cisco Meraki

White Paper

Wireless Health: Powerful Heuristics for Smarter Troubleshooting

JUNE 2018

This whitepaper explores how Cisco Meraki's Wireless Health feature simplifies root cause analysis for all connected wireless clients in a single dashboard, enabling IT teams to proactively manage and answer complex questions without having to manually dig through the entire network stack.

Table of Contents

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Wi-Fi Deployments: More Complex and Critical than Ever Before

In the decades since it emerged from a niche technology, wireless networking has undergone seismic shifts: from its original 802.11a/b standards to the introduction of 802.11n and dual-band (2.4 GHz/5 GHz) Wi-Fi that, with its support for consistent connection speeds above 100Mbps, opened a path for both corporate and modern wireless internet consumption. Corporate adoption of wireless networks created a market for wireless LAN controllers — on-premise devices that provide centralized management of access points (APs) and which are still used by many organizations today.

The current generation of 802.11ac Wave 2 Wi-Fi APs connect wireless clients at speeds greater than 1 Gbps, enabling IT administrators to deploy Wi-Fi as the primary mode of access — and allowing end users to watch 4K videos, transfer multigigabit files, and to make voice-over-IP (VoIP) calls all while sharing the same wireless link. These advances in speed, combined with Wi-Fi's convenience for end users (who can roam untethered from desks with their mobile devices) and the fact that wireless networks can be 50% cheaper to deploy than traditional wired installations[1], has caused wireless adoption to skyrocket.

As more people connect more laptops, smartphones, wearable trackers, and IoT devices to a given wireless network, complexity increases and the potential for degraded performance looms larger. Access point performance can deteriorate under heavy client loads — but adding more APs for additional capacity can introduce co-channel interference which negatively impacts the very clients they were intended to help. More client connections also mean more points of failure, since there are several steps every device must take to successfully associate and pass traffic on a wireless network — any one of which can go awry for various reasons.

Thus, a vicious cycle of increased client load, interference, and points of failure resulting in lengthy troubleshooting sessions and degraded performance can develop if IT admins are not able to rapidly identify root causes of Wi-Fi problems or be alerted to anomalies in usage before they become serious problems.

[1] https://www.cio.com.au/article/521796/wireless_networks_can_cost_50_per_cent_less_than_wired_report/

Why the Wireless Experience Matters

Despite the increasing complexity of wireless networks, ensuring a positive end user experience is critical for organizations looking to maintain a competitive advantage. Given the exponential increase in wireless demand, the strain on older infrastructure designed primarily for coverage — not capacity — is starkly apparent. Not having a carrier-class wireless network that can handle client load, and that can support cutting-edge use cases for location-based client analytics and insights, can impact business results. For example:

- Today's savvy consumer now expects free and public wireless in a variety of venues: cafes, airports, hotels, hospital waiting rooms — and is making purchasing decisions based on customer reviews of wireless amenities. The Hospitality industry, for example, has taken notice: Meraki has been the global brand standard for IHG for over 2 years, deployed at over 5,300 properties and in 800,000 hotel rooms.
- Retailers know that smart wireless networks let them glean actionable insights into customer foot traffic patterns, time spent in store, and loyalty. This kind of data allows for proximity-based marketing, enabling businesses to make better offers or experiences available to customers at appropriate times (e.g., Prada partners with Cloud4Wi Volare and Cisco Meraki to transform in-store customer experience in over 500 stores worldwide). Retailers like Ladbrokes, the world leader in betting and gaming with over 2,700 outlets across Europe, also rely on Meraki wireless' built-in Location Analytics for real-time footfall data across their stores.
- Organizations are collecting data about queue lengths and wait times at cashier stations and front desks, seeing where clients are congregating within their brick-and-mortar spaces — and using this data to improve operational efficiency during peak busy hours.
- Schools and universities are focusing on connected wireless classrooms, 1:1 tablet initiatives, and more interactive and media-rich student engagement in an effort to keep their curriculums current in the high tech era. School districts like Orange County Public Schools, the 9th largest in the US, rely on Meraki's wireless to service over 208,000 students in over 200 schools as they roll out their 1:1 iPad initiative.
- Manufacturers are relying on wireless networks and Bluetooth Low Energy (BLE) beacons to assist with asset tracking of inventory in warehouses and in identifying where key employees are on factory floors if a problem requires their immediate attention.
- Sports stadiums, auditoriums, theaters, and other events venues must compete with at-home viewing options and inspire return visits, so are leveraging wireless networks and location-based services to provide more interactive experiences for fans and attendees. For example, Capital FM Arena, which can seat 10,000 and is one of the UK's premier concert venues, New York's Red Bull Arena, and Real Madrid's WiZink Center (formerly Barclaycard Center) rely on Meraki wireless to improve fan engagement.
- Corporate offices have made a mass migration from wired connections to wireless coverage throughout their (often open floor plan) space, thanks to the convenience wireless affords for collaboration and its lower costs to deploy.

In short, the universal need for robust, reliable wireless networks for business-critical functions cannot be overstated despite the increasing complexity of maintaining and troubleshooting them.

What Can Go Wrong — and Why It's Hard to Diagnose Wireless Networks

There are a myriad factors that impact the quality of a wireless network. It's easy to have a poor deployment with unreliable or obsolete hardware, if a proper site survey hasn't been done, or if wireless is being deployed in an environment rife with heavy interference — no one can cheat the basic physics of good coverage.

But assuming your organization has invested in enterprise-grade equipment that can support the latest wireless protocols, there are other factors which can make identifying the root cause of a wireless latency or connection problem difficult:

- **A particular client** device may be misconfigured or producing "regional" mayhem in a specific part of an office or building, causing nearby clients to experience sluggish connection or download speeds.
- **A specific AP** is experiencing problems like client overload, a dropped uplink connection, or a misconfiguration that prevents it from optimally servicing clients.
- Additionally, there are **several connection steps** — association, authentication, DHCP, and DNS resolution — that must be successfully taken by each client before it is able to pass traffic on a wireless network.

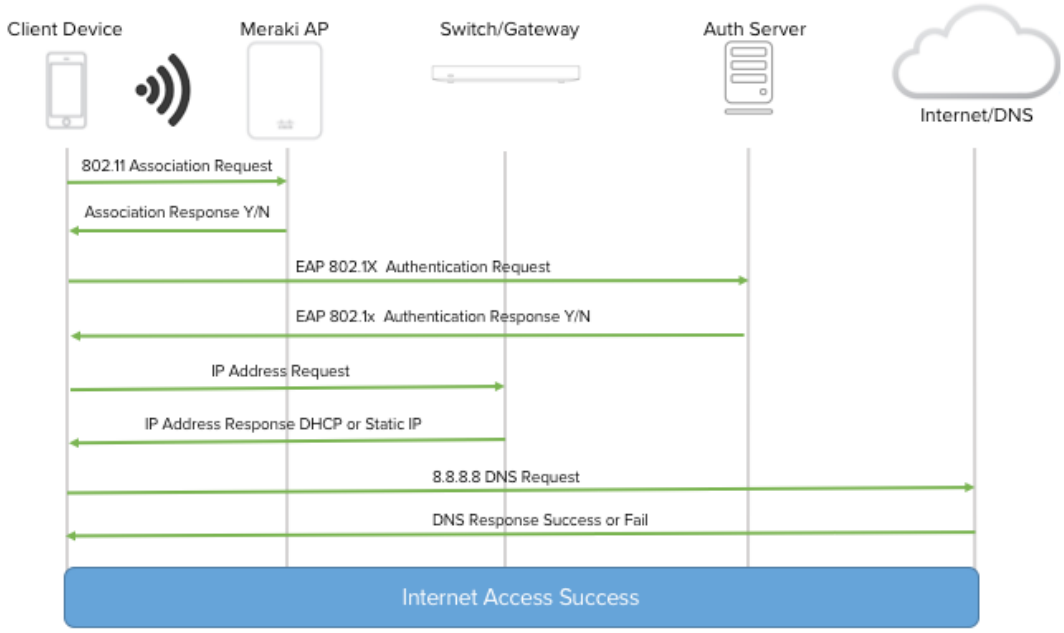


Figure 1: Steps required for a client to successfully connect to a wireless network.

