

10 Ways

Cisco Meraki Switches
Make Life Easier

10 Ways Cisco Meraki Switches Make Life Easier

1. Preconfigure switches for zero-touch deployment
2. Manage all switch ports from a single pane of glass
3. Run remote cable tests and packet captures
4. Identify and locate switch ports
5. Identify bandwidth hogs
6. Save energy and increase wired security
7. Contain rogue DHCP servers
8. Lock down switch access
9. Keep current with seamless updates
10. Spot network trends

1. Preconfigure switches for zero-touch deployment

Cisco Meraki MS switches are 100% cloud-managed and can be fully configured from any Internet-accessible location before ever being powered on. Simply add the switch serial number (or order number for large deployments) to your network using the Meraki web-based dashboard. Once added, the switch is fully configurable. When the switch is first powered on and connected to the Internet, it will pull its settings from the cloud.

Add switches

Add switches from your organization's inventory. When you claim an order by order number, the devices in the order will be added to your inventory. When you claim a device by its serial number, that device will be added to your inventory. Once in your inventory, you can add devices to your network(s).

<input type="checkbox"/>	MAC address ▲	Serial number	Model	Claimed on	Order number	Country
<input checked="" type="checkbox"/>	00:18:0a:53:01:13	Q2AP-7VDF-DTWP	MS22	8/15/2013 12:24 PM		

Adding new MS switch hardware to a branch location in the Cisco Meraki dashboard.

Switches

for the last day ▾

Tag ▾ Move ▾ Clone ▾ Search switches... ▾ 1 switch

<input type="checkbox"/>	Status ▲	Name	Connectivity	LAN IP	MAC address	Model	# active ports	# ports	Tags
<input type="checkbox"/>		00:18:0a:56:02:e6		N/A	00:18:0a:56:02:e6	MS22	- / 52	52	recently-added

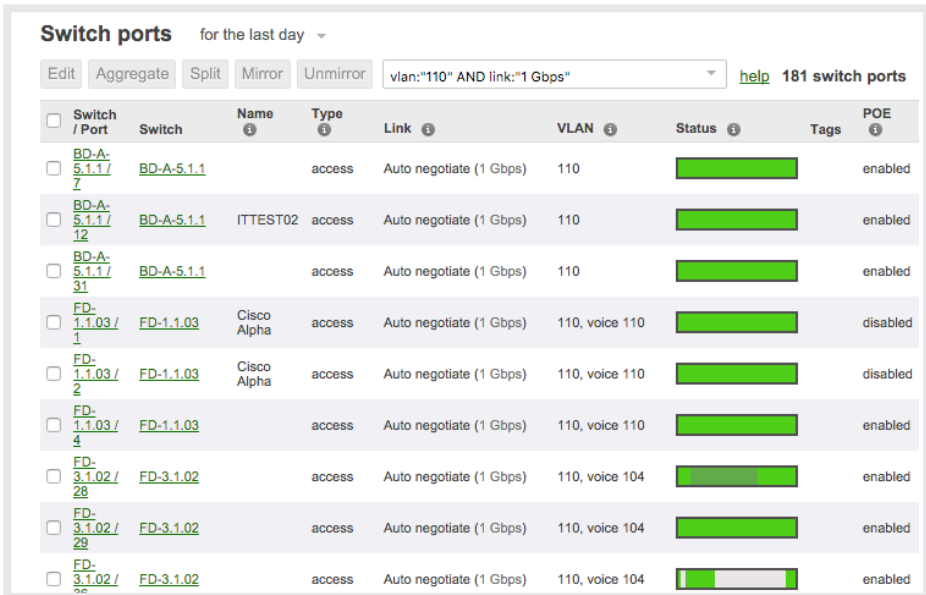
Newly-added switches are fully configurable in the Cisco Meraki dashboard — even before being powered on.

True zero-touch provisioning divorces switch setup from the precondition of physical hardware access. This frees technical staff from travel obligations to remote sites to manually configure switching infrastructure, saving time and money.

2. Manage all switch ports from a single pane of glass










Imagine: you need to reset ports numbered 20-48 (if they are connected to MR24 access points) on all of your switches. You must enable PoE, set a power-saving port schedule, prune all VLANs except VLAN 10, and ensure that these are trunk — not access — ports. How long would that take you?

