



The bridge to possible

# Scalable Meraki Access Switching

Brennan Martin, Senior Technical Marketing Engineer  
@ehFrames

# Cisco Webex App

## Questions?

Use Cisco Webex App to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Live 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 until February 24, 2023.





# Agenda

- Introductions
- Device & Platform
- Core Networking
- Security & Zero Trust
- Catalyst & Meraki
- Wrap up

Who is this  
funny guy, eh?



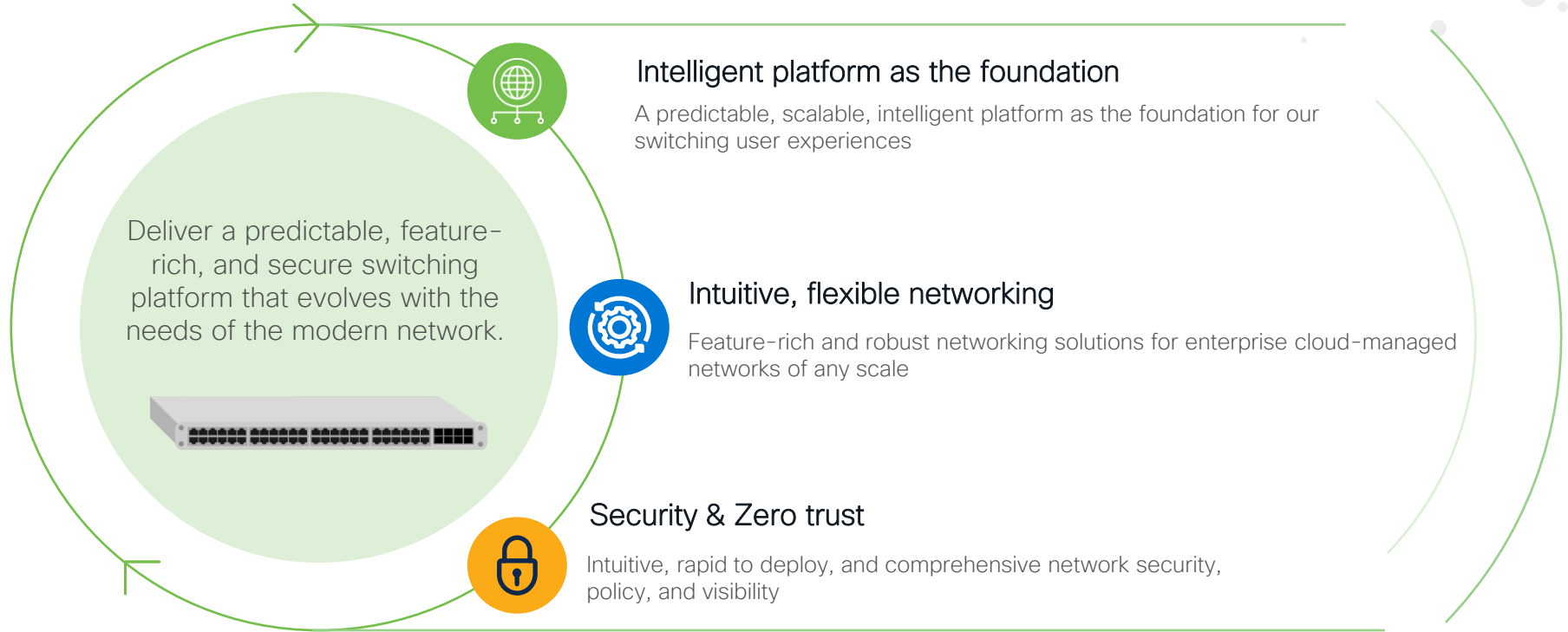
# I'm a Canadian that loves building networks

- Based in Saskatoon, Saskatchewan – Canada
- 16 years in the field deploying networks
- CCIE R/S #50782
- More time underground than in data centers
- Ask me about potash



# Meraki Switching is evolving

# Our vision for the Meraki Switching Experience

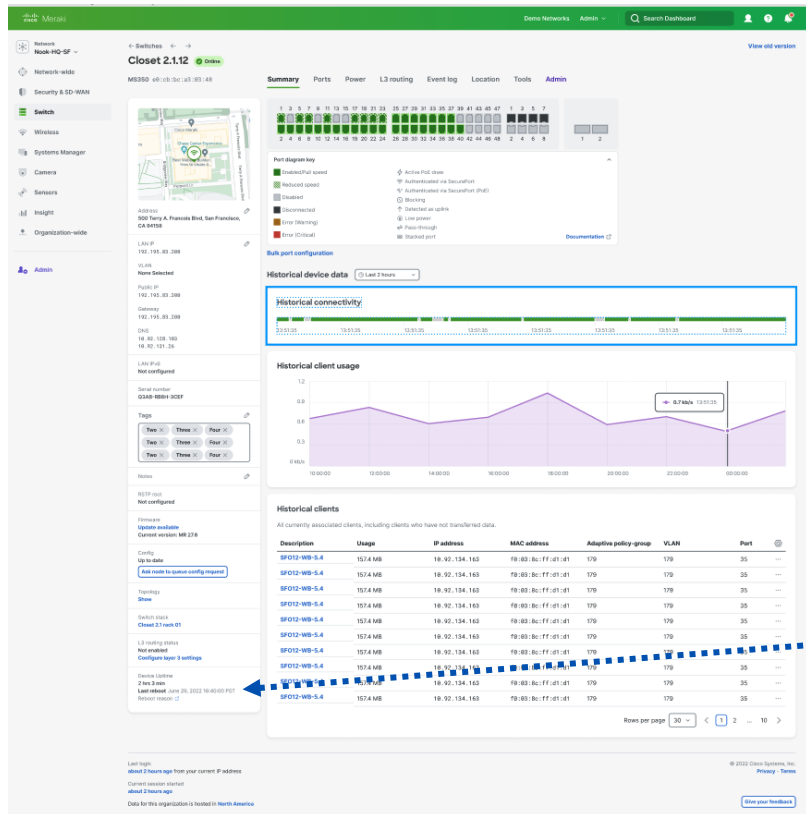


# Device & Platform





# Device Uptime is coming



## Features

Uptime visibility  
Last known reboot with timestamp  
Reboot reasons  
Link to event log  
Available via API

