

Meraki Cloud Networking

For the CLI wired brain

Simerjit Singh
Solutions Engineer –Partners

cisco Live !

Session ID: BRKTRS-2008

Cisco Webex App

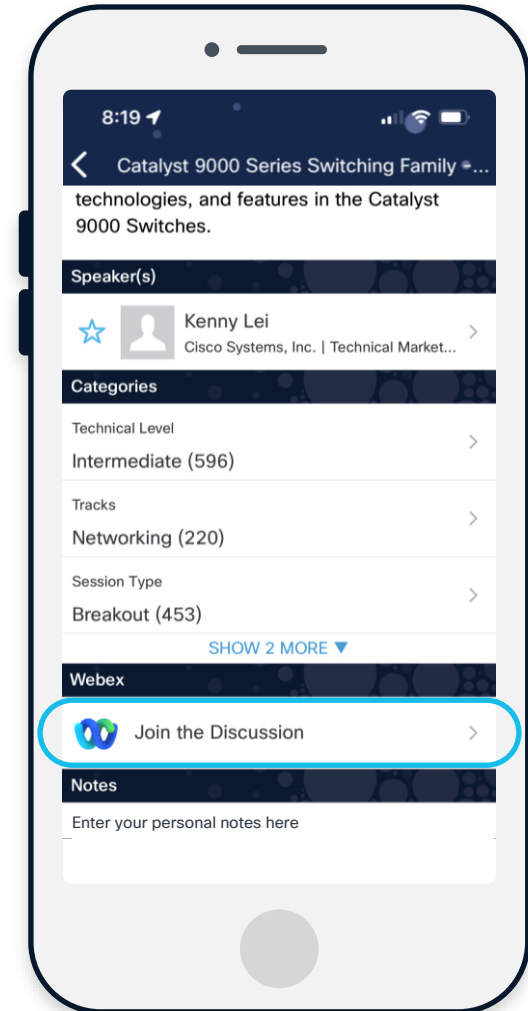
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 14, 2025



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKTRS-2008>

Agenda

- 01 Intro and Unification
- 02 Troubleshooting methodology
- 03 Dashboard connectivity
- 04 Troubleshooting tools
- 05 Extra tools
- 06 Assurance
- 07 Summary

Introduction

Who am I?

simesing@cisco.com

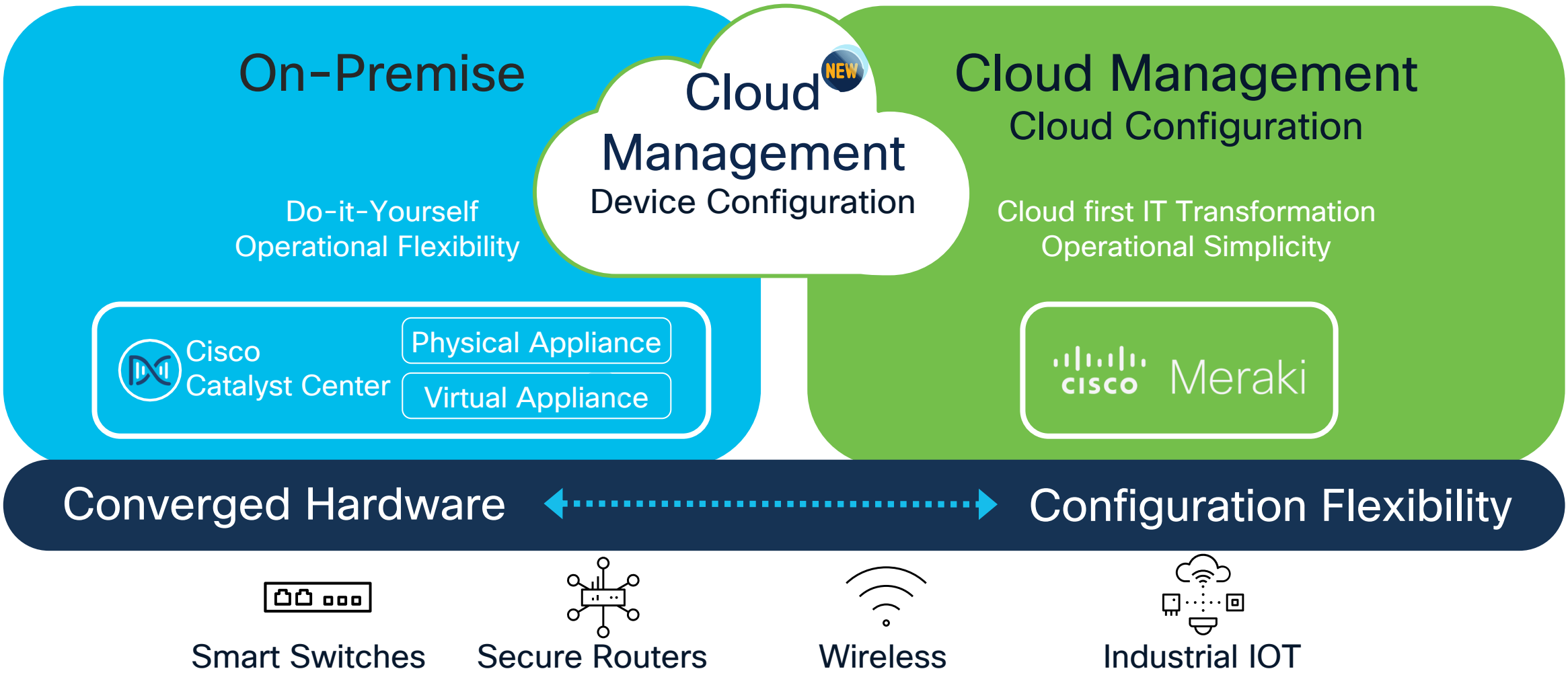


- Married and Father of two !
- Delhi born and raised.
- Started my own PC repairing Company
- Joined Cisco in 2007 (18 Years)
- Worked in India, Singapore and Australia (8+ years)
- Customer Network Architect for 20 years
- **Meraki Pitch Winner (APJ)**
- **Co-Author of Meraki Book**
- **CCIE**

Cisco Unification

Your IT operating model, your way

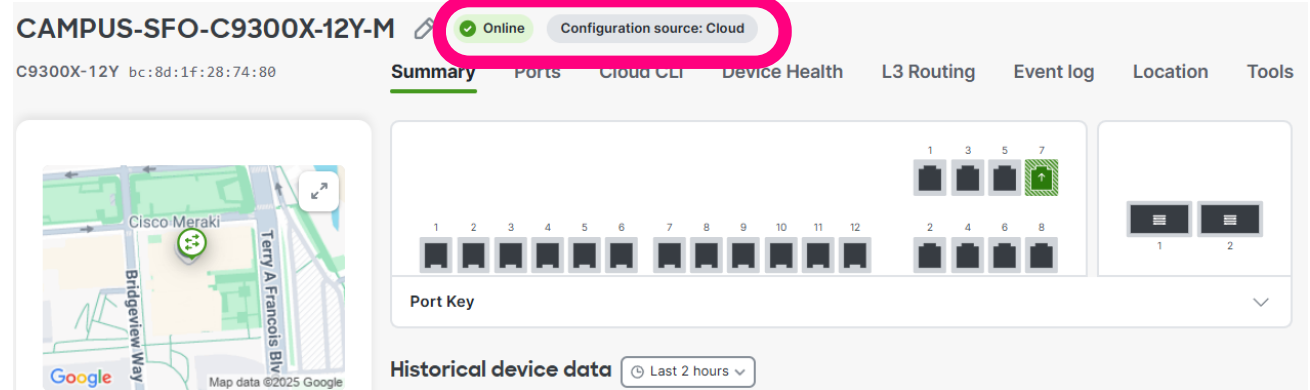
Visibility, flexibility, and simplicity



Cloud management, with cloud configuration

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 – Read Only
- Cloud-based configuration, ZTP, and firmware management



Terminal

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

Close Terminal

Detach

This terminal allows limited access to read-only 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

Introducing: Cloud management, with device configuration

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

Summary Ports Cloud CLI Event log Location Tools Config history



Port Key

Historical device data Last 2 hours

CLI terminal

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

Close terminal

Detach terminal

☐ Capture the session to output a text file

```
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

```
COM3 - PuTTY
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

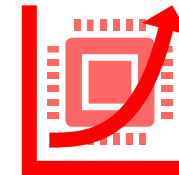
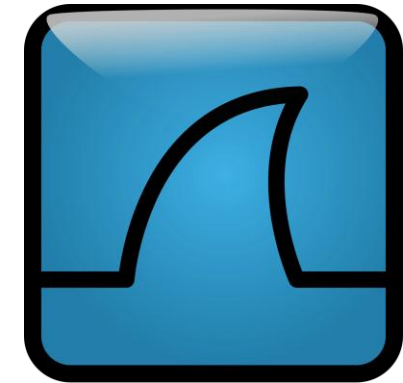
Number of channel-groups in use: 1
Number of aggregators:          1

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

Show Commands /
Live Tools / Show Log

```
4, input feature
*Mar 3 22:35:56.941: UDP src=61111, dst=61111, MCI Check(118), rtype 0, fo
rus FALSE, sendself FALSE, mtu 0, twdchk 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(118), rtype 0, fo
rus FALSE, sendself FALSE, mtu 0, twdchk FALSE
```

