

Meraki SD-WAN

Presented by: LA Networks

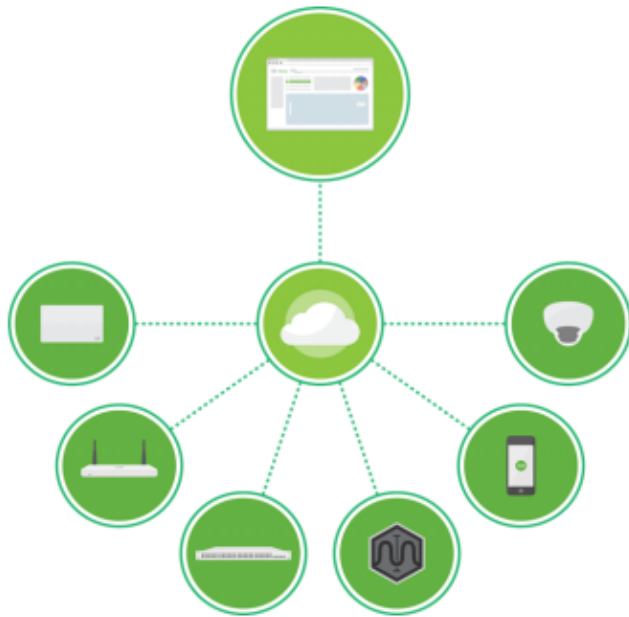


LA Networks – Who We Are

For over 20+ years LA Networks has helped their clients leverage technology by linking their business needs with IT expertise.

- Headquartered in Los Angeles – working on a national/global scale
- Our organization is over 70% engineers with a quarter being CCIEs
- 90% of our engagements are repeat customers and referrals drive 80% of our new business.

Simplifying across IT with Cloud Management



A complete cloud managed IT solution.

Wireless, switching, security, **SD-WAN**, intelligent network insights, endpoint management, and security cameras.

Integrated hardware, software, and cloud services.

550k+
Unique
customers

6M+
Devices
online

30M+
API request
per day

What is SD-WAN?

- “Software-defined WAN (SD-WAN) is a suite of features designed to allow the network to dynamically adjust to changing WAN conditions without the need for manual intervention by the network administrator.”
– Cisco Meraki

Business Drivers for SD-WAN

- User Experience
- **Out-of-Control Costs**
- **Shifting Workloads**
- Increasingly Valuable IT Investment

Under the hood of SD-WAN

Under the hood of SD-WAN: Meraki Auto-VPN



- **Meraki Auto-VPN:** The ability to configure site-to-site, Layer 3 IPsec VPN tunnels in just two clicks on the dashboard over any WAN link.
- **Automatically configured VPN parameters:** The Meraki dashboard acts as a broker between MXs in an organization, negotiating VPN routes, authentication and encryption protocols, and key exchange automatically to create hub-&-spoke or mesh VPN topologies.
- **Redundancy Built-in:** MXs with two uplink will automatically self-heal to re-negotiate VPN tunnels if a primary uplink goes down.

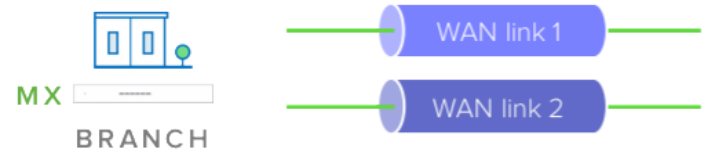
Under the hood of SD-WAN: Driven by Real-Time Performance Monitoring



- Performance metrics of all site-to-site VPN routes are probed and logged approx. every second (Latency, Jitter, Loss, MOS)

Under the hood of SD-WAN: Application-Aware Intelligent Path Control

- Dual Active VPN



- Policy-Based Routing (PbR)



