MR Cloud Managed Wireless Access Points

Overview

The Meraki MR series is the world's first enterprise-grade line of cloud-managed WLAN access points. Designed for challenging enterprise environments, the MR access points use advanced 802.11ac and 802.11n technologies including MIMO, beam forming and channel bonding to deliver the throughput and reliable coverage required by demanding business applications.

Centralized Cloud Management

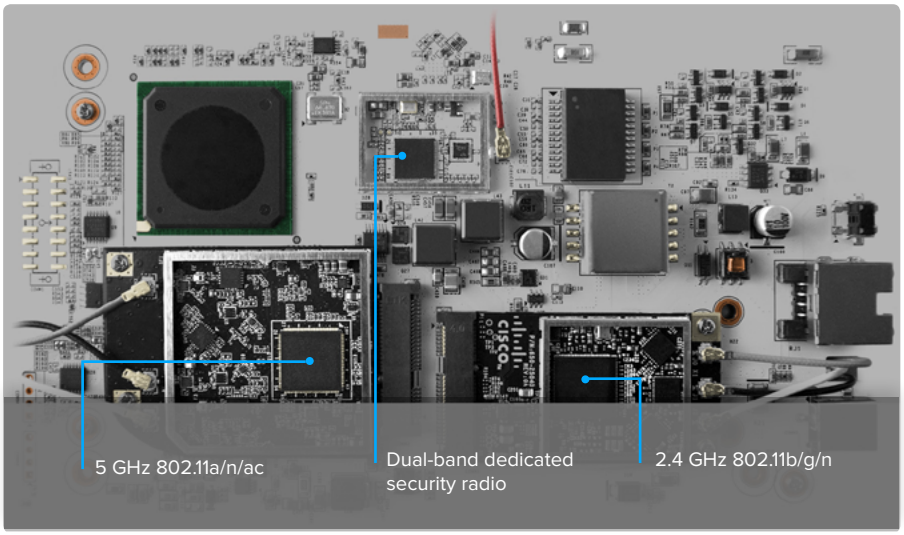
The award-winning Cisco Meraki cloud management architecture provides powerful and intuitive centralized management, while eliminating the cost and complexity of traditional on-site wireless controllers. Seamlessly manage campus-wide WiFi deployments and distributed multi-site networks with zero-touch access point provisioning, network-wide visibility and control, cloud-based RF optimization, seamless firmware updates and more. With an intuitive browser-based user interface, Meraki WLANs configure in minutes without training or dedicated staff. Adding new sites to a network takes minutes, not hours or days, and there's no need to train additional staff to monitor or manage the remote networks. Meraki devices self-provision, enabling large campus and multi-site deployments without on-site IT.

Class-Leading Enterprise Features

The MR series comes equipped with industry-leading features that make them ideal for demanding enterprise deployments:

- Self-configuring, plug-and-play deployment
- 802.11ac and 802.11n MIMO with up to three spatial streams, built for voice and video
- Integrated enterprise security and guest access
- Dedicated radio for security and RF optimization with integrated spectrum analysis (indoor models)
- Integrated intrusion detection and prevention system (WIDS/WIPS)
- Self-learning application-aware traffic analytics engine
- Flexible group policy engine for creating and applying application-aware policies by network, device-type, and end-user
- Self-healing, zero-configuration mesh
- Role-based administration and automatic, scheduled firmware upgrades delivered over the web
- E-mail and text message alerts upon power loss, downtime, or configuration changes

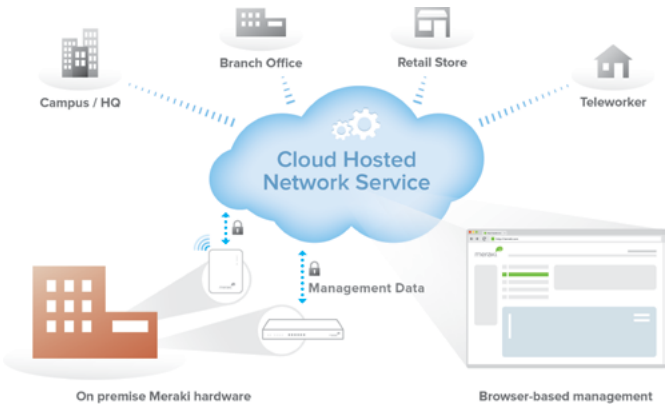
Inside the Meraki MR
Features vary by model