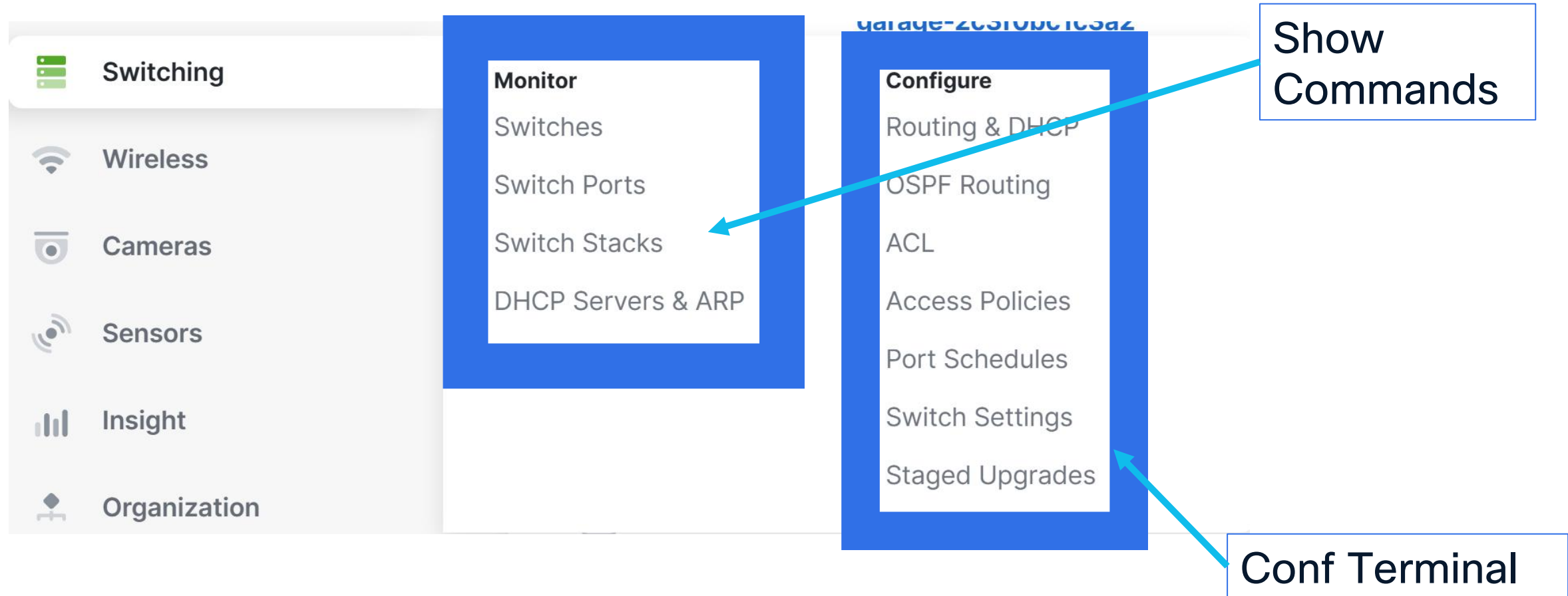
Debug
Commands



Packet Capture

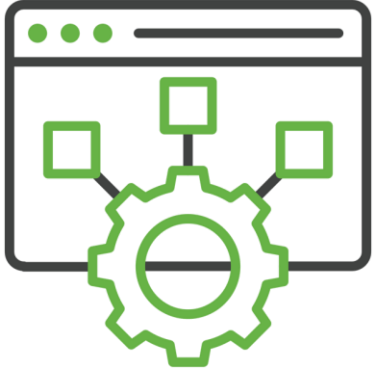
Meraki Monitor / Configure

Like IOS-XE Show Commands and Configure Terminal



Cloud Management Troubleshooting

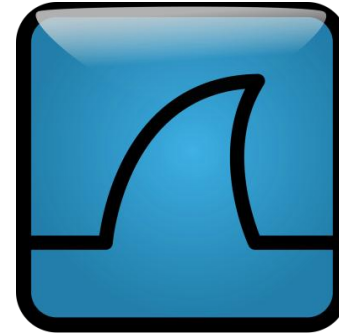
A difference in philosophy



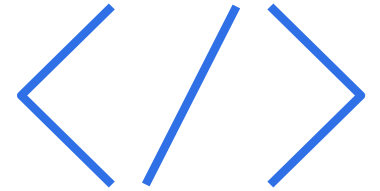
Dashboard GUI
Live Tools
Event Logs



Meraki Assurance
RCA / Intelligence
/ Alerts



Intelligent PCAPs
and Analysis



Meraki Platform
APIs

Dashboard 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

Introducing the AI Assistant

Monitoring

Troubleshooting

Automated Configuration

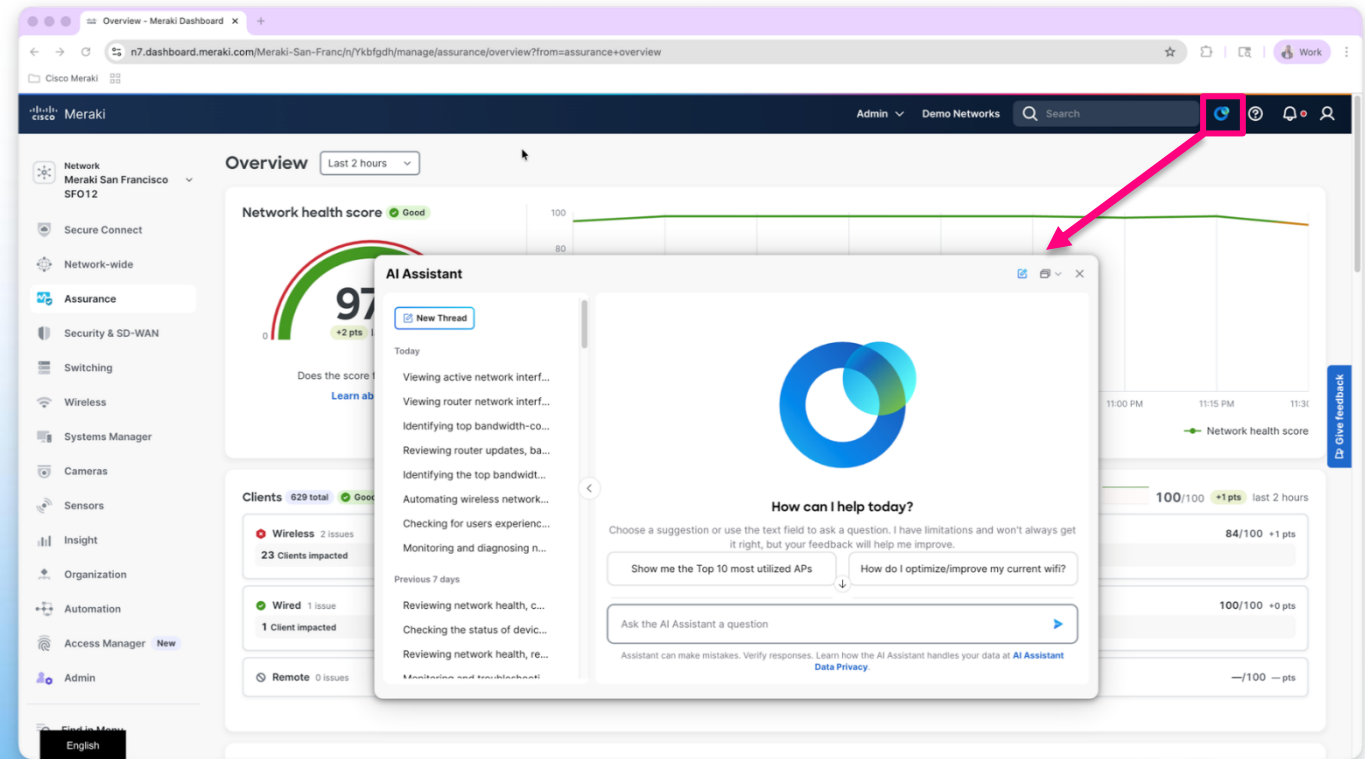


What is the AI Assistant?

The Cisco® AI Assistant is a Generative AI solution designed for simplified, expedited network operations:

- Users make requests with natural language
- AI Assistant interprets request, determines relevant data, and gathers it
- Data is fed to the large language model (LLM) engine for response generation
- Natural language response and relevant tables or graphs are generated

The AI Assistant is launched via dashboard (see below):



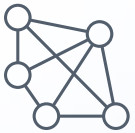
Accelerate network management through Gen-AI conversational interface



Client troubleshooting using unique partnership with Apple, Intel, Samsung



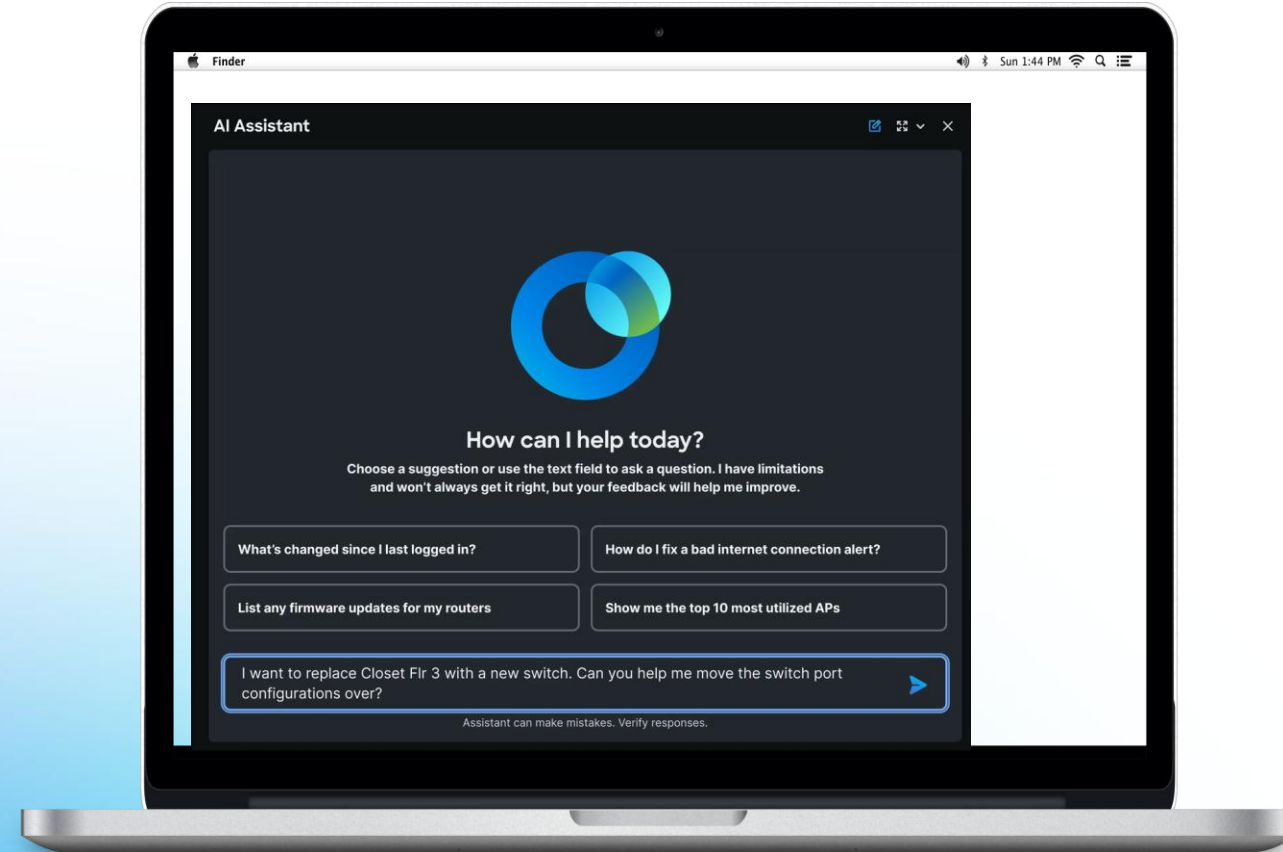
AI-driven RCA, end-to-end network correlation orchestrated through conversational interface



Conduct network change management by conversation

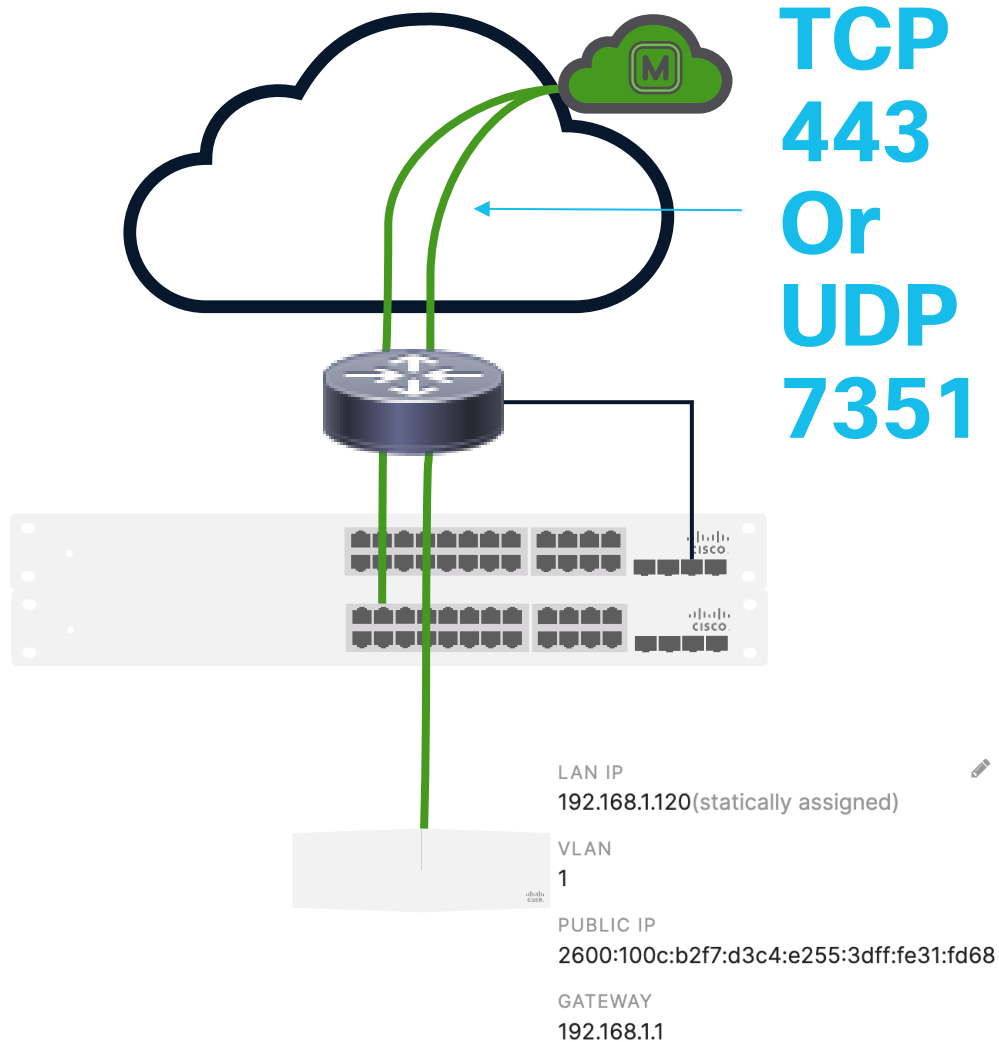


AI-generated summarization of Cisco document libraries and best practices



Dashboard Connectivity

Meraki Management Tunnels



- One tunnel per Meraki Device
- Only exception is stacked C9000+/MS390 switches (1 tunnel per stack)
- Legacy UDP 7351
- Modern TCP 443 FIPS-2 compliant
- SSL Decrypt must be disabled for *.meraki.com
- IPv6 has priority

Resilient connectivity to the cloud



Uplink Auto Config (UAC)

