

Cisco Meraki > SD-WAN

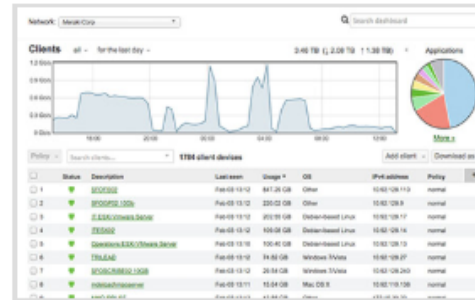
Software-defined WAN is a new approach to network connectivity that lowers operational costs and improves resource usage for multi-site deployments, allowing network administrators to use bandwidth more efficiently and ensure the highest possible level of performance for critical applications without sacrificing security or data privacy.



Transport Independence

Easy-to-configure IPsec overlay using Meraki Auto VPN

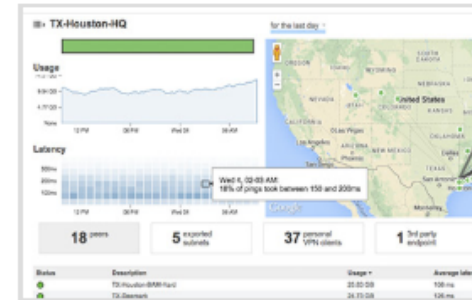
Traffic distribution over multiple pathways (Internet, cellular, MPLS) with built-in load balancing and automatic failover capabilities



Application Optimization

Centralized network visibility and control

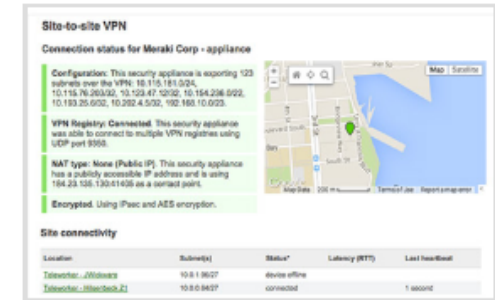
QoS and bandwidth management with Meraki traffic shaping



Intelligent Path Control

Policy-based routing: Traffic path assigned based on source, destination, or application

Dynamic path selection: Traffic path chosen per-application based on loss, latency, and jitter



Secure Connectivity

Intuitive, scalable VPN solution to connect remote sites with ease (Auto VPN)

AES encryption to ensure data privacy

Cisco Meraki > SD-WAN

SD-WAN Features:

Dual-Active VPN uplinks

To support dual WAN uplinks and automatic VPN failover, the MX also has the ability to build multiple VPN tunnels that are active simultaneously on both uplinks, whether they are Internet or MPLS connections. Traffic can then be load-balanced across these tunnels to make optimal use of available bandwidth.

Policy-Based Routing (PbR)

PbR functionality allows administrators to assign traffic to a particular VPN path based on criteria such as traffic protocol, source, destination, or application.

Dynamic path selection

Dynamic path selection allows administrators to set performance thresholds for different types of traffic, in order to ensure that critical applications and data transfers always use the best path based on the loss, latency, and jitter over the available VPN tunnels.



Return on Investment (ROI)

Projected 3 year cost with legacy WAN deployment

Connectivity	\$2,016,000
T1 × 45 at branches (1.544Mbps each)	\$582,000/yr
Broadband × 2 at HQ & DR (45Mbps each)	\$90,000/yr
Content Management	\$153,000
Content filtering software	\$51,000/yr
Maintenance	\$24,750
Hardware Security Appliance	\$8,250/yr
3 year Total Cost of Ownership (TCO)	\$2,193,750

Projected 3 year cost with Meraki (including rip & replace)

Connectivity	\$673,495
Broadband × 38 at HQ & branches (50Mbps each)	\$212,040/yr
WAN Management vendor (one time installation costs)	\$37,375
Meraki Hardware & Licensing	\$599,141
MX, MS, and MR × 41 at branches	\$382,896
MX, MS, and MR licensing	\$72,081/yr
Content Management	Included
Wireless Installation	\$62,257
26 branch offices wired for MR	\$62,257
3 year Total Cost of Ownership (TCO)	\$1,334,893

CISCO MERAKI

The Cisco Meraki MR53 sets the new standard in wireless. Designed specifically for high density and next generation deployments, it's the world's fastest cloud-managed wireless access point.

