cisco Meraki

White Paper

Virtual Stacking

NOVEMBER 2012

This document describes the benefits of Meraki's Virtual Stacking technology and how you can use it to manage a distributed network. In addition, this document will show you how you can architect a stack of Meraki MS Switches to build out high availability networks.

Table of Contents

1 Introduction and Challenges

Network management at the access switch layer has become increasingly challenging over the past decade. With the explosive growth of Ethernet enabled clients in the enterprise, a commensurate rise in the number of ports allocated per user, and the rise of the distributed network, IT managers are dealing with managing large, distributed networks with tools better suited for managing the simple centralized networks of yesteryear.

While stacking technology has been around for more than two decades, it's only within the past decade that mass commercialization has taken place. Stacking technology was invented to address the challenges of switch network management by providing the IT administrator with a single management IP address to manage a "stack" of switches and to improve network resiliency. Without stacking, each switch needs its own management IP address, and as ports and network size grows, this simply does not scale.

The first stacking solutions were developed for network hubs and eventually migrated to switches. Unfortunately, the pace of innovation has not kept up to meet the challenges of modern enterprise networks. An IT administrator from the 1990s who managed "stackable hubs" would easily recognize "stackable switches" from 2012.

Stacking solutions available from traditional vendors usually require expensive proprietary technology, ranging from stacking modules for each switch to stacking cables. In addition, there are limitations on the number of switches that can be stacked, typically four to sixteen, and oftentimes they must be all of the same model. In the best implementations, efficiency is gained by creating a stack of switches that can be managed as one large switch, and in the worst implementations there are questionable gains in efficiency, since it's necessary to session into each of the member switches in a stack. For example, in one implementation, users define a master switch, and while there's a single management IP to gain entry into the stack, each member switch still must be configured independently.

Stacking can reduce management complexity for centrally managed networks, but today, the rise of the distributed enterprise means that stacking often is not enough to efficiently manage the network. Managing distributed networks now involves expensive overlay management software. Costs range from a few thousand dollars to tens of thousands of dollars, and the added complexity, training, and on-going maintenance of servers means that an IT team can quickly become over-burdened.

The answer to these challenges is Meraki's Virtual Stacking, an industry-first technology. Virtual Stacking meets the challenges of managing distributed networks by simplifying network management and reducing total cost of ownership.

Virtual Stacking

Meraki developed Virtual Stacking to allow administrators to manage and configure up to thousands of ports at once using Meraki's cloud management platform. Meraki's platform enables network-wide visibility and control, allowing administrators to monitor and configure switches, wireless access points, security appliances, and even mobile devices. Through a single pane-of-glass, IT administrators can manage their entire distributed network using an intuitive and secure web-based platform.

MS Series Switches can be added to a virtual stack without the need for proprietary stacking modules, cables, or running vendor specific protocols. Switches can be in different physical locations (e.g., New York and California) and administrators still have unprecedented visibility and manageability into all the ports in the virtual stack, greatly simplifying management of large distributed networks. Naturally, switches that are in the same physical location can also be virtually stacked.

Meraki's corporate network is an example of a distributed network, with networks in San Francisco and London, among other office locations that is managed through Virtual Stacking technology.

From the switching layer perspective, Virtual Stacking is used to manage this distributed enterprise network as groups of ports instead of individual switches. At each location, an intermediate distribution frame (IDF) on each floor serves clients located on that floor.

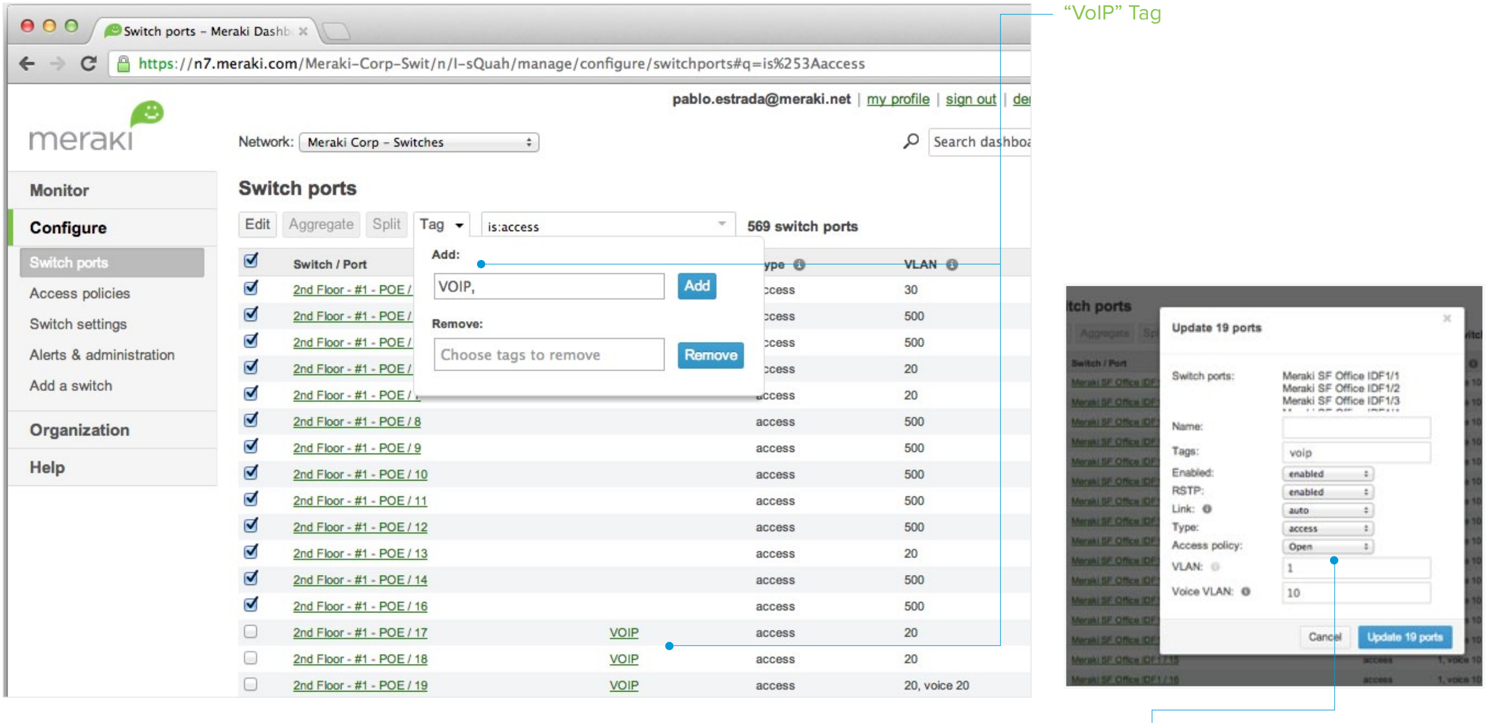
Virtual Stacking is not limited to four or sixteen switches per stack; in fact, thousands of ports can be members of a single virtual stack. This leads to a different challenge in network management, namely how to manage thousands of ports in a single pane-of-glass without overwhelming the administrator? Meraki solves this challenge by integrating switch names, tags, and a live, Google-like search. Administrators can name switches and even ports as they choose, for example, city location and floor assignment, or any other logical classification used by the organization. Tagging enables a second level of classification for even further logical grouping. For example, all VoIP ports can be tagged with "VoIP" and wireless access point ports with "WLAN," enabling easy searching and sorting through ports via the integrated live search. Finally, critical ports can be tagged with tags such as "uplink," so administrators can receive port email or text message alerts of potential network issues. You can also see in real time the status of each switch and every single port in your virtual stack.