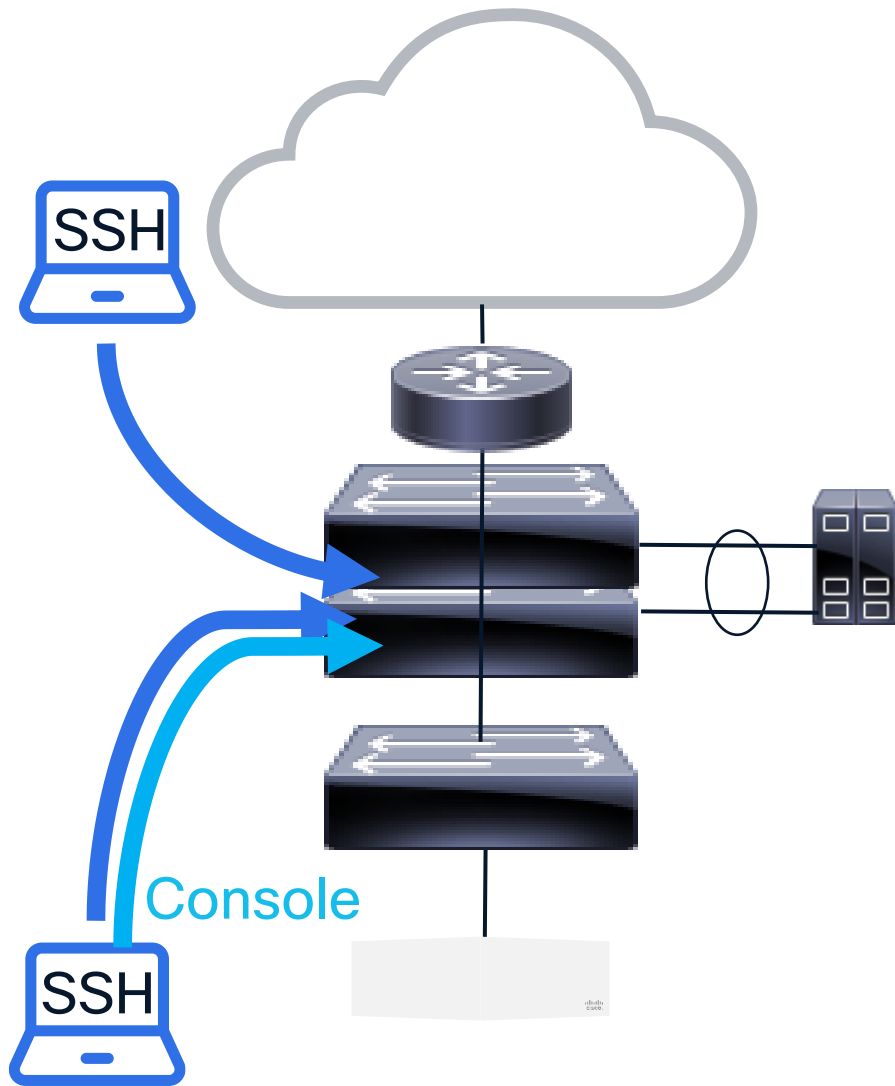
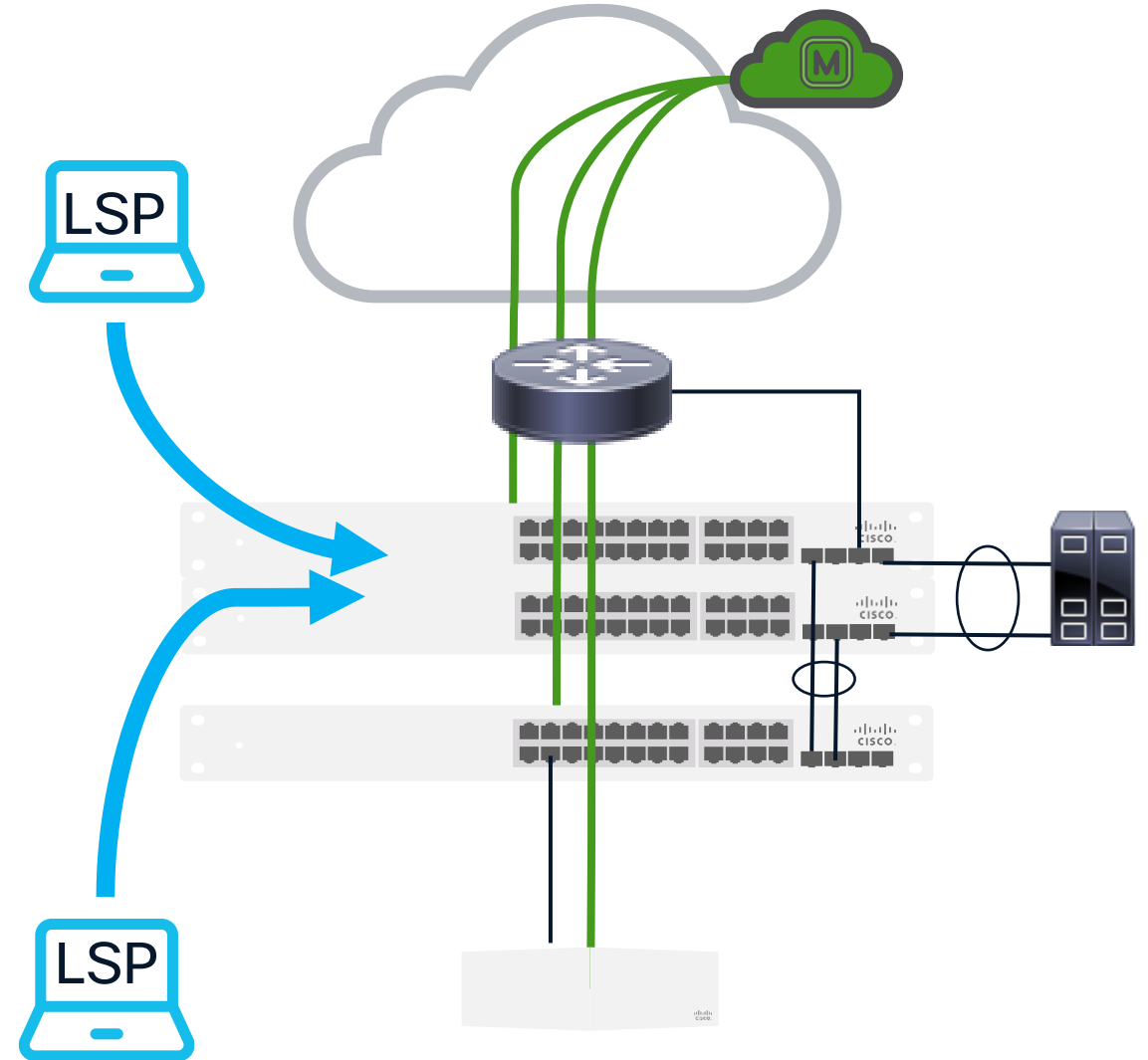
- Automated discovery for dashboard connectivity
- Automated failover / path discovery
- Tunable for primary interface
- Creates stack-ranked interface list



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

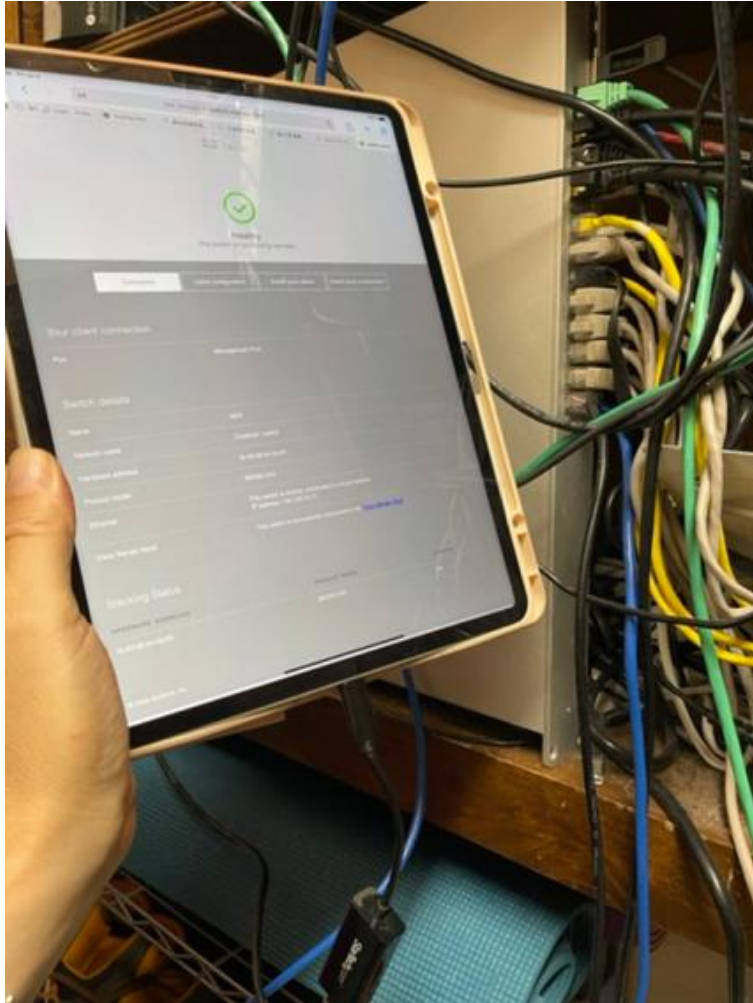
Changes via Traditional and Cloud Managed



LSP = Local Status Page

Break Glass Option

Local Status Page



Verify or restore cloud connectivity:

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

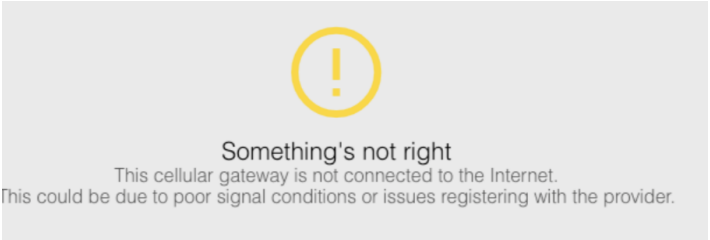
Methods to access:

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

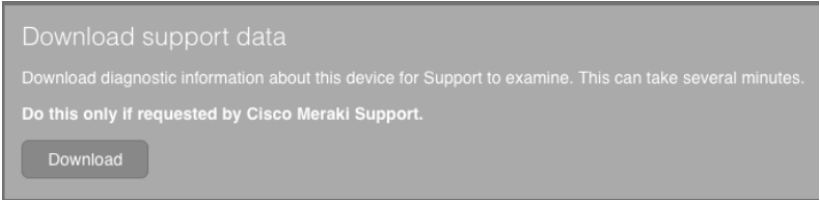
Tip: The LSP is intended to restore cloud connectivity, not to make configuration changes