Meraki MS switches let you succeed in this scenario from your office chair. The dashboard supports intelligent search queries on variables like port type, VLAN, uplink status, port access policy status, and tags:



Switch ports for the last day ▾

Edit Aggregate Split Mirror Unmirror [help](#) 181 switch ports

<input type="checkbox"/>	Switch / Port	Switch	Name	Type	Link	VLAN	Status	Tags	POE
<input type="checkbox"/>	BD-A-5.1.1/7	BD-A-5.1.1		access	Auto negotiate (1 Gbps)	110			enabled
<input type="checkbox"/>	BD-A-5.1.1/12	BD-A-5.1.1	ITTEST02	access	Auto negotiate (1 Gbps)	110			enabled
<input type="checkbox"/>	BD-A-5.1.1/31	BD-A-5.1.1		access	Auto negotiate (1 Gbps)	110			enabled
<input type="checkbox"/>	FD-1.1.03/1	FD-1.1.03	Cisco Alpha	access	Auto negotiate (1 Gbps)	110, voice 110			disabled
<input type="checkbox"/>	FD-1.1.03/2	FD-1.1.03	Cisco Alpha	access	Auto negotiate (1 Gbps)	110, voice 110			disabled
<input type="checkbox"/>	FD-1.1.03/4	FD-1.1.03		access	Auto negotiate (1 Gbps)	110, voice 110			enabled
<input type="checkbox"/>	FD-3.1.02/28	FD-3.1.02		access	Auto negotiate (1 Gbps)	110, voice 104			enabled
<input type="checkbox"/>	FD-3.1.02/29	FD-3.1.02		access	Auto negotiate (1 Gbps)	110, voice 104			enabled
<input type="checkbox"/>	FD-3.1.02/30	FD-3.1.02		access	Auto negotiate (1 Gbps)	110, voice 104			enabled

Dynamically filter for a list of switch ports across models and physical switch locations.

You can specify a subset of switch interfaces (up to 10,000 ports) by using these search criteria and then modify these selected ports at once.

Switch ports for the last day ▾

Edit Aggregate Split Mirror Unmirror is:trunk ldp:"MR32" 1-20 [help](#) 4 switch ports

<input type="checkbox"/>	Switch / Port	Switch	Name ⓘ	Type ⓘ	Link ⓘ	VLAN ⓘ	Status ⓘ	Tags	CDP/LLDP	POE ⓘ
<input type="checkbox"/>	FD-4.2.02/13	FD-4.2.02	B3 AP	trunk	Auto negotiate (1 Gbps)	native 128	 		<input checked="" type="checkbox"/> B3 14D0 <input checked="" type="checkbox"/> A	enabled
<input type="checkbox"/>	FD-4.2.02/20	FD-4.2.02	MR3TWO	trunk	Auto negotiate (1 Gbps)	native 128	 	A1	<input checked="" type="checkbox"/> A2 4F40 <input checked="" type="checkbox"/> B	enabled
<input type="checkbox"/>	FD-5.2.02/2	FD-5.2.02		trunk	Auto negotiate (1 Gbps)	native 128	 	AP Corp	<input checked="" type="checkbox"/> 5 G6 - E	enabled
<input type="checkbox"/>	FD-5.3.02/16	FD-5.3.02		trunk	Auto negotiate (1 Gbps)	native 128	 		<input checked="" type="checkbox"/> 5 J4 - E	enabled

Easily select ports 1-20 servicing MR32 access points that are configured as trunks.

Update 200 ports ✕

Switch ports: FD 5.3.6/15
FD 5.3.6/13
FD 5.3.3/15
FD 5.3.3/16

Name:

Tags:

Enabled:

RSTP:

STP guard:

POE: ⓘ

Link: ⓘ

Port schedule:

Type:

Access policy:

MAC Whitelist:

VLAN:

Voice VLAN: ⓘ

Updating 200 interfaces to enable PoE, apply a port schedule, and ensure they are all trunk ports.

3. Run remote cable tests and packet captures

The Cisco Meraki dashboard offers real-time diagnostics and tools to troubleshoot your MS switches. You can easily perform cable tests to ascertain cable length and to check the health of the wire connecting a client device to your switch.