Rapid Deployment and Scalability

Built from the ground up for multi-site networks, Meraki access points have revolutionized distributed branch wireless networking. Zero-touch deployments, multi-site visibility and control, and automated alerts make deploying, securing, and centrally managing branch networks a breeze.

The Meraki cloud-managed architecture enables plug and play branch deployments and provides centralized visibility and control across any number of distributed locations. Since Meraki MR series APs are managed entirely through the Meraki web-based dashboard, configuration and diagnostics can be performed remotely just as easily as they can be performed on-site, eliminating costly field visits. Each device downloads its configuration via Meraki's cloud, applying your network and security policies automatically so you don't have to provision them on-site.



Meraki Cloud Management Architecture

High Performance RF Design

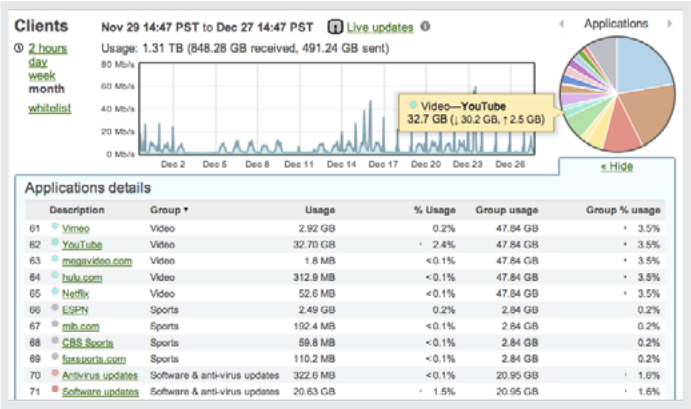
Every Meraki access point continuously and automatically monitors its surroundings to maximize WiFi performance. By measuring channel utilization, signal strength, throughput, signals from non-Meraki APs, and non-WiFi interference, Meraki APs automatically optimize WiFi performance of individual APs and maximize system-wide performance.

Meraki APs have been deployed and proven in the most demanding environments, supporting more than 100 users per AP and collectively serving hundreds of Megabits per second of user traffic to thousands of devices. By eliminating traditional hardware controllers, Meraki also eliminates the performance bottleneck that often chokes high-density wireless deployments.

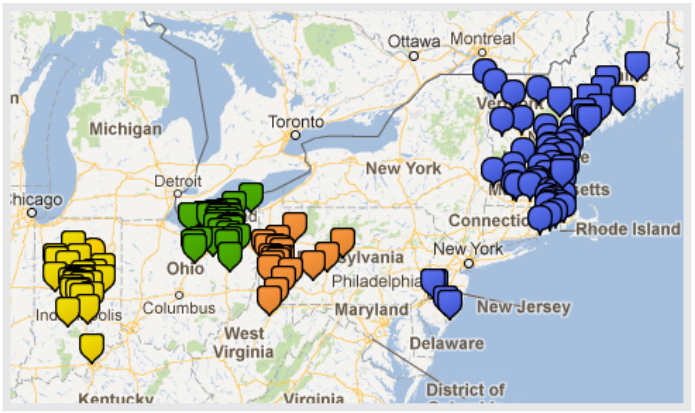
By measuring utilization from neighboring APs, detecting WiFi signals from non-Meraki APs, and identifying non-WiFi interference, Meraki APs continuously stay on top of changing and challenging conditions. Tools such as real-time spectrum analysis and live channel utilization deliver immediate information on the RF environment at any part of the network. Even in dynamic environments, Meraki networks automatically detect and adapt to interference from non-WiFi sources.

