



The bridge to possible

# Meraki Observability

Be the hero, avoid the blame game

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

“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 ;)





CISCO *Live!*

@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?

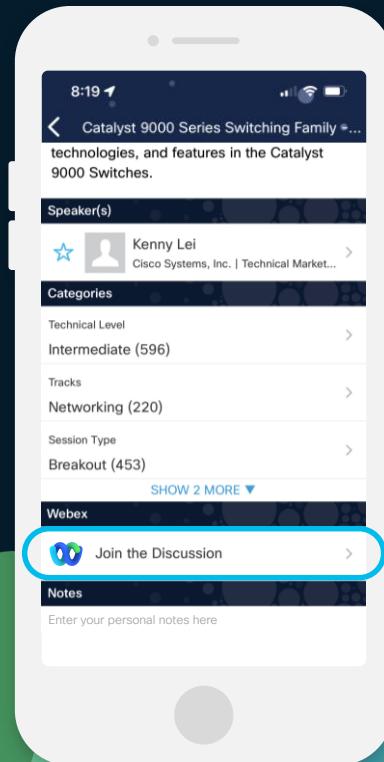
Use Cisco Webex App to chat with the speaker after the session

## 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.

[https://ciscolive.ciscoevents.com/  
ciscoalivebot/#BRKOPS-2013](https://ciscolive.ciscoevents.com/ciscoalivebot/#BRKOPS-2013)





# 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!**

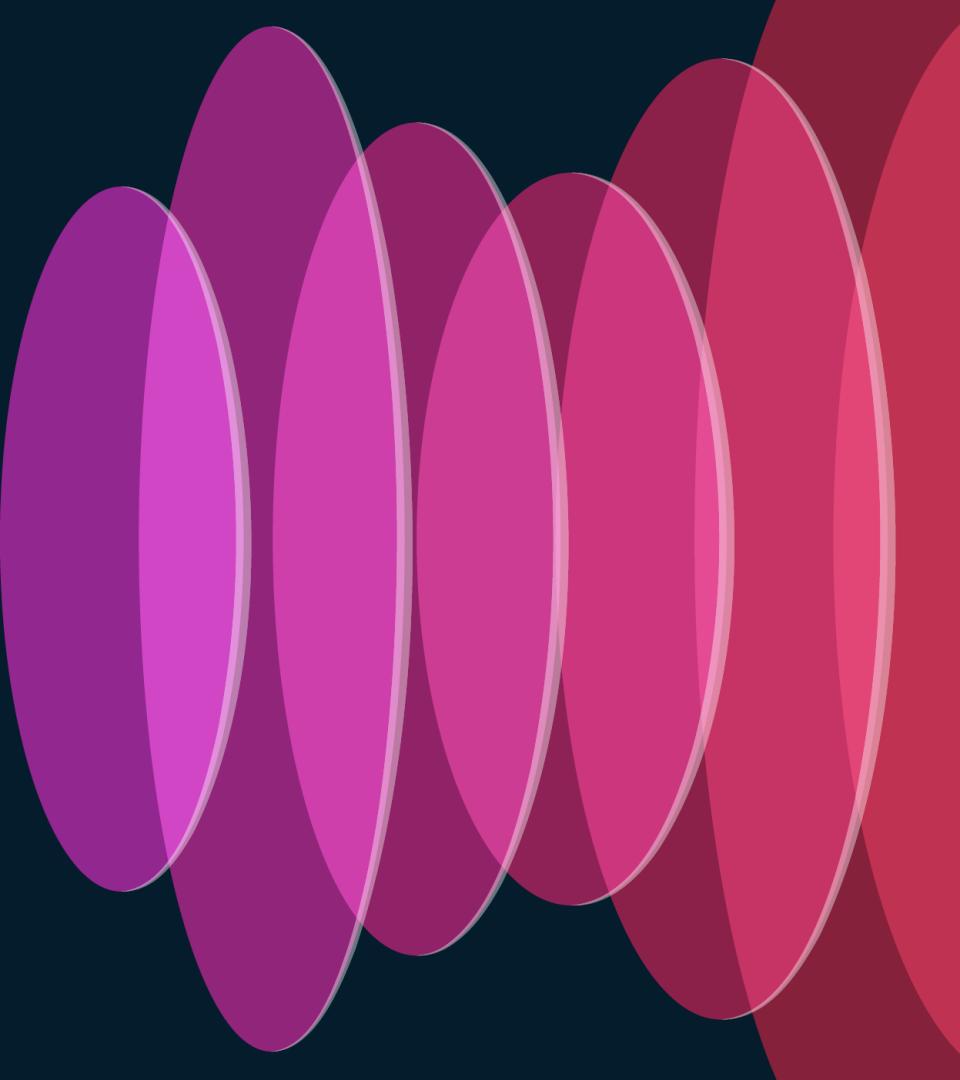
Source: [Forrester Report](#)



## 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 ]
```

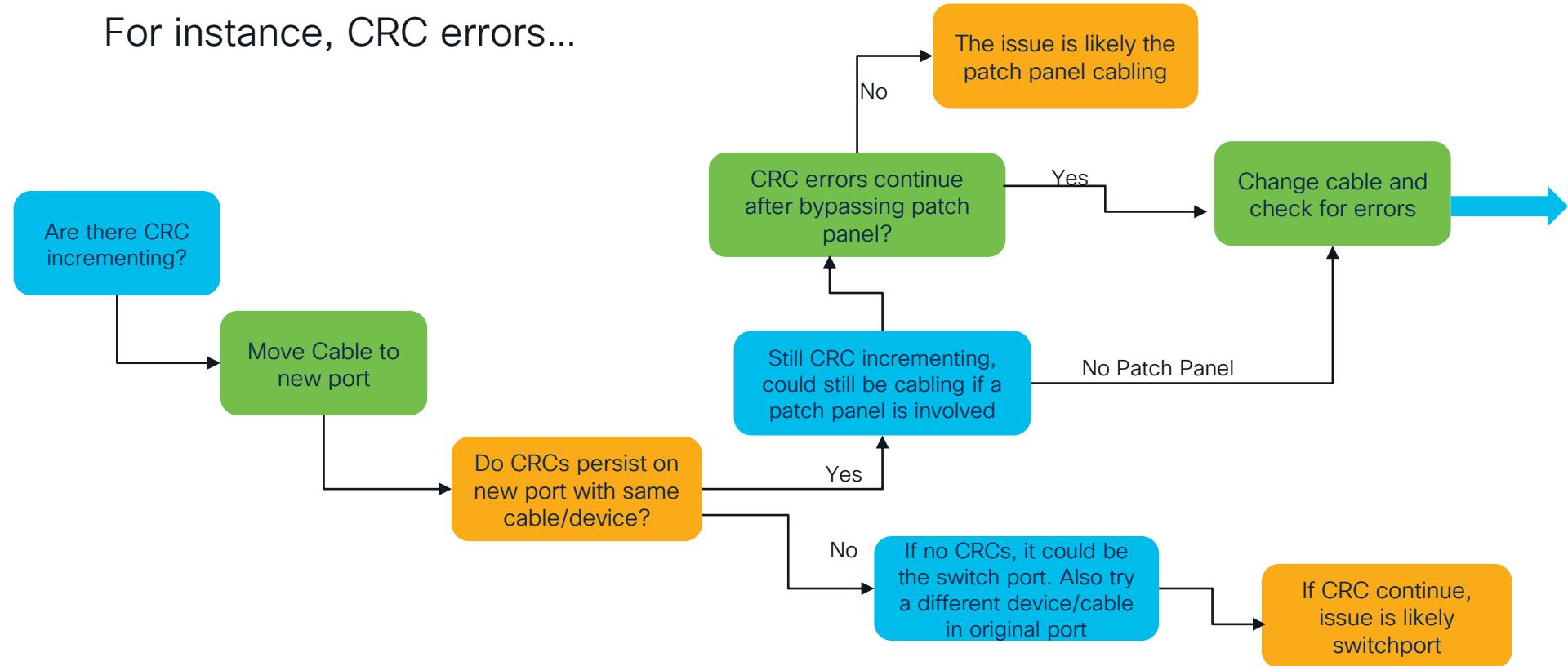
```
Switch# show vlan [ brief | group | id vlan-id | group-name WORD user_count | mtu | name vlan-name | remote-span | summary ]
```

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

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

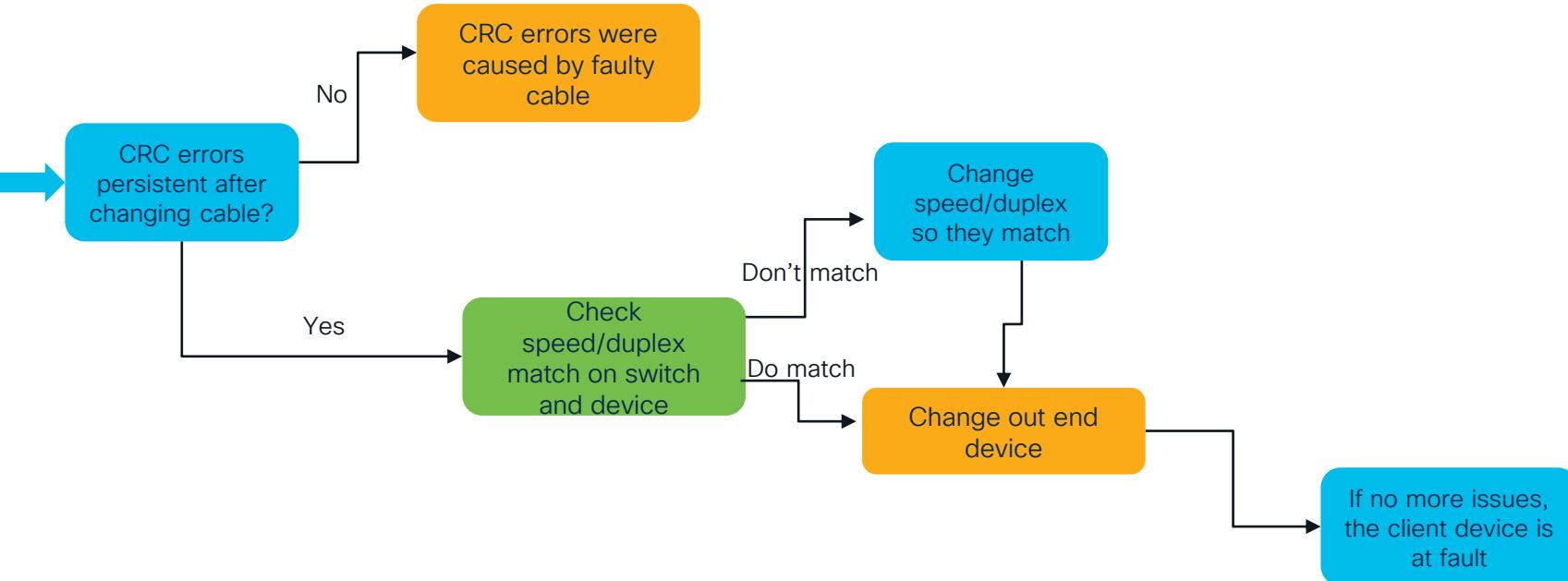
# Manual correlation with the data

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](#)

**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

The screenshot shows the Cisco Cloud Network Controller (CCNC) interface. In the top navigation bar, there are links for Announcements, Help, and a user profile. The main area is titled "Alerts (Beta)".

**CONFIGURATION**

- Port VLAN mismatch** (1): VLAN mismatch error between MS425 / 31 and standalone 2 / 1/MA-MOD-4X10G/4. A "Suggested fix" button is present.

**CONNECTIVITY**

- Unreachable device** (1): Standalone 3.

Below the alerts, there is a timeline from 00 to 08:00 with a "More" button. A "Give your feedback on these alerts" link is available. At the bottom, there are "Add client" and "Download As" buttons, and a search bar for "Device type, OS" with an "IPv4 address" input field.

