



---

## White Paper

### **Taking 802.11 Wireless Productivity to the Edge**

*As wireless technology shifts to faster and higher bandwidth solutions, network management should take a more pro-active on-demand approach.*

Prepared for:  
Bluesocket, Inc.

By  
Shoreline Research

An increasing number of companies in the U.S. and abroad are looking to add wireless local area networks (WLANs) to their IT infrastructures, or expand existing wireless environments, to take advantage of the productivity and cost-savings benefits offered by such systems.

The advantages of deploying a secure 802.11 wireless network are obvious. These networks can improve worker productivity and workflow by eliminating the need to physically connect to a wired network to access or exchange information, either within a single building or across a corporate campus, to support a growing number of mobile workers. They can also be used to provide quick and easy access to information at the *point-of-productivity*, within a conference room or remote meeting area away from a user's desk and stationary PC.

Flexible wireless networks can also be used as a convenience for customers, by providing controlled access to specific Web sites and the Internet, and allow suppliers and partners to upload or download information from corporate intranets and password-protected Web portals.

The productivity benefits and potential of wireless enablement is expected to drive the worldwide market for WLAN equipment at a rate of about 52% through 2010<sup>1</sup>. Not surprisingly, a significant amount of this growth is fueled by the emergence of next-generation mobile business and Web-based applications, as well as the continued demand for wireless voice over wireless LAN (VoWLAN) solutions.

In fact, as more companies make use of IP-based solutions, and enable their workforce with notebook and handheld computers, there will be a stronger emphasis on utilizing wireless networks to provide access a wide range of higher-bandwidth applications and services.

---

<sup>1</sup> Infonetics Research

IT and network managers who are charged with developing and supporting wireless networks must therefore not only plan for the enterprise workloads today, but must also make system choices and strategies that can easily accommodate future requirements and expansion. This is especially true as the wireless networks – like 802.11n - become faster and more able to handle higher-bandwidth applications and reliably function across a wider network environment.<sup>2</sup>

Key considerations include centralized versus decentralized control across a wireless network; intelligent edge solutions, that distribute and balance control functions across a network; support for higher-speed and higher-capability networks, like 802.11n; and scalable network environments, which can adapt to changing workforce and applications requirements.

*“Every wireless deployment is unique and presents it’s own reliability and quality of service challenges (QoS) challenges....”*

Most, if not all of these fundamental architectural decisions must be made early in the design process and usually involve selecting a vendor that can meet demands today and an even wider range of requirements in the future.

This white paper will explore the various points to consider in planning for wireless networks that are scalable and flexible enough to handle the demands of current business applications, can support current higher-speed solutions (like 802.11n Draft 2.0<sup>3</sup>), and are both backward and forward compatible with evolving more robust wireless architectures and standards.

### **Mapping Out a Manageable Wi-Fi Solution**

The first thing to understand in planning for a wireless network of any type is that no two solutions are completely alike. Every wireless deployment is unique and presents its own reliability and quality of service (QoS) challenges that must be identified and mitigated through the configuration of the controller, placement of APs, and structure of authentication and control procedures that impact each user within the wireless

---

<sup>2</sup> See Bluesocket White Paper *Next-Generation Wi-Fi Technologies: Paving the Way for 802.11n Adoption*

<sup>3</sup> The Wi-Fi Alliance, an industry group, began testing 802.11n Draft 2.0 products in June 2007, shortly after the release of the specification.

ecosystem.

The goal is to design and deploy a system that is reliable, accessible and flexible for future needs, which is one of the primary reasons why network administrators should have complete control over how traffic is directed and channeled throughout the network.

The issue of control at both the control plane and the APs is critical as 802.11n is integrated into existing 802.11 a/b/g network environments since higher-bandwidth 802.11n deployments can rely on a smaller number of APs due to the improved signal range and coverage offered by the technology (up to two-thirds less the number of APs normally needed since 802.11n operates at 150M bits/second).

*“The issue of control at both the controller plane and the APs is critical as 802.11n is integrated into existing 802.11 a/b/g networks...”*

One of the most important considerations in planning a wireless network involves the selection of the controller and whether overall network architecture should be centralized or de-centralized in operation. In a centralized configuration, all authentication and network traffic procedures flow through a single controller, while a de-centralized environment shifts a lot of the secondary control procedures to the individual APs and the Wi-Fi area and traffic they manage. Security is not impacted by a de-centralized approach since all initial authentications still flow through the controller and user-defined security protocols.

The choice between a centralized and a de-centralized approach is obviously critical when it comes to the performance of a wireless network today and how it will function when overall throughput is significantly boosted by higher-performance 802.11n technology and with the addition of higher-bandwidth applications.

