For more information on how to Integrating the Apple iPad® Into Enterprise Wireless Networks with Lutrum, please contact us today!

Lutrum

www.Lutrum.com

844-644-4600

Meraki White Paper:

Integrating the Apple iPad® Into Enterprise Wireless Networks

April 2011

This document describes how to integrate the Apple iPad into a network securely and reliably, while providing the proper network experience for users of iPads, tablets and other wireless devices.

660 Alabama St.
San Francisco, California 94110

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

Table of Contents

1 Executive Summary

Network administrators need to carefully evaluate several aspects of security, access, and performance when considering deployment of Apple iPads and other tablets into enterprise networks.

Meraki's cloud-based networks make integration of iPads and tablets painless, and allow networks to survive the inevitable crush of iPads, so users can have the right network experience.

The following are recommended best practices for supporting iPads in enterprise networks:

- Ensure device and data security with integrated, easy-to-use methods provided by Apple
- Use standards-based authentication such as 802.1X if providing access to corporate LAN
- Block access to LAN if providing internet-only WiFi without authentication
- Deploy a wireless LAN with automatic RF optimization to ensure performance and reduce management overhead
- Monitor and shape application usage by deploying a wireless LAN with integrated user/device fingerprinting and application traffic shaping

Configuration of Meraki wireless access points is simplified and optimization is automated, for installations from a few access points to deployments of thousands of access points.

Network performance is automatically optimized and easily monitored, for single-site and multi-site installations, all from one central location over the web.

All of the best practices outlined above are easily implemented with Meraki’s award-winning cloud-based wireless networks.

2 The growth of the Apple iPad in the enterprise

It's no secret the Apple iPad has been a runaway success in the consumer market, with millions of devices sold in less than a full year on the market. Research firm Gleacher & Co. said it estimates 30 million iPads will be sold in 2011, more than double Apple's sales in 2010. Apple's competitors aren't standing still, either, and with new tablet devices entering the market from Samsung, Dell, Motorola, and others, total tablet sales for 2011 are expected to reach 52 million, according to research firm Canalys.

It has become clear that such a popular device will not be restricted to home or recreational use. Recently, Apple COO Tim Cook noted that 80% of the Fortune 100 has deployed or is testing the iPad for employee use. Large enterprises aren't the only organizations considering the iPad. A recent study by Forrester Research shows around 26 percent of enterprises with 1,000 employees or more are using or planning to use tablets for business use.

Tablets can enable mobile access to sensitive data, and their portability virtually guarantees users will travel with this data frequently between home, office, and beyond. Administrators managing wireless networks need not ask if such devices will enter into the workplace - the question is when (and how) they will enter. While certain organizations with strict security and confidentiality constraints may impose complete bans on the iPad and other tablets, most organizations need to find the best way to support the iPad, ensure security for the device and the network, and protect sensitive data, all while providing the proper network experience for all end users.

3 A new Swiss Army knife™ for the enterprise

The iPad is well suited for a wide range of business applications and uses, as illustrated by the breadth of both built-in and user-installable applications. Some are natural extensions of existing desktop programs, while others are causing a paradigm shift in the way users consume, digest, and produce information.

A natural use for the iPad is to work with existing documents that are so pervasive in the corporate environment. The iPad offers the ability to view, edit, and share corporate documents, such as those traditionally produced by spreadsheet or word processor applications, and its inherent mobility allows information to be consumed away from the desk.

Work on more specialized documents is also possible, especially given the touch interface and large display. Visual tools such as drawings, diagrams, and flowcharts used by engineers and designers can now be produced from scratch on a tablet device.

Vital business statistics, such as inventory and sales metrics, can now be delivered to the device, allowing a manager to keep track of critical data while on the go.

Figure 1: MicroStrategy Mobile app shows charts and data trends.

Specialized uses, such as patient monitoring applications and in-depth training tools, are now more interactive and delivered with a convenience that was not previously possible.

For interaction with other computers, the large display and network connectivity bring the ability to share desktops and computer screens to remote users who may be away from the office or desktop. And with tools such as built-in video cameras, video conferencing is now a practical reality. Now is the time for the network administrator to consider how such devices will be deployed and used in the network and what needs to be done to ensure a proper experience for tablet users.

