Introduction to Cloud Managed Networking

Cisco Meraki solution overview
About Cisco cloud-managed networking

Cisco Meraki: a complete cloud-managed networking solution
- Wireless, switching, security, WAN optimization, and MDM, centrally managed over the web
- Built from the ground up for cloud management
- Integrated hardware, software, and cloud services

Leader in cloud-managed networking
- Among Cisco’s fastest-growing portfolios: over 100% annual growth
- Tens of millions of devices connected worldwide

Recognized for innovation
- Gartner Magic Quadrant, InfoWorld Technology of the Year, CRN Coolest Technologies

Trusted by thousands of customers worldwide:
Why cloud managed networking?
The cloud increases IT efficiency

- Turnkey installation and management
- Integrated, always up to date features
- Scales from small branches to large networks
- Reduces operational costs
Cisco Meraki: Bringing the cloud to enterprise networks
An integrated solution for new IT challenges

1 billion iOS & Android devices

Integrated mobile device management

HD video and rich media

Layer 7 application shaping

New business opportunities

Analytics and user engagement

A complete solution out of the-box:
No extra hardware, software, or complexity
Cloud architecture
Cloud-managed networking architecture

Network endpoints securely connected to the cloud

Cloud-hosted centralized management platform

Intuitive browser-based dashboard
Out of band cloud management in every product

Scalable
- Unlimited throughput, no bottlenecks
- Add devices or sites in minutes

Reliable
- Highly available cloud with multiple datacenters
- Network functions even if connection to cloud is interrupted
- 99.99% uptime SLA

Secure
- No user traffic passes through cloud
- Fully HIPAA / PCI compliant (level 1 certified)
- 3rd party security audits, daily penetration testing
- Automatic firmware and security updates (user-scheduled)

Reliability and security information at meraki.cisco.com/trust
Scalable cloud infrastructure

Telmex
Nationwide hotspot and 3G offload network

Dress Barn
Nation-wide deployment spanning hundreds of retail stores

Motel 6
70,000 hotel room deployment

Jeffco School District
80,000 student district with 100+ schools

Proven in 10,000+ endpoint deployments
Intuitive web-based dashboard

- Wired + wireless
- Client fingerprints
- Application QoS
- Instant search
- Location analytics
- Real-time control
SaaS feature delivery

BYOD feature velocity, past 36 months:

- Client Fingerprinting
- Application traffic shaping
- Antivirus scan / NAC
- Mobile device management
- Device-based group policies
- Enterprise app deployment
- MDM-aware access control

Feature updates seamlessly delivered from the cloud (user-scheduled)
Adapts to new devices, applications, and business opportunities
Investing in R&D to address new challenges

Explosion of New Devices | New Business Applications | Operational Efficiency
Solution highlights
Distributed networks

Multi-site visibility and control
Map-based dashboard; configuration sync; remote diagnostics; automatic monitoring and alerts

Zero-touch provisioning
Devices automatically provision from the cloud, no staging required; self-configuring site-to-site VPN

Traffic acceleration
WAN optimization and web caching accelerates and de-duplicates network traffic; application-aware QoS prioritizes productivity apps
High capacity edge networks

Layer 7 application traffic shaping
Throttle, block, or prioritize application traffic with DPI-based fingerprinting; set user and group-based shaping rules

Cloud-base RF optimization
Dynamically avoid interference, optimizing channel selection and power levels

Density-optimized WLAN
RF platform tuned for airtime fairness and performance in dense performance-critical environments

RF optimization and application-aware QoS for high-throughput, high-density WLAN
Bring your own device (BYOD)

Out-of-the-box security, management, and capacity for BYOD-ready deployments

**Device-aware security**
- Device-aware firewall and access control
- Antivirus scan
- LAN isolation
- Bonjour Gateway
- Content and security filtering

**Integrated MDM**
- Enforce encryption, passcodes, and device restrictions
- Deploy enterprise applications
- Remotely lock or wipe devices

**Simplified onboarding**
- Flexible authentication with AD integration, SMS authentication, hosted splash pages, and automatic MDM enrollment
User analytics and engagement

**Optimize marketing and business operations**
Analyze capture rate, dwell time, and new / repeat visitors to measure advertising, promotions, site utilization, etc.

**Built-in analytics**
Integrated into WLAN, no extra sensors, appliances, or software

**Extensible API**
Integrate location data with CRM, loyalty programs, and custom applications for targeted real-time offers
Flexible authentication and access control

Flexible authentication
- Secure 802.1x and Active Directory authentication; Facebook Authentication for branding and targeted social marketing; SMS self-service authentication, Lobby Ambassador, and hosted sign-on splash pages

Dynamic access control
- Assign clients layer 3-7 firewall rules, VLANs, and application-aware quality of service by identity, group, location, or device type
Enterprise-class security features for security-conscious environments

Air Marshal WIDS/WIPS
- Detect wireless attacks; contain rogue APs; cloud-based alerting and diagnostics

User and device aware security
- User, device, and group-based firewall rules (layer 3-7) with Active Directory integration

Complete NG firewall and content security
- Application firewall; content filtering matching 1B+ URLs; antivirus / antimalware filtering; Google safe-search

© 2010 Cisco and/or its affiliates. All rights reserved.
Case studies
Case study: Applebee’s

“The Meraki Dashboard makes it easy to manage the WiFi across all the restaurants, and we have the visibility we wanted.”

