

*Network World and Robin Layland present*

# **The 2011 Wi-Fi Challenge**

**Enterprise Suppliers Respond to the Mobile  
Multimedia Frenzy**



**2011**

## *Introduction:*

### **Enterprise WLANs on Track to Displace Ethernet.....3**



### **The Evolving Network Edge.....6**

Professional Opinions Disclaimer:  
All information presented and opinions expressed in this report represent the current opinions of the author(s) based on professional judgment and best available information at the time of the presentation. Consequently, the information is subject to change, and no liability for advice presented is assumed. Ultimate responsibility for choice of appropriate solutions remains with the reader.

#### **Contact:**

Robin Layland  
Layland Consulting  
(860) 561 - 4425  
Robin@Layland.com

**Copyright © 2011** Robin  
Layland / Layland Consulting

---

---

# Enterprise WLANs On Track to Displace Ethernet

*Vendors bolster Wi-Fi architectures, security, management*

By Robin Layland  
President  
Layland  
Consulting



By Joanie Wexler  
Analyst/Editor  
Joanie M. Wexler  
& Associates



---

The tide is turning as Wi-Fi starts to edge out Ethernet as the primary LAN access network in many enterprise organizations. A confluence of factors is driving the trend toward WLAN access:

- **The user/employee expectation of always-on mobility** is shifting network traffic off of wired networks and onto WLANs.
- **High-speed 802.11n network infrastructures can handle near-Ethernet connect rates.** Some of the newer dual-mode access points, for example, support three spatial streams per radio and deliver 900Mbps connect rates (with actual throughput roughly half that).
- **The price for some 802.11n equipment has fallen to 802.11g price levels.** Offering up to an eight-fold capacity improvement over 802.11g with no price premium, 802.11n has become the default, go-to wireless LAN of choice.
- **A bevy of Wi-Fi-enabled consumer-grade mobile devices is hitting enterprise networks.** 802.11n backbones are arriving just in the nick of time to support them and the flood of traffic they create. Employees often use smartphones and, increasingly, tablet computers for both personal and business activity, creating unstoppable trends known as the “consumerization of IT” and “bring your own device” (BYOD). Whether the employee buys the device, saving the enterprise capital dollars, or whether it’s purchased by IT, users get a far better experience with Wi-Fi than with a slower cellular data network when running today’s high-bandwidth applications.
- **Many mobile applications contain video and multimedia components.** The applications are often collaborative and sensitive to transmission delays, jitter and packet loss. Yet they are quickly joining the enterprise WLAN thanks to IT consumerization and BYOD trends.

Today’s enterprises want their mobile networks to mirror many traits of wired Ethernet networks, of course. Yet with all these trends afoot, new challenges arise in the delivery of consistent and reliable mobile performance, security, and policy enforcement.

## What the WLAN Vendors Are Up To

For the vendors behind the curtain, achieving Ethernet parity with Wi-Fi is a tough nut to crack. The RF medium is shared among all users connecting to a given AP. It is also prone to co-channel interference from other Wi-Fi devices and non-Wi-Fi devices legitimately sharing Wi-Fi’s unlicensed 5GHz and 2.4GHz frequency bands. Voice calls nail up bandwidth for the duration of

## 2011 Wi-Fi Challenge

sessions, lowering the number of users who can connect to the AP. And Wi-Fi has moved beyond just conference rooms and public areas into mainstream workspaces. Broader coverage plus high-bandwidth applications creates a need to install APs in a fairly dense fashion. Consequently, enterprise-class vendors are hard at work building tools and tweaking their architectures to achieve some or all of the following:

- **Add capacity to APs** while building in transmission power control capabilities for proper operation of high-density WLANs. High-density WLANs involve installing many more APs for spectrum reuse and greater capacity. However, having more APs closer to one another can also increase co-channel interference if power levels aren't tuned just right.
- **Avoid traffic bottlenecks** by distributing data plane functions and, depending on vendor, some control plane functions to APs
- **Identify and eradicate interference** and its sources
- **Enable converged management and policy-setting** across Wi-Fi and wired Ethernet environments to lower operational expenses (opex)
- **Reinforce quality of service (QoS)** capabilities with features above and beyond those in the IEEE 802.11e set of QoS standards to handle real-time and streaming traffic on the WLAN
- **Offer flexible management and control options** that include virtual machine (VM) alternatives both in on-premise virtualized servers and as cloud services. Virtualization can simplify operations and reduce capital expenses (capex).
- **Provide access control capabilities** that offer visibility into the mobile device, user, and the location of the user attempting to connect to the corporate network and apply policy accordingly
- **Monitor** the full spectrum of airwaves to detect and mitigate possible intrusions and performance problems
- **Address the branch-office needs** of companies with large numbers of distributed sites with simpler WLAN setups and protection against WAN failures

These are currently the areas where the suppliers attempt to differentiate themselves from their competitors. The 2011 Wi-Fi Challenge serves as a kind of "cheat sheet" that you can use to compare what the respective vendor participants are focusing on and get an idea of their primary strengths.

### Our Challenge to the Industry

So that you can learn specifically what the major enterprise-class vendors are doing to achieve these goals and to help you evaluate potential 802.11n suppliers for your organization, we have brought together six leading enterprise-class 802.11n network system vendors:

- **AirMagnet/Fluke Networks**
- **Aruba Networks**
- **Cisco**
- **Enterasys Networks**
- **Hewlett-Packard**
- **Motorola Solutions**

## 2011 Wi-Fi Challenge

We have challenged these companies to articulate to you, in the following pages, why they should be your enterprise-class Wi-Fi vendor. Though every network has a unique set of challenges, and the vendor responses here can't address every possible nuance, responses to this challenge should educate you about each vendor's primary value proposition.

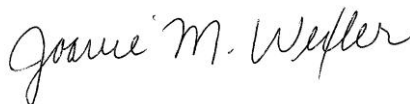
This document is just one part of The 2011 Wi-Fi Challenge. We also encourage you to listen to three audio panel discussions among the participating vendors, moderated by *Network World Wireless Alert* author Joanie Wexler, on the following topics:

- **“High-Density Design Amid the Mobile Explosion”** with Jim Florwick, Technical Marketing Engineer at Cisco, and Rob Haviland, Technical Marketing Engineer at Hewlett-Packard
- **“The Mobility Free-For-All: Controlling Access to Your Network”** with Ozer Dondurmacioglu, Product Marketing Manager at Aruba Networks, and Mike Leibovitz, Product Manager for Wireless LANs at Enterasys Networks
- **“Maintaining Consistent Wi-Fi Performance in Fickle RF Environments,”** with Jesse Frankel, AirMagnet Product Marketing Manager at Fluke Networks, and Manju Mahishi, Director of Wireless Products Strategy at Motorola Solutions

These audio Webcasts are all accessible at the 2011 Wi-Fi Challenge Web site at *Network World*. In addition to the audio format, there is also a text transcript for each discussion available for download at the Web site.

### Read, Listen, and Learn

We invite you to peruse the following documents, provided by the six Wi-Fi vendor participants, which sum up their primary competitive differentiators. We asked the vendors not to address all the issues but instead to concentrate on what they think are the most important ones and where they excel compared with their competition. The next step for you is to read and/or listen to what they have to say, then contact them about issues you consider important that they didn't mention. Let them explain how they can help you build a high-density 802.11n network that meets your performance, security, and management requirements.





# The Evolving Network Edge

## *BYOD with Security*

By William Glynn  
Senior Product  
Marketing Manager  
Enterasys



---

### The Evolving Network Edge

When you talk about the network edge today, you're most likely talking about wireless access. Today's workforce is highly mobile, outfitted with an ever-growing assortment of Wi-Fi-enabled devices, and has an insatiable need for continuous network access.

Consequently, the market is experiencing high growth in wireless LAN deployments throughout all vertical markets, including schools, hospitals, warehouses, small and medium-sized businesses, and virtually every other location where workers or people congregate. Today's business environment requires network access to be omnipresent as well as reliable, and it must provide strong performance with seamless roaming capabilities. While wired networking is still an important component of an enterprise network in data centers and other points of aggregation, the wireless edge continues to grow and has become a dominant factor in all network rollouts and upgrades.