## Benefit

Customers can see device uptime in the dashboard  
Customers can learn events that relate to device reboot

Device Uptime

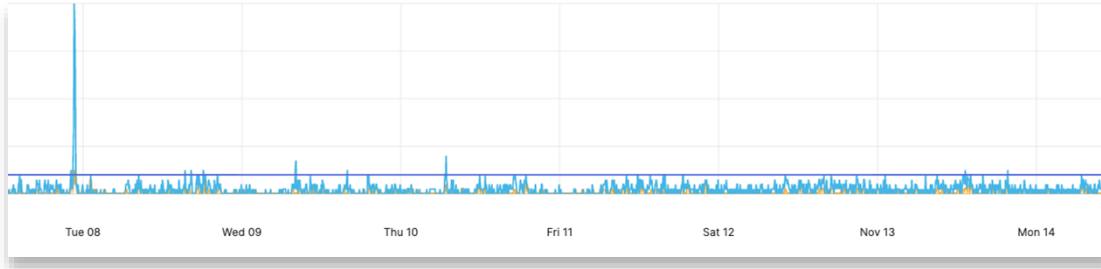
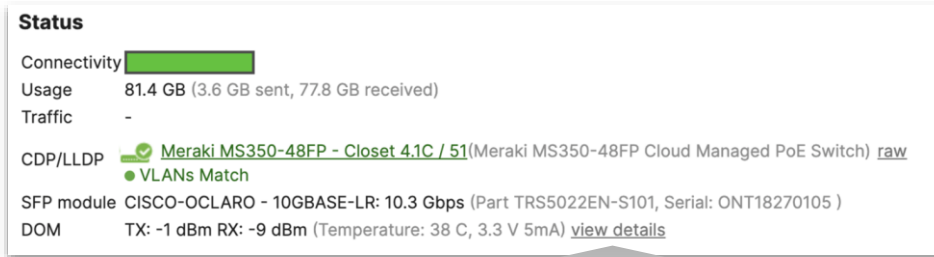
2 hrs 3 min

Last reboot June 29, 2022 16:40:00 PST

Reboot reason [🔗](#)

Reboot reasons like "Dashboard Initiated",  
"Other", and "Firmware Upgrade"

# Digital Optical Monitoring



## Solution Capability

Real-time light levels\*  
Temperature\*  
Voltage\*  
Historical view  
Available via API



## Benefit

Troubleshooting past and present events  
Historical graphs for RCA of events

# Port Management at Scale with Port Profiles

The screenshot displays the 'Switch port profiles' management interface. On the left, a table lists several profiles, with 'My\_switch\_port\_profile\_A' highlighted. An orange box around this profile name has a line pointing to the 'Profile' dropdown in the 'Edit switch port' modal on the right. The modal shows configuration options for a specific switch port, including status, type, access policy, VLAN, and various protocols like STP and UDLD. Below the table, a diagram shows three network switches labeled 'Site 1', 'Site 2', and 'Site n', with blue lines indicating the application of the selected profile to specific ports across these sites.

Name	Date created	# ports
My_switch_port_profile_A	January 12, 12:34 AM	2
My_switch_port_profile_B	January 12, 12:34 AM	5
Switch port profile name 3	January 12, 12:34 AM	0
Switch port profile name 4	January 12, 12:34 AM	12
Switch port profile name 5	January 12, 12:34 AM	33
Switch port profile name 6	January 12, 12:34 AM	0

**Edit switch port**

Switch / port: SFO22-M31-FLOOR1 / 1

Port name: IoT Device

Profile: My\_switch\_port\_profile\_A

Port status: ☒ Enabled

Type: Access

Access policy: Open

VLAN: 1

Voice VLANs: All

Link negotiation: Auto negotiate

RSTP: ☒ Enabled

STP guard: Disabled

Port schedule: Unscheduled

Adaptive policy group: IT: IoT

Port isolation: ☐ Enabled

Trusted DAI: ☐ Enabled

Peer SGT capable: ☒ Enabled

UDLD: Alert only

Tags: Two X Three X

PoE: ☒ Enabled

Buttons: Cancel Save

Building-blocks containing configuration settings for a switchport that can be applied to one or thousands of ports.

- Assign per port range once and **save countless hours** during initial deployment and for the lifespan of the environment
- Create **dynamic rulesets** based on learned information including RADIUS attributes, MAC OUIs, and Discovery Protocols (CDP/LLDP)\*

Early Preview expected Early 2023

*\*Dynamic available via a later release*

# Now you can upgrade in stages

Staged Upgrades can help in several scenarios

## Scenario A

*"I have a one-hour maintenance window each night, but I also have 200 switches."*

## Scenario B

*"I can handle a daily outage for access switches, but only have one window a month to upgrade the core"*

# Improved Staged Upgrades adds flexibility



Reusable Sequences



Defer, Reschedule, and Rollback



Better Upgrade Monitoring



Full API support

## Schedule firmware change

When should this firmware be installed?

*Upgrade times may be staggered depending on the number of devices changing firmware.*

☐ Perform the upgrade now

☒ Schedule staged upgrade

New!