Configuring ports has never been easier with Virtual Stacking's ability to mass edit a group of ports. It takes just a few clicks to, for example, configure the first eight ports on all switches to be access ports on a specific VLAN, apply an 802.1X access policy, disable power-over-Ethernet (PoE), and run rapid spanning tree protocol (RSTP). Creating link aggregates on uplinks, for increased throughput and redundancy, also takes just a few clicks with no command line interface (CLI).

Below is an example of how Meraki uses tags within a network. For switches that serve VoIP clients, we tag these ports with "VoIP" and this allows us to quickly search for only ports that serve VoIP clients as well as configure these ports, regardless of where the switches are located.

FIGURE 1

Tagging & Configuring Ports



"VoIP" Tag

Switch ports – Meraki Dashb

https://n7.meraki.com/Meraki-Corp-Swit/n/I-sQuah/manage/configure/switchports#q=is%253Aaccess

pablo.estrada@meraki.net | my profile | sign out | de

Network: Meraki Corp – Switches

Switch ports

Tag: is:access — 569 switch ports

Add: VOIP,

Remove: Choose tags to remove

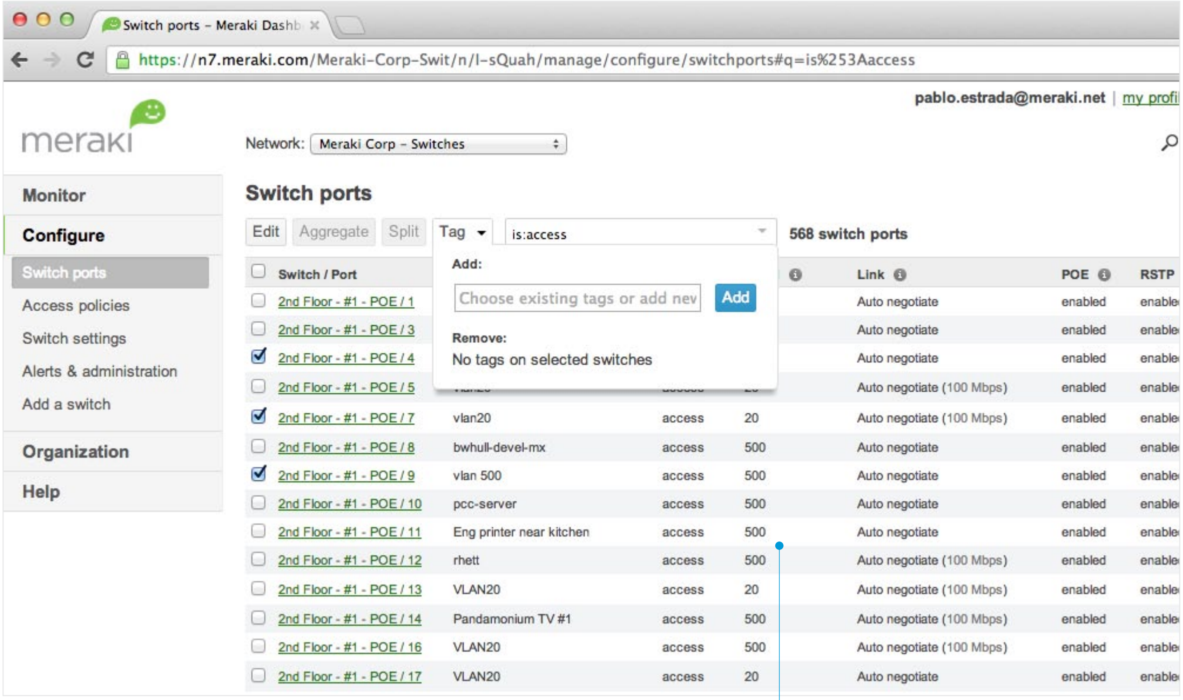
☑	Switch / Port		Type	VLAN
☑	2nd Floor - #1 - POE /		ccess	30
☑	2nd Floor - #1 - POE /		ccess	500
☑	2nd Floor - #1 - POE /		ccess	500
☑	2nd Floor - #1 - POE /		ccess	20
☑	2nd Floor - #1 - POE /		access	20
☑	2nd Floor - #1 - POE / 8		access	500
☑	2nd Floor - #1 - POE / 9		access	500
☑	2nd Floor - #1 - POE / 10		access	500
☑	2nd Floor - #1 - POE / 11		access	500
☑	2nd Floor - #1 - POE / 12		access	500
☑	2nd Floor - #1 - POE / 13		access	20
☑	2nd Floor - #1 - POE / 14		access	500
☑	2nd Floor - #1 - POE / 16		access	500
□	2nd Floor - #1 - POE / 17	VOIP	access	20
□	2nd Floor - #1 - POE / 18	VOIP	access	20
□	2nd Floor - #1 - POE / 19	VOIP	access	20, voice 20

Update 19 ports

Switch ports: Meraki SF Office IDF1/1
Meraki SF Office IDF1/2
Meraki SF Office IDF1/3

