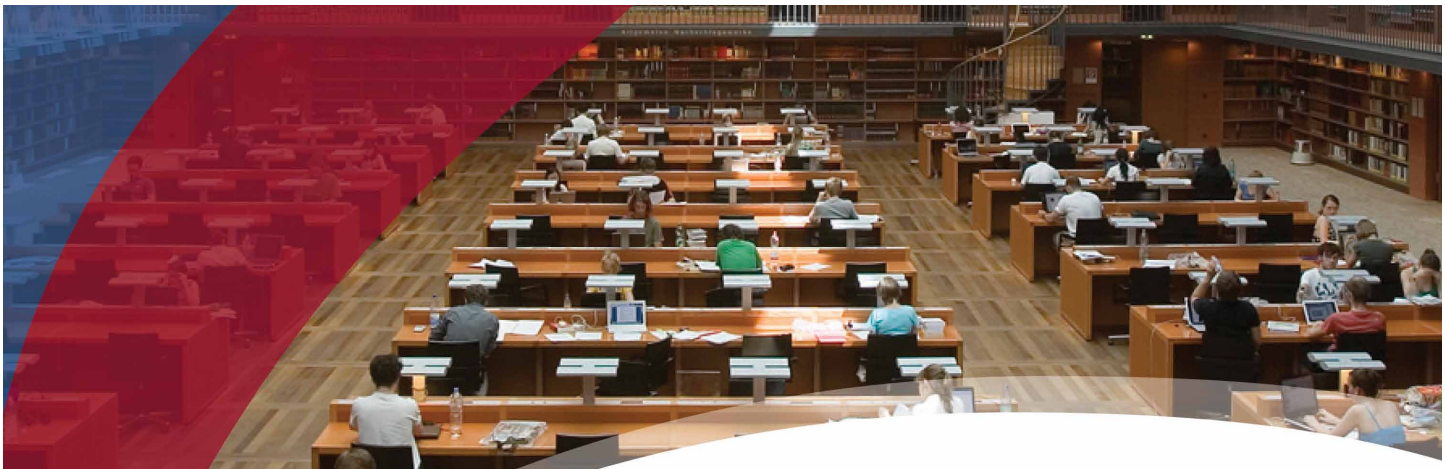

White Paper

BYOD Best Practices

Requirements and Challenges

January 31, 2012

Table of Contents

Introduction

Traditionally, network managers made extensive efforts to ensure the security of their enterprise network by managing "who" and "what" was permitted on the network. Because early network devices were attached via physical (hard-wired) connections, security was a straightforward exercise in physical security. Authentication of a user may have been by application, by the server, or over a VPN, but both users and workstations could be managed via control of physical access to the network.

In today's business environment, mobility is driving much of the network design, and wireless LANs (IEEE 802.11 – Wi-Fi) have become a major component of the corporate network. Most laptops and handheld computers are Wi-Fi enabled and have been adopted by IT as standard network nodes, but they are typically company-owned assets. One major trend that is morphing the wireless network LANscape is the explosive consumer adoption of smartphones[1] and tablets[2] (such as iPads, iPhones, and Android devices). The low price point and broad application support now allow individuals to purchase personal mobile devices. The touchscreen interface has revolutionized the way people use and access content through these devices and has hastened widespread consumer adoption. This provides an individual with the capability of accessing the Internet and using thousands of applications, creating a "move-and-do" culture in which people expect to have connectivity wherever they are. In order to "stay connected," individuals are now bringing personal wireless devices into the work environment. The next logical request is: "Can I use my device on the corporate network for work purposes?" Employees do not want to carry both a corporate *and* a personal wireless device. This in turn can give rise to a new requirement: wireless and network access policies and capabilities to allow users to "bring your own device" (BYOD).

The Aberdeen Group states in the 2011 report "Prepare Your WAN for the BYOD Invasion" that 82% of survey respondents support the idea of an employee accessing the network from their smartphone,[3] and 72% of these companies also supported BYOD for wireless tablet devices. Vastly popular devices from all major smartphone and tablet vendors are dual-mode (Wi-Fi and cellular), and the trend to support BYOD is clearly not "if" but "when." So prevalent is this trend that a new catchphrase has been coined: "the consumerization of IT."

Support for BYOD is not straightforward and requires planning and understanding of the different access scenarios. Since Wi-Fi can be viewed as a network *gateway* for these 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 *guests* with a wireless service to the Internet, which is easily achieved through a captive portal. However, beyond providing wireless service, there are a number of challenges that need to be addressed:

1 The ITU report for 2010 noted that for the Americas, 94% of the available market had purchased a cellular phone.

2 Forbes has projected that >100M iPads will have been sold in North America by 2018. Market research from IDC states that the tablet market has shown a sequential quarter over quarter shipment growth of 88.9%, and 303.8% year-over-year growth.

3 Aberdeen "Prepare your WAN for the BYOD Invasion" (7/2011) also reported that within the next calendar year, 94% of participating businesses would have BYOD support in place.

