MERU NETWORKS®

WHITEPAPER

BYOD in Healthcare

Improving Clinician Productivity and Patient Satisfaction

May 2013

Table of Contents

Introduction

Unlike other professionals who work for single enterprises, doctors usually work for multiple organizations, including private practices and one or more hospitals. All of these businesses have their own communications and electronic medical record (EMR) systems, and doctors are expected to access such systems at any of their work sites no matter where they are working at the moment. Even within one healthcare system, doctors carry multiple communication devices such as pagers and VoIP phones. Remembering different user names and passwords for each email and EMR system and managing multiple communication devices quickly become a drain on clinician productivity.

In today's hospital, mobility is driving much of network design, and Wi-Fi has become major components of corporate networks. Most laptops and handheld computers are Wi-Fi enabled and have been adopted by IT as standard network nodes, but these are typically hospital-owned assets. One major trend that is altering the wireless network LANscape is the explosive adoption of smartphones and tablets (such as iPads, iPhones, and Android devices) by clinicians. Low cost and broad application support now allow clinicians to purchase personal mobile devices.

Touchscreen interfaces have revolutionized the way clinicians use and access content through these devices and have hastened widespread adoption. This enables users to access the Internet and use thousands of applications, creating a "move-and-do" culture in which people expect to have connectivity wherever they are. In order to stay connected, clinicians are now bringing personal wireless devices into the work environment. The next logical request is, "Can I use my device on the hospital network for work purposes?" As doctors work across different businesses or use multiple devices, allowing them to use their own smartphones and tablets to communicate and to access networks appears to be a logical step. This in turn can give rise to a new requirement: wireless and network access policies and capabilities to allow users to bring their own devices. According to a survey conducted by Meru Networks,[1] 79 percent of hospitals allow clinicians to bring their own devices and use them in the hospitals.

Support for "bring your own device" (BYOD) is not straightforward. It requires planning and an understanding of different access scenarios. Since Wi-Fi can be viewed as a network gateway for personal devices, the 802.11 infrastructure and its features are the basic building blocks for implementing a robust BYOD solution. Most certainly there is a need to provide patients and guests with wireless connectivity to the Internet, which is easily achieved through a captive portal. However, beyond providing wireless service, a number of challenges need to be addressed:

[1] http://www.merunetworks.com/collateral/surveys/healthcare-wlan-survey.pdf

CHALLENGES	REMARK
Provisioning of devices	Without an automated method to define a client Wi-Fi profile, provisioning each device with the right security becomes a support issue. Support for the broadest set of possible devices becomes unmanageable when scaling to thousands of users with dozens of device types, OS platforms, and Wi-Fi drivers.
Device management	Without proper network tools, it is impossible to proactively manage devices that may gain access to the network in an ad hoc manner. It is important to know how many and what types of devices are on the corporate network, and who is using the network.
Data privacy and security	Hospitals need to follow stringent HIPAA regulations while allowing BYOD. According to an HIMSS survey,[2] 36 percent of respondents indicated that securing information on mobile devices was the top security concern at their organizations.
Network saturation	There is a limit to the number of devices that can be sustained on a network within available bandwidth, so it is important to have tools that allow management of application flow, bandwidth allocation, and quality of service (QoS) in order to prioritize network access properly. Having a network that supports both 2.4 GHz and 5 GHz services is a key feature in being able to manage bandwidth allocation.
Troubleshooting	Quickly analyzing problems is complicated when diverse devices are on the network, and the process requires the right set of tools.

Table 1 - BYOD Challenges in Healthcare

Early BYOD implementers were faced with a lack of tools and a potential IT support nightmare. Because of this, some hospitals avoided the problem altogether and simply prohibited BYOD. However, avoidance is not a long-term solution, as end-user demand and benefits to hospital are so great that many IT departments are required to implement BYOD policies. In fact, several studies indicate that embracing BYOD results in increased employee productivity and lower TCO, providing a real benefit to the enterprise.