Name:
Tags: voip
Enabled: enabled
RSTP: enabled
Link: auto
Type: access
Access policy: Open
VLAN: 1
Voice VLAN: 10

Configure all "VoIP" ports to be on data VLAN 1 and voice VLAN 10



https://n7.meraki.com/Meraki-Corp-Swit/n/l-sQuah/manage/configure/switchports#q=is%253Aaccess

pablo.estrada@meraki.net

Network: Meraki Corp – Switches

Switch ports

is:access

568 switch ports

Add:

Choose existing tags or add nev

Remove:

No tags on selected switches

☐	Switch / Port				Link	POE	RSTP
☐	2nd Floor - #1 - POE / 1				Auto negotiate	enabled	enable
☐	2nd Floor - #1 - POE / 3				Auto negotiate	enabled	enable
☑	2nd Floor - #1 - POE / 4				Auto negotiate	enabled	enable
☐	2nd Floor - #1 - POE / 5				Auto negotiate (100 Mbps)	enabled	enable
☑	2nd Floor - #1 - POE / 7	vlan20	access	20	Auto negotiate (100 Mbps)	enabled	enable
☐	2nd Floor - #1 - POE / 8	bwhull-devel-mx	access	500	Auto negotiate	enabled	enable
☑	2nd Floor - #1 - POE / 9	vlan 500	access	500	Auto negotiate	enabled	enable
☐	2nd Floor - #1 - POE / 10	pcc-server	access	500	Auto negotiate	enabled	enable
☐	2nd Floor - #1 - POE / 11	Eng printer near kitchen	access	500	Auto negotiate	enabled	enable
☐	2nd Floor - #1 - POE / 12	rhett	access	500	Auto negotiate (100 Mbps)	enabled	enable
☐	2nd Floor - #1 - POE / 13	VLAN20	access	20	Auto negotiate (100 Mbps)	enabled	enable
☐	2nd Floor - #1 - POE / 14	Pandamonium TV #1	access	500	Auto negotiate (100 Mbps)	enabled	enable
☐	2nd Floor - #1 - POE / 16	VLAN20	access	500	Auto negotiate (100 Mbps)	enabled	enable
☐	2nd Floor - #1 - POE / 17	VLAN20	access	20	Auto negotiate	enabled	enable

Configured VoIP ports

The ability to quickly search and apply configuration changes to distributed enterprise networks is extremely powerful. Ports are identified by specific tags, and administrators can configure specific ports across an entire distributed network. With Virtual Stacking, unprecedented scalability and location-independent deployments are a reality.

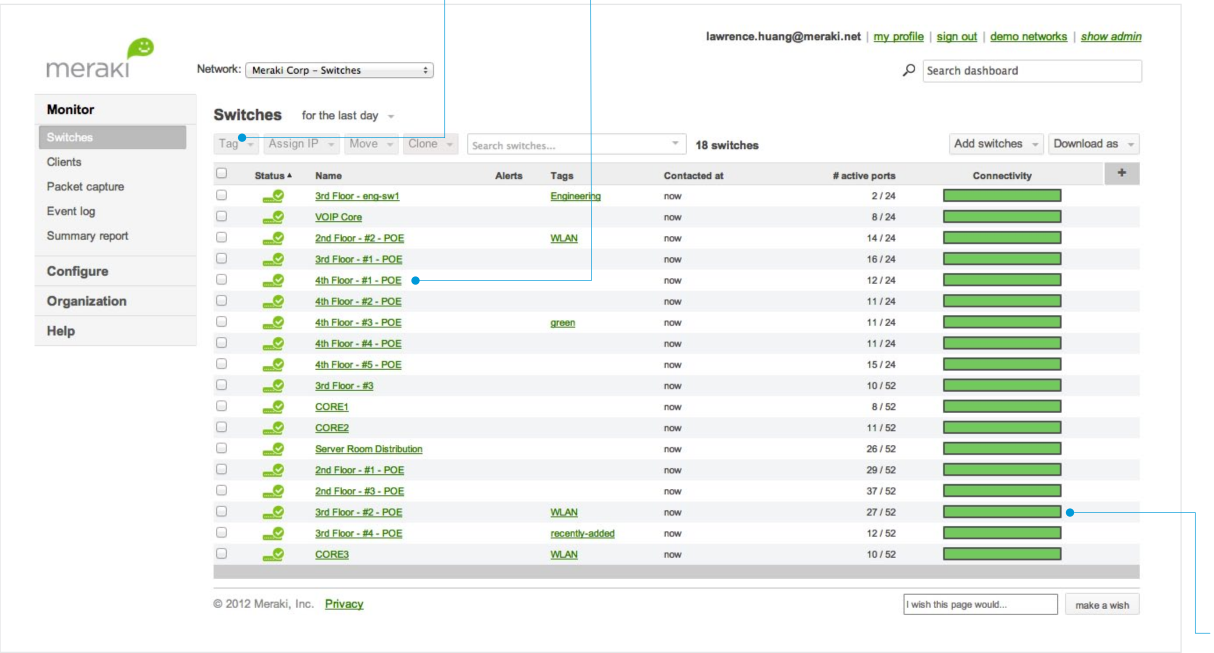
Scalability is as important as ease-of-management when it comes to Virtual Stacking. Switch networks can include up to 10,000 ports in a Virtual Stack while providing users with benefits such as being able to pre-configure a switch before it even arrives on-site using the "Add a Switch" feature or simply copy existing configuration settings to new or existing switches using the "Clone" tool. This allows IT administrators to quickly deploy new switches to branch locations without hiring expensive contractors. Replacing or adding new switches has never been easier.

2 Virtual Stacking

Below is an overview of how Virtual Stacking is laid out. Innovation that meets the challenges of the modern access layer has finally arrived. With Virtual Stacking, IT administrators can easily manage large distributed network deployments while minimizing training costs, configuration errors, and reducing complexity.

