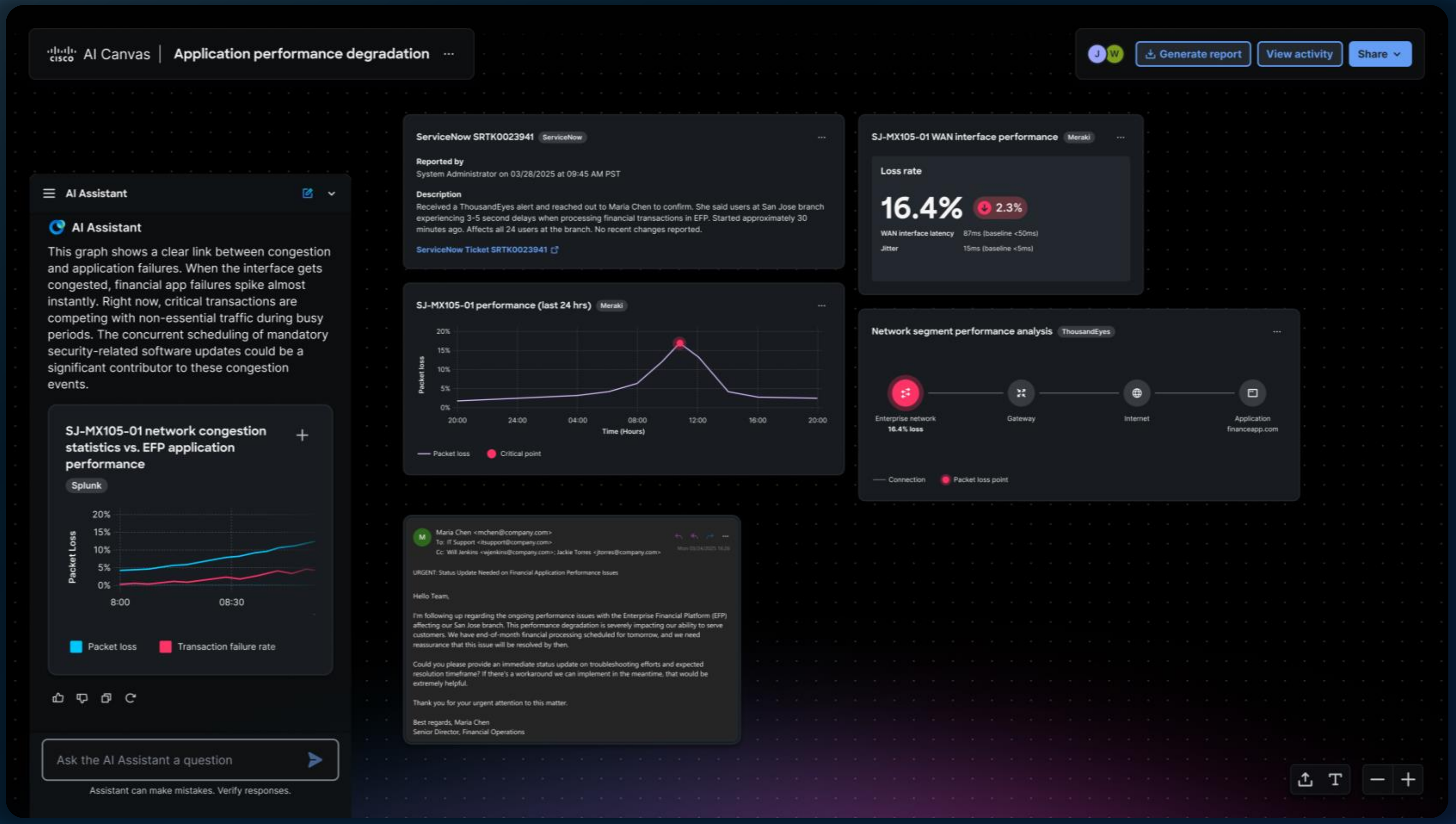
I want to replace Closet Flr 3 with a new switch. Can you help me move the switch port configurations over?

Assistant can make mistakes. Verify responses.