Closet 4.1.7
MS250-48FP 00:18:0a:12:34:56

LAN IP: 10.92.129.200 (via DHCP)
VLAN: 128
Public IP: 184.23.135.130
Gateway: 10.92.129.254
DNS: 10.92.129.117, 10.92.131.26

LAN IPv6: Not configured
Serial number: QAB2-B2QA-ABQ2
Address:

Summary | Ports | Power | Event log | Location | **Tools 1**

Select a tool: Cable test ▼

Warning: This test will disrupt traffic to 100 or 10 Mbit devices.

39,45 Run cable test

Testing the cables attached to ports 39,45 ↻

Port	Link	Length	Status	Pair 1	Pair 2	Pair 3	Pair 4
39	1Gfdx	48 m	OK	ok	ok	ok	ok
45	1Gfdx	57 m	OK	ok	ok	ok	ok

Several real-time diagnostic tools are available within the dashboard, including cable tests.

Deep visibility built into the clients and traffic passing through your fabric let you quickly surmise the layer 1-3 health status of connected devices, whether they've received IP addresses, are on the appropriate VLAN, etc.

Clients > JZITOMERX1V2

Status: currently connected | send WOL ⓘ
Switch / port: Closet 5.2.9 / 39 (topology)

Device type: Intel Windows 7/Vista
Notes: event log | packet capture | add note

Usage for the last 30 days ▼ 3.03 TB (↓ 34.34 GB, ↑ 3 TB) Applications

Network

IPv4 address: 10.92.135.11
IPv6 address (link-local): fe80:0:0:6944:76f5:f59b:6c89
MAC address: 4c:34:88:03:49:4f
VLAN: 132

Ping

80 ms
40 ms
0 ms
Loss rate: --
Average latency: --

Google HTTPS
3.0 TB (↓ 23.4 GB, ↑ 3.0 TB)

Quickly see status for client devices passing traffic through your switch fabric.

You also can take live, streaming packet captures from anywhere in the world you have Internet access. The Cisco Meraki dashboard lets you display packet captures within the dashboard, save captures to a PCAP file for later viewing with industry standard software, or stream the PCAP file to a CloudShark appliance.

Packet capture for switches

Switch: Closet 5.2.1

Ports: 1-20

Output: View output below

Duration (secs): 60

Verbosity: Low

Ignore: broadcast packets multicast packets

Filter expression:

[clear output](#) or [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 TCP or UDP port 53 (DNS)

icmp[icmptype] != icmp-echo and icmp[icmptype] != icmp-echo-reply
all ICMP packets that are not echo requests/replies (i.e., not ping packets):

ether host 11:22:33:44:55:66
packets to and from ethernet host 11:22:33:44:55:66

See more [examples](#).

The maximum packet capture duration is 1200 seconds.
This capture will stop after 60 seconds, or when 5000 packets have been captured. Client traffic statistics will not be recorded while the packet capture is running.

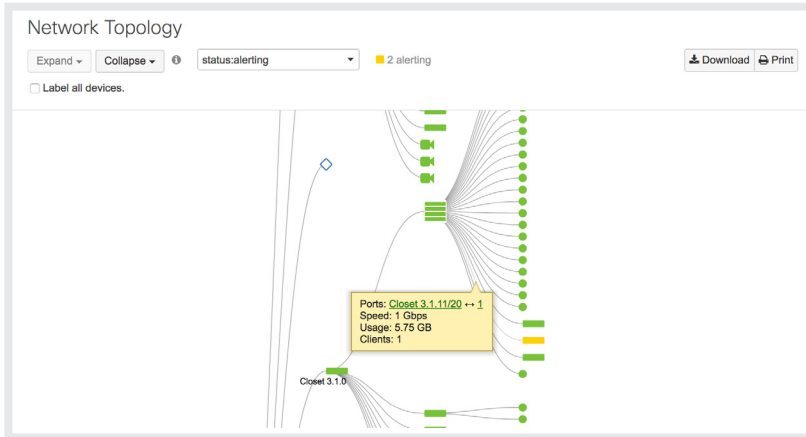
[Packet capture logs](#)

```
--- Start Of Stream ---
21:31:12.536090 ARP, Request who-has 10.92.111.137 tell 10.92.111.254, length 42
21:31:12.646581 IP 10.92.110.171.137 > 10.92.111.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
21:31:12.651487 ARP, Request who-has 10.60.60.1 tell 10.60.60.10, length 46
21:31:12.757543 ARP, Request who-has 10.92.111.254 (ff:ff:ff:ff:ff) tell 10.92.111.182, length 52
21:31:12.777788 ARP, Request who-has 10.92.111.114 (ff:ff:ff:ff:ff) tell 0.0.0.0, length 52
21:31:12.798141 ARP, Request who-has 10.92.111.182 (ff:ff:ff:ff:ff) tell 0.0.0.0, length 52
21:31:12.943990 IP 10.92.109.209.5353 > 224.0.0.251.5353: 0 [1a] [2q] [1au] PTR (QM)? _hap._tcp.local. PTR (QM)? _homekit._tcp.local. (128)
21:31:12.994623 IP 10.92.135.252.5353 > 224.0.0.251.5353: 0 [2q] SRV (QM)? EPSON WF-3520 Series._ipp._tcp.local. TXT (QM)? EPSON WF-3520 Series._ipp._tcp.local. (60)
21:31:13.087012 IP 10.92.111.16.1036 > 255.255.255.255.1037: UDP, length 18
21:31:13.089257 IP 10.92.110.6.54915 > 10.92.111.255.54915: UDP, length 263
21:31:13.132123 ARP, Request who-has 10.92.111.254 (ff:ff:ff:ff:ff) tell 10.92.110.148, length 52
21:31:13.194906 ARP, Request who-has 10.92.110.148 (ff:ff:ff:ff:ff) tell 0.0.0.0, length 52
21:31:13.398490 IP 10.92.110.171.137 > 10.92.111.255.137: NBT UDP PACKET(137): QUERY; REQUEST; BROADCAST
```