A failure in any one of these steps can severely impact network performance, but finding a centralized view of these failures across all networked APs is often impossible. This lack of visibility can add significant and costly time to troubleshooting, and leave IT staff at the mercy of support tickets for learning when problems arise. Because end users often lack the technical expertise to describe their problem in ways that help narrow the scope of the root cause, addressing poor wireless performance can be one of the trickiest and most frustrating experiences for IT staff.

WHAT CAN GO WRONG AT EACH STEP:

- **Association:** When a client first selects a wireless network (SSID) to associate and connect to, that client will automatically send out probe requests to find the "best" available AP (usually the AP with the highest receive signal strength, or RSSI). If the request is successful, the client will associate to the AP in an unauthenticated state. If the association is unsuccessful, the client may not be able to join the wireless network at all.

  An association failure is not necessarily cause for alarm, since all networks experience some association failure in the course of normal operations. For example, if a wireless client is rapidly roaming throughout an office and must choose which of two or more competing APs to associate to, one of these APs will show an association success while the other APs will show an association failure. In this case, the network has performed as expected: a client cannot simultaneously associate to multiple access points!

  Although true association problems are uncommon, when they occur they can result in severe deterioration of end user experience.

- **Authentication:** After the client has successfully associated to an AP, the end user must authenticate to the wireless network. In the example connection shown in Figure 1, RADIUS 802.1x is being used to authenticate end users. When using RADIUS authentication, the AP will send an 802.1x EAP request to the configured RADIUS server that includes the credentials of the connecting user.

  If this authentication request is successful, the user is granted network access and can proceed to the next stage. The most common authentication errors occur because the server declines authorization — e.g. when a user enters an incorrect password or other login credential — or because the RADIUS authentication server is unreachable. When these errors occur, the client will be disassociated from the AP and kicked off the network.

  Failures in authentication cause users to be unable to access a wireless network, and subsequently result in a poor user experience.

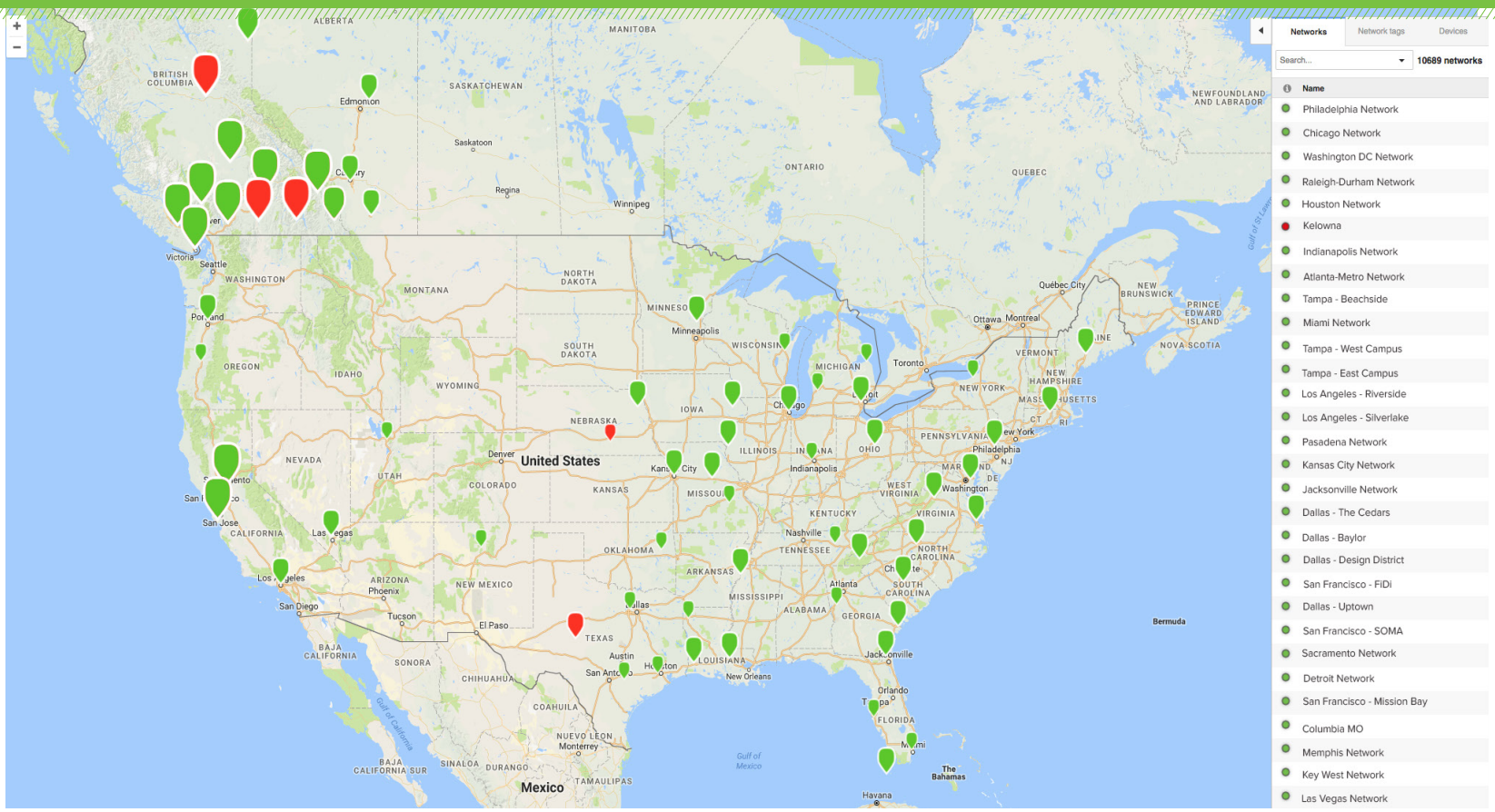
- **IP Addressing:** After the client successfully authenticates to a wireless network, it requires an IP address to communicate with network resources as well as Internet websites and downloadable content. To obtain an IP address, a client device must request one from a DHCP (Dynamic Host Configuration Protocol) server — which is typically connected to the network using a wired connection (in Figure 1, the DHCP server is hosted on the network gateway device).

