802.11n *Challenge*

MAY 2010

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

802.11n

Challenge - 2010

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

Editor/Publisher
Steven Taylor
taylor@webtorials.com

Production Coordinator, Design/Layout Artist
Joanie Wexler, David DeWeese

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.

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.

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.

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.

How Cisco Protects 802.11n Network Performance

Not all Networks Are Created Equal

By Dimitris Haramoglis
Marketing Manager
Mobility Solutions
Cisco

To the casual observer, 802.11n products may seem similar from supplier to supplier. Indeed, all vendors offer support for base-level functionality such as Multiple Input Multiple Output (MIMO), 40MHz channels, and packet aggregation. It's only when you start putting vendors to the test that you begin to see the differences in performance. In recent performance testing, Cisco wireless consistently delivered higher throughput at any distance from the access point compared with the competition, and the performance gap increased significantly with distance from the access point.

Still, 802.11n throughput is just one attribute to consider. Companies need to guarantee that same high level of performance to all their users, and not all solutions deliver in the same way. There are three major trends currently impacting the user experience:

- A mix of 802.11a/g/n clients operating at different speeds
- Proliferation of video traffic
- Growing sources of interference

Cisco has solutions for dealing with the performance challenges caused by each of these issues with its ClientLink, VideoStream and CleanAir technologies, respectively. Let's take a look.

Challenge 1: Mixed-Client Environment

Mobile users have a variety of devices at their disposal. Many of those are and will remain legacy 802.11a/g devices for two reasons. First, client refresh cycles do not necessarily align with network refresh cycles. Second, device vendors still produce devices using non-802.11n radios to contain costs and to increase device battery life.

However, because legacy clients "speak" to the 802.11n AP at much slower rates than 802.11n clients do, the whole system is impacted, effectively deteriorating the performance of 802.11n clients. The problem is further exacerbated as the distance between the access point and the legacy device increases. To help ensure performance protection, companies need to deploy an 802.11n wireless network that can provide bandwidth fairness for existing 802.11a/g devices and newer 802.11n devices.

Cisco Solution to Mixed-Client Environment: ClientLink

Cisco ClientLink technology helps solve the problems of mixed-client networks by making sure that older 802.11a/g clients operate at the best possible rates, especially when they are near cell boundaries. Unlike most 802.11n access points, which only improve the uplink performance, Cisco ClientLink technology improves performance on both the uplink and downlink, providing a better user experience. It uses advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11a/g clients in the downlink direction without requiring feedback.

By providing "more bars anywhere," ClientLink extends the useful life of existing 802.11a/g devices and ensures that all clients on the network, regardless of type, are guaranteed the bandwidth and throughput they need, reducing trouble tickets and helping you realize a faster ROI on your 802.11n network.

Challenge 2: Video Everywhere

Video is truly changing how employees collaborate; how executives communicate key information to employees, shareholders and financial analysts; how businesses communicate with their customers, and how training or educational content is delivered.

As more mobile devices are optimized to deliver rich media and video to users, and video consumption grows ubiquitous, the delivery of video over wireless is becoming even more challenging. Streaming video to multiple devices over the wireless network poses several problems. One is flooding the network even when there is no demand for the content. The result is poor video quality due to lost packets. Performance of other mission-critical applications deteriorates, too, because streaming consumes valuable bandwidth and limits the number of users that can effectively connect to the wireless network. To protect performance, companies need to deploy an 802.11n wireless network that can deliver high-quality video to the mobile user with the same performance and reliability that a wired network provides.

Cisco Solution to Video Proliferation: VideoStream

Cisco VideoStream is a set of features of the Cisco Unified Wireless Network that optimizes the performance of multimedia over the wireless and wired network, as part of Cisco medianet, an intelligent network optimized for rich media. It removes the challenges associated with streaming video over the wireless network by delivering reliable multicast, the enforcement of video priority levels and resource reservation control. These help ensure the quality of existing wireless media sessions is maintained as additional wireless video streams are added to the network.

Based on independent testing performed by Miercom, Cisco VideoStream technology significantly improves the scalability of wireless video delivery by utilizing less bandwidth than the competition and reducing latency and packet loss rate, which results in "the most efficient delivery of standard and high definition media streams" over wireless, according to Miercom.

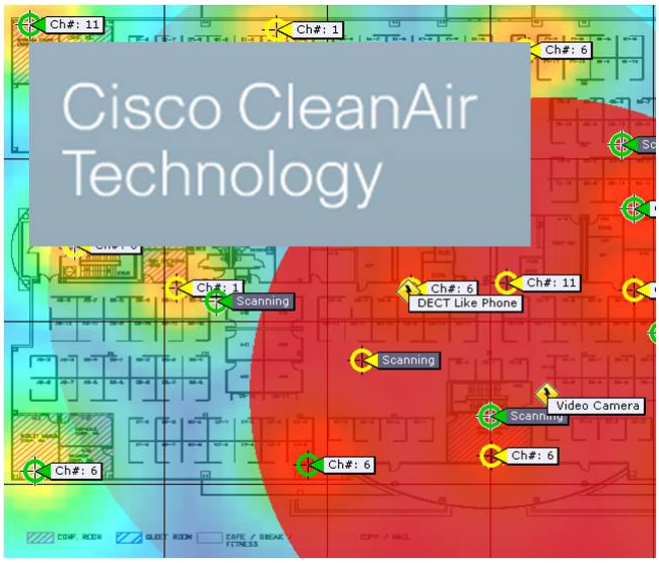
Challenge 3: Interference Threats

Wi-Fi's success is partly attributed to the fact that it operates in an unlicensed spectrum, making the systems readily available to any company interested in building solutions. However, this same benefit also means that manufacturers are building more and more devices that use these unlicensed frequencies for communications. Many of these new devices are using radios operating in the same frequency that can interfere with your 802.11n network.

Bluetooth devices, microwave ovens, cordless phones, neighboring wireless networks and video surveillance equipment are just a few examples of interference that can shut down your wireless network and halt business productivity. Interference can also be malicious and originate from hackers that launch network attacks with jammers or rogue access points. To guarantee performance protection, IT managers need to have visibility into the spectrum to prevent unexpected downtime.

