RESOLUTION

Eliminating the cost and complexity of hardware controllers with cloud-based centralized management

Gone are the days when wireless was only available in a handful of offices or computer labs. Today, nearly every member of the campus community uses a laptop or some wireless-enabled device to access the resources they need on a daily basis. While the benefits of wireless are often well understood, achieving those benefits has historically been complex, expensive, and labor-intensive. IT professionals often have large areas to cover with multiple RF profiles. Performance, security, reliability, and cost constraints add to the challenge.

- **Great Coverage:** In order for the network to be useful, it must be available wherever people need it. In some cases, this will only be common areas such as classrooms and administration buildings. In other cases, wireless must be available campus-wide, including outdoors.
- **High Performance:** Wireless networks must be able to keep up with a rapidly increasing number of users and increased usage per user. Networks must be able to deliver consistent performance even when there are high concentrations of users, as in a conference centres. In addition, voice and video applications are becoming more common, requiring traffic prioritization. Networks must also ensure that a small number of data-hungry clients, such as those participating in file sharing, cannot crowd out everyone else.
- **High Availability:** Wireless networks need to be up all the time. It only takes one or two failures to lose users' trust. Any problems that do arise need to be contained and brought to the attention of the network administrators promptly.
- **Serve Multiple Constituencies:** Wireless networks often serve many different groups of users, each with its own unique requirements. Office users need access to the Internet and specific resources without inconvenience. Specialized devices like phones or security cameras need low latency connections. Future applications will undoubtedly also need to be accommodated.
- **Robust Security:** Since wireless goes beyond the walls of the administration building, it is no longer possible to use physical security to control access to the campus network. A wireless LAN (WLAN) needs robust authentication, authorization, and encryption mechanisms to prevent unauthorized use. The system also needs to integrate with the institution's existing authentication infrastructure, like Active Directory or LDAP.
- **Future Proof:** Constructing a wireless LAN represents a significant time and resource commitment. It is

essential that a WLAN investment last as long as possible. To that end, modular upgrades to the network should be an option. For example, it should be possible to upgrade the access points without upgrading the centralized control system, or to add a voice over Wi-Fi system without rebuilding the network.

- **Easy to Maintain:** IT staff are being asked to do more with less. A wireless LAN needs to be straightforward to install and maintain. Growing a network should not require expensive consultants or time-consuming site surveys. It should be easy to change security policies, add or remove network administrators, and bring new sites online.
- **Low Total Cost:** As with any organization's investment, return on investment must be front and center. Some of the important cost components in building a wireless LAN include:
  - Network design and planning
  - Installation
  - Hardware and software
  - Ongoing maintenance

Why RE-Solution Proposes Meraki

Meraki wireless networking systems were designed from the ground up to build high-quality networks. A Meraki system has two primary components: wireless access points and a web-hosted Cloud Controller.

Wireless APs are deployed throughout the coverage area and communicate directly with users' wireless-enabled devices. Meraki has different APs for different jobs, including 802.11b/g and 802.11n, single and multiple radio APs, as well as indoor and outdoor devices.

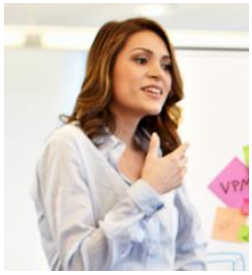
Meraki's Cloud Controller lets network administrators control, manage, and optimize their network from a centralized location. Unlike older architectures, Meraki's controller is provided as a service, eliminating the need for an expensive and difficult-to-install hardware solution.

- **Great Coverage:** A well-designed wireless network will provide good performance no matter where the

client may be. Coverage can be challenging: construction materials, client density, RF noise, and a number of other factors can all effect performance. Meraki has focused on providing a rich set of tools that make it easy for non-experts to build a great wireless network.

- **Intuitive Visualisation Tools:** The first step to providing good coverage is making it easy to picture the coverage. Meraki's visualization tools let network administrators position access point markers on indoor and outdoor maps. These maps show both the signal strength between the AP and each client as well as the signal strength among access points. When network administrators can see an area with poor client performance, they can do something about it.
- **Easy to Move and Add APs:** If a coverage gap is identified, or a cell's capacity has been reached, Meraki makes it easy to add an access point or reposition existing APs. No special controller or AP configuration is required. Adding an AP is as simple as plugging it in.
- **High Performance:** Meraki systems are engineered to provide the throughput needed to keep up with a large number of demanding users in a campus setting. There are a number of techniques used to provide that performance.

Customer Benefits



Setting up a multi-building Meraki network is straightforward. In most cases Meraki recommends placing all the campus APs within a single network on the Cloud Controller. This configuration ensures that each AP has the same configuration. In addition, the Cloud Controller will automatically summarize usage statistics across the entire network. Network administrators can visualize different buildings and the floors on each building using the visualization tools on Meraki Dashboard.