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

**Suggested**

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

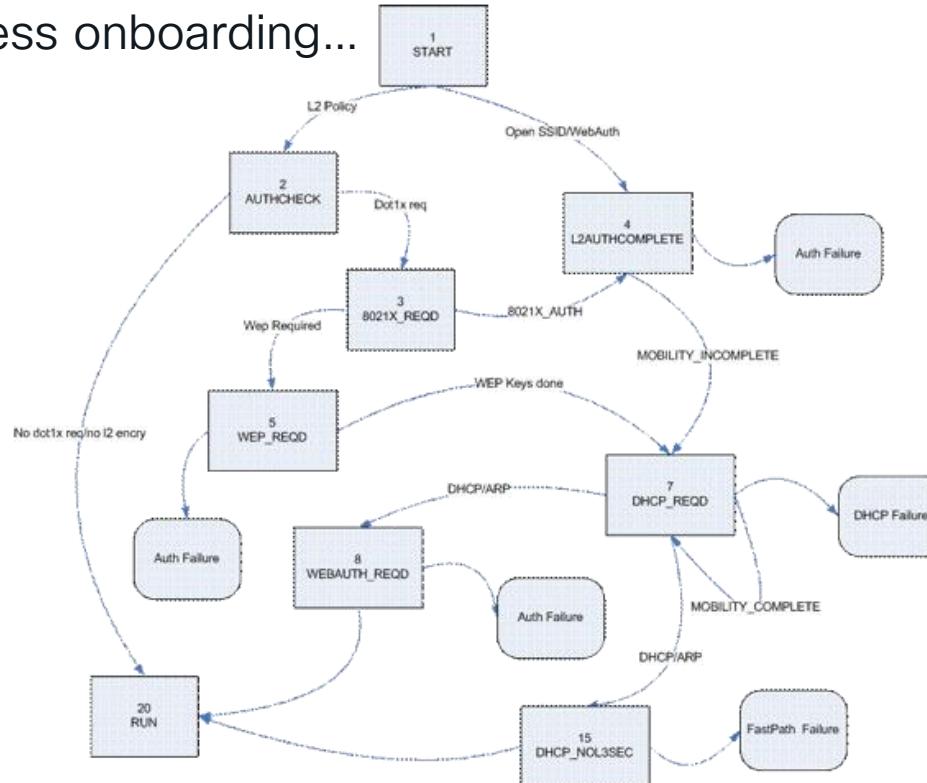
Code	802.11 definition	Explanation
0	Successful	
1	Unspecified failure	For example : when there is no ssid specified in an association request
10	Cannot support all requested capabilities in the Capability Information field	Example Test: Reject when privacy bit is set for WLAN not requiring security
11	Reassociation denied due to inability to confirm that the 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 BSSBasicRateSet parameter
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 QoS) 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 ! 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 Aironet IE is not present for a QIP WLAN
41	Invalid group cipher	Used when received unsupported Multicast 802.11i OUI 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 (0x0B)	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 (0x0C)	TSPEC request refused due to AP's policy configuration (e.g., AP may refuse to deny all TSPEC requests in a TS, or TSPEC will not be supported by the AP for this reason etc). 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 Voice TSPEC coming to a Silver WLAN. Only applies to CCXv4 clients.
202 (0x0D)	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 (0x0E)	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 date of BSS for a narrowband TSPEC.
802.11 Deauth Reason Codes		
When running a client debug, this code will match the ReasonCode from the output: "Scheduling mobile for deletion with delete Reason x, reasonCode y"		
Code	802.11 definition	Explanation
0	Reserved	NOT SUPPORTED
1	Link integrity reason	TBD
2	Precious 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 3 frame received from nonauthenticated station	
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 disassociation is not authenticated with responding station	NOT SUPPORTED
10	Disassociated because the information in the Power Capability element is unacceptable	NOT SUPPORTED
11	Link integrity 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)Associate Request/Probe Response/Beacon frame	NOT SUPPORTED
18	Invalid group cipher	NOT SUPPORTED
19	Invalid pairwise cipher	NOT SUPPORTED
20	Invalid AKMP	NOT SUPPORTED
21	Unspecified 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 TONPs	NOT SUPPORTED
36	Requested from peer QSTA as the QSTA is leaving the QBSS (or resetting)	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
45-6535	45-6535 Reserved	NOT SUPPORTED
6536	Cisco defined	TBD
6537	Cisco defined	Used when the reason code sent in a deassoc req or deauth by the client is invalid - invalid length, invalid value etc

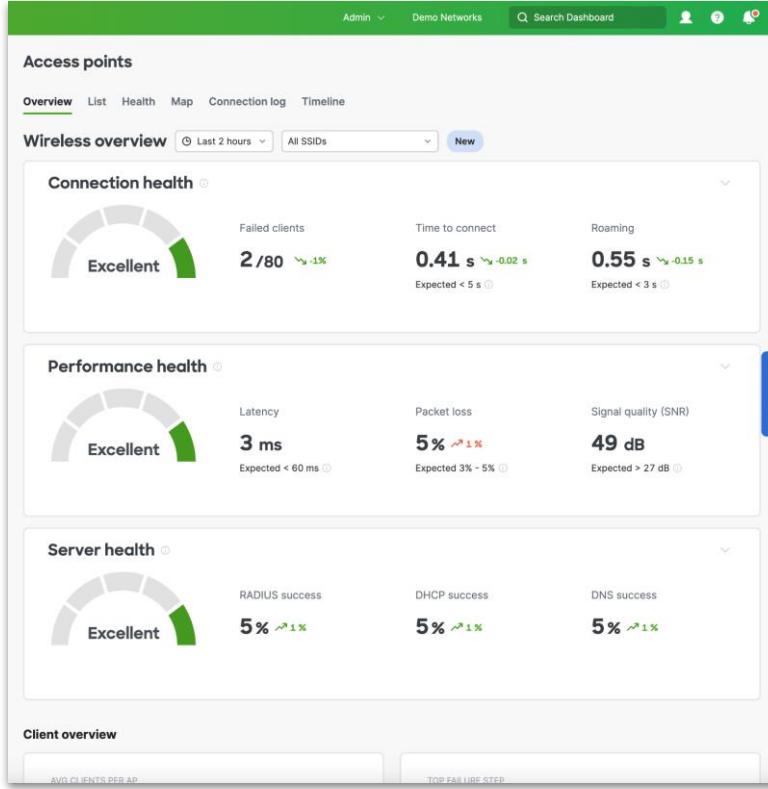
# Manual correlation with the data

For instance, wireless onboarding...



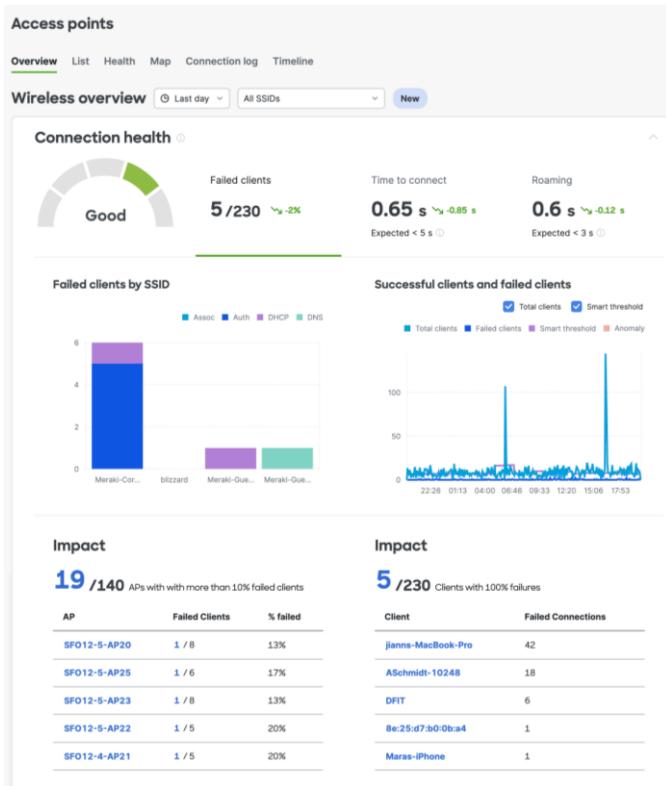
[Understanding Debug on WLAN on Cisco.com](http://Understanding Debug on WLAN on Cisco.com)

# 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

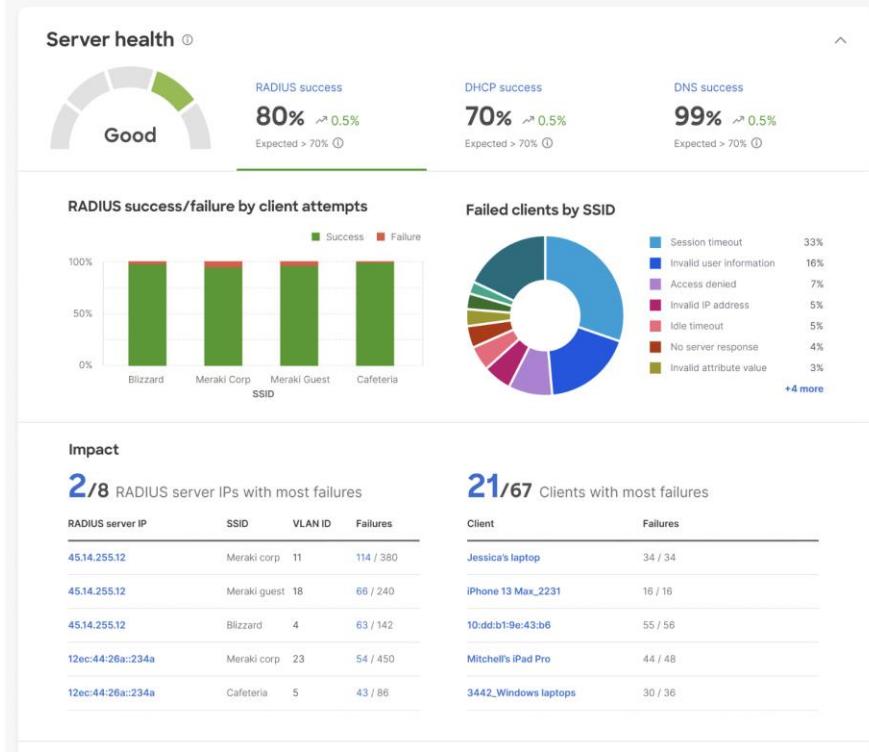
Clients using SBC WiFi with Medium failure of  Association  Authentication  DHCP  DNS for more than 30 minutes

Clients using SBC Public WiFi with Medium failure of  Association  Authentication  DHCP  DNS for more than 30 minutes

Add alert

Show additional recipients

# 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

Roamed from AP [RH3 Lobby 2x2](#) then had a failed connection to SSID [ASURAMS-SECURE](#) on AP [RH3 RM100 30H](#) during authentication because the auth server did not respond.

CHANNEL	BAND	SNR	VLAN ID	RADIUS SERVER	MERAKI REASON (CODE 100)
48	5 GHz	21 dB	5	10.10.80.34	RADIUS timeout

**RADIUS server not responding**

The configured RADIUS server 10.10.80.34 was not responding to valid RADIUS authentication requests on VLAN 5, causing client devices to fail authentication.

Impact  
100 /2134

Evidence ⓘ

Clients

RADIUS Response Rate of 31% for VLAN 5 shows the server was not responding to client authentication requests, but an average RADIUS Response Rate of 89% means the server was responding to clients on other VLANs.

**RADIUS RESPONSE RATE ON VLAN 5**

• 31 %

**AVERAGE RADIUS RESPONSE RATE**

• 89 %

Recommendations

- Check that VLAN 5 is tagged on [ASURAMS-SECURE](#) SSID.