4 iPad security and access

An administrator responsible for the health and integrity of an organization's network has many responsibilities, often including the integration of new devices into the network environment. Traditionally, this involved corporate owned or issued devices.

In the corporate-issued case, the network administrator can deploy the iPad and impose a number of restrictions, such as blocking user access to the iTunes store and app store, or limit access to certain built-in applications, such as YouTube or even the built-in camera. However, these policies may not be well received by users and also require the administrator to review, approve, and deploy any applications deemed to be desirable and allowed for users to access.

Some organizations may deploy corporate-owned iPads and issue them to employees, but others may consider how to integrate user-owned iPads. In either case, prudent network administration considers several aspects of device and network security and access. These can be categorized into four main topics:

1. Device security
2. Data security
3. Network security
4. Application security

Apple integrates security measures into the iPad that directly address each of these areas, so it's worthwhile to understand the device's capabilities and options for deployment so that the administrator can best decide how to integrate the device into the network. Once the device is on the network, data and network resources should not be compromised. The use and load on the network also needs to be considered, especially with emerging applications and enterprise use-cases.

4.1 Device security

The iPad has first-level access protection through a passcode that guards the unlocking of the screen. Administrators can enforce a passcode requirement such that all provisioned devices require the passcode for device use, and they can prevent the user from removing the passcode requirement, even if the user enters the correct passcode and tries to modify the device settings.

The iPad includes additional passcode policy options that will be familiar to administrators enforcing password policies on wired devices, such as desktops. These include:

- minimum passcode length
- minimum number of complex characters
- passcode aging
- maximum number of failed attempts

Administrators may choose options that closely match their existing password policies, or they can take this opportunity to establish more secure policies that are better suited for portable devices.

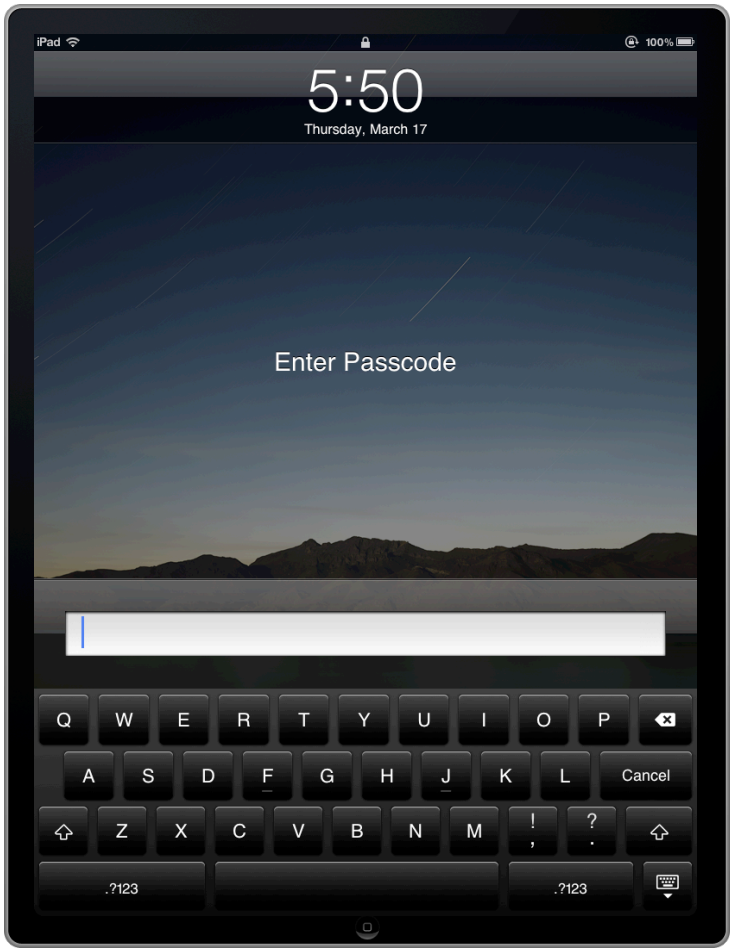

Figure 2: iPad with passcode protection requirement

Figure 3: iOS configuration tool provides granular passcode settings

4.2 Data security

As soon as the iPad begins to access network resources, it has the potential to store sensitive information that needs to be protected. The inherent mobility of the device increases the possibility that it could be lost, stolen, or simply fall into the wrong person's hands, even within the same organization.