☐ Schedule the upgrade for:

06/27/2022

at

12:00

(network local time)



Back

Next

# Firmware Upgrade Status provides visibility

<input type="checkbox"/>	#	Name	Connectivity	Firmware version
<input type="checkbox"/>	1	✓ <a href="#">CAMPUS-SFO-IDF1.1.1-MS390-24UX</a>	<div></div>	MS 14.33.1
<input type="checkbox"/>	2	✓ <a href="#">CAMPUS-SFO-IDF1.1.2-MS390-24UX</a>	<div></div>	MS 14.33.1
<input type="checkbox"/>	3	✓ <a href="#">CAMPUS-SFO-IDF2.1.1-MS355-24X</a>	<div></div>	MS 14.33.1
<input type="checkbox"/>	4	! <a href="#">CAMPUS-SFO-IDF2.1.1.1</a> <span>Monitor Only</span>	<div></div>	IOS XE 17.8.1
<input type="checkbox"/>	5	✓ <a href="#">CAMPUS-SFO-IDF2.1.1.2-MS225-24P</a>	<div></div>	Not running configured version
<input type="checkbox"/>	6	✓ <a href="#">CAMPUS-SFO-MDF1.1-MS425-16-CORE1</a>	<div></div>	MS 14.33.1

## FIRMWARE

[Update scheduled](#)

Upgrade Status: Started

Current version: Not running configured version

Upgrading to: MS 15.14.2

## Upgrade Statuses:

- Pending
- Started
- Skipped
- Cancelled
- Completed

# Core Networking

# Alternate Management Interface



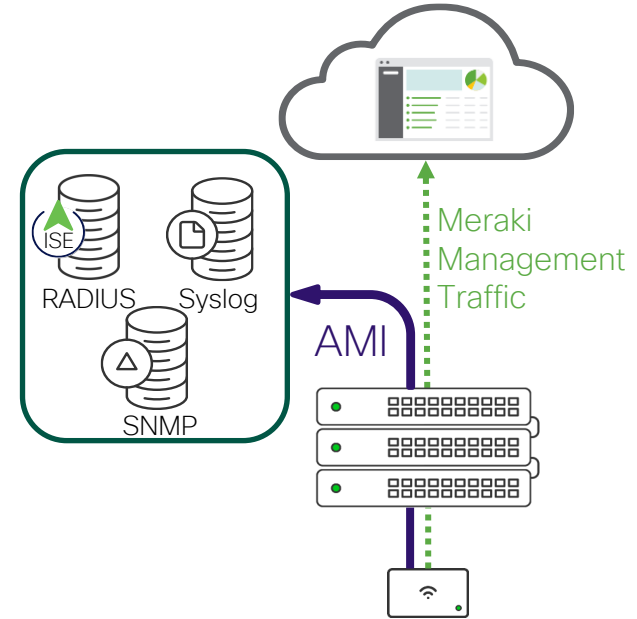
RADIUS, Syslog, and SNMP on a secondary interface



Follows the **data-plane path** vs primary management interface



Separation of cloud from infrastructure management





# Demo

## Guided VLAN Mismatch

# Named VLANs automates translation for you

**VLAN profiles**

**Edit profiles**

Profile name  
Test API

Iname  
Iname

**Named VLANs** [Add a Named VLAN](#)

#	VLAN name	VLAN ID	Actions
1	Employee	100	<a href="#">Save</a> <a href="#">Cancel</a>
2	IOT	110	<a href="#">✎</a> <a href="#">✕</a>
3	DMZ	999	<a href="#">✎</a> <a href="#">✕</a>

**VLAN Groups** [Add a VLAN group](#)

#	Group name	VLAN list	Actions
1	Employees	100-109	<a href="#">Save</a> <a href="#">Cancel</a>
2	IOTDevices	110-119	<a href="#">✎</a> <a href="#">✕</a>
3	Guest	999-1000	<a href="#">✎</a> <a href="#">✕</a>

