

# 802.11n

---

# *Challenge*

**MAY 2010**

Produced by  
Layland Consulting,  
Joanie M. Wexler & Associates,  
and Webtorials



# 802.11n

## Challenge - 2010

Comparison Shopping for 802.11n ..... 3



Automated Wired and Wireless

Networking .....7

### THE CHALLENGE SERIES

#### Produced By

Layland Consulting, Joanie M. Wexler & Associates, and Webtorials, a venture of Distributed Networking Associates, Inc. Greensboro, N.C. [www.webtorials.com](http://www.webtorials.com)

#### Editor/Publisher

Steven Taylor  
[taylor@webtorials.com](mailto:taylor@webtorials.com)

#### Production Coordinator, Design/Layout Artist

Joanie Wexler, David DeWeese

#### Copyright © 2010

Distributed Networking  
Associates, Inc.

#### 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.

## Comparison Shopping for 802.11n

### *What differentiates the Wi-Fi vendors?*

By Robin Layland  
President  
Layland Consulting



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



The official IEEE 802.11n standard was ratified in September 2009, several months after we published our last wireless industry challenge. Since then, enterprise investments in older 802.11a/b/g technologies have quickly dropped off. The competitive ground is currently all about 802.11n, which increases Wi-Fi connect rates by nearly 6 times and actual throughput by nearly 8 times per radio, depending on infrastructure implementation and the client devices in use.

Fortunately, 802.11n systems remain backward compatible with legacy 802.11a/b/g client devices. This allows enterprises to migrate client connections to the more robust 802.11n over time through attrition, as they naturally replace end-user mobile devices. But despite the generations of Wi-Fi technology being interoperable, there are other migration issues that enterprises must plan and budget for. Among them are possible upgrades or new investments in the following areas:

- Controller backplane capacity (in controller-based Wi-Fi implementations)
- Ethernet switch port speeds
- Power-over-Ethernet switch and/or power injector technology
- RF management tools and spectrum analyzers
- New access points (APs) and/or controllers that architecturally handle 802.11n's significantly increased traffic loads in more efficient ways
- Performance benchmark testing tools and/or services

The reason is that aside from just new Wi-Fi technology needed in APs and clients, getting the most from an 802.11n network requires other parts of the IT environment to scale in tandem so that they don't become a choke point. Many of the Wi-Fi vendors participating in this challenge differentiate themselves by addressing some or all of these migration issues, which all contribute to enterprises' ability to ensure wireless performance reliability for end users.

## Making Wi-Fi Like Ethernet

Now that Wi-Fi is becoming a primary LAN access network in many organizations, enterprises want their mobile networks to rival the reliability of wired Ethernet networks. This is a challenging goal when the medium is a shared one, rather than a switched one with dedicated bandwidth, and consists of interference-prone radio frequency (RF) channels instead of a cable snugly affixed at two connecting end points.

As such, Wi-Fi makers are under the gun to show that their systems can maintain 802.11n's average 120Mbps to 170Mbps per-radio throughput reliably enough that the user experience is as close to wired Ethernet as possible.

This is a key area where the suppliers differ. Vendors will discuss at length how their systems diverge architecturally in terms of where they put data plane, control plane, and management plane functions, in large part to ensure reliable performance levels. Ironically, the industry that unleashed large-scale Wi-Fi into the enterprise by creating smart, centralized management controllers that could automatically provision large volumes of relatively simple, distributed radio access points is now doing something of an about-face. Vendors are once again pushing many more functions out into the APs to avoid congestion at centralized controllers and sidestep the distance-induced latency that results when traffic flows from AP to controller and back to AP.

The vendors do not all agree whether functions should be distributed or even which ones should be. The variance on what degree functions are centralized or distributed is one of the key issues that comes up in this challenge. There is no perfect answer to the question, as all sides make compelling arguments. For example, many of the controller-based Wi-Fi vendors have addressed the bottleneck issue with revamped hybrid or newly distributed architectures that balance – or allow you to select how you balance – traffic-forwarding functions and, in some cases, control plane functions.

### What's Fueling 802.11n Adoption?

Ratification of the IEEE 802.11n standard last September was a primary motivator for enterprises to fully embrace the technology. There are other drivers, as well.