- Check that the upstream switch port is configured to pass traffic with VLAN 5.
- Check if the RADIUS server 10.10.80.34 is blocked in the firewall rules for [ASURAMS-SECURE](#) SSID or any ACLs of an upstream device.
- Check the RADIUS server 10.10.80.34 is configured with the correct IP on [ASURAMS-SECURE](#) SSID. Review steps to configure RADIUS in the documentation.
- Try [pinging](#) the RADIUS server 10.10.80.34 from AP [RH3 RM100 30H](#) to verify connectivity.
- Verify the RADIUS server 10.10.80.34 functionality using the [RADIUS test tool](#).
- Follow troubleshooting steps in the [RADIUS issue resolution guide](#).

# 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 11 BAND 2.4 GHz SNR 12 dB

**Sticky Client**  
• Manually disconnect the client and check if it connects to an AP with a stronger signal.

**Evidence**



12 dB

WGTCWES-DSMKG34 26 dB DOUWAP-LibraryMR53 DOUWAPCONF-MR53 26 dB

**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.

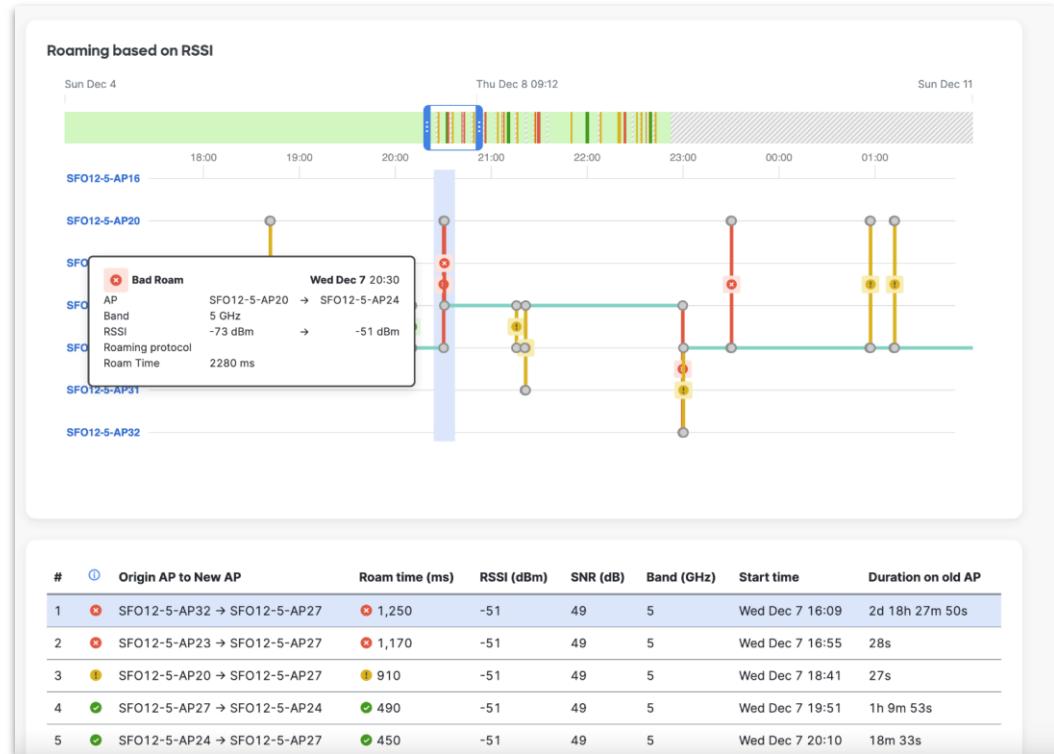
**Disconnect client**

Was this helpful? Like Dislike

# Contextual roaming analytics

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

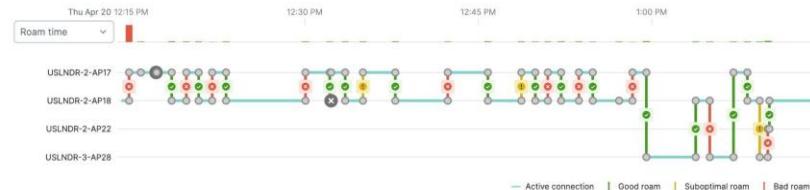
- Tiering of roaming events – good, suboptimal, bad
- Visualization of unique events – sticky or ping-pong clients



# Contextual roaming analytics

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

Selected 1 hour



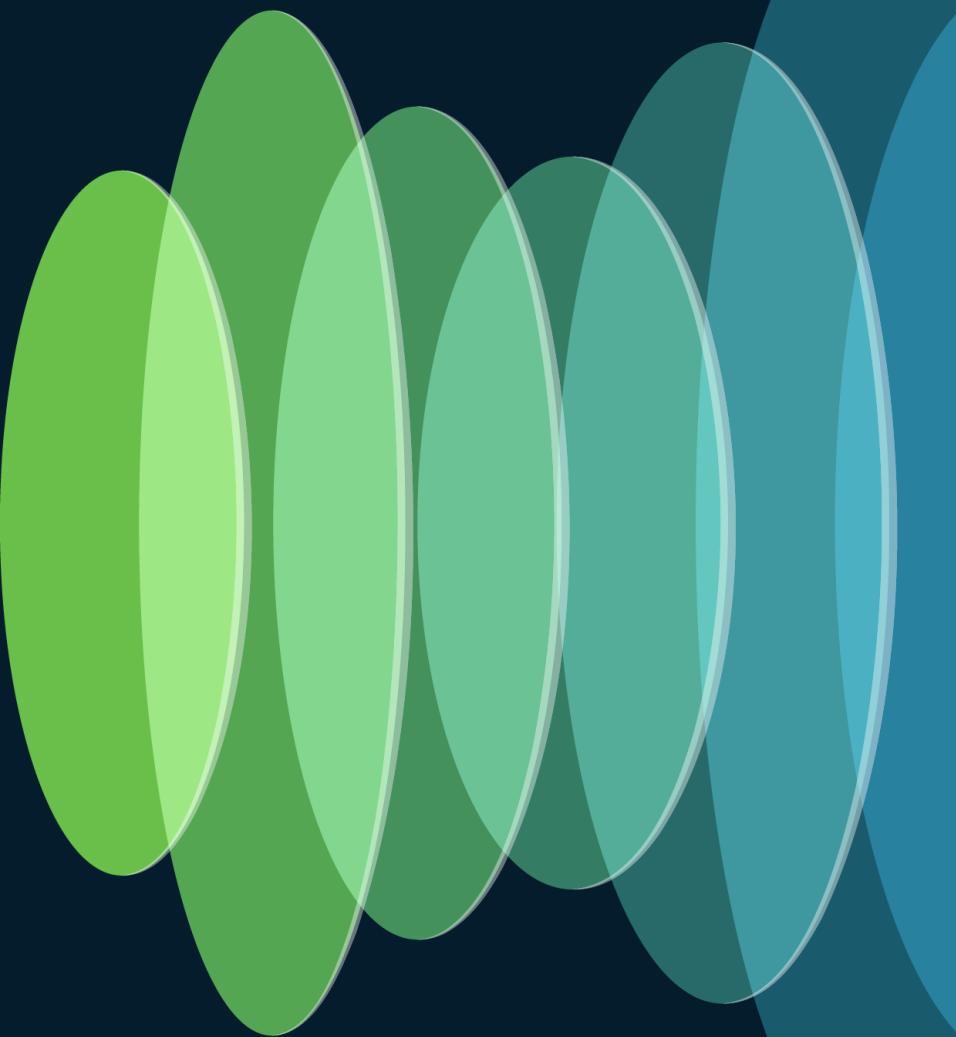
Bad roaming experience

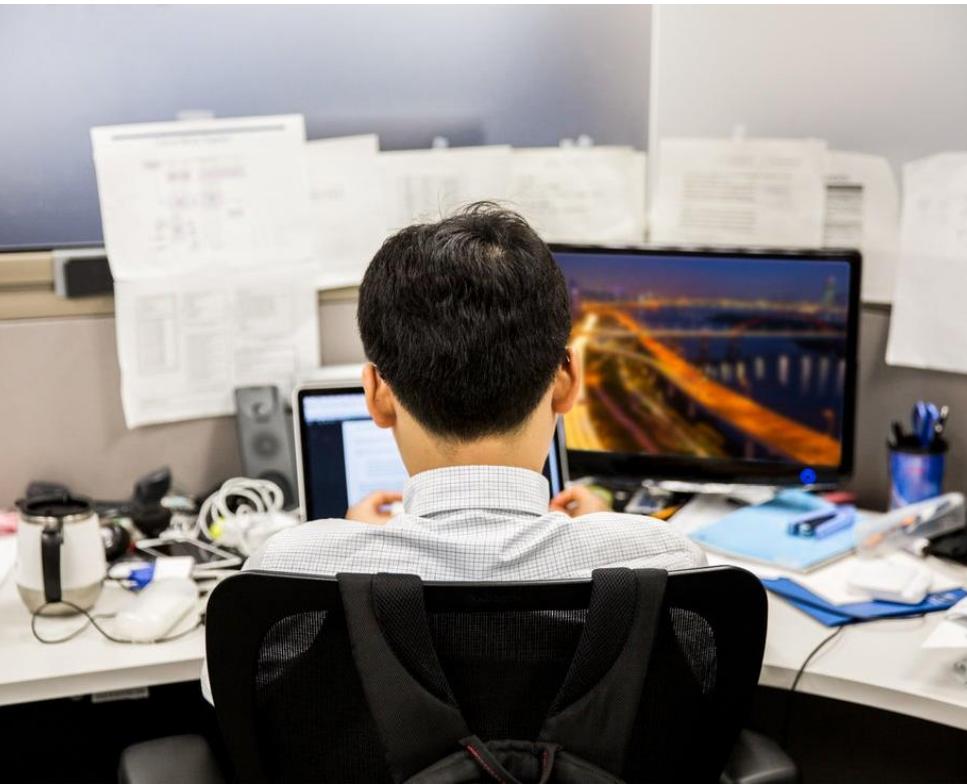
Selected 1 hour



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



## Highlights across all models



Up to  $\times 4$  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

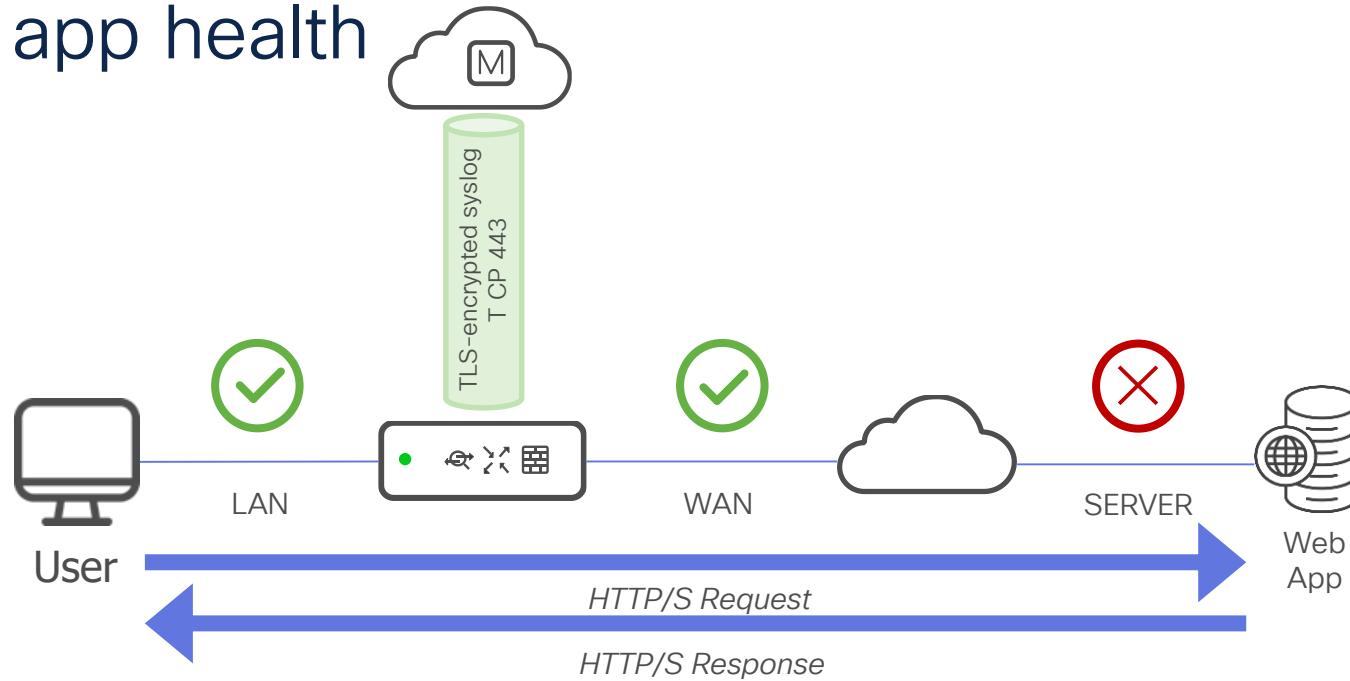
Track VoIP quality by provider and uplink with detailed hop-by-hop analysis actively.