- Dynamic Path Selection



Simply Express Intent

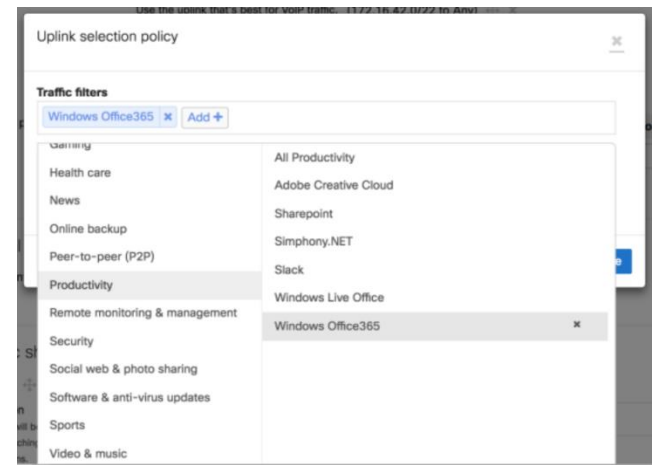
1. Define acceptable performance thresholds

Custom performance classes

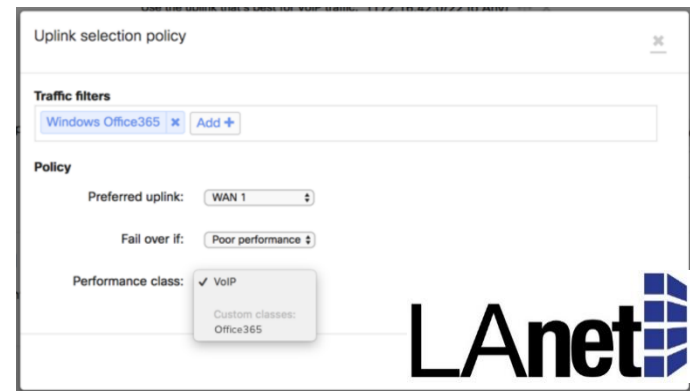
Name	Maximum latency (ms)	Maximum jitter (ms)	Maximum loss (%)	Actions
Office365	10	10	10	X

[Create a new custom performance class...](#)

2. Select from built-in Layer 7 categories and applications



3. Choose preferred uplink and when fail over should occur.



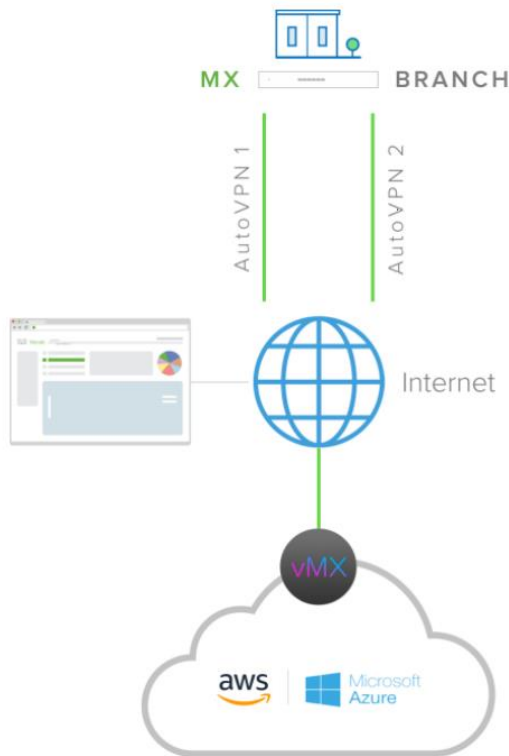
Monitor SD-WAN Traffic Flow Decisions

- Track live flow decisions for uplinks and VPN peers
- Understand context & reason for decision

Source	Destination	Uplink decision	Reason	Policy
172.16.55.10:36684	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"
172.16.55.7:35420	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"
172.16.55.9:54052	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"
172.16.55.10:36740	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"
172.16.55.7:35462	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"
172.16.55.8:45578	10.0.0.6:80	WAN 2	Performance-based	Prefer WAN 1. Fail over if poor performance for "Cloud Application"

But wait it get's BETTER!!!