Using the Local Status Page

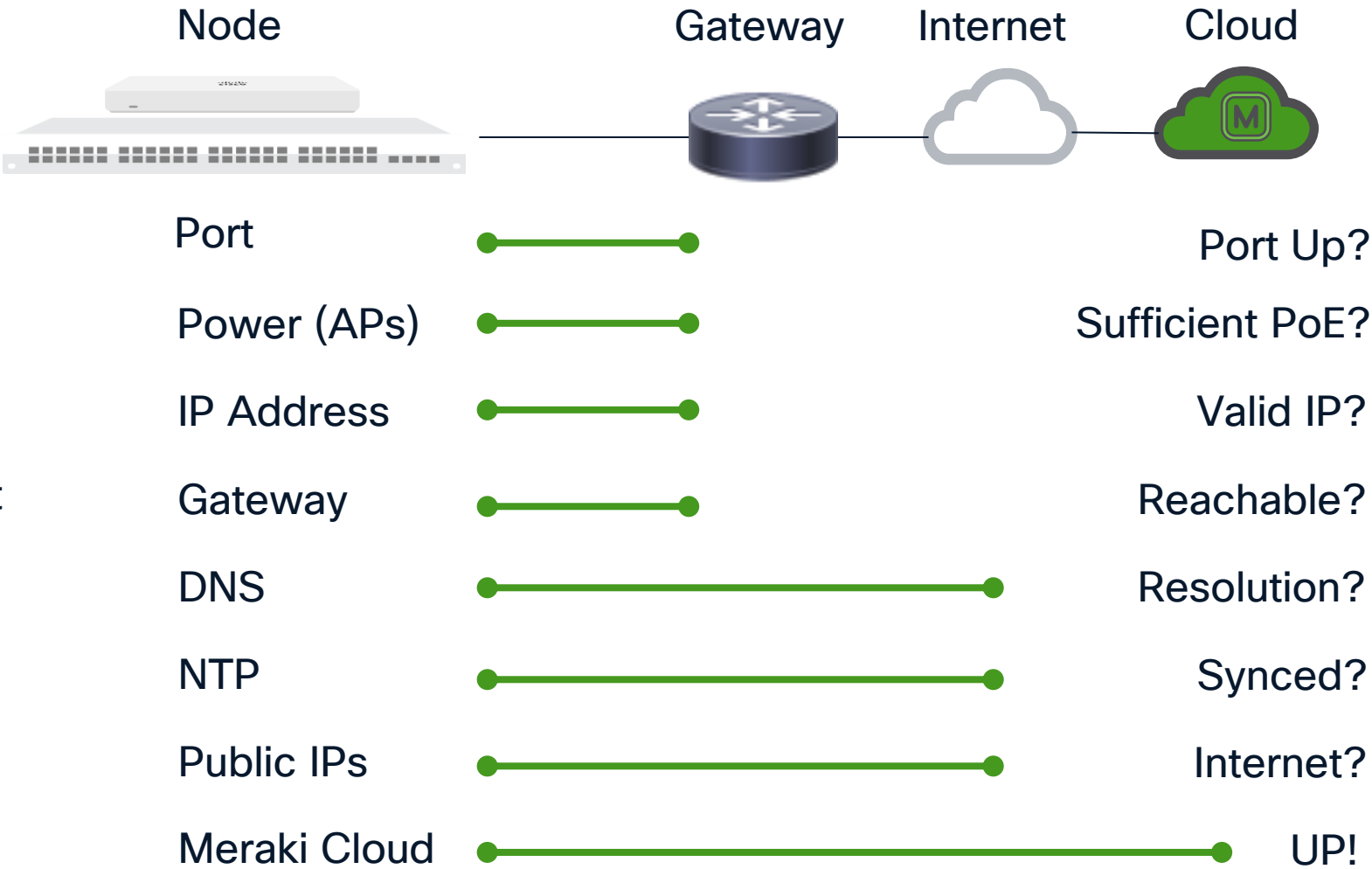
Troubleshooting Cloud Connectivity



Support Bundle = Show tech-support



Note: Support bundle is encrypted



Topology and Change Best Practices

Furthest from the edge first

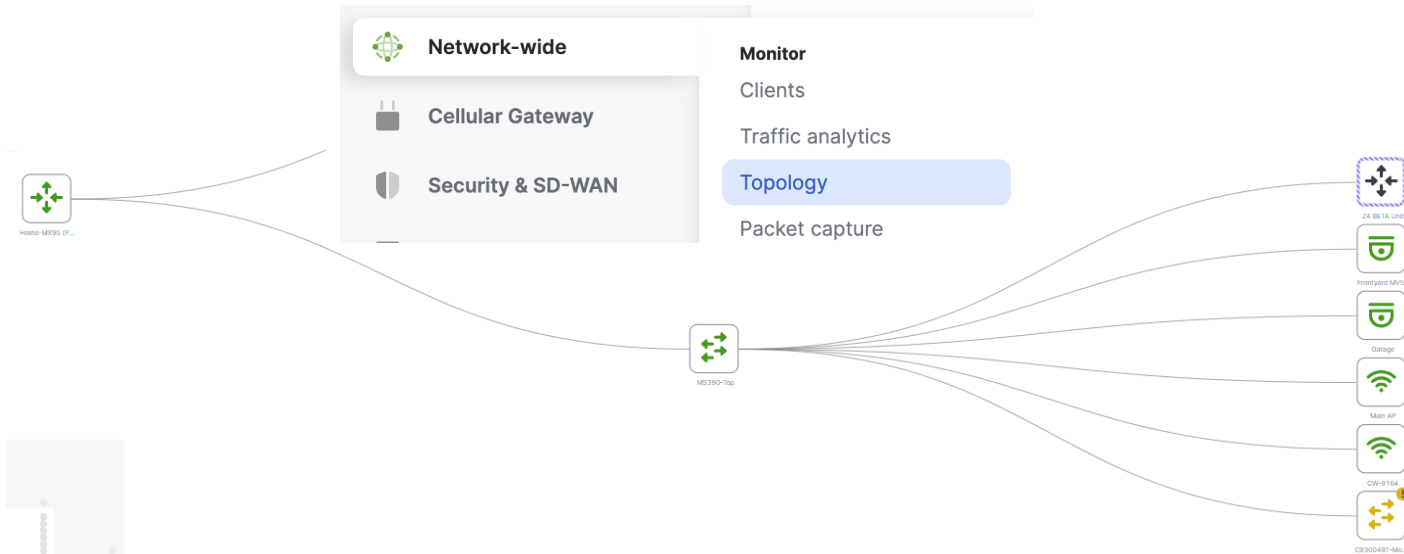
Traditionally topology must be verified by LLDP/CDP and MAC address tables

Visualization requires network diagrams which are only as accurate as the last update

```
C930048T-Hybrid#show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf      Hold-time  Capability  Port ID
VPN Concentrator    Gi1/0/1        120        R           0
Home-MX95           Gi1/0/48       120        R           2

Total entries displayed: 2
```



Platform based topology is dynamically updates with native visualization

Tip: When troubleshooting underlying changes to connectivity, focus on working from right to left

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 and static IP.



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

Factory Reset



Search

AI Assistant

how should I do hardware reset on my c9300 switch

AI Assistant

13:56

To perform a hardware reset on your Cisco Catalyst C9300 switch, follow these steps:

1. While the switch is powered on, locate the mode button on the front panel. (There is also a backup reset pin on the rear of the switch, below and to the left of the console port.)
2. Press and hold the mode button for the desired reset level:
 - Level 1 Reset: Hold for at least 1 second but less than 8 seconds. This performs a basic reset.
 - Level 2 Reset (Day 0 Config, Keep Firmware Image): Hold for at least 8 seconds but less than 20 seconds.
 - Level 3 Reset (Factory Reset, Day 0 Config): Hold for 20 seconds or more. This will restore the switch to its original factory settings.

The switch LEDs will indicate the reset level:

- Level 1: Short 0.5-second on/off cycle
- Level 2: Short, long alternating cycle
- Level 3: Long 3-second on/off cycle

Release the button when the desired LED pattern is observed. The switch will then reboot and apply the selected reset.

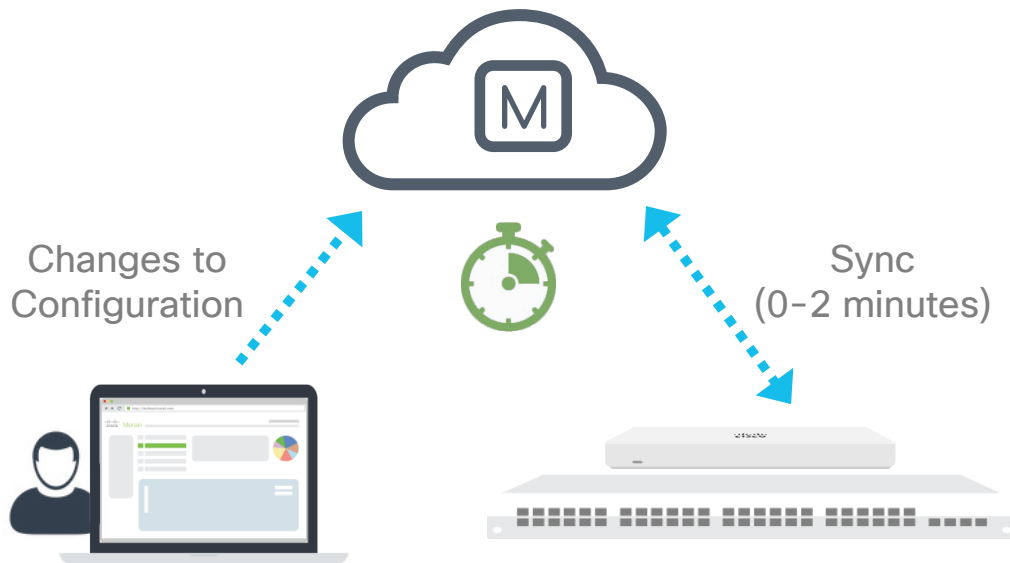
For more details and safety information, see the official documentation: [Resetting Cisco Meraki Devices to Factory Defaults](#)

Ask the AI Assistant a question

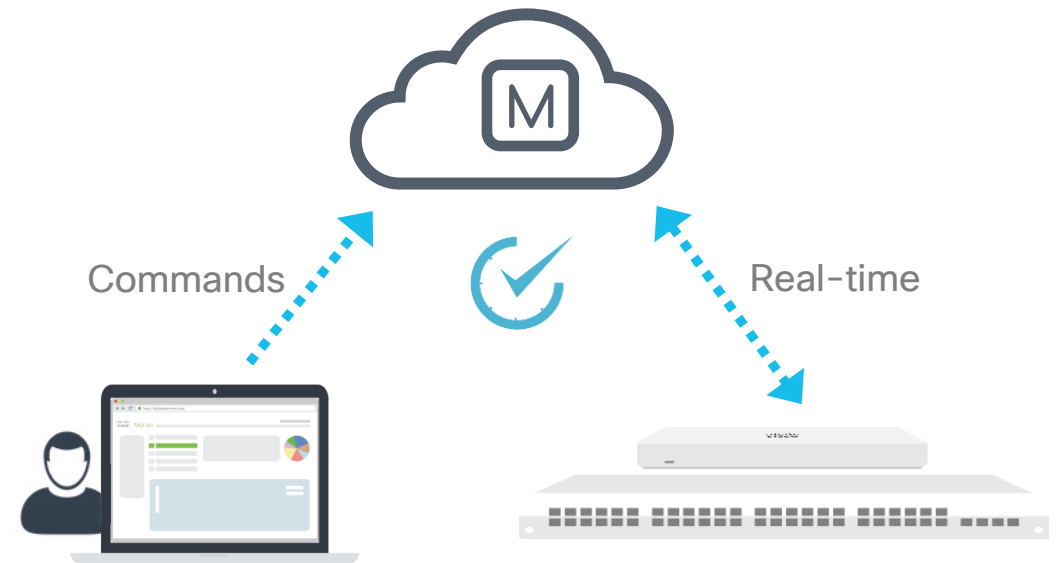
Live Tools for Troubleshooting

Dashboard Sync and Real - Time Tools

Configuration Updates



Live tools



Commands in real-time: ping, traceroute, DNS test, port status, DHCP leases, cycle ports, and more

Live Tools Demo



Summary

L3 routing

Event log

Location

Tools

Ports

[Configure ports on this](#)

Port 1
AGGR/0
Trunk: native VLAN 1
Connected
Auto negotiate (1 Gbps)

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Historical device data

for the last day

Connectivity

12:00

16:00

20:00

00:00

04:00

© 2025 Cisco and/or its affiliates. All rights reserved.

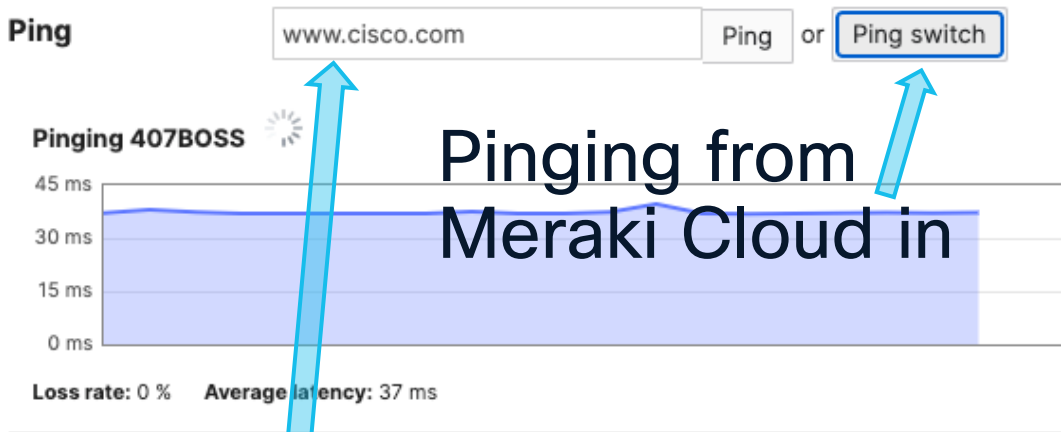
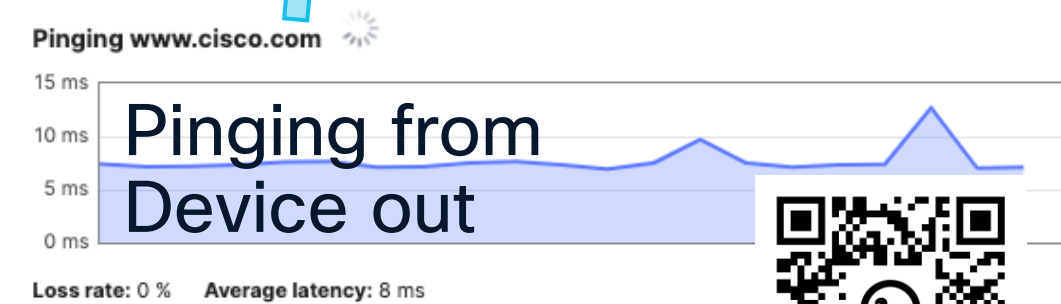
BRKTRS-2008

Live Tools

Ping



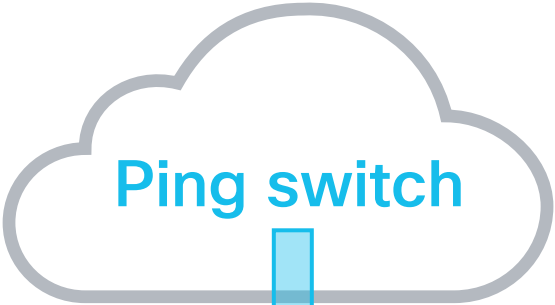
Ping can be sourced from Meraki



L3 Source Interface
Routing Details:



Ping IP
or
Domain



Switching MONITOR

Insight Switches

Summary Ports Power L3 routing Event log Location Tools

Live Tools

My Trace Route (MTR)

MTR Num cycles:

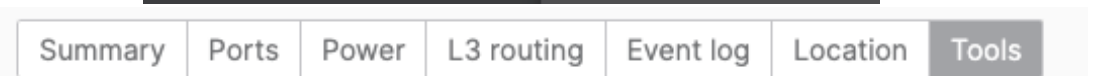
MTR to icmp.canireachthe.net for 10 cycles

