



Meraki Solution Guide: Higher Education

Version 1.0, March 2009

Wireless is becoming a vital element of an educational institution's infrastructure. This document summarizes the requirements for a campus wireless network and describes how IT professionals can use Meraki to meet those requirements.

Copyright

© 2009 Meraki, Inc. All rights reserved.

Trademarks

Meraki® is a registered trademark of Meraki, Inc.



www.meraki.com

99 Rhode Island St.
San Francisco, California 94103

Phone: +1 415 632 5800
Fax: +1 415 632 5899

Table of Contents

1 The Benefits of Wireless 5

2 Requirements for a Wireless Campus..... 6

2.1 Great Coverage 6

2.2 High Performance 6

2.3 High Availability 6

2.4 Serve Multiple Constituencies 6

2.5 Robust Security 7

2.6 Physical Appearance and Security 7

2.7 Future-Proof..... 7

2.8 Easy to Maintain 7

2.9 Low Total Cost..... 7

3 The Meraki Approach 8

3.1 System Overview 8

3.2 Meraki in Campus Environments 9

3.3 Great Coverage 9

3.3.1 Intuitive Visualization Tools 10

3.3.2 Easy to Move and Add APs 10

3.3.3 Mesh That Works..... 10

3.4 High Performance 10

3.4.1 802.11n 10

3.4.2 Channel Planning and Optimization 11

3.4.3 No Controller Bottleneck 11

3.5 High Availability 11

3.6 Serve Multiple Constituencies 12

3.7 Robust Security 12

3.7.1 VPN 12

3.7.2 Pre-Shared Keys 13

3.7.3 Authorized Users 13

3.8 Physical Appearance and Security 13

3.9 Future-Proof..... 13

3.10	Easy to Install and Maintain	13
3.10.1	Wiring	14
3.10.2	Intuitive User Interface	14
3.10.3	Automatic Upgrades	14
3.11	Low Total Cost.....	14
4	Moving Beyond the Main Campus	15
4.1	Research Labs	15
4.2	Off-Campus Housing	15
5	Conclusion	16
6	References.....	17

1 The Benefits of Wireless

Gone are the days when wireless was only available in a handful of classrooms 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.

Wireless classrooms enable students and faculty to learn and teach more efficiently. Residential areas benefit from ubiquitous access and reduced wiring expense. Campus operations can make use of the infrastructure to streamline on-campus systems like ID card readers. Guests and alumni can easily access the Internet whether they are outside on the quad or at the stadium.

In some cases, educational institutions are even opting to reduce or eliminate the number of wired ports they install. Just as people are increasingly abandoning land lines in favor of mobile phones, campuses with fast, reliable wireless coverage are beginning to leave their wired connections behind.

2 Requirements for a Wireless Campus

While the benefits of wireless are often well understood, achieving those benefits has historically been complex, expensive, and labor-intensive. There are good reasons for this: covering an educational institution, large or small, is far more difficult than covering a home or small office. IT professionals often have large areas to cover with multiple RF profiles. Performance, security, reliability, and cost constraints add to the challenge.

In the next two sections of this guide, we will review the requirements for an educational campus network. We will then describe how Meraki can help IT professionals build a wireless network that meets those requirements in an efficient, cost-effective manner.

2.1 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. Coverage can also extend to dormitories other areas that round out the campus environment.

2.2 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 large classroom or library. 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.

2.3 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.

2.4 Serve Multiple Constituencies

Wireless networks often serve many different groups of users, each with its own unique requirements. Faculty and staff require secure access to the campus LAN. Students 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.

2.5 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.

2.6 Physical Appearance and Security

Unlike switches or firewalls, wireless access points (APs) are often mounted in publicly accessible locations throughout a campus. As a result, it is important that APs can be easily concealed, if required, or that they look aesthetically pleasing if out in the open. In some environments it is also important to be able to physically secure the APs to deter theft or tampering.

2.7 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.

2.8 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.

2.9 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

3 The Meraki Approach

This section explains how a Meraki system can help IT organizations build a robust, secure, and high-performance office network.

