



The bridge to possible

Meraki Observability

Be the hero, avoid the blame game

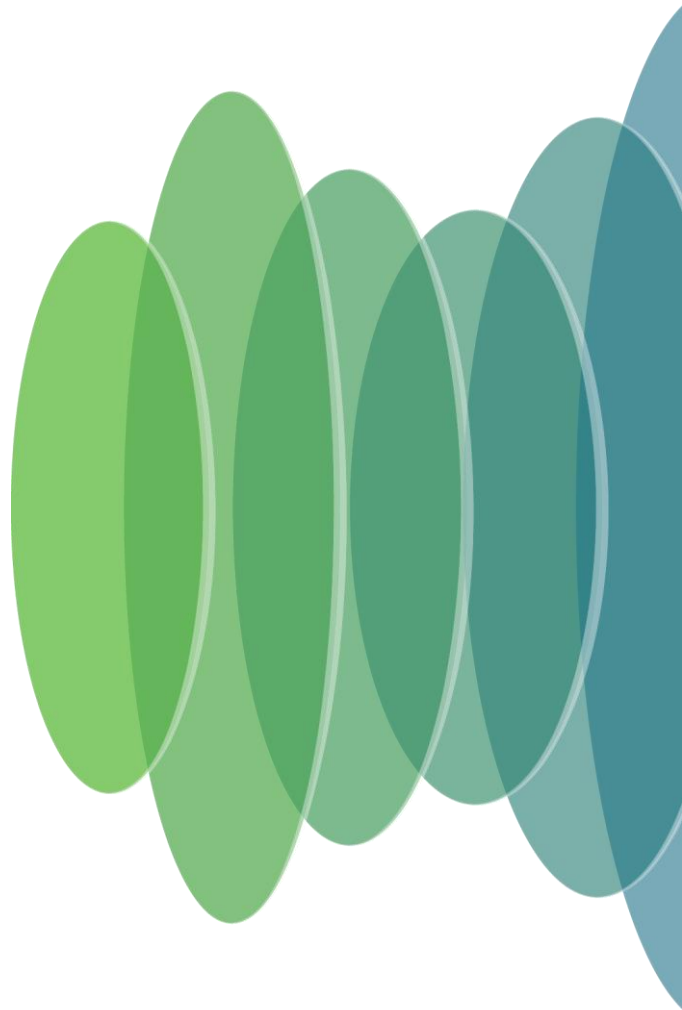
Paul Hasstedt – Technical Solutions Architect, Cisco Meraki
BRKOPS-2013

CISCO *Live!*

#CiscoLive

“If I had a dollar for every packet I’ve sent to prove my innocence, I would have retired 10 years ago!”

-Multiple Network Engineers in this room
...probably ;)





@PaulHasstedt

- Colorado born and raised, now living in Phoenix, AZ
- Masters in Music with an emphasis in Vocal Performance/Conducting
- Previously professional opera singer and middle school music teacher
- Joined Cisco 2016 -> Meraki 2018

Cisco Webex App

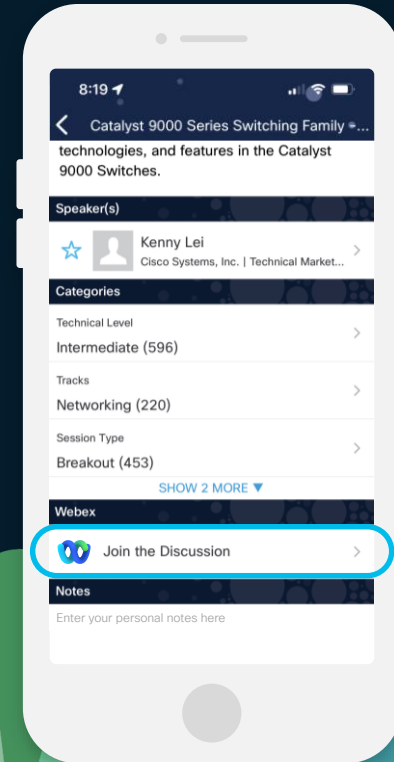
Questions?

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 June 7, 2024.





Agenda

- A Hero's challenge
- Device Health Champion
- Meraki Insight Master
- ThousandEyes Power
- Demo

The tsunami of data



“I have copious amounts of spare time to do manual correlation of the data...”



“It’s always been easy to keep track of how distributed our users and resources are...”



“Identifying the device or service that is our issue’s root cause is very straightforward...”

-Probably no one who has ever worked in IT...



Number of hours spent on Deploying, Scaling and
Managing an IT infrastructure
is 10 hours a week!

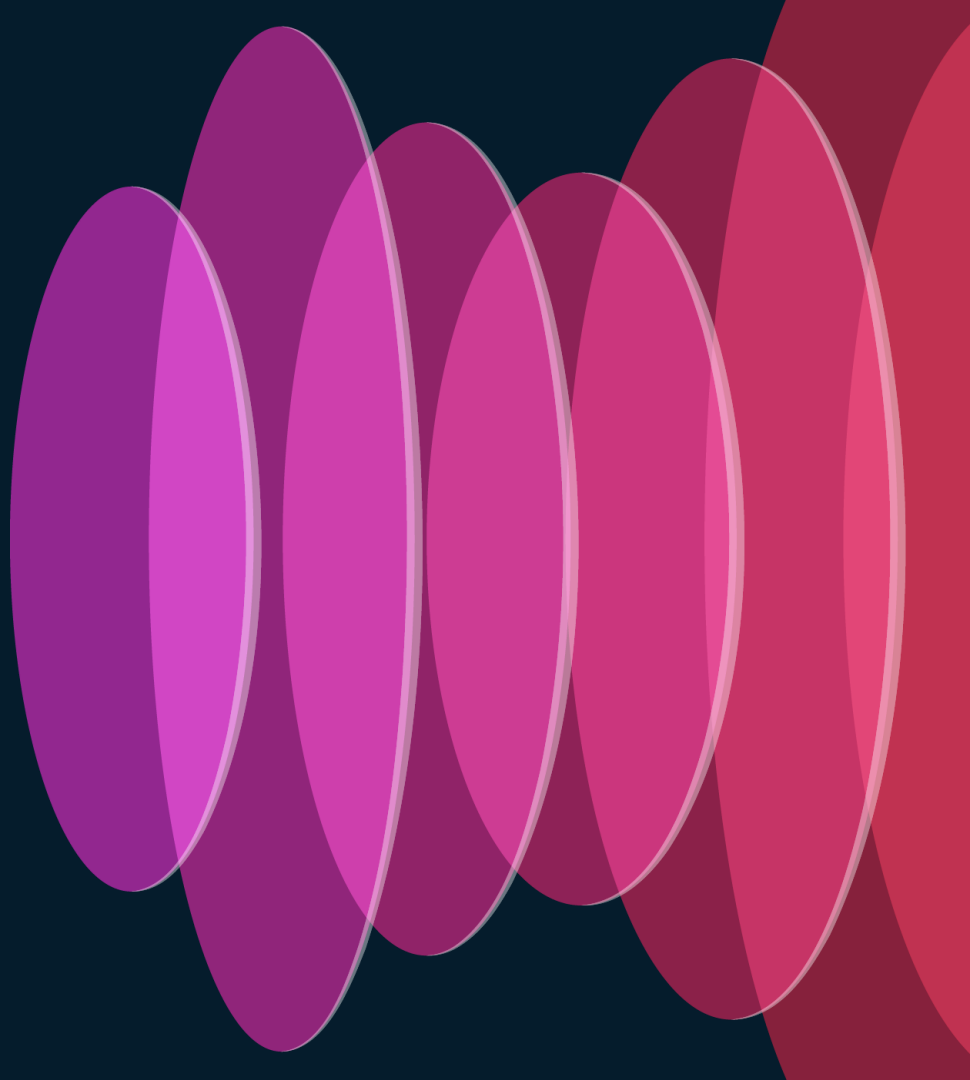
Source: Forrester Report



Meraki's Mission

Simplifying powerful technology to free
passionate people to focus on their mission

Device Health Champion






“...to clarify, you’re calling me from your laptop that is connected to the wifi, to tell me the wifi is down...”

-Anyone who has worked in support...



Traditional visibility

Tool	Cost	Overhead
All things cli/debug	-	
SNMP, Netflow, syslog	\$	
Wifi spectrum analyzer and monitoring software	\$\$\$	

All the switching data

```
Switch# debug platform vlan [ error | event ] [ switch switch-number ]
```

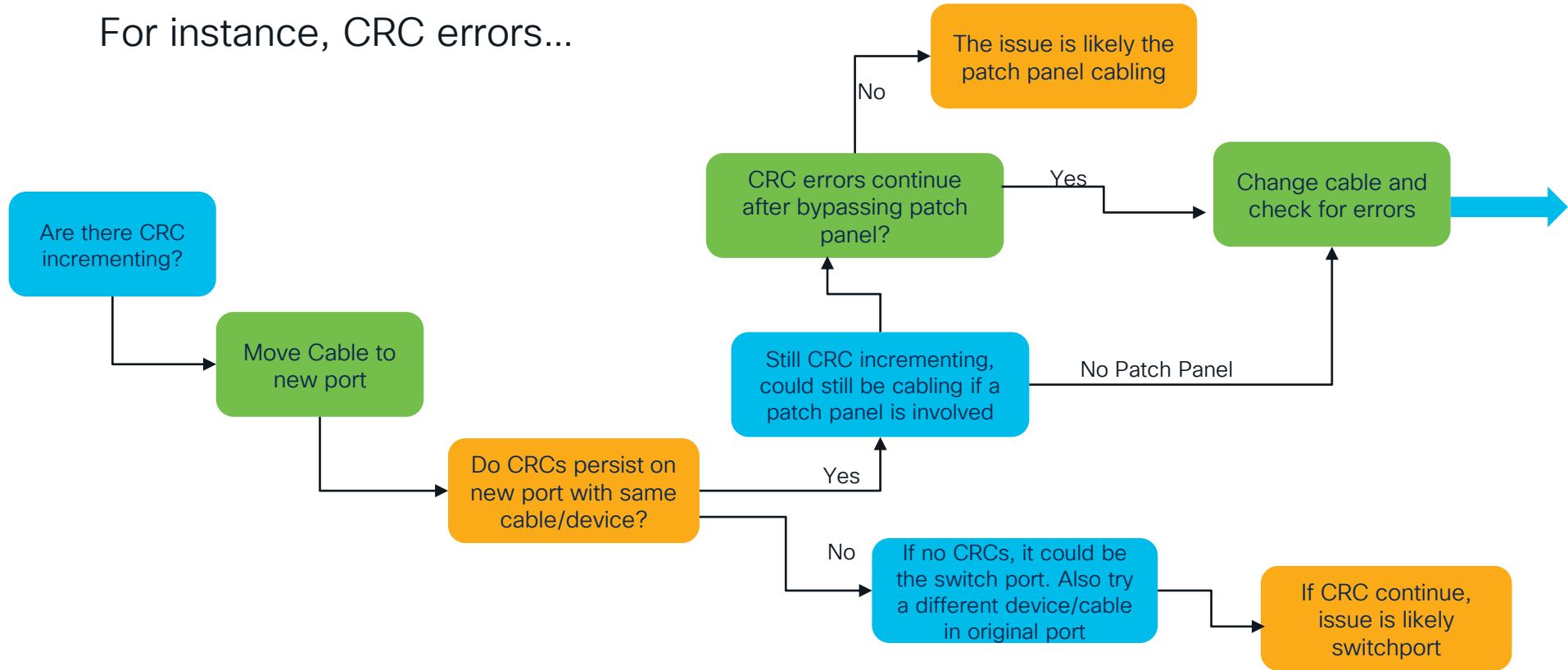
```
Switch# show vlan [ brief | group | id vlan-id | group-name WORD user_count | mtu | name vlan-name | remote-span | summary ]
```

```
Switch# show interface ethernet 1/1 | i CRC
```

```
Switch# show cable-diagnostics tdr interface gigabitEthernet 0/1
```

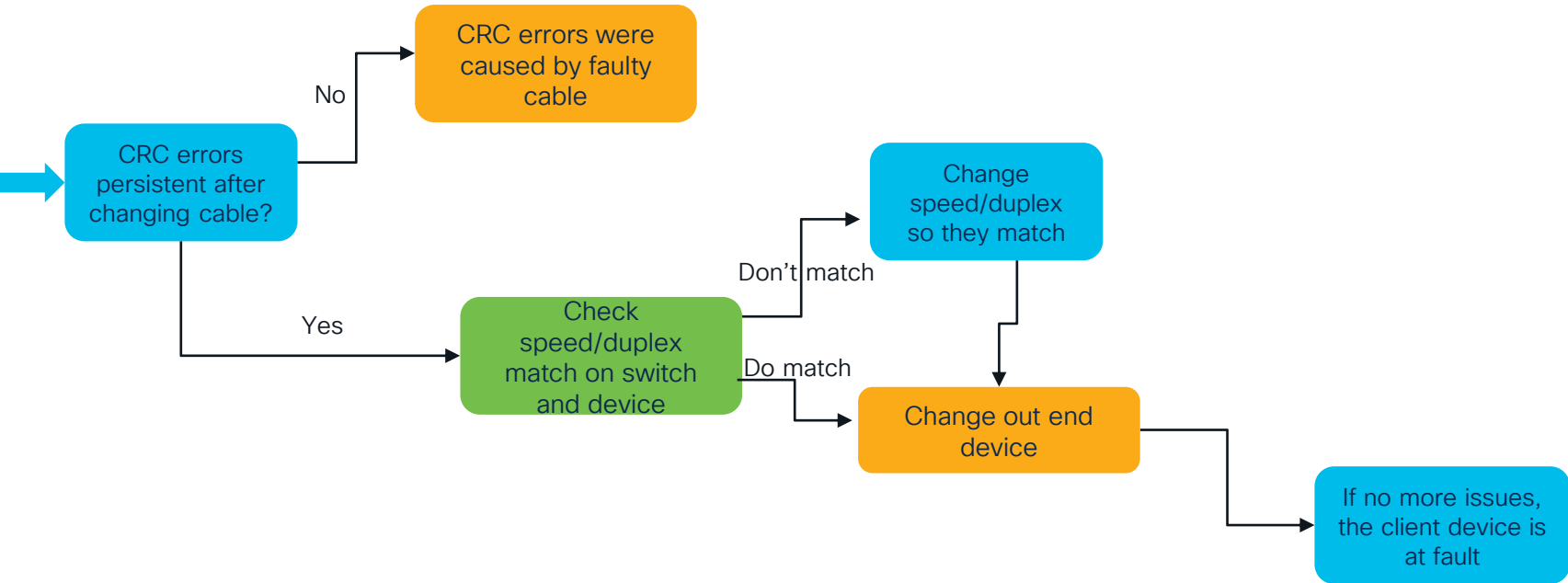
Manual correlation with the data

For instance, CRC errors...