The iPad has highly robust data security, starting with always-on 256-bit AES hardware encryption of data. This is similar to hardware encryption offered on laptop disk drives that, once enabled, are always on and cannot be disabled by the user. In the event the device is compromised, the data cannot be extracted from the device without the proper AES keys. This protects the data and even discourages malicious activities in the first place, since the 256-bit AES encryption acts as a deterrent.

The always-on encryption includes sensitive data, such as email and attachments. Optionally, the administrator can enable encryption of the iPad backup. As with all iOS devices, the iPad is periodically synchronized to a computer running iTunes, and it stores a backup of the iPad data in case of device loss or damage. This computer may be a user's personal computer and not managed by the IT administrator. Since the security of this computer is unknown, backup encryption provides an additional level of data protection.

The strength of the 256-bit key used for encryption is based on the passcode used for device unlock. Thus, ensuring passcode strength increases the protection of the device and the data it stores, including its backup data on a host computer.

In case the device is lost or accessed by an unauthorized person, there are two methods possible for permanent disabling of the iPad. A local data wipe can be initiated after a defined number of failed passcode attempts, and a remote data wipe can be initiated when the device is out of the owner's control, wiping data even if the device has been unlocked with the correct passcode.

4.3 Network security

Network access, authentication, and security methods common in many enterprise wireless networks are natively supported by the iPad.

Physical network access protection through 802.1X ensures the iPad can authenticate against existing RADIUS systems, including standards-based access such as EAP and others.

Secure wireless network access is provided via support for WPA2-Enterprise, including 128-bit AES encryption, protecting the wireless interface from attack with the same high level of security often used by corporate laptops with wireless access.

Users who travel away from the office campus can continue to access corporate resources through built-in support for VPN. Supported VPN methods include IPsec, L2TP, and others.

Figure 4: VPN (L2TP) configuration

Authentication protection for the VPN is provided through the support of x.509 digital certificates (including VPN on demand) and two-factor authentication devices such as RSA SecurID, or basic authentication through MS-CHAPv2.

The wide variety of supported standards for authentication, access, and wireless security, including on-premise and remote access, ensures the iPad can be smoothly integrated into existing environments that already have established and robust security policies, and that the iPad will not compromise network security through insecure authentication or access methods.

4.4 Application security

The proliferation of iOS applications through Apple's App Store enables users to discover, download, and install apps for myriad uses, from productivity tools to social networking and photo sharing to task management and games. Already there are over 65,000 apps available for the iPad, and over 350,000 for the iPhone, all of which run on the iPad.

Even with so many available applications, neither company-deployed nor user-installed applications (from the App Store) pose a threat to data security. The iPad's operating system isolates all applications, ensuring one application cannot read or write information into another. Furthermore, the applications themselves are shielded from system components, ensuring a rogue app will not compromise or take control of the file system, network access, security credentials, or the entire device. Security credentials such as usernames, passwords, and identities are stored in an encrypted keychain.

The iPad's built-in platform-level security ensures safe handling and encryption of application and user data.

5 Network considerations

Once an organization determines that the iPad is capable of securely accessing and retaining sensitive information in local and remote environments, it is worthwhile to consider the impact of the iPad on the network environment.

Access to the corporate network via the iPad is normally via WiFi - there are no wired ports at all. While the iPad is available with a 3G cellular connection, the connection is slower than WiFi, its use requires a data plan, and the quality of cellular service is not under the control of the network administrator. Therefore, it is imperative that the wireless infrastructure be ready for the iPad.

5.1 Preparing the wireless infrastructure

On a corporate location or campus, an 802.11n wireless network will provide the best experience for all wireless users, especially in high-density and high-throughput situations. This may require an upgrade of the wireless infrastructure, if it is based on older standards, such as 802.11b or 802.11g, or if it is based on single-stream (non-MIMO) 802.11n access points. Newer access points, such as the Meraki MR24 Cloud-Managed Access Point, deliver triple-stream MIMO for high capacity and throughput, up to 450 Mbps per radio, and often have two concurrent radios. This significantly increases the aggregate data rate to 900 Mbps.

