



# Mastering Your Meraki Dashboard

Uncover Hidden Insights and Troubleshoot Effectively

Lina Alduaikat - CCIE #68079  
Technical Consulting Engineer  
BRKMER-2844



I can't log in! **Network Down!**

I can't print!

**Wi-Fi isn't working!**

**The Internet is broken!**

System is down

One device never connects!

**The VPN is broken!**

Can't send emails

The whole office is offline!

Nothing works!

**Servers are down!**

# About Me

- Hiking enthusiast
- Badminton Ninja
- Passionate about Oud
- Cisco Exam Advisory Group
- CCIE certified
- +5 Years experience in TAC



# Webex App

## Questions?

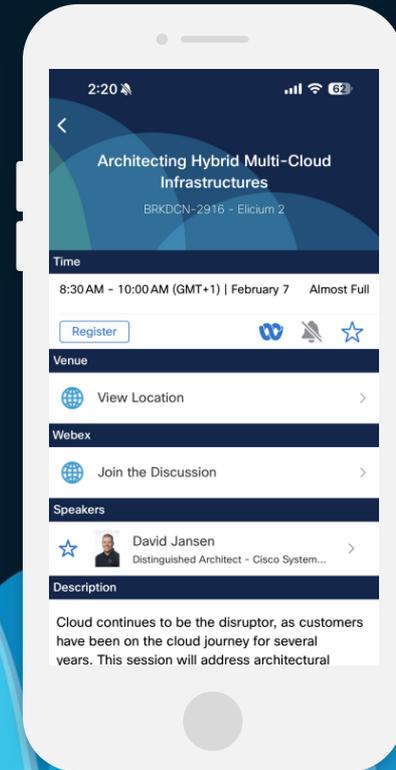
Use the Webex app to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events 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 February 28, 2025.

**CISCO** *Live!*



# Agenda

- Introduction
- Overview of Meraki dashboard
- Unveiling Powerful Insights
  - ✓ Insights
  - ✓ Packet captures
  - ✓ Live Tools
- Troubleshooting
  - ✓ Dashboard Intelligence
  - ✓ Real-World Scenario
  - ✓ Getting Help
- Practical Tips
- Conclusion

# Before We Go Pact

- Watch out for Hidden Slides 
- Key Insights for real challenges
- Make the most of what you have
- Demos cover:
  - ✓ Common problems you'll relate to
  - ✓ Core products MR, MX, and MS

# Introduction



# What You Will Learn

-  Understand Meraki Cloud architecture and Dashboard Navigation
-  Discover Insights and Tools for simplifying daily tasks
-  Learn how to resolve common issues through practical demos
-  Learn Tips and Hacks for efficiency

# Why Mastering Troubleshooting Skills Matters Even with TAC Support?



Cost Efficiency



Business Impact



Faster Resolution



Proactive Maintenance



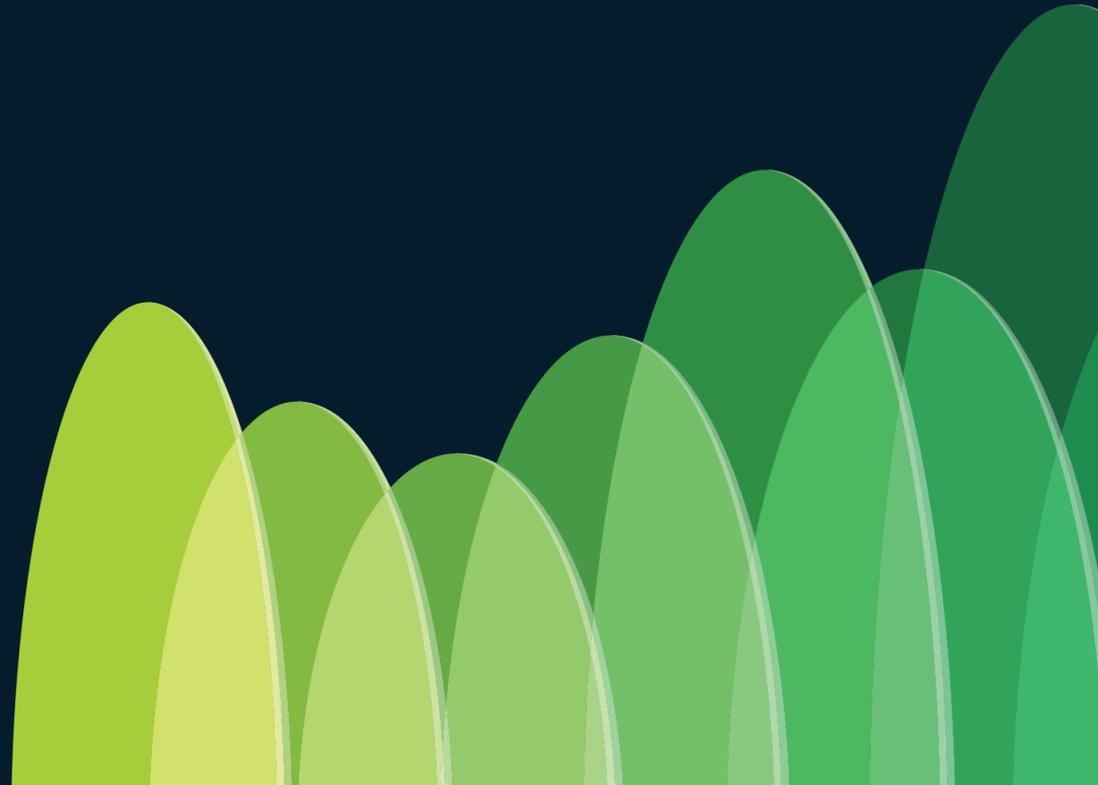
Collaboration with TAC

*“Having the right tools is just the start; knowing how to use them unlocks their true potential.”*

Lina Alduaikat  
Cisco

**CISCO** *Live!*

# Overview of Meraki Dashboard



# Meraki Cloud Architecture

out of band control plane

## Scalable

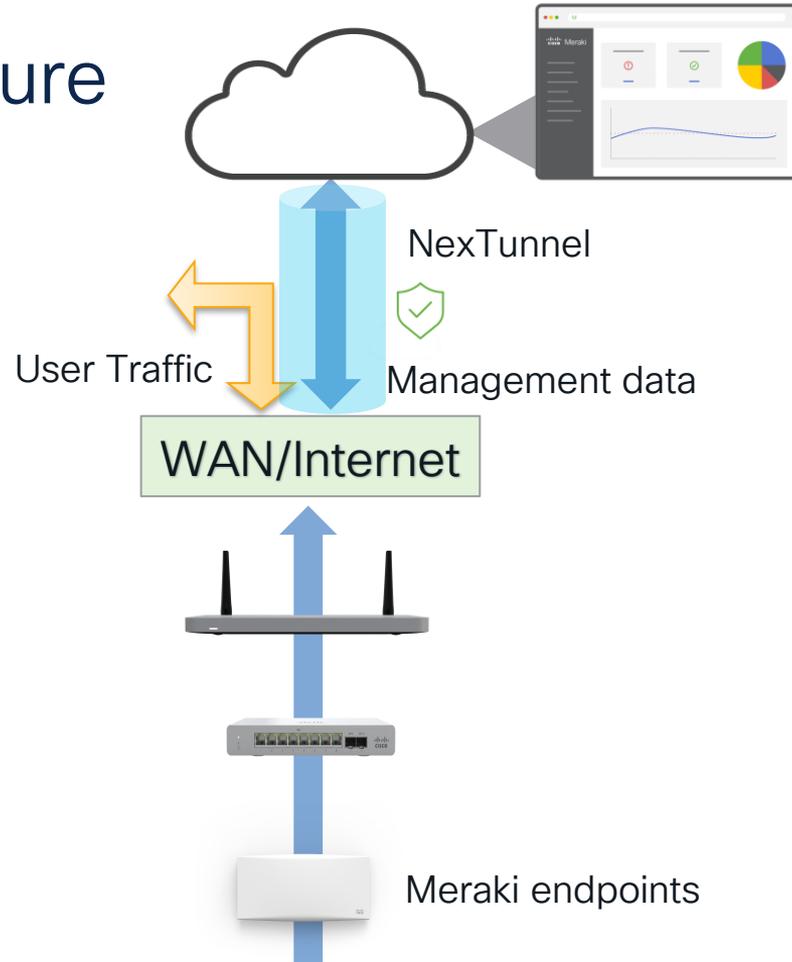
- Unlimited throughput: No bottlenecks
- Add devices or sites within minutes

## Reliable

- Uninterrupted network during outages
- 99.99% uptime SLA Secure

## Secure

- No user traffic passes through the cloud
- FIPS 140-2 compliant



# Meraki Dashboard Menus

Network

Network-wide

Security & SD-WAN

Switching

Wireless

Systems Manager

Cameras

Sensors

Insight

Organization

English

### Clients

Uplinks 2 total  
All Online ✓

WAN appliances 1 total  
All Online ✓

Switches 4 total  
All Online ✓

Access points 15 total  
All Online ✓

### Usage and clients

Usage 43.1 GB (↓40.07 GB, ↑3.03 GB)

Status	Description	Last seen (UTC-0)	Usage	Client type, OS	IPv4 address	Policy	
<input type="checkbox"/>	Wired	Martin Nash	Dec 20 2024 03:52	21.49 GB	Other	172.17.10.114	Whitelisted

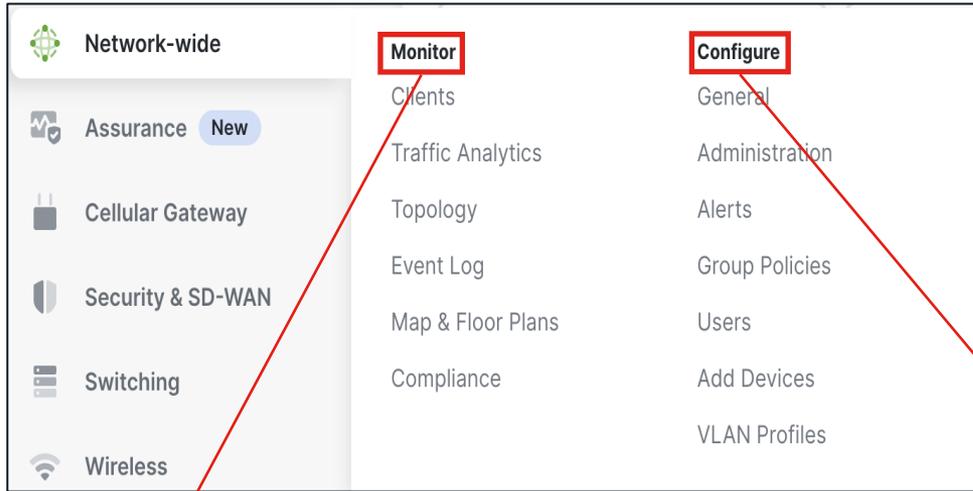
Product-specific

- ✓ Hardware
- ✓ Software

Organization

Only Organization admins have access

# Meraki Dashboard Key Sections



Observe the status, performance, and health of your Meraki network devices and clients. It is primarily for monitoring and troubleshooting.