IPv4

#	Host	Packets			Pings			
		Loss%	Snt	Last	Avg	Best	Wrst	StDev
1	192.168.1.1	0	10	60.6	59.8	0.5	60.7	52.8
2	192.168.2.254	0	10	1.2	1.6	1.1	41.0	12.5
3	99.112.184.1	0	10	2.2	2.6	1.8	42.3	12.6
4	71.155.112.90	0	10	3.9	4.1	3.7	34.9	9.7
5	???	100	10	0.0	0.0	0	0	0
6	32.130.24.47	0	10	5.1	5.5	4.9	114.6	34.9
7	4.68.39.1	0	10	8.0	7.5	4.4	64.7	18.2
8	4.14.129.74	0	10	5.9	5.6	5.2	95.4	28.4
9	???	100	10	0.0	0.0	0	0	0
10	209.206.55.10	0	10	74.9	41.6	4.8	74.9	36.2
11	209.206.55.10	0	1	5.3	5.3	5.3	5.3	0.0

MTR

MTR



Num cycles:

Note: Packet loss in middle is sign of blocked ICMP
True packet loss will show loss at destination working up from bottom

Live Tools

MAC Forwarding Table

MAC forwarding table

Run

MAC forwarding table



Filter by:

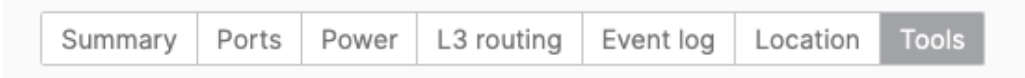
67 MAC addresses

MAC	Port	VLAN
30:23:03:4f:bd:ff	1	10
00:04:4b:ce:80:7d	1	10
b0:52:16:bf:b5:3f	1	10
b8:e9:37:5e:5e:a0	1	10
2c:3f:0b:5b:34:96	1	1
00:0c:1e:03:4f:c7	1	1
70:6b:b9:0f:dd:01	AGGR/0	1
2c:3f:0b:5b:34:95	1	1
7a:8b:75:09:d5:98	1	11
a8:46:9d:1b:10:0f	1	1

10 results per page

< 1 2 3 ... 6 7 >

Note: This is the equivalent to “show mac address-table”



MAC forwarding table

Run

Live Tools

Cable Test



Cable test

Warning: This test may disrupt traffic on this port.

ports (ie. 1-5,7,11,20-23)

Run cable test

Per switch port

Testing the cable attached to port 5

Port	Link	Length	Status	Pair 1	Pair 2	Pair 3	Pair 4
5	1Gfdx	2.5 m	OK	ok	ok	ok	ok

Meraki Powered OSI Layer 1 Troubleshooting

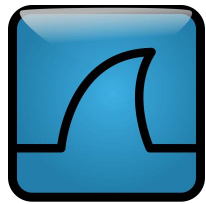
Also, great way to test new cabling installs

```
407BOSS#
407BOSS#test cable-diagnostics tdr int gig 1/0/13
TDR test started on interface Gil/0/13
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
407BOSS#
*Jan 11 19:19:54.382: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/13, changed state to down
*Jan 11 19:19:55.385: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed s
tate to down
*Jan 11 19:19:58.383: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed s
tate to up
*Jan 11 19:20:00.386: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/13, changed state to up
407BOSS#
407BOSS#show cable-diagnostics tdr int gig 1/0/13
TDR test last run on: January 11 19:19:53

Interface      Speed Local pair Pair length      Remote pair Pair status
-----
Gil/0/13      1000M Pair A      9  +/- 10 meters Pair B      Normal
               Pair B      9  +/- 10 meters Pair A      Normal
               Pair C     10  +/- 10 meters Pair D      Normal
               Pair D      9  +/- 10 meters Pair C      Normal
```

Note: This is the equivalent to “test cable-diagnostics” command

Packet Capture



Packet capture for switches ▾

Switch: 407BOSS ▾

Ports: 1

Output: View output below ▾

Duration (secs): 60

Verbosity: Low ▾

Ignore: ☐ broadcast packets

☐ multicast packets

Filter expression:

icmp

[clear output](#) or

[Start capture](#)

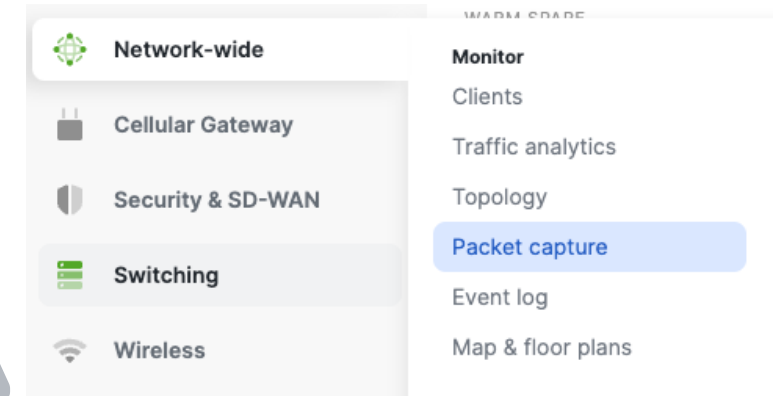
--- Start Of Stream ---

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 ---

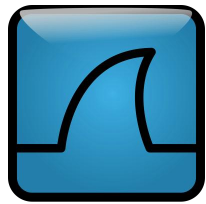
Per Meraki Device

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 training 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 tel/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
```



Help Desk
Administrator

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

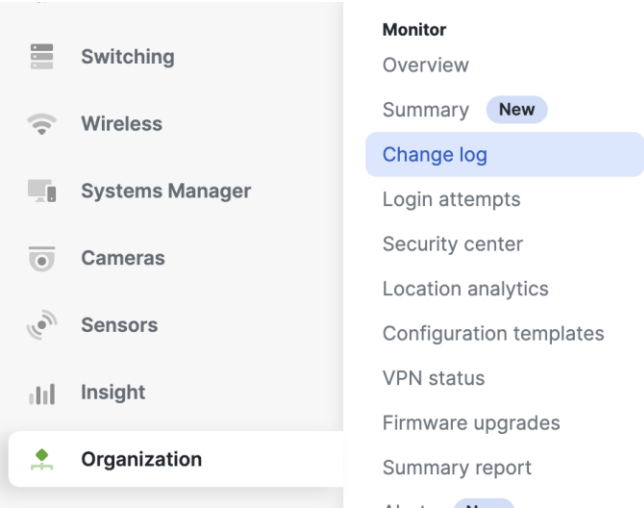
Customer unable to access to Internet

Start capture

Schedule capture

Change Log and Event Log

Change Log



The fastest way to get your bearings during an outage is to look for what has changed in last 2 years

Searchable by Admin, Network, Tag, Time

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

Fulfills change-log compliance requirements such as PCI

Tip: Support usually starts here

Clark & Friends Change Log

Q Search Change Log

1001 changes dating back to 3/7/2023 [Load more changes](#)

[Download as CSV](#)

Time (UTC)	Admin	Network	SSID	Page	Label	Old value	New value
Feb 28, 2024 16:04	Jason Clark	—	—	Port Profiles	Profile updated at	2023-10-23T20:27:41Z	2024-02-28T16:04:13Z
Feb 28, 2024 16:04	Jason Clark	—	—	Port Profiles	Profile name	Data	Data Profile
Feb 28, 2024 16:03	Jason Clark	—	—	Port Profiles	Profile updated at	2023-06-30T14:47:18Z	2024-02-28T16:03:05Z
Feb 28, 2024 16:03	Jason Clark	—	—	Port Profiles	Profile name	Test	Data Profile

Change Log



AI Assistant



You

What has changed since I last logged in

AI Assistant

23:58

Here's a summary of what has changed in your Meraki Sydney SYD05 network since your last login:

Date	Change	Changed by
Nov 8, 2025, 05:20 AM GMT+11	Allowed VLANs on IT Switch port 1 updated from "1-4094" to "1,60,100,150,961,1491-1492"	luis.tirado@meraki.net /SSO
Nov 7, 2025, 01:05 PM GMT+11	MAP App Config [Enterprise Agent] updated from version 0.67.0 to 0.68.0	MAP API User
Oct 25, 2025, 03:35 AM GMT+11	Node SSH keys updated	noe.hernandez@meraki.net /SSO



Event Log

Network Chatfield

Network-wide

Cellular Gateway

Security & SD-WAN

Switching

Wireless

Monitor

Clients

Traffic analytics

Topology

Packet capture

Event log

Map & floor plans

Time (UTC)

Jan 10, 2023 19:18

Admin

Gordon I

Switch: Any

Client: Any

Before: 01/11/2023 11:24 (CST)

Event type include: All

Event type ignore: None

Search

Reset filters

Event log

for switches

for security appliances

for cameras

for cellular gateways

for access points

for devices

for switches

for sensors

Switch: Any

Event type include: All

Search

Reset filters

Download as

Time (CST)

Jan 11 08:18:05

Jan 11 01:56:10

Jan 11 01:54:58

Switch: Any

Client: Any

Before: 01/11/2023 11:24 (CST)

Event type include: All

Event type ignore: MAC address flapping

Search

Reset filters

Download as

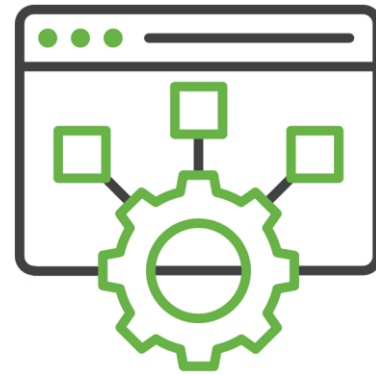
Time (CST)	Switch	Client	Event type	Details
Jan 11 00:30:26	Office IDF		Port STP change	Port 4 disabled→designated
Jan 11 00:30:26	Office IDF		Port status change	port: 4, old: down, new: 1Gfdx
Jan 11 00:30:23	Office IDF		Port STP change	Port 4 designated→disabled
Jan 11 00:30:23	Office IDF		Port status 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:DD:00, 3049; expected E0:55:3D:31:FD:68, 3840

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

Firmware

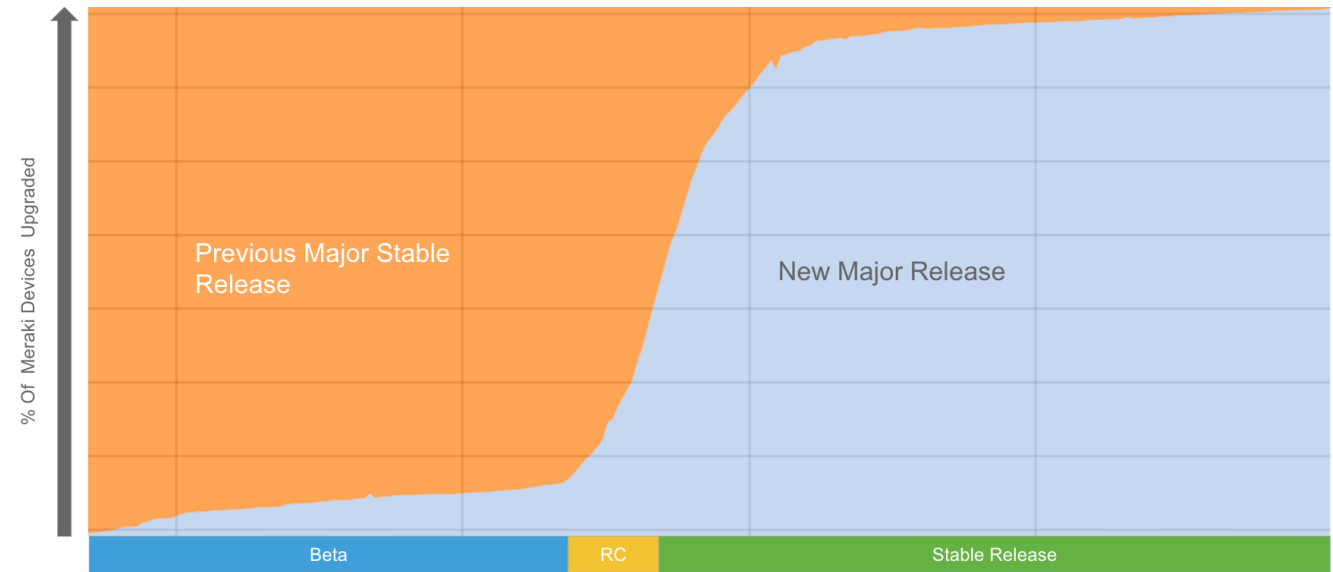
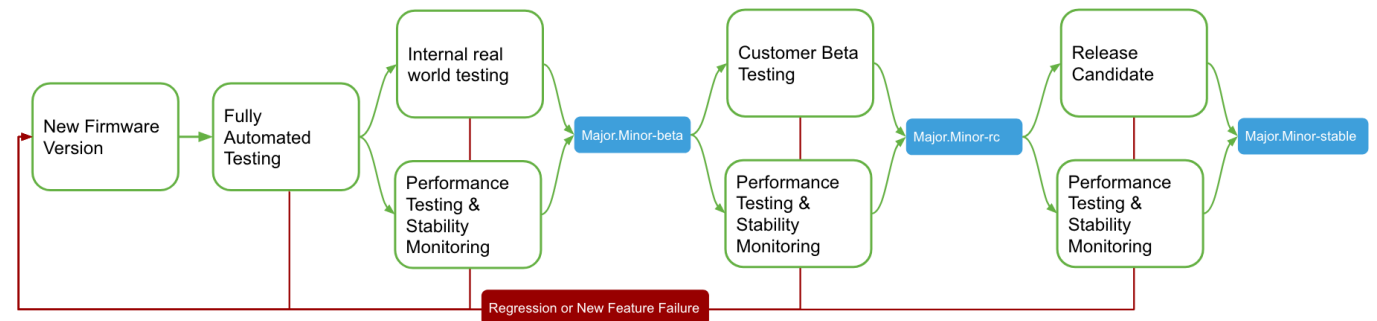
Firmware = Troubleshooting?

Firmware is absolutely part of the troubleshoot 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

Meraki Firmware Life Cycle



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

Search...

Expand All Collapse All

Suggested Releases

Cupertino-17.9.4a

Bengaluru-17.9.4a

Latest Release

Cupertino-17.9.4a

IOSXE-17.9.4a

Dublin-17.9.4a

Bengaluru-17.9.4a

All Release

17

16

Tftpd32 by Ph. Jounin

Current Directory: C:\Users\vmware\Desktop Browse

Server interfaces: 192.168.1.200 Intel(R) 82574L Show Dir

Tftp Server Tftp Client DHCP server Syslog server Log viewer

peer	file	start time	progress	date	Size
192.168.1.1:51845	>c2800nm-adve...	12:33:31	N/A	023	1193.60 MB

```
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# 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!