The iPad supports 802.11n in the 2.4 GHz and 5 GHz bands. Radio interference is generally reduced in the 5 GHz band compared to the 2.4 GHz band, and there are many more non-overlapping channels simply due to the larger spectrum allocation in 5 GHz. A properly designed network will steer clients to 5 GHz where possible, leaving the 2.4 GHz band with slower, 2.4 GHz-only clients. This means the connection speed of the iPad and other 802.11n 5 GHz clients will not be slowed by 802.11b/g clients.

It is also prudent to consider adequate coverage of areas likely to see the iPad: these could be conference rooms, common areas (such as a cafeteria), or even outdoor areas, since users can easily wander outdoors with the iPad to work on documents, read and send email, or even attend an online meeting.

Automatic management of AP radio settings is critical to success in a high-density wireless environment with mixed client types. When devices from iPads to laptops to smartphones all attempt to use the wireless network, the installation and configuration of access points is key to success. A large number of APs covering a broad area creates hundreds of radio settings that can possibly be configured. In the days of autonomous APs, each radio's settings had to be individually configured for channel selection, power setting, band assignment, and possibly failover routing. This approach is not suitable at scale and can lead to configuration and management headaches, as well as a high likelihood for user error. Automatic management of access point radio settings is the recommended approach, allowing each access point to send information and statistics to a cloud-based centralized controller about interference, client usage, power level, and neighboring access points. The access points can then be coordinated automatically to provide optimal service based on those statistics.

5.2 Considering network traffic types

As the iPad increases the client density on the wireless network, it's important to ensure that the wireless experience for existing clients, such as laptops, is not degraded. Additionally, there may be certain critical traffic types that should be prioritized, such as VoIP or video conferencing, regardless of the access device. On the other hand, the iPad's portability, large screen, long battery life, and available applications facilitate new traffic types that were previously impractical, such as downloading an entire high-definition movie and viewing it on screen. It's important to consider the application and traffic types that will be generated by the iPad's use, and see how they impact the network.

Common use cases for the iPad include email and calendar applications, and the iPad provides built-in support for Microsoft Exchange Server and ActiveSync, as well as support of standards such as IMAP, SMTP, CalDAV, LDAP, and CardDAV. Push is supported for email, calendar, and contacts, meaning the iPad can use these protocols on demand.

Other business applications include document reading and editing, which can easily involve large files of tens of megabytes, meeting, webcast, and remote desktop applications, and business-specific applications such as virtual environments, database query applications, and teaching tools.

The iPad is a natural platform for video creation and consumption, particularly through VoIP and video conferencing applications. Applications such as Skype and Fring make voice and video calls easy, and applications such as WebEx and GoToMeeting let users join conference calls and meetings when away from their desk. Apple's own FaceTime® application makes video calls extremely simple, especially with the front- and rear-facing cameras on the iPad 2.

Since voice and video conferencing are often desirable and even business-critical applications, it's important to distinguish these from other video services, such as YouTube and Hulu. While video sites such as YouTube aren't new, the iPad may alter behavior of visitors to these sites. Whereas previously a user may have viewed a four minute video clip on the desktop, and then returned to a business task, the iPad now lets the same user go to a conference room or cafeteria and stream lengthy, bandwidth-intensive clips. Applications such as Netflix allow the user to stream feature-length movies, potentially creating significantly increased bandwidth demands on the wireless network. Even social networking sites, now more accessible than ever, can have heavy bandwidth needs from viewing hundreds of embedded photos and videos. Thus it is critical to be aware of network traffic, the demands applications have on bandwidth, and to have a tool that allows the desired applications to flow freely, while throttling less-desirable activities.

6 Enabling the proper network experience

Meraki enables the network administrator to deploy a secure, reliable, high-performance wireless network that meets the demand of bandwidth-intensive mobile devices such as the iPad and other tablets. Meraki's Cloud Controller brings centralized, network-wide management via the web, without the need for dedicated on-site IT.

6.1 Infrastructure

Meraki's enterprise 802.11n wireless cloud-managed wireless access points provide the access infrastructure necessary for demanding environments. Meraki 802.11n dual-radio access points support up to 900 Mbps with triple-stream 3x3 MIMO and support up to 50% more clients than 2x2 MIMO access points.