FIGURE 2

Virtual Stack of Switches



lawrence.huang@meraki.net | my profile | sign out | demo networks | show admin

Network: Meraki Corp – Switches

Switches for the last day

18 switches

□	Status ▲	Name	Alerts	Tags	Contacted at	# active ports	Connectivity
□	✓	3rd Floor - eng-sw1		Engineering	now	2 / 24	🟩
□	✓	VOIP Core			now	8 / 24	🟩
□	✓	2nd Floor - #2 - POE		WLAN	now	14 / 24	🟩
□	✓	3rd Floor - #1 - POE			now	16 / 24	🟩
□	✓	4th Floor - #1 - POE			now	12 / 24	🟩
□	✓	4th Floor - #2 - POE			now	11 / 24	🟩
□	✓	4th Floor - #3 - POE		green	now	11 / 24	🟩
□	✓	4th Floor - #4 - POE			now	11 / 24	🟩
□	✓	4th Floor - #5 - POE			now	15 / 24	🟩
□	✓	3rd Floor - #3			now	10 / 52	🟩
□	✓	CORE1			now	8 / 52	🟩
□	✓	CORE2			now	11 / 52	🟩
□	✓	Server Room Distribution			now	26 / 52	🟩
□	✓	2nd Floor - #1 - POE			now	29 / 52	🟩
□	✓	2nd Floor - #3 - POE			now	37 / 52	🟩
□	✓	3rd Floor - #2 - POE		WLAN	now	27 / 52	🟩
□	✓	3rd Floor - #4 - POE		recently-added	now	12 / 52	🟩
□	✓	CORE3		WLAN	now	10 / 52	🟩

© 2012 Meraki, Inc. Privacy

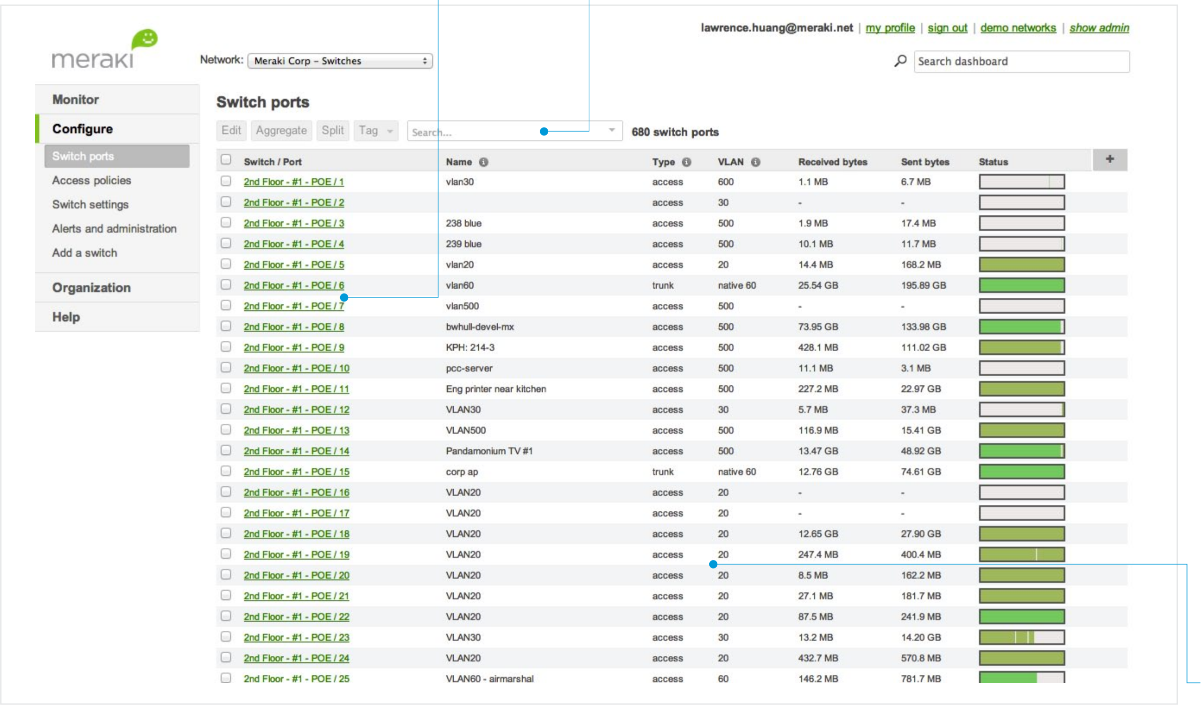
Tags

Named Switches in a Virtual Stack

Health Status of Switches

FIGURE 3

Virtual Stack of Ports



lawrence.huang@meraki.net | my profile | sign out | demo networks | show admin

Network: Meraki Corp – Switches

Switch ports

680 switch ports

□	Switch / Port	Name	Type	VLAN	Received bytes	Sent bytes	Status
□	2nd Floor - #1 - POE / 1	vlan30	access	600	1.1 MB	6.7 MB	
□	2nd Floor - #1 - POE / 2		access	30	-	-	
□	2nd Floor - #1 - POE / 3	238 blue	access	500	1.9 MB	17.4 MB	
□	2nd Floor - #1 - POE / 4	239 blue	access	500	10.1 MB	11.7 MB	
□	2nd Floor - #1 - POE / 5	vlan20	access	20	14.4 MB	168.2 MB	
□	2nd Floor - #1 - POE / 6	vlan60	trunk	native 60	25.54 GB	195.89 GB	
□	2nd Floor - #1 - POE / 7	vlan500	access	500	-	-	
□	2nd Floor - #1 - POE / 8	bwhull-devel-mx	access	500	73.95 GB	133.98 GB	
□	2nd Floor - #1 - POE / 9	KPH: 214-3	access	500	428.1 MB	111.02 GB	
□	2nd Floor - #1 - POE / 10	pcc-server	access	500	11.1 MB	3.1 MB	
□	2nd Floor - #1 - POE / 11	Eng printer near kitchen	access	500	227.2 MB	22.97 GB	
□	2nd Floor - #1 - POE / 12	VLAN30	access	30	5.7 MB	37.3 MB	
□	2nd Floor - #1 - POE / 13	VLAN500	access	500	116.9 MB	15.41 GB	
□	2nd Floor - #1 - POE / 14	Pandamonium TV #1	access	500	13.47 GB	48.92 GB	
□	2nd Floor - #1 - POE / 15	corp ap	trunk	native 60	12.76 GB	74.61 GB	
□	2nd Floor - #1 - POE / 16	VLAN20	access	20	-	-	
□	2nd Floor - #1 - POE / 17	VLAN20	access	20	-	-	
□	2nd Floor - #1 - POE / 18	VLAN20	access	20	12.65 GB	27.90 GB	
□	2nd Floor - #1 - POE / 19	VLAN20	access	20	247.4 MB	400.4 MB	
□	2nd Floor - #1 - POE / 20	VLAN20	access	20	8.5 MB	162.2 MB	
□	2nd Floor - #1 - POE / 21	VLAN20	access	20	27.1 MB	181.7 MB	
□	2nd Floor - #1 - POE / 22	VLAN20	access	20	87.5 MB	241.9 MB	
□	2nd Floor - #1 - POE / 23	VLAN30	access	30	13.2 MB	14.20 GB	
□	2nd Floor - #1 - POE / 24	VLAN20	access	20	432.7 MB	570.8 MB	
□	2nd Floor - #1 - POE / 25	VLAN60 - airmarshal	access	60	146.2 MB	781.7 MB	