The packet capture tool allows deep analysis of traffic flowing through switch interfaces.

4. Identify and locate switch ports

Meraki Topology – a dynamic logical map of the entire network and all connected Meraki devices, lets you see exactly how things are connected. A simple mouse-over and you know exactly how a switch is interconnected. The dynamic search lets you enter in the name or even status of a switch to filter the topology based on your search terms.



Topology showing the interconnect between a closet stack and an alerting access switch

Locating where an Ethernet wall jack terminates is as easy as connecting your laptop to the jack, opening a web browser, and navigating to **switch.meraki.com**. This URL directs to a locally-hosted page on the upstream switch that advertises the switch's name, model, MAC, IP, and on which port the wall jack terminates.

Meraki

Connection Uplink configuration Switch ports status Switch ports configuration

Your client connection

Client IP	10.3.0.35
Client MAC	00:18:0a:06:a0:cd
VLAN	10
Port	13

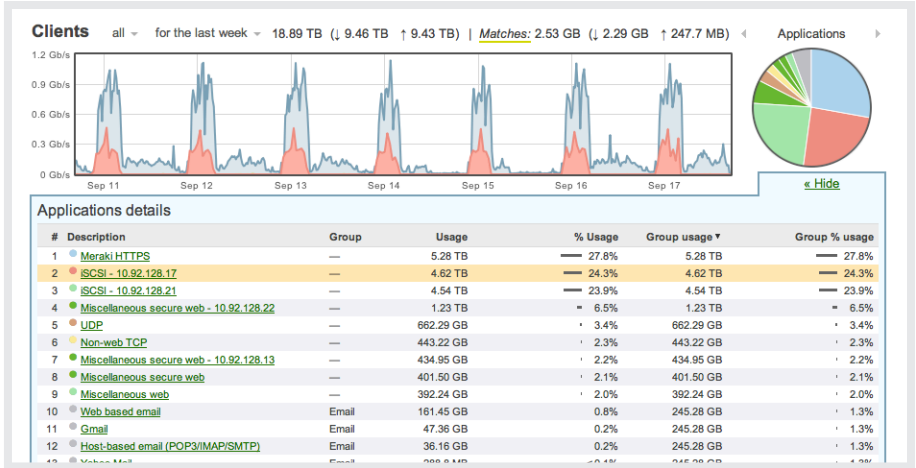
Switch details

Name	Eng 5.2.1
Network name	Engineering - MS - switch

This local switch page shows the tested wall jack terminates on port 13 of our MS350 switch.