802.11ac Wave 2 Performance with Dedicated Air Marshal Radio

➤ PERFORMANCE

Up to 5 times faster WiFi 100% compatibility.

➤ SOFTWARE

So Smart: Software that optimizes and secures your wireless network

➤ SEAMLESS INTEGRATION

A True Fit: The MR53 integrates seamlessly into existing wireless environments



The Cisco Meraki MR53

802.11ac Wave 2 Performance with Dedicated Air Marshal Radio

PERFORMANCE

Up to 5 times faster WiFi 100% compatibility

Using wider channel bandwidths, more efficient transmission technologies, and less crowded channels at 5 GHz help the MR53 achieve speeds up to 2.5 Gbps, while also providing administrators complete visibility and control.

➤ CHANNEL BANDWIDTH

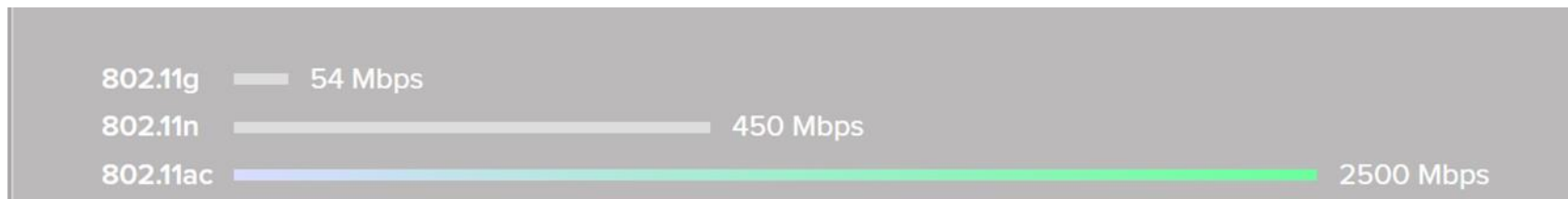
The MR53 increases the channel bandwidth — the size of the pipe used to transmit data — up to 160 MHz. These wider channels enable faster transmissions and increase aggregate performance in dense multi-client environments.

➤ MODULATION

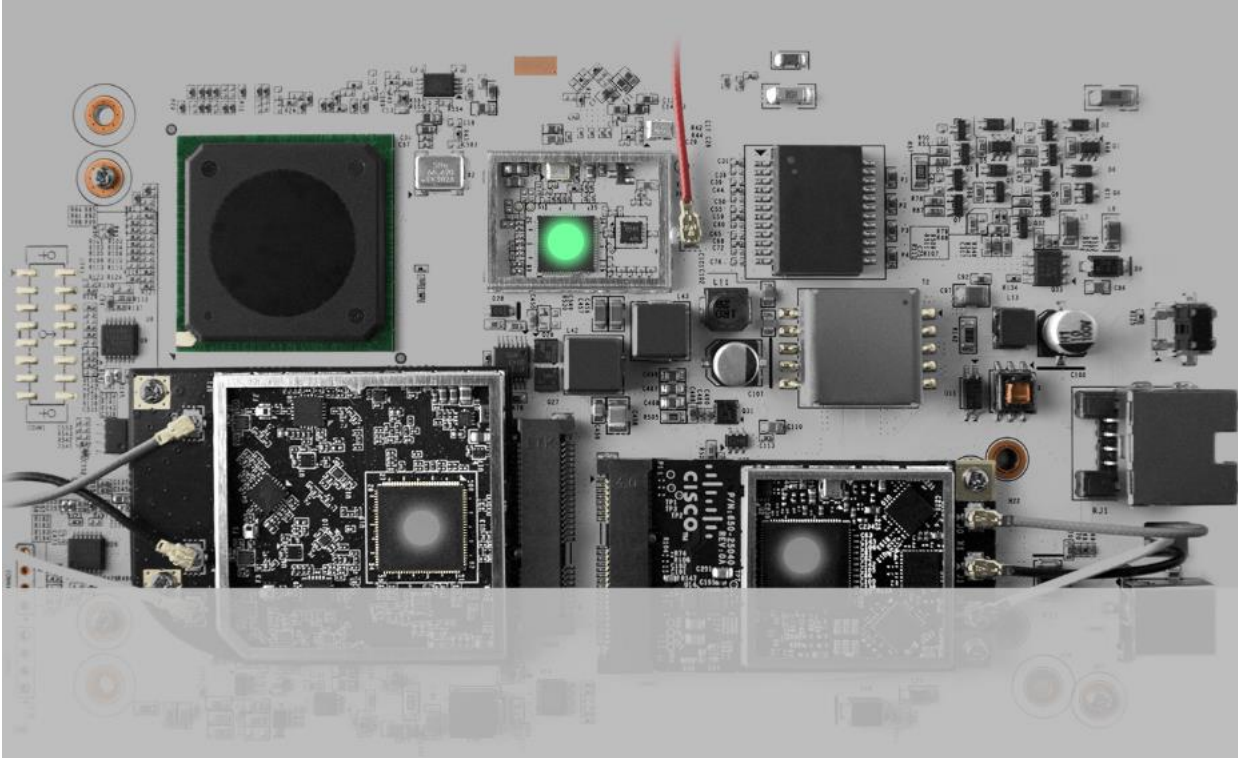
With enhanced modulation, the MR53 encodes data more efficiently. By sending more data over the air in less time, the MR53 can support more clients at once, and speeds uploads and downloads of large files and video.