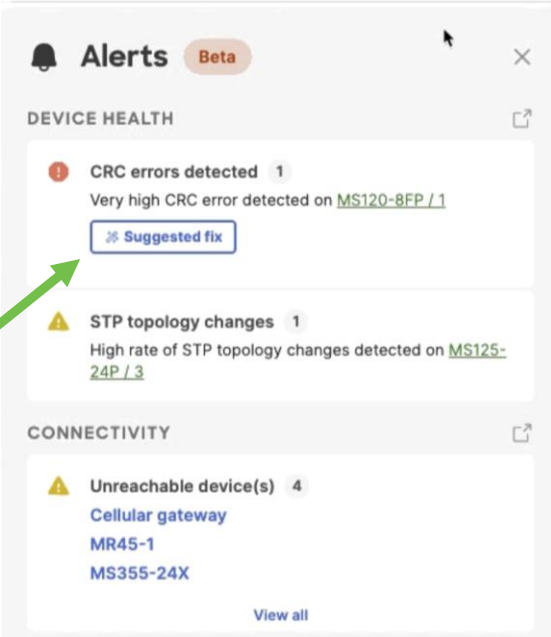


Manual correlation with the data

For instance, CRC errors...



Targeted switching data



Alerts Beta

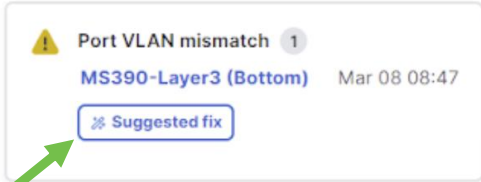
DEVICE HEALTH

- CRC errors detected** 1
Very high CRC error detected on [MS120-8FP / 1](#)
[Suggested fix](#)
- STP topology changes** 1
High rate of STP topology changes detected on [MS125-24P / 3](#)

CONNECTIVITY

- Unreachable device(s)** 4
[Cellular gateway](#)
[MR45-1](#)
[MS355-24X](#)
[View all](#)

A green arrow points from the 'Suggested fix' button in the CRC errors alert to the 'Suggested fix' button in the Port VLAN mismatch alert on the right.



Port VLAN mismatch 1
[MS390-Layer3 \(Bottom\)](#) Mar 08 08:47
[Suggested fix](#)

Switch clients

Total connected switch clients
7

Events and errors

STP events

✓ 0 switches

Loop detection

✓ 0 switches

Active ports with errors

✓ 0 ports

Suggested fixes

< Suggested fix

CRC errors detected
Very high CRC error detected on [MS120-8FP / 1](#)

Results of cable test

✓ The cable is healthy

Tested element	Result
Link	100hdx
Length	39 m
Status	✓
Pair 1	✓
Pair 2	✓

Cancel

Run test again

Next suggestions

< Suggested fix

CRC errors detected
Very high CRC error detected on [MS120-8FP / 1](#)

There are a few suggested fixes for CRC errors.

Suggested fix: Fix speed/duplex mismatch

There is a speed/duplex mismatch between [MS120-8FP / 1](#) and [MS125-24P / 3](#)

Device/port	Link negotiation
MS120-8FP on 1	100 Megabit half duplex (forced)
MS125-24P on 3	100 Megabit full duplex (forced)

Cancel

Fix link negotiation

Suggested fixes

Alerts Beta

CONFIGURATION

Port VLAN mismatch 1
VLAN mismatch error between **MS425 / 31** and **standalone 2 / 1/MA-MOD-4X10G/4**
[Suggested fix](#)

CONNECTIVITY

Unreachable device 1
Standalone 3

[Give your feedback on these alerts](#)

[Add client](#) [Download As](#)

Device type, OS	IPv4 address
	192.168.129.1
	192.168.128.155
	192.168.128.77
	192.168.128.147

Port VLAN mismatch
VLAN mismatch error between **MS425 / 31** and **standalone 2 / 1/MA-MOD-4X10G/4**

Suggested fix: Match VLAN configuration

The recommendation is to match the VLAN settings from standalone 2 / 1/MA-MOD-4X10G/4.

Change log

Port	31	1/MA-MOD-4X10G/4
Device	MS425	standalone 2
Type	Trunk	Trunk
Native VLAN	1	1
Allowed VLANs	1-1000	1-999

[Cancel](#) [Edit manually](#) [Accept suggestion](#)

Port VLAN mismatch
VLAN mismatch error between **MS425 / 31** and **standalone 2 / 1/MA-MOD-4X10G/4**

Result

The changes are saved, and there is no longer a mismatch.

Port	31	1/MA-MOD-4X10G/4
Device	MS425	standalone 2
Type	Trunk	Trunk
Native VLAN	1	1
Allowed VLANs	1-999	1-999

All the wireless data

```
(AP-01) >debug capwap client {ble | detail | efficient-  
upgrade | error | events | flexconnect | info | keepalive  
| payload | pmtu | qos | reassembly | security}
```

```
(Wifi Controller) >debug client 00:00:00:00:00:00
```

```
(Wifi Controller) >debug aaa all enable
```

```
(Wifi Controller) >show debug
```

Reason code comprehension

802.11 Association Status Codes

Code	802.11 definition	Explanation
0	Successful	
1	Unspecified failure	For example : when there is no ssid specified in an association request
10	Channel support not requested capabilities in the Capability Information field	Example Test: Reject when privacy bit is set for WLAN not requiring security
11	Reassociation denied due to inability to confirm that association exists	NOT SUPPORTED
12	Association denied due to reason outside the scope of this standard	Example : When controller receives assoc from an unknown or disabled SSID
13	Responding station does not support the specified authentication algorithm	For example, MFP is disabled but was requested by the client.
14	Received an Authentication frame with authentication transaction sequence number out of expected sequence	If the authentication sequence number is not correct.
15	Authentication rejected because of challenge failure	
16	Authentication rejected due to timeout waiting for next frame in sequence	
17	Association denied because AP is unable to handle additional associated stations	Will happen if you run out of AIDs on the AP; so try associating a large number of stations.
18	Association denied due to requesting station not supporting all of the data rates in the BSSBasicRateSet parameter	Will happen if the rates in the assoc request are not in the BasicRateSet in the beacon.
19	Association denied due to requesting station not supporting the short preamble option	NOT SUPPORTED
20	Association denied due to requesting station not supporting the PBCC modulation option	NOT SUPPORTED
21	Association denied due to requesting station not supporting the Channel Agility option	NOT SUPPORTED
22	Association request rejected because Spectrum Management capability is required	NOT SUPPORTED
23	Association request rejected because the information in the Power Capability element is unacceptable	NOT SUPPORTED
24	Association request rejected because the information in the Supported Channels element is unacceptable	NOT SUPPORTED
25	Association denied due to requesting station not supporting the Short Slot Time option	NOT SUPPORTED
26	Association denied due to requesting station not supporting the DSSS-OFDM option	NOT SUPPORTED

27-31	Reserved	NOT SUPPORTED
32	Unspecified, QoS-related failure	NOT SUPPORTED
33	Association denied because QAP has insufficient bandwidth to handle another QSTA	NOT SUPPORTED
34	Association denied due to excessive frame loss rates and/or poor conditions on current operating channel	NOT SUPPORTED
35	Association (with QBSS) denied because the requesting STA does not support the QoS facility	If the WMM is required by the WLAN and the client is not capable of it, the association will get rejected.
36	Reserved in 802.11	This is used in our code 1 There is no blackbox test for this status code.
37	The request has been declined	This is not used in assoc response; ignore
38	The request has not been successful as one or more parameters have invalid values	NOT SUPPORTED
39	The TS has not been created because the request cannot be honored; however, a suggested TSPEC is provided so that the initiating QSTA may attempt to set another TS with the suggested changes to the TSPEC	NOT SUPPORTED
40	Invalid information element, i.e., an information element defined in this standard for which the content does not meet the specifications in Clause 7	Sent when Aronet IE is not present for a CKIP WLAN
41	Invalid group cipher	Used when received unsupported Multicast 802.11i Out Code
42	Invalid pairwise cipher	
43	Invalid AKMP	
44	Unsupported RSN information element version	If you put anything but version value of 1, you will see this code.
45	Invalid RSN information element capabilities	If WPA/RSN IE is malformed, such as incorrect length etc, you will see this code.
46	Cipher suite rejected because of security policy	NOT SUPPORTED
47	The TS has not been created; however, the HC may be capable of creating a TS, in response to a request, after the time indicated in the TS Delay element	NOT SUPPORTED
48	Direct link is not allowed in the BSS by policy	NOT SUPPORTED
49	Destination STA is not present within this QBSS	NOT SUPPORTED
50	The Destination STA is not a QSTA	NOT SUPPORTED
51	Association denied because the ListenInterval is too large	NOT SUPPORTED
200 (bxCIE)	Unspecified, QoS-related failure. Not defined in IEEE, defined in CCXv4	Unspecified QoS Failure. This will happen if the Assoc request contains more than one TSPEC for the same AC.

201 (bxCIE)	TSPEC request refused due to AP's policy configuration (e.g., AP is configured to deny all TSPEC requests on this SSID). A TSPEC will not be supported by the AP for this reason code. Not defined in IEEE, defined in CCXv4	This will happen if a TSPEC comes to a WLAN which has lower priority than the WLAN priority settings. For example, a Silver TSPEC coming to a Silver WLAN. Only applies to CCXv4 clients.
202 (bxCIE)	Association Denied due to AP having insufficient bandwidth to handle a new TS. This cause code will be useful while roaming only. Not defined in IEEE, defined in CCXv4	
203 (bxCIE)	Invalid Parameters. The request has not been successful as one or more TSPEC parameters in the request have invalid values. A TSPEC SHALL be present in the response as a suggestion. Not defined in IEEE, defined in CCXv4	This happens in cases such as PHY rate mismatch. If the TSRS IE contains a phy rate not supported by the controller, for example. Other examples include sending a TSPEC with bad parameters, such as sending a data rate of 85K for a narrowband TSPEC.