Manually provisioning each device for secure 802.1X Wi-Fi access is time consuming, and configuration varies from device to device. To simplify Wi-Fi provisioning, IT may be tempted to implement private shared key (PSK) security. Allowing individuals to provision their own devices is a security risk, because they might ignore IT policy and configure their devices to circumvent essential security settings. This approach often does not enforce authentication of users via a corporate directory prior to provisioning the device, and thus everyone gets the same access settings regardless of their organizational role. A lack of BYOD policies and services makes troubleshooting difficult because there is no way to automatically receive trace logs or to assist remotely.

[2] http://himss.files.cms-plus.com/HIMSSorg/Content/files/leadership_FINAL_REPORT_022813.pdf

BYOD Requirements

Most IT managers acknowledge the need to support BYOD, but many have little understanding of possible BYOD solutions. What follows is a brief analysis of the requirements for BYOD in hospital settings.

Allowing virtually any Wi-Fi–compliant device on the network can be a daunting challenge, and hospital IT teams need to clearly address the following issues:

1. ***Provisioning user-owned wireless devices without jeopardizing the security of the network***
   Manual configuration of each device's Wi-Fi profile by the IT team is not a scalable practice. Manual configuration by end users is exponentially more risky because of the complex nature of the operation. Configuration is not a one-time event: there is enough device and user churn year over year to overwork any IT team. The optimal solution would be a self-provisioning application that requires little or no intervention from IT support. To ensure network security, any person attempting to access the network must be identified and authenticated against a trusted network source, such as Active Directory, using the settings defined by an IT policy created to handle the complexities of diverse user types and mobile OS products.

2. ***Limiting access to network resources based on the class of user/device pairs***
   To properly manage network resources, there must be a mechanism by which a user is granted access to a defined set of network resources and services. Each user (clinician, patient, guest) may have unique access service and resource rights on the same network. This can be based on either a user class or on individual permissions and device classes, but it is necessary to ensure that network resources are secure and accessed only by those permitted to do so from authorized devices.

3. ***Managing hospital-owned devices and user-owned devices***
   The basic requirement here is the ability to identify the device of the authenticated user. This is necessary because a user may have two or more Wi-Fi devices connected to the network. Identifying what is hospital owned and what is user owned may dictate the network services available to a given user/device pair. [3]

4. ***Scaling without compromising network bandwidth***
   Logically, there is a limit to the number of devices and classes of applications that the network can simultaneously support. With BYOD, which may cause a higher device-to-user ratio, it is critical to estimate user traffic loading and to have the ability to analyze bandwidth problems when they occur. A sophisticated BYOD solution will also provide methods for traffic-load partitioning in order to maximize resources with minimal impact on the user community.

5. ***Keeping track of devices and how they are being used***
   To properly manage a dynamic BYOD environment, it is important to be able to produce network-level transaction and client-state reports for troubleshooting. This requires that the infrastructure itself support the capability for real-time and after-the-fact reporting and troubleshooting. This information is vital for the review of bandwidth demands that is necessary for network planning.

[3] Complementary mobile device management (MDM) services can support this distinction and allow device-specific features like "wipe" (to delete device-resident data) or other device-directed commands.

6. ***Managing a single user with multiple wireless devices***
   Some industry analysts[4] have described the network user of the near future as having two or more devices: a laptop, a smartphone, and a wireless tablet, for instance. With wireless devices, mobile workers can perform their duties as long as they have a Wi-Fi connection. As a result, it is important to be able to support a single user who is logged into the network from two devices concurrently. Full logging and tracking of multiple devices must be provided, along with the ability to generate summary reports by user.

7. ***Managing a consistent set of applications across a varying set of mobile devices***
   In order to manage assets or applications as network resources are managed, a BYOD solution must be able to associate a user/device pair to a specific class of applications and restrict access to other resources.

8. ***Managing corporate data written to a mobile device***
   In an ideal deployment, a BYOD solution does not permit corporate data to be written to mobile device storage. To achieve this level of control, a true virtual desktop infrastructure (VDI) should be implemented and should complement any BYOD-imposed security controls. Without a VDI, mobile device control would be under the domain of a mobile device management (MDM) solution (application specific or device level) and might allow deletion of specific data objects or force a “wipe” (deletion of all data) of the device itself.