For example, product prices are falling to rival those of 802.11g, making the choice of 802.11n more or less a no-brainer. Some dual-radio enterprise-class 802.11n access points (APs) have come onto the market in the \$600-\$700 price range, delivering 802.11n benefits at 802.11g prices. Single-radio 802.11n APs are available for less than \$500, though the dual-band option will be preferable to most organizations. The reason is that the single-radio devices on the market today tune to the noisy 2.4GHz band, where channel-bonding capabilities aren't available and where older devices slow down 11n radios.

Finally, 802.11n is turning into a primary data access network, and desktop phones are disappearing in favor of Wi-Fi-enabled handsets. Video and social networking applications are increasing the need for bandwidth, QoS, and reliability across the airwaves to users' mobile devices. It all adds up to the need for 802.11n standard technology and the vendor innovations that sit on top of it.

Another big emphasis is on improving wireless resource management and spectrum analysis tools to battle interference, which has a big impact on being able to deliver reliable throughput at range in an Ethernet-esque fashion. Spectrum analyzers scour Wi-Fi frequencies for sources of interference to provide network administrators with visibility into the conditions of the airwaves. By knowing what kinds of devices are out there and where, IT can keep the air as uncluttered as possible, all to help wireless emulate wired Ethernet to the optimum degree.

### Our Challenge to the Industry

To help you evaluate potential 802.11n suppliers for your organization, we have brought together six leading enterprise-class 802.11n network system vendors:

- [Aerohive](#)
- [Bluesocket](#)
- [Cisco](#)
- [Enterasys](#)
- [Motorola](#)
- [Trapeze Networks](#)

We have challenged these companies to articulate to you, in the following pages, why they should be your 802.11n 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.

Part 2 of this challenge will involve a series of multivendor panel discussions among the participating vendors that we will moderate. These will be available at no charge in Webcast (audio) format at the Webtorials site in June 2010. A number of the evaluation issues outlined below will be discussed in more depth during these sessions in a conversational roundtable among the sponsors and us.

### Key Evaluation Criteria

Among the issues we recommend considering when evaluating 802.11n suppliers:

- **Architecture.** Does the system distribute or centralize data forwarding, QoS, security and other functions – or a little of both? How scalable is the solution, and what kind of business continuity failover capabilities are built into it?
- **Throughput Reliability.** While 802.11n generally offers 300Mbps connect rates per radio, vendor products differ in the actual throughput they deliver reliably at range. The number of radios supported in an AP is a consideration. In addition,

many vendors offer features above and beyond the 802.11n standard to boost throughput and keep it reliable.

- **Wireless Resource Management Tools.** Does the system automate site survey tasks for planning your network design? Can it alert you to potential problems and interference sources in the environment? How does it handle RF management to avoid interference?
- **Power Requirements.** Can a vendor's 802.11n AP work with the 12.95 Watts of power provided by the widely installed 802.3af Power-over-Ethernet (PoE) standard or do they require an upgrade to higher-power 802.3at-2009 switches or injectors? Compare what functions and features across systems that operate within the 802.3af power budget to determine what, if any, functions a given vendor might sacrifice when using the lower power levels.
- **Voice and Video.** Does the gear support any algorithms beyond the 802.11e quality of service (QoS) standards to optimize real-time voice and video sessions? What are they and how effective are they?
- **Location Capabilities.** Does the system have a location engine and applications – either from the Wi-Fi vendor or a partner – to gather and correlate location data and deliver it for use in a meaningful way, such as to asset tracking or E911 applications?
- **Security.** Does the system have any additional security features, such as built-in firewalls and wireless intrusion detection/prevention systems (WIDS/IPS)? How are policies and user profiles set and do they interface with your existing policy engine?
- **TCO.** The total cost of ownership, of course, is a factor in every enterprise IT decision. Besides the normal cost of equipment and licenses, make sure to consider any automated tools embedded into the system and the associated opex savings they provide.

This is just a sampling of issues to consider when comparing 802.11n solutions. We asked the participating 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 what they have to say, then contact them about issues you consider important that they didn't mention.