  A common, but often overlooked, issue is when the network's available pool of IP addresses has been misconfigured and is too small to accommodate the number of devices trying to connect. This results in the DHCP server exhausting its reserve of available addresses, and thus being unable to service new requests — preventing clients from accessing the Internet or communicating with other networked devices. Other issues, like DHCP servers becoming overloaded or going offline for some reason, can also impact addressing service.

  The end result is a user who appears to be connected to the wireless network, but who is unable to pass any traffic. From the end user's perspective, they think they have successfully joined the network and are experiencing a high latency problem or that the wireless network is simply "down."

- **DNS Accessibility:** Finally, after the user has associated, authenticated, and has received an IP address, the last step gating access to network resources is the ability to resolve domain names. This is the process of turning human-readable web domain addresses, such as www.google.com into computer-readable IP addresses, such as 123.45.6.78. This process is handled by DNS (Domain Name Service) servers, which are usually hosted within an organization's network via a wired connection. In Figure 1, the client is using Google's DNS server at IP address 8.8.8.8 for name resolution.

  Failures at this final stage can be caused if connectivity to the DNS server is lost, is slow to respond, or is misconfigured to the point that its ability to reliably provide name service is crippled. Even though a user who has successfully associated, authenticated, and obtained a network IP address is technically "online," the Internet depends on DNS resolution to function; without operational DNS, the wireless experience for an end user will still be one that appears to be "down" or non-functioning.



Cisco Meraki: Innovating IT Management Since 2006

Meraki revolutionized the networking industry over a decade ago by upending the prevailing paradigm of on-premises, controller-based wireless networks and inventing the future: intuitive, massively scalable, cloud-managed IT. With **3.85 million devices** currently under management — and serving over **92 million clients in a 24 hour period** — our cloud architecture is the largest, most heavily tested, and most relied-upon in the world for mission critical, cloud-managed deployments.

Since pioneering the cloud-managed IT era, Meraki has developed an entire portfolio of wireless products and features designed to help network administrators rapidly hone in on the root causes of issues, and to troubleshoot those remotely — saving time and money. Today, Meraki's cloud-managed wireless offering is the most powerful and robust available, with actionable insights on every page of our intuitive web-based dashboard, a host of built-in tools for remote management and troubleshooting, and indoor / outdoor access points and antennas suitable for any use case.

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com

Anomaly Detection and Trend Analysis

By leveraging the distributed processing power of our massive cloud infrastructure, Meraki intelligently analyzes wireless networks, visualizes trends, and detects anomalies at the following levels:

- Organization-wide
- Network-wide
- Per SSID
- Per group of tagged APs

This visibility allows IT staff to quickly identify troubling patterns and problematic clients across customizable time periods, and to proactively mitigate issues before they become full-scale emergencies.

In *Figure 2*, for example, above-average bandwidth consumption has been detected for specific days during the past 3 months, identifying 10 clients with abnormally high usage which are listed on the lower right.

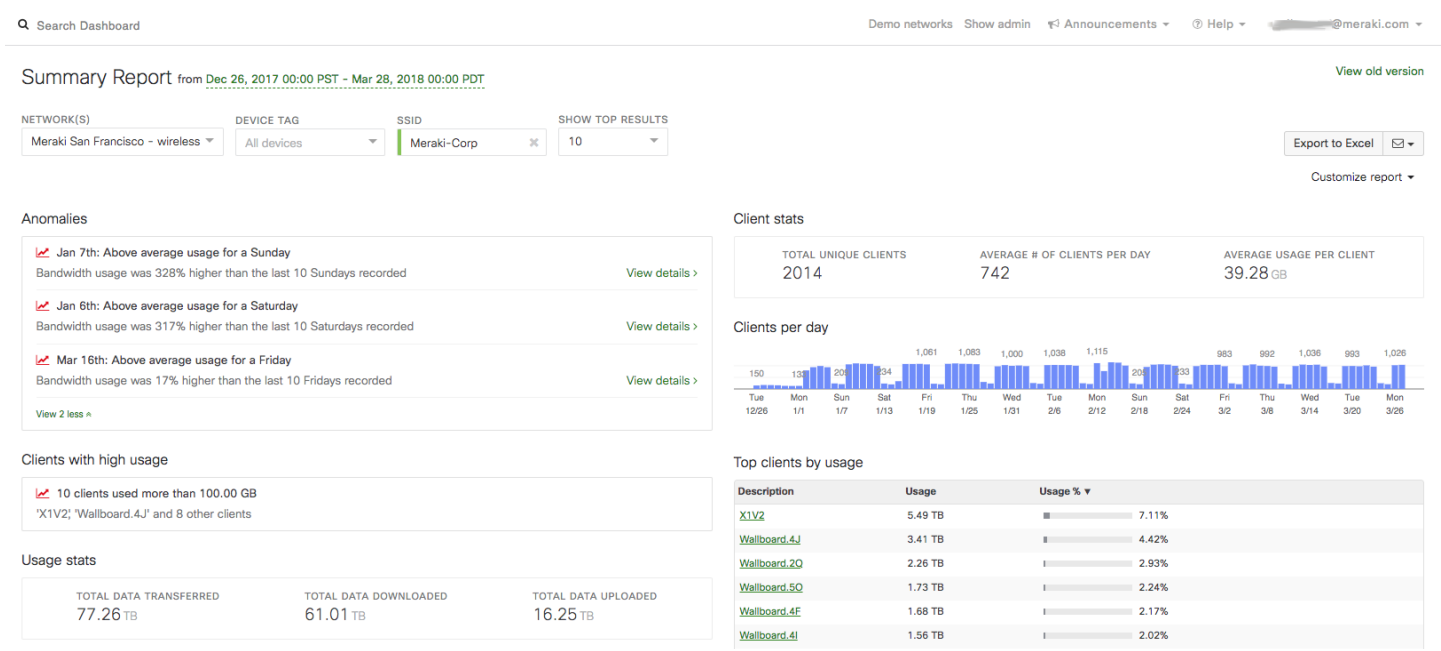


Figure 2. Anomaly detection and trend analysis for a specific SSID (Meraki-Corp) on a specific wireless network. Holistic data for an entire organization (wired and wireless) is also available.

To better understand why, for example, January 6th was an anomalous Saturday for our Meraki-Corp SSID, we can drill down to view usage patterns for every Saturday in our selected time frame, and see which application contributed most towards this unusual behavior.