Named Ports in a Virtual Stack

Live Search Bar

Port Details and Statistics

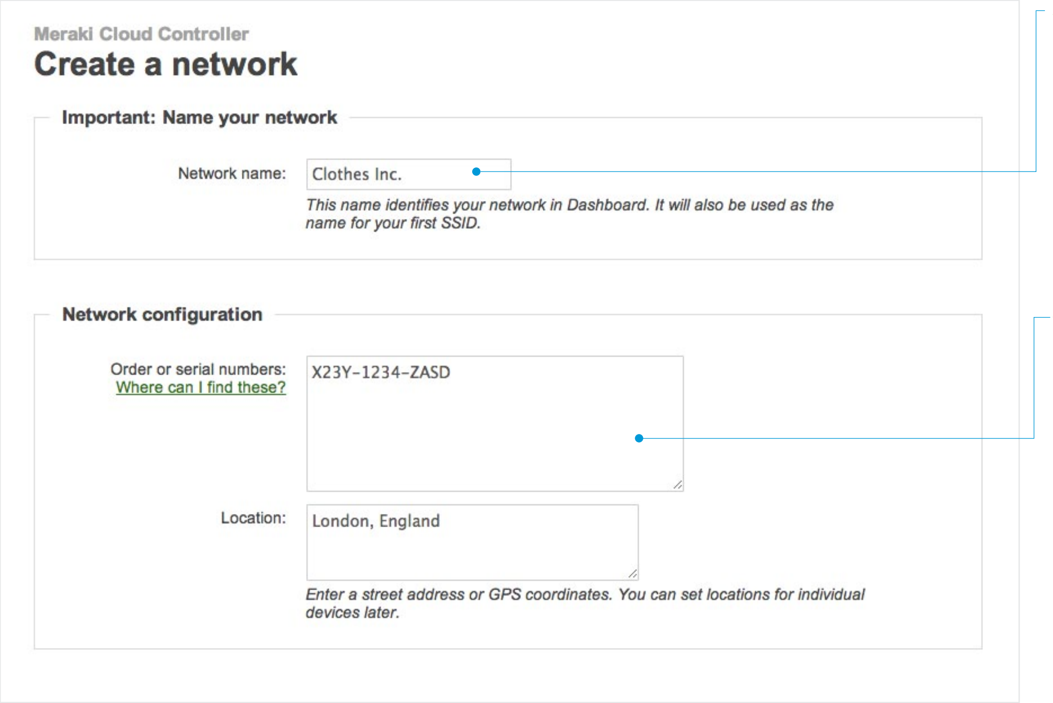
2.1 Retail Example

Consider a retail company that has 50 stores across North America and is undergoing a network refresh. The IT team wants to deploy a common network infrastructure across all their stores. They plan on using 24 port PoE switches at these locations and want to assign ports 1-10 to VoIP phones and ports 11-15 to wireless access points. Ports 16-23 will be disabled and reserved for future use while port 24 is a trunk to upstream devices. The goal is to complete the upgrade in three months with a controlled rollout process. The IT team will oversee installation and bring-up on-site at the company's flagship stores but will not be available at all locations. Instead, they plan to hire contractors to install equipment at the remaining locations, so they want a way to ensure the remaining deployments are as quick and error-free as possible.

Meraki's Virtual Stacking technology makes this type of deployment simple. IT can configure a test store network, verify configuration settings, and then use Meraki's "add a switch" and "clone" features to add new switches with predefined configurations to the network.

EXAMPLE DEPLOYMENT/SWITCH CONFIGURATION STEPS

1—Create switch network



Meraki Cloud Controller

Create a network

Important: Name your network

Network name: Clothes Inc.

This name identifies your network in Dashboard. It will also be used as the name for your first SSID.

Network configuration

Order or serial numbers: X23Y-1234-ZASD

Where can I find these?

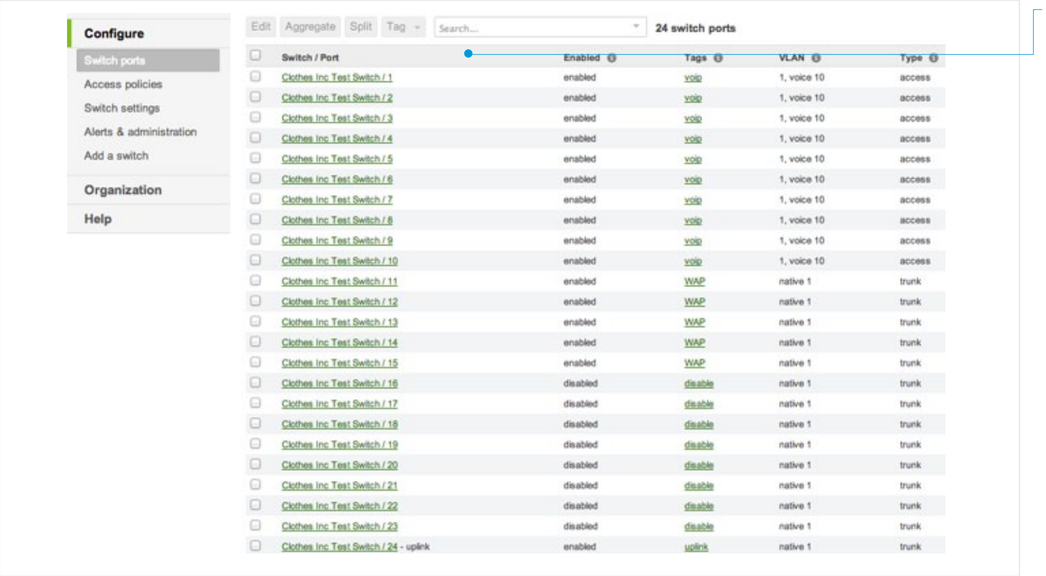
Location: London, England

Enter a street address or GPS coordinates. You can set locations for individual devices later.