Extension to Public Cloud Services



- Extend MX Deployments to IT services located in AWS or Microsoft Azure with site-to-site auto VPN to a virtual MX(vMX)
- Leverage SD-WAN on vMX the same way as a physical MX for optimal path selection to IT services hosted in AWS or Azure.
- Up to 500Mbps VPN throughput



Meraki Insight

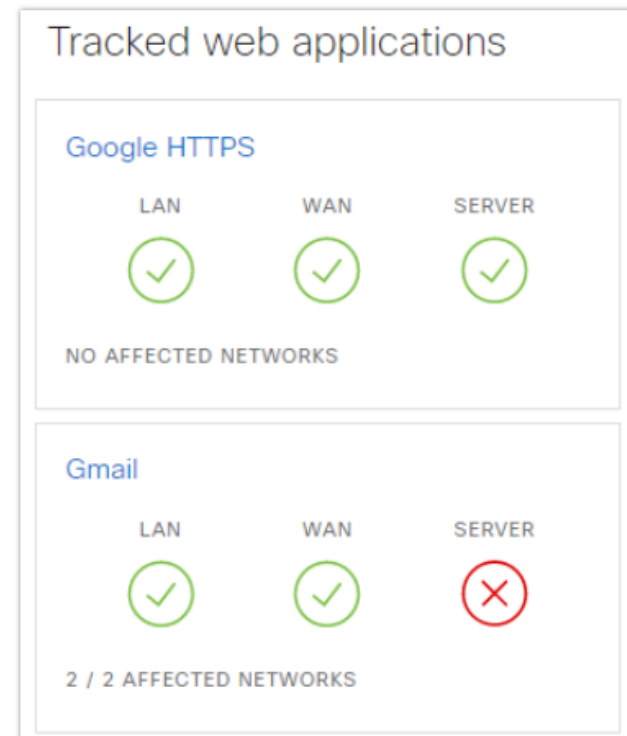
Optimize User Experience, Accelerate IT

MI Overview

- Meraki Insight is designed provide an easy way to monitor the performance of Web Applications and WAN Links on the network.
- Easily identify if any issues are likely being caused by the network or an application.

MI Web App Health

- Utilizing MI an MX can be configured to monitor and track all traffic associated with specific Web Applications.
- A Performance Indicator display created for each application being monitored and provides a quick reference to the quality of the user experience relative to a specific Web Application, based on thresholds defined by an Admin.



MI WAN Health

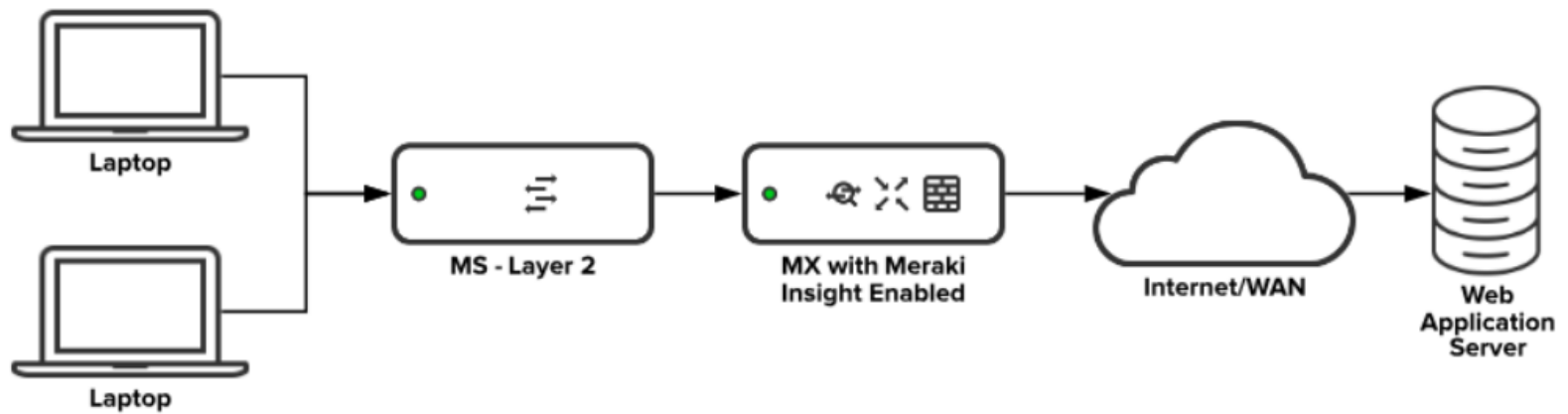
- The WAN Health feature is designed to monitor WAN transports.
- Helps to proactively troubleshoot service provider issues