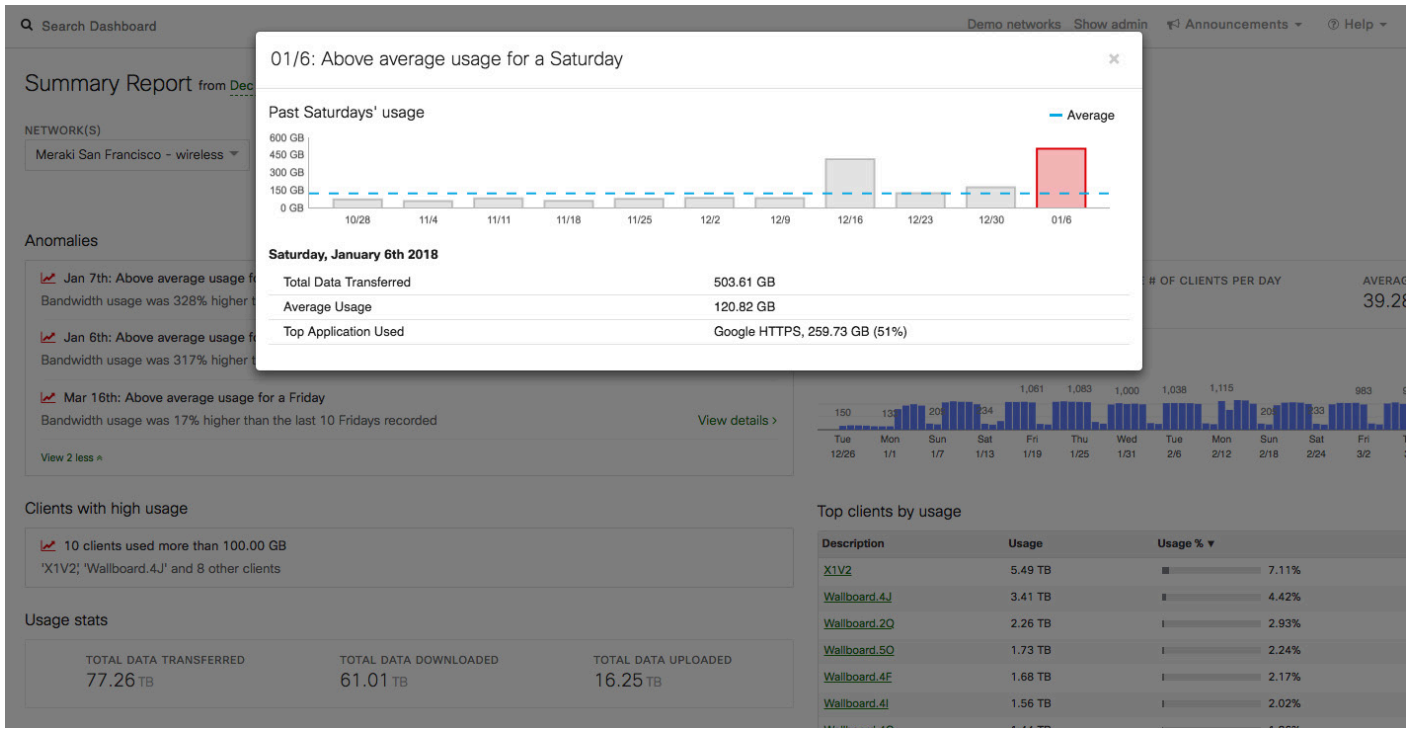


Figure 3. Anomaly analysis details show bandwidth consumed over time and top applications.

Additionally, alerts can be configured to notify IT when network usage exceeds chosen thresholds within specified time periods, such as 20 minutes, or if APs go offline or into automatic mesh mode. These canary-in-a-coal-mine alerts allow for more proactive troubleshooting by IT before the network becomes deluged by acute, anomalous usage.

Whether your network has a single Meraki device or, like one of our largest customers, **over 27,000 active devices** under management (see *Figure 4*), you can get immediate visibility into usage patterns across SSIDs, Meraki devices, clients, and applications from any Internet-connected device, wherever in the world you happen to be.

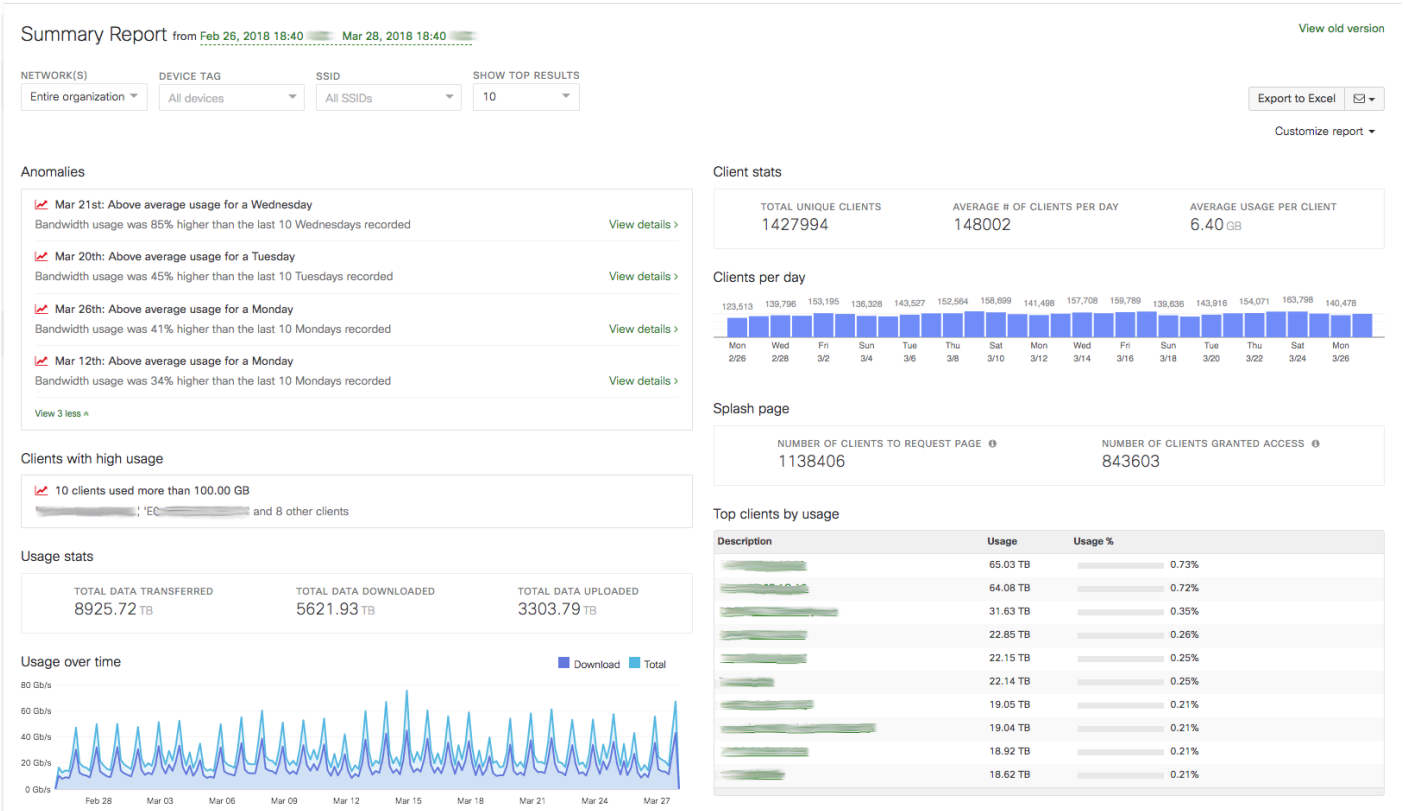


Figure 4. Anomaly detection and trend analysis for one of Meraki's largest customers.