Cisco Solution to Interference: CleanAir Technology

CleanAir technology is an industry first and uses silicon-level intelligence to create a self-healing, self-optimizing wireless network that mitigates the impact of wireless interference and optimizes 802.11n network performance.



Cisco CleanAir technology locates and shows the impact of interference sources within the network

While other companies make claims about interference detection and handling, only Cisco has invested in creating a CleanAir radio ASIC embedded into the access point to detect and classify wireless interference sources while simultaneously serving network traffic. As a result, the system produces far more granular interference visualization than standard Wi-Fi chipsets. This enables more intelligent decisions and policies for automatic remedial action and faster troubleshooting across the entire network due to its system-wide integration. It can also provide historical views of interference and the flexibility to reconfigure access points as sensors to analyze RF remotely. By handling spectrum analysis in hardware, access points can simultaneously serve traffic and maintain air quality without any performance impact. The net result for IT is a wireless network that understands the impact interference is having on wireless performance and can take automatic steps to mitigate that impact.

Performance: More than Just Mbps

If you are about to evaluate an 802.11n wireless network, you are probably getting ready for vendor bake-offs and most likely performance vs. price is one of your key decision metrics. This is the right approach, as long as “performance” includes more than just Mbps and “price” represents the total cost of ownership. Performance should be measured to reflect the realities of your business requirements, and these will more than likely include scenarios such as the ones described above. Namely, a mixed-client environment where wireless video is consistently increasing in use and the user experience is affected by interference from other devices.

The Cisco Unified Wireless Network provides the solution to all these problems through technological superiority such as ClientLink, VideoStream and CleanAir technology, which build on the Cisco Aironet heritage of RF excellence – a heritage built through the years on a combination of engineering talent, silicon development, antenna design, software and product design, and an unwavering focus in leading the access market, whether wired or wireless.

For more information about Cisco’s solutions described here, please visit:
http://www.cisco.com/go/wireless

Automated Wired and Wireless Networking

No Network Overhaul Needed For 802.11n

By William Glynn
Senior Product Marketing Manager
Enterasys

The 'Two-Network' Problem

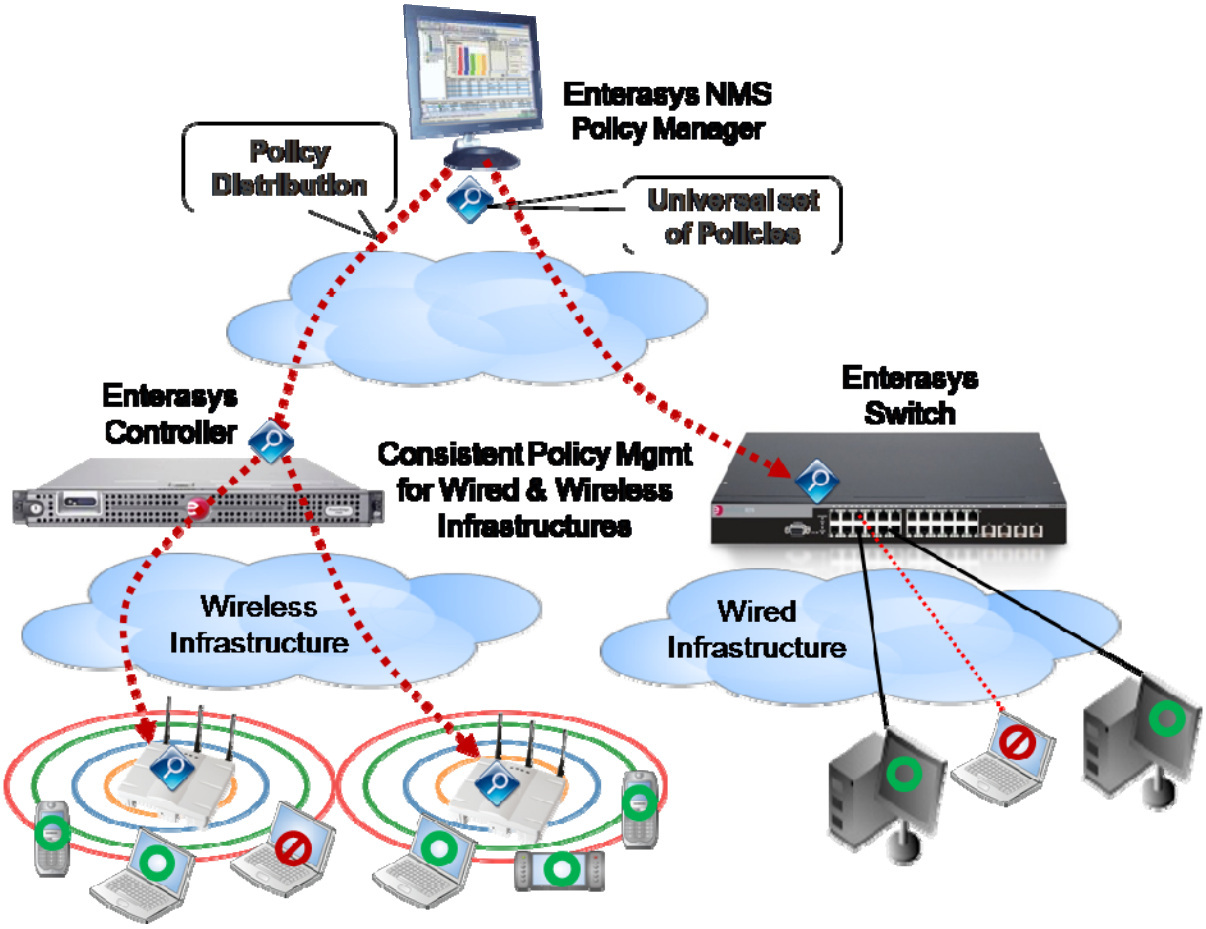
Enterprise networks typically comprise both wired and wireless LANs and provide network access for both office-bound and mobile workers. Unfortunately, these infrastructures are usually managed as two distinct networks, a practice that dramatically increases operational costs and unnecessarily complicates 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.