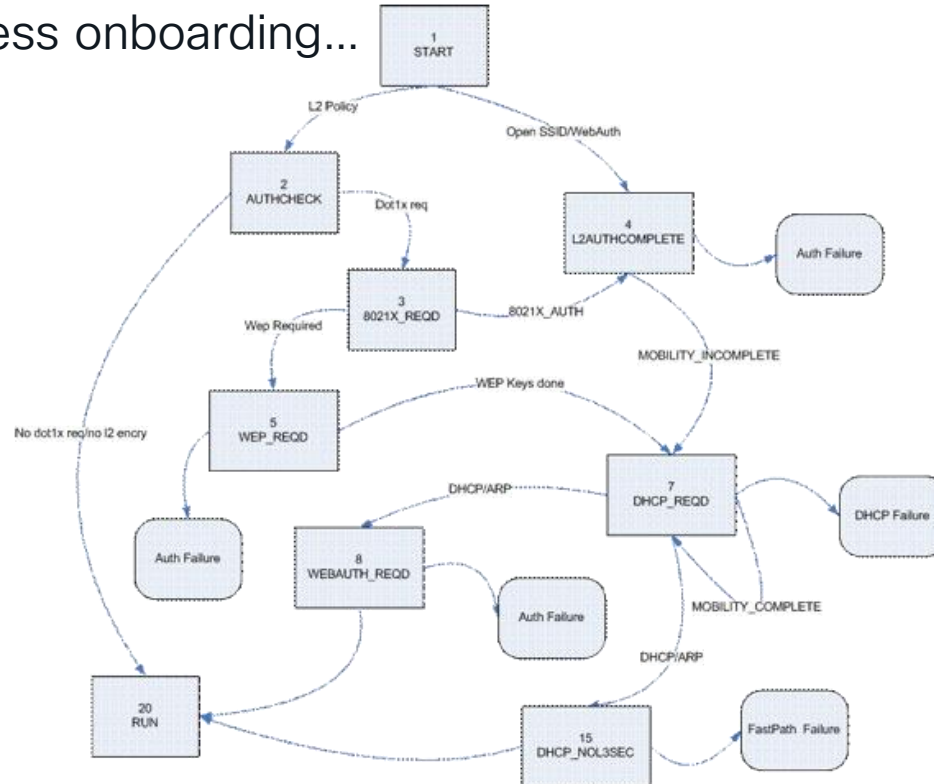
802.11 Deauth Reason Codes

When running a client debug, this code will match the ReasonCode from the output: "Scheduling module for deletion with delete Reason x, reasonCode y"

Code	802.11 definition	Explanation
0	Reserved	NOT SUPPORTED
1	Unspecified reason	TBD
2	Previous authentication no longer valid	NOT SUPPORTED
3	Station is leaving (or has left) BSS or ESS	NOT SUPPORTED
4	Disassociated due to inactivity	Do not send any data after association;
5	Disassociated because AP is unable to handle all currently associated stations	TBD
6	Class 2 frame received from nonauthenticated station	TBD
7	Class 3 frame received from nonassociated station	NOT SUPPORTED
8	Disassociated because sending station is leaving (or has left) BSS	TBD
9	Station requesting (re)association is not authenticated with responding station	NOT SUPPORTED
10	Disassociated because the information in the Power Capability element is unacceptable	NOT SUPPORTED
11	Disassociated because the information in the Supported Channels element is unacceptable	NOT SUPPORTED
12	Reserved	NOT SUPPORTED
13	Invalid information element, i.e., an information element defined in this standard for which the content does not meet the specifications in Clause 7	NOT SUPPORTED
14	Message integrity code (MIC) failure	NOT SUPPORTED
15	4-Way Handshake timeout	NOT SUPPORTED
16	Group Key Handshake timeout	NOT SUPPORTED
17	Information element in 4-Way Handshake different from (Re)Association Request/Probe Response/Reassociation frame	NOT SUPPORTED
18	Invalid group cipher	NOT SUPPORTED
19	Invalid pairwise cipher	NOT SUPPORTED
20	Invalid AKMP	NOT SUPPORTED
21	Unsupported RSN information element version	NOT SUPPORTED
22	Invalid RSN information element capabilities	NOT SUPPORTED
23	IEEE 802.1X authentication failed	NOT SUPPORTED
24	Cipher suite rejected because of the security policy	NOT SUPPORTED
25-31	Reserved	NOT SUPPORTED
32	Disassociated for unspecified, QoS-related reason	NOT SUPPORTED
33	Disassociated because QAP lacks sufficient bandwidth for the QSTA	NOT SUPPORTED
34	Disassociated because excessive number of frames need to be acknowledged, but are not acknowledged due to AP transmissions and/or poor channel conditions	NOT SUPPORTED
35	Disassociated because QSTA is transmitting outside the limits of its TPCPs	NOT SUPPORTED
36	Requested from peer QSTA as the QSTA is leaving the QBSS (or rejoining)	NOT SUPPORTED
37	Requested from peer QSTA as it does not want to use the mechanism	NOT SUPPORTED
38	Requested from peer QSTA as the QSTA received frames using the mechanism for which a setup is required	NOT SUPPORTED
39	Requested from peer QSTA due to timeout	NOT SUPPORTED
40	Peer QSTA does not support the requested cipher suite	NOT SUPPORTED
46-65	Reserved	NOT SUPPORTED
65535		
66	Client deauth	TBD
67	Client deauth	Example: Send a Deauth to the AP with the reason code to be invalid, say zero
68	Used when the reason code sent in a deassoc req or deauth by the client is invalid - invalid length, invalid value etc	

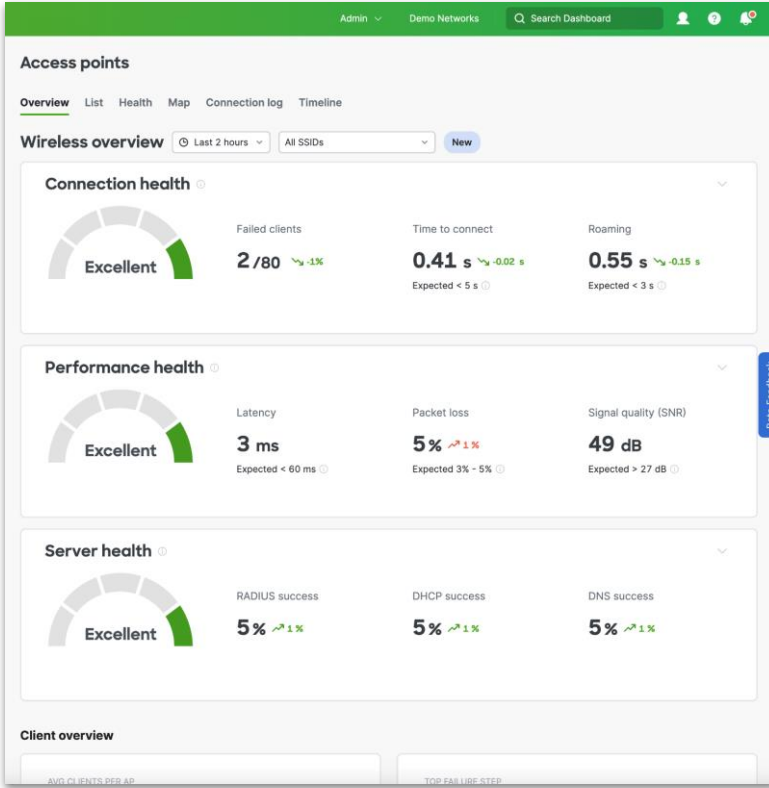
Manual correlation with the data

For instance, wireless onboarding...



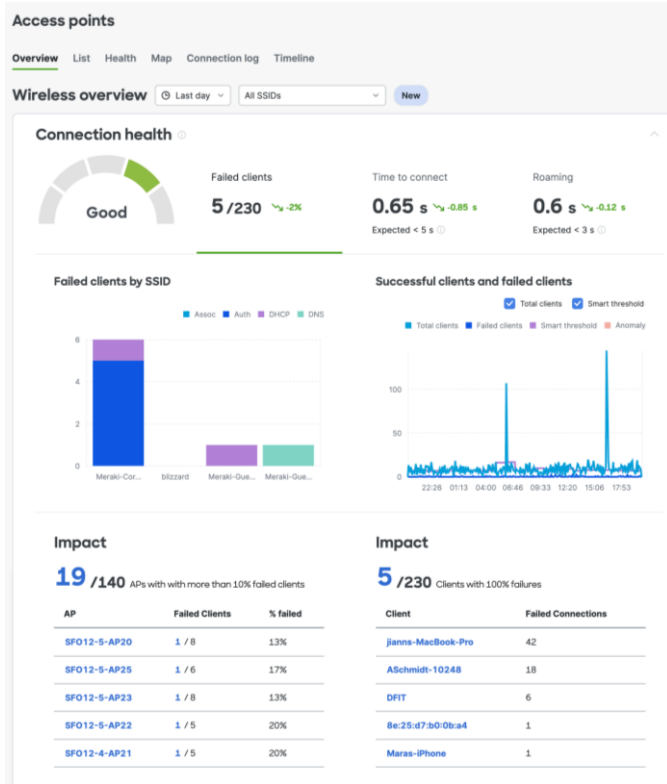
[Understanding Debug on WLAN on Cisco.com](#)

Wireless experience dashboard



- Built-in intelligence
- Easy to grasp views

Connection health



- Simplified 2-click workflow
- Smart threshold – No manual, too high or too low syndrome

☒ Clients fail to connect to the wireless network

☐ Enable smart thresholds

Clients using with failure of ☒ Association ☒ Authentication ☒ DHCP ☒ DNS for more than

Clients using with failure of ☒ Association ☒ Authentication ☒ DHCP ☒ DNS for more than

[Add alert](#)

Server health

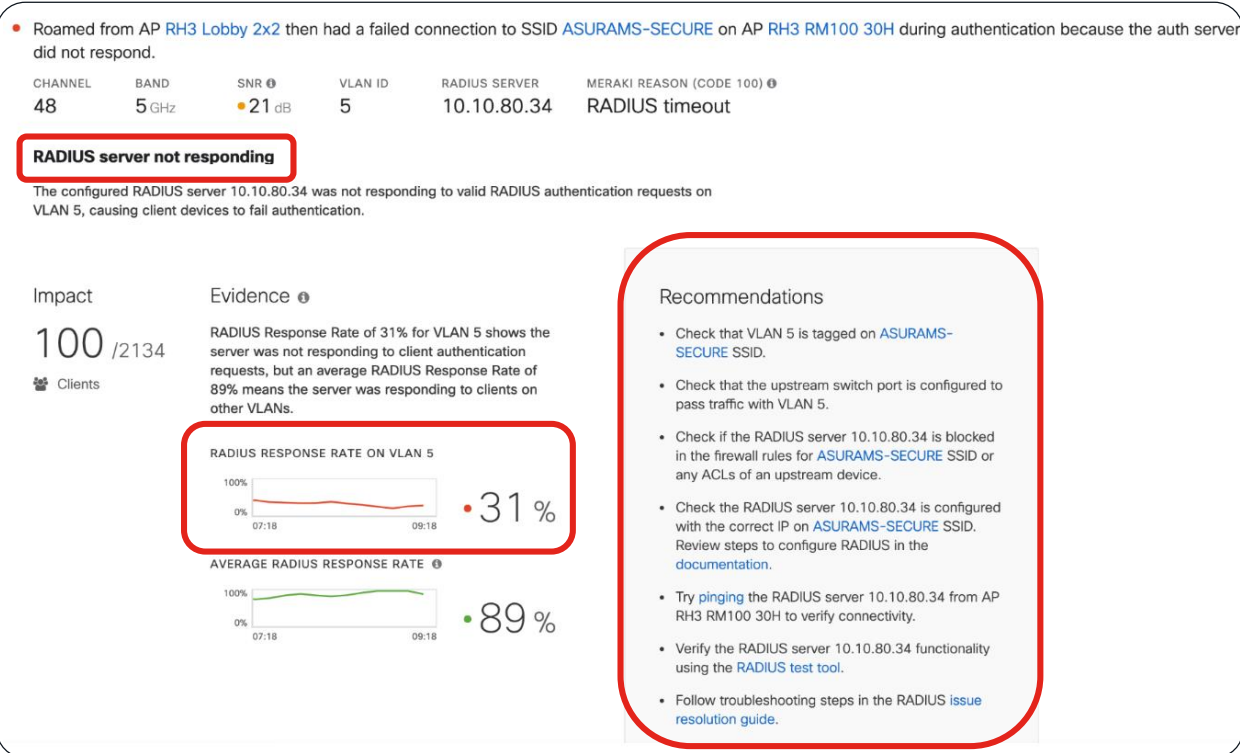


- Network servers – RADIUS, DHCP, DNS
- Top failures brought to your attention

Automated root cause analysis

Impact, evidence, and data-driven recommendations to solve problems

- Natural-language descriptions of client connection behavior



Sticky client analysis

Impact, evidence, and data-driven recommendations to solve problems

- Clear recommendations to remediate detected problems

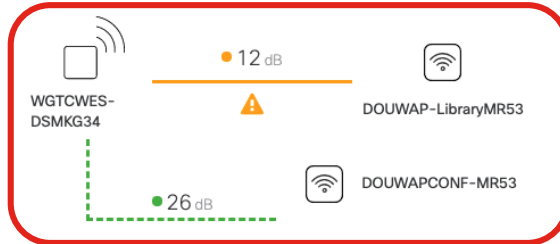
- Poor performance connection to SSID [WGTC-Public](#) for 4 hours on AP [DOUWAP-LibraryMR53](#) due to suboptimal AP selection.

CHANNEL	BAND	SNR ⓘ
11	2.4 GHz	● 12 dB

Sticky Client ⓘ

- Manually disconnect the client and check if it connects to an AP with a stronger signal.

Evidence



Recommendations

Try to force the client to re-select a more optimal AP by having the client disassociate and reassociate.

Note: Client devices choose which AP to connect to. Meraki APs cannot force a client to choose a particular AP. [Read more...](#)

This may temporarily disrupt the client's connection.