Using Auto RF, each access point is constantly monitored and optimized from the cloud, eliminating the need for the administrator to manually monitor and optimize each AP and instead automatically adapting the network to changing interference conditions via the cloud. Multi-radio, multi-channel mesh routing and automatic mesh failover offer fault tolerance and provide robust and fast coverage in hard-to-wire areas.

6.2 Security and authentication

Meraki integrates enterprise security features, including access and authentication through WPA2-Enterprise with 802.1X/RADIUS, stateful policy firewalls, VLAN tagging, and guest network access. This allows the network to be configured with a high level of security that still allows the iPad to associate and authenticate safely.

Devices other than iPads, such as home-owned laptops and tablets, can pose a threat to the network as virus entry points. Built-in network access control (NAC) protects the network even further by blocking access from clients with insufficient virus protection from accessing the network.

Meraki wireless networks meet enterprise security requirements, wireless performance requirements, and relieve the administrator from the painstaking duty of manually optimizing individual access points.

6.3 Traffic shaping and analysis

Ensure business-critical traffic is prioritized and recreational traffic is throttled with integrated traffic shaping and analysis. Each access point includes an integrated layer 7 packet inspection, classification, and control engine, allowing QoS policies to be set based on traffic type. Mission critical applications are easily prioritized, while setting limits on recreational traffic, e.g. peer-to-peer, music, and video streaming, to ensure smooth network operation under the increased load of the iPad. Find the most bandwidth-intensive applications used on the network and see which users consume the most bandwidth, in aggregate and by application.

6.4 Reporting and monitoring tools

Identifying iPads and other tablets is as easy as entering “ipad” into a Google-like search box. Administrators can immediately see the devices consuming the most bandwidth, as well as an application and protocol profile for each device.

Integrated client location tracking lets administrators pinpoint clients who may be experiencing poor conditions and see them on a Google map or even an office floor plan.

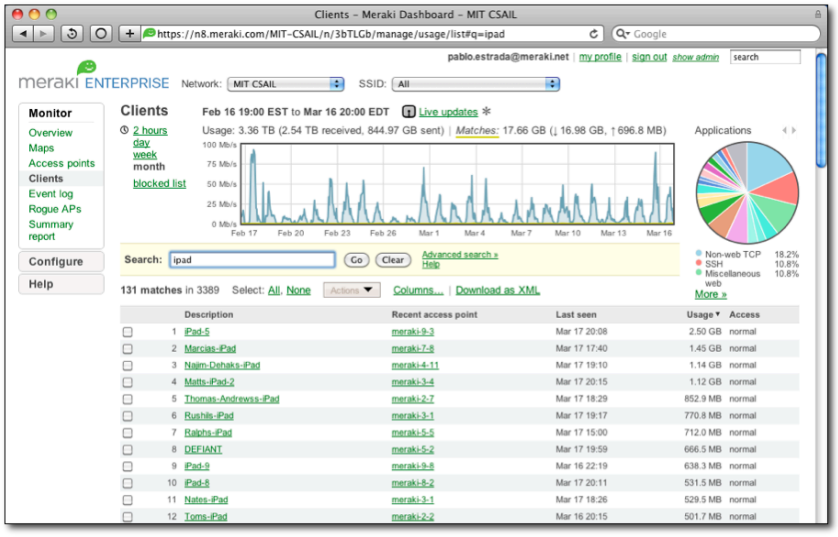

Figure 5: Finding iPads on the network is as easy as searching for “ipad”

7 Conclusions

The proliferation of iPads and other tablets is already here, and the extension from consumer use to enterprise use shows no sign of slowing down. Network administrators are already faced with ever-increasing demands, and the emergence of new client devices accentuates this further. As new client devices expand the possibilities of information consumption and creation, especially with mobile devices, new applications consume more network resources than ever.

A network administrator needs to protect critical assets while providing the right network experience for all end users. This requires careful consideration of device, data, and network security, as well as network performance.

Meraki's cloud managed networks provide the infrastructure necessary to support iPads and other mobile devices. Configuration of wireless access points is simplified and optimization is automated, for installations from a few access points to deployments of thousands of access points. Network performance is automatically optimized and easily monitored, for single-site and multi-site installations, all from one central location over the web.

8 References

Apple, Inc. (2010). iPad in business deployment scenarios. Cupertino: Author.