A Truly Distributed, Virtual Architecture

- *Zero Failover and Zero Packet Loss*
- *Optimized Performance*
- *Scalability*
- *Tighter Edge Security*

By Patrick Foy
VP of Engineering
Bluesocket, Inc.

WLAN® 802.11n is a distributed architecture that supports decisions at the edge of the network and control at the core of the network in a centralized appliance or server. This solution is a fully distributed architecture where no user traffic is forwarded to the centralized controller. Security, quality of service, and mobility are not compromised – vWLAN® provides these traditionally centralized data features at the edge of the network.

The use of "smart" 802.11n access points allows forwarding of data traffic directly to the wired network and frees enormous capacity within the wireless controller. More capacity means the vWLAN® can deliver enhanced wireless management and control performance with far less dedicated hardware. Distributing the data plane in the APs offers significant advantages over architectures that keep the data plane in the central controller (see table).

Capability	Distributed Data Plane	Centralized Data Plane
System Capacity	Over 300Gbps (across all APs in a 1500-AP installation)	Typically 20-30Gbps (in a single-controller, 1500-AP installation)
Failover	Zero-Second / Zero Packet Loss	Multiple Seconds
Security	Trust Boundary at the Edge	Trust Boundary at the Core

Every device in your network adds to your operating expenses – cost to install and manage it, cost to power it, cost of maintenance fees, cost of upgrading, and eventually cost to dispose of it. Then add redundancy on top of it. The desire to minimize hardware and virtualize the solution has become less of a fashion statement and more of a business requirement.

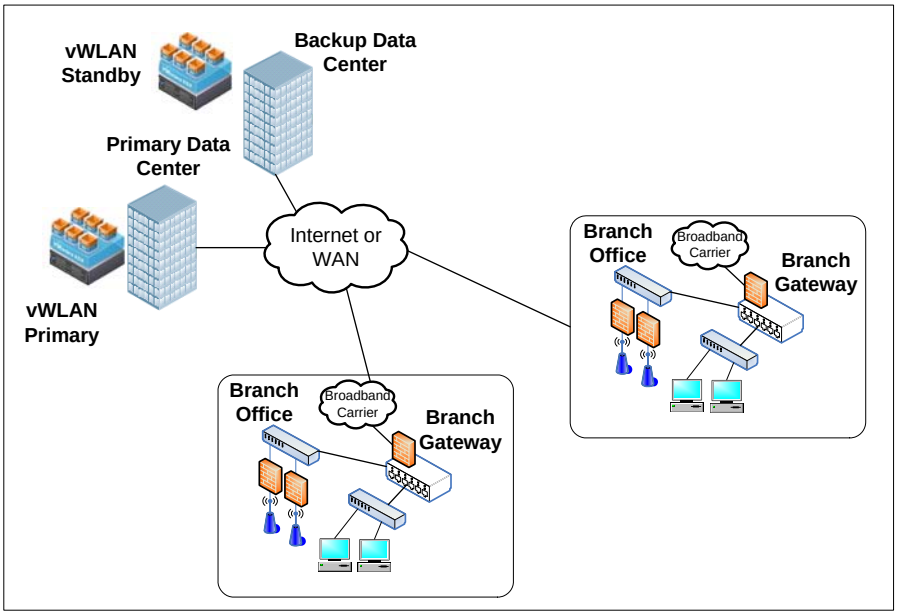
vWLAN® solution is abstracted from the centralized controller hardware and is being packaged as a virtual machine that can be deployed on the existing servers of larger technology vendors, on VMware or on a vWLAN® appliance. A software-based controller greatly simplifies expanding, reconfiguring, and managing the network, resulting in significant ongoing costs savings for customers. Maintaining your wireless solution should not consume all your time. We believe it's possible to do more with less when it comes to your network deployment.

vWLAN® Advantages

• ***Zero Failover and Zero Packet Loss.*** vWLAN's high availability guarantees that users never experience service disruption and their session information is maintained during a failover event. It's a zero-failover-time with zero-packet-loss solution. Since user traffic is no longer flowing through the centralized controller, the APs continue passing traffic when the primary vWLAN® fails. Bluesocket's smart APs establish a connection to a secondary vWLAN® and automatically synchronize client information while continuing to pass user traffic. Users are unaware a failure occurred in the system. When the primary vWLAN® is back online, the APs transition from the secondary to the primary vWLAN® with no packet loss.

vWLAN's primary and backup can be deployed anywhere in the network as long as there is network connectivity to the APs. For example, vWLAN's virtual machines can be deployed at geographically separated datacenters, and APs at branch offices auto discover the vWLANs at the data center.

The zero-packet loss high-availability scheme also enables seamless software upgrades to the system. Instead of scheduling a maintenance window to perform a software upgrade on the appliance, the secondary vWLAN® can be upgraded, and then a forced failure can be performed on the primary vWLAN® so that all the APs transition to the secondary vWLAN®. After the primary is upgraded, all the APs automatically return to the primary – again without disruption to the user.



vWLAN's high-availability scheme with zero downtime is suited for mission-critical environments that cannot afford to have their network go down for even a second.

• ***300Gbps of System Throughput.*** With vWLAN® 802.11n, system capacity is no longer computed by the backplane capacity of the hardware-based controller; rather, it's determined by the aggregate throughput of the APs. For example, in a 1500-AP deployment with 802.11n APs, each capable of forwarding over 200Mbps of traffic, the vWLAN® system capacity is over 300Gbps. This number demonstrates a revolutionary change from centralized WLAN solutions whereby each controller typically has 20-30Gbps data plane capacity.

• ***Optimized Performance.*** vWLAN® offers many class/quality of service components including bandwidth management, admission control, packet prioritization, and load balancing to assure each user's traffic is handled appropriately to provide the highest performance.

Bluesocket's Over the Air Fairness algorithm allows an administrator to influence airtime usage based on the identity of the end user or device. In the Bluesocket™ solution, all classes of users and devices share the media prioritized based on the administrator's configurations. Data isn't just distributed to the APs; it's also distributed between users and devices within the AP.