While anomaly detection and trend analysis offer insights for proactive issue prevention, wireless problems happening in real time are often challenging to solve thanks to the many connection steps necessary — from client association to resolving Internet domain names— that serve as failure points. IT admins need additional insights for effective root cause analysis in these circumstances.

Wireless Health:
Powerful Heuristics for Smarter Troubleshooting

To further simplify wireless troubleshooting for busy IT admins, we've introduced Meraki Wireless Health. At its core, Wireless Health is a powerful heuristics engine that rapidly identifies anomalies impacting end users' experience across every stage of client connectivity — association, authentication, IP addressing, and DNS availability — for rapid root cause analysis and response.

Using Wireless Health, an IT administrator can immediately see whether users are able to successfully access the wireless network and easily identify wireless utilization and RF conditions. Wireless Health can identify problematic access points and clients, as well as connectivity stages that are resulting in failures. Granular details about the reason for failures can be explored to better understand root cause.

QUICKLY DIAGNOSE ISSUES USING MERAKI WIRELESS HEALTH

When trying to identify where a wireless network is experiencing poor performance, having centralized visibility across all networked APs is critical — and this visibility is what Meraki Wireless Health provides from the moment you engage with it.

The overview report offers high-level summaries of wireless health to help rapidly identify the most problematic sites, APs, or clients experiencing failed connections and latency:

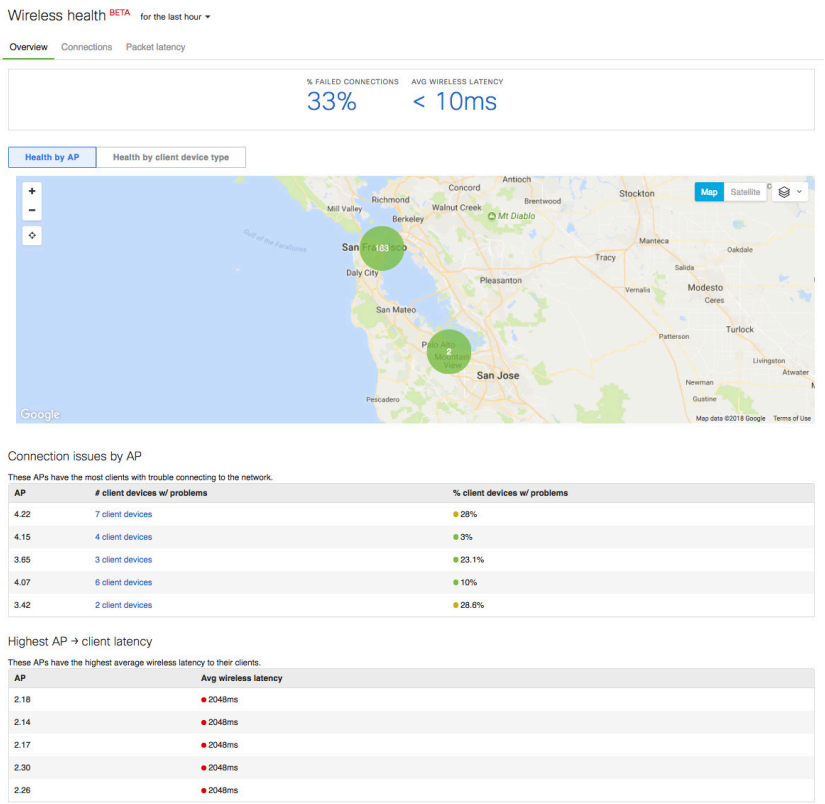


Figure 5. Meraki Wireless Health overview report.

It's possible to drill down into the overview report map to see whether poorly performing devices are clustered in meaningful ways:

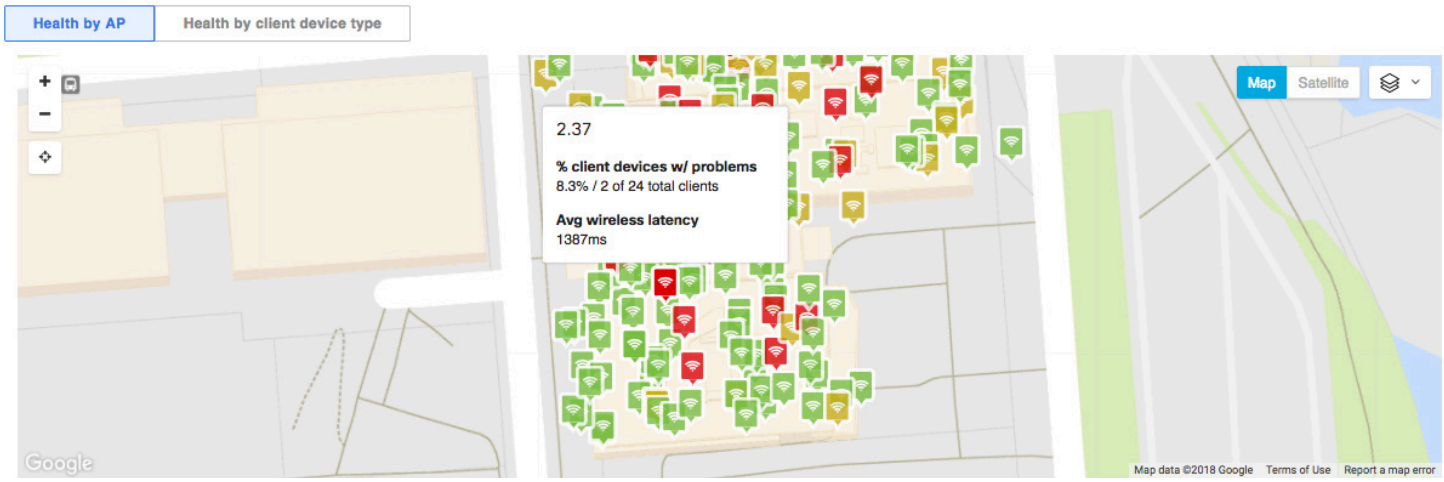


Figure 6. See which APs are experiencing the worst latency and connection failures.

To better understand why these APs and clients are performing poorly, Wireless Health's connections report displays network-wide metrics on current and historical failures across all stages of connectivity. This makes it immediately clear whether clients are experiencing problems associating to access points, authenticating to the network, receiving an IP address, resolving internet domain names, or experiencing some other issue.