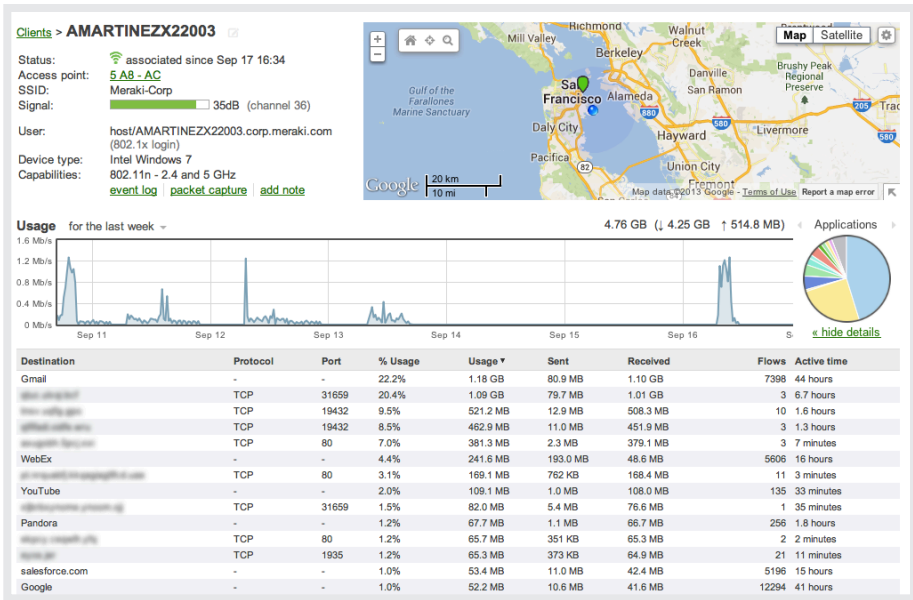
5. Identify bandwidth hogs

The Meraki dashboard will display sortable, searchable information on clients, devices, and application usage. A Google-like contextual search allows you to dynamically filter clients by device type (e.g. “iPad” or “Android HTC”), operating system, MAC, IP address, username, or device name.



Deep layer 7 visibility gives MS switches insight into the types of devices and applications passing traffic.

Drill down deeper into any application or connected client to view specific usage patterns for it.



The Meraki dashboard displays rich details about clients and applications.

6. Save energy and increase wired security

You may want to disable ports to save energy during off-peak hours or to prevent devices from accessing your network. Set schedules for a range of ports based on pre-configured templates or any timing of your choosing.

Port schedules
Local time zone: America - Los Angeles (You can set this on [Alerts & administration](#))

Energy Savings used by 0 ports

New Port Schedule used by 0 ports

Templates: [8 to 5 daily](#) [8 to 5 on weekdays only](#) [weekdays only](#) [always on](#) [always off](#)

Day	Status	During	0:00	4:00	8:00	12:00	16:00	20:00
Monday	enabled	8:00 - 17:00			↓		↓	
Tuesday	enabled	8:00 - 17:00			↓		↓	
Wednesday	enabled	8:00 - 17:00			↓		↓	
Thursday	enabled	8:00 - 17:00			↓		↓	
Friday	enabled	8:00 - 17:00			↓		↓	
Saturday	disabled	6:30 - 24:00	↓					↓
Sunday	disabled	0:00 - 24:00	↓					↓

[Add a new port schedule](#)

Port schedules prevent access to the switching fabric at the times you specify.

Applying port schedules to a range of switch interfaces takes less than 2 minutes using the Meraki dashboard. Apply policies to any port, regardless of switch model or geographic location, from anywhere in the world you have Internet access.

7. Contain rogue DHCP servers

MS switches perform DHCP snooping to identify which devices are responding as DHCP servers on your network, letting you automatically detect and block unauthorized, rogue devices. In the image below, for example, we've blocked all DHCP servers by default except for our authorized server with MAC address aa:bb:cc:dd:ee:ff. Combined with automatic detection alerts, this secures us from rogue servers which may be added to the network at any time.

DHCP servers

Configure DHCP servers DHCP servers running on layer 3 switches in this network can be configured on the [Routing and DHCP](#) page.

Email alerts

Default DHCP server policy

Note: Switches with configured DHCP servers are always allowed.

Allowed DHCP servers

DHCP servers for the last 2 hours

Description	MAC	VLAN	Subnet	IP	Last seen	Recent packet	Policy	
SD-WAN Security 1	00:18:0a:00:00:00	108	10.92.108.0/23	10.92.109.254	3 minutes	view packet	blocked	
CORE_1 (interface CORP_WIFI)	88:15:44:00:00:00	132	10.92.132.0/22	10.92.135.254	38 seconds	view packet	allowed (configured server)	
CORE_1 (interface Cisco Voice)	88:15:44:00:00:00	104	172.16.20.0/23	172.16.21.254	60 seconds	view packet	allowed (configured server)	

results per page

“Set it and forget it” rogue DHCP server containment, built into every Meraki MS switch.