**Edit switch port**

Name  
Employee Desk Port

Port status  
☒ Enabled

Type  
Access

Access policy  
Open

VLAN  
Employee

Voice VLAN  
VoIP

Link negotiation  
Auto negotiate

Single VLAN ID  
to Name

Group of VLANs  
to Name

RADIUS based  
assignment

Static  
Assignment

# Security & Zero Trust



# Security Fundamentals

# SecurePort securely automates Wi-Fi expansion



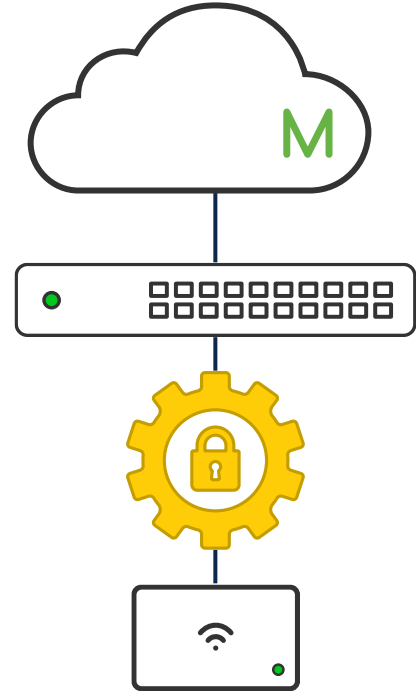
Automating AP switchports securely



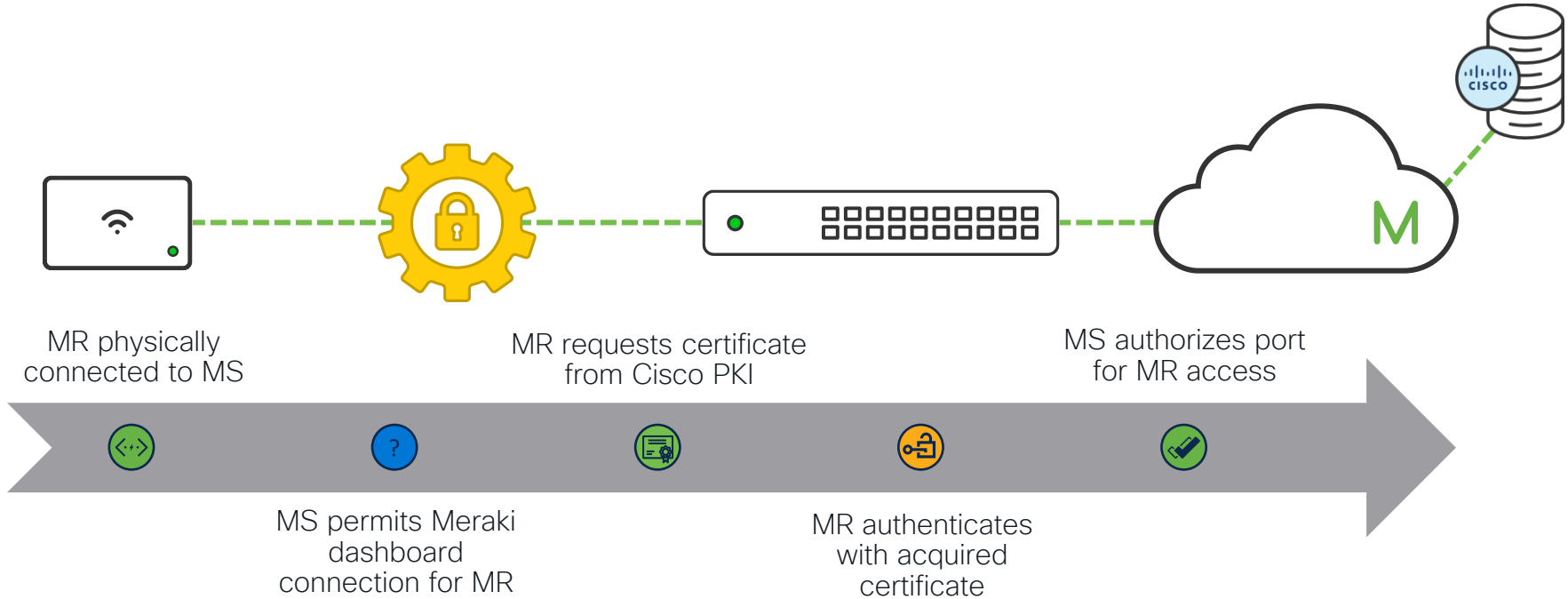
Consistent **configuration** of ports



TLS credential-based **verification** of the AP



# This is how SecurePort works



# Enforce Segmentation with Group Policy ACL



Per-session 802.1X inbound  
ACL enforcement



Named ACL orchestration



On-the-fly ACL update  
(no CoA required)

Name

Schedule

Bandwidth  unlimited [details](#)

Hostname visibility

Firewall and traffic shaping

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	<input type="text" value="Allow"/>	<input type="text" value="TCP"/>	<input type="text" value="10.10.1.4"/>	<input type="text" value="1883"/>	MQTT-1883	<input type="text" value="⚙️"/> <input type="text" value="✖"/>
2	<input type="text" value="Allow"/>	<input type="text" value="TCP"/>	<input type="text" value="10.10.1.4"/>	<input type="text" value="1884"/>	MQTT-1884	<input type="text" value="⚙️"/> <input type="text" value="✖"/>
3	<input type="text" value="Deny"/>	<input type="text" value="Any"/>	<input type="text" value="10.0.0.0/8"/>	<input type="text" value="Any"/>	Block 10-8	<input type="text" value="⚙️"/> <input type="text" value="✖"/>
4	<input type="text" value="Deny"/>	<input type="text" value="Any"/>	<input type="text" value="172.16.0.0/12"/>	<input type="text" value="Any"/>	Block 172-12	<input type="text" value="⚙️"/> <input type="text" value="✖"/>
5	<input type="text" value="Deny"/>	<input type="text" value="Any"/>	<input type="text" value="192.168.0.0/16"/>	<input type="text" value="Any"/>	Block 192-16	<input type="text" value="⚙️"/> <input type="text" value="✖"/>
	<input type="text" value="Allow"/>	<input type="text" value="Any"/>	<input type="text" value="Any"/>	<input type="text" value="Any"/>	Default rule	

[Add a firewall rule](#)



Filter-ID → Dashboard  
Group-Policy

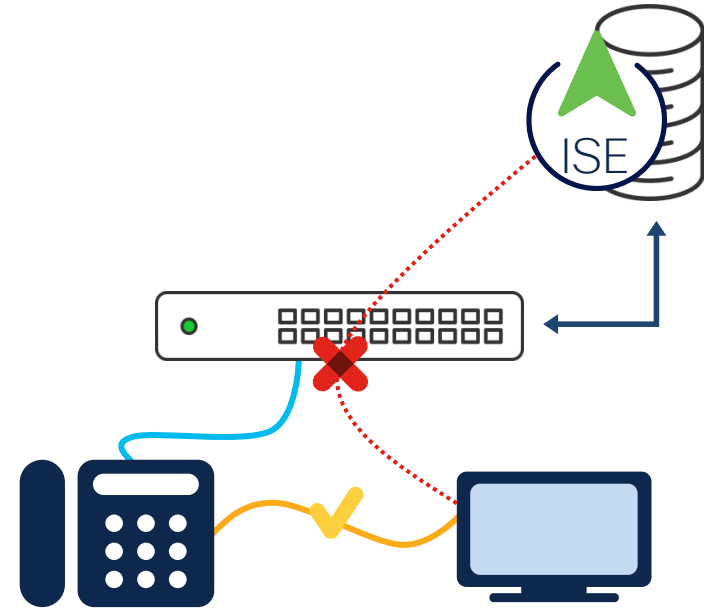


# Use Failed-Auth VLAN for quarantined access

Low impact endpoint remediation



Failed Auth VLAN Assignment  
low impact remediation into  
limited access VLAN\*



\*VLAN must be configured with limited access



# Critical VLAN keeps devices online during outages

Critical service availability when your auth server isn't reachable



Critical Voice and Data  
connectivity during RADIUS outage



# Don't compromise security for energy savings

## 802.1X Control Direction



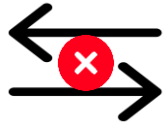
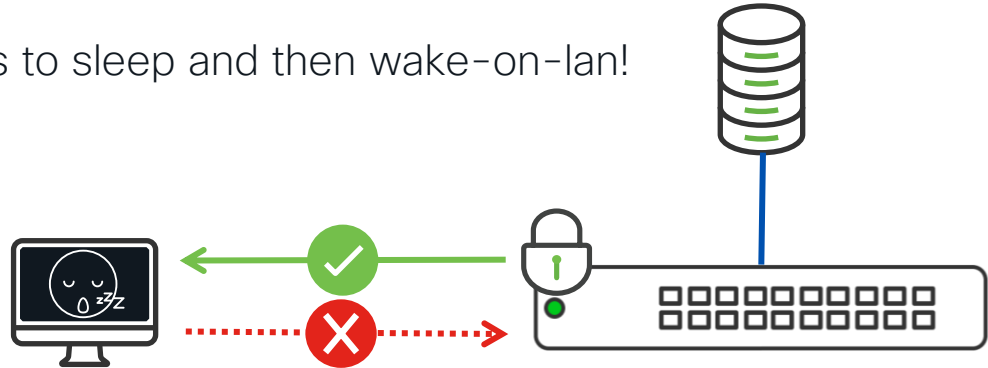
### Energy Savings

Put those cash registers to sleep and then wake-on-lan!