## Internet Outages

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

# Web app health

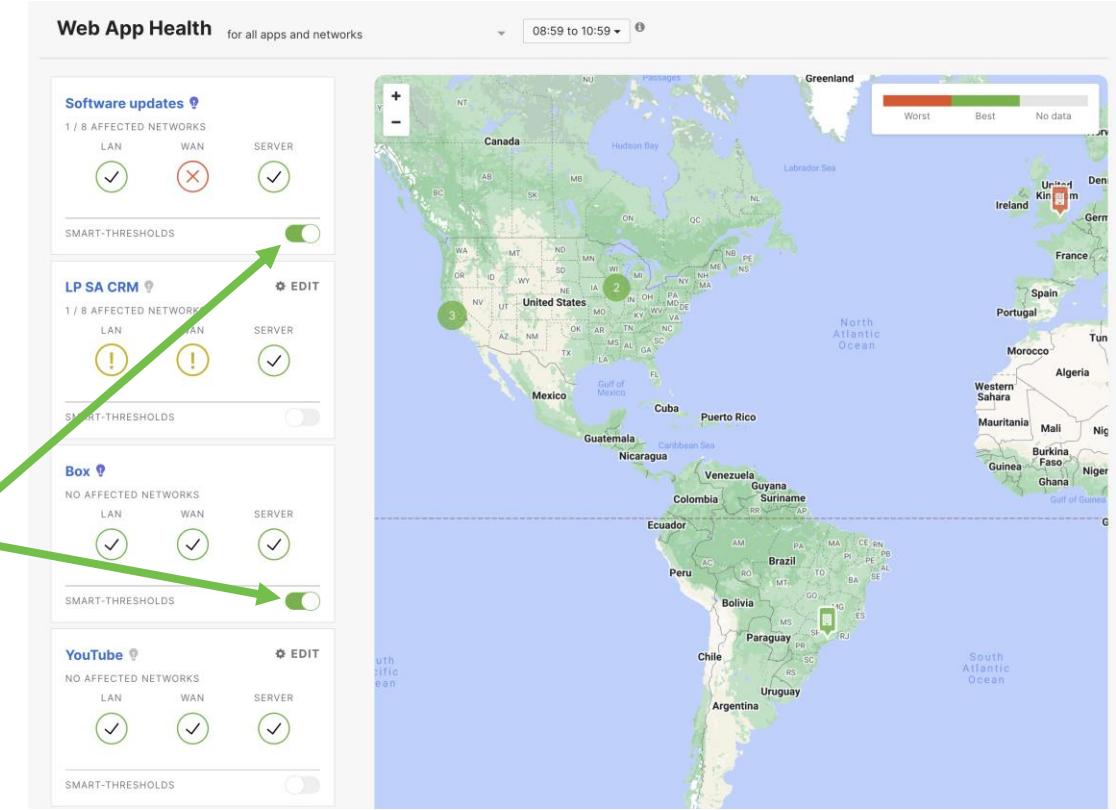


# Web app health

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



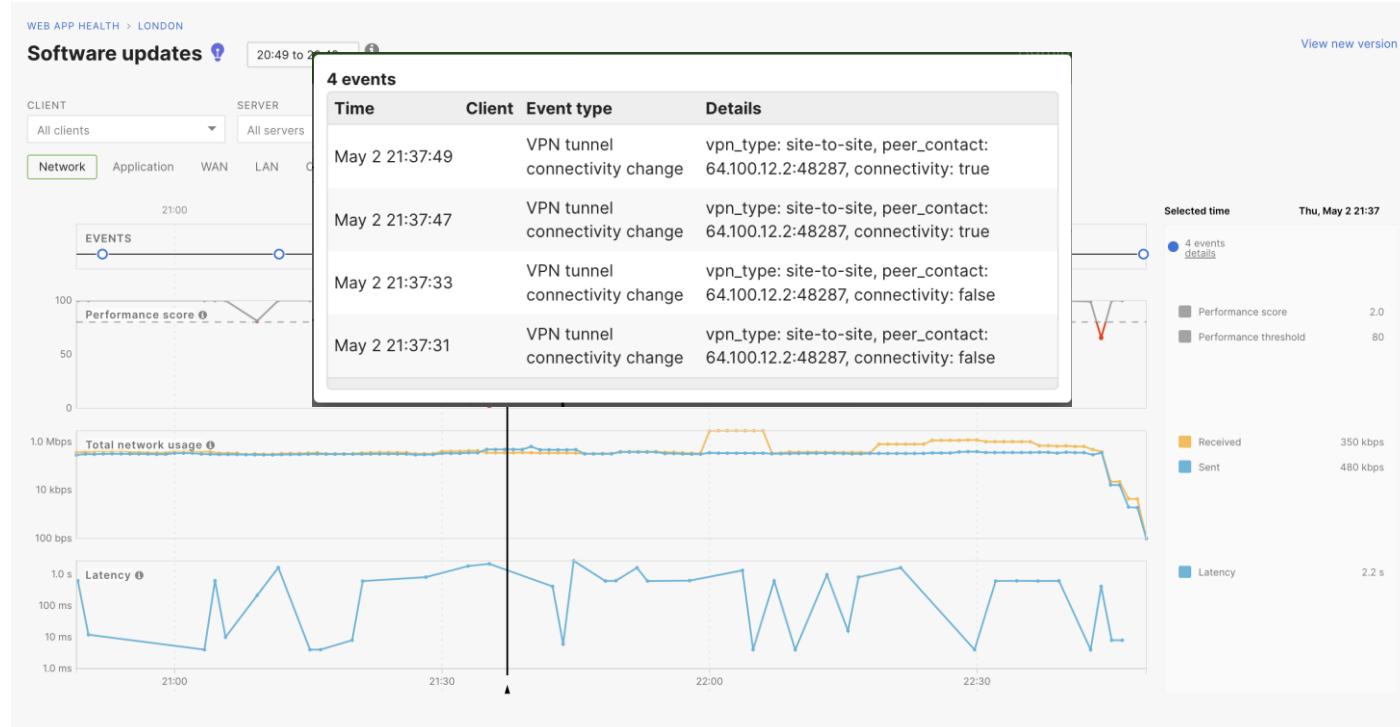
Smart-thresholds for automatic alerting barriers unique for each location



# Web app health



# Web app health



# Web app health



# WAN Health

WAN health Last 2 hours  ⓘ View old version

1 offline  ⓘ 3 Poor performance  ⓘ 0 High usage  ⓘ 25 online  ⓘ

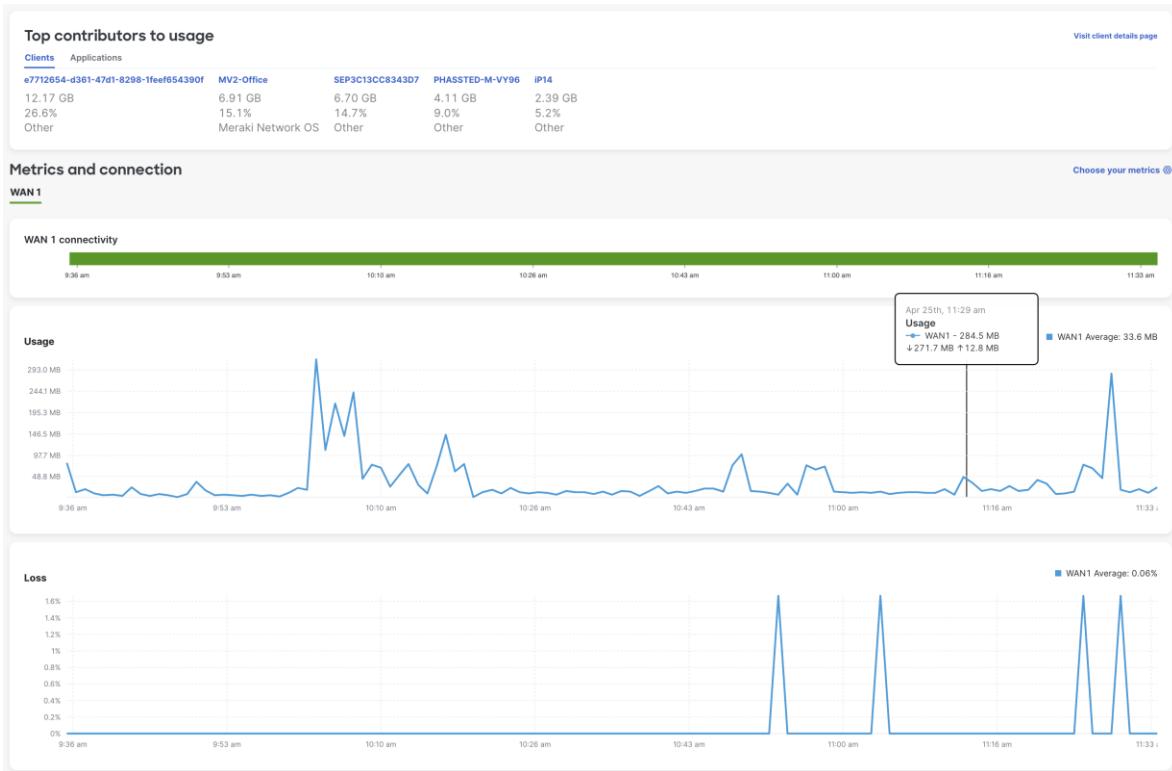
Search 4 Status ⓘ Network tags ISPs ⓘ Uplinks  ⓘ Reset all 49 Results Download

Network	Type	Availability	Total usage	Average throughput	Loss	Average latency	Speed test <span>Beta</span>	Network tags	% Capacity	⋮
San Francisco	WAN 1	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 1.10 GB, ↑ 1.17 GB	↓ 1.20 Mbps, ↑ 1.27 Mbps	0.00%	9.9 ms	<span>Run speed test</span>	Campus Catalyst	↓ 1.14 %, ↑ 1.21 %	
San Francisco	WAN 2	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 44.35 MB, ↑ 173.46 MB	↓ 48.33 Kbps, ↑ 189.03 Kbps	30.32%	620 ms	<span>Run speed test</span>	Campus Catalyst	↓ 0.00 %, ↑ 0.02 %	
Sydney	WAN 1	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 450.11 MB, ↑ 67.82 MB	↓ 494.36 Kbps, ↑ 74.48 Kbps	0.03%	9.8 ms	<span>Run speed test</span>	MultiWAN Retail ThousandEyes	↓ 0.19 %, ↑ 0.03 %	