Leslie McMasters, Network Administrator, Apple American Group
Case study: Milpitas Unified School District

- California school district with 14 schools, 10,000 students
- Deployed cloud-managed firewall, 500 wireless APs (indoor + outdoor), and 100 Ethernet switches
- Enabled 1:1 Google Chromebook deployment and BYOD policy
- Application visibility and control optimizes bandwidth across 10k+ clients

“The Dashboard, the traffic shaping, and the MDM were real advantages. We can see the traffic and devices on the fly.”

Chin Song, Director of Technology, Milpitas Unified School District
Case study: Mosaic

“The Meraki solution has provided us with a secure, centrally managed distributed network.”

Daniel McDonald, Systems Integration Manager, Mosaic

- Healthcare and services provider with 5,000 employees, 40 facilities across 11 states
- Deployed 350 cloud-managed wireless APs, switches, and security appliances
- HIPAA-compliant WiFi for electronic medical records and guest access
- Centrally managed by small IT staff
Product Families
MR wireless access points

5 models including indoor / outdoor, high performance and value-priced

Enterprise-class silicon including RF optimization, PoE, voice / video support

Lifetime warranty on indoor APs

Feature highlights

BYOD policies
Application traffic shaping
Guest access
Enterprise security
WIDS / WIPS
Location analytics
New wireless APs

MR18
General purpose 11n AP
Dual-concurrent 2x2, 600 Mbps

MR26
High performance 11n AP
Dual-concurrent 3x3, 900 Mbps
For high-density deployments

Industry’s only cloud-managed 802.11n APs with dedicated security radio

Technology from flagship MR34 brought to 802.11n family for uncompromised security and RF management
The Cisco Meraki MR34

802.11ac with Application QoS
For increased throughput and density

Dedicated Security Radio
3rd radio for Air Marshal and RF management

Built for Cloud Management
Seamless deployment, fully integrated features

The most advanced cloud-managed access point
3rd radio tames hostile RF environments

Radio dedicated to scanning and protecting RF environment
- Instantly detects and mitigates interference, vulnerabilities, and attacks on all channels
- 3rd radio enables full-time scanning with full-performance client access on 2.4 GHz and 5 GHz radios

Deeply-integrated with cloud-based software solutions: Air Marshal (security), Auto RF (performance)

No added cost or complexity
- Typical deployments: radio operates in background (zero-config)
- Power users: rich tools available for security and RF management
- No added cost: no extra hardware, software, or licenses
Protect network with dedicated scanning radio linked to powerful cloud-based software

Detects and classifies nearby APs using rich heuristics

Identifies vulnerabilities and attacks:
- Unmanaged / insecure APs plugged into LAN
- Malicious rogues spoofing WLAN
- Packet floods, malicious broadcasts

Contains rogue APs, blocking clients from associating
Auto RF: zero-config optimization for dynamic environments

Scans all channels for interference, tuning performance with cloud intelligence

Optimized for mixed 802.11ac and 802.11n environments

Cloud-based engine analyzes RF data, optimizes channels and power across network

Responds automatically to challenging or dynamic RF environments

Visualize interference with high-resolution spectrum analyzer
Security radio available across entire indoor portfolio

2013 indoor portfolio

- MR16
  - 2 stream 802.11a/b/g/n
  - 600 Mbit/s

- MR24
  - 3 stream 802.11a/b/g/n
  - 900 Mbit/s

- MR34
  - 3 stream 802.11ac
  - 1.75 Gbit/s

2014 indoor portfolio

- MR18
  - 2 stream 802.11a/b/g/n
  - 600 Mbit/s

- MR26
  - 3 stream 802.11a/b/g/n
  - 900 Mbit/s

- MR34
  - 3 stream 802.11ac
  - 1.75 Gbit/s
802.11ac with application QoS

3 stream, dual concurrent radios with 1.75 Gbps aggregate radio rate for high throughput and density

Layer 7 application fingerprinting classifies and controls evasive, encrypted, and P2P traffic
- Inspects packets and applies policies at full .11ac speed
- Prioritize business apps, real-time traffic
- Limit recreational, bandwidth-hungry apps

User and device fingerprinting for identity-based QoS policies

Airtime fairness algorithms for high-density networks

Cloud-based signature updates respond to new apps
Part of a complete solution

- Multi-site management
- User fingerprints
- Real-time control
- Instant search
- Location analytics
- Application QoS

Same out-of-the-box feature set as other Meraki MR wireless APs
MX security appliances

6 models scaling from small branch to campus / datacenter
Complete networking and security in a single appliance

Feature highlights
Zero-touch site to site VPN
WAN optimization
NG firewall
Content filtering
WAN link bonding
Intrusion detection
**MS access & aggregation switches**

**Feature highlights**
- Voice and video QoS
- Layer 7 app visibility
- Virtual stacking
- PoE / PoE + on all ports
- Remote packet capture, cable testing

**Gigabit access switches** in 8, 24, and 48 port configurations, PoE available on all ports

**10 Gigabit SFP+ aggregation switches** in 24 and 48 port configurations

**Enterprise-class performance and reliability** including non-blocking performance, voice/video QoS, and a lifetime warranty
Systems Manager mobile device management

Device Management controls iOS, Android, Mac, and Windows devices

Cloud-based - no on-site appliances or software, works with any vendor’s network

100% free - available at no cost to any organization, sign up at meraki.cisco.com/sm
Thank you.