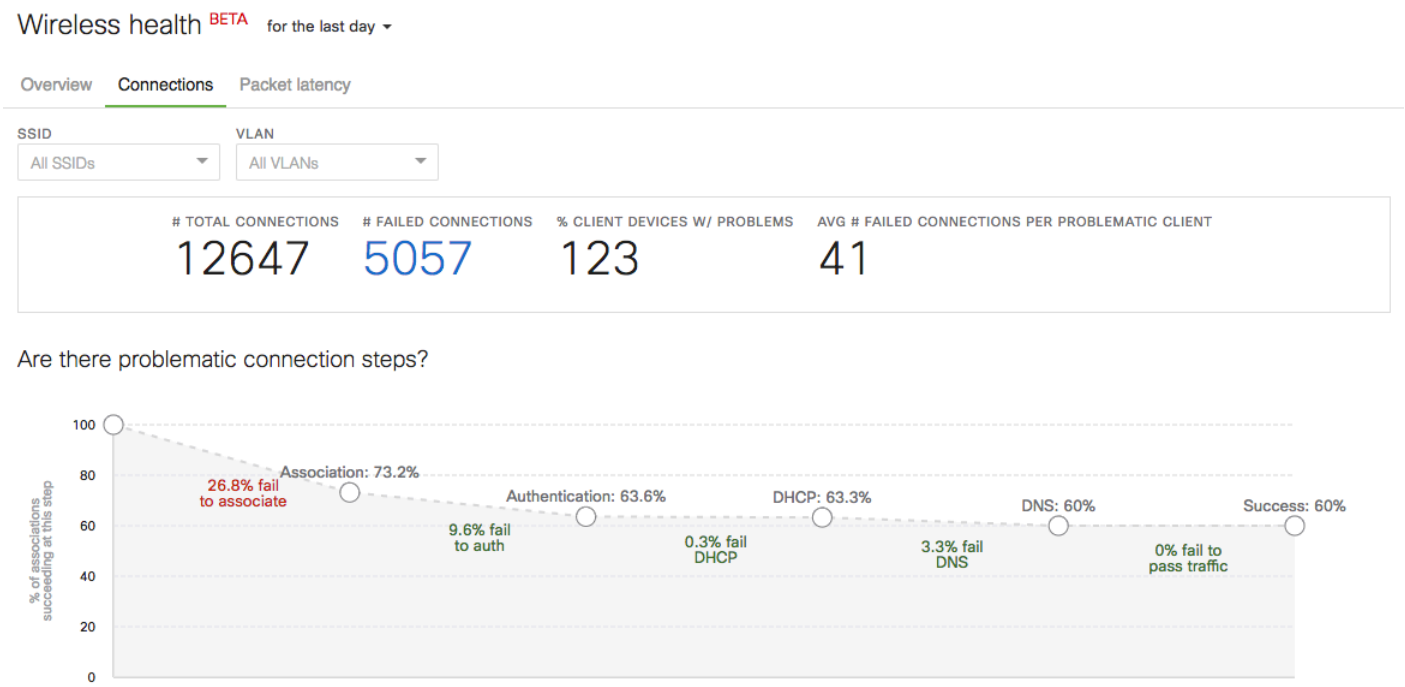


Figure 7. Meraki Wireless Health displays network-wide failures across each stage of client connectivity, allowing rapid root cause identification of poor network performance.

Like the overview report, the connections report also provides a map enabling quick identification of problematic APs based on location. This is especially useful if floor plans have been uploaded into the Meraki dashboard and APs have been accurately placed, because this map provides details into the number of clients on each AP impacted by specific connection failures:

Connection issues by AP

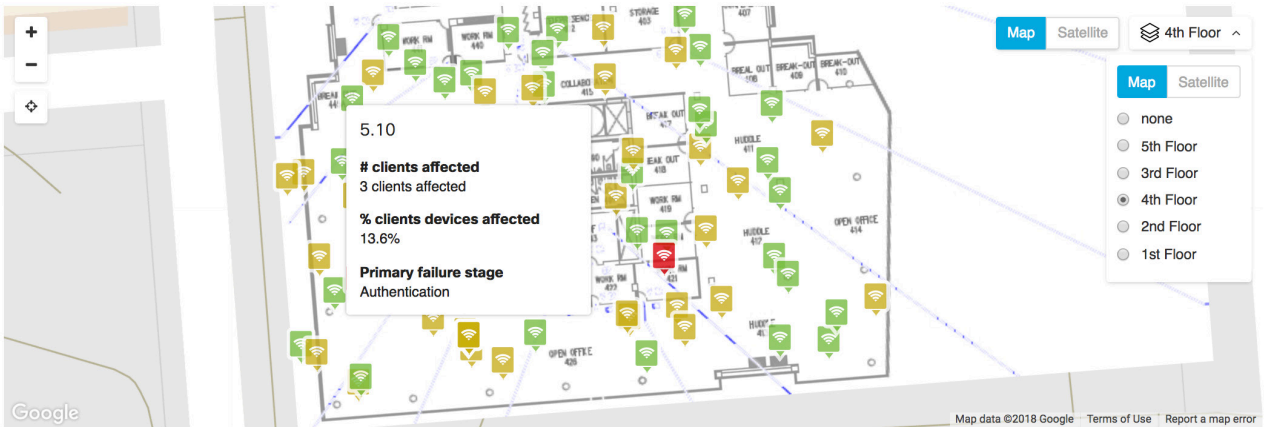


Figure 8. AP 5.10 is primarily experiencing authentication failures.

Finally, the connections report provides sortable failure statistics grouped by AP, client device, and client device type. This enables IT staff to rapidly identify:

- APs with the most failed connections
- APs with the highest number (or percentage) of total clients experiencing problems
- Which specific clients have the highest number (or percentage) of failed connections
- Which types of devices are experiencing the most problems

AP	# client devices w/ problems	% client devices w/ problems	Primary failure stage	# failed connections ▾
4.22	7 client devices	28%	Association	145 failed connections
4.15	4 client devices	3%	Authentication	60 failed connections
3.65	3 client devices	23.1%	Authentication	54 failed connections
4.07	6 client devices	10%	Authentication	53 failed connections
3.42	2 client devices	28.6%	Association	51 failed connections

5 results per page 1 2 3 ... 36 37

Connection issues by client

Client device	% failed connections	# failed connections ▾	Primary failure stage
iPad	66.3%	118 connections	Association
ECUTTLERX230	66.4%	89 connections	Association
54:33:cb:4b:f6:f5	56.5%	39 connections	Association
f0:98:9d:0c:26:64	56.6%	30 connections	Association
c8:3c:85:d9:3a:7d	61.2%	30 connections	Association

5 results per page 1 2 3 ... 129 130

Connection issues by client device type

Device type	# client devices w/ problems ▾	% client devices w/ problems	Primary failure stage
Apple iPhone	22 client devices	10%	Authentication
Mac OS X 10.13	15 client devices	10.6%	DHCP
Mac OS X 10.12	12 client devices	14%	DHCP
Windows 10	4 client devices	3.8%	Authentication
Mac OS X 10.11	3 client devices	13%	Association

5 results per page 1 2 3

Figure 9. APs and clients are sorted here by # failed connections, while client type sorted by # clients with problems.

For example, in *Figure 9*, we can see that for the past hour, AP 4.22 has been experiencing potentially troublesome association failure rates, that a device named “iPad” may be having the most issues associating to nearby APs, and that iPhones, as an overall group, are experiencing the highest number of authentication issues.

If we wanted to more deeply explore any of these issues, we could click on the appropriate column links. For example, drilling down into the 118 failed connections for the client named “iPad” brings us to the failed connections log. Here we see the client is struggling with both the association and authentication steps — and likely the core issue is authentication, because once the client fails to authenticate it’s automatically disassociated from the AP.