Creating a fully integrated, easily managed, and secure WLAN with wire-like performance need not be an exorbitantly costly and time-consuming endeavor fraught with pitfalls and gotchas. Enterasys Wireless solutions dramatically lower the cost of upgrading indoor and outdoor WLANs so you realize the benefits of 802.11n while eliminating unnecessary and time-consuming switch and infrastructure replacement costs. Enterasys solutions deliver these benefits, in part, with the following:

- **Specialized mounting hardware** that leverages existing brackets to streamline installation
- **Automated AP discovery, configuration, and optimization** to reduce installation and start-up time
- **Full support for 3x3 MIMO operation with .af power**, which eliminates the need to re-cable the POE infrastructure

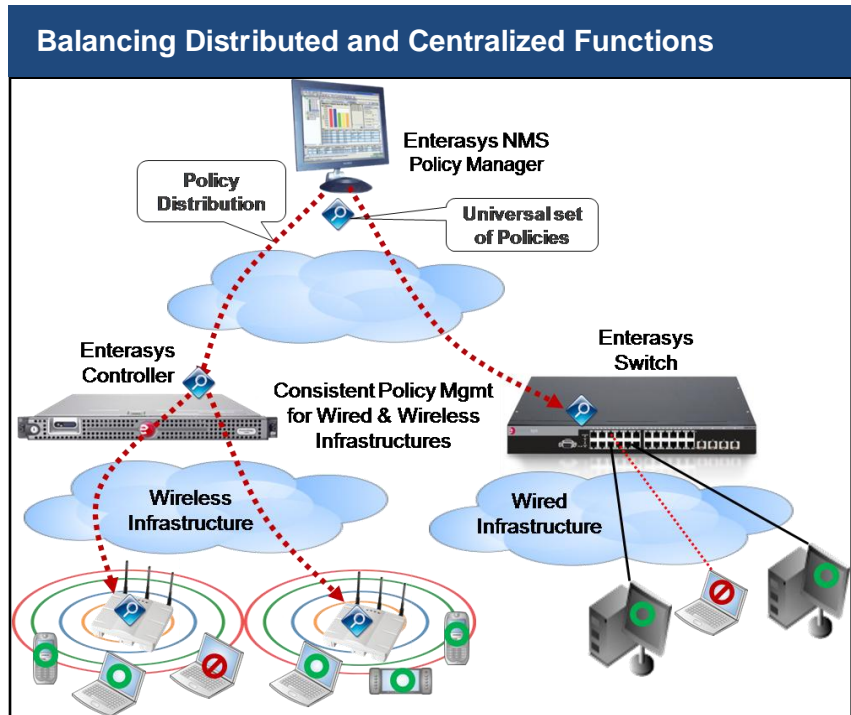
### Building a Unified Access Layer

Leading IT organizations now demand mobile, transparent, and always-on wired-to-wireless edge services. This new unified access layer requires two components. The first is intelligent access components that distribute access control and business service resiliency across the entire infrastructure. Second, these distributed access components must be manageable from a single management console to ensure consistency and minimal management overhead.

## 2011 Wi-Fi Challenge

Enterasys' unified access layer portfolio delivers both the distributed access components and centralized visibility and management needed to maximize network performance and reduce risks. These solutions provide scalability and resiliency with minimal dependence on a central management plane.

The common thread that binds Enterasys' unified access portfolio is Enterasys' exclusive automated role-based architecture. Uniquely, Enterasys enables multi-user authentication, authorization, access control, and traffic flow optimization, ensuring transparent access to business services and unparalleled mobility. This automated role-based provisioning system lowers OPEX costs and ensures consistent access to business services whether users are plugged into the wall or are untethered and moving freely across the campus.



Network management is complicated by the fact that most enterprise networks typically comprise both wired and wireless LANs, which is why Enterasys has taken a leadership role in integrating wired and wireless LAN management (**see figure**). The two network infrastructures can be managed and secured as a single entity to significantly simplify network management and deliver ongoing operational cost savings. A hallmark feature of Enterasys solutions is the ability to eliminate the inefficient and time-consuming task of manual, switch-by-switch or controller-by-controller network configuration changes. The benefits are not only efficiency but also error reduction, since manual operations for network configuration changes (e.g., setting up individual telnet sessions to each switch and performing access control list changes and re-ordering) are eliminated.