➤ SPECTRUM

The MR53's 802.11ac radio operates exclusively in the 5 GHz band, a less-crowded spectrum enabling wider channels with less interference. A second radio is dedicated to supporting legacy 802.11b/g/n clients at 2.4 GHz.



The Cisco Meraki MR53



Dedicated Security

The MR53 includes the industry's first cloud-managed third radio dedicated to optimizing the RF environment and securing the airwaves. This third radio is dual-band, providing spectrum intelligence across 2.4 GHz and 5 GHz frequencies and full-time security protection from network vulnerabilities.

DUAL-BAND >
Dedicated security radio

5 GHz
802.11a/n/ac

2.4 GHz
802.11b/g/n



The Cisco Meraki MR53

Software

So Smart

Software that optimizes and secures your wireless network

- Auto RF
- Air Marshal
- Traffic Shaping

Auto RF

Auto RF aggregates network-wide spectrum analytics through the Meraki cloud platform to automatically determine access point power levels and channel assignments. The full-time scanning capabilities of the dedicated third radio allow the MR53 to dynamically adjust and optimize the RF environment for connecting clients.



The Cisco Meraki MR53

The screenshot displays the Cisco Meraki Air Marshal dashboard for the 'Engineering - MR' network. The interface includes a sidebar with navigation options like Monitor, Overview, Map, Access points, Clients, Traffic analytics, Packet capture, Event log, Air Marshal (selected), Splash logins, RF Spectrum, Login attempts, Presence heatmap, Summary report, PCI report, Configure, Organization, and Help.

Air Marshal Configuration:

- Scanning APs:** 6 APs with separate scanning radios, 2 APs in dedicated Air Marshal mode, 8 APs scanning total.
- LAN containment:** Don't contain APs seen on the LAN.
- Keyword containment:** One keyword per line.
- Off-channel scans:** Opportunistic and mandatory scans.
- Mandatory scan schedule:** 4:00 AM, S M T W T F S.