WAN Health for the last 2 hours ▾

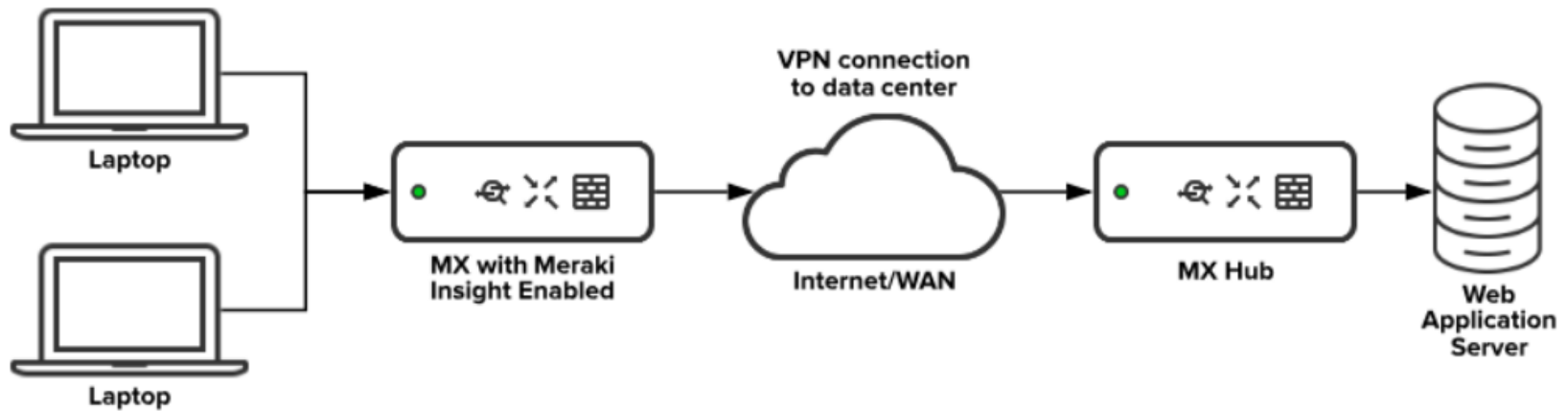
[WAN Health documentation](#)