[Disconnect client](#)

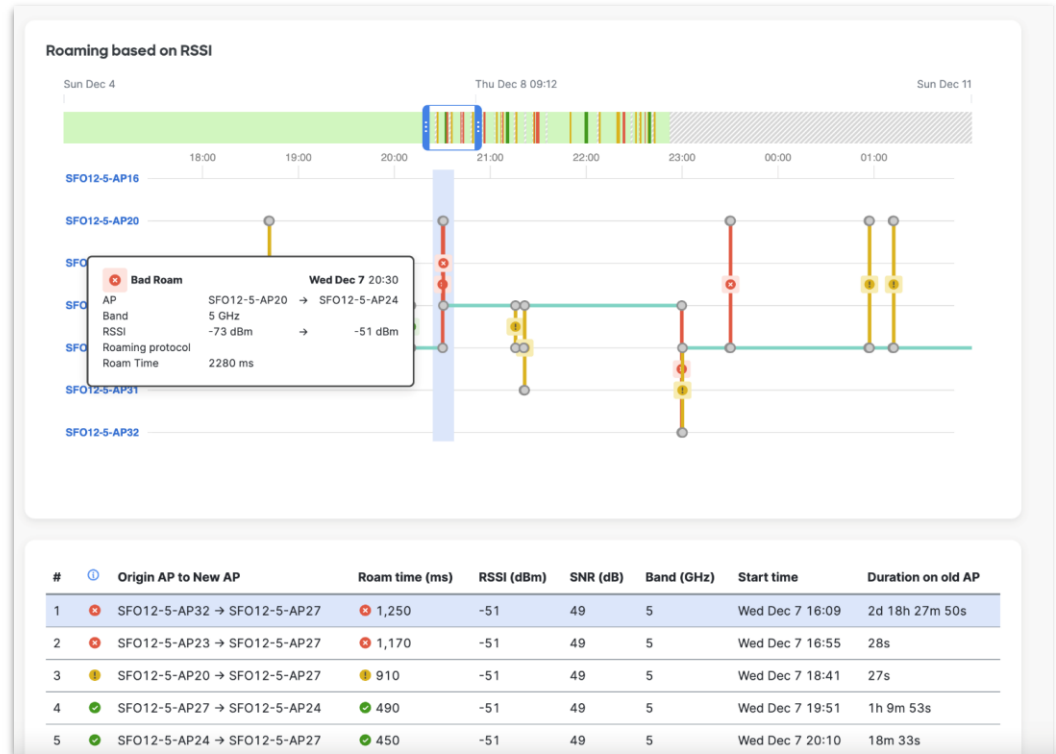
Was this helpful?



Contextual roaming analytics

Impact, evidence, and data-driven recommendations to solve problems

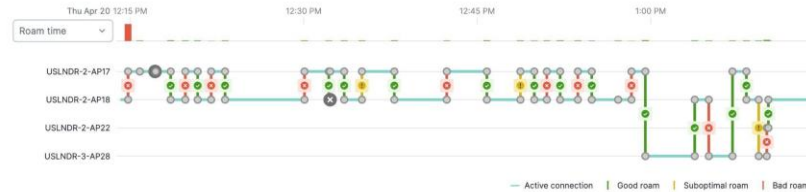
- Tiering of roaming events – good, suboptimal, bad
- Visualization of unique events – sticky or ping-pong clients



Contextual roaming analytics

Impact, evidence, and data-driven recommendations to solve problems

Selected 1 hour



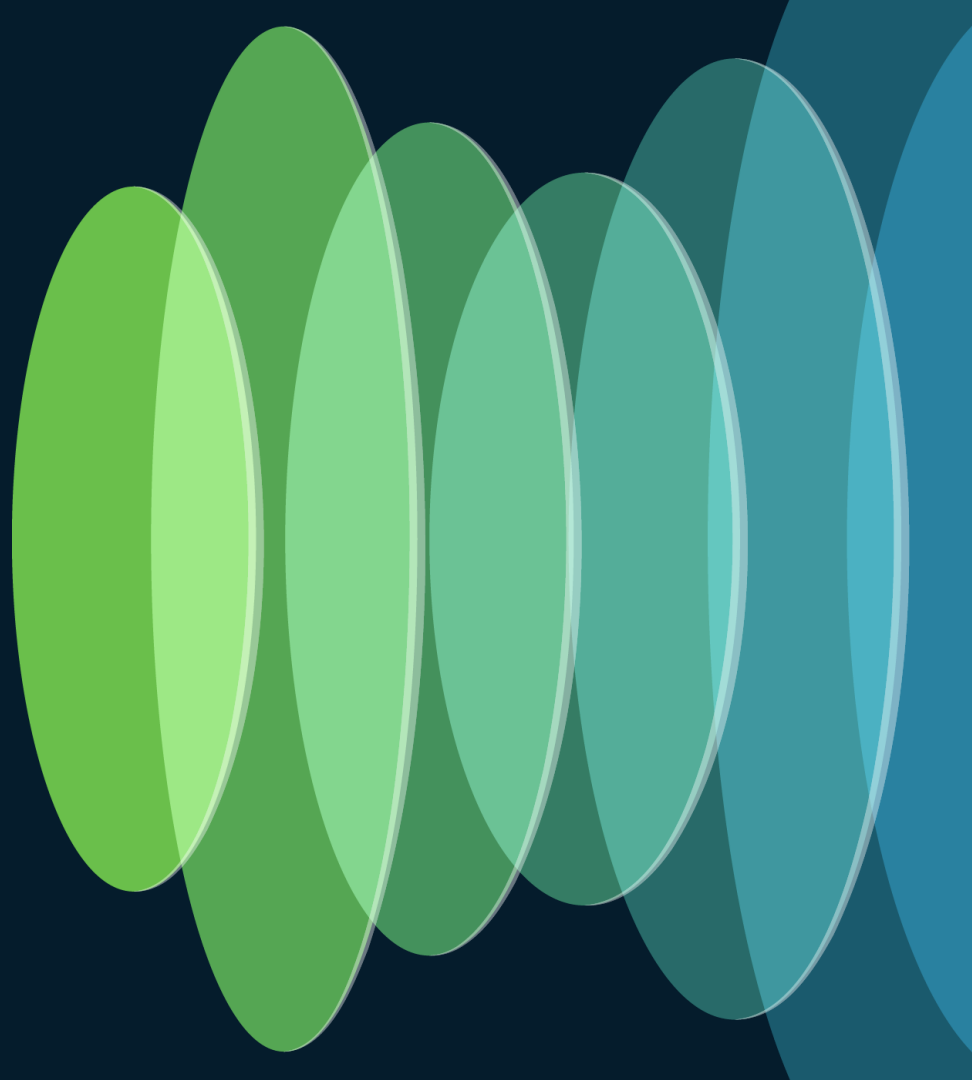
Bad roaming experience

Selected 1 hour



Good roaming experience

Meraki Insight Master



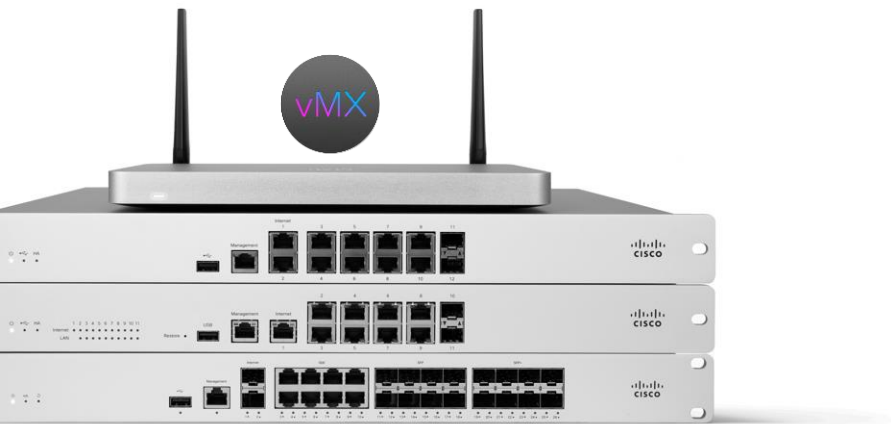


“I play a game to see how long the line behind me will queue up if I play the Cisco on hold music and tell everyone: ‘Shhh, I’m on with TAC...’”

...Me 10 years ago

Meraki Insight building blocks

MX security and SD-WAN appliances



cisco *Live!*

Highlights across all models



Up to x4 WAN ports



3G / 4G / LTE USB as
single-WAN or failover



Models with embedded LTE
modem



High availability mode and
automatic WAN failover



Additional Ethernet ports
with PoE/PoE+ options



Virtual appliances for
hybrid cloud

Insight analytics

Reduce troubleshooting time from hours to minutes



Web App Health

Passive monitoring of critical applications across your LAN, WAN, and application server—wherever it is.



WAN Health

Actively monitor ALL of your organization's diverse uplinks, including cellular, and home-user uplinks, in one view.



VoIP Health

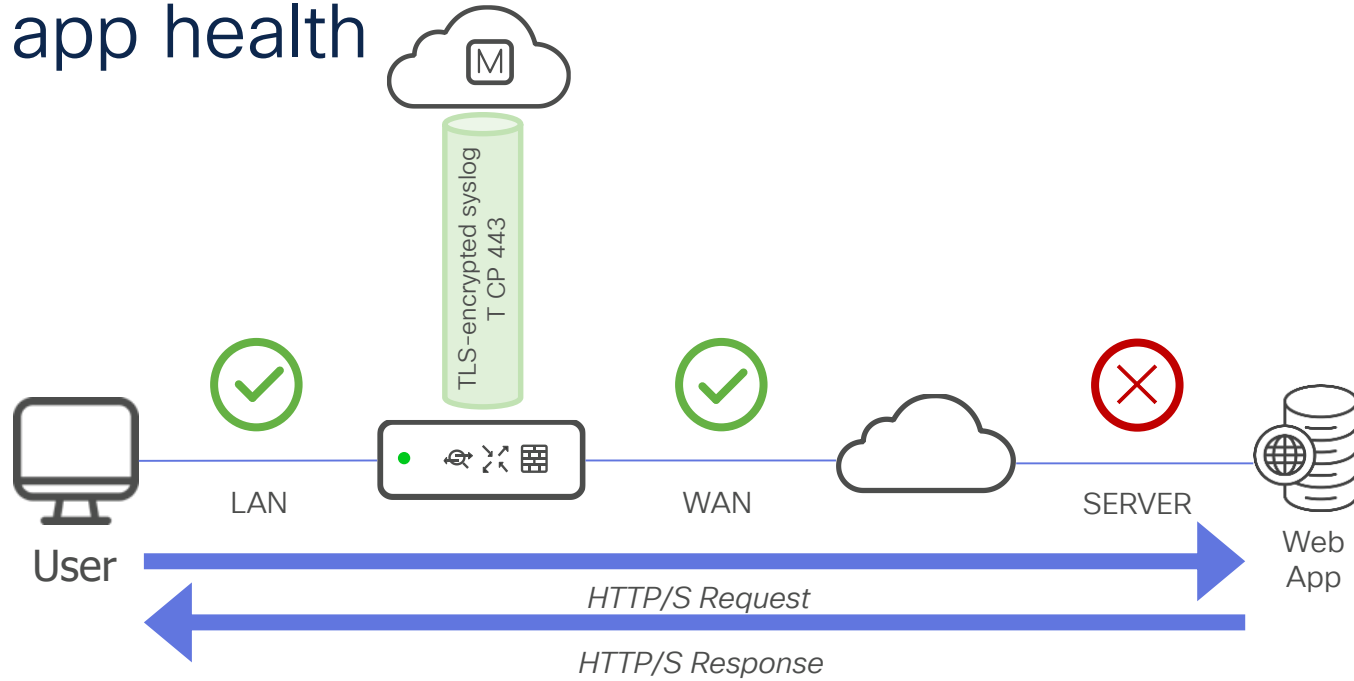
Track VoIP quality by provider and uplink with detailed hop-by-hop analysis actively.



Internet Outages

At-a-glance view of global internet health over the last 24 hours powered by Thousand Eyes.