### Security

Robust Authentication



### Default 802.1X policy blocks both directions

New option **inbound-only** to block traffic from host prior to authorization

# Security Visibility

# MS390 Device sensor adds granular profiling

## RADIUS Accounting Enhancements



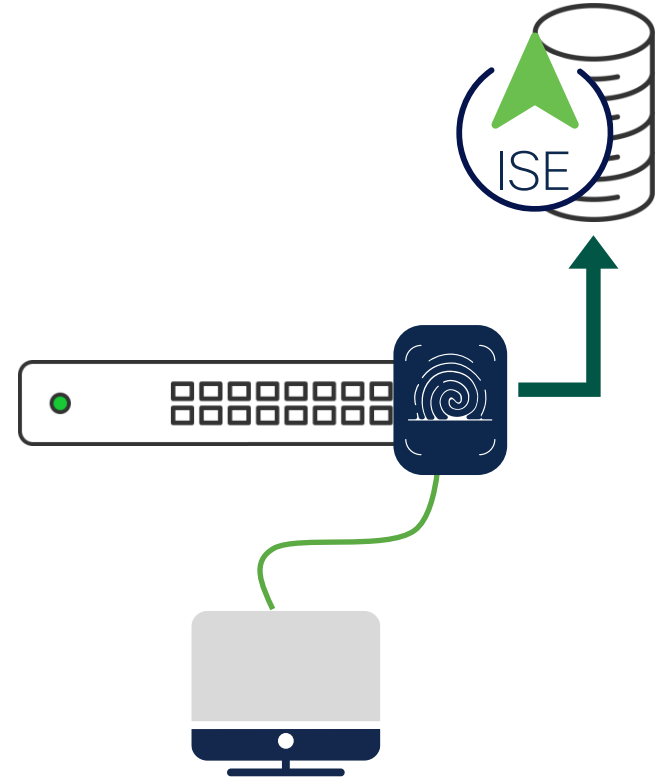
Granular profiling data made for  
Cisco Identity Services Engine



LLDP, CDP, HTTP, and DHCP  
attributes



Updates done **dynamically** over  
RADIUS accounting



# NetFlow & Encrypted Traffic Analytics

NetFlow v10 (IPFIX) with IPv4 / IPv6 / Adaptive Policy / NBAR / ETA

## AVC NetFlow\*

IPv4 and v6 records built for  
Cisco Secure Analytics

## NetFlow and ETA

on every port on every  
supported switch in the network



## Encrypted Traffic Analytics\*\*

for in-depth analysis of traffic  
without MiTM decryption

## Adaptive Policy\*\*

Export of Source Security  
Group Tags (SGTs)

NetFlow traffic reporting	Enabled: send netflow traffic statistics ▼
NetFlow collector IP	10.10.0.45
NetFlow collector port	2055
Encrypted Traffic Analytics	<input checked="" type="checkbox"/>
ETA collector port	9996

## Requires Advanced Licensing

\* should work with any standard up-to-date collector

\*\* When integrated with Cisco Secure Network and/or Cloud Analytics

# Adaptive Policy & Secure Analytics

Informed policy creation and validation



Global flow visibility and context



Group based policy and traffic flow tracking



Up to 90 Days of Historical data

## Cell Details

### TRAFFIC INFORMATION



### Traffic Volume:

Start:...

End:...

### PROTOCOLS

- ▲ ICMP (11KB) ...
- ▲ TCP (2.5GB) ...
- ▲ UDP (0.6MB) ...

### PORTS

- 22/SSH (320MB) ...
  - 80/HTTP (100MB) ...
  - ▲ 443/HTTPS (2GB) ...
  - ▲ 54180 (52MB) ...
- [View Flows](#)
- [View Offending Traffic Flows](#)

### ISE DATA

#### ISE Policy

Enabled ✓

#### SECURITY GROUP ACLS

Name: DevProdCommunication  
IP Version: IP Agnostic  
ACES: Deny IP  
permit tcp eq 80  
permit tcp eq 22