3.1 System Overview

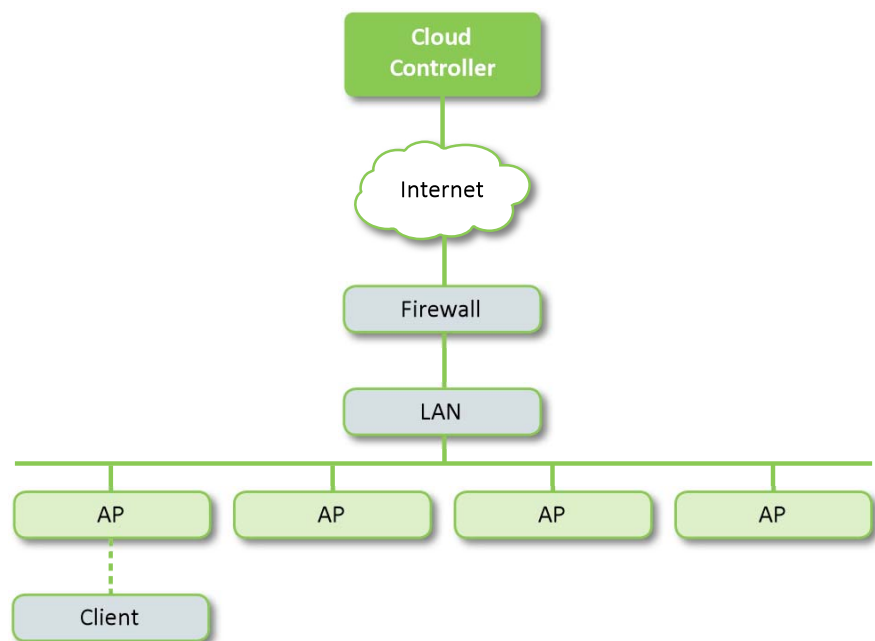
Meraki wireless networking systems were designed from the ground up to build high-quality campus networks. A Meraki system has two primary components: wireless access points and a web-hosted Cloud Controller.

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.

Figure 1 shows an overview of the Meraki system.

Figure 1 – Meraki Architecture



Meraki APs communicate with the Cloud Controller over a persistent tunnel using industry-standard protocols. Network administrators log into

the Cloud Controller through a web browser. Over the web, they can access all of the wireless networks in the organization’s account.

For more information on the Meraki architecture, see the Meraki Architecture White Paper.

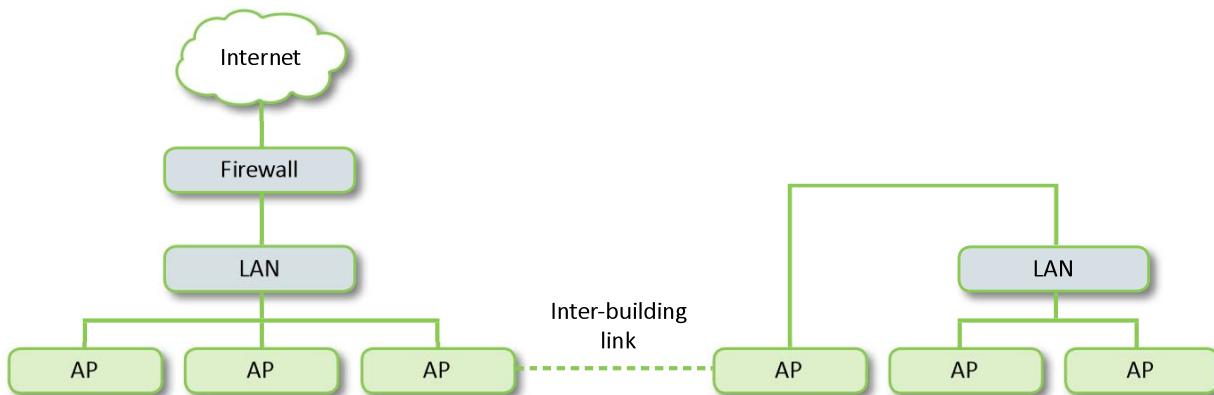
3.2 Meraki in Campus Environments

Many colleges and universities have multiple buildings on a single campus. The wireless network should enable users of the network to move easily from one building to another.

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.

IT managers can also use Meraki radios to create a high-speed, wireless point-to-point bridge between two buildings. Figure 2 illustrates this configuration.

Figure 2 – Point-to-Point Bridge



3.3 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.

3.3.1 Intuitive Visualization 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.

3.3.2 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.

3.3.3 Mesh That Works

Mesh networking allows access points to repeat the signal of other access points, eliminating the need to run Ethernet cabling to each AP. Mesh makes it quick to provide enhanced coverage to hard-to-reach areas by just plugging in an AP to power. Meraki's award-winning mesh protocols automatically find the best route back to the wired network, without any manual configuration whatsoever.

Mesh is especially useful for covering outdoor areas since LAN connectivity is often lacking outdoors.

For more detailed information on how to achieve great wireless coverage, see the Meraki Network Design Guide.

3.4 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.

3.4.1 802.11n

The underlying radio hardware has a significant effect on the overall system performance. When high performance is a requirement, Meraki recommends deploying dual-band 802.11n access points, like the Meraki MR14 or MR58.

The following table shows how the radio performance of a dual-band 802.11n Meraki system in a typical mixed-client environment.

Access Point	Client Traffic	Total Client Traffic
2.4 GHz 20 MHz channel	75% 802.11g clients @ 36 Mbps 25% 802.11n clients @ 104 Mbps	53 Mbps
5 GHz 40 MHz channel	100% 802.11n 2x2 clients @ 216 Mbps	216 Mbps
Total traffic (half-duplex)		269 Mbps

For more information on 802.11, see the Meraki 802.11n White Paper.