Switch Network Name

Order or Serial Number

2—Configure switch ports

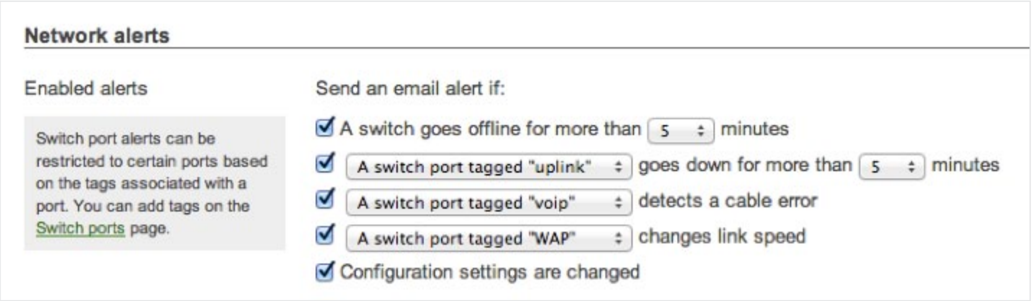


24 switch ports

□	Switch / Port	Enabled	Tags	VLAN	Type
□	Clothes Inc Test Switch / 1	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 2	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 3	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 4	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 5	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 6	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 7	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 8	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 9	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 10	enabled	voip	1, voice 10	access
□	Clothes Inc Test Switch / 11	enabled	WAP	native 1	trunk
□	Clothes Inc Test Switch / 12	enabled	WAP	native 1	trunk
□	Clothes Inc Test Switch / 13	enabled	WAP	native 1	trunk
□	Clothes Inc Test Switch / 14	enabled	WAP	native 1	trunk
□	Clothes Inc Test Switch / 15	enabled	WAP	native 1	trunk
□	Clothes Inc Test Switch / 16	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 17	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 18	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 19	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 20	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 21	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 22	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 23	disabled	disable	native 1	trunk
□	Clothes Inc Test Switch / 24 - uplink	enabled	uplink	native 1	trunk

Ports 1-10: VoIP
Ports 11-15: WAP
Ports 16-23: Disabled
Port 24: Uplink

3—Define per port alerts for critical ports such as "uplink"



Network alerts

Enabled alerts

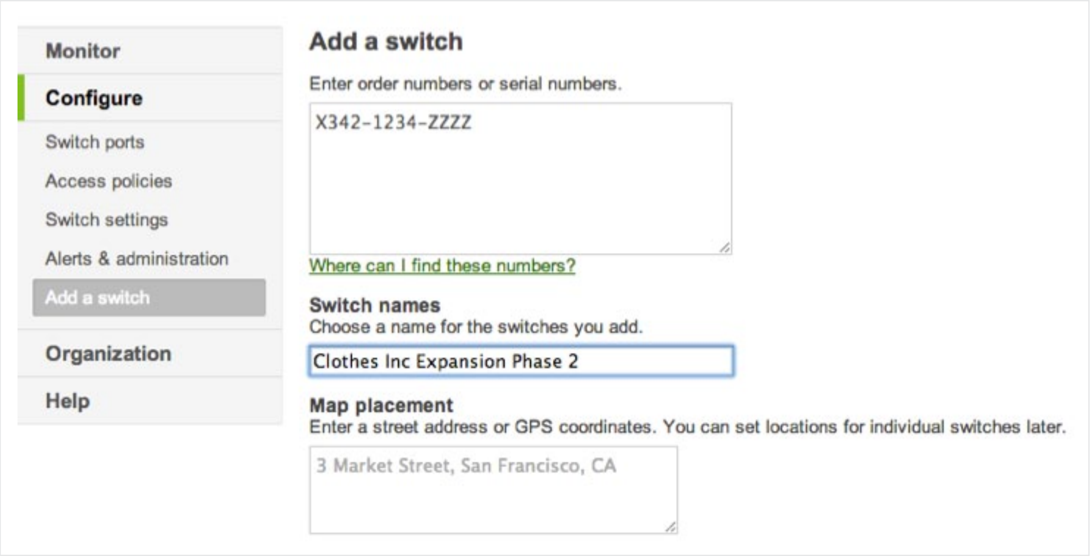
Switch port alerts can be restricted to certain ports based on the tags associated with a port. You can add tags on the Switch ports page.

Send an email alert if:

- ☑ A switch goes offline for more than 5 minutes
- ☑ A switch port tagged "uplink" goes down for more than 5 minutes
- ☑ A switch port tagged "voip" detects a cable error
- ☑ A switch port tagged "WAP" changes link speed
- ☑ Configuration settings are changed

4—Verify configuration and settings in test network and deploy to flagship stores

5—Add new switches to network by order number or serial number



Add a switch

Enter order numbers or serial numbers.

X342-1234-ZZZZ

Where can I find these numbers?

Switch names

Choose a name for the switches you add.

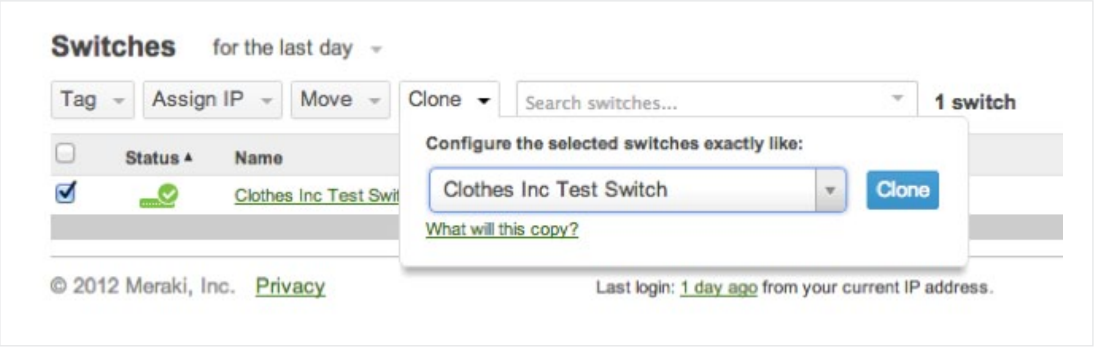
Clothes Inc Expansion Phase 2

Map placement

Enter a street address or GPS coordinates. You can set locations for individual switches later.