Set up and manage your Meraki network. This is primarily for configuring settings, policies, and device parameters.

Unveiling  
powerful insights

CISCO *Live!*



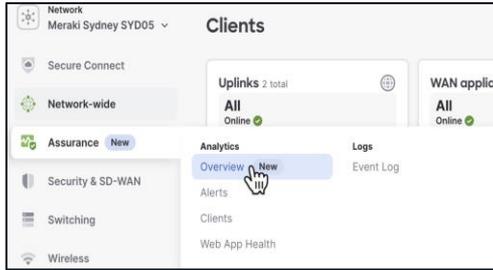
# Insights

CISCO *Live!*



# Meraki Assurance

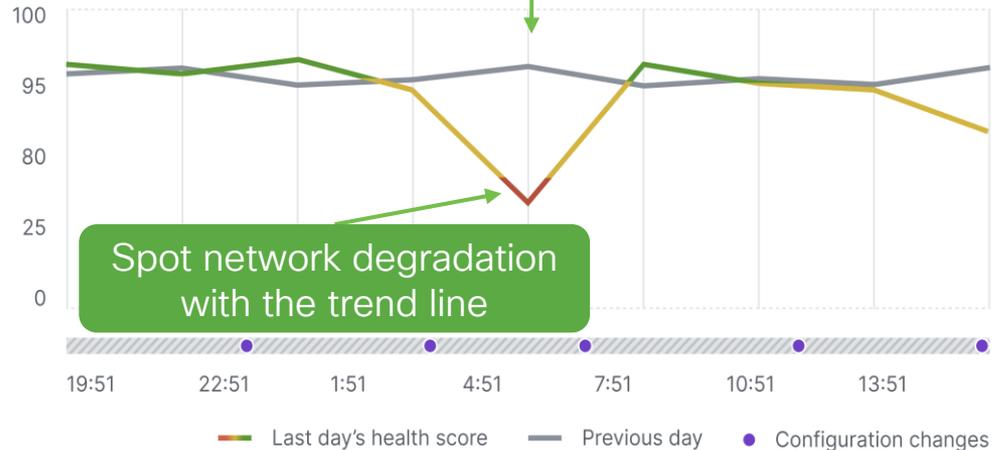
## Proactive Insights, Trusted Uptime



### Network health score ⚠ Fair ⓘ

Some end clients are unable to access their applications and have moderate interruption from the network.

Overall network score and insights



# Client Impact Module

**Clients** 130 total ✔ Good

✖ **Wireless** 3 issues  
33 Clients impacted

✔ **Wired** 0 issues

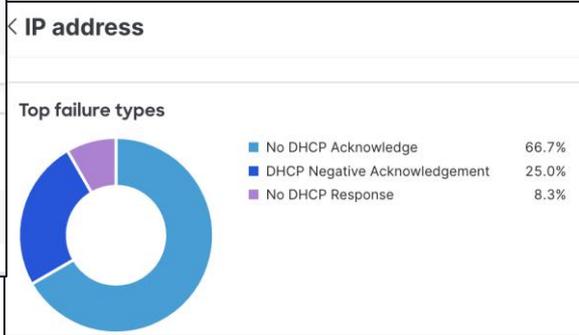
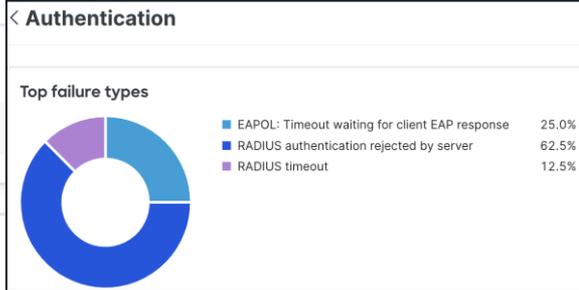
- **Remote** 0 issues

⚠ **Wireless**  
3 issues · 56 impacted clients

**Association**  
41 Clients impacted

**Authentication**  
7 Clients impacted

**IP address**  
12 Clients impacted



100/100 0 pts last day

81/100 -11 pts

100/100 +0 pts

-1/100 - pts

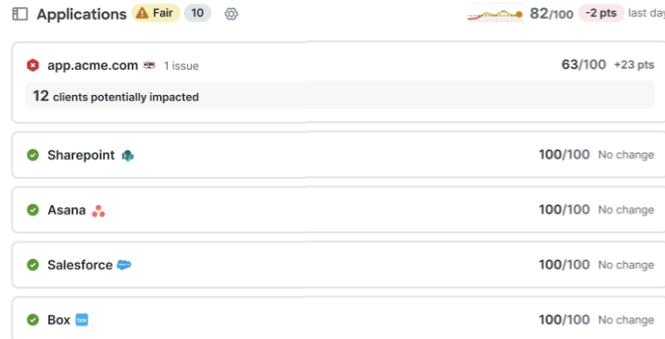
# ThousandEyes Assurance Integration

Seamless Visibility and Proactive Insights



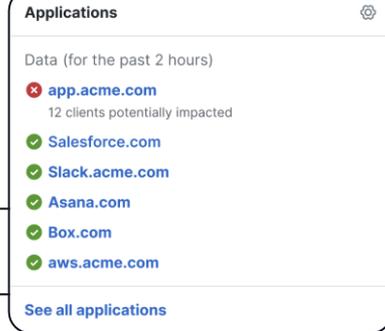
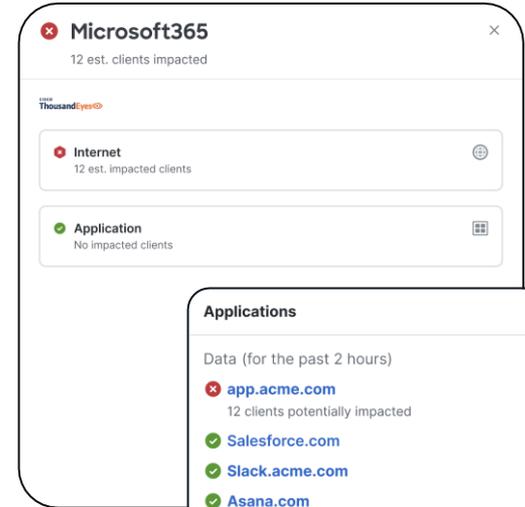
## Assurance Overview Dashboard

- Per-Application Health
- Visibility beyond the WAN
- Internet or application issue
- Single-client workflows



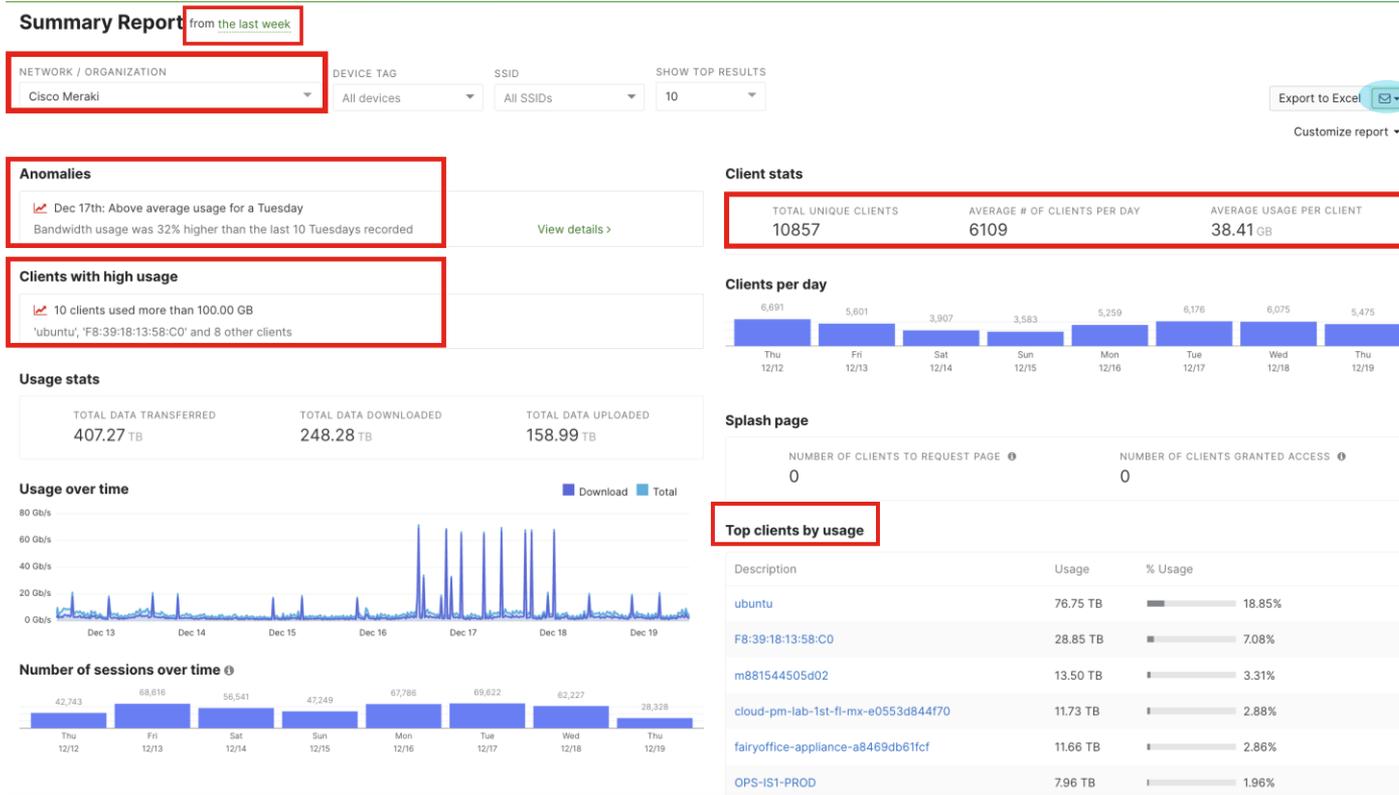
## Single Client Dashboard

### Current client connections



# Summary report

## Transform Data into Actionable Insights



Export to Excel 

Schedule report 

Email

Schedule old report

# Change Log

- Network London ▾
- Secure Connect
- Network-wide
- Assurance New
- Cellular Gateway
- Security & SD-WAN
- Switching
- Wireless
- Systems Manager
- Cameras
- Sensors
- Insight
- Organization