Configuration Source: Device mode
firmware upgrades road-mapped

Schedule firmware change

When should this firmware be installed?

Upgrade times may be staggered depending on the number of devices changing firmware.

☒ Perform the upgrade now

☐ Schedule staged upgrade

☐ Schedule the upgrade for:

03/08/2024

 at

13:00 ▼

 (network local time)

Back

Next

[Learn more](#)

**MS 16.7**
Released Oct 24, 2023
[Release notes](#)

[Schedule upgrades](#)

Scheduled

Firmware Management



AI Assistant

You

is this switch sfo12-4-2-sw-01-pdu running on latest firmware

AI Assistant

14:01

Your switch sfo12-4-2-sw-01-pdu is currently running firmware version CS 17.2.1. The latest completed switch firmware upgrades in your organization are to MS 17.2.2/CS 17.2.1.1 or newer, which means your switch is running on the latest available firmware for your network (Meraki San Francisco SFO12).

If you need to confirm or schedule future upgrades, you can check the Meraki Dashboard for pending updates.

Source: Device firmware version and recent upgrade history for Meraki San Francisco SFO12.

You

how many switches in my network Meraki San Francisco SFO12 are not running on latest firmware

AI Assistant

14:03

SFO12 switch firmware status

Number of switches not running the latest firmware	Latest firmware version	Status of pending upgrades
0	MS 17.2.1/CS 17.2.1.1	No pending switch firmware upgrades

Ask the AI Assistant a question

Meraki Assurance

**Dashboard Intelligence,
Root Cause Analysis,
Intelligent Alerting**

Operationalize and Day N NetOps

Introducing the Assurance Menu



Organization-wide

Cameras

Sensors

Insight

Organization

Monitor

Overview

Summary New ✓

Alerts

Users

Change Log

Configure

Settings

Integrations Ne

API & Webhooks

Configuration Syr

MDM

- Now organization-wide
- Full stack network health
- Tools haven't moved
- Health score and trends

Organization insights

Impacted networks

1

/8

+0

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](#)

Q Search

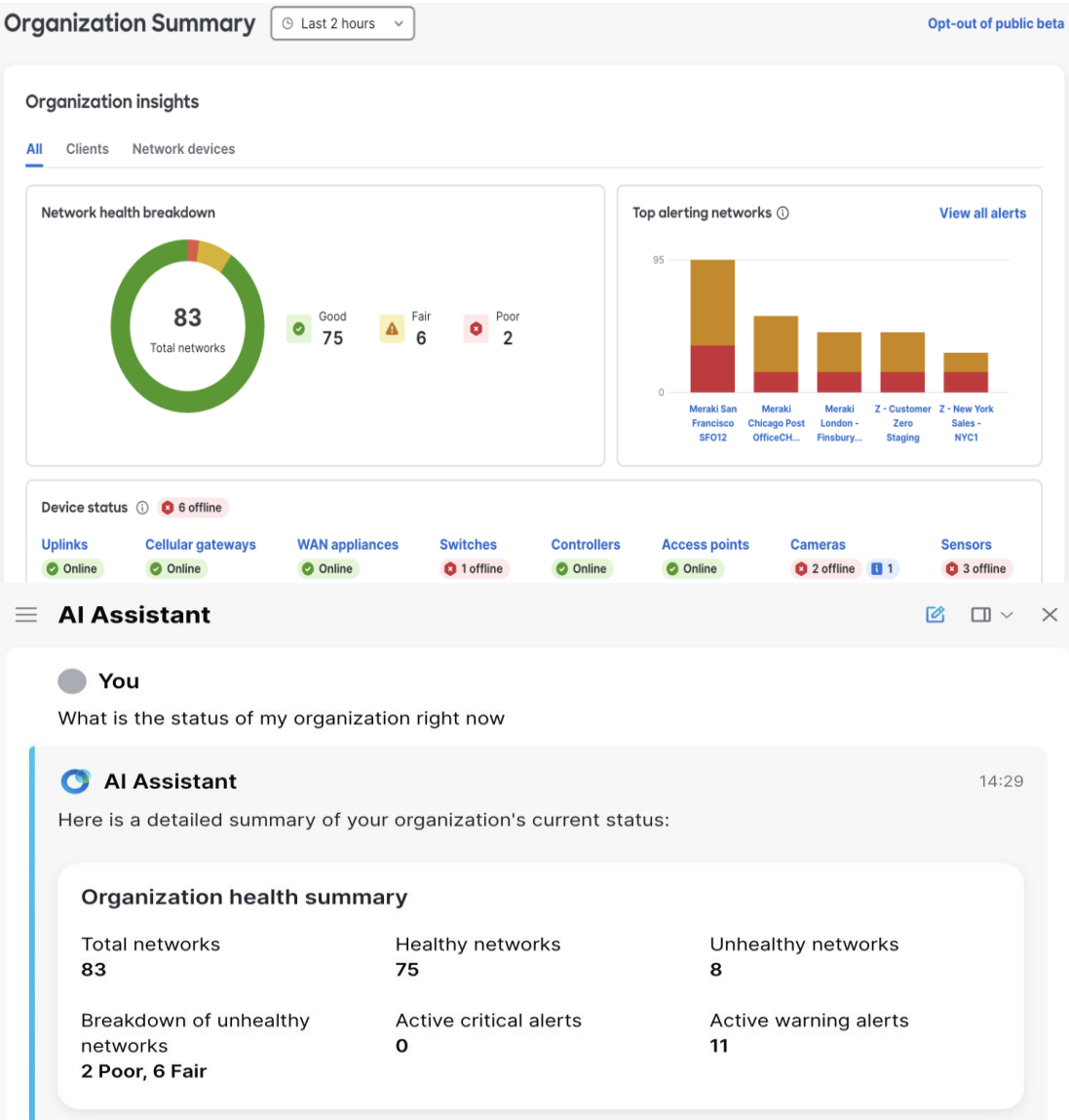
Health status

14 results

Network	Health score	Score change	Network tags	Clients	Network devices	Infrastructure	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