GOOD		DOWN		POOR PERFORMANCE		HIGH USAGE										
● 12		● 0		● 0		● 0										
<input type="text" value="(status:good OR status:poorPerformance OR status:highUsage OR status:down)"/>																
Uplink Status	Network Name	Availability	Jitter	ISP	Uplink Type	Loss	Notes	Average Throughput	Total Usage	% Capacity	Average Latency	Affected Apps	Signal (dBm)	Ping Destination	Reference Signal Received Power (RSRP)	Network Tags
● Active	Datacenter-NA - appliance	<div style="width: 100%;"></div>	180 μs	sonic.net	WAN 1	0.00%		+ 174.12 kb/s, ↑ 187.52 kb/s	+ 152.91 MB, ↑ 164.66 MB		4.0 ms		-	8.8.8.8 ▾		Datacenter
● Ready	Datacenter-NA - appliance	<div style="width: 100%;"></div>	170 μs	sonic.net	WAN 2	0.00%		+ 6.31 kb/s, ↑ 4.94 kb/s	+ 5.63 MB, ↑ 4.41 MB		3.9 ms		-	8.8.8.8 ▾		Datacenter
● Active	Datacenter-SA	<div style="width: 100%;"></div>	240 μs	monkeybrains.net	WAN 1	0.00%		+ 20.42 kb/s, ↑ 16.20 kb/s	+ 17.92 MB, ↑ 14.21 MB		4.4 ms		-	8.8.8.8 ▾		Datacenter
● Active	London - appliance	<div style="width: 100%;"></div>	170 μs	sonic.net	WAN 1	0.00%		+ 38.24 kb/s, ↑ 125.64 kb/s	+ 34.55 MB, ↑ 113.03 MB	+ 0.36%, ↑ 5.99%	3.8 ms		-	8.8.8.8 ▾		Branch
● Active	London - appliance	<div style="width: 100%;"></div>	1.0 ms	sonic.net	WAN 2	31.53%		+ 168.49 kb/s, ↑ 100.18 kb/s	+ 148.80 MB, ↑ 88.82 MB	+ 3.21%, ↑ 1.91%	90 ms		-	8.8.8.8 ▾		Branch

MI: Scenario 1: SaaS-based (HTTP/S) Applications



MI: Scenario 2: Data Center (HTTP/S) Applications



Meraki SD-WAN Licensing

Enterprise	Advanced Security	Secure SD-WAN Plus
-Essential SD-WAN -Secure connectivity & basic security	-All enterprise features -Fully featured unified threat management	-All advanced security features -Advanced analytics with machine learning powered by Meraki Insight -Smart SaaS QoE -Tag-Based Segmentation

- Advance Security & Secure SD-WAN Plus licenses and features are only available on the MX devices, not on Z-Series devices, or any other Meraki series of devices.
- License Options: 1, 3, 5, 7, and 10 Years

How to choose a Cisco SD-WAN Solution

Consider Cisco SD-WAN Powered by Meraki if...

- Needs are fairly simple
- You have no more than two transports + LTE
- You are leveraging Meraki
- You are looking for simple management, orchestration and automation

Consider Cisco SD-WAN Powered by Viptela if...

- You have a more complex use case
- You have more than two transports
- You are already leveraging Cisco routers
- You are looking for advanced routing.
- You are looking for secure isolation of enterprise assets using segmentation.
- You are looking for optimizing connectivity to multicloud or SaaS applications

Differences between SD-WAN powered by Meraki vs Viptela

SD-WAN Core Feature (Meraki and Viptela)

Overlay:

- Basic 2-link overlay with LTE backup
- Links: Ethernet, LTE
- Hub & Spoke, full mesh and partial mesh topology
- Cloud Management
- Basic BGP
- Platforms for on-premises and cloud deployments

Cloud:

- DIA plus security
- Virtual platforms for AWS and Azure

Security:

- Enterprise firewall
- IPS, URL Filtering, and cloud security
- Talos powered threat intelligence

SD-WAN Premium Features (Viptela only)

Overlay:

- Overlay with 3+ links and LTE active-active
- Links: Ethernet, LTE active plus T1, E1 and DSL
- Hub & Spoke, full mesh, partial mesh within multiple VPNS
- Cloud managed or on-premise managed
- Full routing support BGP, OSPF, VRRP, IPv6, and multicast
- Platforms for on-premise, cloud and virtual deployments
- TCP optimization, WAN acceleration, and WAN optimization

Cloud:

- DIA plus security plus real-time SaaS optimizations
- Virtual platforms for AWS, Azure, and GCP
- Map VPCs and VNETs to SD-WAN segments

Security:

- Enterprise firewall
- IPS, URL Filtering, and cloud security
- Talos powered threat intelligence
- Segmentation for isolation of business partners, lines of business, and M&A

Demo