Web app health

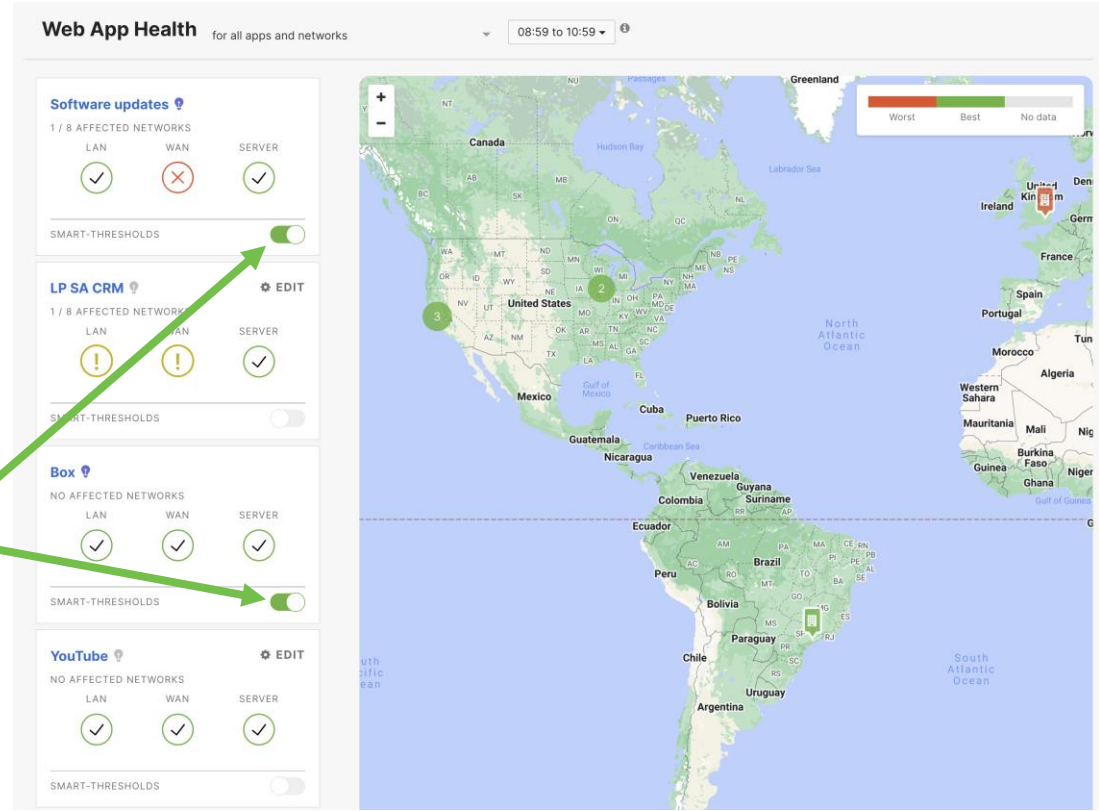


Web app health

- Differentiate performance analytics and troubleshooting between LAN, WAN, and public servers



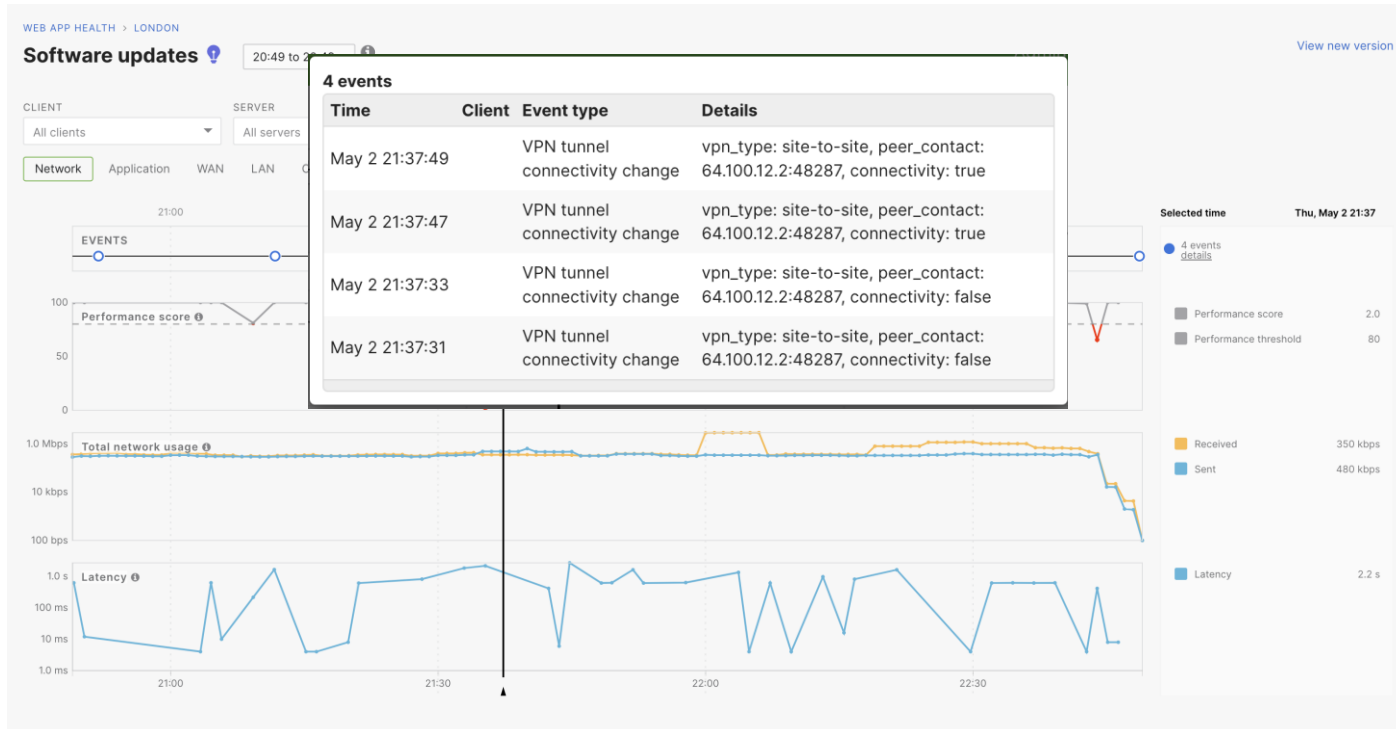
Smart-thresholds for automatic alerting barriers unique for each location



Web app health



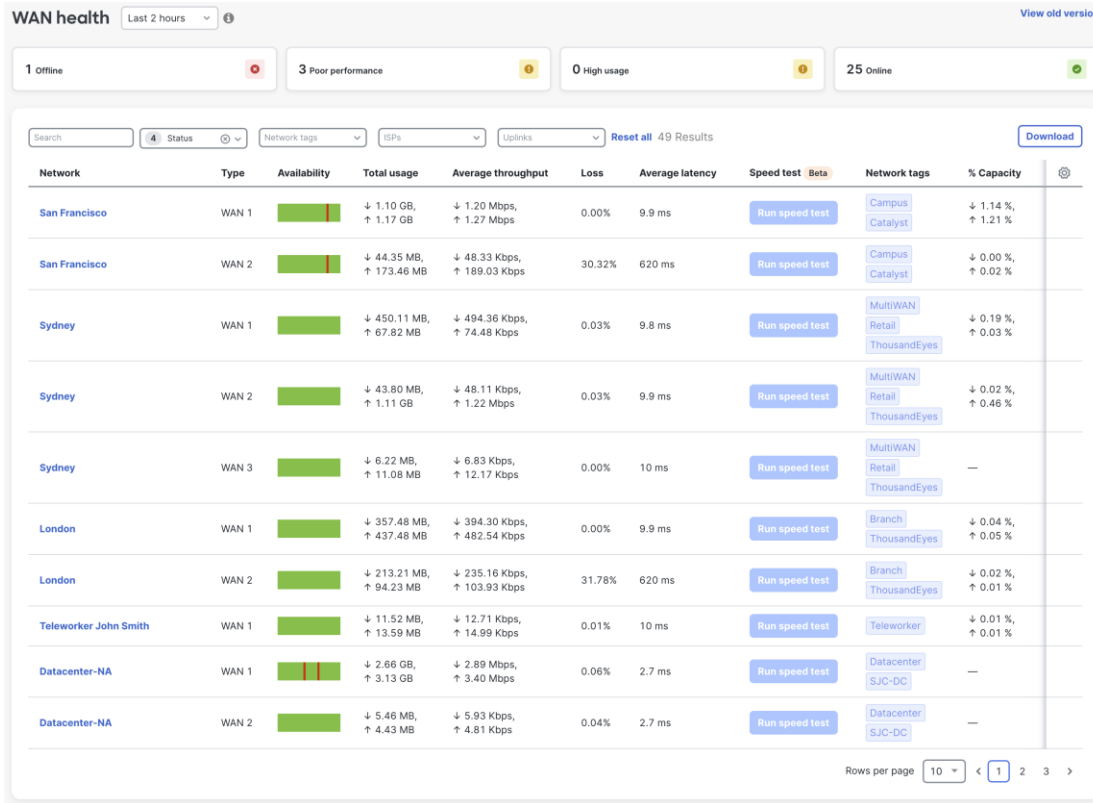
Web app health



Web app health



WAN Health



- At-a-glance for org-wide cellular and uplinks availability

WAN Health

Top contributors to usage

Clients	Applications					Visit client details page
e7712654-d361-47d1-8298-1feef654390f	MV2-Office	SEP3C13CC8343D7	PHASSTED-M-VY96	IP14		
12.17 GB	6.91 GB	6.70 GB	4.11 GB	2.39 GB		
26.6%	15.1%	14.7%	9.0%	5.2%		
Other	Meraki Network OS	Other	Other	Other		

Metrics and connection

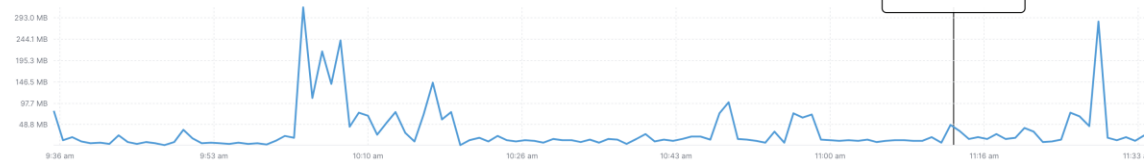
WAN 1

Choose your metrics

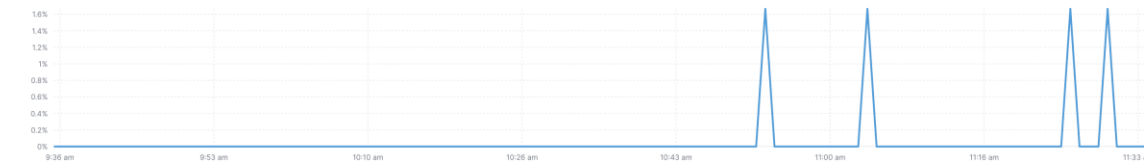
WAN 1 connectivity



Usage

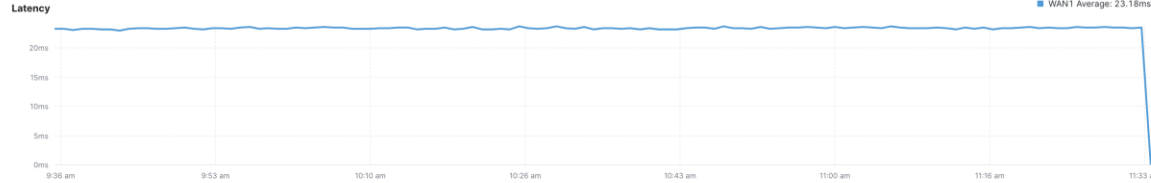


Loss



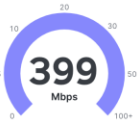
- Quickly isolate ISP issues and cellular failover