8. Lock down switch access

All Meraki MS switches support 802.1X wired authentication, enabling port-based access policies that enforce authentication via user credentials or device MAC address.

If a RADIUS server has been defined, users or devices that are not recognized are automatically placed into a guest/remediation VLAN, eliminating any potential security risk to the network.

Access policies

Access policies

Name

RADIUS servers ⓘ

#	Host	Port	Secret	Actions
1	<input type="text" value="10.5.3.1"/>	<input type="text" value="5060"/>	<input type="text" value="*****"/>	<input type="button" value="↕ ×"/> <input type="button" value="Test"/>

[Add a server](#)

RADIUS testing ⓘ ⌵

Guest VLAN ⓘ

Voice VLAN clients ⓘ ⌵

Switch ports
There are currently 0 [Switch ports](#) using this policy

[Remove this access policy](#)

[Add an access policy](#)

Secure your wired network by requiring user or device-based authentication.

9. Keep current with seamless updates

Firmware and dashboard updates are pushed seamlessly from the cloud to all your Cisco Meraki devices without any pre-staging, manual downloads, or trips onsite to install patches. Every quarter, new features are released; this feature velocity future-proofs your hardware investment.

You choose the date and time to apply your switches' firmware updates — or you can opt out entirely.

Firmware upgrades

Try beta firmware What is this?

Upgrade window What is this?

Switches upgrade **The switches in this network are configured to run the latest available firmware. Last upgraded on Saturday, June 22, 2013 at 20:43 PDT.**

Upgrade as scheduled.

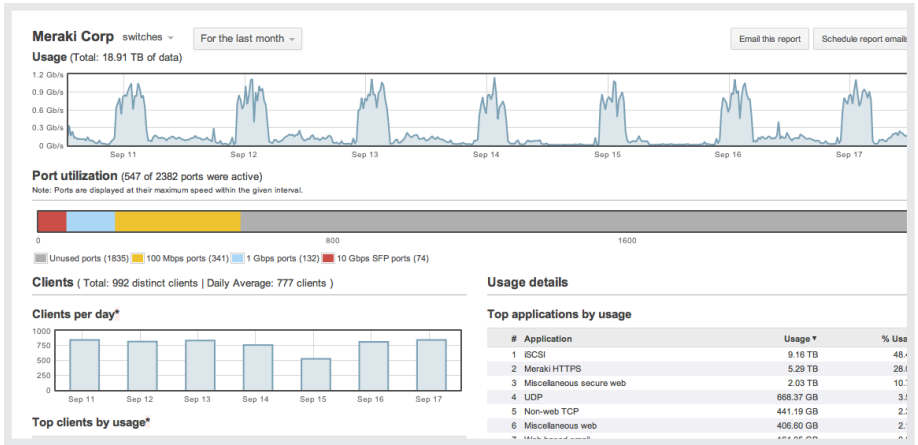
Reschedule the upgrade to: at PST

Perform the upgrade now.

Seamless updates save you time otherwise spent manually downloading and applying patches.

10. Spot network trends

Summary reports display useful trend digests. Quickly spot top applications, power consumption hogs or clients, and devices that are consuming bandwidth over the period of the report. Email a copy of the report to yourself or others, or schedule a regular report to be sent to your inbox.



Summary reporting distills large amounts of statistical detail into a “big picture” that is easily digested and shared.

Meraki MS switches provide detailed, searchable logs as well as digestible summary reports on trend statistics. Change logs track every configuration made to your switches, by whom, by date. Built-in, Google-like contextual search lets you quickly focus on only those events you want to see.

Meraki Inc. change log

"may 09" switch VLAN: 128 cl 3 changes in 4894 changes dating back to Jul 25 2012 [load more changes](#)

Time (UTC)	Admin	Network	Old value	New value
May 09 22:26	Chris Hilsenbeck	Meraki Corp - switch	Removed: Native VLAN: 1 all Trunk	Added: VLAN: 128 Access Voice VLAN:

We’ve searched here for all changes to our switching fabric performed on May 9th by “Chris” that affected VLAN 128.