9. ***Allocating bandwidth to specific users or devices***
   BYOD environments need to support multiple applications that vary in bandwidth demand. Standard Web applications place little demand on bandwidth, but voice and video applications can place high demands. The ability to manage bandwidth by user/device pair is important to ensure network reliability. Load balancing and applying fairness rules to application-specific traffic are important to ensure the best experience for all network users.

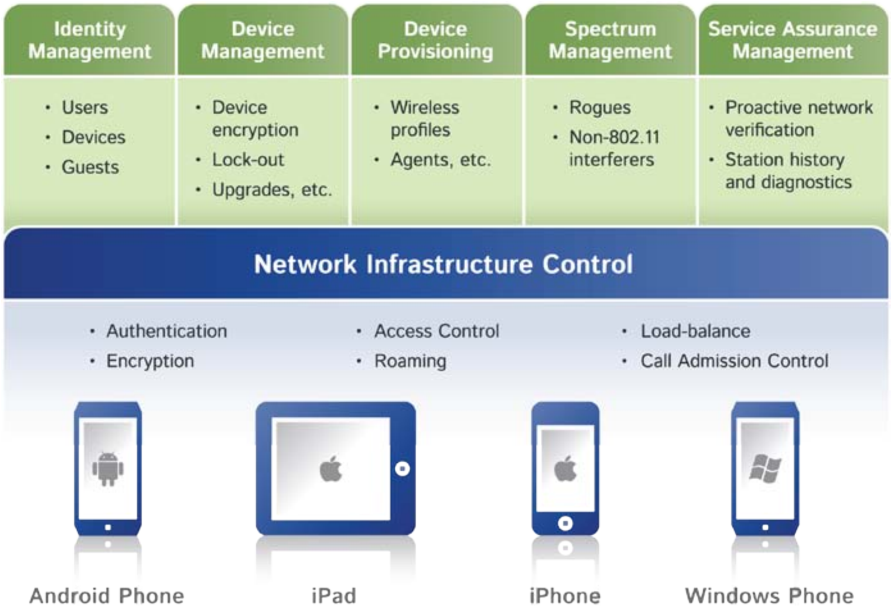

Figure 1 - BYOD Solution Architecture

[4] Forrester, “US Workforce Technology & Engagement Online Survey” (Q2-2011), estimated up to 3.2 devices per user, and iPass, “The iPass Mobile Workforce Report” (2011), estimated 2.7 devices per user would become the norm in the enterprise.

BYOD Deployment Guidelines

Plan for Implementing a BYOD Solution

For support of BYOD policies, proper planning is important. An understanding of the current Wi-Fi capacity and coverage is a major component of this planning. A BYOD solution may require adding additional APs for increased bandwidth and coverage. Identifying the limitations of the Wi-Fi network and taking corrective actions ahead of operational deployment are also critical to success. Another important part of the planning exercise is to assume an increase in the number of mobile devices per user.

An initial step in the planning is deciding how to partition and allocate network resources with regard to assignment to classes of users or devices. The majority of legacy devices are 2.4 GHz technology. This RF range tends to be congested more easily. One simple bandwidth policy to consider is to segregate the 5 GHz–capable devices from the 2.4 GHz devices for bandwidth optimization. When defining policies based on application type, bandwidth and latency for video and voice (VoIP) applications will require higher QoS levels than simple Web-based applications do.

IT managers must clearly define the local resources (printers, faxes, etc.) and Internet resources that will be accessible to guest users, so that infrastructure provisioning can be defined properly. The same level of partitioning may be required for different classes of business users, for controlled access to proprietary or confidential company-managed data and resources.

Provisioning Infrastructure and Devices

Once the planning is complete, the wireless (and possibly the wired) network must be provisioned and configured. Existing network routers, switches, session border controllers, firewalls, and wireless network elements may need to be reconfigured to fully support the desired mobile feature set. Following this, management software must be completed and test plans executed to verify that the configuration behaves as expected for the possible user and device combinations.

Proactively Managing and Troubleshooting

The mobile user community needs to be trained and brought on line. If the BYOD infrastructure is set up correctly, individuals can enter and exit the network via self-provisioning services, with few or no work orders generated for IT support. When problems do occur, the IT team can employ tools that identify the problem areas within the network and analyze the transaction history in order to solve the problems.