## Cisco Meraki Platform change log

network:"San Francisco - switch" ▾

41 changes in 2985 changes dating back to Dec 30 2022

Download as CSV

Time (UTC) ▾	Admin	Network	SSID	Page	Label	Old value	New value
Nov 26, 2024 23:22	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 15	RSTP: disabled	RSTP: enabled STP Root guard: disabled STP BPDU guard: disabled STP Loop guard: disabled
Nov 26, 2024 23:07	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 16	Name:	Name: CMP CW9176D1
Nov 26, 2024 23:05	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 14	Name:	Name: CMP CW9176I
Nov 26, 2024 23:04	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 15	Name: CMP CW9178I	Name: CMP CW9178I eth1
Nov 26, 2024 23:04	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 13	Name:	Name: CMP CW9178I eth0
Nov 26, 2024 23:03	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 15	Type: access VLAN: 205	Type: trunk Native VLAN: 1
Nov 26, 2024 23:03	TEAdmin6	<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 15	Port: disabled	Port: enabled
		<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 15	Name: MPLS Link	Name: CMP CW9178I
		<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 5	Port: enabled	Port: disabled
		<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 8	Port: disabled Type: access VLAN: 10 Voice VLAN: 20	Port: enabled Type: trunk Native VLAN: 1
		<a href="#">San Francisco - switch</a>		Switch ports	CAMPUS-SFO-IDF2.1.1-MS355-24X / 7	Port: disabled Type: access VLAN: 10 Voice VLAN: 20	Port: enabled Type: trunk Native VLAN: 1

**Monitor**

- Overview
- Summary New
- Alerts
- Change Log ✓
- Wireless LAN Controllers New
- Security Center
- Location Analytics
- Configuration Templates
- VPN Status
- Firmware Upgrades
- Summary Report

**Configure**

- Settings
- Integrations New
- API & Webhooks
- Configuration Sync
- MDM
- Administrators
- Camera and Sensor Roles
- License Info
- Inventory
- SIM Cards New
- Branding
- Policy Objects
- Adaptive Policy
- Cloud On-Ramp
- Cloud Integrations
- Early Access New
- Certificates

**CISCO** *Live!*

BRKMER-2844

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

24

# Event Log



- Network London ▾
- Secure Connect
- Network-wide
- Assurance New
- Cellular Gateway
- Security & SD-WAN
- Switching
- Wireless
- Systems Manager
- Cameras
- Sensors
- Insight
- Organization

## Event log

Client: Any
Before: 12/16/2024 23:56 (GMT)

Event type include: All
Event type ignore: None

« newer
older »

	Category	Event type	Details
25-24p-683a1e4a8e8a	DHCP	DHCP lease	vap: 0, vian: 1, ip: 172.17.1.7 <a href="#">more »</a>
	DHCP	DHCP lease	vap: 0, vian: 10, ip: 172.17.10.16 <a href="#">more »</a>
	BGP	BGP session established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512
	BGP	BGP session no longer established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512, new_state: Close
	BGP	BGP received notification	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512 <a href="#">more »</a>
	BGP	BGP session established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512
	BGP	BGP session no longer established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512, new_state: Close
	BGP	BGP received notification	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512 <a href="#">more »</a>
	Meraki VPN	VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 155.190.209.3:35013, connectivity: true
	BGP	BGP session established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512
	Route tracking	Route connection change	peer_type: i3_vpn, peer: BC:33:40:C9:6C:7E, connection_status: connected
	Meraki VPN	VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 155.190.209.3:35013, connectivity: true
	Route tracking	Route connection change	peer_type: i3_vpn, peer: BC:33:40:C9:6C:7E, connection_status: disconnected
	Meraki VPN	VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 155.190.209.3:35013, connectivity: false
	Meraki VPN	VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 155.190.209.3:35013, connectivity: false
	BGP	BGP session no longer established	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512, new_state: Close
	BGP	BGP sent notification	peer_ip: 6.11.167.137, local_as: 64512, remote_as: 64512 <a href="#">more »</a>

for endpoints  
 for cellular gateways  
 for security appliances  
 for switches  
 for access points  
 for cameras  
 for sensors  
 for Catalyst switches

peer\_ip: 6.11.167.137, local\_as: 64512, remote\_as: 64512 [« hide](#)  
 error\_code 4  
 error\_subcode 0  
 desc Hold timer expired

Monitor
 

Clients	General
Traffic Analytics	Administration
Topology	Alerts
<b>Event Log</b> ✓	Group Policies
Map & Floor Plans	Users
Compliance	Add Devices
	VLAN Profiles



# More on Meraki Splunk Integration?

<https://www.youtube.com/watch?v=5jkwb2xgBQs>

<https://www.youtube.com/watch?v=R1B-YuF-7M8>

# Topology

## Instant Network Map with Zero Prep!

The screenshot displays the Cisco Network-wide Topology interface. The left sidebar contains navigation options: Network London, Secure Connect, Network-wide (highlighted with a red box), Assurance (New), Cellular Gateway, Security & SD-WAN, Switching, Wireless, Systems Manager, Cameras, Sensors, Insight, and Organization. The main area shows a network map with nodes and connections. The top navigation bar includes tabs for L2 - Link layer and L3 - Networking layer, along with Expand/Collapse buttons, a search bar, and status indicators for 8 online and 2 alerting devices. A 'Label all devices' checkbox is checked. A red box highlights the 'Network-wide' menu item, which is expanded to show 'Monitor' (Clients, Traffic Analytics, Event Log, Map & Floor Plans, Compliance) and 'Configure' (General, Administration, Alerts, Group Policies, Users, Add Devices, VLAN Profiles) options. A yellow box highlights a device: BRANCH-LON-MDF1.1-MS125-24P (MS125-24P), showing 9 active ports and 16 direct clients. Another yellow box highlights a device: BRANCH-LON-1.3-CW9162I (CW9162I), showing 2 direct clients and a 'Country detection mismatch' alert. A red box highlights the alert message: 'This device has disabled the 6 GHz frequency band because there are no active SSIDs using WPA3 encryption.' A green checkmark icon is visible in the bottom left corner of the interface.

# Clients Page

**Uplinks** 2 total  
All Online

**WAN appliances** 1 total  
All Online

**Access points** 3 total  
1 Alerting

Usage: 11.71 GB (↓8.41 GB, ↑3.3 GB)

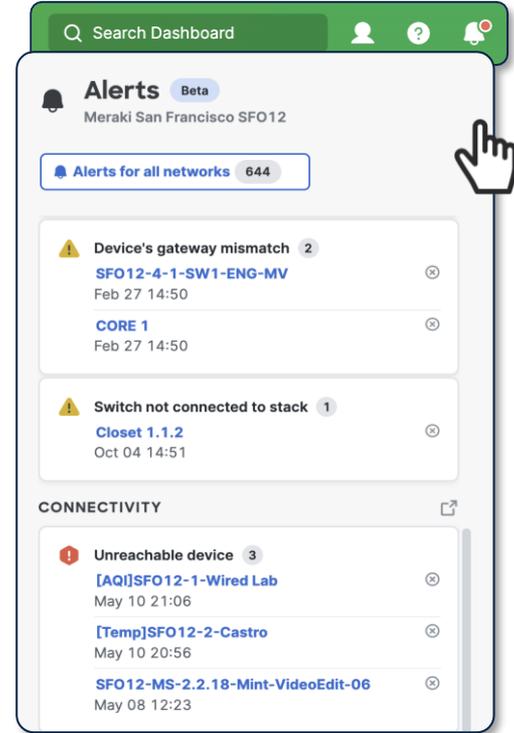
Search for clients: [Search for clients] Status, type, OS [v] Connected to [v] VLAN [v] Policy [v] 22 results [Download]

Status	Description	VLAN	MAC address	IPv4 address	Port	Connected to	Usage	Adaptive policy group
Wired	9c:38:18:1a:9c:81	1	9c:38:18:1a:9c:81	172.17.1.12	10	BRANCH-LON-MDF1.2-MS130-8X	1.51 GB	—
Wired	Ben Nugent	10	00:ce:39:d0:fe:7b	172.17.10.15	5	BRANCH-LON-MDF1.1-MS125-24P	1.41 GB	—
Wired	Val Johnson	10	00:ce:39:c8:76:7b	172.17.10.13	1	BRANCH-LON-MDF1.1-MS125-24P	1.35 GB	—
Wired	Switch	0	b4:4c:90:20:06:80	172.31.128.83	—	BRANCH-LON-MDF1.1-MG52	1.29 GB	—

# Alerts Hub

## Network-level

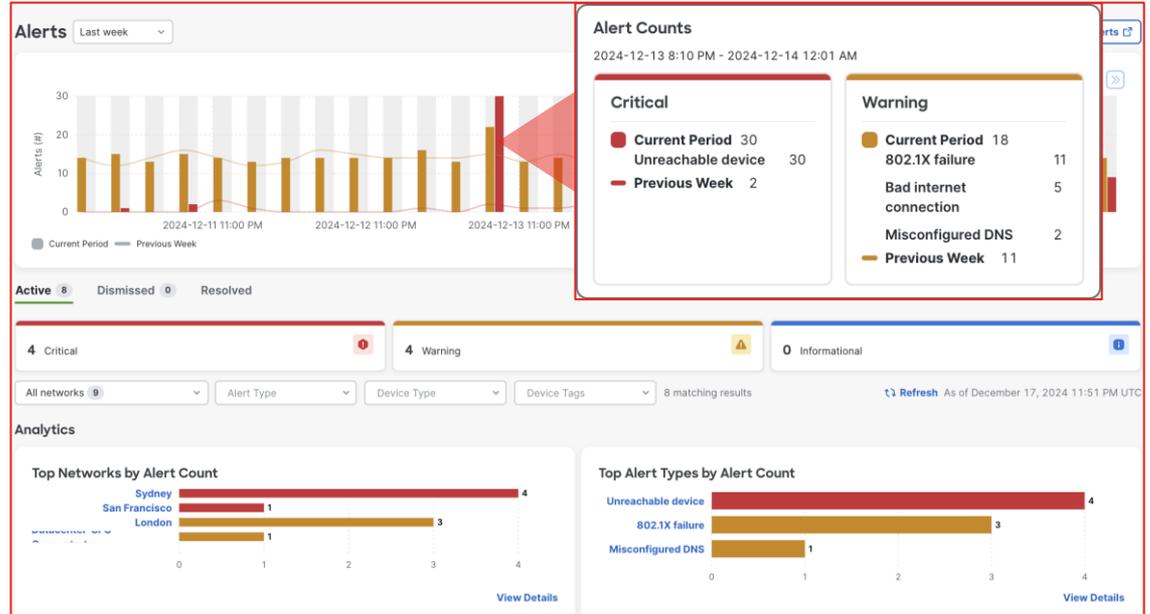
- Alerts are always one click away
- Quickly navigate to the problematic device
- Inline links to step-by-step troubleshooting
- Consolidates alerts from a single network.