Performance is not only designed into the vWLAN® architecture. It's also designed into the hardware. Bluesocket's BSAP-1800 won **Network World's Clear Choice award** for overall best 802.11n Enterprise AP. The BSAP-1800 includes a patent-pending embedded MIMO antenna, which eliminates dead spots and offers higher system performance. Bluesocket's superior antenna technology is optimized to provide maximum coverage.

• ***Scalability.*** vWLAN® scales to 1500 APs on a single vWLAN® appliance with seamless L2 and L3 roaming between any AP in the system. Adding APs to the system doesn't require a reconfiguration of the WLAN network; rather, it's as simple as installing APs and applying additional AP licenses to the vWLAN® appliance. The only way to future proof yourself in an environment so saturated with technologies is to work with a vendor that has a flexible solution that can easily expand as you build out your WLAN.

• ***Tighter Edge Security.*** In vWLAN®, a user's role is determined by his or her identity. User roles are managed by the central control software but are enforced by the AP. The roles contain multiple attributes including service policies, VLAN/subnet assignment, bandwidth, and QoS. A single SSID can be used to support multiple roles, eliminating the need to manage multiple SSIDs. Each user role can have an associated schedule, which determines when the role is active (date and time). This is particularly useful for guest users or in a facility that has specific operating hours; for instance, between 9am and 5pm.

Bluesocket's Guest Access is the most extensive secure guest access solution on the market including a built-in guest manager for front-desk administrators, hotspot billing for automatic account generation, and Friends and Family so authorized users can create accounts for their guests. The guest access solution also enables guests to create their own account and then the system will email their login credentials to them. Using their iPhone or Blackberry, users can retrieve the login credentials and securely log in to the wireless system.

BlueProtect™ is Bluesocket's integrated endpoint client scanning solution. With BlueProtect™, you can be confident that client devices connecting to the corporate wireless network are safe and will not introduce threats into the network environment. Managed via the administration GUI of vWLAN®, BlueProtect™ allows IT staff to monitor, control, and enforce policies relating to anti-virus, anti-spyware, firewall, files/registry, OS/patch level, and peer-to-peer applications. The BlueSecure W-IDS is integrated into vWLAN® and is used to identify and contain rogue APs and a host of WLAN DoS and spoofing attacks that threaten the security of your network.

Summary

The turnkey vWLAN® 802.11n solution produces incredible improvements in throughput, reliability, and availability. vWLAN® 802.11n offers the complete range of integrated wireless features into one flexible architecture. Bluesocket™ is committed to delivering excellence in wireless solutions today that are scalable to future advances in technology.

For more information about the Bluesocket™ solutions described here, please visit: http://www.bluesocket.com/ or call Bluesocket™ at 1-781-328-0888

802.11n: The Beginning of the End of Controllers

By Devin Akin
Chief Wi-Fi Architect
Aerohive Networks

Reliability at Mach-3

Today's leading analysts agree that reliability is the most prevalent concern among consumers of Wi-Fi technology. As prices have fallen and capabilities have grown, Wi-Fi technology has moved from convenience to mission-critical – sometimes life-critical. In addition, the variety of applications, each with its own requirements, found in today's enterprise is staggering.

Creating Wi-Fi that "just works" even with minimal requirements, is a tall order, but due to 802.11n, vendors are now under tremendous pressure to create Wi-Fi that "just works at Mach-3." Various kinds of video, high-density client environments, bad RF environments, VoIP, high throughput, branch office networking, resilient mesh, location tracking, and a broad range of client and application compatibility are just a *few* areas where vendors are currently investing their time. From the 50,000-foot view, one might marvel at how a technology so complex and broad reaching can keep the wheels from falling off, much less work reliably. Consider that a 1975 Chevette can hold together at 40 mph, but going 8X faster would be a different story.

Realistically, 802.11n supports 8 times the throughput of 802.11a/g. More is possible, but 8 is a reasonable multiplier in most cases. Why does it matter? With all of the traffic that 802.11n will be able to support, controllers will suddenly be a significant bottleneck. 802.11n's capacity will necessitate controller upgrades and often Ethernet infrastructure upgrades as well. To put this in perspective, suppose you have a little water in your basement. It may be irritating, but it's likely bearable. If you have 8 times as much water, it's time to call a contractor to make some major repairs. A multiplication factor of 8, when you're talking about client traffic over a wireless infrastructure, can be the difference between "anyone can do it" and "almost nobody can do it."

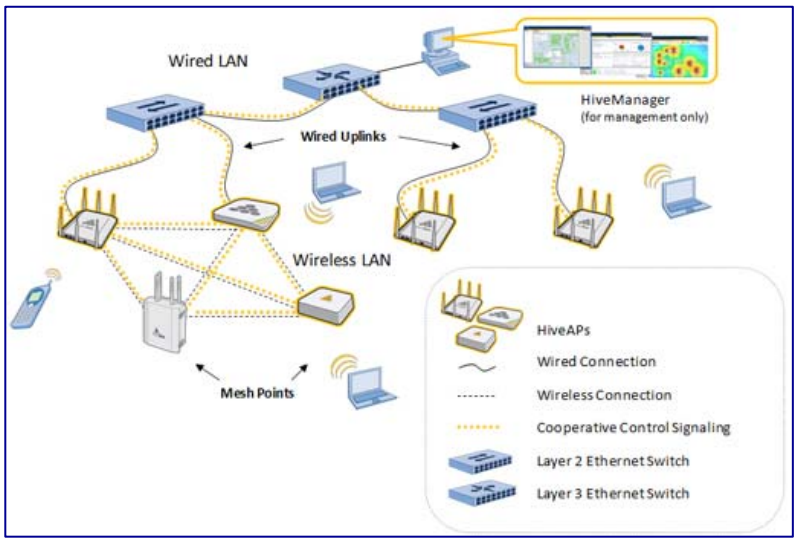
A House Built on Sand

Now that I've painted the bleak picture that is reality, let's make it worse. What if we connected all Internet routers into one giant router, and just because we don't want a single point of failure, we make that router redundant. Besides the fact that these two routers would cost a gazillion dollars, does this architecture make sense from a scalability or availability standpoint?