Meru BYOD Solution Architecture

Meru Networks is the premier provider of enterprise-class WLAN solutions, which now include the Guest Management and Smart Connect features of Meru Identity Manager that together deliver the best solution for enterprises to manage the BYOD phenomenon. Identity Manager is integrated with Meru controllers, offering device fingerprinting to identify the type of device and determine whether or not the device is a corporate asset. Meru Identity Manager solves the problem of delivering enterprise wireless network access for all, enabling one-click self-provisioning of client devices for secure 802.1X connectivity. It is also compatible with third-party wireless LAN solutions.

Smart Connect

Smart Connect provides identity-based access, device registration, and policy management for corporate and user-owned devices of all types. A license option of Meru Identity Manager, Smart Connect surmounts the greatest obstacle to BYOD secure connectivity by simplifying 802.1X access and the provisioning of Wi-Fi devices under centralized IT policies. New users simply access a provisioning Web portal, enter appropriate identifying information (name and password), and Wi-Fi profiles are created automatically on their systems.

Smart Connect Features:

- 10-minute, wizard-based setup for configuring network profiles
- Integrated, customizable portal for end-user access, without additional server requirements
- Integrated, role-based authentication to map network profiles to users
- Integrated monitoring and reporting from a single location
- Support for all major platforms, including Windows, Mac OSX, iOS, and Android
- Support for WPA, WPA2, 802.1X, PEAP-MSCHAPv2, PEAP-GTC, WPA-PSK, and WPA2-PSK

The major benefit of Meru Smart Connect is that users are responsible for registering themselves, and thus there is no security risk due to publishing the security key to a new user. IT is responsible for defining the different access policies, but beyond this there is little support burden.

Guest Management

To provide patients and guests Internet or network access without putting network security at risk, the Meru BYOD solution supports guest management, which allows sponsors to create guest accounts in a secure, controlled manner. Automating this process as much as possible frees IT resources from having to directly manage the process of supporting guests on the network. Identity Manager provides both a sponsor portal and a self-registration portal for visitors. For hospital personnel, once the user’s device identity is established, Identity Manager automates the process of configuring the device for secure access. Guest devices may have limited network resources available for security reasons. Meru’s Identity Manager solution supports a large variety of devices including iOS devices (iPhone and iPad), Android devices, MacBooks, and Windows laptops.

Service Assurance Application Suite

The Meru Service Assurance Application Suite includes E(z)RF® Network Manager and Service Assurance Manager (SAM), providing proactive network monitoring, logging, and testing to ensure the network is optimized for mobile devices and to assist with troubleshooting and reporting. Capabilities supported by the Service Assurance Application Suite include identifying and reporting the status information of all registered wireless stations. Via a visual representation of the network structure, management functions can be employed, including selection and replay of client-state information for the purpose of diagnosis and troubleshooting.

BYOD increases traffic loads on a network:

- More users have access to the network.
- Each user potentially has multiple devices.
- Mobile applications are sophisticated and have increased bandwidth demand.

Because of this, SAM was designed to detect connectivity issues within a wireless network and can validate traffic paths through the network (including wired infrastructure and services such as RADIUS and DHCP). Connectivity issues are quickly identified so that proactive steps can be taken to resolve the problem.

An additional valuable component of this suite is Meru Spectrum Manager. The performance and reliability of the WLAN can be degraded by RF interference. The source can be other Wi-Fi devices or other products using the ISM band (Bluetooth, cordless phones, etc.). All of these can generate interference and disrupt the operation of the WLAN. Spectrum Manager can be used to identify and locate the sources of interfering RF to get the WLAN back on track.

End-device Management

The last major element in a BYOD deployment is management of end devices. There are several options available, ranging from simply managing the base access of individuals to implementation of a commercial MDM solution to deploying a complete VDI. The first option is the simplest and can be managed directly from Meru Network Management applications.

Meru has validated some of the commercially popular MDM solutions and has found them complementary to all the Meru management services. Products such as these can take proactive command over the behavior and content of a mobile device. In the case of a device being lost or stolen, the device can be directed to wipe its data from permanent local storage, preserving the security of the corporate data.