Introducing the Assurance Menu



Operationalize and Day N NetOps



Network-specific

Assurance **New**

Cellular Gateway

Security & SD-WAN

Switching

Analytics

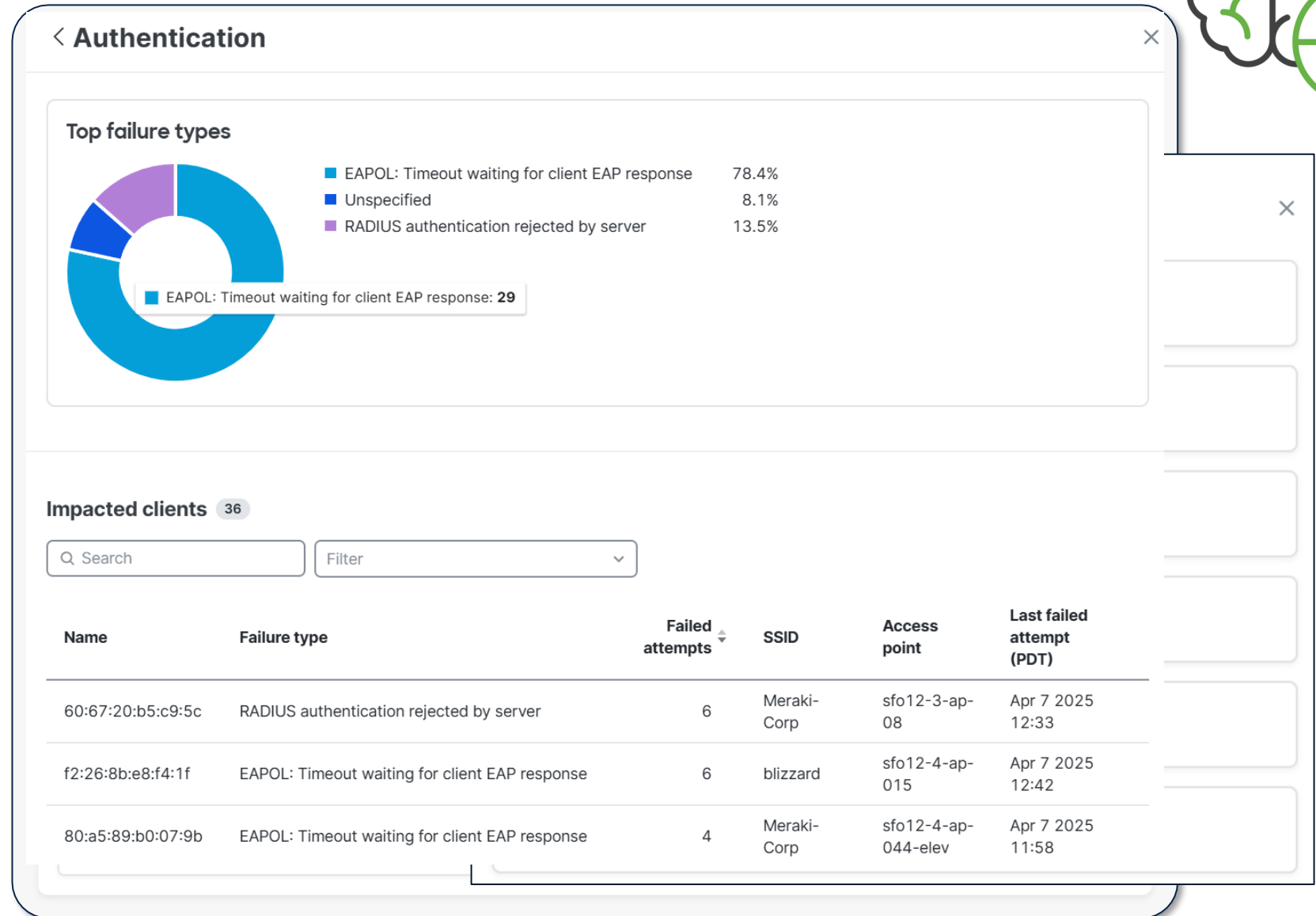
Overview **New** ✓

Alerts

Clients

Web App Health

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

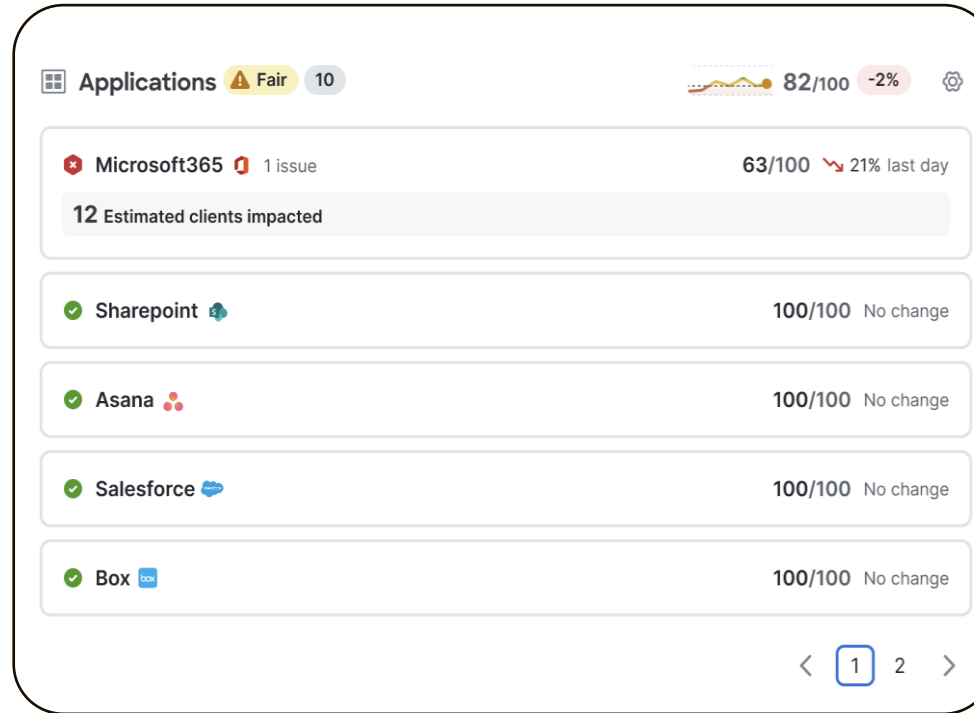
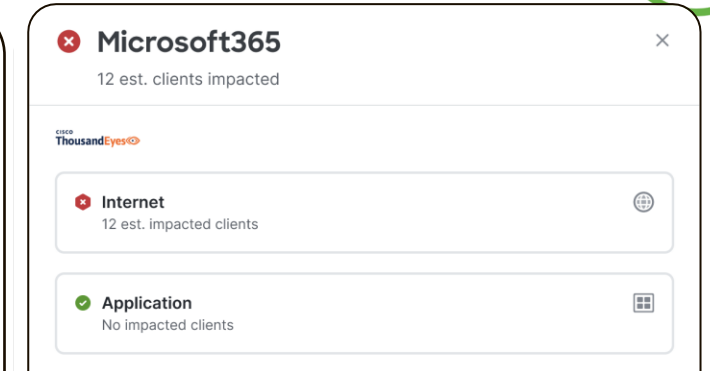
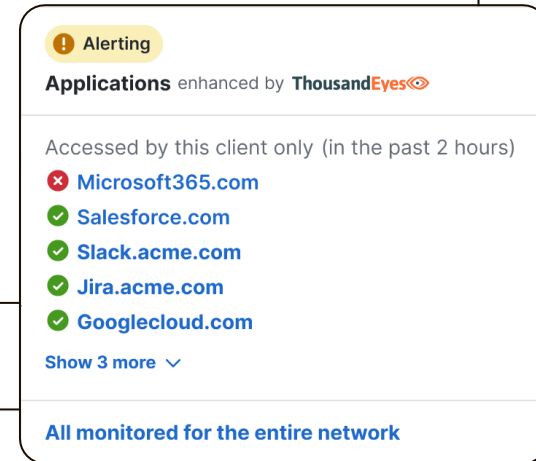
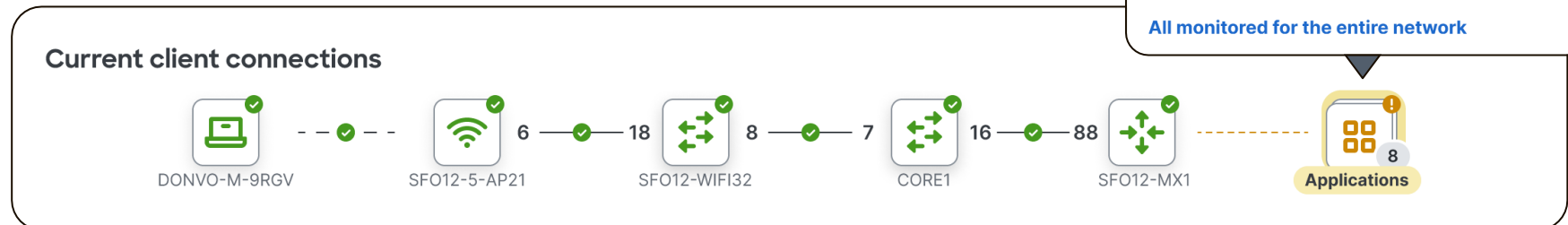


Operationalize and Day N NetOps

ThousandEyes Assurance Integration



- Per-application health
- Visibility beyond the WAN
- Differentiate internet and application issues
- Single-client workflows



Organization Wide Intelligent Alerts

What's happening across your network



Monitor

Overview

Summary

Alerts

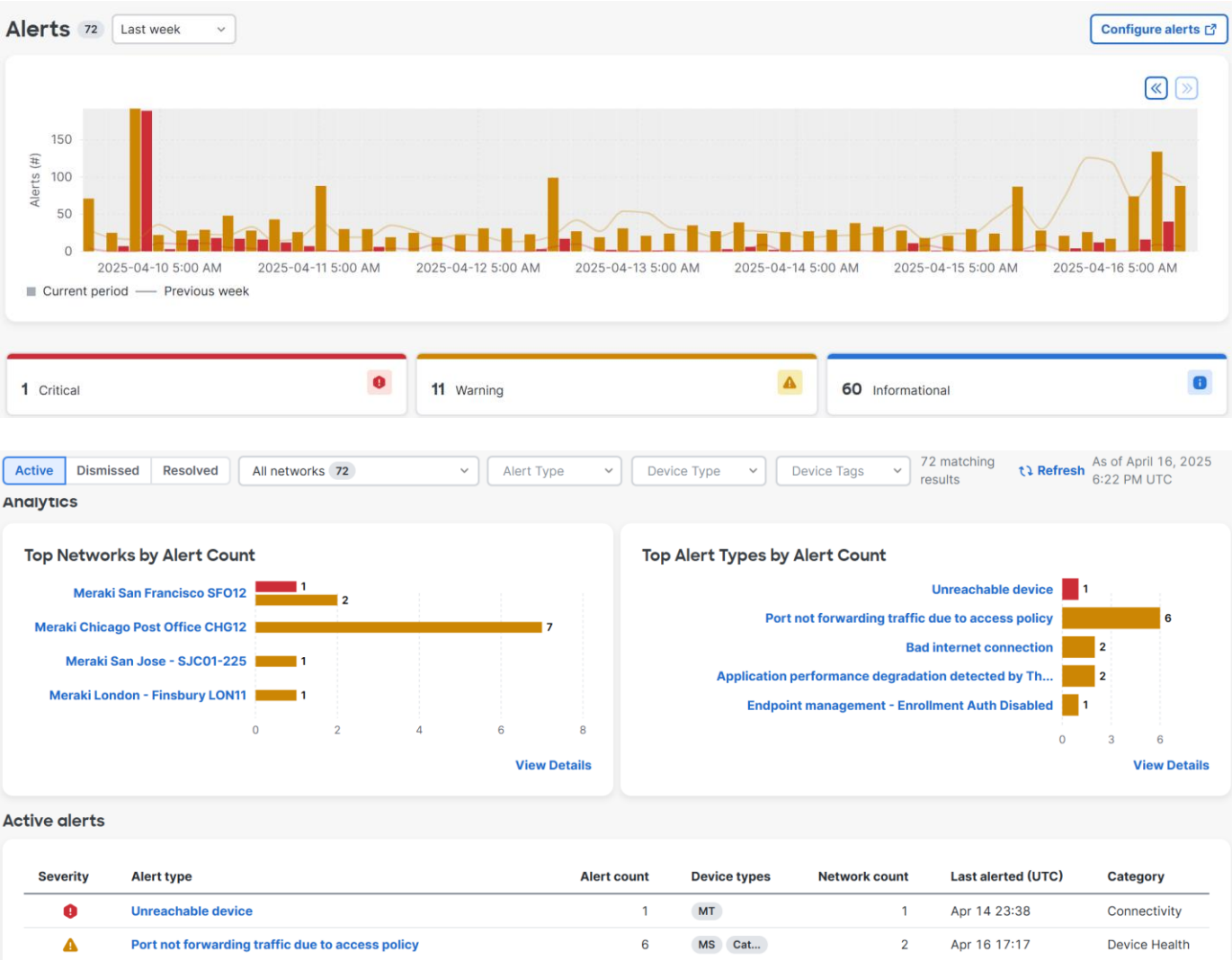
Configure

Settings

Integrations

API & Webhooks

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



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 



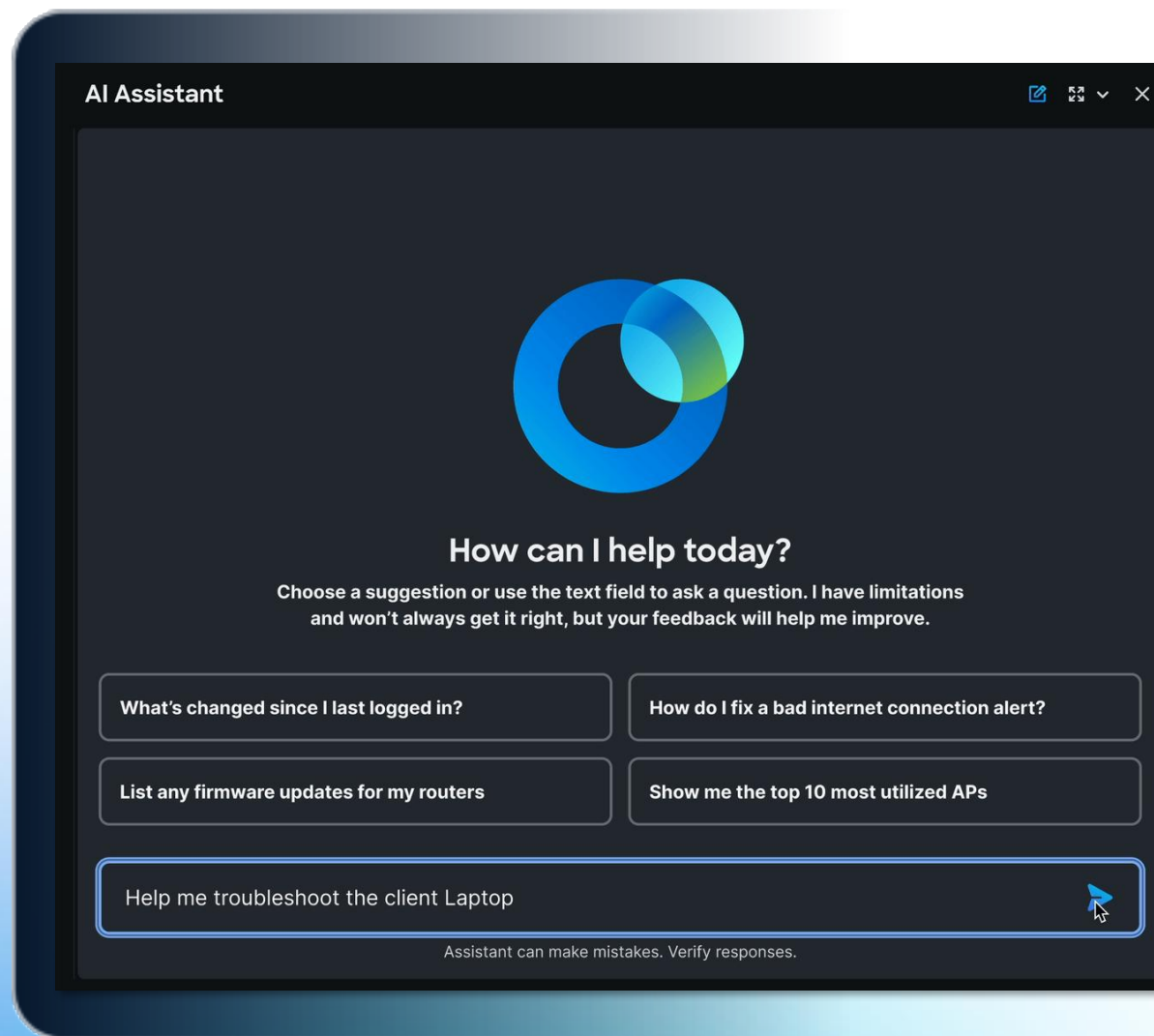
Recommendations

- 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.