# Organization Alerts

## Organization level

- A timeline/trend line
- Analytics graphs
- All alerts in a single place



# Packet Capture

CISCO *Live!*



# Legacy Packet Capture



**Network-wide**

- Monitor
- Assurance
- Security & SD-WAN
- Switching
- Wireless
- Insight

**Packet capture** for security appliances

Security appliance: 14:9f:43:1a:64:0a

Interface: Internet

Output: Download .pcap file (for Wireshark)

Duration (secs): 60

Filter expression:

File name: PL-KRK04-POD1 - appliance\_MX-14\_9f\_43\_1a\_

**Start capture**

**Sample filter expressions**

- host 10.1.27.253**  
packets to and from ip address 10.1.27.253
- host 10.1.27.253 and port 53**  
packets to and from ip address 10.1.27.253 and port 53
- icmp[icmptype] != icmp-echo a**  
all ICMP packets that are not echo
- ether host 11:22:33:44:55:66**  
packets to and from ethernet host 11:22:33:44:55:66
- pppoes and ip**  
IP packets encapsulated in PPPoE

See more [examples](#).

The maximum packet capture duration is 60 seconds. This capture will stop after 60 seconds.

**Current client connection**

2c:1a:b2:d4:3d:04

2c:3f:0b:be:7f:e2

34:56:fe:2c:8b:c9

14:9f:43:1a:64:0a

**Focused Capture**

[View more details](#)

**Packet capture**

Name	Device type	LAN IP
	MS120-8LP	192.168.128.3 (via DHCP)

**Services** for the past 7 minutes

- ✓ No DNS problems detected
- ✓ No RADIUS issues detected
- ✓ No OSPF routing issues detected
- ✓ No L3 host issues detected

# Intelligent Capture

**Packet capture** For access points ▾

**New capture** Stored captures Proactive PCAP Enablement

**Access Points**  
Access Points Select ▾

**Interface**  
Wireless ▾

**Output**  
Save to cloud ▾

**Duration (secs)** ⓘ  
60

**Capture filters**

[View example filters](#)

**File name**  
karthik.iy\_2024-07-19T23:54:34Z

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

**Start capture**

1: Capture Device

2: Output

3: Duration

4: Filters

5: File name

6: Notes

7: Start Capture

## Sample Filter Expressions

### DHCP

port 68 or port 67 [Copy](#)

### Subnet Filter e.g. net 10.168.10.0/24

net {subnet/mask} [Copy](#)

### DNS or DNS over TLS

port 53 or port 853 [Copy](#)

### RADIUS

port 1812 or port 1813 or port 1645 or port 1646 [Copy](#)

### ⚠ Selected device is currently unsupported

CS based switches (MS390/C9300-M) and Cloud monitored Catalyst do not yet support Intelligent Capture. This will be added in a future release. For now please use the legacy mode by clicking the button below.

[Cancel](#) [Go to legacy](#)

# Proactive PCAP Enablement

## Network-wide > Intelligent capture

- Navigate to Proactive PCAP Enablement tab
- Select Enable the auto capture for some devices.
- You can choose to enable this feature on a per access point basis, by tag, or for all devices
- To view proactive captures, go to the Network-wide > Monitor > Clients page and select the client you are troubleshooting from the list.

The screenshot shows the 'Packet capture' configuration page for access points. The 'Proactive PCAP Enablement' tab is selected. Under 'Proactive PCAP enablement', the option 'Enable the auto capture for some devices' is selected. Under 'Select devices', three tags are visible: 'Living room 9162', 'Mesh', and 'Upstairs 9166'. Under 'Select tags', the tag 'recently-added' is visible. A 'Save' button is located at the bottom left of the configuration area.

# Use Assurance to View Proactive PCAP Taken for Clients

CLIENTS Try new version

Roomba-3144460C51007770 

Overview Connections Performance Roaming **Timeline** Stored captures

History 05:27 to 17:26

SSID	ACCESS POINT	BAND	CONNECTION STEP	STATUS	PACKET CAPTURE
All SSIDs	All Access Points	All bands	All connections	All statuses	Yes 

Jul 22 09:30:13	● Successful connection to SSID <a href="#">msnjs2023</a> for a few seconds on access point <a href="#">CW9178-minse</a> .				Packet capture
	CHANNEL	BAND	SNR ⓘ		
	6	2.4 GHz	● 34 dB		
					<a href="#">Download packet capture</a> <a href="#">View in packet viewer</a>
Jul 22 09:30:13	● Failed connection to SSID <a href="#">msnjs2023</a> on access point <a href="#">CW9178-minse</a> during association.				Packet capture
	CHANNEL	BAND	SNR ⓘ		
	6	2.4 GHz	● 34 dB		

# Packet Capture Analysis

## Effortless Packet Diagnostics

- Analyse common issues (DHCP, ARP, ICMP) quickly
- Supports uploaded, scheduled, or proactive captures
- Provides actionable findings and evidence

### Dashboard Intelligence

**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:0a:60:38
- a8:46:9d:fd:dd:59
- 2c:3f:0b:d4:95:e9
- 00:1f:ca:b3:31:c0
- 52:54:dd:99:3b:a8
- e0:d3:b4:fd:96:74
- 68:3a:1e:0a:1c:f6

**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

- ARP Requests have responses Failed 13

**ICMP** 2/2 tests failed

- Missing ICMP responses Failed 2

**Missing ICMP responses**

**ICMP request to 8.8.8.8 has no response**

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

**Packets**

**Details** ICMP request failed from 172.20.193.76 to 8.8.8.8

**ICMP request to 172.20.193.81 has no response**

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

**Packets**

**Details** ICMP request failed from 10.92.135.56 to 172.20.193.81

# Capturing Traffic on Multiple Interfaces

A complete picture of how traffic is flowing

- New Tab to the Right
- Add Tab to Reading List
- Add Tab to New Group
- Move Tab to Another Window >
- Reload
- Duplicate

The screenshot shows the Meraki dashboard interface for a network named 'Meraki London - Finsbury LON11'. The 'Packet capture' section is active, showing the following configuration: Security appliance: LON11-MX1, Interface: LAN (highlighted with a red box), Output: Download .pcap file (for Wireshark), Duration (secs): 60, Filter expression: (empty), and File name: Meraki London - Finsbury LON11 - appliance\_1. A blue 'Start capture' button is visible at the bottom.

The screenshot shows the Meraki dashboard interface for the same network. The 'Packet capture' section is active, showing the following configuration: Security appliance: LON11-MX1, Interface: Internet 1 (highlighted with a red box), Output: Download .pcap file (for Wireshark), Duration (secs): 60, Filter expression: (empty), and File name: Meraki London - Finsbury LON11 - appliance\_1. A blue 'Start capture' button is visible at the bottom.

Why it matters?

# 1:1 NAT

## WAN and LAN Traffic on an MX Security Appliance

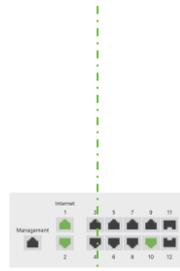
104.17.32.2 1:1 192.168.128.29

WAN

No.	Time	Source	Destination	Protocol	Source MAC	Dest MAC	Size
1	0.000000	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
2	1.018323	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
3	2.013596	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
4	3.027540	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
5	4.031133	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
6	5.044046	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
7	6.059167	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
8	7.062156	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
9	8.076536	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74
10	9.074916	66.74.83.217	104.17.32.2	ICMP	Meraki_B5:dd:e4	Meraki_07:11:05	74

LAN

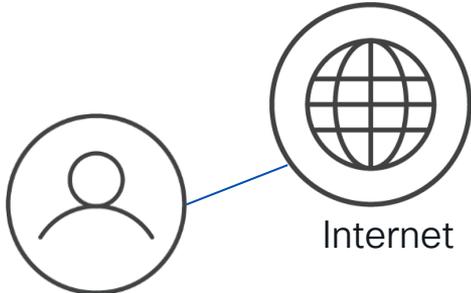
No.	Time	Source	Destination	Protocol	Source MAC	Dest MAC	Size
1	0.000000	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
2	1.014245	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
3	2.012565	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
4	3.022080	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
5	4.026161	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
6	5.040105	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
7	6.043690	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
8	7.057131	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
9	8.071732	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78
10	9.074721	66.74.83.217	192.168.128.29	ICMP	Meraki_07:11:04	Dell_27:09:36	78



MX86

Pre-Processed

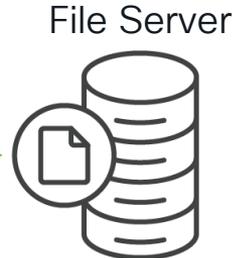
Post-Processed



Internet



MS120



File Server

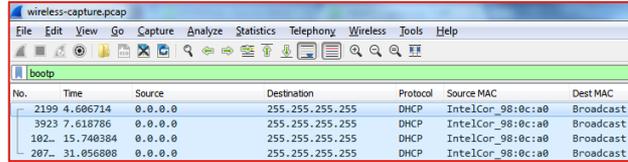
66.74.83.217

192.168.128.29

*CISCO Live!*

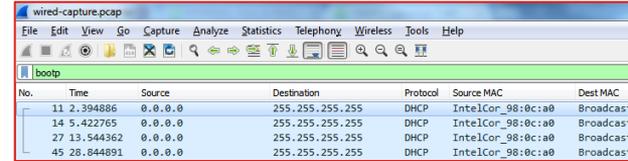
# DHCP

## Wireless and Wired Traffic on an MR Access Point



wireless-capture.pcap

No.	Time	Source	Destination	Protocol	Source MAC	Dest MAC
2199	4.606714	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
3923	7.618786	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
102.	15.740384	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
207.	31.056808	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast



wired-capture.pcap

No.	Time	Source	Destination	Protocol	Source MAC	Dest MAC
11	2.394886	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
14	5.422765	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
27	13.544362	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast
45	28.844891	0.0.0.0	255.255.255.255	DHCP	IntelCor_98:0c:a0	Broadcast