The VDI option in today’s market provides only a fragmented solution, because not all mobile devices are currently supported. A VDI solution, however, eliminates most mobile device management issues, because the solution consists essentially of secure terminal emulators, and data is not stored on the mobile devices but on the remote VDI server. This provides a more secure approach from the enterprise perspective.

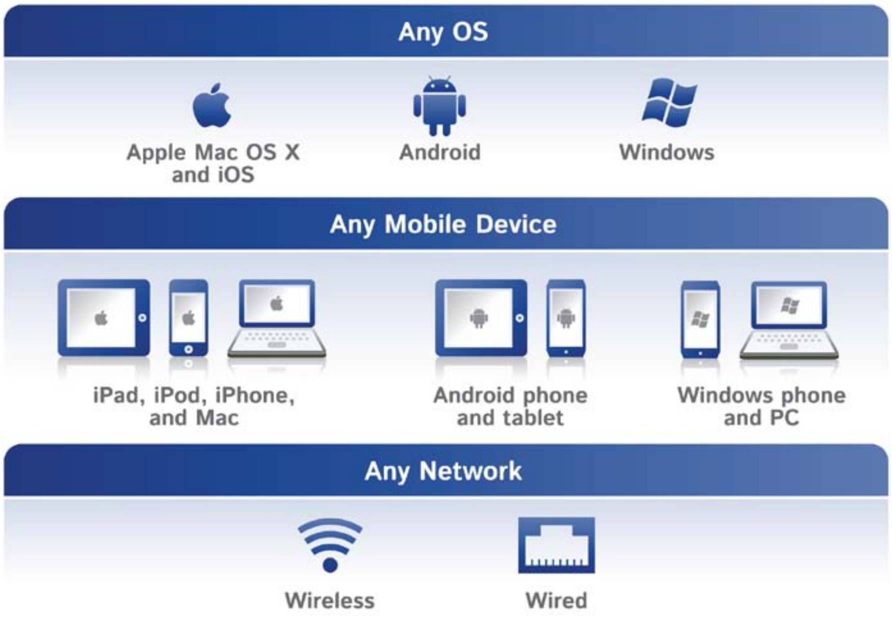

Figure 2 - New BYOD Topology

Summary

BYOD is a phenomenon in growing demand in the healthcare industry. Hospitals face common challenges of provisioning mobile devices for secure access to the network and scaling the WLAN solution to meet the onslaught of devices without an overwhelming burden on IT.

REQUIREMENT	COMMON BYOD PRACTICE	MERU BYOD SOLUTION (Best Practice)
Provision multiple user-owned devices without jeopardizing network security while minimizing impact on IT resources	Manual client Wi-Fi provisioning	One-click self-provisioning by users based on predefined secure access policy using Identity Manager and Smart Connect
Limit access to network resources by user/device pair	n/a	Identity Manager policy management options, Meru controller's firewall, and QoS capabilities
Manage corporate-owned and employee-owned devices differently	n/a	Identity Manager device registration and management
Scale the wireless network without compromising bandwidth	Best-guess network design	Channel layering and port mapping to segregate user community for optimized bandwidth utilization, combined with policy and QoS rules enforced by Meru controllers based on rules defined in Identity Manager
Monitor and log network-attached user/device pairs	n/a	Implementation of 802.11i, plus wireless resource partitioning for best usage model
Manage single users with multiple devices	Manually configure VLANs, switch ACLs, and firewalls	User- and device-specific profile management
Manage application access across a varying set of mobile devices	n/a	Device identification and fingerprinting, and fine-grained policy based on the device and user identity
Manage mobile-device local data	n/a	Use of Identity Manager policies to limit client access to network data, and deployment of an MDM solution
Intelligent bandwidth management based on user class	n/a	Meru controller policy enforcement module and Identity Manager

Table 2 - Meru Answers to BYOD Requirements

Powering the Wireless Enterprise

Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T: 1 408.215.5300
F: 1+1 408 215 5301
E: meruinfo@merunetworks.com

For more information about Meru, visit www.merunetworks.com.