Just as the adoption of 11g APs drove the need for centralized control (thin AP) architectures, the adoption of 11n access points will drive the need for distributed data (intelligent AP) architectures.

One element that is driving the need for more bandwidth and higher-capacity wireless network environments is an increased use of mobile applications especially those that involve constant uploading and downloading of information from remote locations through a network.

The mobile applications market is expected to grow to \$9 billion by 2011 primarily fueled by users in the small and enterprise business sectors, according to Compass Intelligence. This year alone, businesses in the U.S. are expected to spend roughly \$3.8B on mobile applications.<sup>4</sup>

*“..selectively shifting some of the routing and control functions to intelligent APs can reduce or eliminate network latency and other operational problems.”*

The increased use of mobile and remote applications and wireless client systems (notebook, handheld computers, etc.) is also generating a need for more intelligence and control at the wireless access points and at the very ‘edge’ of networks. In most cases, network traffic is routed through these devices to a centralized controller and then back to the specific AP or the applications server. However, the proliferation of handheld and even embedded wireless devices within a typical organization has the potential to create network traffic problems’ like signal latency, and have a negative impact on a network’s quality of service (QoS).

Taking a decentralized approach to wireless networking and having the ability to selectively shift some of the routing and control functions to intelligent APs *on-demand* can reduce or eliminate network latency, jitter and other network problems, and enhance the higher-bandwidth capabilities of mixed 802.11 a/b/g and 802.11 Draft 2.0 configurations.

A decentralized on-demand wireless architecture can also avoid many of the network traffic *bottlenecks* associated with centralized systems where all of the network traffic flows back to the controller and the entire network is potentially vulnerable to high availability issues.

---

<sup>4</sup> Compass Intelligence, May 2007

## **802.11n: Delivering on the Performance Promise**

802.11n is a wireless standard, ratified by the IEEE, that defines both client and access point (AP) radio technology that operates in the 5GHz range and could very well push access speeds to 100M bits/second or more (four to five times greater than current wireless networks). Because it operates in a higher frequency than the majority of 802.11 networks, and makes use of 'smart' multiple-input multiple-output (MIMO) antenna and radio technology, 802.11n also:

- Is more resilient and reliable when it comes to signal interference and its ability to overcome physical obstructions in the workplace;
- Requires less APs, since 802.11n equipment has more robust transmission and receiver capabilities;
- Has a higher bandwidth capability to handle increased video, location-based and voice applications;
- Offers vastly improved rate versus range performance capabilities and therefore has better interaction with the controller and other APs in the wireless network.

Ratification of the final specification and products based on it is not expected until 2009. However, 802.11n Draft 2.0 is now available and products based on it are expected to be fully compatible with existing 802.11 networks (although only 'pure' 802.11n systems will be able to fully deliver the speed and performance promised by the technology).

Some wireless solutions vendors try to resolve this problem by increasing the throughput capabilities at the controller to handle the greater flow of traffic in high-bandwidth networks. However, this is a 'band-aid' solution that may work temporarily, but is not scalable as demands on the network increase. In fact, the only solution in this case might be to add a second controller to support the increased traffic flow.

A better alternative is to offload some operations to the 'points of activity' within the network, or at the individual APs, which can handle such things as data encryption and decryption before routing traffic back through the controller. An intelligent edge

solution also provides faster access speeds and improved QoS since data is automatically received and sent through the AP switch, so long as a user is authenticated at the controller.

### **Impact of Next-Generation Applications on Wireless Networks**

The next five years will see a rapid and sustained increase in mobile and wireless applications as companies continue to expand their mobile workforces – especially as wireless technologies like Wi-Fi and emerging WiMAX provide a stronger backbone to support these systems.

Mobile applications and services include traditional email and messaging, as well as sales force automation tools, location-based software, collaborative technologies and SaaS solutions.

In fact, mobile business applications and services are expected to generate well over \$100 billion on worldwide revenue by 2012, according to ABI Research.<sup>5</sup> VoWLAN and VoIP voice services will boost this figure even further as companies embrace IP-based mobile telephony in an effort to reduce costs and improve interaction among workers and customers and next-generation mobile handsets that incorporate Wi-Fi chipsets as a communications option.<sup>6</sup>

Despite its low-bandwidth demands, VoWLAN applications are expected to play a pivotal role in the enterprise as a productivity booster, and key technology in such mission critical applications as healthcare and hospital networks (see *Wireless in Action* case history sidebar).