# Live Tools Demo

CISCO *Live!*



IPv6  
is Coming

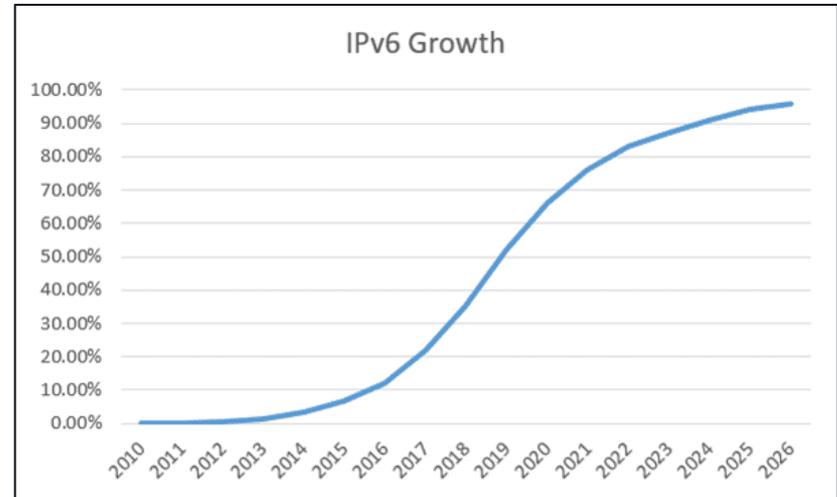




# IPv6

## Embracing the Future: IPv6 Transition and Troubleshooting

- **Larger** addressing space
- Simpler header (No IP-level checksum)
- **Efficient** forwarding/routing
- Simplified Network Configuration
- Auto-configuration (SLAAC)





# Troubleshooting IPv6

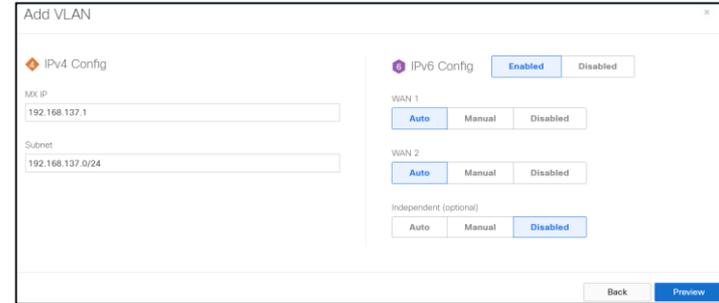
All Cisco Meraki networking devices can pass IPv6 traffic

Same link-local and solicited-node multicast for all VLANs

- ✓ Useful for analyzing pcaps and general IPv6 troubleshooting

Tools for IPv6 are the same as those available for IPv4

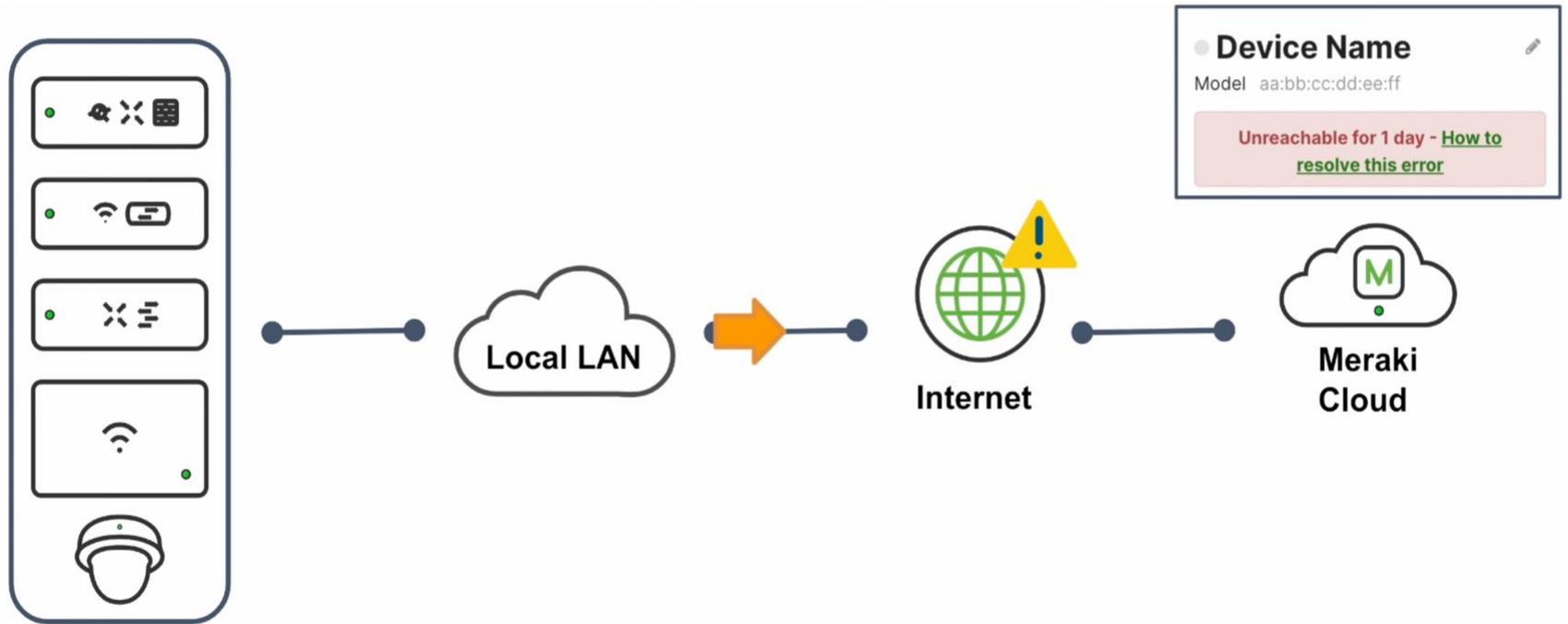
- ✓ Ping
- ✓ Traceroute
- ✓ MTR
- ✓ DNS Lookup



ID ▲	VLAN name	Version	Config	VLAN interface IP	Uplink	Group policy	VPN mode
1	Management	4	Manual	10.0.60.254/24	Any	None	Enabled
		6	Manual	2001:::2001:::64	WAN 1		
		6	Auto	fe80:::2001:::0f5 (Link-local)	--		
		6	Auto	ff02:::2001:::0f5 (Solicited node multicast)	--		

# Local Status Page (LSP)





# Out-of-Band Log Fetching (OOB) Support Data Bundle (SDB)



For troubleshooting issues on devices that are unable to be accessed via the cloud.

Meraki

Connection Uplink configuration Switch ports status Switch ports configuration

Uplink configuration  
Configure the uplink Internet connection on this switch.

IP configuration

IP assignment

VLAN

IPv6 assignment

Web proxy  
HTTP will be used for the device to communicate with the Cisco Meraki cloud if UDP communication is blocked

Use a proxy?

**Download support data**  
Download diagnostic information about this device for Support to examine. This can take several minutes.  
**Do this only if requested by Cisco Meraki Support.**

© Cisco Systems, Inc.



Encrypted



15sec to 1min

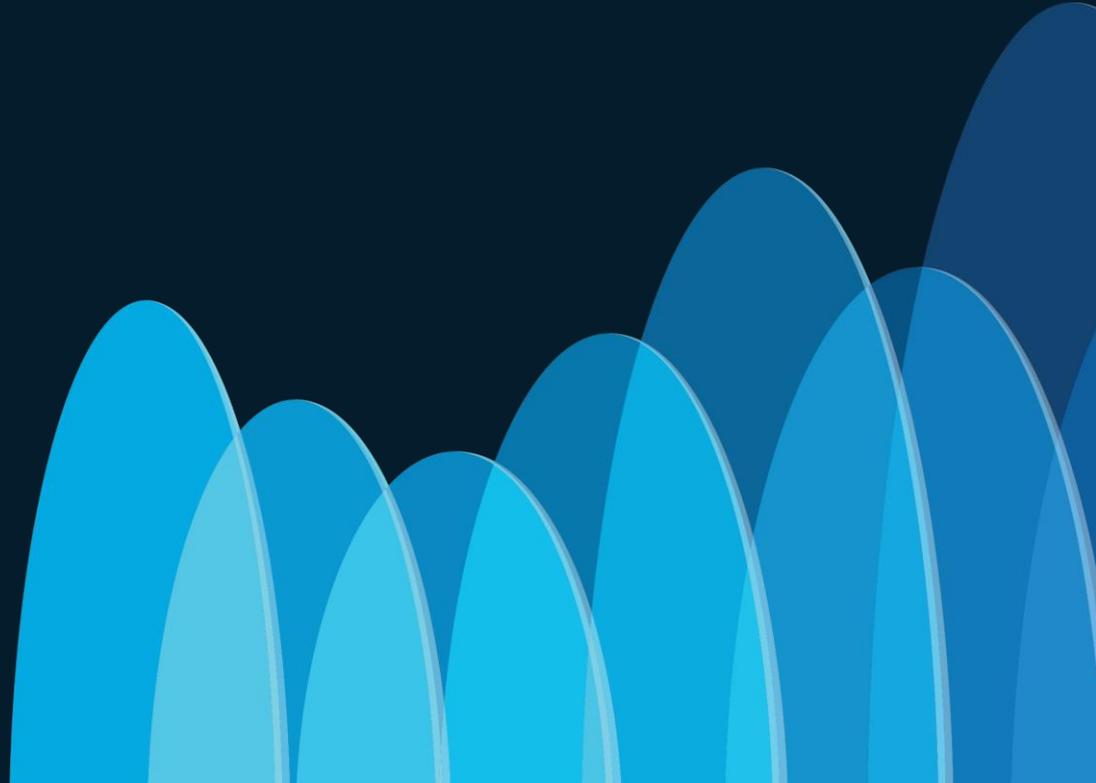


Meraki support

It's recommended to use an up-to-date version of Chrome, Firefox, or Safari

**cisco** Live!

# Troubleshooting



# Cisco Meraki Study

- ✓ IT departments **spend** 43% of their time troubleshooting issues in enterprise networks alone.
- ✓ 42% of organizations **saved** 50-70% or more time deploying, maintaining, and troubleshooting IT since they began using **Meraki**.

# Dashboard Intelligence

CISCO *Live!*



# Root Cause Analysis

## Guided Troubleshooting Flow

### CRC

Configuration Mismatch issue

Cable and other issues

**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](#)

[Give your feedback on these alerts](#)

© 2022 Cisco Systems, Inc. [Give your feedback](#)

**Suggested fix**

CRC errors detected  
Very high CRC error detected on **MS120-8FP/1**

**Suggested fix: cable test**

A damaged cable can cause CRC errors.