Real-time and historical metrics ensure maximum system-wide performance. Wireless channels, AP output power, and client connection settings are automatically adapted to changing performance and interference conditions, eliminating the need for tedious manual adjustment of dozens of independent parameters.

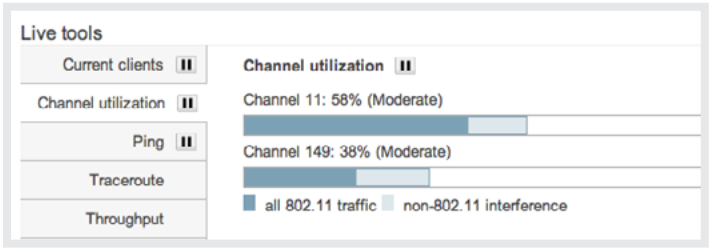
Mesh networking, included in every Meraki AP, extends coverage to hard to wire areas and creates a self-healing network that is resilient to cable and switch failures, continuing to operate despite failures or configuration changes in the rest of the network, without the need for manual configuration or optimization.



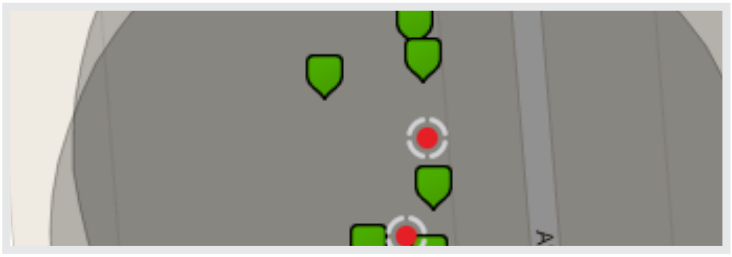
User Analytics and Traffic Shaping



Multi-Site Management



Live Troubleshooting Tools



Air Marshal: Real-Time Wireless Intrusion Prevention System

Enterprise Security and a Dedicated Radio

The MR series comes equipped with complete out-of-the-box enterprise class security. Segment wireless users, applications, and devices; secure your network from attacks and enforce the right policies for each class of users. A built-in stateful policy firewall, 802.1X/RADIUS support, and native Active Directory integration deliver fine-grained access control, while a guest access firewall provides secure, Internet-only guest WiFi in just one click. Integrated network access control (NAC) provides end-user anti-virus scanning for accurate client device posture asessment to protect your wired and wireless network against virus infections.