- **Channel Planning and Optimization:** Since wireless spectrum is shared among multiple APs and clients, it is important to put different APs on separate channels to maximize performance. The Meraki Cloud Controller keeps networks running at peak capacity by automatically finding the best set of channels for each AP to use, whether it is wired or not. Furthermore, since changing channel settings can briefly interrupt client access, Meraki allows the network administrator to control when channel changes take place, e.g., only when approved by the network administrator or when the office is closed at night.
- **No Controller Bottleneck:** Since Meraki APs do not send data packets through a hardware controller, there is no need to worry about controller backplane or port capacity. In addition, the Cloud Controller does not introduce any latency between the client and its host, which can occur with a hardware-based controller. For example, imagine a client is talking to a file server in the same building. In a hardware controller solution, traffic must flow from the AP to the controller, and then back to the file server. The further away the controller is, the higher the latency. In a Meraki network, traffic flows directly from the client to the file server.
- **High Availability:** The cost of downtime increases as more and more clients use the wireless network. Meraki systems provide high availability in several ways. First, the hosted approach eliminates the hardware controller, which is often a single point of failure. Instead, Meraki networks run off of a number of globally distributed data centers. In addition, the Meraki system is engineered to continue running even if the connection to the Cloud Controller is lost. One of the reasons this is possible is that the Cloud Controller is not in the data path. That is, client traffic flows directly from the AP to its destination. In the event of a lost connection, some services, such as remote management, are not available, but client traffic continues to route. Meraki networks also tolerate access point failures well. Even when deployed in a mesh configuration, fail-over from one node to another occurs nearly

instantaneously. Clients seamlessly move to a different AP and continue operation. Network administrators can also elect to receive email alerts when a failure event happens, allowing them to respond quickly.

- **Serve Multiple Constituencies:** It is key to be able to meet the needs of multiple groups of users, including faculty, staff, and students, each with its own set of service parameters. To meet this requirement, Meraki networks allow network administrators to create multiple virtual access points (VAPs). Each VAP has its own identity, including Service Set Identifier (SSID), security, and other policy settings. The table below shows a typical configuration when an educational institution needs to support staff, guests, and wireless VOIP phones.

Service Parameter	Virtual AP 1	Virtual AP 2	Virtual AP 3
Users	Faculty/Staff	Students	Phones
Security	Access to LAN	Internet only	Access to LAN
Client bandwidth	Unlimited	5 mbit/s	Unlimited
Quality of service	Normal	Normal	High
Authentication	802.1x / LDAP	Open	WPA2-PSK
SSID	Administration	Student	Admin – Phone

Each Meraki access point can have up to 15 uniquely configurable VAPs. Furthermore, VAPs can be created with just a few clicks.

- **Robust Security:** It is important to be able to lock down the organization's network. A WLAN solution needs to have a broad set of security tools available to match the needs of different organizations. While each organization is likely to have its own particular set of security requirements, we describe some of the most common configurations below.

- **VPN:** In this approach, all wireless traffic is routed outside the firewall. Those needing to access LAN resources, such as file shares, VPN back into the campus network as if they were outside the LAN. The segregation of WLAN from LAN traffic can be accomplished using VLAN tagging. Alternately, Meraki has a built-in LAN isolation feature which will prevent wireless clients from routing traffic to LAN addresses.

- **Physical Appearance and Security:** Unlike IT equipment such as servers and switches, access points often need to be mounted in public spaces. Aesthetics can sometimes be an important consideration. Meraki access points, including the enterprise-class MR11 and MR14, are designed to blend into campus environments. They feature internal antennas, small LEDs, and mounting options that can hide all wiring. They can also be mounted in areas like walls, dropped ceilings, or even in the plenum space. When physical security is a concern, Meraki APs can be padlocked to their mount plates, which also prevents the Ethernet cable from being unplugged.

- **Intuitive User Interface:** "Enterprise-class" does not have to mean "hard to use." The use of a web-based browser with a streamlined interface means that even nonexperts can configure and maintain a Meraki network. There are no rigid configuration files and no need to learn a new command line syntax.

- **Low Total Cost:** As with any infrastructure investment, it is important to consider all the cost elements of a wireless network. The total cost of a wireless network has several components, including the hardware, installation, wiring, training, and maintenance. Meraki offers benefits in each of these cost

buckets. The following table shows where cost savings are possible.

Cost Component	Legacy	Meraki	How?
Controllers/Appliances	£££	-	Use the cloud
Wiring	£££	-	No dedicated wiring
Installation	£££	£	Plug and play; no controller config
Access points	£££	£	Move intelligence from AP to the cloud
Training	££	£	Intuitive, web-based management
Upgrades	£	-	Automatic web upgrades

A Meraki solution is an efficient way to deploy wireless throughout an organization.

Proposed Cisco Meraki Product Families

RE-SOLUTION offers these components with the following features and benefits:

MR Wireless Access Points	Feature Highlights
	MR Meraki Access Points BYOD policies Application Visibility & Control Guest access Enterprise security WIDS / WIPS Mesh routing 6 models including indoor/outdoor, high performance (802.11ac) and value-priced Enterprise-class silicon including PoE, voice/video optimization Lifetime warranty on indoor APs

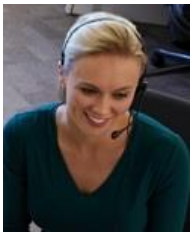
MX Security Appliances	Feature Highlights
	MX Meraki Cloud Managed Security Zero-touch site to site VPN WAN optimization NG firewall Content filtering WAN link bonding Intrusion detection 6 models scaling from small branch to campus / datacenter Complete networking and security in a single appliance

MS Access & Aggregation Switches	Feature Highlights
	MS Meraki Cloud Managed Switches 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

Cisco Meraki Webinar

Sign up for one of featured webinars qualified attendees will receive a free Cisco Meraki access point for Joining https://meraki.cisco.com/webinars?ref=1KmQWsE

Conclusion



Wireless has become a critical part of every business network infrastructure, enhancing users experience and productivity while enabling businesses to operate more efficiently. Meraki's complete wireless offering can help IT organizations deploy campus wireless quickly, easily, and at a price which will not strain the tight budgets of any business.

RE-Solution Technical Team would be pleased to discuss this solution with you in more detail. We can be reached at support@re-solution.london or 0203 828 6458.