ALPHA

AI Canvas

- Troubleshooting and execution across multiple domains
- One shared workspace for NetOps, SecOps, IT, and execs
- Built on the foundation of the Deep Network Model
- Interface to ask and explore in natural language
- Guides you through diagnostics, decisions, and action inside the canvas



AI Assistant

This graph shows a clear link between congestion and application failures. When the interface gets congested, financial app failures spike almost instantly. Right now, critical transactions are competing with non-essential traffic during busy periods. The concurrent scheduling of mandatory security-related software updates could be a significant contributor to these congestion events.

SJ-MX105-01 network congestion statistics vs. EFP application performance

🟦 Packet loss 🟥 Transaction failure rate

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

ServiceNow SRTK0023941

Reported by
System Administrator on 03/28/2025 at 09:45 AM PST

Description
Received a ThousandEyes alert and reached out to Maria Chen to confirm. She said users at San Jose branch experiencing 3-5 second delays when processing financial transactions in EFP. Started approximately 30 minutes ago. Affects all 24 users at the branch. No recent changes reported.

ServiceNow Ticket SRTK0023941

SJ-MX105-01 WAN interface performance

Loss rate
16.4% ↓ 2.3%

WAN interface latency	87ms (baseline <50ms)
Jitter	15ms (baseline <5ms)

SJ-MX105-01 performance (last 24 hrs)

— Packet loss ● Critical point

Network segment performance analysis

Maria Chen <mchen@company.com>
To: IT Support <itsupport@company.com>
Cc: Will Jenkins <wjenkins@company.com>; Jackie Torres <jtorres@company.com>

URGENT: Status Update Needed on Financial Application Performance Issues

Hello Team,

I'm following up regarding the ongoing performance issues with the Enterprise Financial Platform (EFP) affecting our San Jose branch. This performance degradation is severely impacting our ability to serve customers. We have end-of-month financial processing scheduled for tomorrow, and we need reassurance that this issue will be resolved by then.

Could you please provide an immediate status update on troubleshooting efforts and expected resolution timeframe? If there's a workaround we can implement in the meantime, that would be extremely helpful.

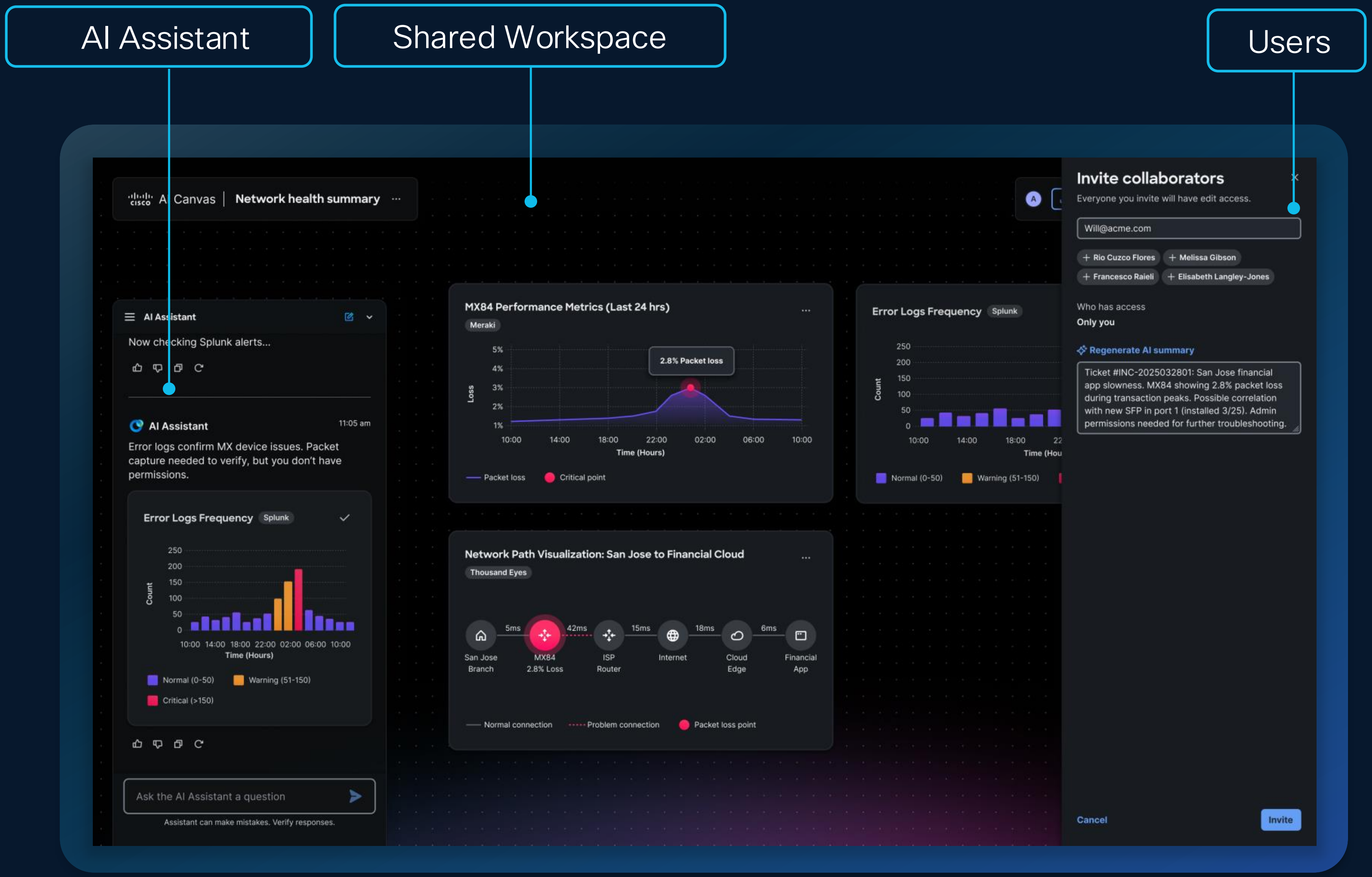
Thank you for your urgent attention to this matter.