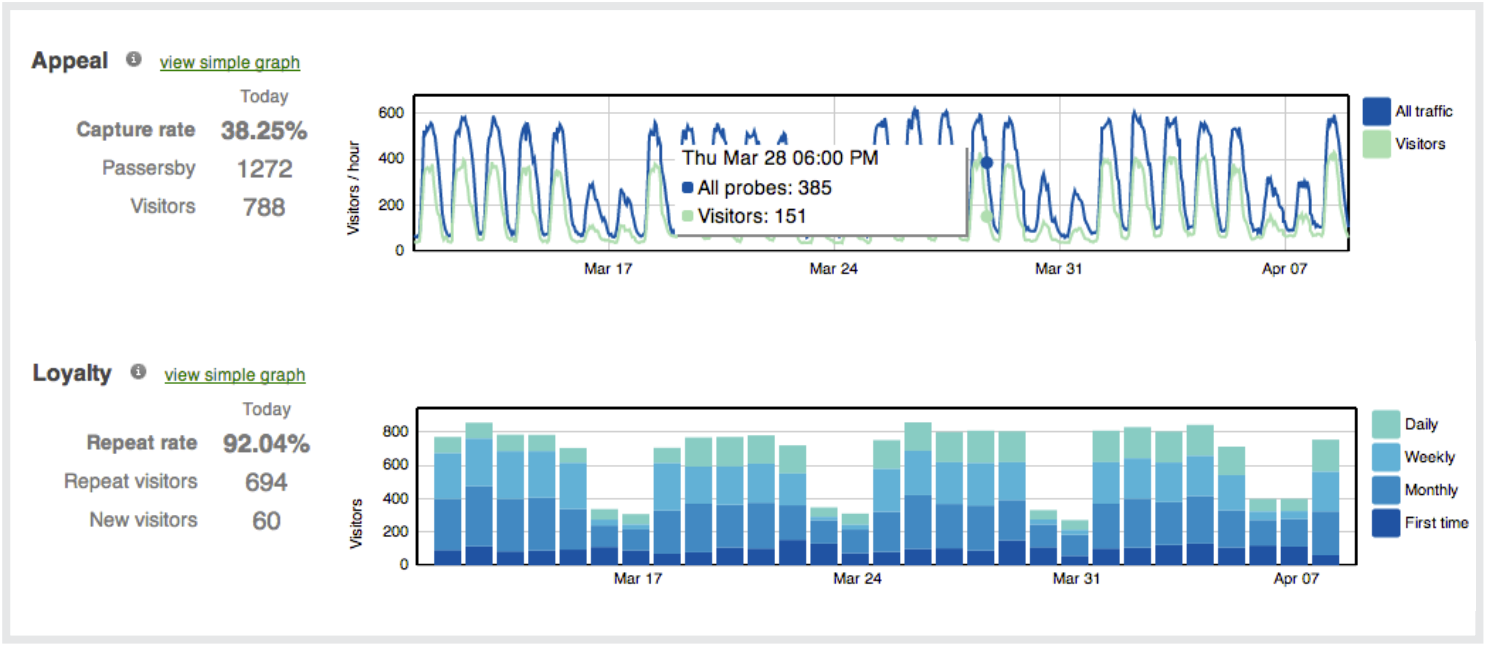
Indoor APs feature a radio dedicated to full-time scanning, rogue AP containment, and automatic RF optimization. With Air Marshal, it is possible to set up a real-time wireless intrusion detection and prevention system (WIDS/WIPS) with user-defined threat remediation policies and intrusion alarms, enabling secure wireless environments without complex setup or systems integration. Auto RF eliminates the need for manual RF configuration by scanning the environment for utilization, interference, and other metrics, and computing the optimal channel and power settings for every AP in the network. Meraki WLANs are fully HIPAA and PCI compliant.

Built-in Guest Access

Meraki cloud management provides the ability to customize and integrate splash pages onto each Meraki MR access point, with options for click-through or sign-on splash using your own RADIUS server or the Meraki cloud-based RADIUS user database. The Meraki MR series features a complete array of built-in captive portal tools, including a guest ambassador portal for new-user sign-on, splash sign-in tracking, application blocking and traffic shaping, free and paid tiers of access, integrated credit-card processing and prepaid codes generation, and splash by-pass for corporate-issued or recognized devices.

Presence

The Meraki MR series tracks probing MAC addresses from associated and non-associated clients. This data is exported in real time from the access points to Meraki's cloud for analytics; information is then calculated and then presented in the Meraki dashboard to display metrics such as user dwell-time, repeat visits and capture rate (people passing by vs. coming inside a site). This information can be used by retailers, hospitality, and enterprise customers to understand foot traffic and visitor behavior across sites, and can facilitate an optimization of opening hours, marketing initatives, and staffing policies.

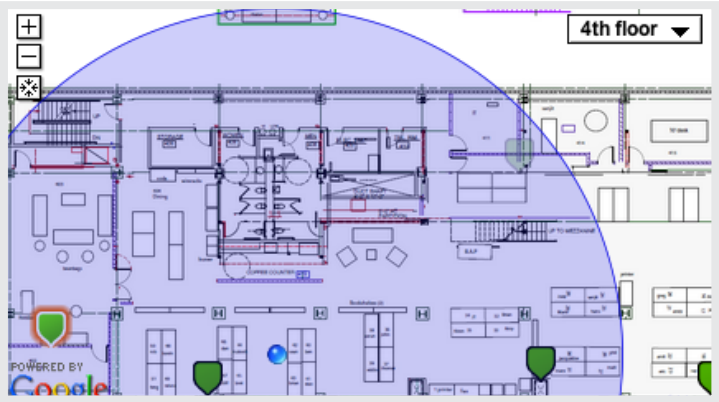


Presence Analytics (for non-associated clients)