It's a rhetorical question. The Internet (the most spectacular example of a resilient network) and your routed and switched LAN are built on distributed intelligence for linear and unlimited scalability and maximum availability. Why would you want your Wi-Fi infrastructure to be different? So, I'm saying that today's de facto standard, controller-based architecture is nowhere near reliable or resilient enough for tomorrow's mission-critical application support and introduces single points of failure. The entire model is a house built on sand…

Solution: A New Architecture

Enough about the problems already. Let's now focus on the solution. Placing the data and control plane intelligence into each AP means that you can leverage the CPU horsepower of each AP to process QoS, encryption/decryption, firewall rules, and all other Wi-Fi functions at the optimum point: the network edge.



As an example, suppose a 10-lane highway (gigabit Ethernet) changed abruptly into a variable-lane highway of 1-4 lanes (Wi-Fi). Would you try to coordinate (microsecond-by-microsecond) cars from a 10-lane highway onto a variable-lane highway at the point where they meet or 2 miles upstream? Likewise, would you try to coordinate frames from gigabit Ethernet onto a congested Wi-Fi medium at the controller (20 ms upstream) or at the AP, where the interfaces meet?

Fully distributed intelligence also means having the ability to leverage an AP's Ethernet connectivity speed through distributed data forwarding and removal of the "operational modes" that are so prevalent among controller-based vendor implementations. An AP should be able to dynamically adjust to any role (portal, mesh, branch, etc.) or environment, while offering its full range of features. Keep in mind that distributed forwarding doesn't equal controller-less. Many of today's Wi-Fi controller vendors support distributed forwarding, but in order to use this function, sacrifices must be made. Bypassing the controller has consequences.

Aerohive's solution implements the control plane as software operating between APs, introducing added resilience and security, decreased cost, and complete removal of bottlenecks and single points of failure.

Vint Cerf, VP and Chief Internet Evangelist at Google (and often called the "Father of the Internet"), said in a 2009 interview, "Part of my motivation when I was working on the Internet was exactly to build a system that did not have any central control. Recall that this was being supported by the US defense

department, and one of the things that the defense department wants is highly reliable and resilient system. One way to achieve that is to not have any central place that could be attacked and destroyed in therefore interfere with the operation of the net. So the consequence of this, I would say 'decentralized architecture' is that it is highly resilient to a variety of impairments and in consequence of that, it's very hard for anybody to shut the Internet down entirely."

To give you some perspective, consider that routing protocols are control protocols. Routers are autonomous, yet coordinate among themselves using routing protocols. Aerohive APs do likewise, enabling failover/failback, dynamic mesh routing with best-path forwarding, and a variety of other high-availability features. It's a fully distributed system, and it's Wi-Fi that won't die.

Bob O'Hara, who is on Aerohive's Board of Advisors and co-founded the first controller-based WLAN company, Airespace, recently stated, "The advantages to a fully distributed system are the ability to have a much more reliable system. You can have any single point in that network fail, and as long as the radio coverage is sufficient to cover the areas lost by that failed device, you still have full services, full connectivity." (Ref: http://www.aerohive.com/resources/multimedia/BobOHara_episode1.html)

Wi-Fi That Won't Die

802.11n's 8-fold speed increase, along with today's demanding applications, causes tremendous strain on controller-based networks. For this reason, every controller vendor will be forced to deploy a fully distributed solution sooner or later.

As an example, if you have 100 802.11a/g dual-radio APs that have a maximum possible throughput of 45Mbps (22.5Mbps per radio), then the total network capacity, under optimum conditions, is 4.5Gbps. Today's highest-end controllers can handle this much throughput, but only barely considering encryption/decryption, QoS, roaming clients, RF environment changes, and many other wireless network events. While controller interfaces may be faster than this, the controller CPU(s) is/are not. When you push this aggregate throughput up by 8X, you're at 36Gbps for 100 APs. This kind of throughput would take a large rack of controllers to handle. Now consider that many of today's larger enterprise Wi-Fi deployments can reach well over 5,000 APs. Yes, that's 1.8Tbps. Say goodbye to controllers.

Many controller-based vendors have already begun the long march toward re-architecting their solutions for a fully distributed architecture. It will take a significant amount of time, effort, and experimentation in YOUR network, but they will get there…or they will die trying. Why wait for other vendors to get there when Aerohive is already there?

…and in the immortal words of Paul Harvey: "Now you know the *rest* of the story."

For more information about Aerohive's solutions, please visit: http://www.aerohive.com/solutions or call Aerohive at (866) 918-9918.

NonStop Wireless for Always-on Enterprises

Delivering Scalability and Reliability other Vendors only Dream About

By Mark Cowtan
Director Marketing
Trapeze Networks

Trapeze Networks' 802.11n advantage comes from a highly distributed architecture designed for scalability and resilience. We knew back in 2002 Wi-Fi was going to be big, and as more and more workers embraced mobility, it was clear that scalability and reliability would become major considerations.

Although security concerns reigned the first few years of enterprise Wi-Fi, Trapeze, like most other vendors, trusted that IEEE standards would solve the issues in due course. So we contributed experts to steer, and in several cases chair, those IEEE sub-committees. However, it was evident that standards would likely not address the looming scalability and reliability issues. That's why Trapeze focused on those topics as well as management as our key areas for differentiation and value. To that end, Trapeze built a hybrid centralized/distributed architecture and has amassed a patent portfolio of 62 inventions (10 awarded, 52 pending) mostly related to seamless roaming and wireless resource management.

As you will shortly learn, our approach removes many of the performance, capacity, and reliability obstacles inherent to most vendor implementations. While a few competitors mimic some of our scalability features, only Trapeze has tackled both scalability and reliability and backed it up with world-class WLAN management.

Better Scalability Through Superior Resource Management

Don't confuse bandwidth with scalability: Although the now-ratified 802.11n standard increases per-radio bandwidth six-fold and actual AP throughput about 10 times, the standard itself does little to improve wireless network scalability.