Best regards, Maria Chen
Senior Director, Financial Operations

AI Assistant embedded in AI Canvas

Introducing AI Canvas

- Single canvas for cross domain troubleshooting
- Generative UI with reasoning built-in
- Keeps NetOps, SecOps, IT and execs on the same page



AI Assistant

Shared Workspace

Users

AI Canvas | Network health summary

AI Assistant

Now checking Splunk alerts...

AI Assistant 11:05 am

Error logs confirm MX device issues. Packet capture needed to verify, but you don't have permissions.

Ask the AI Assistant a question

Assistant can make mistakes. Verify responses.

Invite collaborators

Everyone you invite will have edit access.

Will@acme.com

+ Rio Cuzco Flores + Melissa Gibson + Francesco Raieli + Elisabeth Langley-Jones

Who has access
Only you

Regenerate AI summary

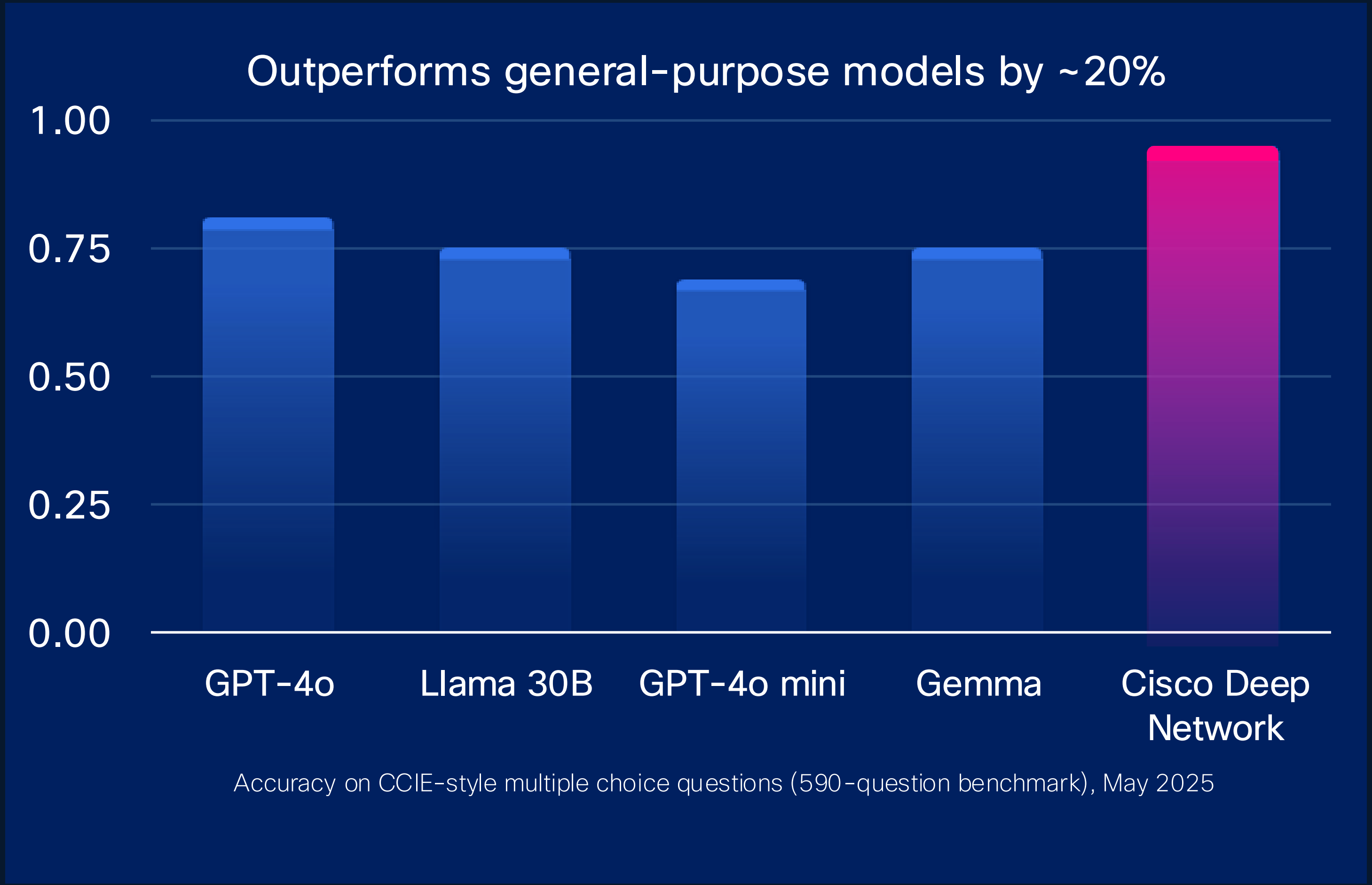
Ticket #INC-2025032801: San Jose financial app slowness. MX84 showing 2.8% packet loss during transaction peaks. Possible correlation with new SFP in port 1 (installed 3/25). Admin permissions needed for further troubleshooting.

Cancel Invite

Deep Network Model

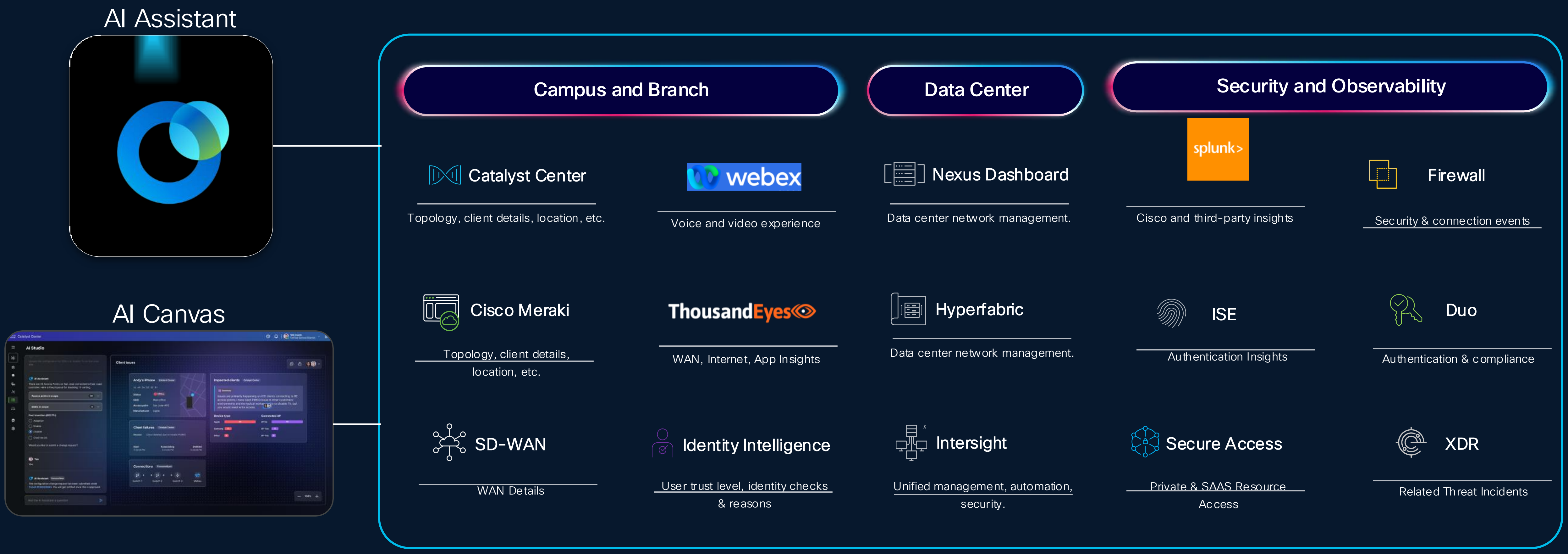
Purpose-built for networking,
Expert accuracy