Sydney	WAN 2	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 43.80 MB, ↑ 1.11 GB	↓ 48.11 Kbps, ↑ 1.22 Mbps	0.03%	9.9 ms	<span>Run speed test</span>	MultiWAN Retail ThousandEyes	↓ 0.02 %, ↑ 0.46 %	
Sydney	WAN 3	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 6.22 MB, ↑ 11.08 MB	↓ 6.83 Kbps, ↑ 12.17 Kbps	0.00%	10 ms	<span>Run speed test</span>	MultiWAN Retail ThousandEyes	—	
London	WAN 1	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 357.48 MB, ↑ 437.48 MB	↓ 394.30 Kbps, ↑ 482.54 Kbps	0.00%	9.9 ms	<span>Run speed test</span>	Branch ThousandEyes	↓ 0.04 %, ↑ 0.05 %	
London	WAN 2	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 213.21 MB, ↑ 94.23 MB	↓ 235.16 Kbps, ↑ 103.93 Kbps	31.76%	620 ms	<span>Run speed test</span>	Branch ThousandEyes	↓ 0.02 %, ↑ 0.01 %	
Teleworker John Smith	WAN 1	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 11.52 MB, ↑ 13.59 MB	↓ 12.71 Kbps, ↑ 14.99 Kbps	0.01%	10 ms	<span>Run speed test</span>	Teleworker	↓ 0.01 %, ↑ 0.01 %	
Datacenter-NA	WAN 1	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 2.66 GB, ↑ 3.13 GB	↓ 2.89 Mbps, ↑ 3.40 Mbps	0.06%	2.7 ms	<span>Run speed test</span>	Datacenter SJC-DC	—	