Intelligent troubleshooting and RCA



- Finds root cause—not just the alert
- Provides full stack visibility
- Pinpoints the issue and guides the fix

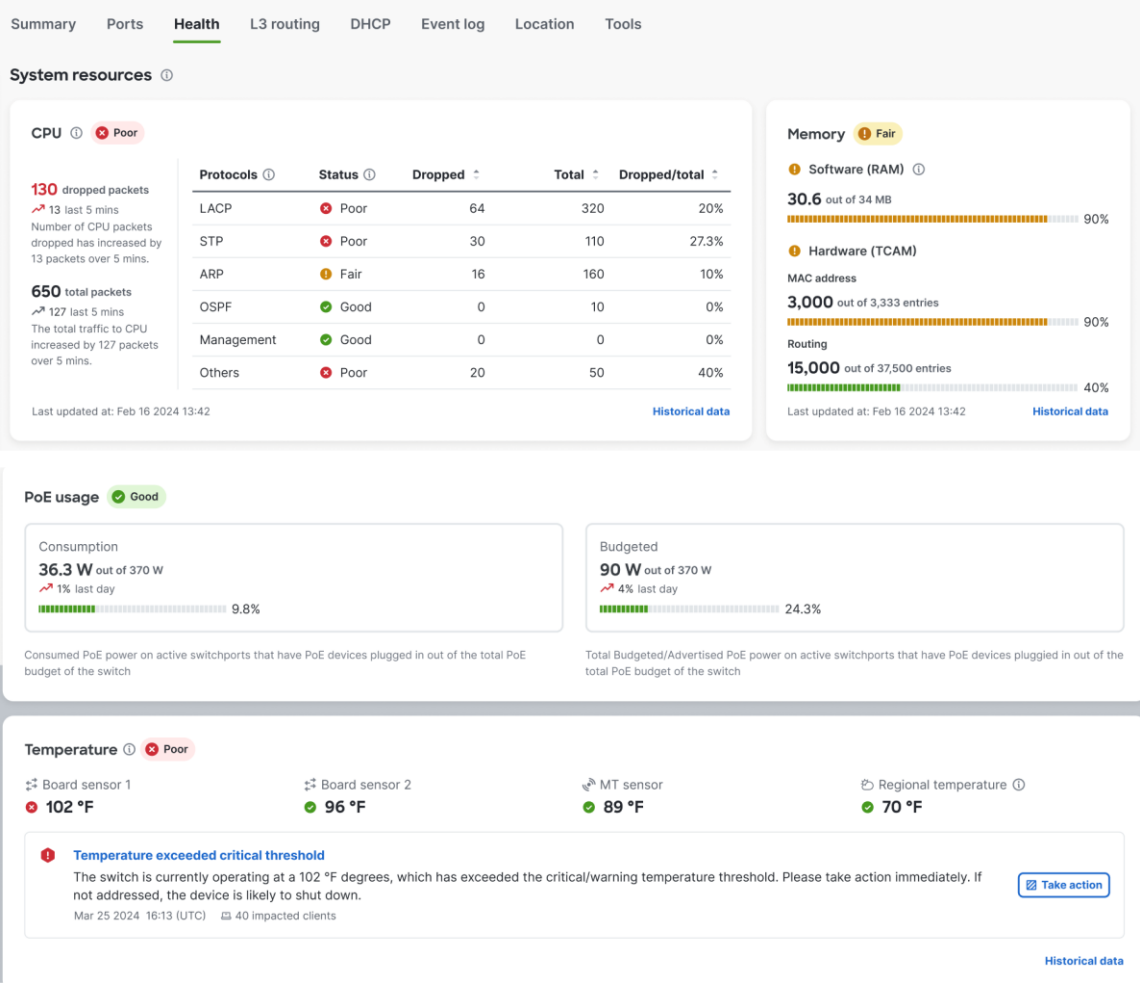
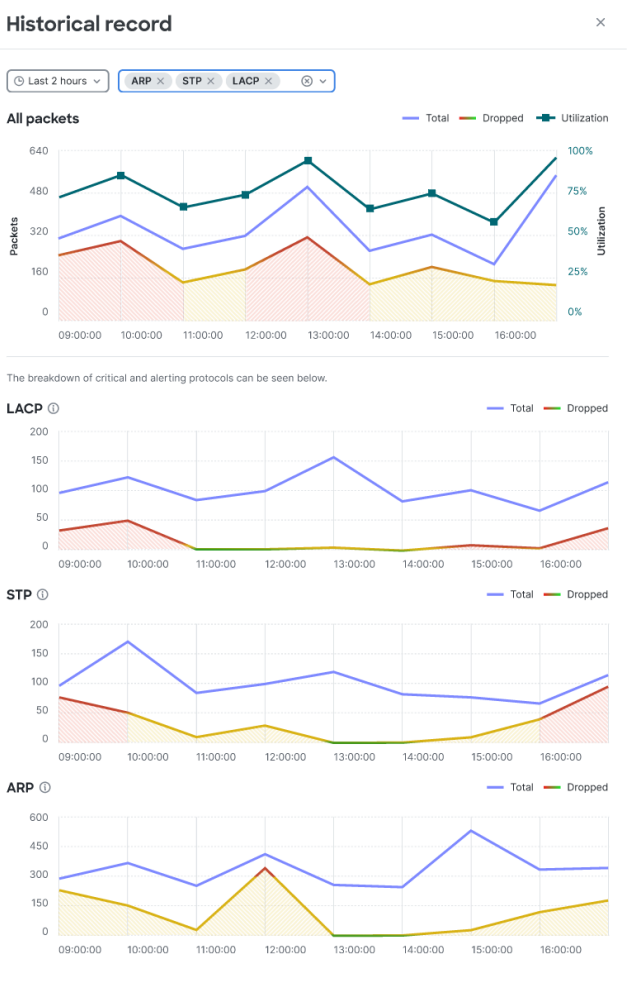


Device Health Tab

Providing visibility into health metrics for switching and wireless

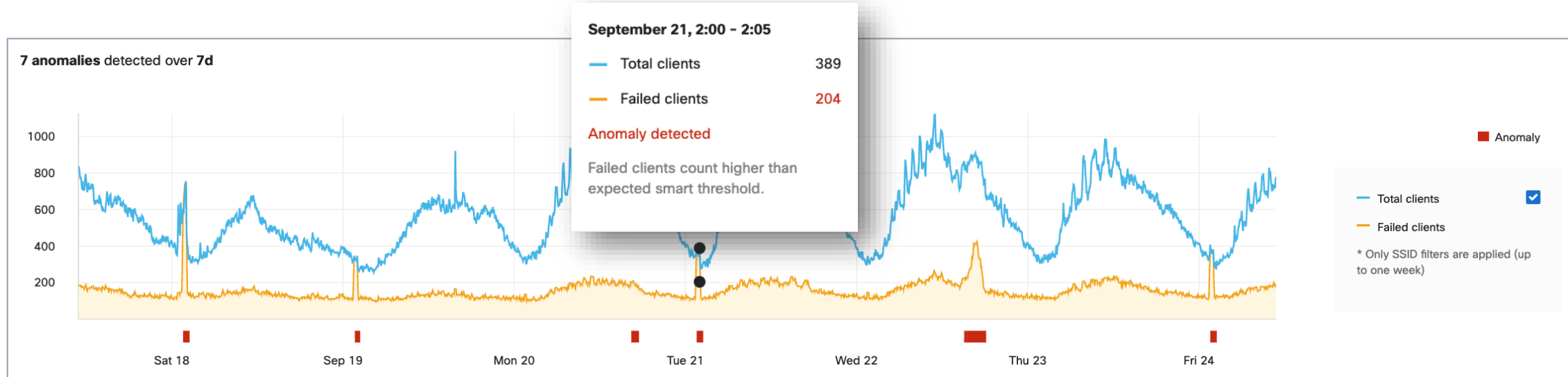


- Track physical statistics
 - Power
 - Temperature
- Resource Metrics
 - CPU/Memory
 - TCAM
 - PoE



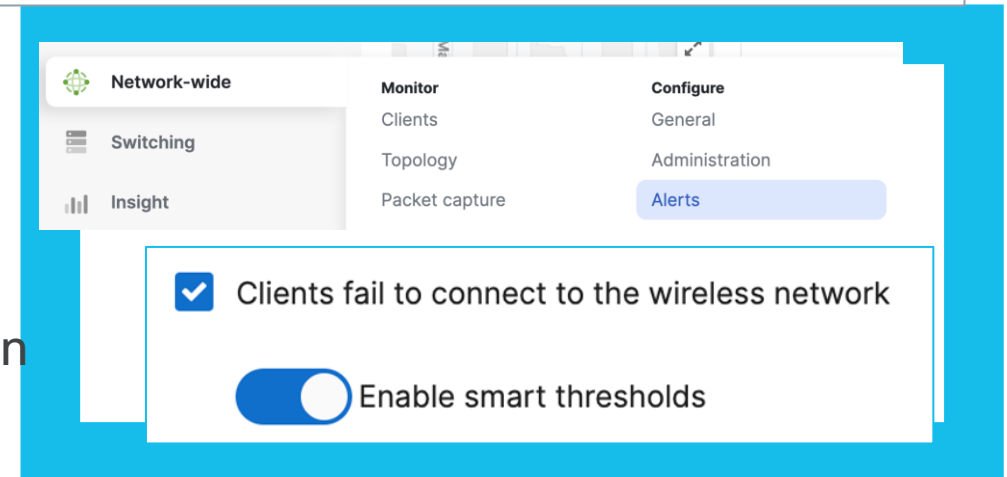
Smart Thresholds for Wireless

Intelligent-Driven anomaly detection



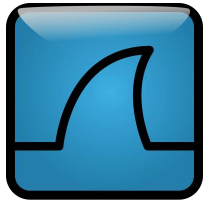
Not enabled by default

- **Simple, familiar UX**, using new Wi-Fi dataset
- Machine learning powered **anomaly detection**
- Industry leading **one month** historical information



Intelligent Capture

Streamline Troubleshooting - Schedule, Store, and Proactive Captures



Intelligent Capture

For switches

New capture

Stored captures

Scheduled captures

Select switch(es) to capture

Single switch

Multiple switches

Switch

Enter ports

Output

Save to cloud

Duration (secs)

60

Capture filters

View example 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

Cancel

Schedule

Proactive PCAP enablement

Disable the auto capture for all devices

Enable the auto capture for all devices

Enable the auto capture for some devices

Save

Intelligent Capture

For switches

New capture

Stored captures

Scheduled captures

Search

Device

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	<div><div></div>Saved to cloud</div>	Manual	22.6 kB		<div><div>View report</div></div>	...	
☐	Dec 11, 02:42 PM	Clark Home - switch-C930048T-Monitored	C930048T-Monitored / GigabitEthernet1/0/1	Jason Clark	<div><div></div>Saved to cloud</div>	Manual	13.6 kB		<div><div>View report</div></div>	...	

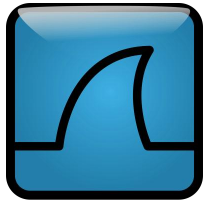
Rows per page

10

< 1/1 >

Intelligent Capture

Proactive Captures and Analysis



Intelligent Capture

For access points ▾

New capture

Stored captures

Proactive PCAP Enablement

Proactive PCAP enablement

☐ Disable the auto capture for all devices

☒ Enable the auto capture for all devices

☐ Enable the auto capture for some devices

Save

☐	Time	Name	Access Points	User	Status	Source	Client	Packet Count	Step	Reason	Notes	File size	Analyze	Action	
☐	Mar 30, 12:42 PM	f0:ad:4e:0f:24:28_1prmm4_auth_bad_password	Main AP	Auto capture	Saved to cloud	Auto capture by Meraki cloud	f0:ad:4e:0f:24:28	85	Authentication	Invalid authentication		16.8 kB	View report	...	
☐	Mar 30, 12:36 PM	f0:ad:4e:0f:24:28_KmlyFJ_auth_bad_password	Main AP	Auto capture	Saved to cloud	Auto capture by Meraki cloud	f0:ad:4e:0f:24:28	88	Authentication	Invalid authentication		17.8 kB	View report	...	

- Health issues detected by Meraki will automatically trigger a Capture
- Monitors Association, Authentication, DHCP, and DNS failures
- 7 Days of retention up to 4GB per network

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

Packet Capture Analysis Summary

Tests summary

Protocols
3/3 protocols failed

DHCP
1/2 tests failed

ARP
1/1 tests failed

ICMP
2/2 tests failed

MAC address summary

These MAC addresses appeared in at least one of the failed tests.

6c:7f:0c: a8:46:9d: 2c:3f:0b: 00:1f:ca: 52:54:dd: e0:d3:b4: 68:3a:1e:

Device summary

These devices appeared in at least one of the failed tests.

Switch E Switch C - SPARE Switch H

DHCP

1/2 tests failed

Multiple DHCP servers seen All tests passed

DHCP Transactions completed Failed 12

ARP

1/1 tests failed

Missing ICMP responses

ICMP request to 8.8.8.8 has no response

Packets 2, 7, 51, 117, 128, 138, 160, 187, 232, 252, 264, 303, 317, 368, 388, 408, 450, 470, 516, 562, 574, 594, 604, 623, 674, 685, 702, 715, 753, 796, 806, 819, 832, 869, 917, 931, 981, 1006, 1027, 1069, 1086, 1116, 1139, 1161, 1183, 1255

Details ICMP request failed from 172.20.193.76 to 8.8.8.8

ICMP request to 172.20.193.81 has no response

Packets 4, 46, 98, 121, 129, 146, 181, 221, 244, 254, 297, 310, 328, 377, 395, 432, 461, 473, 536, 565, 588, 598, 606, 653, 676, 689, 705, 744, 791, 801, 810, 821, 854, 903, 921, 937, 999, 1016, 1042, 1075, 1094, 1129, 1153, 1165, 1243

Details ICMP request failed from 10.92.135.56 to 172.20.193.81

Summary

Summary

- Operationalize using a platform approach
- Lean in and trust the dashboard
- Live Tools are real-time
- Leverage Meraki Assurance
- Embrace PCAP (it makes you a better network engineer)

Complete your session evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Thank you

CISCO Live !