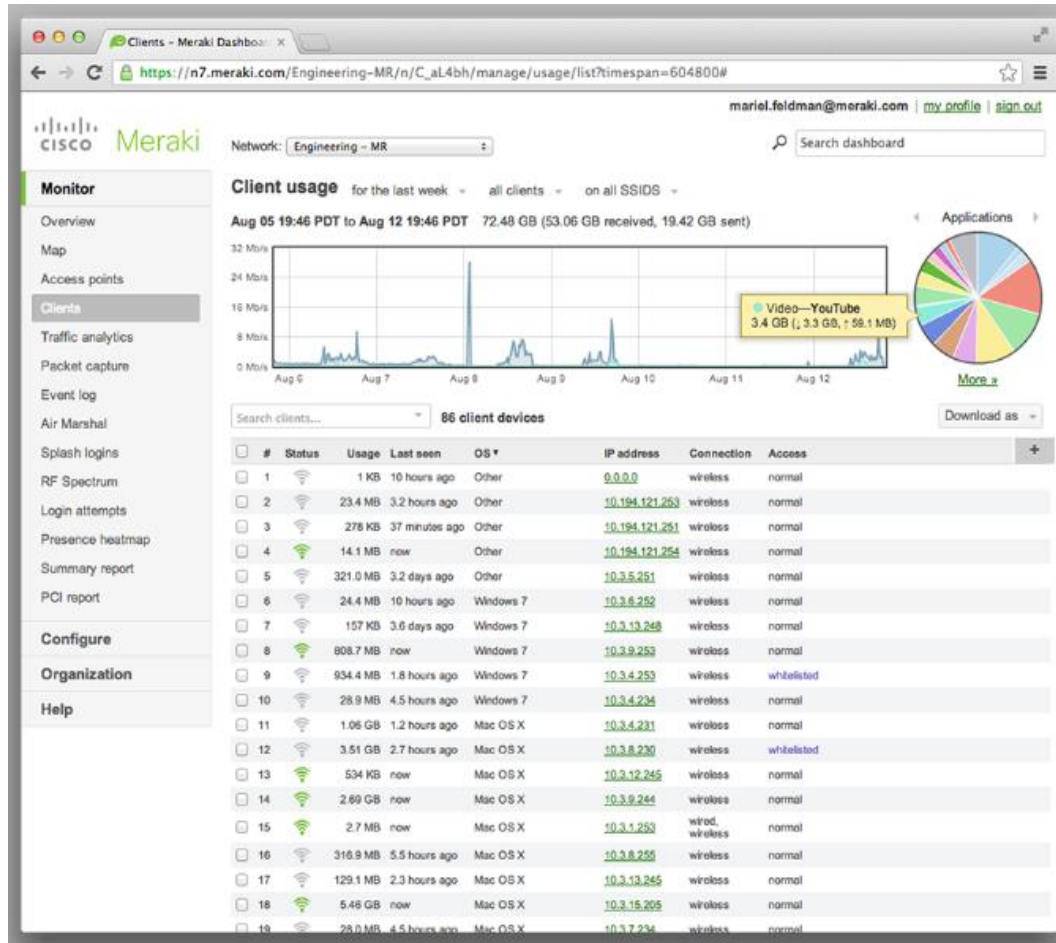
41 Rogue SSIDs | 120 Other SSIDs | 25 Spoofs | 0 Malicious broadcasts | 307 Packet floods

Containment	SSID	Last seen	First seen	# APs	Rogue because
uncontained	33 hidden SSIDs	Aug 12 19:48	Jun 4 23:26	33	Seen on LAN
uncontained	foooo	Aug 6 01:06	Aug 5 23:41	1	Seen on LAN
uncontained	ZaBu - S3	Aug 6 10:36	Aug 6 09:40	1	Seen on LAN
uncontained	MerakiWork WiFi	Aug 6 13:03	Jul 30 14:17	2	Seen on LAN
uncontained	Air-A56208	Aug 6 14:27	Aug 6 14:21	1	Seen on LAN
uncontained	PereiraODoll	Aug 7 08:53	Aug 7 07:44	9	Seen on LAN
uncontained	Meraki-Engineering-PSK-Topaz	Aug 7 12:42	Jul 17 15:27	5	Seen on LAN
uncontained	POD-Guest	Aug 7 16:36	Aug 7 07:44	10	Seen on LAN
uncontained	A3	Aug 9 08:28	Aug 9 08:24	1	Seen on LAN
uncontained	ManagedDevice	Aug 9 08:33	Aug 9 07:59	2	Seen on LAN

Air Marshal

The MR53 features a dedicated scanning and rogue AP containment system without interrupting client traffic. Its built in wireless intrusion prevention system (WIPS) scans the wireless environment for vulnerabilities and neutralizes threats such as nearby rogue APs.

The Cisco Meraki MR53



Traffic Shaping

Prioritize mission critical applications like VoIP and throttle or block recreational applications such as YouTube or P2P file sharing, even at faster 802.11ac speeds. The MR53 includes an integrated Layer 7 packet inspection, classification, and control engine, enabling you to set QoS policies based on traffic type.

The Cisco Meraki MR53



A True Fit

The MR53 integrates seamlessly into existing wireless environments

Upgrading a wireless network has never been easier. The MR53 supports existing 11a/b/g/n clients to make migration simple. Deploy the MR53 to add 802.11ac capacity into an existing WiFi network, and manage everything from the dashboard.