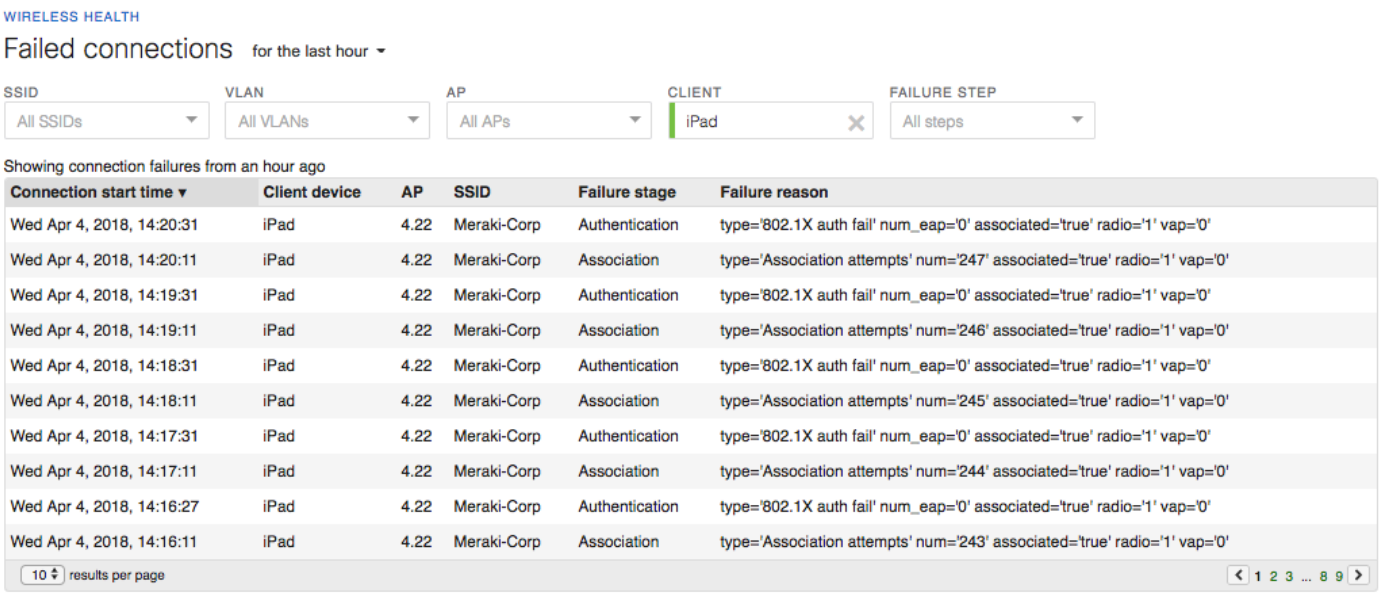


Figure 10. Columns in the Failed Connections log are sortable and filterable.

It’s possible to filter the failed connections log by timestamp, SSID, VLAN, specific AP, specific client, or stage of connection failure to narrow or broaden visibility. This can quickly narrow the scope of troubleshooting by showing failures across these categories.

DIAGNOSING PROBLEMS WITH PACKET LATENCY

Whether you’ve just deployed a new wireless network or wish to tune an existing one, you’ll want to gauge your network’s responsiveness to client requests, measured as latency. Latency is a critical factor in an end user’s overall wireless experience, with high latency levels giving the perception of sluggish performance. Because of its importance, packet latency is a critical metric monitored in Meraki Wireless Health.

Latency problems often arise because of two situations: interference and overload. Wireless interference occurs when two access points can hear each other on the same channels (overlap) and thus compete for the same clients (contention). From a client’s perspective, contention leads to packet errors, which in turn lead to attempts to re-send data, ultimately resulting in increased latency.

Most Meraki APs come with a dedicated, dual-band scanning radio for AutoRF, Meraki’s sophisticated channel optimization algorithm that automatically detects and adjusts radio settings for power, signal strength, and channel selection based on environmental factors — such as

interference, usage demand, and airtime availability — in real time. Because of their dedicated third radio, these APs have full visibility into RF conditions on all channels, and the AP and Meraki dashboard are able to make rapid channel planning decisions that help mitigate wireless interference in high-density RF environments.

For many deployments, AutoRF can ensure a good baseline channel configuration. However, it's always possible to fine-tune Meraki APs' radio settings. For example, an IT admin could choose to deploy RX-SOP (Receive Start of Packet), which helps mitigate co-channel interference in extremely dense environments by allowing an AP to disregard transmissions that do not meet a specified signal strength threshold.

Figure 11. Fine-tuning a Meraki AP can include adjusting radio settings or configuring RX-SOP.

The second factor contributing to high latency, wireless overload, occurs when an AP literally runs out of physical resources needed to serve all its client requests. Symptoms of this scenario could be an access point displaying high latency but operating on a clean, low interference channel. The cause for latency in this case would likely be due to the AP consistently experiencing extreme client load.

Meraki APs automatically deploy intelligent client load balancing, a feature which uses information about the state of the network and wireless client probes to steer a client to the best available access point during association. To achieve the speed necessary for steering clients, distributed intelligence is required among the APs, which operate without cloud interaction to gather and share RF and client metrics in real time and to optimize the client load between them.

For example, Figure 12 shows a real customer's theater deployment usage statistics during a live event; you can see the relatively even, automatic distribution of clients across the various APs

thanks to Meraki client load balancing:

Top devices

Name	Model	# Clients	Usage	Usage %
AP12	MR52	471	26.94 GB	21.64%
AP15	MR42E	198	18.29 GB	14.69%
AP8	MR53E	303	16.54 GB	13.28%
AP14	MR42E	645	12.78 GB	10.27%
AP7	MR53E	348	11.32 GB	9.09%
AP4	MR53E	319	7.89 GB	6.33%
AP6	MR53E	342	6.77 GB	5.44%
AP5	MR53E	329	6.73 GB	5.40%
AP10	MR53E	378	5.56 GB	4.47%
AP13	MR53E	355	5.28 GB	4.24%

Figure 12. Algorithms automatically balance Meraki client load across available APs.

Although the native client load balancing algorithms built into every Meraki AP should optimize client distribution for most deployments, issues can arise in extremely dense or heavy-load scenarios (this is true of any wireless vendor).

Meraki Wireless Health enables IT admins to rapidly identify worst-performing traffic from a latency point of view.