Datacenter-NA	WAN 2	<div style="width: 80%;"><div style="width: 100%; background-color: #2e6b2e;"></div></div>	↓ 5.46 MB, ↑ 4.43 MB	↓ 5.93 Kbps, ↑ 4.81 Kbps	0.04%	2.7 ms	<span>Run speed test</span>	Datacenter SJC-DC	—	

Rows per page 10 < 1 2 3 >

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

# WAN Health



- Quickly isolate ISP issues and cellular failover

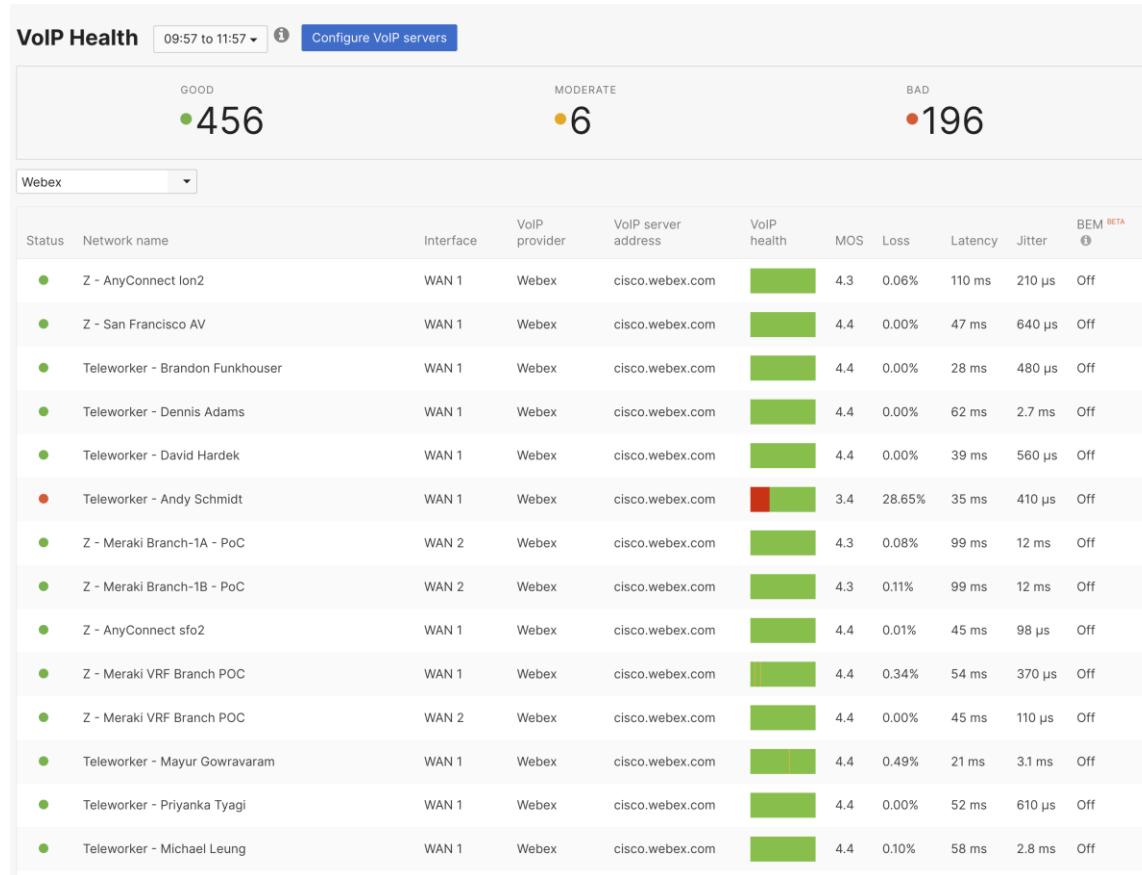
# WAN Health



- Detailed speed test results included history of previous tests

# 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

• Z - San Francisco AV - WAN 1 - Webex Apr 18 12:03 to Apr 25 12:03 ⓘ

VoIP path details

Origin network	Z - San Francisco AV
MX uplink	WAN 1
VoIP provider	Webex
VoIP server address	cisco.webex.com

Security Appliance → ISP → Internet → VoIP

Show hop-by-hop analysis Refresh

Target VoIP server diagnostics

MOS	4.4	LOSS	0.00 %	LATENCY	46.46 ms	JITTER	0.19 ms
-----	-----	------	--------	---------	----------	--------	---------

MOS

Loss

Latency

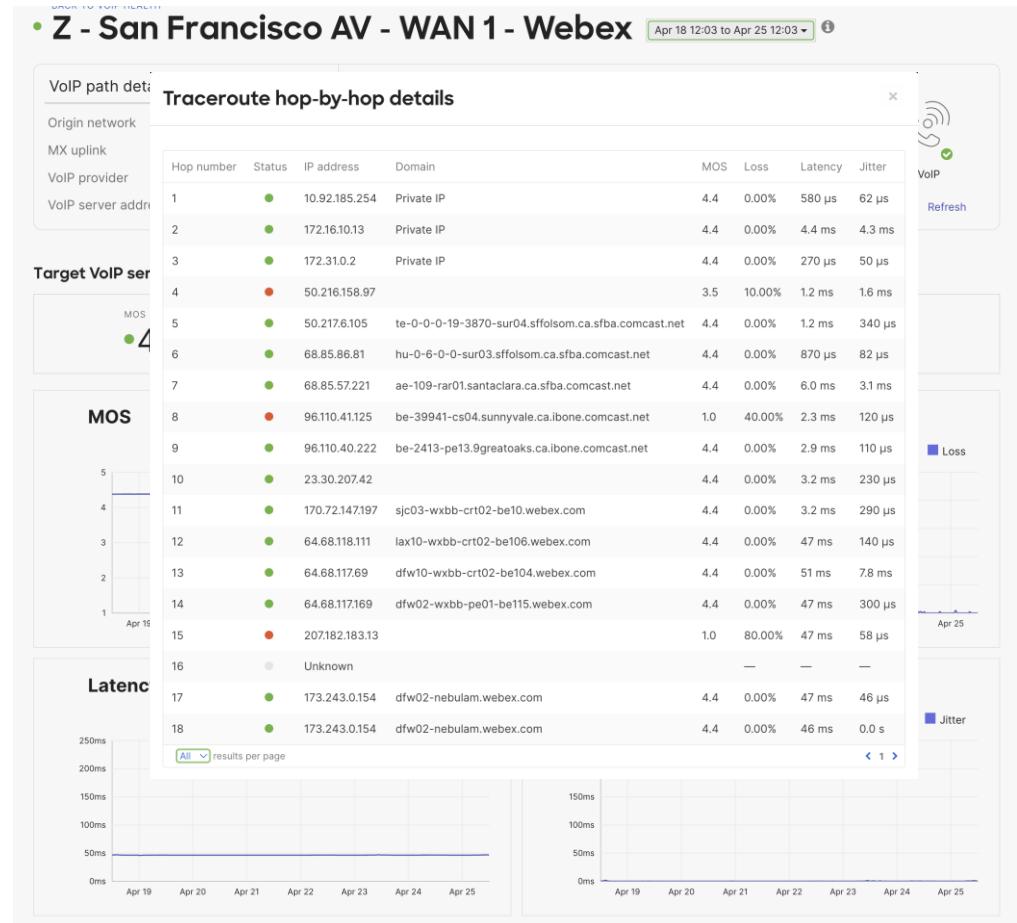
Jitter

BRKOPS-2013

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 49

# 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      Locations  
32      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

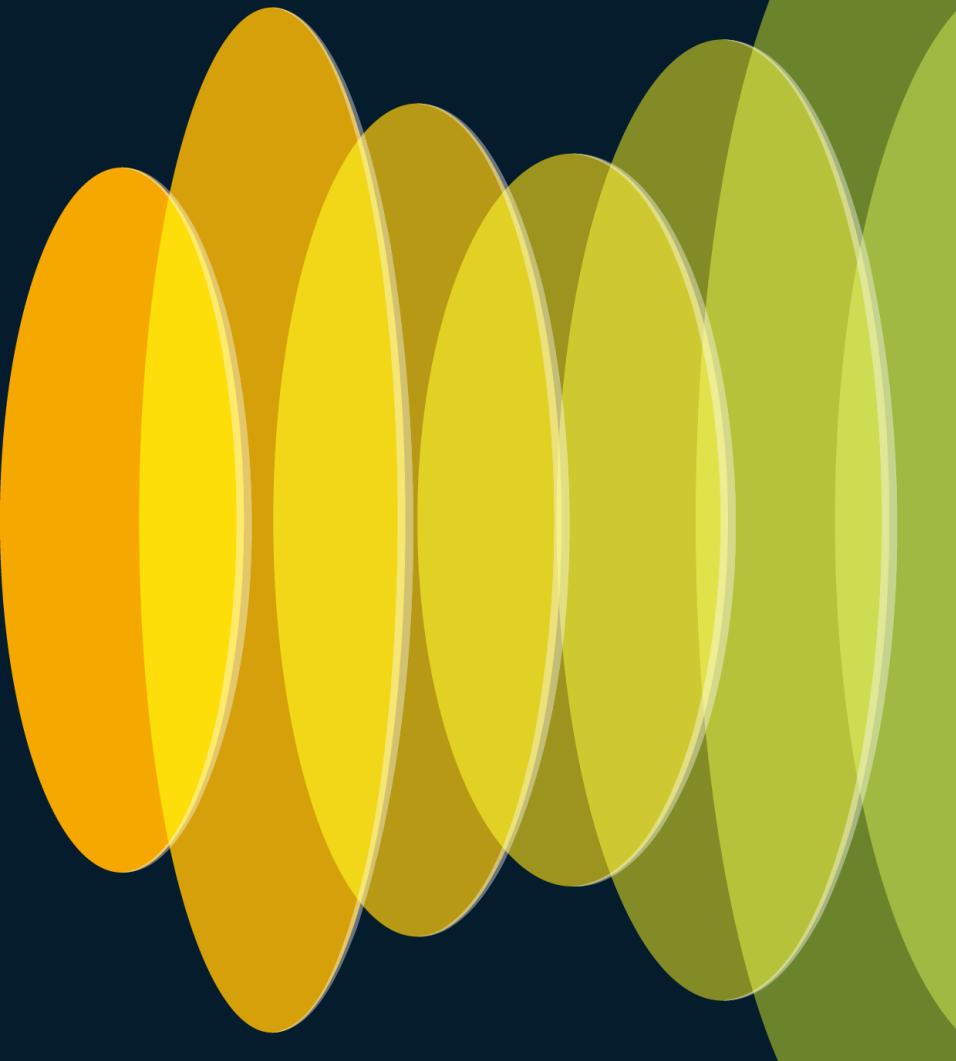