The point is that network scalability has much more to do with resource management than data rates. Here's a simple example: Imagine you want to deploy wireless VoIP on a large scale, all across your facility or campus. A common best practice is use call admission control (CAC) to prevent too many clients from using the same AP, and thereby ensuring a minimum guaranteed bandwidth for each client, if they are all on voice calls. But what if they are NOT all on voice calls at the same time, which is mostly the case? Unfortunately, most CAC implementations are too crude to detect call state, so once the CAC limit is reached, they simply turn new or roaming clients away, regardless of how many existing clients are actually on a call. The fact is, unless they are all on calls at the same time, AP resources are wasted, while users are denied service. Yikes, that's not good!

In contrast, with a more dynamic CAC approach – one that can identify active calls rather than potential voice users – it is possible to easily quadruple the density of VoIP users that can be served by the same number of APs in the same footprint. That's scalability. You see, the failure in this example is not a shortage of bandwidth; it is the mis-management of the resources in a real-world context. More examples are illustrated in the table below.

Also on the topic of VoIP, as Session Initiation Protocol (SIP) makes its way into VoIP, systems need to inspect packets to distinguish voice calls from other traffic. Trapeze combines dynamic CAC with SIP awareness to detect active SIP calls, while simultaneously monitoring WMM signaling, and to differentiate them from non-SIP clients. The system then provisions resources appropriately for all client types. Special voice panels included in our management platform, RingMaster, provide great visibility on voice activity and service quality.

Don't Forget Wi-Fi is Shared Ethernet. Make no mistake: bandwidth is an issue too. From a performance standpoint, 802.11n, even with its 300Mbps connect rate, is a 15- to 20-year backwards step in time – before shared Ethernet became switched Ethernet. And why did switching happen? Because shared Ethernet performance falls off a cliff once critical mass of users/activity level is reached. Yet, in 2010 we're trying to put advanced services, such as VoIP, on a shared medium. Amazingly, it actually works! But for how long? The answer to that question has everything to do with each vendor's approach to resource provisioning and very little to do with 802.11n standards.

Problem	Implications	Trapeze Solution
Front door: Lots of people (e.g., students entering an auditorium) enter an area through the front door.	All active clients latch onto the nearest AP they detect, causing some APs to be overloaded, while others are idle.	**Client Load Balancing** spreads client sessions evenly over APs, giving each more consistent performance levels.
Transient hot spots: Some areas of the building get busy all of a sudden, while others are under-utilized.	The controller serving the busy APs must carry all the load and could get congested and degrade user experience.	**AP Load Balancing** dynamically assigns loaded APs evenly over ALL available controllers, resulting in more consistent performance under duress.
Network latency: Centralized forwarding, encryption, and security policy enforcement at the WLAN controller add round-trip latency and jitter.	Centralized architectures degrade voice quality, increasing the probability of marginal / unacceptable service.	**Distributed Forwarding** lets APs perform cut-through switching at the network edge, enabling voice traffic to take the shortest path.
2.4GHz Saturation: Most clients, especially phones, PDAs and industry-specific devices, default to 2.4GHz.	Causes over-subscription of the relatively narrow 2.4GHz band, while the wider 5GHz is largely unused	**Band Steering** (patent 7,577,453) transparently moves 5GHz-capable clients to 5GHz band, freeing up 2.4GHz for voice and increasing aggregate capacity 30-40%
Air time hogs: Legacy clients (802.11a/b/g) including all Wi-Fi phones, need more transmission airtime per megabit than 11n clients.	Legacy clients are bandwidth parasites. Their slow transmissions can block 11n client transmissions and degrade aggregate cell throughput.	**Weighted Fair Queuing** enforces airtime fairness between clients, which maximizes cell throughput and ensures timely servicing of high-priority traffic.
Session CAC: Once session-CAC limit is reached, AP cannot accept new clients, regardless of activity level.	Even when all clients on an AP are idle, new clients and roaming clients (including voice) get denied service.	**Dynamic CAC** only restricts new connections when the maximum number of active voice calls is reached and always accepts roaming calls.
Shared bandwidth: When many active users are on the network, average per-user bandwidth diminishes.	Applications that require minimum bandwidth guarantees may be starved, resulting in poor quality.	**Bandwidth Limiting,** combined with Weighted Fair Queuing, allows per-SSID or per-user bandwidth min / max, guaranteeing minimum service levels.

Even ignoring the added complications of dealing with RF, It is easy to see that Wi-Fi being a shared medium warrants more intelligent resource management. But when you consider deeply the networking implications of mobile users entering, moving around in, and leaving an area, the need becomes even more obvious. Several common problems that some vendors have ignored or simply cannot solve with their architecture are displayed in the above table.

By solving all these problems together, the Trapeze architecture maximizes per-user bandwidth availability for users when they initially connect and throughout the duration of their session as they roam seamlessly from AP to AP campus-wide indoors and outdoors. This ensures higher aggregate throughput for both Greenfield 802.11n deployments and mixed a/b/g/n deployments and does so at much lower total cost than other systems. The distributed architecture, which leverages the additive processing power of each AP, means we don't need such "big iron" WLAN controllers as those vendors who rely on centralized forwarding and security. And by combining the distributed architecture with intelligent resource management, we can handle higher densities of mission-critical clients without needing more APs.

Undisputed Reliability Leader

As mentioned earlier, only Trapeze has tackled both scalability and reliability and backed it up with world-class WLAN management. In fact, it has been over two years since Trapeze introduced controller virtualization techniques – the foundation for its Hitless Failover capabilities – validated by The Tolly Group in December 2008 to not lose active voice calls even under catastrophic failure conditions. Yet, not a single WLAN vendor has come close to challenging Trapeze's Hitless Failover claim of non-stop session-level availability, with real-world reliability tests.

Trapeze challenges any WLAN vendor to a real-world reliability bakeoff, any time and place.

"The company's Non-Stop Wireless is more than a slogan. Its use of virtual controller cluster functionality is highly innovative," according to Stan Schatt of ABI Research, who ranked Trapeze #1 in resiliency in ABI's July 2008 "802.11n Vendor Matrix" report. Current Analysis, Gartner and Frost and Sullivan – who gave us a WLAN innovation award for it in 2008 – have drawn similar conclusions about Trapeze's reliability advantage.