3 Market Street, San Francisco, CA

6—Clone switch settings using "clone" tool to clone newly added switch to be exactly like existing "Clothes Inc Test Switch."



☑ Clothes Inc Test Swit

Configure the selected switches exactly like:

Clothes Inc Test Switch

What will this copy?

© 2012 Meraki, Inc. Privacy

Last login: 1 day ago from your current IP address.

7—Ship switches to retail sites for contractors to install (no additional configuration required)

If any configuration changes need to be made, the IT staff can search by names or tags and edit all the VoIP ports across all 50 sites or all the WLAN ports with just a few clicks.

3 Building Resilient Networks

While traditional stacking is used to simplify switch management, many IT administrators need resilient networks with redundancy and high availability to support business continuity. Traditionally, increased redundancy is achieved by providing two physical paths between any of the switches in a stack, thus providing alternate paths so that losing one switch or uplink does not sever connectivity to the rest of the network.

Again, this often involves proprietary stacking modules and cables, along with vendor specific protocols for re-convergence in case one of the physical links fails. In addition, many vendors have limitations on which switch models support physical stacking, and they often can't be mixed-and-matched in one stack.

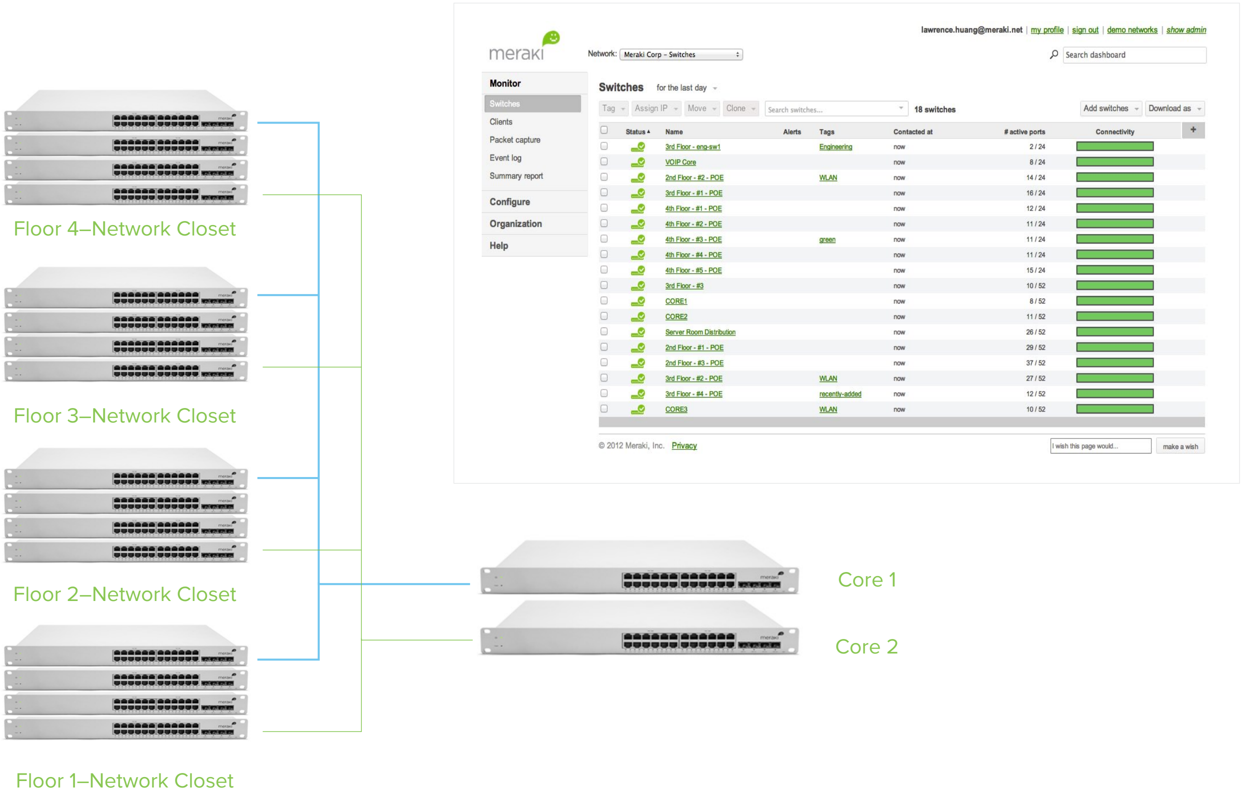
As discussed earlier, Meraki's MS Series Switches support redundant architectures using standards-based modules and protocols, such as LACP and RSTP. The end result is a network that has all the benefits of Virtual Stacking with no single point of failure.

Below is an example of a resilient switch network at Meraki's headquarters. Each floor has an IDF, with four switches per wiring closet, all of which are managed through a single pane-of-glass, the Meraki dashboard.

A closer look at the IDF on the third floor reveals a group of MS42P switches with 10G uplinks. The connection between the switches uses standards-based 10G Twinax cabling.