Many companies are presently investigating or have already deployed IP-based unified communication solutions, which are based on the industry-standard session initiation protocol (SIP), which provides support for two-way VoIP telephone calls and more

*The optimal solution is to provide technology and software support at the edge devices, by deploying flexible and intelligent APs that can be adapted for changing user and applications demands.*

---

<sup>5</sup> ABI Research, Aug. 2007 <http://www.abiresearch.com/abiprdisplay.jsp?pressid=896>

<sup>6</sup> ABI Research estimates that 263.8 million mobile handsets were shipped in 2Q 2007, a year-over-year quarterly increase of 13%

advanced collaborative messaging and multimedia conference sessions involving PCs, cell phones and wireless handsets.

SIP-based solutions (like those offered by Pingtel Corp., recently acquired by Bluesocket, Inc.) can also be used to merge video, voice, data and location-based services into a single application.

Nearly half of all telecom users, or 1.2B VoIP subscribers, worldwide will be using some type of SIP-based service operating over enterprise and public networks, says market researcher ABI Research. This activity will generate over \$150B in service revenues each year with cumulative infrastructure capital expenditures of more than \$10B by 2012, much of it earmarked for messaging, video sharing and converged voice and multimedia services.<sup>7</sup>

As more voice-enabled traffic is introduced to a wireless network, the ability to quickly route this traffic with the least amount of impact on the control plane, and manage this routing capability *on the fly*, is critical to the overall performance and QoS of the wireless network. On-demand routing and control are also essential to pave the way for fixed mobile convergence (FMC) architectures and solutions.

### **Securing a Flexible, on-Demand Edge Network**

Recent security breaches involving major retailers and online service providers have underscored the need for strong and reliable security in wireless networks. Legislation enacted by local towns and counties in the U.S. also presently mandate that businesses should have defined security architectures in place to prevent accidental and intentional misuse of business wireless networks.<sup>8</sup>

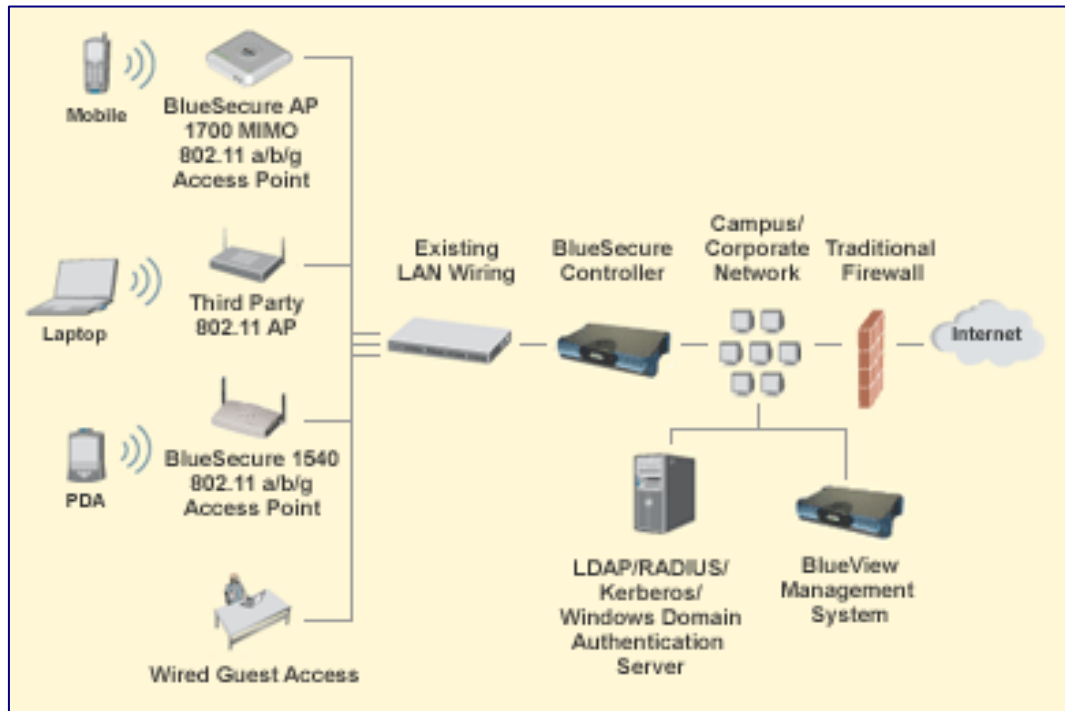
---

<sup>7</sup> ABI Research forecasts almost 1.2 billion SIP-based users by 2012, with most subscribing to several forms of messaging and video sharing services.