Table 1. BYOD Challenges

CHALLENGE	REMARKS
Manual provisioning of devices	Without an automated method to define a client Wi-Fi profile, provisioning each device 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.
Security	The use of inherently insecure devices on a secure corporate network requires differentiated access control for these devices.
Networks saturation	By definition, there is an upper limit to the number of devices that can be sustained on a network within the available bandwidth. It is important to understand this limit and to have the 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	Being able to analyze problems quickly is complicated when diverse devices are on the network and requires the right set of tools.

Early BYOD implementers were faced with a lack of tools and a potential IT support nightmare. Because of this, some companies avoided the problem altogether and simply prohibited BYOD. However, avoidance is not a long-term solution, as end user demand is 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.[4]

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 may ignore IT policy and configure their devices to circumvent essential security settings. This approach often does not enforce authentication of the user via a corporate directory prior to provisioning the device, and thus everyone gets the same access settings regardless of their organizational role. Lack of BYOD policies and services makes troubleshooting difficult because there is no way to automatically receive trace logs or to be able to assist remotely.

4 Aberdeen BYOD Research Brief, 2/2011 – Enterprises reporting in this brief experienced a drop in TCO and an increase in productivity when deploying BYOD.

Requirements, Challenges, and Benefits of BYOD

Most IT managers acknowledge that there is a real need to support BYOD, but many have little understanding of possible BYOD solutions. What follows is a brief analysis of the requirements, challenges, and benefits of BYOD.

Requirements

Allowing virtually any Wi-Fi–compliant device on your network can be a daunting challenge, and you will need to clearly address the following questions:

1. ***How to provision user-owned wireless devices without jeopardizing the security of the network?***
   Manually configuring each device's Wi-Fi profile by the IT team is not scalable. Manual configuration by the end user is exponentially more risky because of the complex nature of the operation. This 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 requiring 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 (e.g., Active Directory) using the settings defined by an IT policy created to handle the complexities of diverse user types and mobile OS products.

2. ***How to limit access to network resources based on the class of user/device pair?***
   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 (company or consumer) may have unique access service and resource rights on the same network. This can be based either on a user "class" or on individual permissions and device class, but it is necessary to ensure that network resources are secure and accessed only by those permitted to do so from authorized devices.

3. ***How to manage corporate-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 corporate owned and what is user owned may dictate the network services available to that user/device pair. [5]

4. ***How to scale without compromising the network bandwidth?***
   Logically, there is a limit to the number of devices and classes of applications that the network can simultaneously support. With BYOD, where there may be 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 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.

5. ***How to keep track of devices and how they are being used?***
   To properly manage a dynamic BYOD environment, it will be 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.

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

7. ***How to manage a consistent set of applications across a varying set of mobile devices?***
   In order to manage assets or applications like managing network resources, a BYOD solution must be able to associate a user/device pair to a specific "class" of applications and restrict access to other resources. Just as Meru's Wi-Fi solution asserts control over access to network services, the BYOD solution must do the same at the application level.

8. ***How to manage 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. ***Can I assign specific bandwidth allocations 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 is important to ensure the best experience for all network users.

6 Forrester Q2-2011, "US Workforce Technology & Engagement Online Survey," estimated up to 3.2 devices per user, and the iPass March 2011 report, "The iPass Mobile Workforce Report", estimated 2.7 devices per user would become the norm in the enterprise.

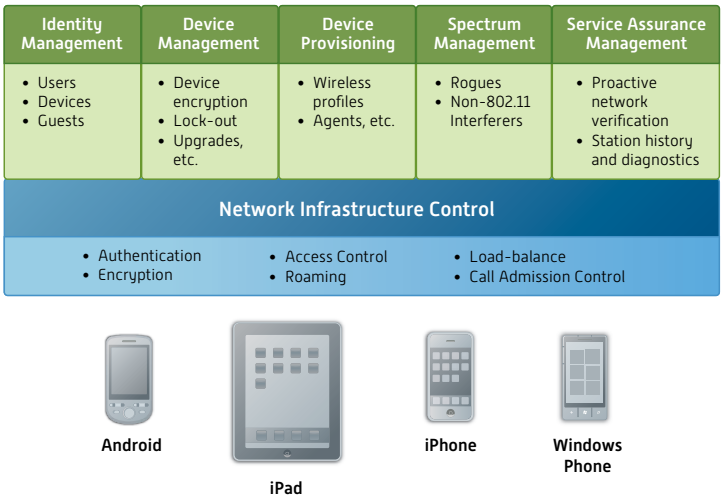

Figure 1. BYOD Solution Architecture

Benefits

Although implementing BYOD policies requires additional effort on the part of IT, there are a number of corporate benefits to be derived:

1. ***Improved employee satisfaction*** – Wi-Fi–enabled devices of all kinds are being brought in greater numbers to the work place by employees, to campus by students, to hospitals by physicians, to hotels by guests, and to stores by shoppers. It is practically impossible to impose mass restrictions without escalating frustration of users. For many, support of BYOD is a matter of customer satisfaction or employee morale, and has the added benefit of reducing the propensity of users to deploy rogue access points or Wi-Fi hotspots through their mobile phones or laptops.