⚠ Testing the cable may disrupt the traffic on this port

[Cancel](#) [cable test](#)

[Give feedback about this alert](#)

[Documentation on CRC errors](#)

### VLAN Mismatch

**Health**

UPLINK(S) 1/1 healthy MIX 1/1 healthy SWITCHES 3/5 healthy

**Clients** all - for the last day -

4 client devices

Status	Description	Last seen	Usage	Device type, OS	IPv4 address
🟢		Feb 16 09:32	232 KB	Other	192.168.129.1
🟡	98-18-88-00-5b-81	Feb 16 09:14	113 KB	Other	192.168.128.155
🟡		Feb 16 09:27	108 KB	Other	192.168.128.77
🟡	98-18-88-01-46-81	Feb 16 09:24	93 KB	Other	192.168.128.147

**Suggested fix**

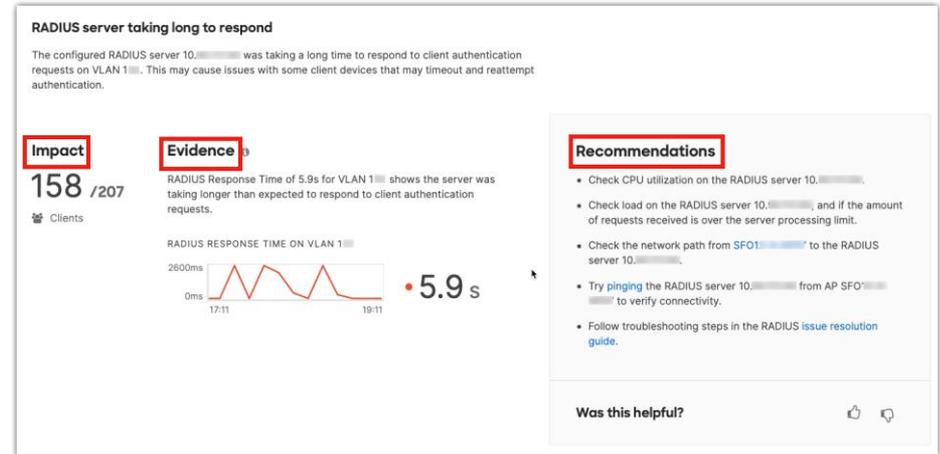
Port VLAN mismatch  
VLAN mismatch error between **MS425 / 31** and **standalone 2 / 1/MA-MOD-4X10G/4**

© 2022 Cisco Systems, Inc. [Give your feedback](#)

# MR Automated Root Cause Analysis

Impact, evidence and recommendation

- Correlates network events for deeper insights.
- Identifies the scope of network issues.
- Provides actionable resolution steps.



# Smart Thresholds

## Intelligent Limits for Enhanced Network Oversight

- Detects anomalies using intelligent, data-driven thresholds
- Reduces false alarms by adapting to network behaviour
- Highlights potential issues for proactive troubleshooting

7 anomalies detected over 7d



**Network-wide** Configure

- Traffic Analytics
- Topology
- Intelligent Capture
- Administration
- Alerts** ✓
- Group Policies

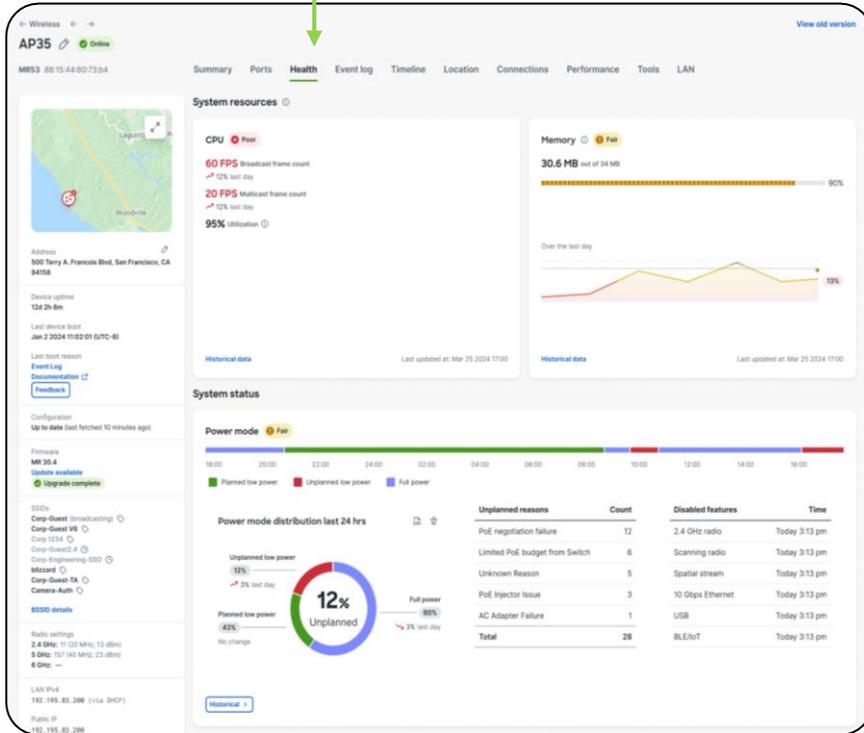
Clients fail to connect to the wireless network

Enable smart thresholds

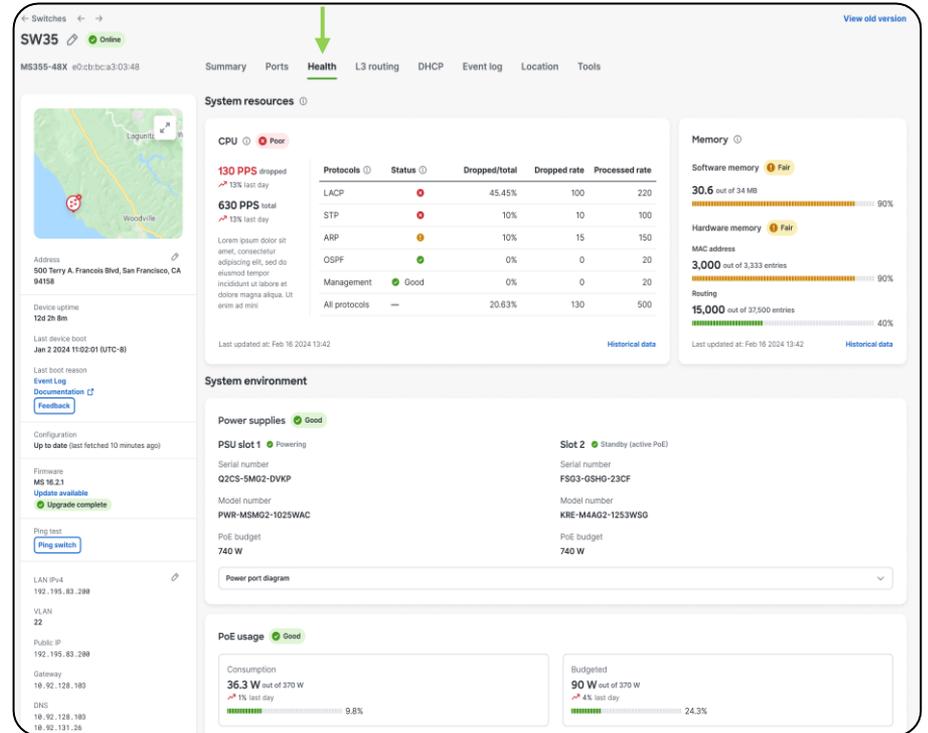
# MR and MS Health Tab

Top-down assurance overview to single device troubleshooting workflow

New wireless Health tab



New switches Health tab



# API-Driven Troubleshooting

CISCO *Live!*

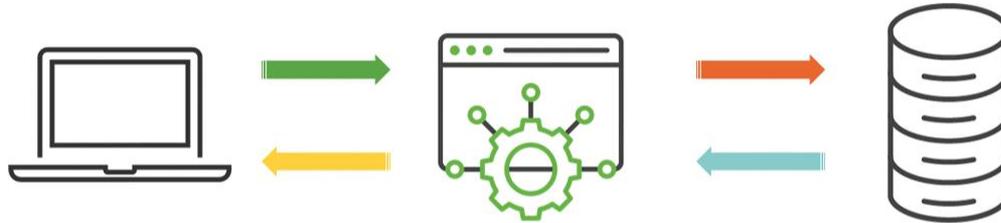




# Meraki Dashboard API

## How do APIs work?

---



1. User initiates an API request through the API's Uniform Resource Identifier (URI).
2. API receives the request and makes a call to the server.
3. Server sends a response containing the requested data to the API.
4. API forwards the requested data to the User.

- [Meraki Developer Hub](#)
- [Postman Collections](#)



# Uses of the Meraki Dashboard API

include, but are not limited to

**1**  
Add new organizations, admins, networks, devices, VLANs and SSIDs

**2**  
Use automation scripts to rapidly provision multiple new sites

**3**  
Automatically onboard and off-board teleworker devices

**4**  
Build dashboards designed to meet the needs of unique use cases



# Access and utilize Meraki Dashboard APIs

API key acts as the equivalent of a username and password

To generate an API key:

- ✓ Navigate to Organization > Configure > API & Webhooks
- ✓ Select the Overview tab
- ✓ Click Generate API Key

The screenshot shows the Cisco Meraki Dashboard interface. The top navigation bar is green with the Cisco Meraki logo. The main content area is divided into a left sidebar and a main panel. The sidebar contains navigation options: Global Overview, Organization (Sample Org Inc.), Network (Head Office, Network-wide), Security & SD-WAN, Switching, Wireless, Cameras, and Organization (selected). The main panel is titled 'API & Webhooks' and has three tabs: Overview (selected), API keys and access, and Webhooks. Under the 'Overview' tab, there is a section for 'API monitoring and management' with a list of bullet points: 'Generate and manage API keys and permissions', 'Monitor API usage, success, and failure rates (coming soon)', and 'Track marketplace application integrations (coming soon)'. A 'Generate API Key' button is highlighted with a red box, with a note 'Maximum of 2 keys' next to it. Below this is a 'Quick links' section with links to 'Meraki API documentation' and 'Meraki community'.



# Troubleshooting API requests

- What **call** am I trying to make?
- Is this call **appropriate** for the information I'm trying to return, update, post, or delete?
- What **behavior** is the API call displaying, and is it expected?\*
- What data or response code is the API call returning?\*\*\*

## Common Errors and Behaviours

Status Code	Error Notification	Description and Troubleshooting
200	OK	The API request has been <b>successfully completed</b> and a response has been received from the server.
400	Bad Request	This error indicates a <b>malformed JSON payload</b> . Validate the text/JSON being used with a tool like jsonlint.com
401	Unauthorized	This error indicates an issue with the <b>API key</b> inputted. Confirm that the API key is correct.
403	Forbidden	This error occurs when a <b>read-only admin</b> attempts a call that will alter data in the dashboard ( <b>PUT/POST/DELETE</b> ). Adjust account admin rights if user must be able to return these calls.
404	Not Found	This error indicates an issue with the API endpoint. Confirm that the API endpoint/URL is correct.
429	Too Many Requests	This error indicates that the user has submitted more than the <b>maximum allowed API calls</b> per second, per organization. For Meraki Dashboard APIs, this limit is 10 calls. This error will also appear if: <ul style="list-style-type: none"><li>• One organization reaches the limit for API calls made across multiple organizations</li><li>• Limit is exceeded when sourced from a single IP</li></ul>
500	Server Error	This error is most likely related to an <b>application error</b> and will require further investigation.
502/504	Request time out	This error occurs if the API request took longer than <b>60 seconds</b> to process and may require further investigation to establish a cause.