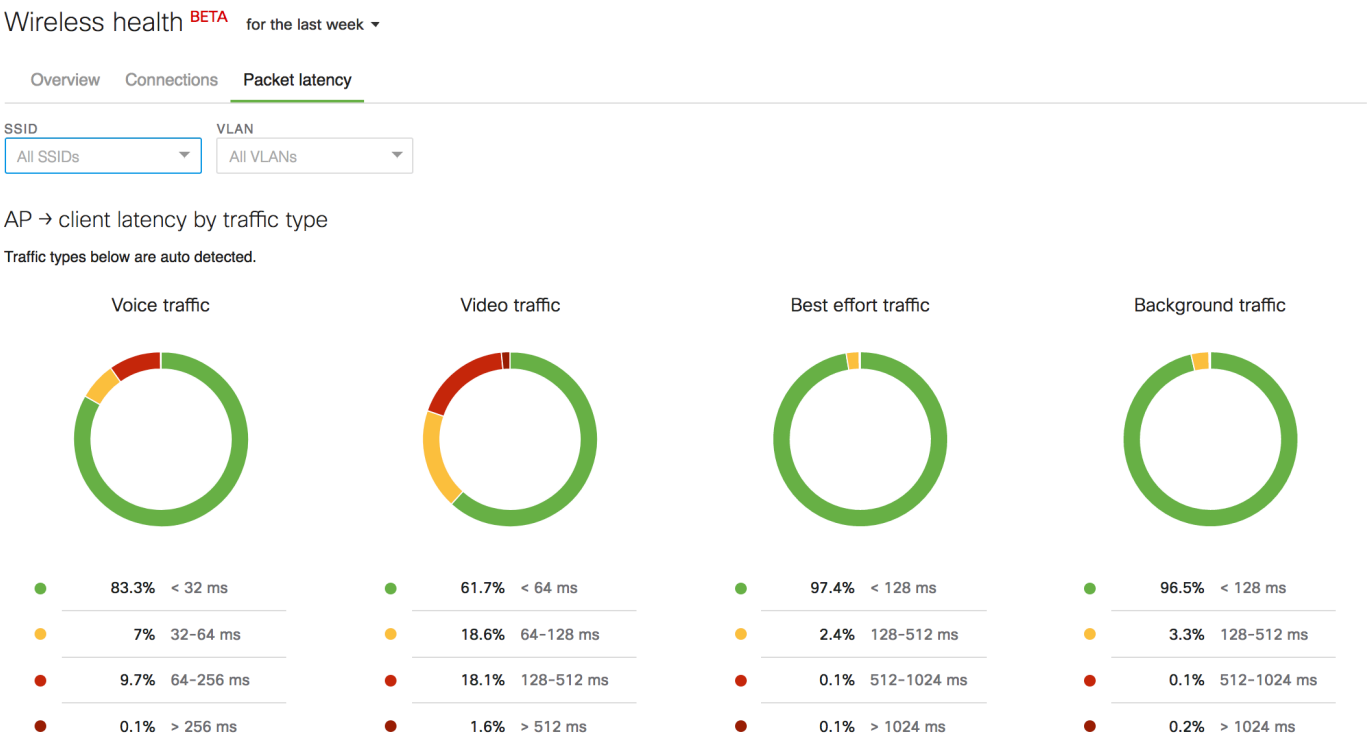
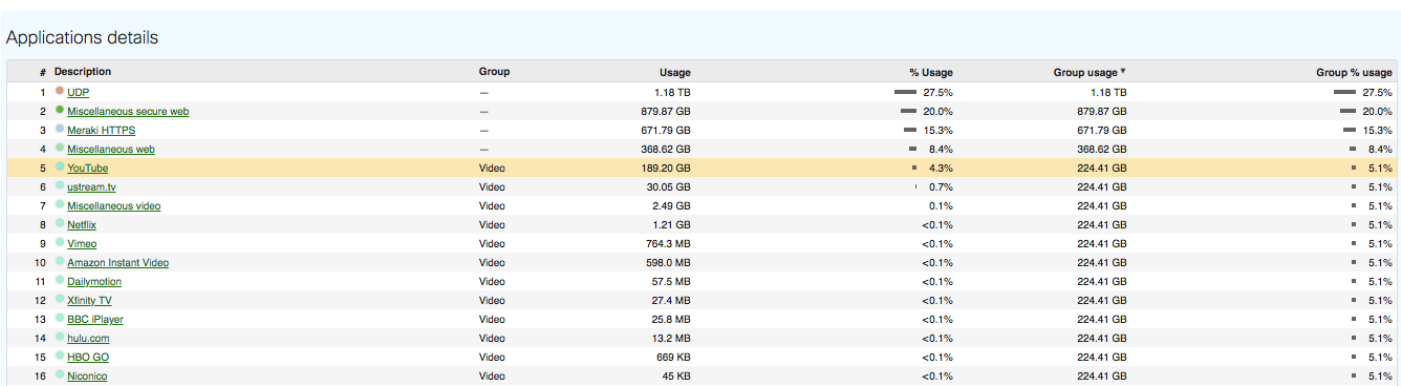


Figure 13. Wireless Health measures packet latency by traffic type, highlighting any performance degradation

By quickly visualizing what percentage of latency-critical traffic — like voice and video — are suffering from poor performance, Wireless Health narrows the scope of troubleshooting and allows IT staff to dive deeper into specific applications' usage patterns to identify bandwidth hogs or problematic clients.



Applications details

#	Description	Group	Usage	% Usage	Group usage ▾	Group % usage
1	UDP	–	1.18 TB	27.5%	1.18 TB	27.5%
2	Miscellaneous secure web	–	879.87 GB	20.0%	879.87 GB	20.0%
3	Meraki HTTPS	–	671.79 GB	15.3%	671.79 GB	15.3%
4	Miscellaneous web	–	368.62 GB	8.4%	368.62 GB	8.4%
5	YouTube	Video	189.20 GB	4.3%	224.41 GB	5.1%
6	ustream.tv	Video	30.05 GB	0.7%	224.41 GB	5.1%
7	Miscellaneous video	Video	2.49 GB	0.1%	224.41 GB	5.1%
8	Netflix	Video	1.21 GB	<0.1%	224.41 GB	5.1%
9	Vimeo	Video	764.3 MB	<0.1%	224.41 GB	5.1%
10	Amazon Instant Video	Video	598.0 MB	<0.1%	224.41 GB	5.1%
11	Dailymotion	Video	57.5 MB	<0.1%	224.41 GB	5.1%
12	Xfinity TV	Video	27.4 MB	<0.1%	224.41 GB	5.1%
13	BBC iPlayer	Video	25.8 MB	<0.1%	224.41 GB	5.1%
14	hulu.com	Video	13.2 MB	<0.1%	224.41 GB	5.1%
15	HBO GO	Video	669 KB	<0.1%	224.41 GB	5.1%
16	Niconico	Video	45 KB	<0.1%	224.41 GB	5.1%

Figure 14. Sorting application usage by type helps identify problematic video applications and the clients consuming them.

Meraki Wireless Health is thus a powerful heuristics engine leveraging the massive scale and processing power of Meraki's cloud architecture to give empirical insights into the root causes of wireless connectivity issues. It is available to all Meraki wireless customers at no additional cost or charge, and seamlessly complements the other effective, remote troubleshooting features — including remote packet capture, spectrum analysis, and RF event analytics — that are built into the Meraki wireless platform.

About Cisco Meraki

Founded in 2006, Meraki has grown to become the world's most scalable, feature-rich, and reliable cloud-managed IT solution. Over 250,000 unique customers and 3.85 million Meraki devices are under management around the world. Our comprehensive set of solutions includes wireless, switching, security, endpoint management, and security cameras, all centrally managed from Meraki's intuitive web-based dashboard interface. This gives network administrators visibility and control, without the cost and complexity of traditional architectures.

To learn more, please visit our website (meraki.cisco.com) or join us for a live webinar (meraki.cisco.com/webinars) and receive a free Meraki wireless access point and cloud management license so that you can experience the Meraki magic in your own environment.

Cisco Systems, Inc. | 500 Terry A. Francois Blvd, San Francisco, CA 94158 | (415) 432-1000 | sales@meraki.com