In addition to improved scalability and system-level reliability, Trapeze's approach also has important implications for roaming efficacy. How a client roams between APs that are governed by the same controller is well defined in the standards. However, how roaming is supposed to occur between APs managed by different controllers is not defined, and is much more complicated to accomplish. That's because session-level security information about an active session is normally kept on the "home" controller governing the AP the client is on. When a user roams at layer 3 to an AP that is managed by a different controller, it is usually necessary to tunnel the traffic back to the "home" controller. This added leg of the journey is inefficient, and increases the likelihood of session timeouts for latency sensitive applications. Incidentally, this is partly why some vendors want to sell you "big iron" controllers so that all sessions terminate in one place. But the problem for you is that you need another "big iron" controller for redundancy – ca-ching! ca-ching!

But Trapeze's *Identity Based Networking* (patent 7,529,925) together with a *System and Method for Distributing Keys in a Wireless Network (*patent 7,551,619) and *Station Mobility Between Access Points* (patent 7,221,927) solve this problem elegantly by distributing session keys between controllers in advance of roaming clients. So when a client roams to an AP managed by a different controller, it is recognized immediately, avoiding tunneling altogether. The implications are far reaching, especially for synchronous applications (voice, telepresence, telemetry) in large networks. The Trapeze approach delivers seamless mobility campus-wide by treating all indoor and outdoor APs as one homogenous mobility domain.

In summary, Trapeze Networks 802.11n solution offers the best scalability and reliability in the business, backed up with mature lifecycle WLAN management. To learn more about Trapeze Networks NonStop Wireless, please visit: http://www.trapezenetworks.com or call 1.888.768.6625.

Migrating to 802.11n

Adaptive WLAN Solves Trust, Congestion Issues

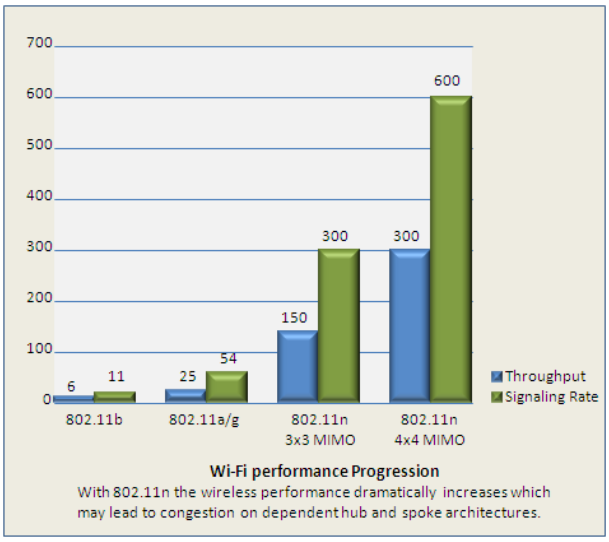
MOTOROLA

By Andrew Peters
Director, Product Marketing
Motorola Wireless LAN

IT's Big Challenge: Trust Wireless As Much As Wired without Extraordinary Costs

IT departments are looking for wireless networks to be the operational equivalent of the wired network in terms of reliability, security, manageability, and cost. Tasked to prov ide users with optimal quality of experience, network administrators need to have the confidence that each user or device gets reliable and secure access to voice, video and data applications. They need a wireless network that is agile enough to grow and change with the needs of the operation without forklifts, gimmicks or band-aid fixes. Finally, they need to continually find the means to drive down the cost of operations.

As IT organizations leverage 802.11n WLANs for business- or operational-critical infrastructure, they are faced with two key challenges that can seriously affect the cost, complexity, quality of applications, and ultimately, the success of the 802.11n wireless initiative.



1) Wired Network Congestion: Can the back-end wired network handle six times increase in access network traffic from the migration to 802.11n?
2) Network Trust: Can IT provide fast, secure WLAN so it's as trusted as a wired network?

802.11n Increases the Burden on the Wired Network

The centralized WLAN is a "hub-and-spoke" architecture that requires backhaul of virtually all wireless traffic to a controller. This hub-and-spoke architecture can create costly scalability and performance issues, including:

Increased burden on the wired network: Backhauling traffic across the wired network significantly increases the load and support costs.	**Scalability:** The hub-and-spoke network can only scale to the processing limitations of the controller and available bandwidth of the network, requiring additional, larger, more expensive controllers supported by bigger and more expensive switches.

Throughput bottleneck: Wired network congestion and general health can limit wireless network performance and create latency that affects voice and video traffic.	**Limited investment protection:** The traffic increases on 802.11n will likely require costly upgrades to the supporting wired infrastructure.
Reliability: Single points of failure as networks are more or less dependent on a single path and control.	**Quality assurance:** While the network has to be always-on, it's also critical to maintain the requisite quality for applications, especially those that are bandwidth hungry and latency sensitive.
Cost: Forklift upgrading the wired infrastructure or adding controllers everywhere creates cost and manageability issues.	

Network Trust

Wired Ethernet networking is a mature and trusted technology. IT departments typically have centralized management, monitoring, and troubleshooting tools for the wired network, including network sniffers, in addition to security assessment or scanning tools to provide high levels of operational assurance.

Wireless networks present a new and complex challenge to IT operations. These networks are affected by radio interference and attenuation (disruption from physical obstructions such as walls, crates, people, etc.) that could be intermittent or permanent and need to be diagnosed for resolution. While the wireless network can resolve many of these issues, other disruptions can seriously affect productivity. If the WLAN is a network of convenience, users can just plug into the wired LAN and IT could dispatch a technician.

When IT troubleshoots wireless network issues, they are often faced with:

Problem identification: Interference can be intermittent and affect user productivity while being difficult to isolate.	**Cost:** It is very expensive to dispatch technicians, especially when improperly diagnosed disruptions that are likely to be phantoms and cannot be resolved by a field technician.
Mean time to repair: Interference often requires technicians to be dispatched to isolate, recreate, and solve the problem, which can take hours to weeks depending on severity and availability.	**Productivity:** Wireless network outages and interference affects productivity and causes opportunity-loss costs.
Phantom issues: Most "wireless" problems actually are not related to the wireless network. It is usually DNS servers, firewall filters and router ACL issues that keep users from accessing their applications.	