WAN Health



- Detailed speed test results included history of previous tests

Download speed test



Download speed history

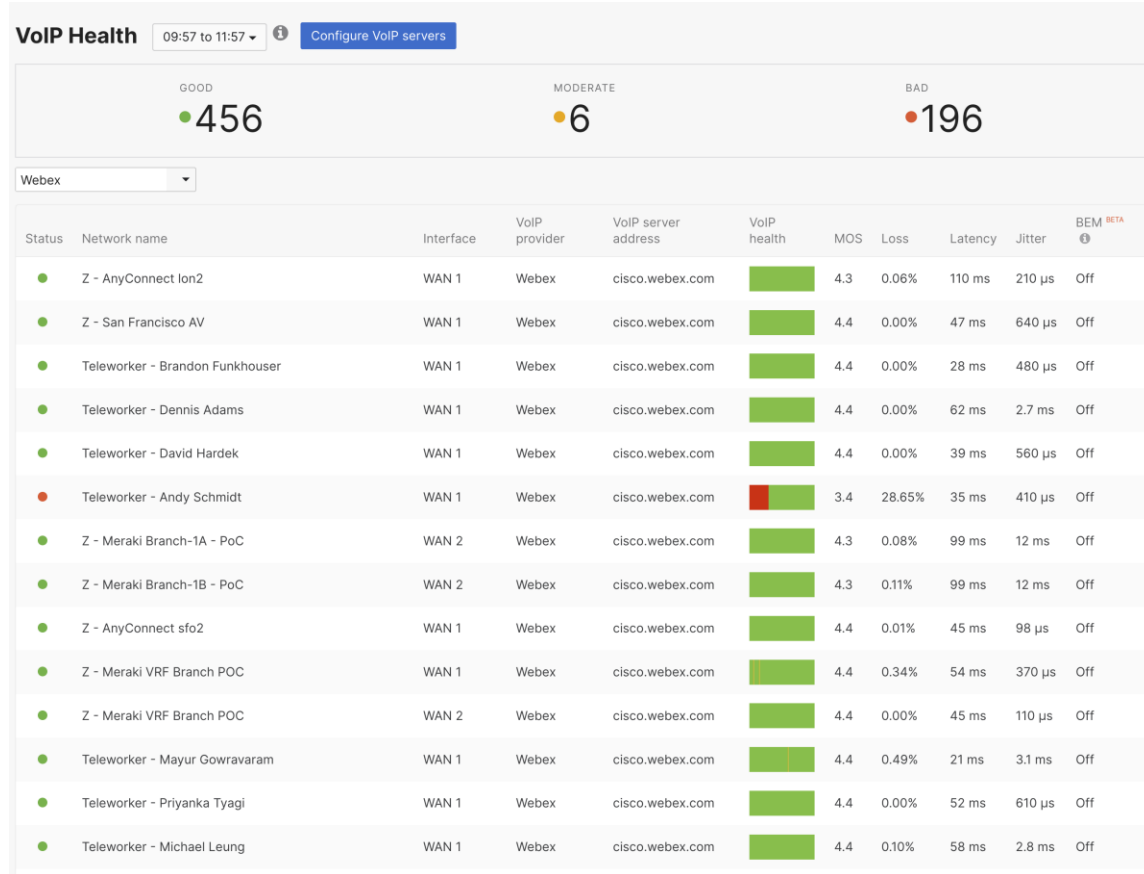
Last 2 hours

Average 350 Mbps



VoIP Health

- Track org-wide performance on SaaS and on-prem VoIP services on all uplinks



VoIP Health

- Quickly identify VoIP degradation via hop-by-hop analysis



VoIP Health

- Quickly identify VoIP degradation via hop-by-hop analysis



Internet Outages

Internet Outages Overview

Outage Events

Refreshed a minute ago

Last 24 hours ▾

Outages

32

Locations

28

Microsoft Corporation
39 minutes ago, affecting 2 locations

Amazon.com, Inc.
39 minutes ago, affecting 1 location

The Corporation for Financing & P...
59 minutes ago, affecting 1 location

Zayo Bandwidth
1 hour ago, affecting 1 location

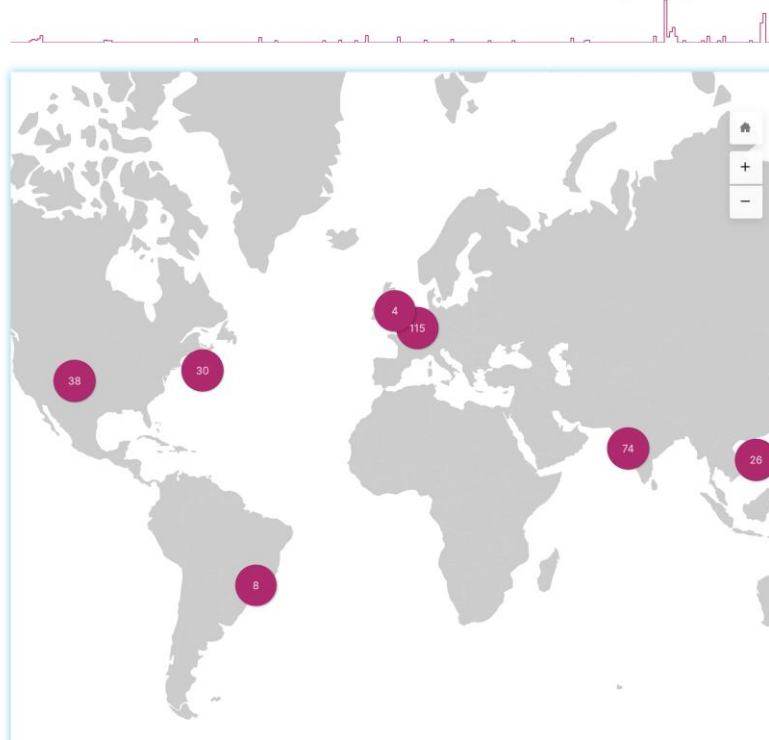
Portlane Network
1 hour ago, affecting 1 location

Microsoft Corporation
2 hours ago, affecting 1 location

Emirates Internet
2 hours ago, affecting 1 location

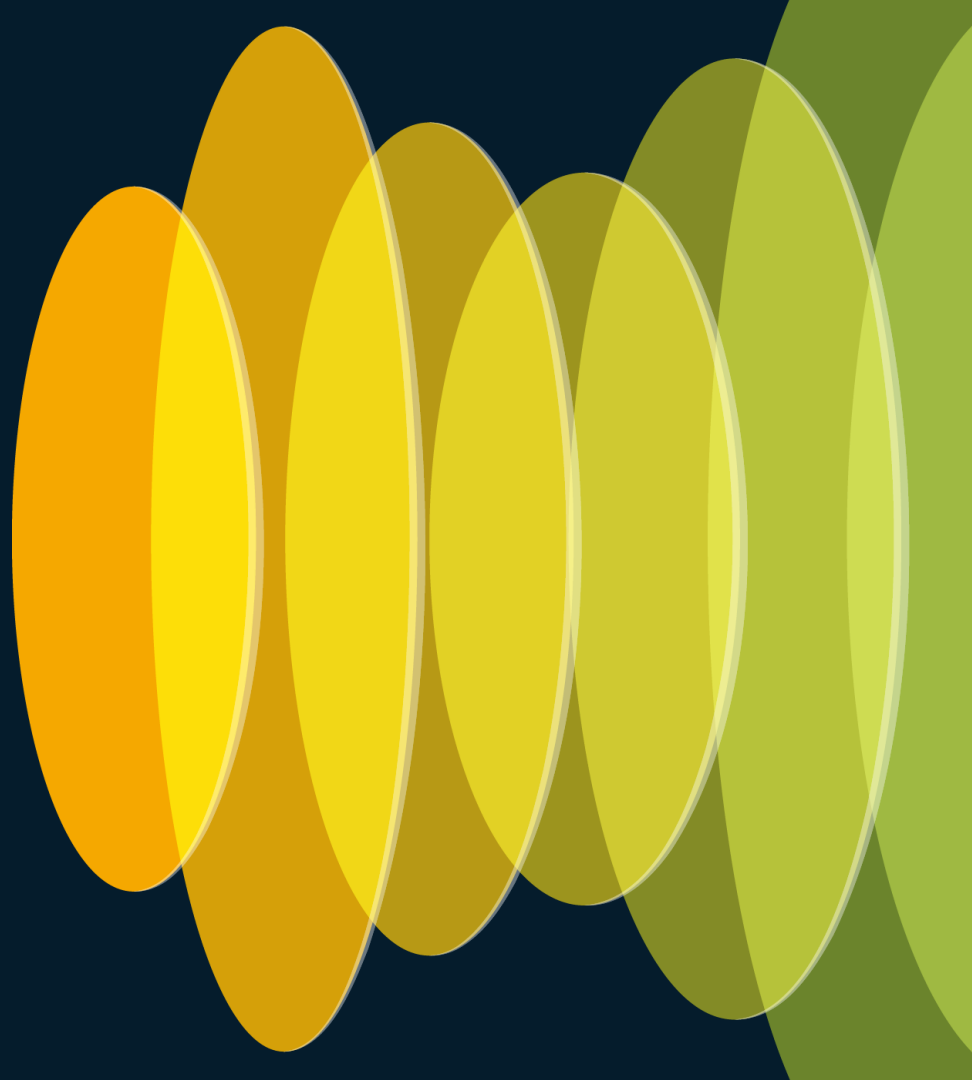
1 - 7 of 32 < >

ThousandEyes
powered by Internet

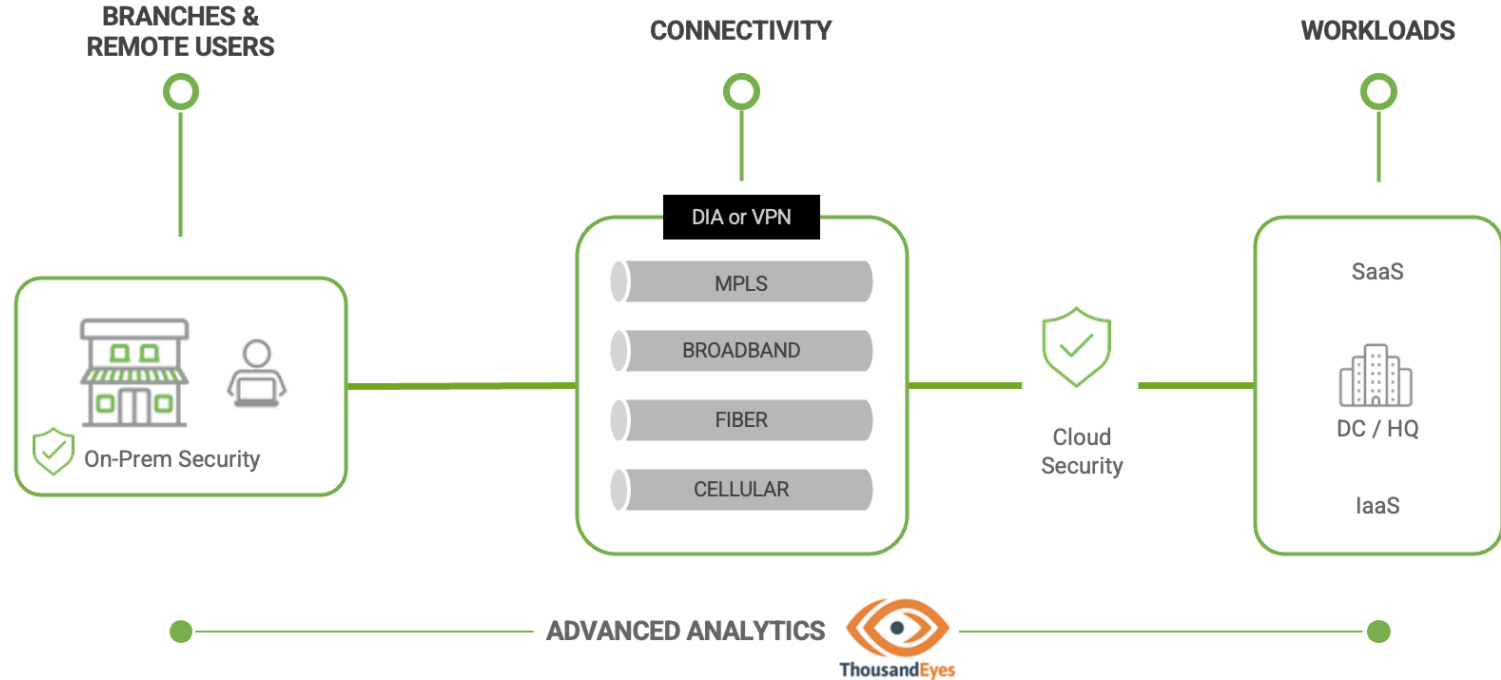


- Global view of ISP outages powered by ThousandEyes
- Evaluate performance of other ISPs in your regional branches

ThousandEyes Power



Active observability across every domain

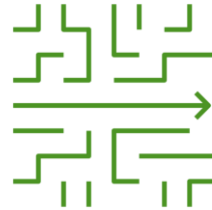


ThousandEyes Agent

Zero additional hardware needed



Always on visibility to monitor critical SaaS applications



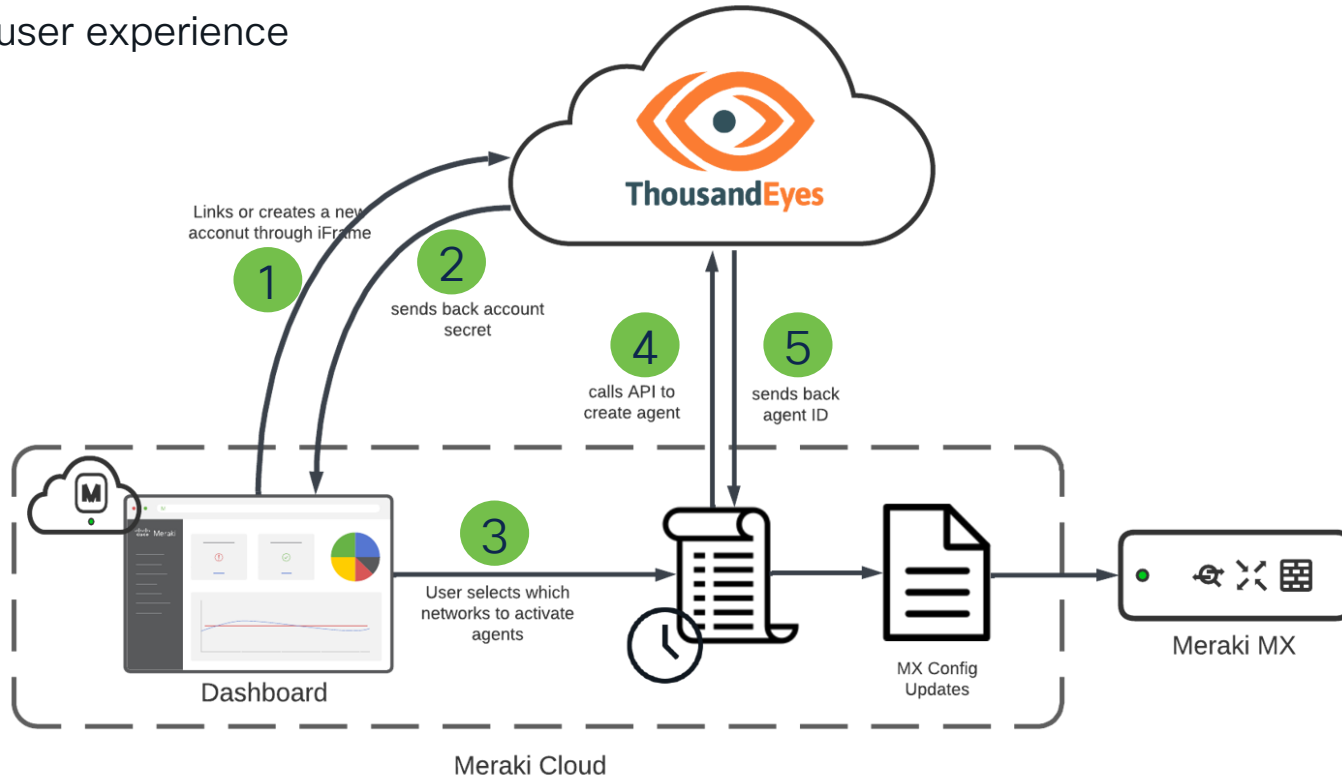
Instantly activate ThousandEyes across your entire MX fleet in minutes