Catalyst + Meraki =



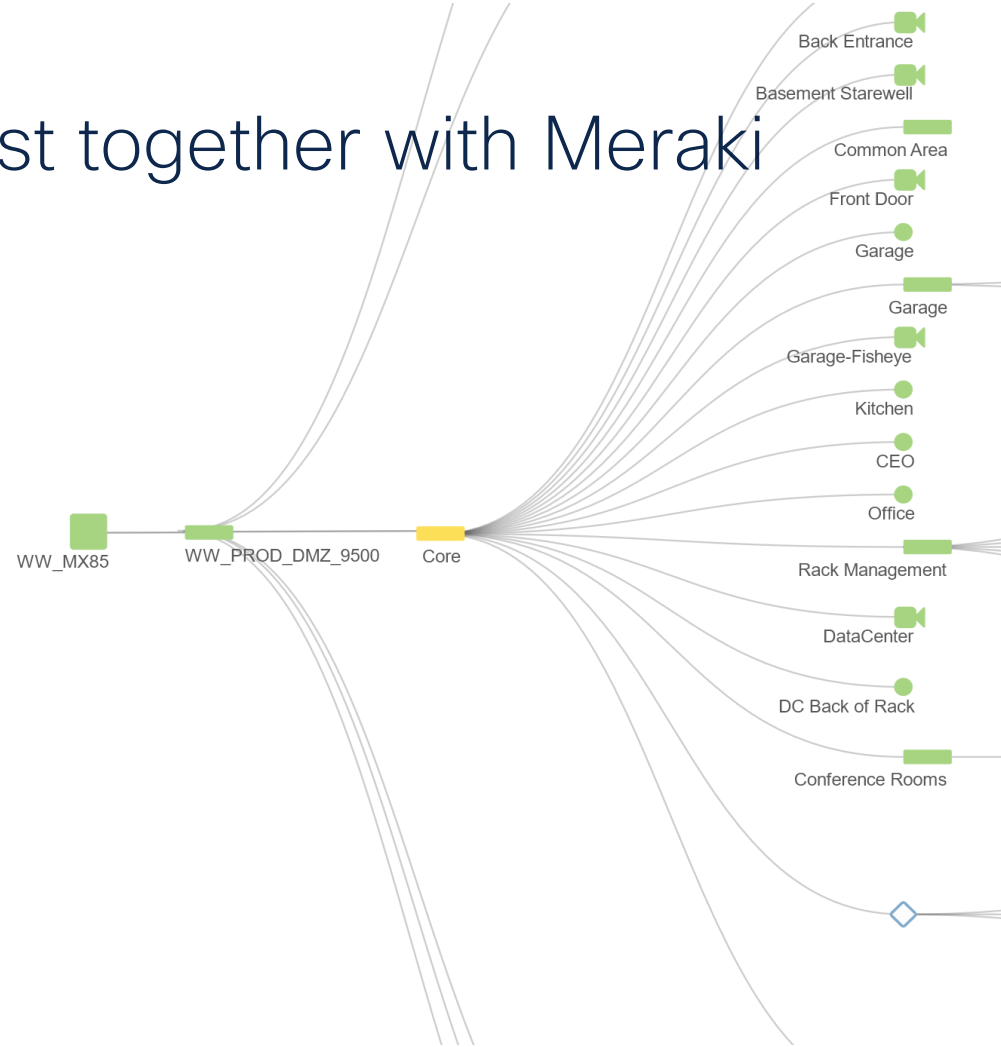
# For the first time: Catalyst together with Meraki

Cloud Monitoring for Catalyst

Single Pane-of-Glass

Monitoring and Alerts

Configuration Visibility





# This is the same intuitive Meraki monitoring experience



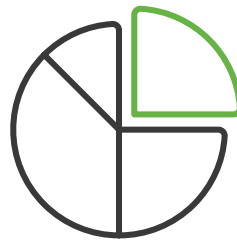
Centralized  
view of the  
entire  
network



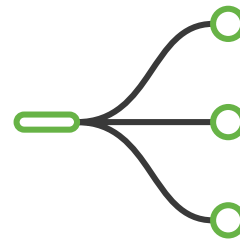
Realtime  
status of  
switch  
health



Remote  
monitoring



Layer 7  
visibility\*



Network  
topology

\*(DNA Advantage License required for full feature set)

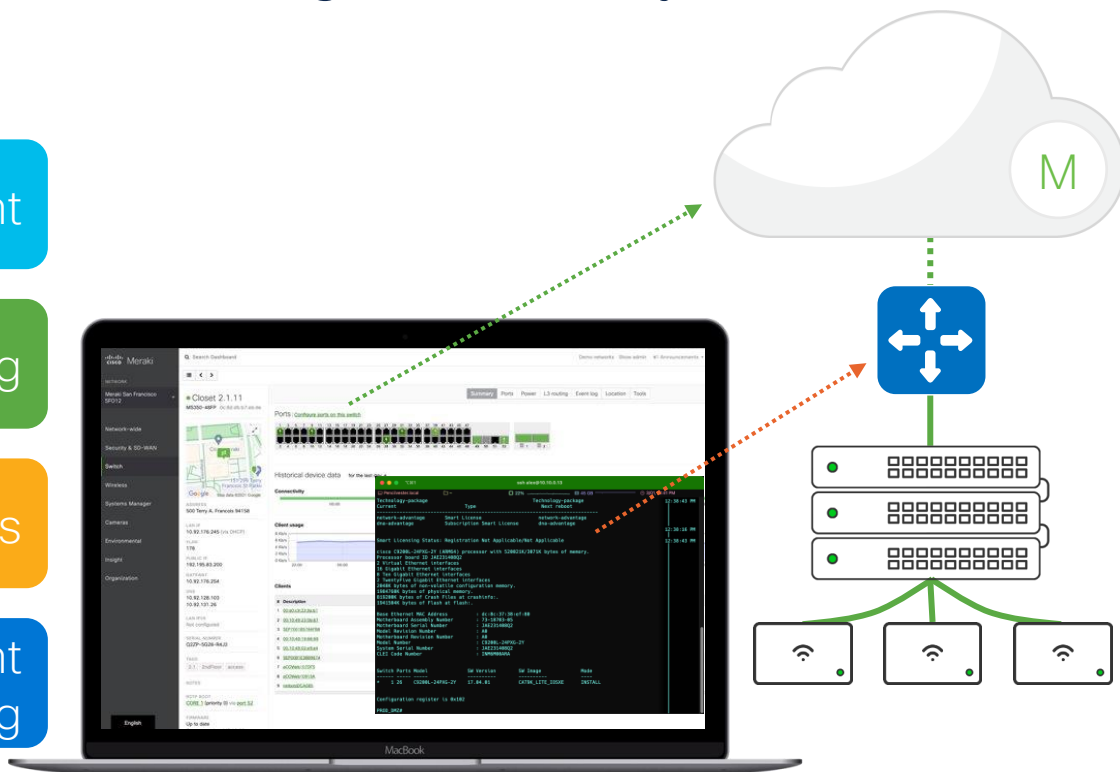
# What does Cloud Monitoring for Catalyst mean?