BYOD-ready, Out of the Box

User-owned devices have exploded onto networks everywhere, with new iPads, Androids, and smartphones connecting every day. Meraki MR series APs feature built-in support for BYOD and make it easier than ever to securely track and support user-owned iPads, tablets, smartphones, and laptops – without extra appliances, licenses, or complex VLAN configurations. Using integrated Layer 7 client fingerprinting, client devices are automatically identified and classified, letting you distinguish between iPads and iPhones, device operating systems, and even manufacturer. Device-specific policies can be automatically applied to restrict, quarantine, or throttle user-owned devices. Client fingerprinting combined with a heuristics-driven reporting engine allows you to generate detailed reports of BYOD clients that have connected, measure the bandwidth and applications they've accessed, and even see their percentage of total traffic. Bonjour forwarding facilitates seamless discovery of Apple devices across VLANs, rounding out a full BYOD-centric feature set.

Complete with a free mobile device management (MDM) client agent called Systems Manager, monitor each of your organization's devices, showing useful metrics including client hardware/software information and recent location, and centrally manage your corporate devices with a great degree of granulaity; log in with remote desktop or command-line, push new applications, and remotely lock and erase devices.



Client Location Tracking

Top operating systems

#	OS	# Clients ▾	% Clients	Usage	% Usage
1	Apple iPhone	843	38.5%	163.22 GB	7.8%
2	Mac OS X	495	22.6%	1.20 TB	59.0%
3	Apple iPad	168	7.7%	78.78 GB	3.8%
4	Apple iPod	167	7.6%	45.13 GB	2.2%
5	Windows 7	158	7.2%	304.96 GB	14.6%
6	Android	144	6.6%	13.77 GB	0.7%
7	Windows XP	59	2.7%	26.85 GB	1.3%
8	Windows Vista	44	2.0%	81.39 GB	3.9%
9	Apple iOS	31	1.4%	1.40 GB	0.1%
10	Mac OS X 10.6	28	1.3%	84.06 GB	4.0%

Device Reporting and Analytics

Assign group policies by device type: Enabled: assign group policies automatically by device type

What is this?

Groups for device types

Device type	Group policy	Actions
Android	throttle	✕
iPad	whitelist	✕

Add group policy for a device type.

Device-Based Group Policies

Auto-Tunneling VPN Technology

Leveraging the Meraki cloud architecture, site-to-site VPNs can be enabled via a single click without any command-line configurations or multi-step key permission setups; Meraki cloud management automatically tunnels, hole punches, and configures devices to eliminate the complexity seen in traditional VPN setups. Complete with IPsec encryption, deploy the following architectural setups within minutes:

- Teleworker VPN: Securely extend the corporate LAN to remote sites wirelessly, using the MR series with your own server or a Meraki MX
- Site-to-site VPN: Multi-branch VPN w/ WAN optimization and Content Filtering (using Meraki MX Security Appliance)
- Secure roaming: Layer 2 and layer 3 roaming for large campus environments

Distributed Packet Processing

Meraki devices execute packet processing at the edge. Each wireless access point features a high performance CPU that enforces layer 3-7 firewall policies, application QoS, network access control (NAC), and more. Meraki networks scale seamlessly: add capacity by simply deploying more APs, without concern for controller bottlenecks or choke points.

Every Meraki wireless access point is built with the packet processing resources to secure and control its client traffic, without need for a wireless LAN controller. Meraki APs are built with a high performance CPU, hardware-accelerated encryption, and extended memory resources to implement stateful firewall policies, voice and video optimization, and even layer 7 traffic classification and QoS.