The use of dual-radio 802.11n APs is one of the keys to getting high performance. However, high quality access points alone are not enough.

3.4.2 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.

3.4.3 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.

3.5 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.

3.6 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 4 VAPs. Furthermore, VAPs can be created with just a few clicks.

3.7 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.

3.7.1 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.

3.7.2 Pre-Shared Keys

In the traditional approach to wireless security, users are given a common “pre-shared” key. The IT department may put the key on each client device, or distribute the key itself. WEP was the first key technology, but it has since been replaced with the more secure WPA2. A major advantage of the pre-shared key approach is that it is simple and quick to implement. However, it can be difficult to maintain with a large or changing user base.

3.7.3 Authorized Users

In this approach, each wireless LAN user receives a unique username and password. The user list can be stored on an existing database, like a RADIUS, LDAP, or Microsoft Active Directory server. Alternately, the user list can be hosted by Meraki. Users provide their login credentials through either a web page portal (hosted by Meraki), or using an industry standard 802.1x client.

3.8 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.

3.9 Future-Proof

Meraki provides both 802.11b/g and 802.11n access points. Organizations that decide to deploy b/g today have a seamless upgrade path to 802.11n technology should the need arise. It is also possible to deploy a mixed network, putting 802.11n in areas with high use, and b/g in less heavily trafficked areas.

Meraki also provides an upgrade path beyond 802.11n. One of the key attributes of the Meraki Cloud Controller is that it never becomes obsolete. If a school decides to upgrade its access points two or three years down the road, the Meraki Cloud Controller is guaranteed to be compatible.

3.10 Easy to Install and Maintain

Campus WLAN systems can be difficult for non-experts to design, install, and maintain, leading to expensive and time-consuming implementations. Meraki has gone to great lengths to simplify these processes.

3.10.1 Wiring

Whether APs are mounted on walls, ceilings, or in the plenum space, access point wiring can end up taking a significant amount of time. Power over Ethernet (PoE) is the simplest and cheapest way to power access points. PoE reduces expensive electrical wiring work by making use of existing Ethernet cabling. All Meraki 802.11n APs support the 802.3af PoE standard.

The use of mesh can also greatly simplify the wiring task. Meraki mesh works out of the box with zero configuration, making it easy to plug in repeaters where there is no convenient Ethernet port. The use of multiple radios on an access point also greatly improves the performance of mesh access points.

3.10.2 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 non-experts can configure and maintain a Meraki network. There are no rigid configuration files and no need to learn a new command line syntax.

3.10.3 Automatic Upgrades

Finally, unlike legacy systems requiring manual upgrades which may be time-consuming and disruptive, Meraki keeps the system software up-to-date automatically.

3.11 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.

4 Moving Beyond the Main Campus

Many educational institutions need to cover more than just the central campus. Additional coverage areas may include off-campus labs, research centers, or off-campus housing. This section describes how a network can be extended to cover these areas cost effectively and securely while still maintaining centralized management and control.

4.1 Research Labs

Many educational institutions want to provide wireless coverage throughout their network of offsite facilities, e.g., research centers and labs. However, these sites, or branches, often lack IT staff familiar with the wireless network.

Other solutions require that each remote location either have its own hardware controller (which is expensive) or have a connection back to the campus data center (which may not always be possible and may represent a single point of failure). Meraki does not require that branches have an MPLS or VPN connection in order to function properly, making it easier to set up branches quickly. It also makes it feasible to set up temporary campus-controlled networks at meetings, conferences, or seminars.

Meraki recommends setting up a different wireless network for each branch site. This configuration makes it easy to isolate network events to the site in which they are taking place and to view statistics and reports per site. Each branch uses its own configuration, while still giving the network administrator a centralized view of all the Meraki networks managed by the organization.

4.2 Off-Campus Housing

Students tend to be some of the heaviest users of wireless networks. Applications like video streaming, file sharing, and VOIP are quite common. In addition, user density is very high. The challenge for off-campus housing is often not getting ubiquitous coverage, but getting adequate bandwidth to users.

Meraki recommends a dense deployment of high-speed 802.11n access points. The APs will require multiple non-overlapping channels to get the capacity needed. Automatic channel planning can help greatly.

In addition, bandwidth throttling is often a must to ensure that a small number of users cannot dominate the network. Meraki's integrated bandwidth shaping engine can implement this policy.

Finally, physical security can often be a concern in student housing. Meraki recommends securely mounting APs with padlocks, and placing them out of sight and out of reach.

5 Conclusion

Wireless has become a critical part of the higher education network infrastructure, enhancing student life while enabling campuses 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 educational institutions.

6 References

1. Meraki Network Design Guide
2. Meraki Architecture White Paper
3. Meraki 802.11n White Paper

These reference documents are available for download at meraki.com.