# Automated Wired and Wireless Networking

## *No Network Overhaul Needed For 802.11n*

By William Glynn  
Senior Product  
Marketing Manager  
Enterasys



---

### The 'Two-Network' Problem

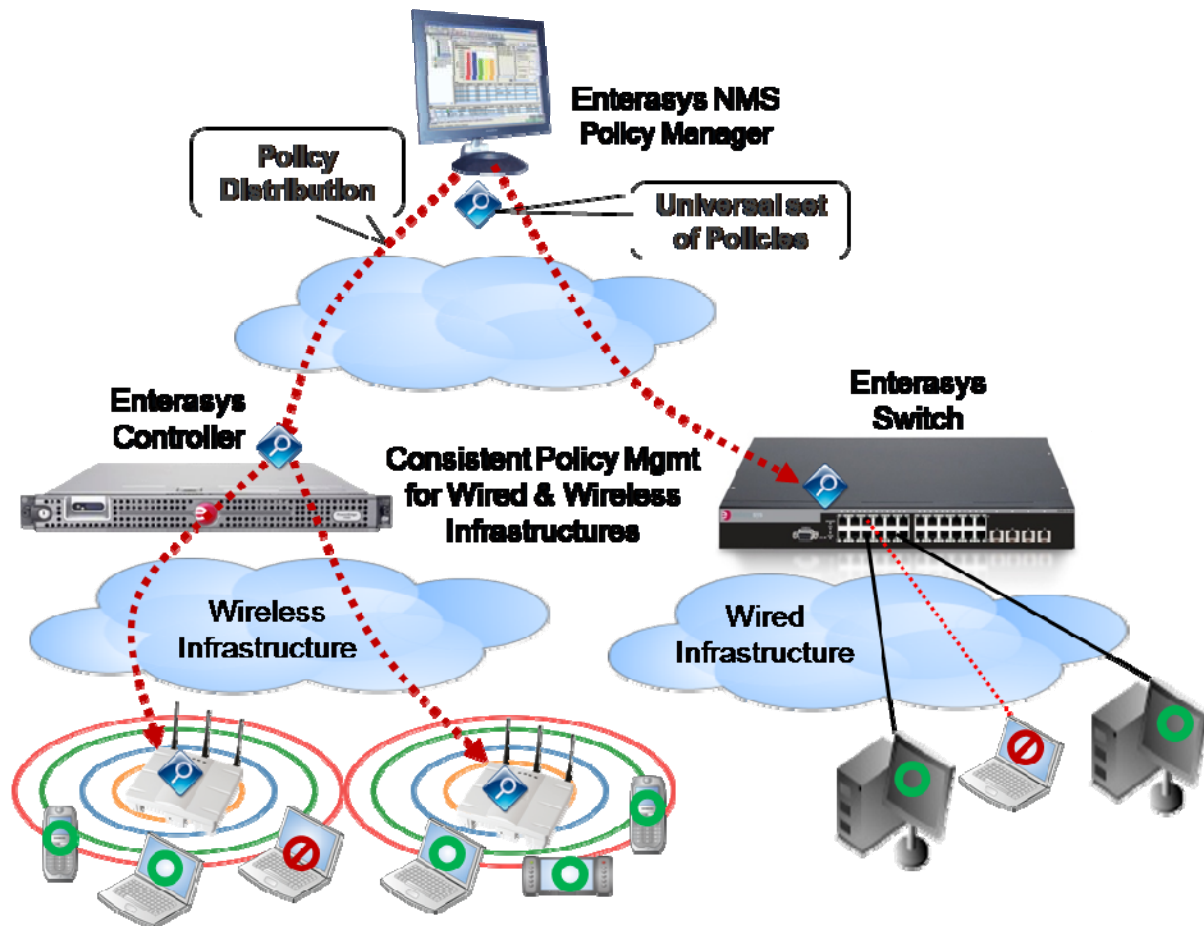
Enterprise networks typically comprise both wired and wireless LANs and provide network access for both office-bound and mobile workers. Unfortunately, these infrastructures are usually managed as two distinct networks, a practice that dramatically increases operational costs and unnecessarily complicates network security. Further, enterprises have an insatiable appetite for wireless, which, along with the recently standardized 802.11n technology, exacerbates this "two-network" problem.

So although 802.11n delivers numerous operational advantages related to capacity, bandwidth, wireless coverage, and signal quality, it also conjures up the image of expensive and disruptive upgrades to both the wired and wireless infrastructures. Not to worry, however: a simple and cost-effective 802.11n upgrade can be accomplished without having to re-purchase and re-install the entire network. In fact, a wireless LAN upgrade also presents an opportunity to create, or at least lay the foundation for, a single integrated wired/wireless network with automated network management that significantly reduces operational complexity and costs.