Flexible management

Best in class cloud monitoring

Low-overhead hybrid designs

Maintaining CLI management  
Bring your own config



# These are the currently supported platforms



## Models

Catalyst  
9200/L  
9300/L/X  
9500/X

Firmware  
IOS-XE 17.3+

Licensing  
Advantage  
Essentials\*\*

# Here are the licensing considerations

Advantage Licensing  
Client Tracking  
and Traffic Analytics



Essentials Licensing  
Client Tracking Only

Read-only configuration

Converged client view

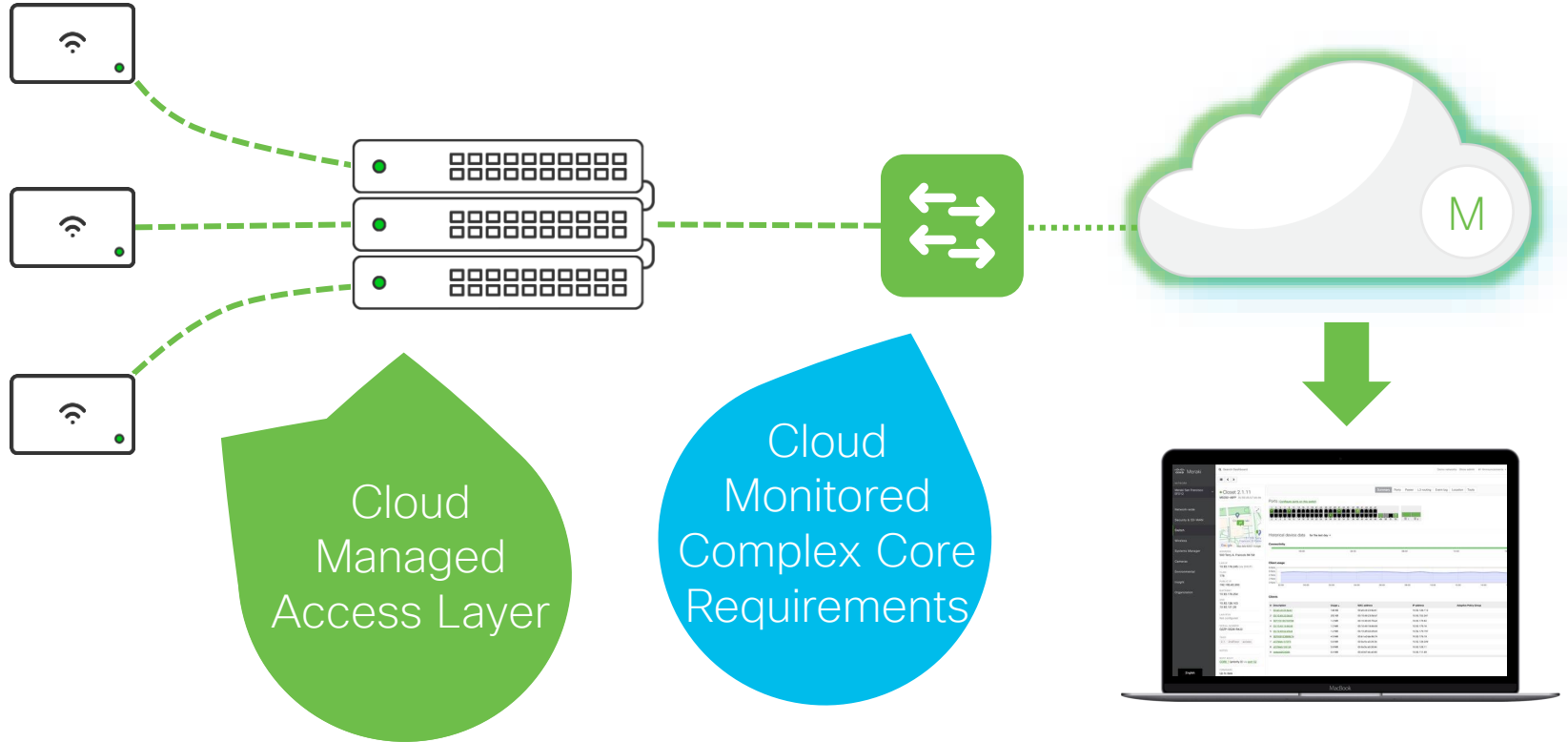
Port bandwidth usage

Alerts & live t-shoot tools

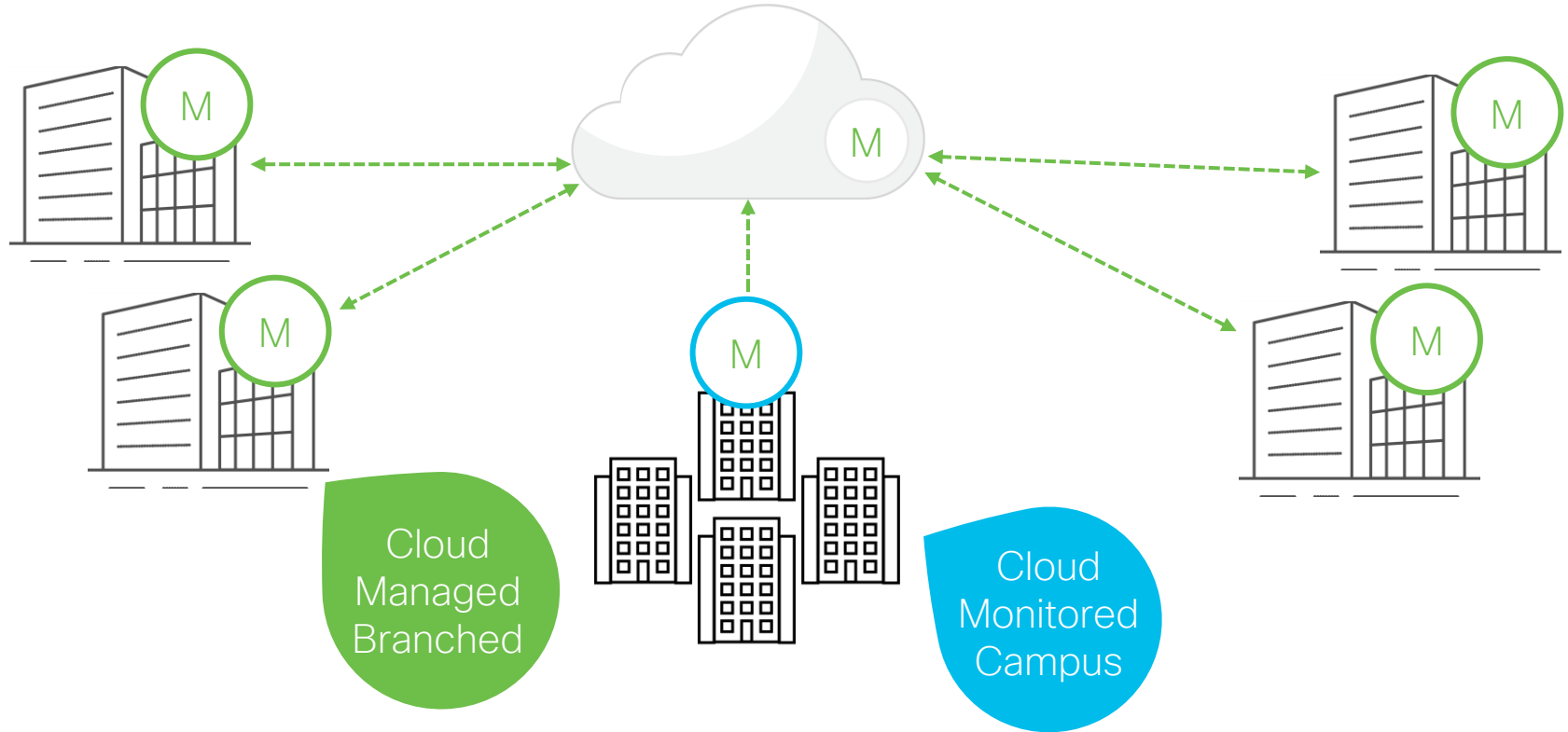
Firmware / config tracking

Unified topology view

# Cloud monitoring in the tiered use case



# Cloud monitoring in the hybrid org



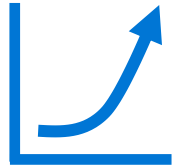
# Cloud Monitoring By The Numbers

Supported  
Switches



Catalyst  
9300

Onboarded



6K+

Average Time to  
Onboard



2:14<sub>min</sub>

Cost



\$0

Customers



700+

Geographies



NA  
60%

Average  
Feedback



4.8/5

Eligible  
Customers



100%

The background of the slide is decorated with a cluster of circles of various sizes and colors, including shades of blue, green, orange, and red, concentrated on the right side. Scattered circles in light blue and grey are also present in the upper left area.

# Demo

Cloud Monitoring for Catalyst Onboarding



A decorative graphic in the top right corner of the slide, consisting of a dense cluster of circles in various sizes and colors, including shades of blue, green, orange, and red, against a dark blue background.

# Wrap up

Please fill out your surveys!

Onboard a Catalyst today!

# Continue your education

## Cisco Meraki

Manage your IT infrastructure from one simple and secure dashboard and use it as a platform to improve your users' experience

Feb 7 | 11:30

### **IBOMER-2885**

Unprecedented Productivity with Cross-Platform Capabilities in the Meraki Dashboard