The Enterasys Wireless Management Suite provides a powerful centralized management platform for the Enterasys Wireless portfolio. As an integrated component of the Enterasys Network Management Suite (NMS), Wireless Manager consolidates configurations across the entire WLAN to provide global management capabilities. Integrated security across the wired/wireless network enables quick diagnosis and resolution of threats, and real-time, at-a-glance location capabilities detect rogue users and shut down hot spots by exact location, addressing a critical enterprise challenge.

One of the biggest strengths of the Enterasys Wireless products is their deployment flexibility. Enterasys provides complete flexibility over the location of the controller as well as how the WLAN is managed, which reduces costs, simplifies management, and removes the barriers to deploying a wireless edge. Customer deployment options include:

- A typical on-premise wireless deployment where controllers are collocated in proximity to the access points and self-managed by the customer
- A private cloud model where the controller is centralized in the customer's data center and self-managed by the customer
- A managed services model where the controller is centralized in the customer's data center and remotely managed by a managed service provider

## 2011 Wi-Fi Challenge

- A public cloud/managed services model where the customer's controller is located in a provider's data center as part of a hosted service, which is then combined with a managed service where a managed service provider remotely manages the controller

The mobile workforce has also had a dramatic impact on the portable device market and has given rise to the consumerization of IT. The explosion of smartphones and WiFi-enabled devices has led to the popularity of "Bring Your Own Device" (BYOD) programs, because they enable employees to work from the device of their choice, increasing employee satisfaction and productivity while decreasing corporate IT CAPEX costs. However, BYOD programs can increase IT workload and pose security challenges. Enterasys Wireless solutions can help you manage BYOD programs while dramatically reducing your time, cost, and effort.

### Security from the Inside Out

Enterasys has always secured networks from the inside out by securing both the wired and wireless access layer together as a single infrastructure. Security concerns don't stop after a user or a device is granted access to the network; a secure network must provide continuous monitoring of the wired and wireless infrastructure as well as automatically deal with threats in real time as they arise.

Utilizing an authentication system, network access control (NAC) products, as well as an integrated centralized management and monitoring system, the Enterasys solution offers complete ability to automatically enable threat containment and threat mitigation regardless of where or how the user or the device is accessing the network. As an example, a personal iPad might be allowed onto the network to gain Internet access but be restricted from communicating with any of the key corporate infrastructure components.

Security is enhanced via the Enterasys role-based policy control, which is integral to the wired and wireless switching infrastructure. Policies are created once on the centralized Enterasys NMS and then propagated to the edge of the network and enforced right at the point of ingress on the wired switch or the wireless access point. Once the policies are created, which includes both security and quality of service attributes based upon user and device type, the entire system is completely automated and enables the IT administrator to guarantee a consistent, secure network experience across the entire network infrastructure.

### The Multidimensional Approach

Today's unified access layer of wired and wireless services requires a multidimensional approach to deliver the service-level and security protection demanded by enterprises and educational organizations. Enterasys offers a full complement of integrated networking solutions ensuring the highest level of resiliency and availability to business services without sacrificing security and performance.

The entire network can be managed via an integrated wired/wireless management solution that runs as a virtualized management application with mobile access to provide anytime, anywhere visibility and control. Enterasys provides great flexibility for supporting wireless in the cloud by embedding intelligence into its access points, which enables the wireless LAN controller to reside anywhere in either a private or public cloud where it can be self-managed or managed by a third-party wireless services provider. The role-based policy management system is integral to the entire wired and wireless network, providing a secure network starting right at the point of ingress.

By automatically detecting and authenticating devices, Enterasys supports all types of network devices and fully enables a BYOD program while maintaining network security. Since the AP and the controller are covered by a lifetime warranty, an Enterasys WLAN solution also minimizes total ownership costs.

---

**For more information about the Enterasys solutions described here, please visit [www.enterasys.com](http://www.enterasys.com) or call Enterasys at 978-495-6824.**