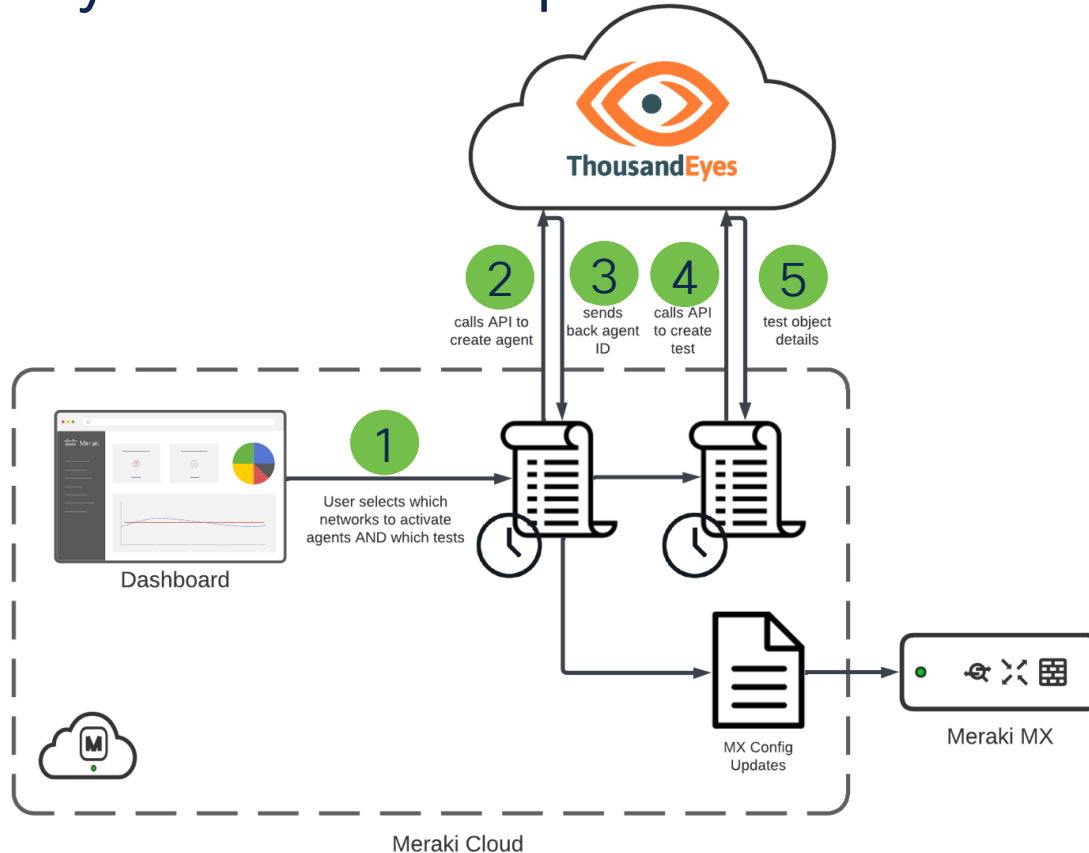
Integration includes 1 free test per SD-WAN+ license (up to 50)

Agent Activation

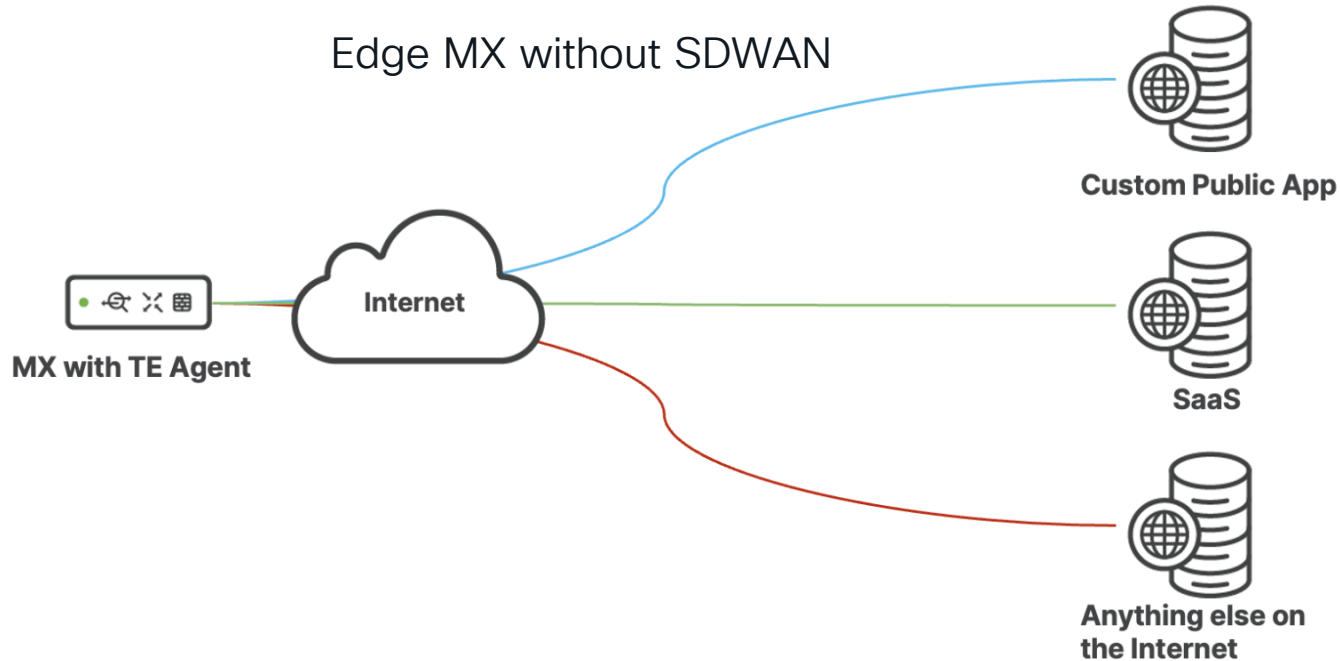
Seamless user experience



ThousandEyes Test Template Creation

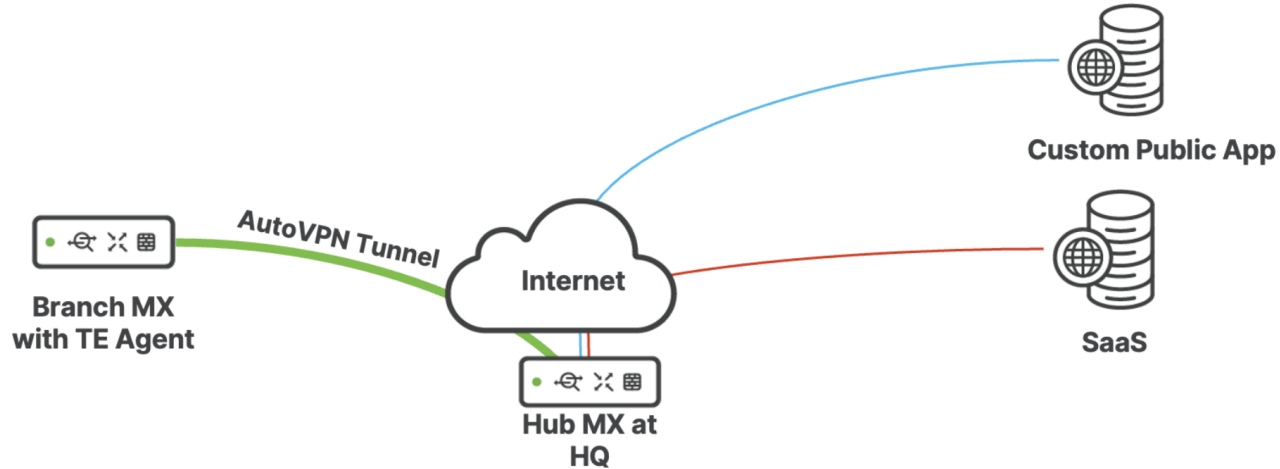


Deployment characteristics

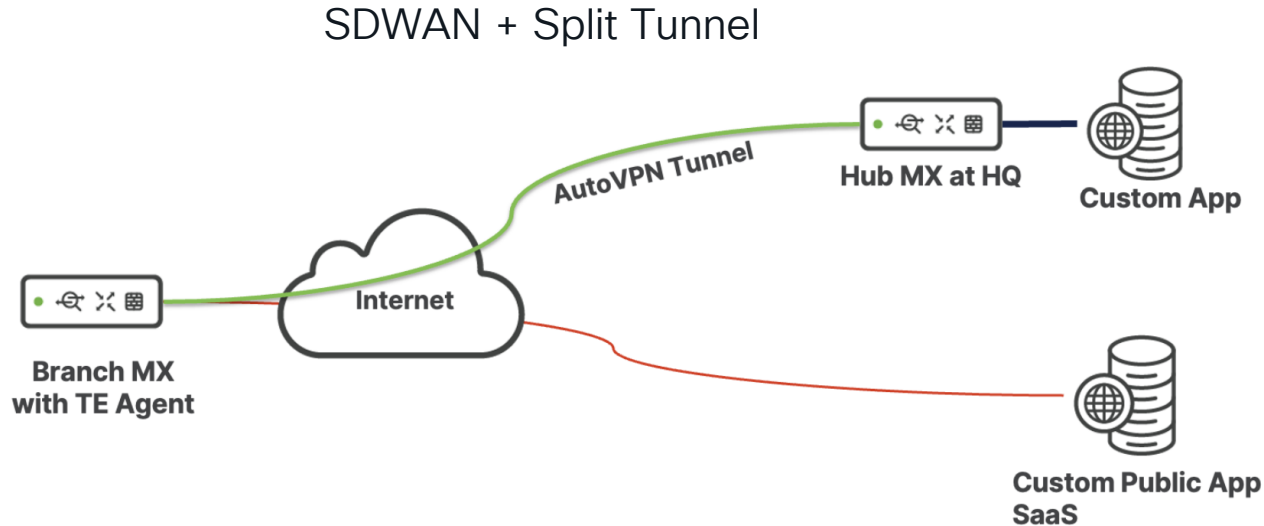


Deployment characteristics

SDWAN + Full Tunnel

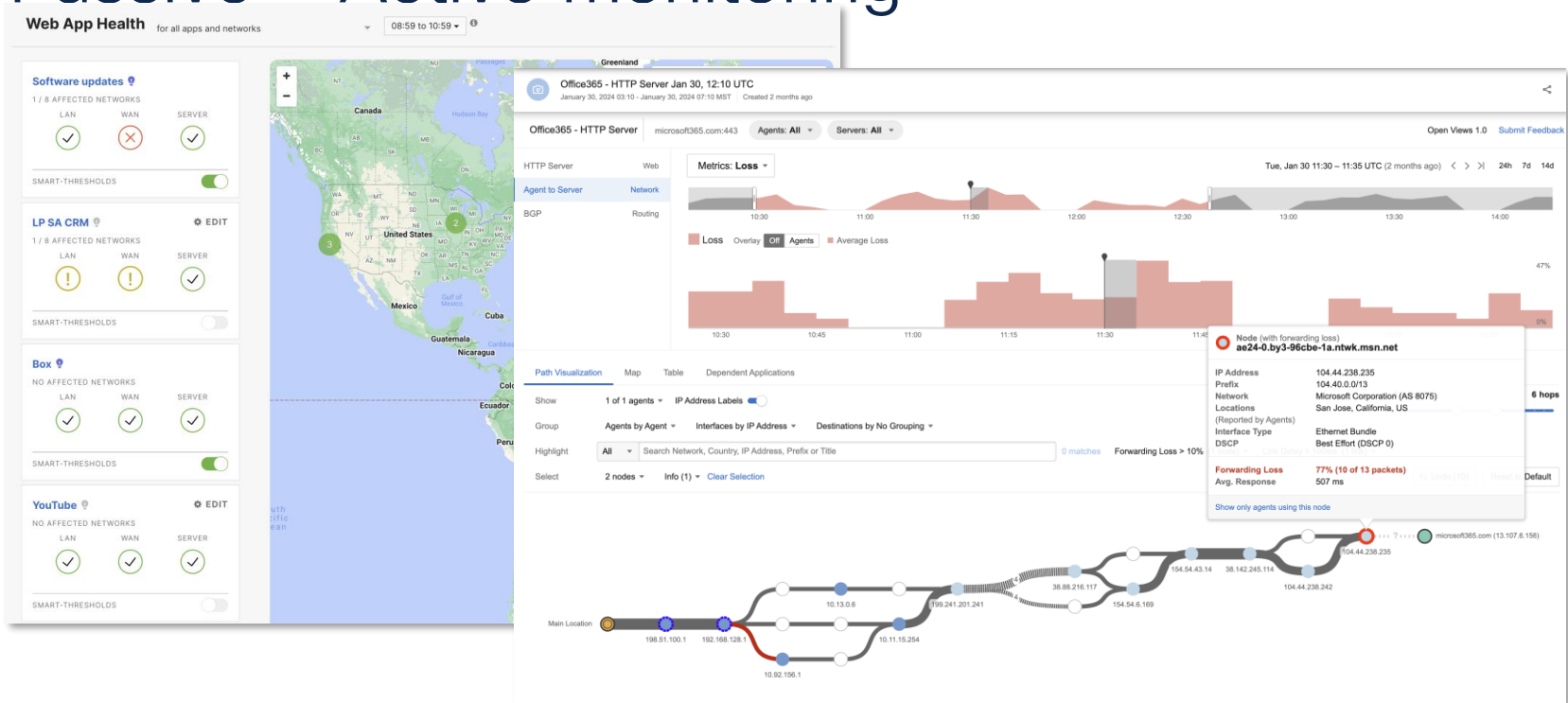


Deployment characteristics



Most Common Deployment

Passive + Active monitoring



Linking accounts between two dashboards

- Simple onboarding user experience
- Supports existing or new ThousandEyes customers
- Built in workflow to create a new account if needed