Feb 7 | 13:30

### **BRKMER-1415**

Scalable Meraki Access Switching

Feb 7 | 14:45

### **BRKMER-2514**

10 Things You Don't Know About Meraki Wireless

Feb 7 | 17:20

### **PSOMER-1789**

Navigating A More Sustainable Future: Use Technology as the Anchor

Feb 8 | 13:30

### **BRKENS-2201**

Monitor your Catalyst 9000 switch from Meraki Dashboard

Feb 8 | 13:30

### **BRKMER-1752**

Experience the Journey to IPv6-Only With Cisco Meraki

Feb 8 | 16:30

### **BRKMER-1662**

Sustainability by Cisco Meraki IOT: Small Actions, Big Impact

Feb 8 | 17:00

### **BRKOPS-2810**

Simplifying network management with Meraki API

Feb 9 | 08:45

### **BRKMER-2399**

Meraki Wireless from a Troubleshooter Perspective

Feb 9 | 10:30

### **BRKMER-2663**

Cisco Meraki: Enabling Infrastructure as Code

Feb 9 | 15:45

### **BRKMER-1003**

Cisco+ Secure Connect - Connect and Secure with Meraki

Feb 10 | 11:15

### **FINISH BRKMER-2021**

One Day in the Life of Catalyst and Access Point in the Meraki Cloud

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>





The bridge to possible

# Thank you

# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).

# Meraki Switches



# MS Access/Multi-Use/Campus Portfolio



MS120	MS125	MS210	MS225	MS250	MS350	MS355	MS390	MS410	MS425	MS450
Access					Multi-Use			Fiber Aggregation/Campus		
Up to 1GbE Ethernet					Up to 10GbE Ethernet (mGig)			10 GbE SFP+ Fiber		

Uplink Speeds	1GbE SFP	10GbE SFP+	1GbE SFP	10GbE SFP+		10GbE SFP+	40GbE QSFP+		10GbE SFP+	40GbE QSFP+	100G QSFP28 Uplinks
PoE/PoE+	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Physical Stacking	Virtual only	Virtual only	✓	✓	✓	✓	✓	✓	✓	✓	✓
Modular Power Supply			✓	✓	✓	✓	✓	✓	✓	✓	✓
Layer 3 Routing			*	*	✓	✓	✓	✓	✓	✓	✓
Redundant PSU					✓	✓	✓	✓	✓	✓	✓
Modular Fans						✓	✓	✓	✓	✓	✓
UPoE						✓	✓	✓			
Adaptive Policy								✓			
Modular Uplinks								✓			
StackPower								✓			

CISCO *Live!*

ALL IN