### Automated Single-Policy Management

Enterasys has taken a leadership role in integrating wired and wireless LANs. The two network infrastructures can be managed and secured as a single entity to significantly simplify network management and deliver ongoing operational cost savings. An Enterasys wired/wireless solution provides the ability to create global, role-based priority and access policies that are universally applied across the entire infrastructure and are enforced directly at the point of network entry (see diagram, next page).

In other words, automated single-policy management ensures the same superior user experience whether the user attaches via a wired or wireless connection while also reducing network management complexities and improving network security. Enterasys Wireless solutions uniquely simplify wireless connectivity by reducing IT administrative workload and operational costs by automating connectivity tasks, streamlining network management procedures, consolidating IT security functions, and boosting overall 802.11n performance.



***Policies are created once and then automatically distributed and applied to both the wired and wireless infrastructures.***

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.

Consider that the ratio of network operations staff to users for an Enterasys network is typically 1 staff member for every 2,000-5,000 users. This compares quite favorably with a typical industry ratio of 1 staff member for every 200-500 users and enables the redeployment of key personnel to more strategic projects in the enterprise.

### **Easy Migration to 802.11n**

An 802.11n upgrade using Enterasys Wireless access points does not require new Ethernet switches with the higher-powered 802.3at Power over Ethernet (PoE) capabilities or the addition of costly midspan power injectors. Unlike competitive offerings that require up to 30 watts of power, Enterasys Wireless provides a fully powered and fully featured 3x3 MIMO 802.11n solution via an existing 802.3af PoE

connection (the same connection type used to power today's 802.11a/b/g access points). Enterasys consumes less than 15.4 watts of power and provides measurable savings on energy costs.

The ability to reuse the existing switching infrastructure means that an Enterasys Wireless 802.11n network upgrade primarily consists of deploying only new 802.11n access points, thus minimizing capital expense. By leveraging the existing 802.3af PoE infrastructure and providing specialized mounting hardware that enables new access points to be quickly affixed to existing mounting brackets from other wireless vendors, Enterasys makes the physical installation both a time- and cost-effective procedure.

In addition, to further simplify the deployment process, Enterasys Wireless access points use multiple automated broadcast discovery modes to interoperate with the existing DHCP infrastructure and provide features showing a visual indication of signal strength to enable easy antenna adjustment and maximize signal strength. All told, Enterasys access points can be automatically discovered, configured, and optimized without cumbersome manual steps, saving significant time and effort for the networking staff. Once deployed, an Enterasys 802.11n WLAN operates as an integral and seamless component of the overall enterprise network.

By providing a fully powered, dual-radio, 3x3 MIMO 802.11n solution via an existing 802.3af PoE connection, along with automated management, Enterasys Wireless is the most cost-effective, energy efficient, and easily deployed 802.11n upgrade solution on the market today.

### **Flexible Architectural Modes**

Most WLAN vendors force their customers to preselect either a distributed or centralized operational model and then lock the customer into that choice, sometimes forcing different product selections. However, Enterasys Wireless doesn't require such a choice.

Intelligent access points enhance the WLAN component of the integrated wired/wireless network and align WLAN operations with enterprise needs by providing 802.11a/b/g/n capabilities for both distributed and centralized network deployments. In addition, customers can simultaneously support both operational models without the complex, time-consuming reconfigurations required by other wireless solutions. This flexibility enables customers to optimize the distribution of the processing load between the access points and the controller to deliver exceptional performance in line with business requirements, while the WLAN environment remains easy to manage.

### **Price/Performance Leader**

Enterasys has set the benchmark for a low-cost enterprise 802.11n access point with dual radios starting at \$685, including a comprehensive lifetime warranty. Benefiting from the comprehensive lifetime warranty that protects their investment, Enterasys customers can save \$140,000 in maintenance fees over the life of the equipment compared to a competing 200-access point deployment. Combining its automated network management features with its comprehensive lifetime warranty, Enterasys Wireless provides the most cost-effective 802.11n upgrade solution from all perspectives, including capital expense, installation costs, operational expense, and overall investment protection.

**For more information about the Enterasys solutions described here, please visit:**  
<http://www.enterasys.com> or call Enterasys at 978-684-1000.