2. ***Lower communication costs*** – BYOD, leveraging Wi-Fi, has a direct impact on a business's monthly cellular communication costs and the costs of purchasing or upgrading mobile devices. BYOD means that IT (or the company) is no longer forced to purchase a cell phone or tablet for the user.

3. ***Lower support costs*** – A BYOD solution that supports self-provisioning will drastically lower the number of IT support tickets generated. Additionally, smart troubleshooting tools will facilitate fast resolution to network problems. Some studies are beginning to show that users who bring their own devices to work tend to troubleshoot them first before calling for help; ownership and familiarity may engender a greater sense of personal responsibility.

4. ***Increased productivity*** – Users are already familiar with their smartphone or tablet, and BYOD has been shown to be more productive in mobile environments.[7] This can also virtually eliminate device training by IT.

5. ***Increased WLAN security control*** – A BYOD solution allows subscribers easy access to a secure network that has monitoring capabilities to alert the IT department of problems such as congestion or device failures.

7 Forrester Q2-2011, "US Workforce Technology & Engagement Online Survey."

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 is critical to the success of the BYOD implementation. Another important part of the planning exercise is to assume an increase in the number of mobile devices per user (e.g., tablet and smartphone).

An initial step in the planning is to decide 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.

IT managers must clearly define the local (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, provisioning and configuration of the wireless (and possibly the wired) network must be done. 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 results in the expected behaviors for the different possible user and device combinations.

Proactively Manage and Troubleshoot

The mobile community needs to be trained and brought on line. If the BYOD infrastructure is set up correctly, individuals may 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 will employ tools that identify the problem area 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 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.

Smart Connect

Smart Connect provides identity-based access, device registration, and policy management for corporate and user-owned devices of all types.

Smart Connect is a license option to the Meru Identity Manager platform that solves the greatest barrier 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 the Wi-Fi profile is created automatically on their system.

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
- Supports all major platforms, including Windows, Mac OSX, iOS, and Android
- Protocols supported: WPA, WPA2, 802.1x, PEAP-MSCHAPv2, PEAP-GTC, WPA-PSK, 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 the new user. IT is responsible for defining the different access policies, but beyond this there is little support burden.

Guest Management

To provide visitors/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. By automating this process as much as possible, IT resources are freed 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 corporate users, 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:

1. More users have access to the network.
2. Each user potentially has multiple devices.
3. 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 proactive steps can be taken to resolve the problem.

An additional valuable component of this suite is 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 and help get the WLAN back on track.

End Device Management

The last major element in a BYOD deployment is management of the end device. 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 the 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 of the mobile device management issues because the solution is essentially secure terminal emulators and data are not stored on the mobile devices but on the remote VDI server. This provides a more secure approach from the enterprise perspective.

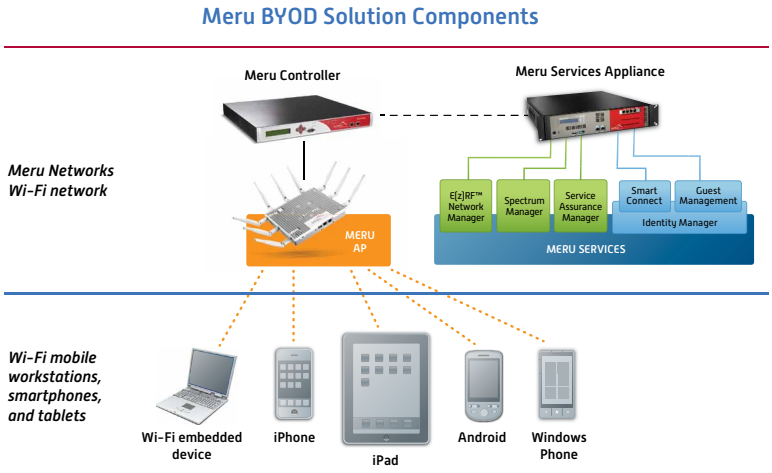

Figure 2. Meru BYOD Topology

Summary

BYOD is a phenomenon in growing demand in the industry; enterprises large and small, schools, retail businesses, and healthcare providers are all at various stages of adoption. They face the 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.

Table 2. Meru Answers to BYOD Requirements

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 – 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 controller 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 user 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 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

This paper identifies requirements and challenges facing IT organizations considering support for employees bringing personal devices into the enterprise. Meru is a key player in the 802.11 marketplace and has extended its product family and professional services to provide premier support for BYOD implementations. Meru's Identity Manager platform offers a highly scalable solution that meets the demands of today's highly dense environments with thousands of users connecting simultaneously to the network from a plethora of devices. Meru's virtualization architecture, combined with identity-based access and provisioning, supports device identification, self-enrollment, authentication, authorization, and policy enforcement. Meru's controllers and access points provide the right solution for enterprises to support iPhones, iPads, Androids, and other smartphones and tablets entering the workspace.

For further information about Meru, visit **www.merunetworks.com**.

Powering the Wireless Enterprise

Corporate Headquarters
894 Ross Drive
Sunnyvale, CA 94089
T +1 408.215.5300
F 1 +1 408.215.5301
E info@merunetworks.com