FIGURE 4

Network Resiliency



lawrence.huang@meraki.net | my profile | sign out | demo networks | show admin

Network: Meraki Corp – Switches

Search dashboard

Switches for the last day

Search switches... 18 switches

□	Status ▲	Name	Alerts	Tags	Contacted at	# active ports	Connectivity
□	✓	3rd Floor - eng-sw1		Engineering	now	2 / 24	🟩
□	✓	VOIP Core			now	8 / 24	🟩
□	✓	2nd Floor - #2 - POE		WLAN	now	14 / 24	🟩
□	✓	3rd Floor - #1 - POE			now	16 / 24	🟩
□	✓	4th Floor - #1 - POE			now	12 / 24	🟩
□	✓	4th Floor - #2 - POE			now	11 / 24	🟩
□	✓	4th Floor - #3 - POE		green	now	11 / 24	🟩
□	✓	4th Floor - #4 - POE			now	11 / 24	🟩
□	✓	4th Floor - #5 - POE			now	15 / 24	🟩
□	✓	3rd Floor - #3			now	10 / 52	🟩
□	✓	CORE1			now	8 / 52	🟩
□	✓	CORE2			now	11 / 52	🟩
□	✓	Server Room Distribution			now	26 / 52	🟩
□	✓	2nd Floor - #1 - POE			now	29 / 52	🟩
□	✓	2nd Floor - #3 - POE			now	37 / 52	🟩
□	✓	3rd Floor - #2 - POE		WLAN	now	27 / 52	🟩
□	✓	3rd Floor - #4 - POE		recently-added	now	12 / 52	🟩
□	✓	CORE3		WLAN	now	10 / 52	🟩

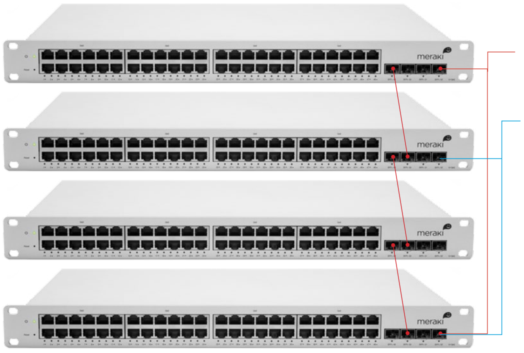
© 2012 Meraki, Inc. Privacy

I wish this page would...

FIGURE 5
Example of Stacking
Meraki MS

RSTP is running on the example above. In this case, one of the side links is blocked under normal operating conditions, and the stack is divided up into 2 x 2 switch pairs. Each of the pairs uses its respective 10G uplink, providing redundant uplinks for the stack.

When designing a switch network for high availability and redundancy, it's important to understand and plan for link failures.



10G between IDF switches

10G between IDF switches

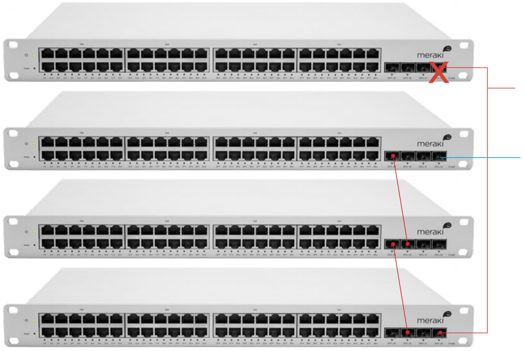
Fully redundant, no single point of failure

Virtual Stacking for simplified management

Upgrades managed through cloud with no manual intervention needed

FIGURE 6
Single Side Link Failure

In the event of a single side link failure, RSTP will re-converge in 1-2 seconds.



10G uplinks to MDF uses standards-based SFP+

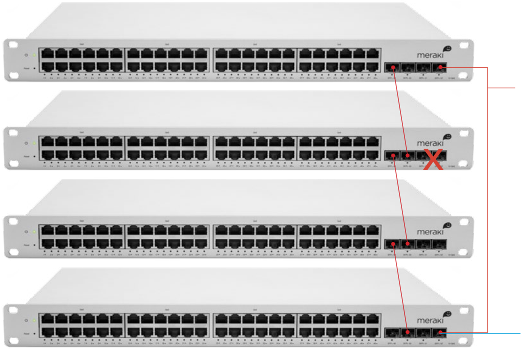
Connections between switches use standards-based Twinax cables

RSTP running on network with 1-2 second re-convergence time

20Gbps stacking bandwidth

FIGURE 7
Single Uplink Failure

With a single uplink failure, RSTP will unblock one of the side links so all four switches in a stack can use the remaining 10Gbps uplink.



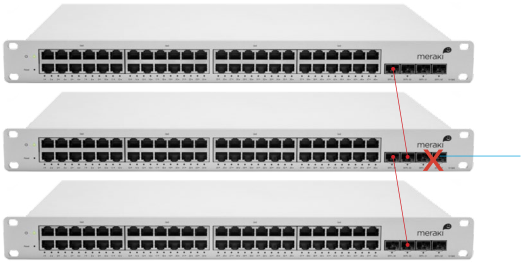
No proprietary stacking modules

No proprietary stacking cables

No hard limitations on the number of switches in a stack

FIGURE 8
Single Switch Failure

With a single uplink failure, RSTP will unblock one of the side links so all four switches in a stack can use the remaining 10Gbps uplink.



MS Series designed with enterprise class components for high MTBF

Full Lifetime hardware warranty with next-day advanced replacement

The examples above show that a physical stack of MS Series Switches can be built using standards-based hardware and protocols. The architecture provides high availability and resiliency to potential network link and hardware failures, all without using proprietary stacking modules or cables.

3.1 Comparing Traditional Stacking to Virtual Stacking

Traditional Stacking Benefit Claimed	Traditional Stacking Reality	Virtual Stacking Reality
Simplified management and monitoring via a single management IP	Limited typically to 4-16 switches in a stack May require expensive proprietary stacking modules and cables	Scalable to thousands of switch ports in a Virtual Stack, regardless of geographic location No proprietary stacking modules or cables
Single configuration file for a stack of switches	Need to back-up this configuration and copy per stack...not scalable for large deployments without expensive network management overlay	Single interface for configuration that gets applied automatically to all switches in Virtual Stack
Centralized image upgrades	Session into the "master" switch for stack and upgrade master	Firmware updates can be set to automatic for all switches with no user intervention
Reducing the number of uplink ports	High bandwidth uplinks may require additional configuration, such as LACP	Easily configure link aggregates for high bandwidth and redundancy
Resiliency	Resilient against uplink, sidelink, and switch failure but often requires proprietary modules, cables, and protocols	Resilient against uplink, sidelink, and switch failure with standards-based modules and protocols

Conclusion

Virtual Stacking is the innovation that has been missing in enterprise networking at the access layer. Meraki's MS Series switches with Virtual Stacking simplify network management so that distributed enterprise networks can easily be managed through an intuitive single pane-of-glass. IT administrators can now monitor and configure anything from a single port to thousands of ports with a solution that is scalable, resilient, and cost effective without the need for expensive proprietary hardware or network management overlays. In addition, building resilient networks is simple with standards-based hardware and protocols.