1 - 7 of 32 < >

ThousandEyes  
powered by Internet

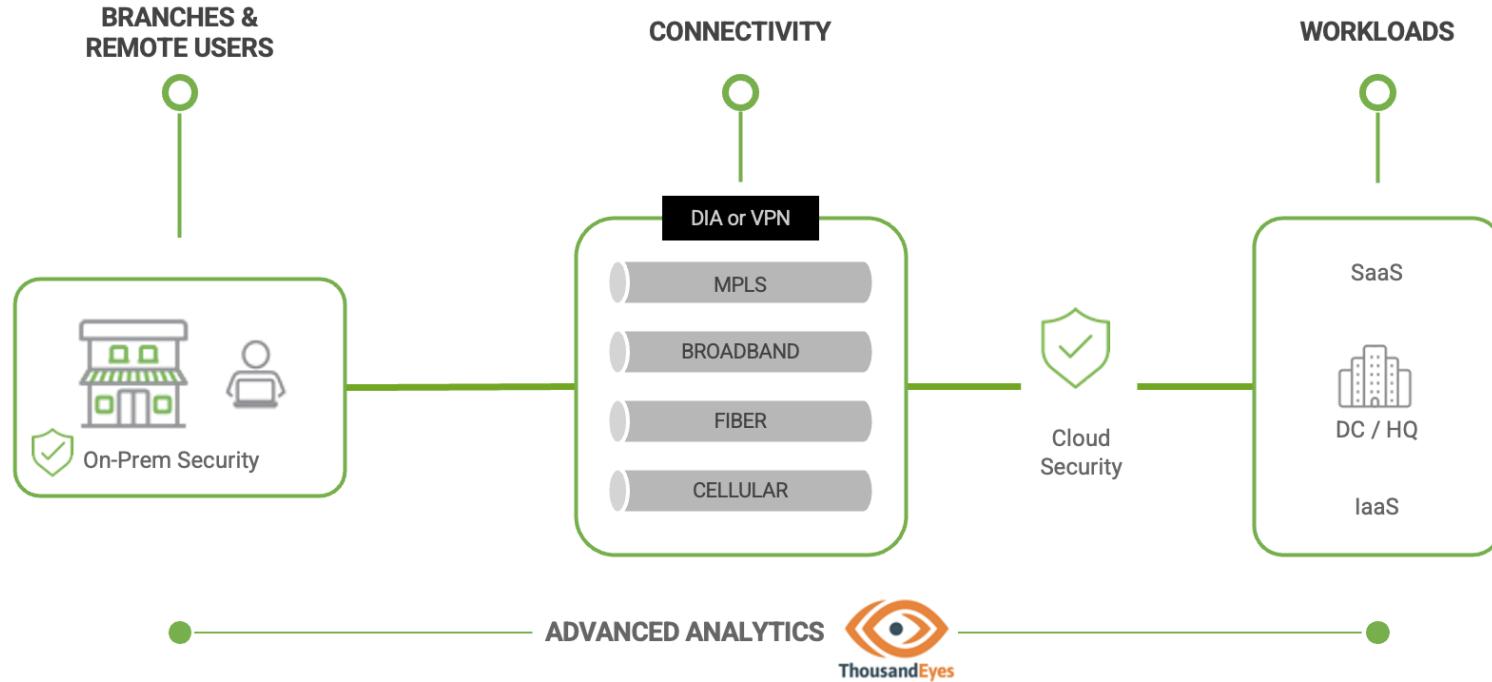


- Global view of ISP outages powered by ThousandEyes
- Evaluate performance of other ISPs in your regional branches

# ThousandEyes Power



# Active observability across every domain

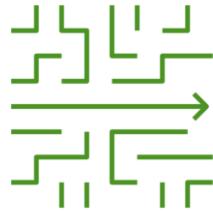


# ThousandEyes Agent

Zero additional hardware needed



Always on visibility to monitor critical SaaS applications



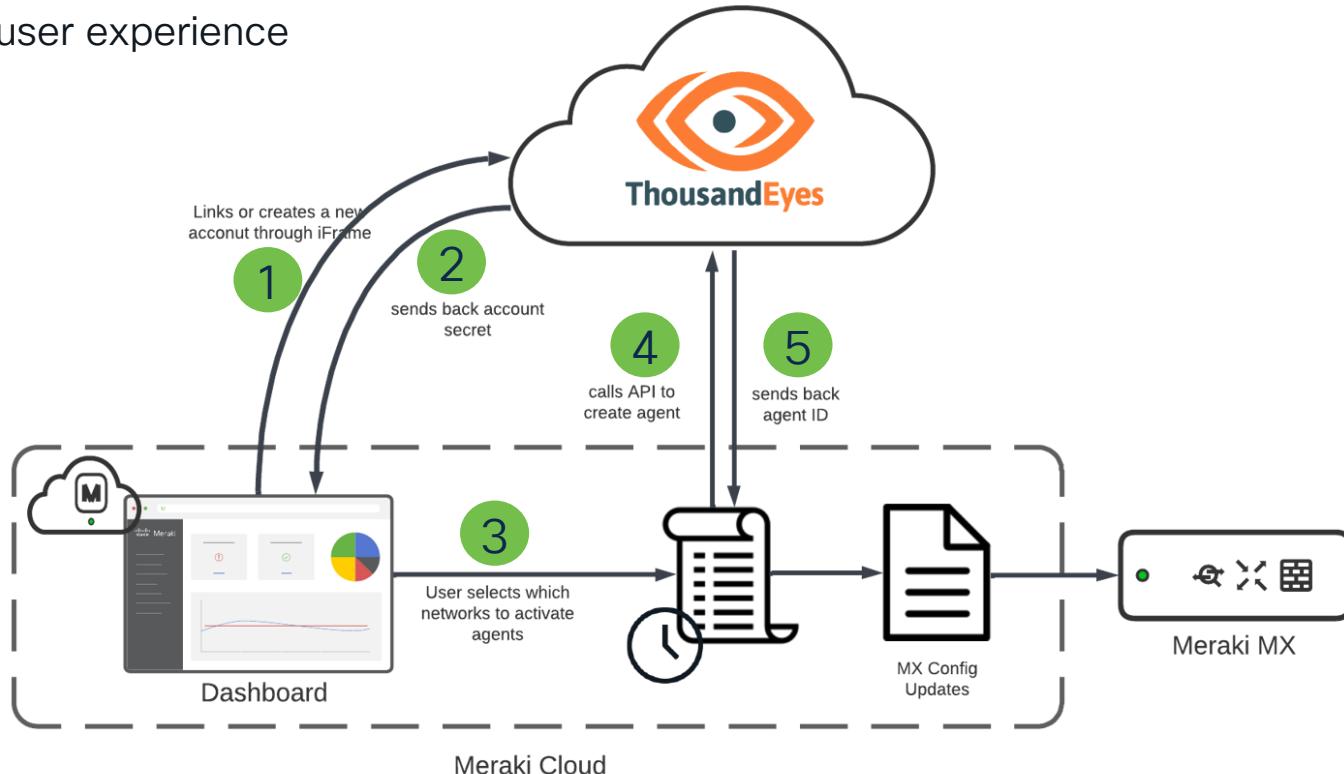
Instantly activate ThousandEyes across your entire MX fleet in minutes



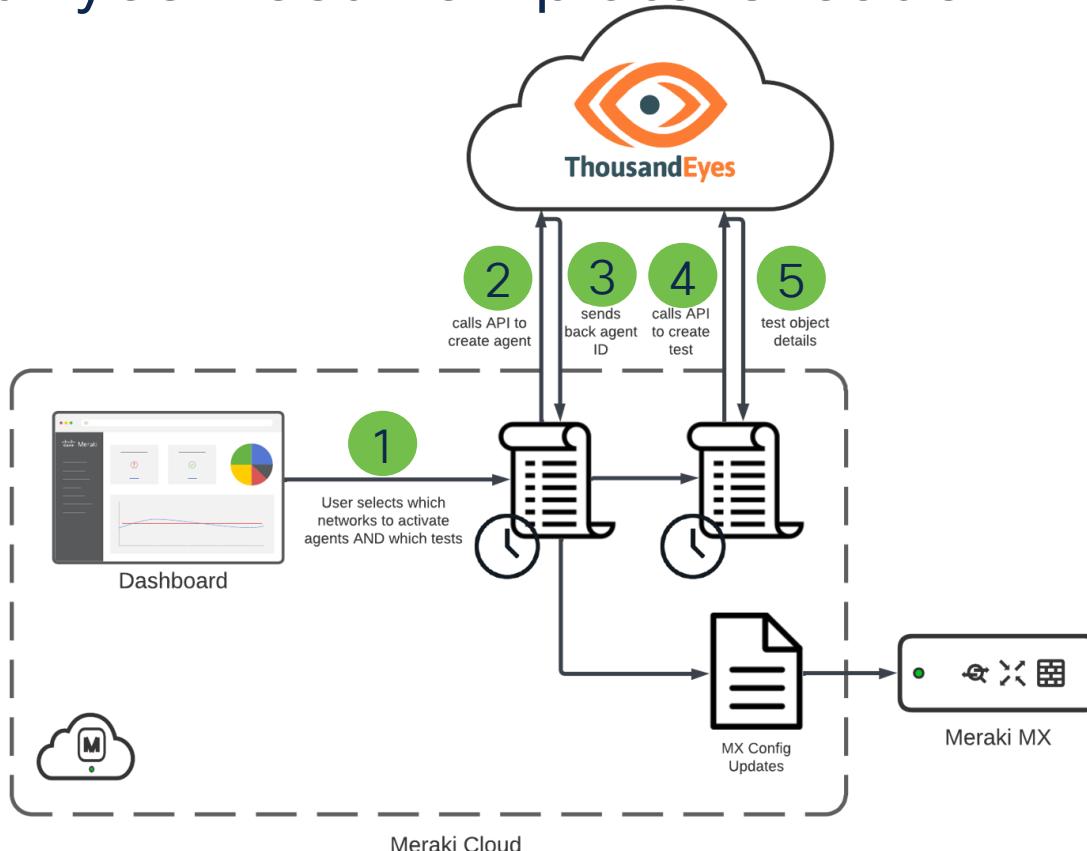
Integration includes 1 free test per SD-WAN+ license (up to 50)

# Agent Activation

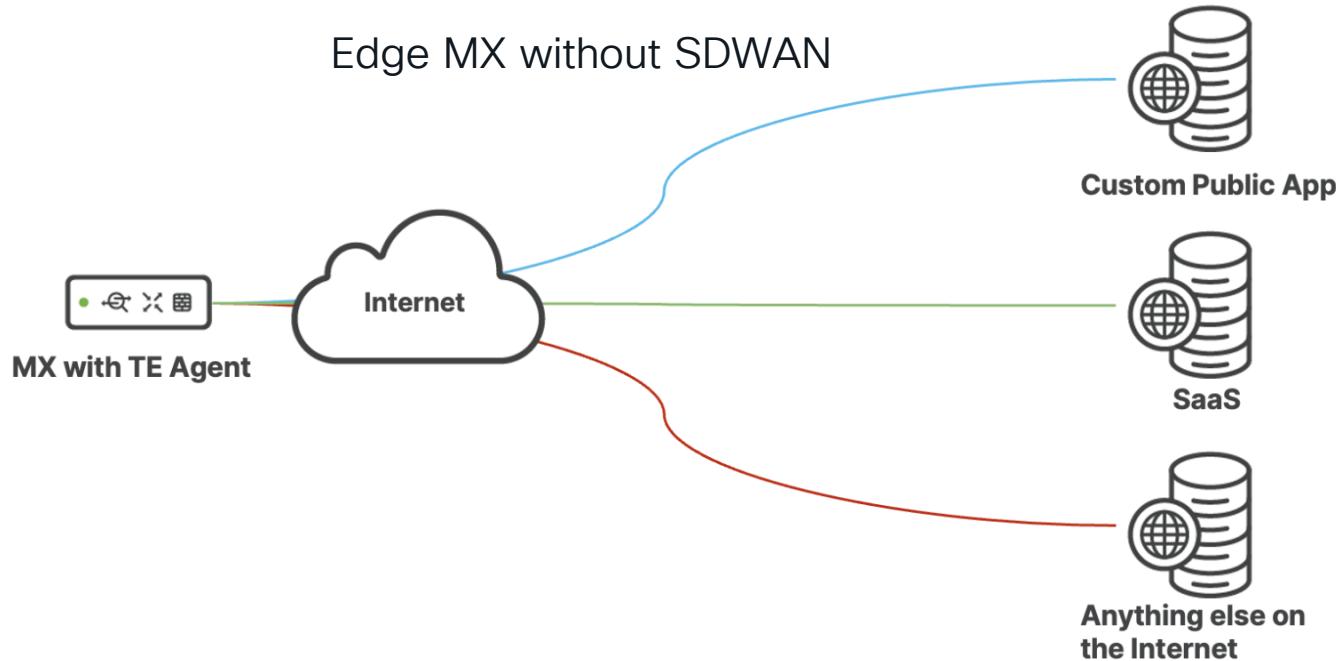
Seamless user experience



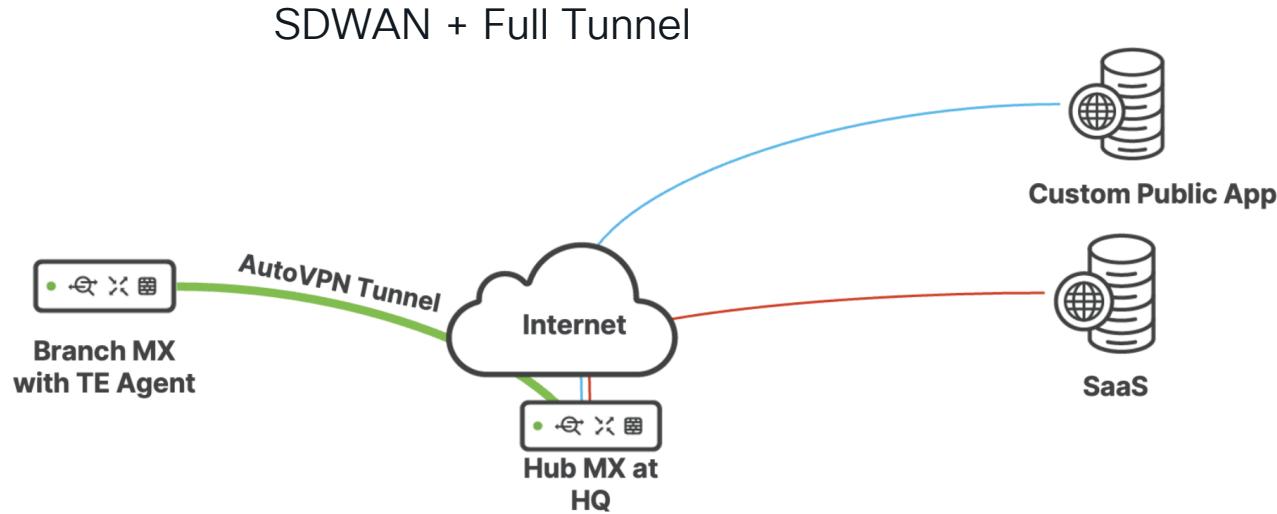
# ThousandEyes Test Template Creation



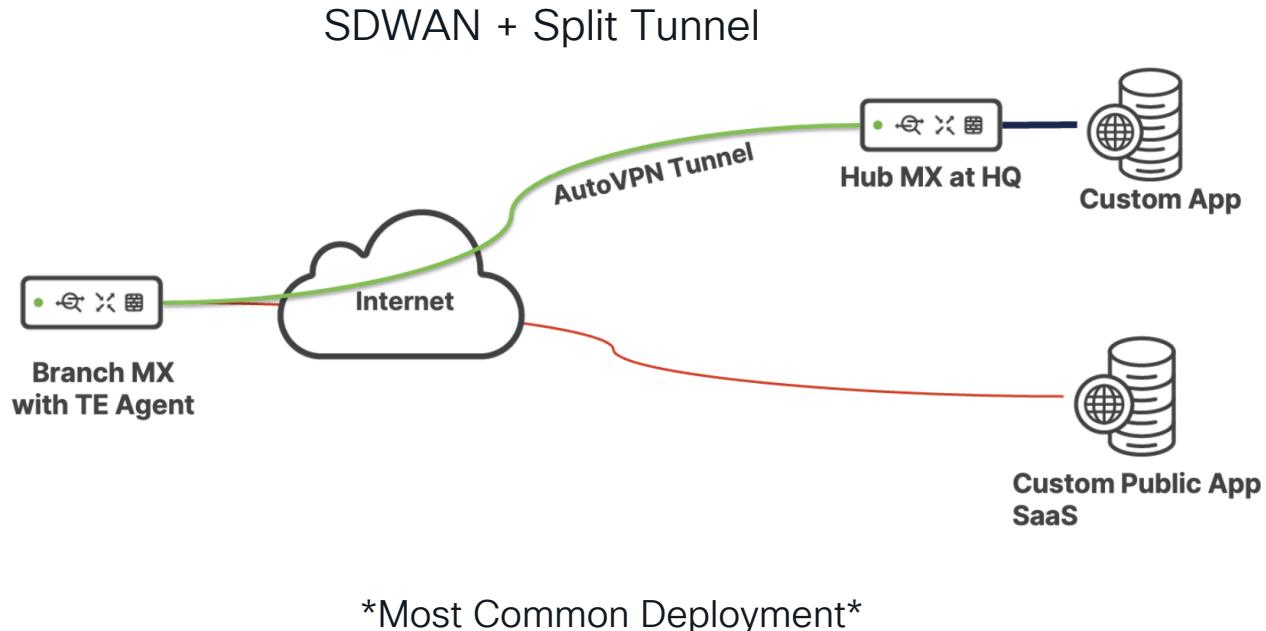
# Deployment characteristics



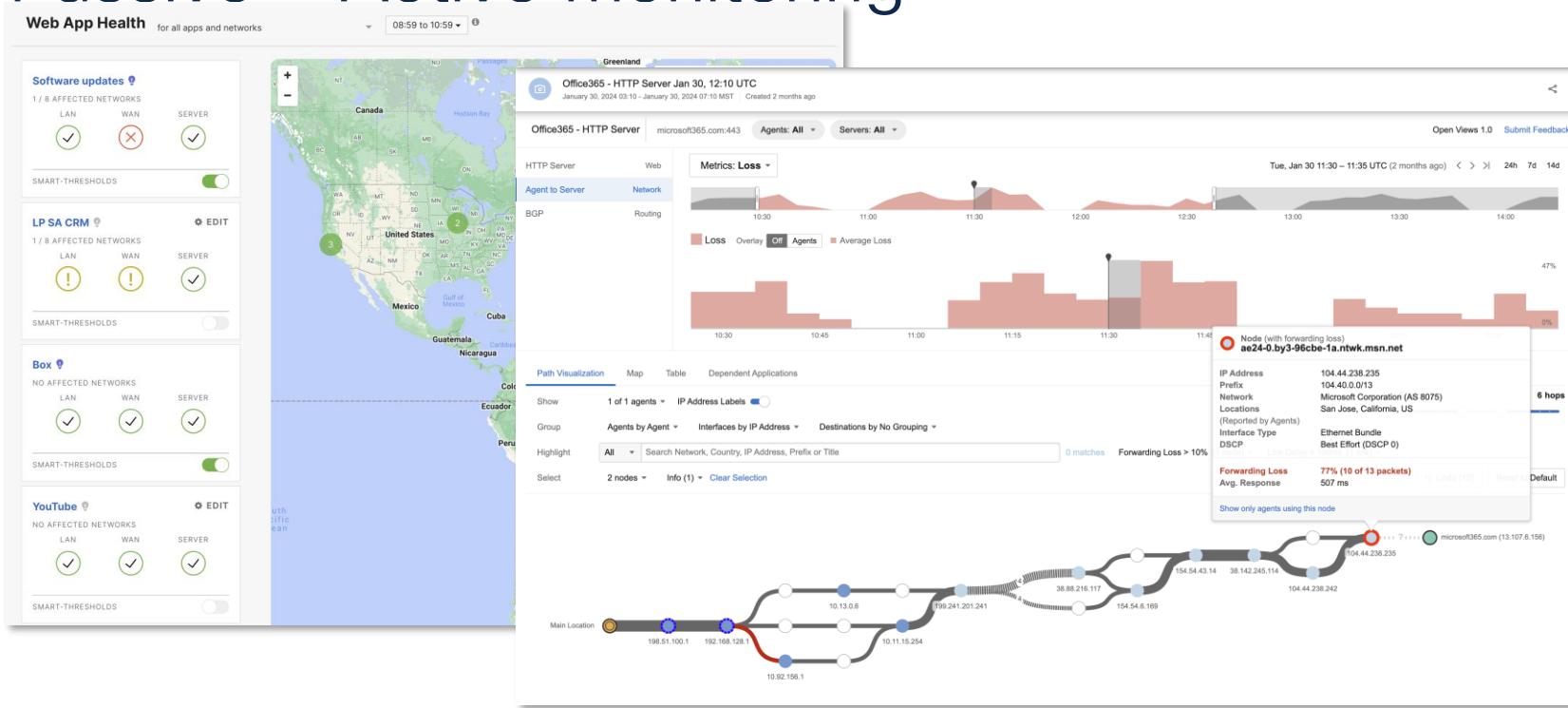
# Deployment characteristics



# Deployment characteristics

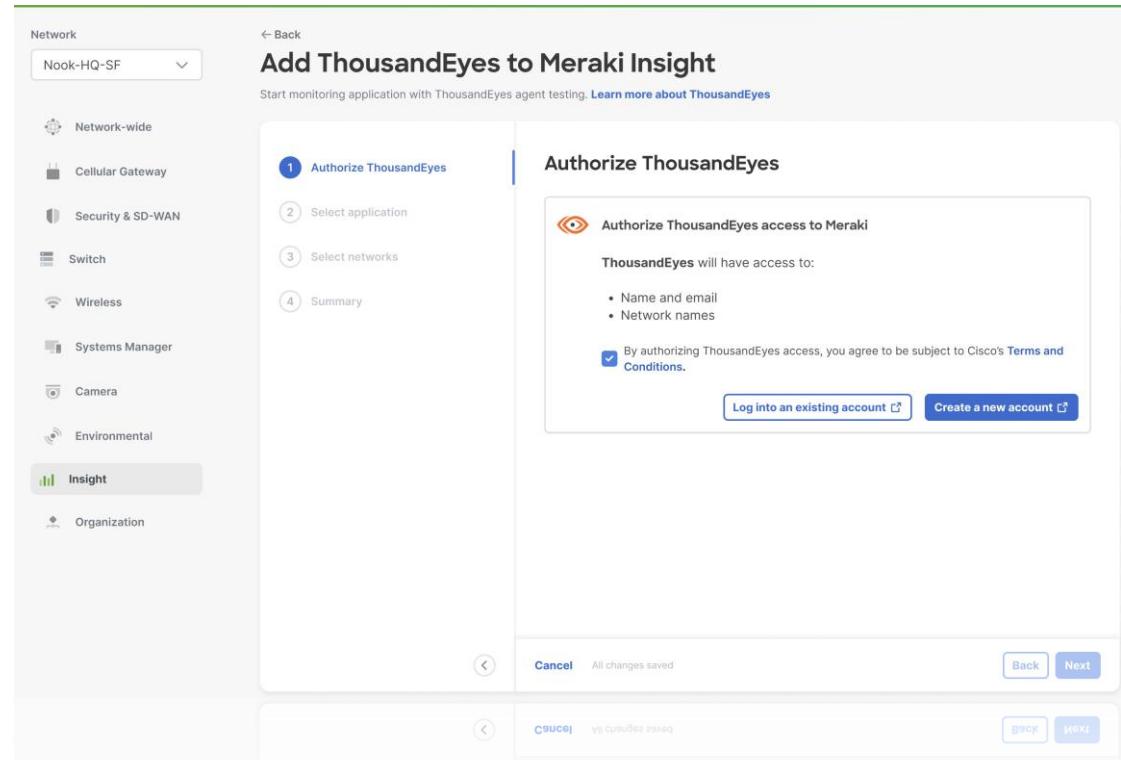


# Passive + Active monitoring



# 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



# Activate application tests

Monitor Critical Applications for SD-WAN Beta

1 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.