The Motorola 802.11n Advantage

Motorola's next-generation adaptive WLANs address the pitfalls of these traditional approaches and are designed to meet the challenges and take full advantage of the benefits of 802.11n networking. These high performance wireless networks rely on an adaptive architecture that automatically adjusts to its environment to meet the connectivity, quality and security needs of the user and application. These solutions are specifically designed to overcome key 802.11n challenges by providing the following:

1. **Distributed Architecture to Resolve Network Congestion** – The adaptive access point can mesh, accelerate, secure, load balance, and even reroute to ensure resilience, which relieves the burden of the wired network to provide these services. The network pervasively tunes itself to minimize RF interferences and attenuations affecting user sessions. Analysis tools for troubleshooting and spectrum analysis can be activated on-the-fly on any radio without requiring specialized sensors. The mesh capability of the adaptive architecture reduces the load on the wired network from 802.11n as traffic can route directly across the mesh. In addition, latency and associated costs are reduced while reliability and scalability are increased substantially.

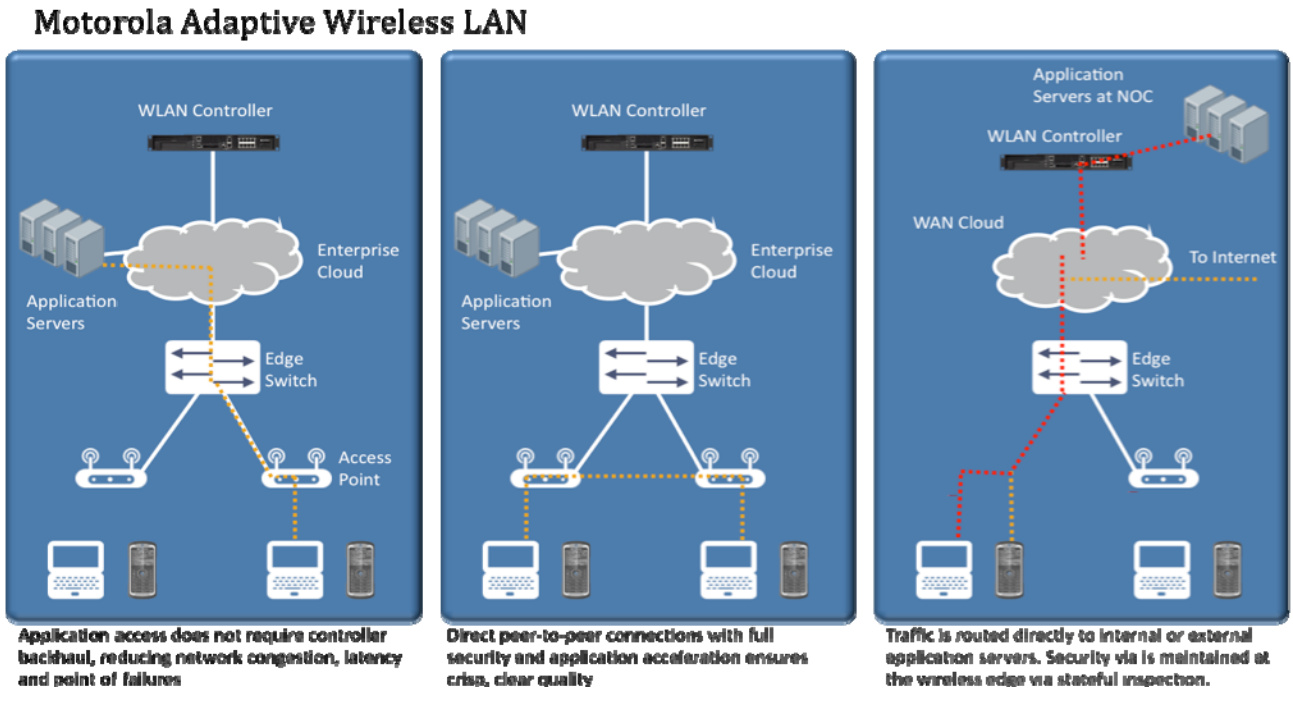
Motorola Adaptive AP – The tri-radio 802.11a/b/g/n AP-7131 Wireless Access Point provides unparalleled resiliency and flexibility, enabling deployment as either a standalone wireless access point or adopted by a Motorola wireless controller for centralized configuration and management.

2. **Network Assurance Creates Network Trust** – While the adaptive network continually tunes and optimizes, IT now has greater control with access to a suite of software tools that is integrated into the adaptive APs to proactively identify communications interference for repair. IT can centrally operate tools to proactively scan for security compliance vulnerabilities and issues that can affect network users and ensure the network is secure and fully operative before problems affect users and security. IT can either use dedicated dual-band sensors (so they can scan both 2.4GHz and 5GHz concurrently) or they can convert any Motorola 802.11n radio on the fly and use it for troubleshooting, spectrum analysis or security.

Motorola provides a suite of tools that enables a level-one helpdesk technician to troubleshoot to ensure it is a wireless issue before issuing a ticket (as wireless connectivity issues are typically in the wired network or server). The level-two technician can use Motorola RF, spectrum, and forensics analysis tools on any AP to determine the root cause before deploying a technician, if required.

As a result, Motorola helps IT now offer wireless networking with the same performance and reliability as wired — giving users the *same trust in the wireless network that users have in the wired network*.

Motorola Adaptive Networks eliminate single points of failure, are highly scalable, and distribute intelligence, security and networking features, such as switching and routing, throughout the network. Every adaptive access point can independently apply security, accelerate applications, route traffic and make optimization decisions, such as power or load sharing, in collaboration with its AP neighbors and the wireless controller. The result is a far more reliable, secure and high-performance network.



For more information about Motorola's solutions described here, please visit: http://www.motorola.com/Business/US-EN/Business+Product+and+Services/Wireless+LAN or call Motorola at 1-866-416-8545.