\*API call responses contain a code that indicates the status of the information returned.

\*\*Meraki Dashboard APIs use standard **RFC 9110 HTTP** Status Codes

# Maximizing Efficiency with Smart API Usage



## Efficient API endpoint

- “Get Organization Devices Statuses”: Pulling all devices can return excessive data, especially with dozens of devices.
- **Inefficient:** Repeatedly pulling the same data leads to unnecessary overhead.
- **Efficient Alternative:** Use “Get Organization Devices Availabilities Change History” which only returns data for devices with status changes (e.g., 10 devices out of 100).
- **No Changes:** If no devices’ status changes, the response will be null, reducing unnecessary data transfer.

## Get Organization Devices Statuses

**Operation Id:** `getOrganizationDevicesStatuses`

**Description:** List the status of every Meraki device in the organization

```
GET /organizations/{organizationId}/devices/statuses
```



## Get Organization Devices Availabilities Change History

**Operation Id:** `getOrganizationDevicesAvailabilitiesChangeHistory`

**Description:** List the availability history information for devices in an organization.

```
GET /organizations/{organizationId}/devices/availabilities/changeHistory
```

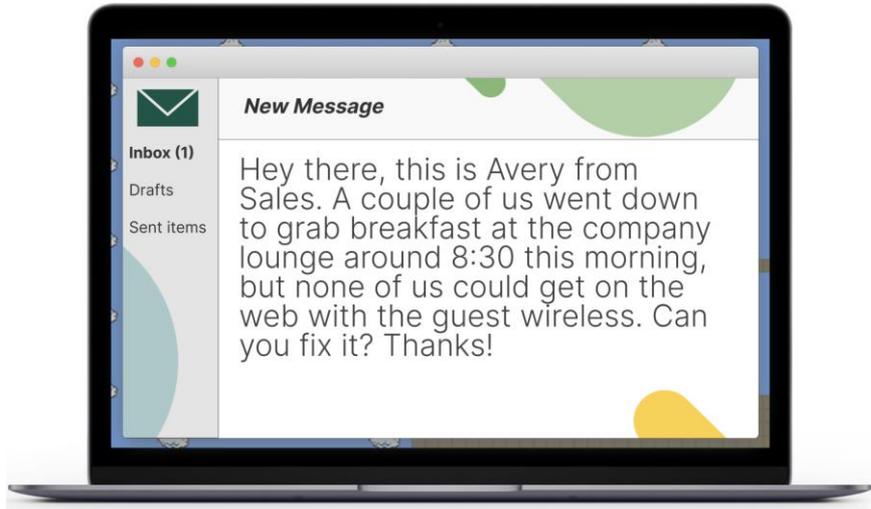
# Real-World Scenario

CISCO *Live!*



# Wireless Network Connectivity

Let's troubleshoot!



# Getting Help

CISCO *Live!*

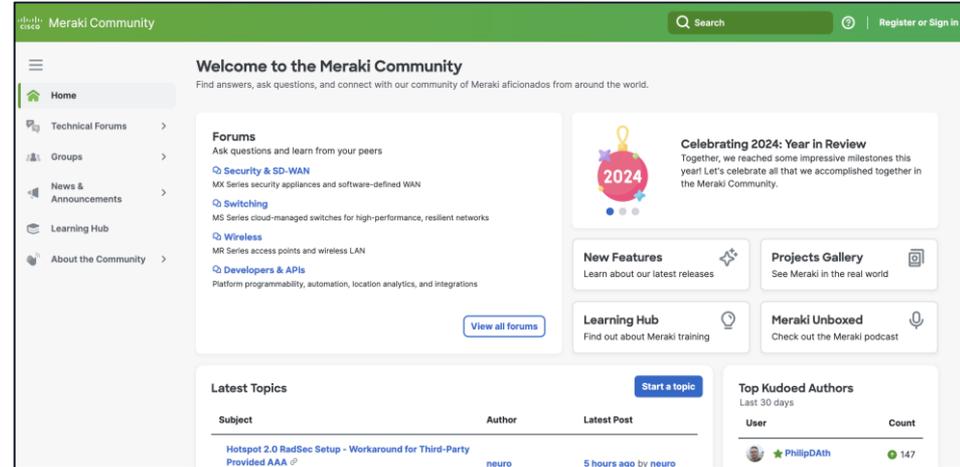


# Meraki Community

- Official Meraki Forum
- Gain insights from experienced Meraki users
- Connect with a global community of peers
- Find answers to common issues
- No additional cost to join.
- Accessible at <https://community.meraki.com/>



Scan me!



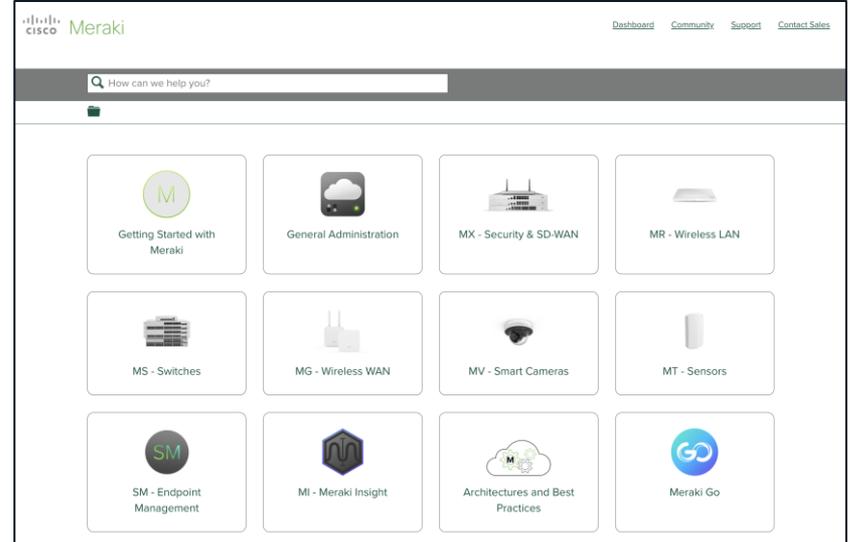
The screenshot shows the Meraki Community website homepage. The header is green with the Cisco logo and 'Meraki Community' text. A search bar and 'Register or Sign In' link are on the right. A left sidebar contains navigation links: Home, Technical Forums, Groups, News & Announcements, Learning Hub, and About the Community. The main content area features a 'Welcome to the Meraki Community' message, a 'Forums' section with links to Security & SD-WAN, Switching, Wireless, and Developers & APIs, and a 'View all forums' button. There are also promotional tiles for 'Celebrating 2024: Year in Review', 'New Features', 'Projects Gallery', 'Learning Hub', and 'Meraki Unboxed'. At the bottom, there are sections for 'Latest Topics' (with a table) and 'Top Kudoed Authors'.

Subject	Author	Latest Post
Hotspot 2.0 RadSec Setup - Workaround for Third-Party Provided AAA	neuro	5 hours ago by neuro

User	Count
PhilipDATH	147

# Meraki Documentation

- Comprehensive Knowledge Base
  - Searchable and Organized
  - Always Up-to-Date
  - Backed by Experts
  - Accessible either at <https://documentation.meraki.com/>
- Or via Help>Get help on the dashboard



# Meraki Support

## Recommended Actions and Best Practises



### 24x7 Telephone and E-mail support

- ✓ Error or Log Analysis: Open an **email** case and attach a screenshot of the error/log
- ✓ Service Impact: **Call** support immediately for **urgent or complex** issues
- ✓ Root Cause Analysis (RCA) Needed: **Avoid rebooting**; contact TAC first

\*Connect to support more easily using the **“Call Me Now”** option in the dashboard—no need to dial manually; the system links you directly to an engineer to support you.

Navigate to '?' icon > 'Get help & cases' > documentation > call me now



# More on Call Me Now feature and Contacting Support

- [https://documentation.meraki.com/General\\_Administration/Support/Contacting\\_Support](https://documentation.meraki.com/General_Administration/Support/Contacting_Support)
- [https://documentation.meraki.com/General\\_Administration/Support/Contacting\\_Support/Call\\_Me\\_Now](https://documentation.meraki.com/General_Administration/Support/Contacting_Support/Call_Me_Now)

# Practical Tips



# Smart Configuration for Better Performance

Security & SD-WAN > SD-WAN & traffic shaping

- **Traffic shaping**

Use traffic shaping to prioritize critical applications.

- **Bandwidth**

Adjust bandwidth settings based on your environment's needs.

The screenshot shows the 'Traffic shaping rules' configuration page. It includes settings for 'Per-client bandwidth limit' and 'Per-SSID bandwidth limit', both set to 'unlimited'. There are also checkboxes for 'Enable SpeedBurst' and 'Enable default traffic shaping rules'. Below these settings is a table of default rules.

Traffic Type	DSCP tag
SIP (Voice)	46 (EF - Expedited Forwarding, Voice)
All Advertising, All Software Updates, All Online Backups	10 (AF11 - High Throughput, Latency Insensitive, Low Drop)
WebEx, Skype	34 (AF41 - Multimedia Conferencing, Low Drop)
All Video & Music	18 (AF21 - Low Latency Data, Low Drop)

There are no traffic shaping rules.  
[Create a new rule](#)

**Pro Tip:** Regularly review and update settings as new applications or devices are added to the network

# Stay Informed: Enable Alerts Proactively

Network-wide > Alerts

- **Major** Events

Set up for key events like device downtime.

- **Minor** Events

Avoid excessive notifications for minor events.