**Cisco WebEx** (selected)

Office 365 Suite

Office 365 Sharepoint

Zoom

Box

Salesforce

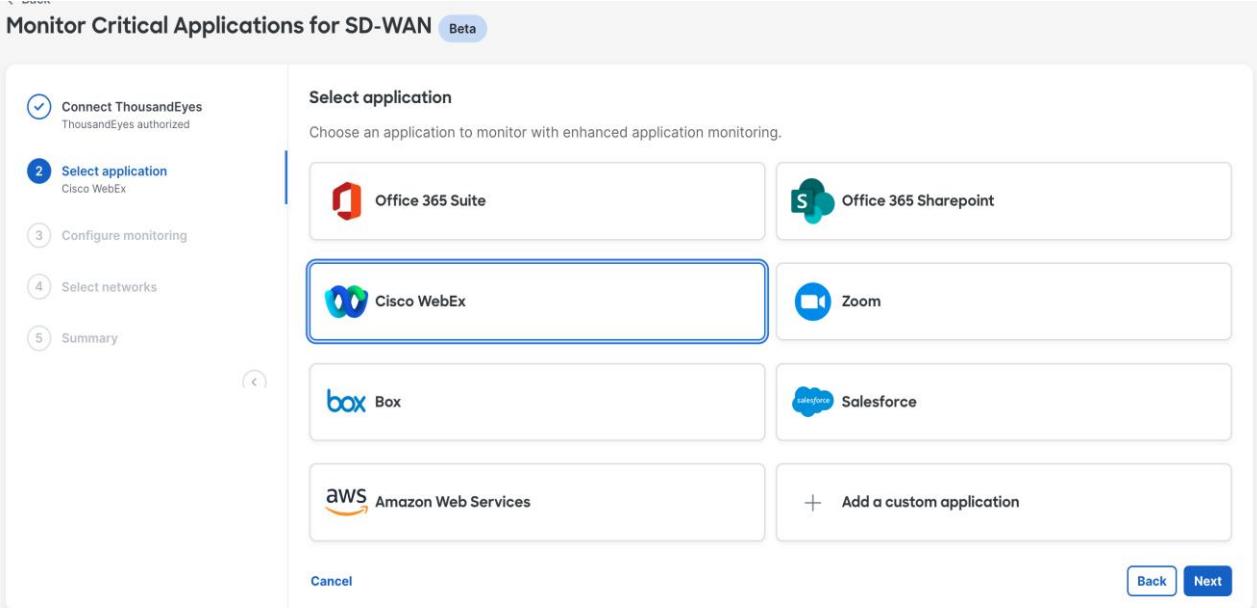
Amazon Web Services

+ Add a custom application

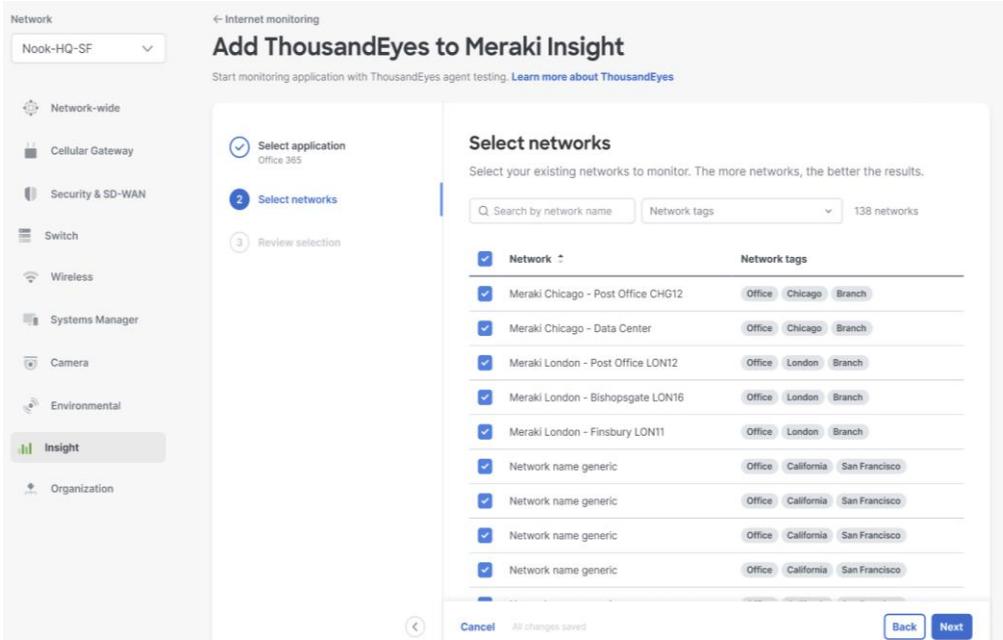
Cancel

Back

Next



# Activate agents: Select via tags



The screenshot shows the 'Add ThousandEyes to Meraki Insight' wizard. The left sidebar lists network components: Network-wide, Cellular Gateway, Security & SD-WAN, Switch, Wireless, Systems Manager, Camera, Environmental, and Insight (which is selected). The main pane is titled 'Select networks' and instructs the user to 'Select your existing networks to monitor. The more networks, the better the results.' It features a search bar, a 'Network tags' dropdown, and a list of 138 networks. The list includes: Meraki Chicago - Post Office CHG12, Meraki Chicago - Data Center, Meraki London - Post Office LON12, Meraki London - Bishopsgate LON16, Meraki London - Finsbury LON11, Network name generic, Network name generic, Network name generic, and Network name generic. Each entry is preceded by a checkbox and includes 'Network tags' (e.g., Office, Chicago, Branch, London, California, San Francisco). At the bottom are 'Cancel' and 'Next' buttons.

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

# Meraki bi-directional data integration

Assurance overview Last day

Organization Meraki

Organization-wide

Insight

Network HQ-Boston

Network-wide

Assurance

Cellular Gateway

Security & SD-WAN

Switching

Wireless

Systems Manager

Your end user experience score is **Fair**  
Some end clients are unable to access their applications and have moderate interruption from the network.

74 /100 3% last day

End user experience score Last day Last day average

Clients: Poor 3,000

Wireless: 2 issue 970 impacted clients

Applications

Data (for the past 2 hours)

- Office365: 1/100 13% 65 potentially impacted clients
- cisco.sharepoint.com: 100 0 Client unimpacted, 105 others potentially impacted
- myremoteapplication.com: 100 0 Client unimpacted, 0 others potentially impacted
- Webex - cisco: 100 0
- AWS: 100 0
- app.slack.com: 100 0
- Salesforce - meraki: 100 0
- meraki.atlassian.net: 100 0
- thousandeyes.atlassian.net: 100 0
- thousandeyes.enterprise.slack.com: 100 0

See all applications

Current client connections

SFO12-5-AP21 6 18 SFO12-WIFI32 8 7

Cisco Live!

#CiscoLive BRKOPS-2013 © 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public 75

# ThousandEyes enriched with Meraki data

Endpoint wireless health  
powered by Meraki MR

Segment Visualization Application: MS Teams

AGENT SF-iPhone-15-ProMax LOCAL NETWORK CAMPUS-SFO-3.14... VPN 10.20.0.1 PROXY 123.12.11.1 INTERNET APPLICATION MS Teams

Agent Local Network VPN Proxy Internet Applications Meetings

**Local Network**

Gateway	
BSSID	00:13:49:12:45:02
Channel	40
Gateway Latency	21ms
Gateway Loss	40
Gateway Score	Good
IP Address	192.168.4.115
Link Speed	789 Mbps
Phy Mode	802.11ac (Wi-Fi 5)
Router	192.168.4.1
Retransmission Rate	0.1%
SSID	Company-Work-Network
Throughput	789 Mbps
Wi-Fi Signal Quality	45%

Access Point Verified by Meraki

AP Name: Bad or no signal and very slow  
Connected Clients: Wireless performance  
Signal-to-Noise-Ratio: Bad

Go To Meraki AP

Path visualization with  
Meraki MX health data

Test: MS 365 - Web - External api.teams.com Agents: BOS-Meraki-MX-3523 Servers: All Reset

Enterprise Agent Boston, MA 1 Alert | Meraki MX

Agent Details

Public IP	255.125.32.1
Network	NTT America, Inc. (AS 2914)
Location	Boston, Massachusetts

Interface Details

IPv4 Address	255.125.32.1
Prefix	255.125.32.1/12

Measurements from this Agent

Loss	25%
Latency	41ms
Jitter	7ms
TCP Mass	1440 bytes
Min. Path MTU	1500 bytes
Active Alerts	SFO - MS Teams
Probing Mode	tcp-sack-mode
Path Trace Mode	Classic

Meraki MX Data

Connected Devices	34
Device Health Score	TBD
Firmware	MT 16.7

Show On Timeline Show Only This Agent Go To Meraki

Forwarding Loss > 20% (1 Node)

Enriched CEA data with Meraki 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](http://www.CiscoLive.com/on-demand)

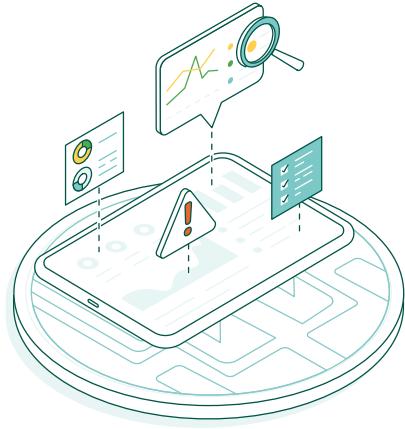
Contact me at: [phassted@cisco.com](mailto:phassted@cisco.com)

# “Wrap it up, Hasstedt!”

Everyone in this room  
...probably ;)

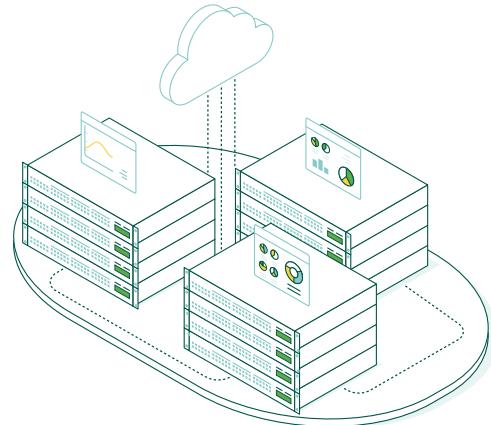


# Conquer the tsunami of data



## 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