- More precise reasoning for troubleshooting, configuration, and automation
- Fine-tuned on 40+ years of expertise and expert-vetted for accuracy
- Evolves with live telemetry and real-world Cisco TAC and CX insights



Accuracy on CCIE-style multiple choice questions (590-question benchmark), May 2025

AgenticOps with Cross-Product Skills and Unified Data



AI Assistant

AI Canvas

Campus and Branch

Catalyst Center
Topology, client details, location, etc.

webex
Voice and video experience

Cisco Meraki
Topology, client details, location, etc.

ThousandEyes
WAN, Internet, App Insights

SD-WAN
WAN Details

Identity Intelligence
User trust level, identity checks & reasons

Data Center

Nexus Dashboard
Data center network management.

Hyperfabric
Data center network management.

Intersight
Unified management, automation, security.

Security and Observability

splunk>
Cisco and third-party insights

Firewall
Security & connection events

ISE
Authentication Insights

Duo
Authentication & compliance

Secure Access
Private & SAAS Resource Access

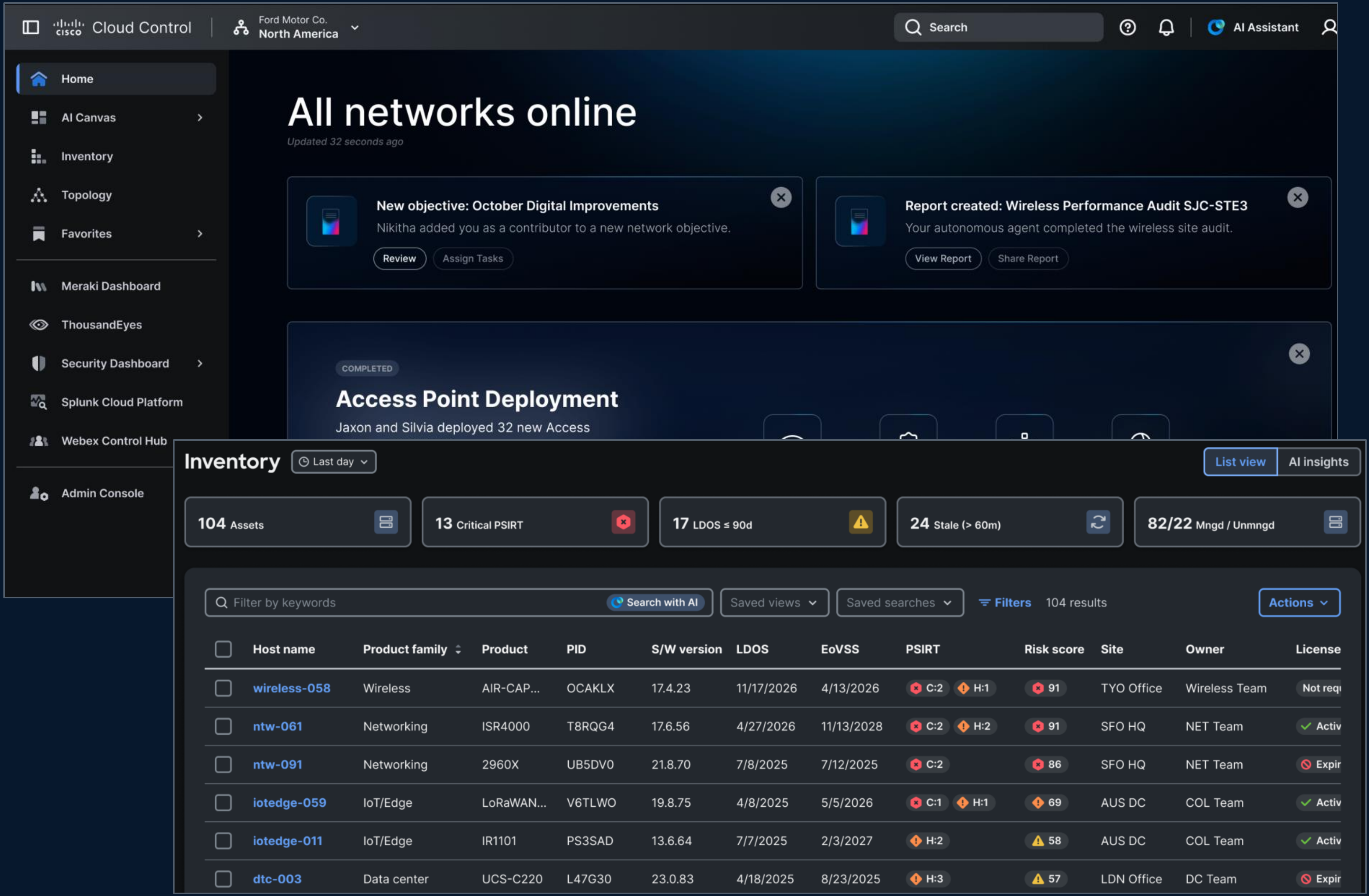
XDR
Related Threat Incidents

Introducing – Cisco Cloud Control

Alpha

The Cisco Cloud Platform

- View inventory and topology across domains
- Integrate Cisco platforms such as Meraki, Canvas, Thousand Eyes, Webex
- Built with Cisco AI intelligence and insights



All networks online