The screenshot displays the Cisco Meraki dashboard interface. On the left, a sidebar menu lists various network management categories: Network-wide, Cellular Gateway, Security & SD-WAN, Switch, Wireless, Systems Manager, Camera, Environmental, Insight (highlighted), and Organization. The main content area is titled 'Add ThousandEyes to Meraki Insight' and includes a '← Back' link. Below the title, a subtitle reads 'Start monitoring application with ThousandEyes agent testing. [Learn more about ThousandEyes](#)'. The workflow is presented in a multi-step format with a progress indicator on the left showing four steps: 1. Authorize ThousandEyes (active), 2. Select application, 3. Select networks, and 4. Summary. The active step, 'Authorize ThousandEyes', contains the following content: a ThousandEyes logo, the heading 'Authorize ThousandEyes access to Meraki', a section titled 'ThousandEyes will have access to:' listing 'Name and email' and 'Network names', a checkbox labeled 'By authorizing ThousandEyes access, you agree to be subject to Cisco's Terms and Conditions.' which is checked, and two buttons at the bottom: 'Log into an existing account' and 'Create a new account'. At the bottom of the main content area, there are 'Cancel' and 'Next' buttons, with a status message 'All changes saved'.

Activate application tests

Monitor Critical Applications for SD-WAN Beta

✓ Connect ThousandEyes
ThousandEyes authorized

2 Select application
Cisco WebEx


3 Configure monitoring


4 Select networks


5 Summary


Select application


Choose an application to monitor with enhanced application monitoring.


 Office 365 Suite


 Office 365 Sharepoint


 Cisco WebEx

 Zoom

 Box

 Salesforce

 Amazon Web Services

 Add a custom application

Cancel

Back

Next

Activate agents: Select via tags

Network

Nook-HQ-SF

Network-wide

Cellular Gateway

Security & SD-WAN

Switch

Wireless

Systems Manager

Camera

Environmental

Insight

Organization

← Internet monitoring

Add ThousandEyes to Meraki Insight

Start monitoring application with ThousandEyes agent testing. [Learn more about ThousandEyes](#)

1 Select application
Office 365

2 Select networks

3 Review selection

Select networks

Select your existing networks to monitor. The more networks, the better the results.

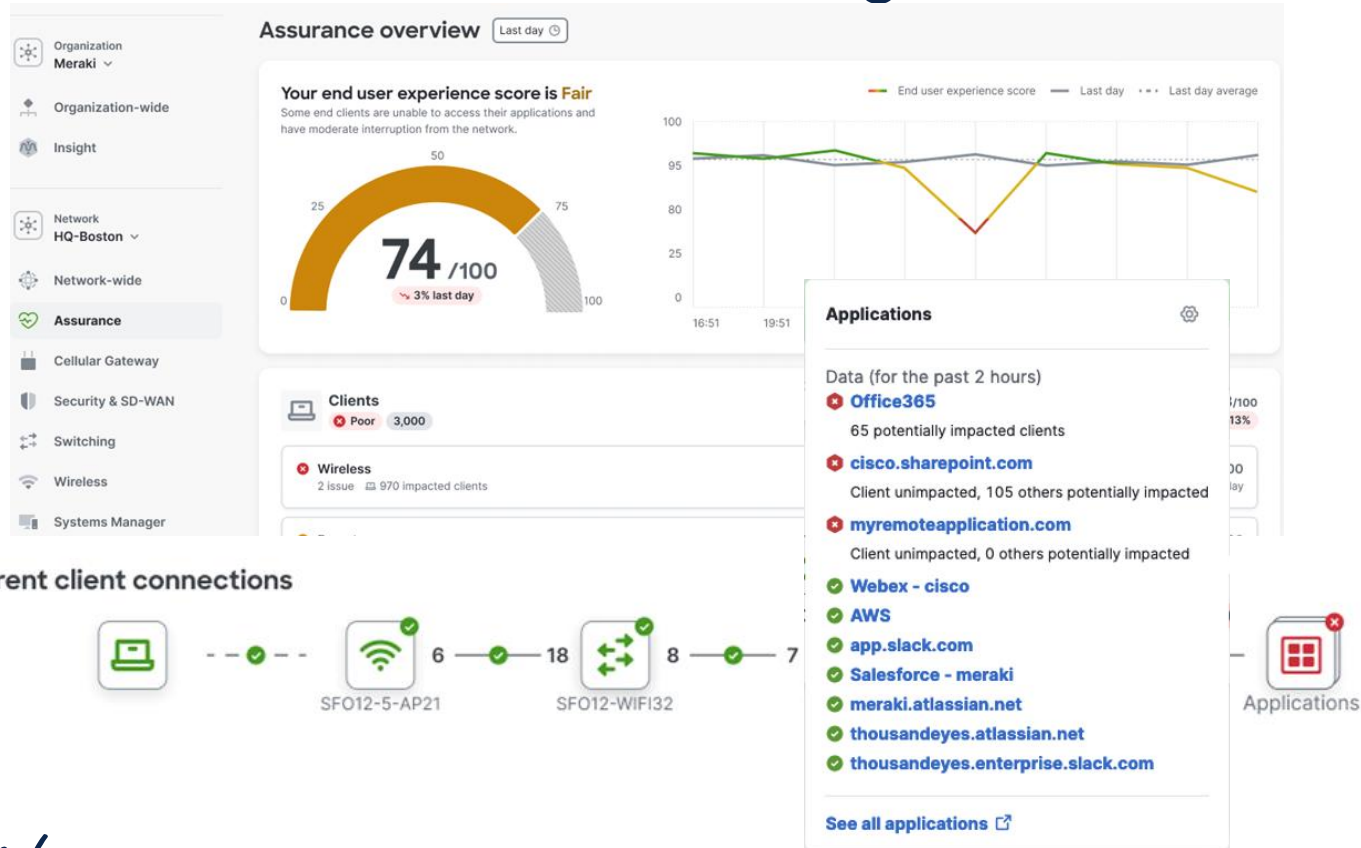
Q Search by network name Network tags 138 networks

Network	Network tags
<input checked="" type="checkbox"/> Meraki Chicago - Post Office CHG12	Office Chicago Branch
<input checked="" type="checkbox"/> Meraki Chicago - Data Center	Office Chicago Branch
<input checked="" type="checkbox"/> Meraki London - Post Office LON12	Office London Branch
<input checked="" type="checkbox"/> Meraki London - Bishopsgate LON16	Office London Branch
<input checked="" type="checkbox"/> Meraki London - Finsbury LON11	Office London Branch
<input checked="" type="checkbox"/> Network name generic	Office California San Francisco
<input checked="" type="checkbox"/> Network name generic	Office California San Francisco
<input checked="" type="checkbox"/> Network name generic	Office California San Francisco
<input checked="" type="checkbox"/> Network name generic	Office California San Francisco

Cancel All changes saved Back Next

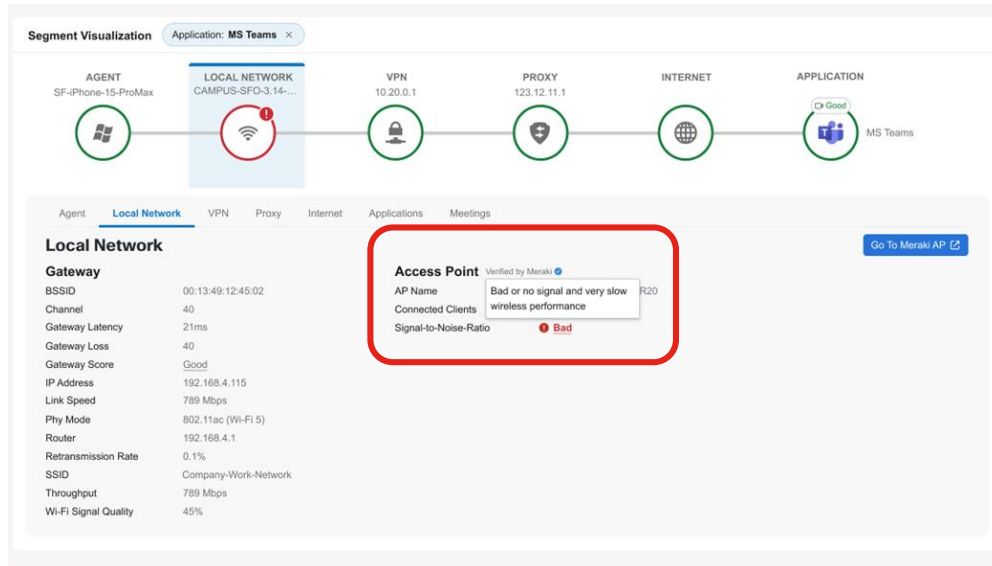
- Compatible networks will auto-populate (MX model and firmware dependence)
- Select networks individually or en masse

Meraki bi-directional data integration

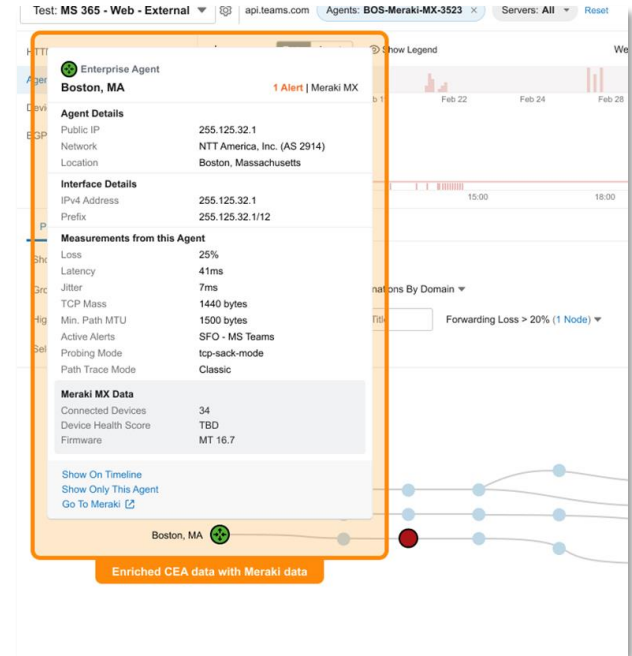


ThousandEyes enriched with Meraki data

Endpoint wireless health
powered by Meraki MR



Path visualization with
Meraki MX health data



Continue your education

- Visit the Cisco Showcase
DEMO 5 or **AI Hub**
- Book your one-on-one
Meet the Engineer meeting
- Attend the interactive education
with DevNet, Capture the Flag,
and Walk-in Labs
- Visit the On-Demand Library
for more sessions at
www.CiscoLive.com/on-demand

Contact me at: phassted@cisco.com

“Wrap it up, Hasstedt!”

Everyone in this room
...probably ;)

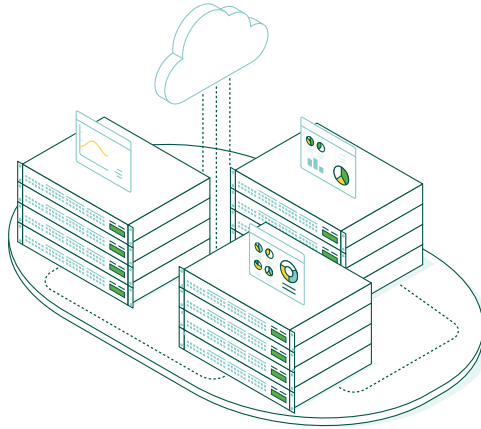


Conquer the tsunami of data



Device Health:

Targeted and correlated data, with recommended fixes has never been easier to navigate



Meraki Insight: Differentiate issues between LAN/WAN/Server and reduce troubleshooting time with passive monitoring



Meraki + ThousandEyes:

Always-on, active monitoring for critical SaaS infrastructure that deploys effortlessly on your existing MXs



What have we learned?

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn **exclusive prizes!**



Complete your surveys in the **Cisco Live mobile app**.



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive