White Paper

Network Topology

JANUARY 2015

This document describes the benefits of Cisco Meraki's Network Topology technology and how you can use it to visualize and troubleshoot your network. In addition, this document describes how the technology works.

Table of Contents

1 Introduction

Increased network visibility is no longer a luxury but is now table stakes for network administrators. Visibility means having insight into the network topology, network traffic, clients, points of congestion and discovering unexpected cloud applications running on the network. This previously hard to uncover information arms IT teams with the information they need to improve network performance and also react quickly when there is a problem.

Oftentimes, tools that enable this visibility require new hardware and software to manage and support. These tools can be expensive, error-prone, and typically not deliver on the promise of improved visibility without significant customization. This complexity means that many tasks such as creating a network topology are done manually rather than investing the time and capital for more automated solutions.

Network topology can be a physical or logical map of a network and is used by teams to outline a new network design build-out, troubleshoot issues when they come up, and plan for future network growth. The primary tools used to create network topologies today come in two varieties: automated and manual, with manual being the dominant solution since automated solutions often fail at addressing accuracy and rendering speed.

Manually created network topologies can be painstaking to develop, prone to revision errors, and difficult to maintain as networks change and grow. Because of the effort involved to keep this topology documentation up-to-date, this leads teams down the path of finding automated solutions.

Although third-party vendor solutions can automate topology creation, their compatibility with installed networking equipment can be spotty—leading to accuracy errors and slow rendering speeds.

Cisco Meraki already integrates industry-leading technologies like client and layer 7 application visibility and control and now has automated network topology to further extend the network visibility and insights available to network administrators. This technology addresses limitations with other solutions today and delivers on ease-of-use, accuracy, and rendering speed.
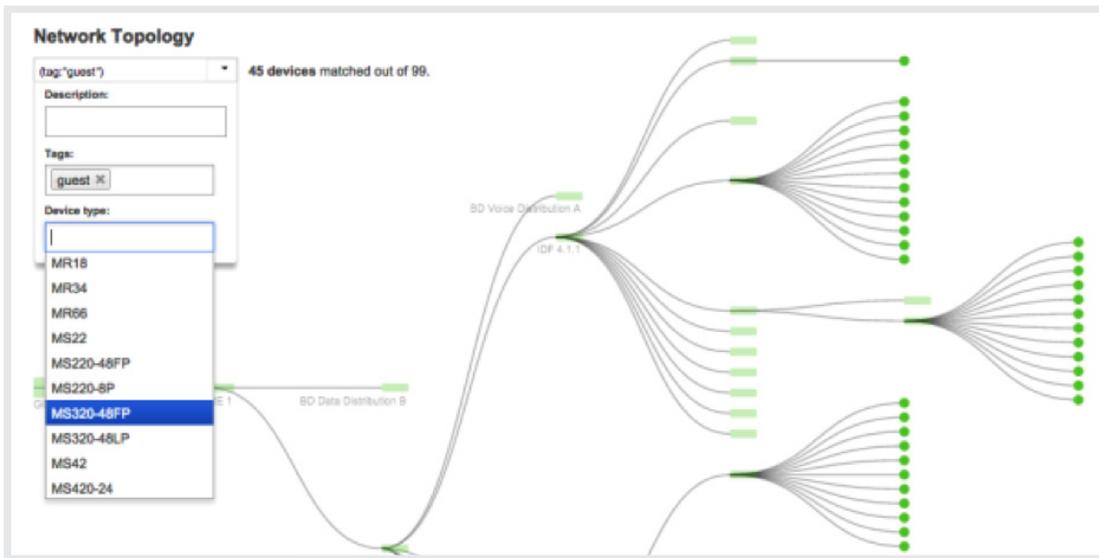
2 Cisco Meraki Network Topology

Cisco Meraki's network topology automatically and intelligently maps Meraki security appliances, switches, and access points in the network, giving administrators a hierarchical, physical layout of how equipment interconnects. The topology is also interactive, letting IT admins do things like search for network devices by name, tag, or device type to quickly view how equipment is deployed.
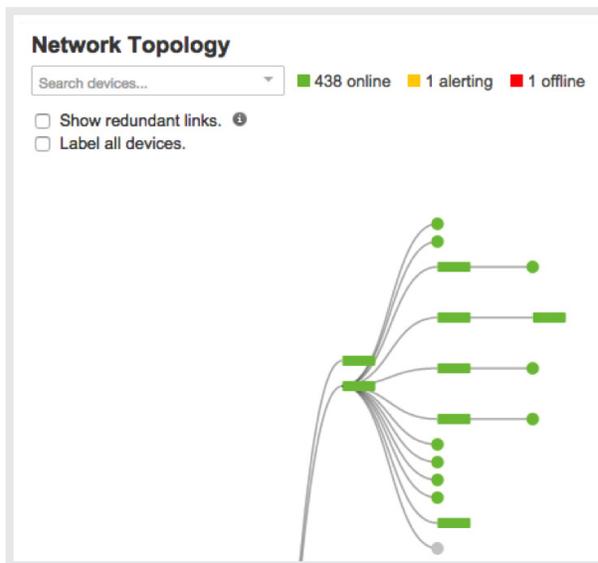
In the topology view, squares represent MX security appliances, rectangles represent MS switches, and circles represent MR access points. Non-Meraki equipment is also detected if it is one hop away (and will appear as an empty diamond); depending on the protocols supported by a non-Meraki device, the topology view may be able to discern discovery protocol data like model type, IP, and manufacturer. For example, Cisco switches and routers will also include extensive information based on Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP).

Network Topology

(tag:"guest")   45 devices matched out of 99.
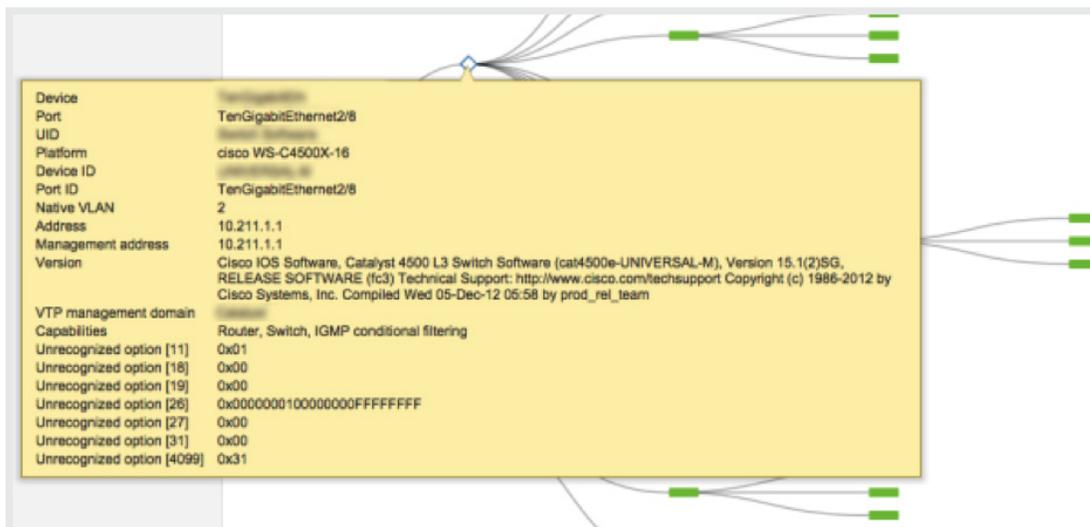
Looking at equipment in a corporate network tagged "guest," and running a guest SSID or guest VLAN. Gear not meeting our search criteria is automatically dimmed.

Network topology is available for all Meraki customers running combined networks with Meraki equipment (MS, MX, or MR), or for customers running uncombined switch networks. To get the full benefits of topology, however, Meraki MS switches should be deployed since Meraki MS switches are the primary data collection agents that the topology algorithms depend on for accuracy.

The network topology feature shows up in combined networks under Network-wide > Topology in the Meraki dashboard; otherwise, check Monitor > Topology in uncombined switch network.

In addition, it's easy to quickly see alerting or disconnected equipment that may require additional troubleshooting, and (if the alerting device is a Meraki AP, switch, or security appliance), click into that device to troubleshoot further.

IDF 5.3.3
MS320-48LP switch

Direct clients: 17

A power supply is offline.
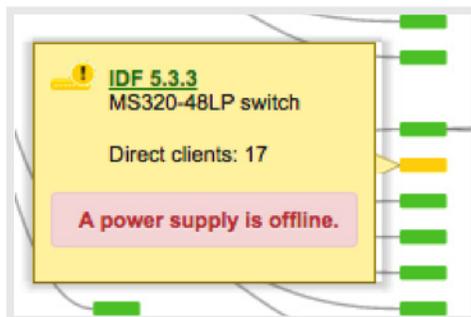
Learning which physical links in the network that are most heavily-trafficked is also effortless; simply hover over individual network links to learn statistics about that connection's negotiated speed, usage, and number of directly connected clients using it in the past day. This makes it simple to to diagnose physical bottlenecks in the network.
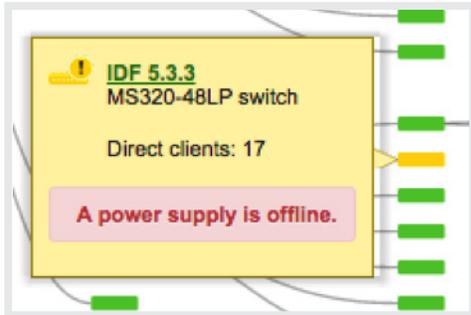
While it's helpful to see active links, it's also useful to view links or specific switch ports that have been blocked by the Spanning Tree protocol (STP), which helps prevent data loops.
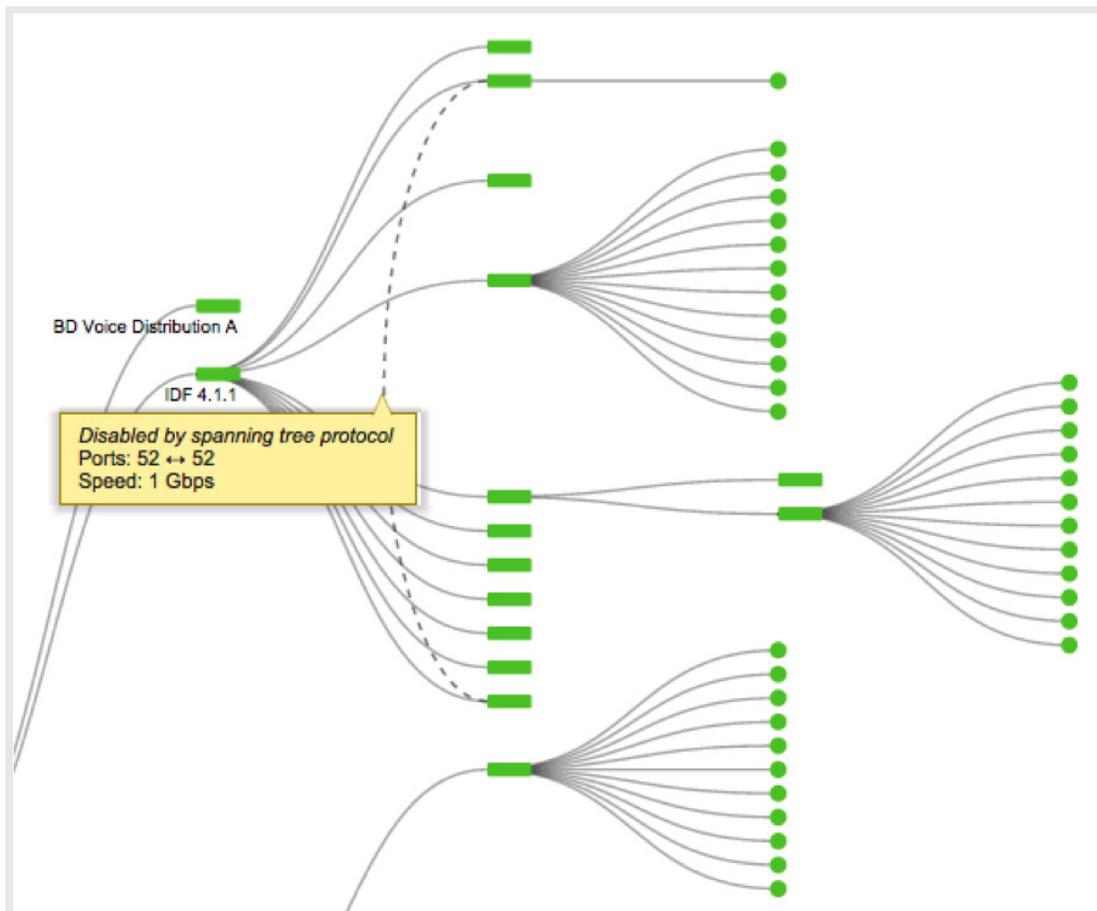
By default, if entire links have been disabled by STP, they will be hidden from view. To see all physical links—not just those currently forwarding traffic thanks to STP— select the checkbox to "show redundant links."

3 The Technology

Cisco Meraki's built-in network topology is ground breaking since it addresses ease-of-use, accuracy, and rendering speed and doesn't require additional hardware or software to manage. So how does the technology work?

The underlying technology takes all available network and device data, groups the data logically, and applies multiple filters to create an accurate network topology diagram.

The core technology behind network topology relies on Cisco Meraki switches. Cisco Meraki switches can detect data such as CDP/LLDP, network client devices, uplink state, switch port status, STP information, and much more. To make sense of this data requires intelligent algorithms that can not only parse the data in near real time but also accurately render an usable outcome.

First, the algorithm loads all available data into a structured database and the data is passed through multiple logic filters to sort out useful data from superfluous information. After the initial filters are applied, the data is logically grouped and defined but is still missing important information such as how switches are uplinked to each other as well as to other devices such as our MX security appliances.

Additional logic filters are then applied to further build the network topology.

- Uplink detection filters are applied to build the initial network map with uplinks drawn in

- Unmanaged device filters are applied to detect devices such as unmanaged switches, which may redraw the network tree

- Descendant node filters are applied to determine the connections between the root of the network topology and the end devices in a topology

All of these passes and redrawings are transparent to the end user.

At this point, the network topology consists of groupings of network trees and is close to the final output but a last pass is needed to detect how these groups of trees are interconnected as well as show third party devices that are one hop away. The final result is an accurate network topology that shows how Cisco Meraki MX Security Appliances, MS Switches, MR Access Points, and third party devices that are one hop away are connected.
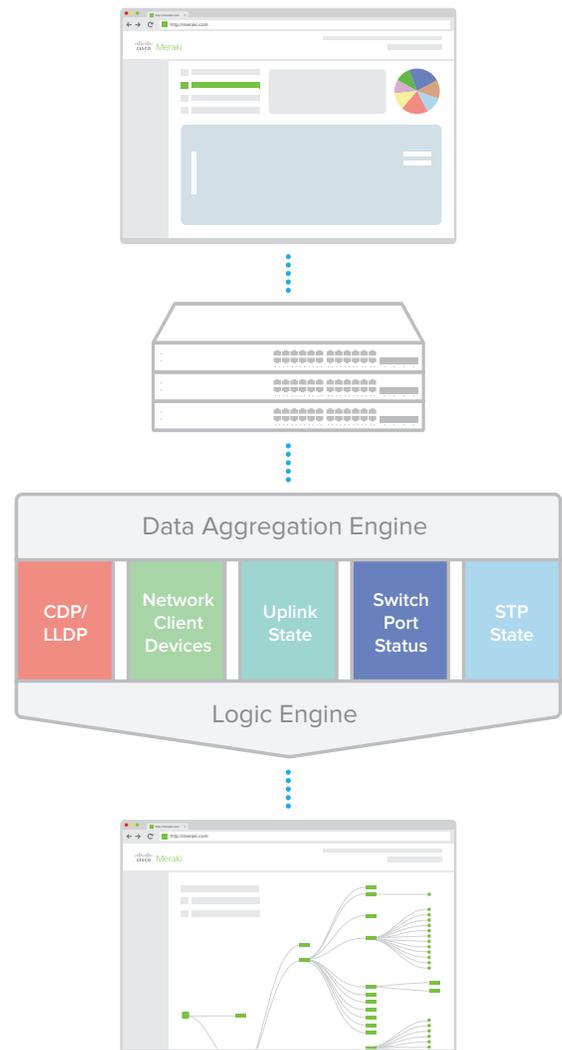
4 Conclusion

Network topology is an incredibly powerful feature that further extends Cisco Meraki's network visibility and provides admins a greater understanding of their infrastructure. Administrators no longer need to rely on manual, out-of-date topologies or third party automated solutions that fail at accuracy and rendering speed and instead can rely on an accurate, dynamic network topology built in Dashboard.

Topology shows device status, alerts, the amount of network traffic going over links, and even third party devices that are one hop away from Cisco Meraki switches that support CDP/LLDP.

This built-in visibility is another incredible feature that helps network administrators deliver a resilient, enterprise network with no additional hardware or software required.