Updated 32 seconds ago

New objective: October Digital Improvements

Nikitha added you as a contributor to a new network objective.

Report created: Wireless Performance Audit SJC-STE3

Your autonomous agent completed the wireless site audit.

COMPLETED

Access Point Deployment

Jaxon and Silvia deployed 32 new Access

Inventory

104 Assets | 13 Critical PSIRT | 17 LDOS ≤ 90d | 24 Stale (> 60m) | 82/22 Mngd / Unmngd

104 results

□	Host name	Product family	Product	PID	S/W version	LDOS	EoVSS	PSIRT	Risk score	Site	Owner	License
□	wireless-058	Wireless	AIR-CAP...	OCAKLX	17.4.23	11/17/2026	4/13/2026	C:2 H:1	91	TYO Office	Wireless Team	Not requ
□	ntw-061	Networking	ISR4000	T8RQG4	17.6.56	4/27/2026	11/13/2028	C:2 H:2	91	SFO HQ	NET Team	✓ Activ
□	ntw-091	Networking	2960X	UB5DV0	21.8.70	7/8/2025	7/12/2025	C:2	86	SFO HQ	NET Team	Expir
□	iotedge-059	IoT/Edge	LoRaWAN...	V6TLWO	19.8.75	4/8/2025	5/5/2026	C:1 H:1	69	AUS DC	COL Team	✓ Activ
□	iotedge-011	IoT/Edge	IR1101	PS3SAD	13.6.64	7/7/2025	2/3/2027	H:2	⚠ 58	AUS DC	COL Team	✓ Activ
□	dtc-003	Data center	UCS-C220	L47G30	23.0.83	4/18/2025	8/23/2025	H:3	⚠ 57	LDN Office	DC Team	Expir

Summary

Summary

- Operationalize using a platform approach
- Lean in and trust the dashboard
- Change troubleshooting from reactive to proactive
- Leverage AI Powered Assurance
- Embrace PCAP (it makes you a better network engineer)

CISCO Connect

Thank you

CISCO