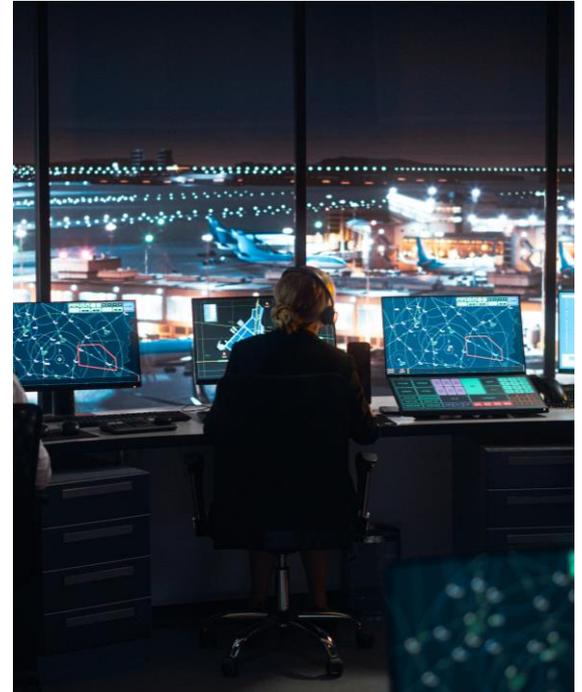
- **Tailor** Alerts

Customize alerts to match your network's needs.

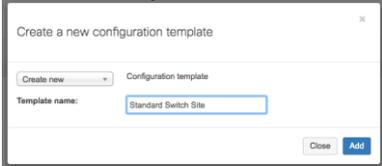
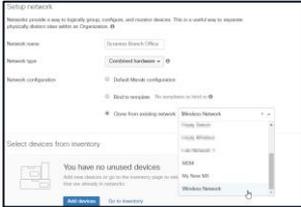
- **Real-Time** Alerts

Use email notifications or webhooks for real-time alerts and integration.

[Available Alerts](#)



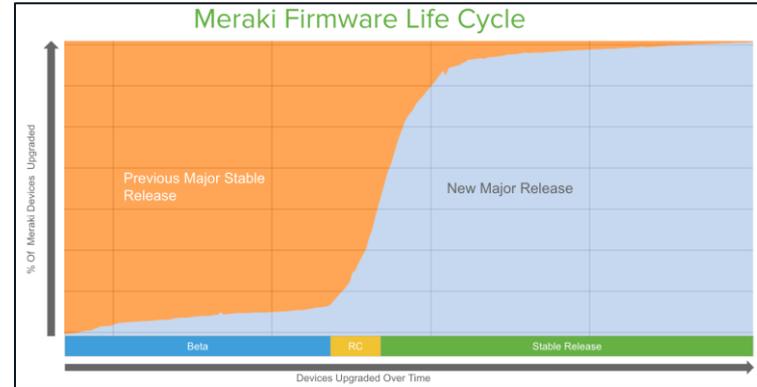
# Automate Device Management and Configuration

Templates	API	Clone	Firmware
<p>Deploy configuration updates across <b>multiple locations quickly</b></p>  <p>The screenshot shows a dialog box titled "Create a new configuration template". It has a "Create new" dropdown menu set to "Configuration template". Below that, there is a text input field for "Template name" containing "Standard Switch Site". At the bottom right, there are "Close" and "Add" buttons.</p>	<p>Leverage API integrations for custom automation</p>  <p>The icon depicts a central gear with several nodes connected to its perimeter, representing network automation or API integration.</p>	<p>Clone networks or templates to deploy identical settings faster</p>  <p>The screenshot shows a network configuration interface. It includes sections for "Network name", "Network type" (set to "Configured hardware"), "Network configuration" (with options for "Default Network configuration" and "Match template"), and a "Select devices from inventory" section. A message at the bottom states "You have no unused devices".</p>	<p>Enable Auto-Update for Firmware to keep devices secure and up-to-date automatically</p>  <p>The icon shows a rectangular device with a green arrow pointing down into it, and a circular arrow around the device, symbolizing automatic updates or a refresh cycle.</p>

# Firmware Upgrade

Organization > Firmware Upgrades

- Meraki's **default** firmware settings
  - ✓ No automatic beta firmware deployments
- Review Release Notes
- Leverage **Stable** Firmware Versions
- Test the **beta code** in your designated test networks **first**.
- Monitor the Upgrade Process
- **Revert** if Needed (The rollback option is available for customers for up to 14 days)



The screenshot shows the "Latest firmware versions" page. At the top, there are tabs for "Stable", "Stable release candidate", "Beta", and "Other available versions". A blue banner promotes the cloud-native IOS XE 17.15.1. Below the banner, there are two rows of firmware version cards. Each card includes an icon, the version number, the release date, and a "Release notes" link.

Version	Release Date
MX 18.211.2	Released Jun 5, 2024
MR 31.1.5.1	Released Dec 9, 2024
MV 6.1.2	Released Nov 4, 2024
MT 2.0.1	Released Aug 26, 2024
MG 3.212	Released Sep 19, 2024
CS 17.1.4	Released Nov 15, 2024
MS 17.1.3	Released Dec 5, 2024
IOS-XE 17.12.3	Released Jul 27, 2024

# Conclusion



# For the Curious: Detailed Sessions on Key Topics

Wed, Feb 12 3:30 PM



[DEWKS-2845]  
Automate Meraki Alerting & Response with  
**Webhooks** and AWS Lambda

Wed, Feb 12 4:00 PM



[BRKMER-1887]  
Seeing the Invisible: Integrating **Splunk** and Meraki  
for Large Scale Data Analysis

Thu, Feb 13 8:45 AM



[BRKOPS-2528]  
Succeed with Test-Driven Network **Automation** -  
Practical Examples Using Python and your  
Network's APIs

Thu, Feb 13 3:30 PM



Meraki and **Ansible**: A Collaboration Made in the  
Cloud [DEVNET-1399]

Thu, Feb 13 3:45 PM



[BRKEWN-2399]  
Meraki Wireless from a **Troubleshooter** Perspective

# Key Takeaways



Dashboard = Your Best Friend: Dive in and let it do the heavy lifting

Assurance: Let Meraki **watch** things for you.

PCAP Prodigy: Captures aren't scary—they're your **superpower**.

Troubleshooting – follow the clues with an **open** mind!

Live Tools = Real-Time Magic: Quick fixes are just a click away!

# Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

# Continue your education

- Visit the Cisco Showcase for related demos
- 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 [ciscolive.com/on-demand](https://www.ciscolive.com/on-demand). Sessions from this event will be available from March 3.

Contact me at:

<https://www.linkedin.com/in/lina-al-dwaikat/>

You've Earned the  
Troubleshooter Badge!



# Call Of Action



- ✓ **Deep Dive:** Explore related sessions and [on-demand](#) resources
- ✓ Join the [Community](#): Connect with the Meraki community for insights and support
- ✓ Explore [Learning Hub](#): Boost your skills with the Meraki Learning Hub
- ✓ **Save Time:** Use AI-powered troubleshooting to streamline issue resolution
- ✓ **Stay Proactive:** Monitor and prevent issues with dashboard alerts and insights
- ✓ **Explore More:** Tap into Meraki [Documentation](#) for quick answers

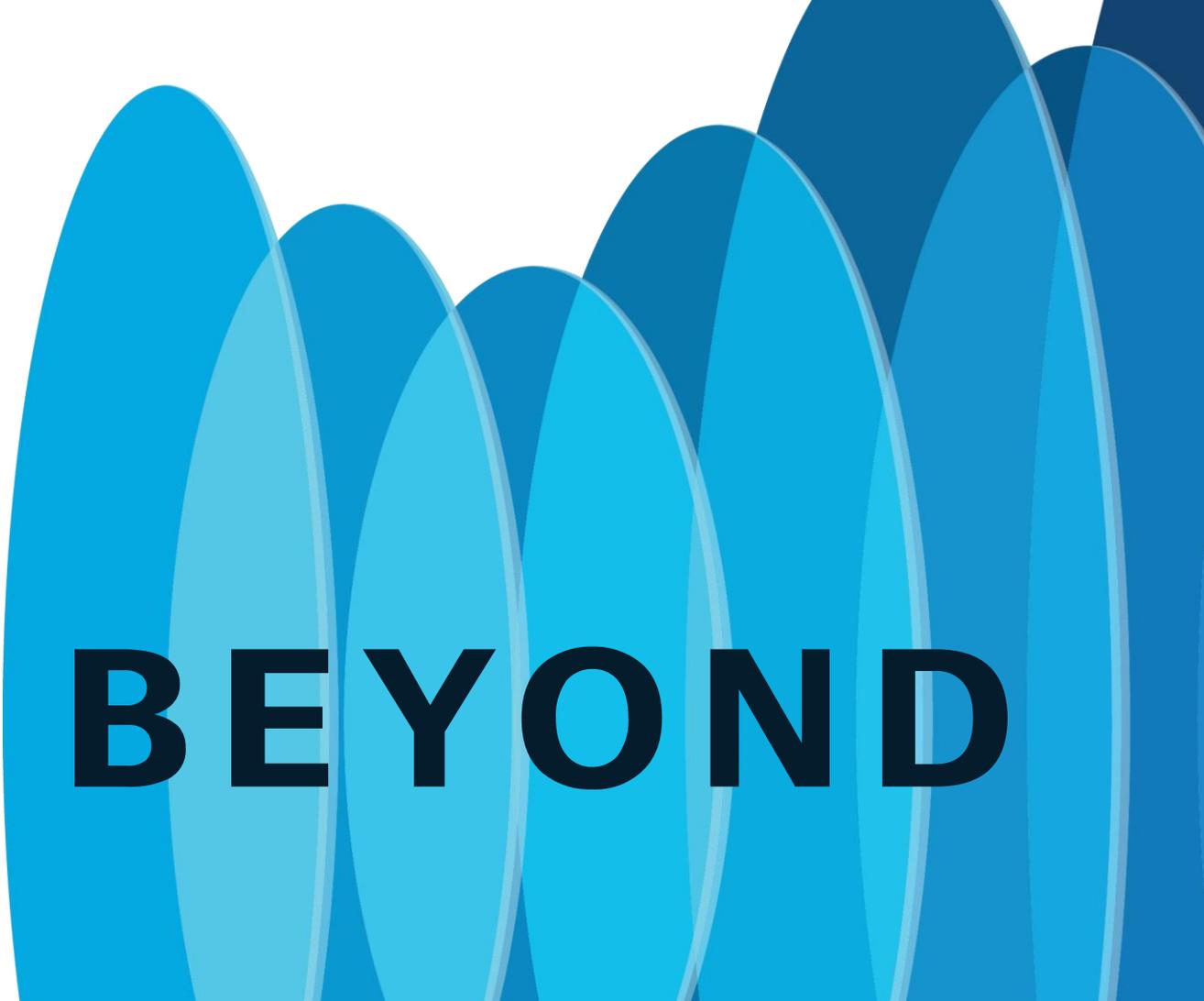


Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

A series of overlapping, rounded, teardrop-shaped abstract forms in various shades of blue, ranging from light to dark, positioned on the right side of the image.