<http://www.abiresearch.com/abiprdisplay.jsp?pressid=879>

<sup>8</sup> *Lawmakers Crack Down on Wi-Fi Crime*, InternetNews.com, April 2006

## An Enterprise-wide Edge-to-Core Wireless Solution



*Courtesy Bluesocket, Inc.*

The need for tighter security will become even greater as wireless networks are enhanced with more robust technologies, like 802.11n, that are designed to support higher bandwidth and a new class of multimedia-rich applications and messaging traffic.

Since these technologies offer greater coverage across a wireless environment, the security fences designed to protect the network should be flexible enough to adapt to shifts in user and applications demand. Ideally, the network administrator should not only manage the policies and procedures that reside on the central controller, but also the elements of these protective routines that operate on the thin client APs at each the point of user access.

Security requirements in a typical enterprise wireless network should include:

- Open Systems Interoperability, to ensure a system can easily be expanded and accommodate evolving technologies and software;
- Flexible Mobility, allowing users to authenticate once and roam across the network and sub-networks without the need for secondary or proprietary client software;
- A role-based approach to user management and privileges, defined by destinations (server router, IP address), services, user locations, time and date schedules, and available bandwidth (especially in mixed voice/data networks);
- Strong data encryption capabilities (supporting IPsec in VPN and firewalls) and industry-accepted standards such as Microsoft's native L2TP/IPsec implementations;
- The ability to shift on-demand some security responsibilities (encryption/decryption, etc.) from the controller to the intelligent APs at the edges of the network, while maintaining authentication integrity with the central controller;
- Real-time monitoring of intrusion detection, worm detection, unauthorized or bandwidth-violating data exchanges, and protection against 'zero day' attacks and breaches.

*Points to consider in planning for a mixed 802.11 a/b/g and 802.11n networks are ease of deployment and use, quality of service (QoS), flexibility, and scalability of the entire WLAN infrastructure.*

### **Conclusion: Planning for Today, Preparing for Tomorrow in Wireless**

Even before the Wi-Fi Alliance began testing products based on the Draft 2.0 of the IEEE's 802.11n specification in June 2007, wireless solutions vendors started marketing products supporting the technology and promised TCP/IP throughput speeds up to 200M bits/ and a more robust coverage capability.

Products based on the final 802.11n specification are not expected until sometime in 2009, although equipment based on the Draft 2,0 specification will be backward compatible with those based on the final standard as well as existing 802.11 a/b/g systems, according to the Wi-Fi Alliance.<sup>9</sup>

---

<sup>9</sup> The *Wi-Fi Alliance* is a non-profit independent group dedicated to promoting a universal standard for high-speed wireless. The group presently has more than 300 member companies from 20 different countries.

## Taking Productivity to the Edge: A Decentralization Checklist

Next-generation wireless access points (APs) that employ multiple antennae (MIMO) technology can deliver up to a 30% or greater improvement in signal range and performance than conventional single-antenna APs, resulting in better coverage across a network and better support for higher-bandwidth applications when used with mixed 802.11 a/b/g and 802.11n Draft 2.0 technologies.

However, the dual radio technology offered by MIMO architectures is just a framework for these 'thin access' devices that play an increasingly important role in wireless edge networking. The additional features and functions built into specific wireless APs make a significant difference in how the overall network performs and how the network manages traffic in a bandwidth-intensive environment. Wireless solutions that are best equipped to handle current and evolving enterprise needs should offer the following features:

- Automatic configuration across any Layer 2 or Layer 3 networks, allowing for easier deployments and upgrades and improved interoperability with the controller. These access points can also be directly attached to existing Ethernet switches and across any subnet boundaries;
- Field upgradeable radio cards that can support the fully-ratified version of 802.11n when it becomes available in 2009, and eliminates 'forklift' replacement of existing APs;
- DynamicRF™ technology that automatically adjusts AP resources based on activities in the wireless environment to achieve optimal performance and minimize RF noise and interference. Client load balancing and fast roaming (automatic or on-demand) can also help support high-bandwidth or low-latency VoIP applications.
- Built-in security that can locally detect rogue clients, ad-hoc networks and spoofing attacks (working with the controller) and improve security throughout the RF environment;
- A user-defined on-demand capability that works with existing controller procedures and authentication rules, but can locally manage functions like encryption and decryption of wireless traffic to offload demands on the centralized controller. The result is faster, more responsive wireless networks.

*DynamicRF™ is a trademark of Bluesocket, Inc.*

---

Companies with existing 802.11 wireless networks, or those planning to deploy Wi-Fi

networks within their organizations are encouraged to incorporate early 802.11n Draft 2.0 products into their design because of the immediate benefits the technology will provide to the mixed network and the mitigation of any compatibility issues with future systems.

For obvious reasons, however, it is critical that management systems be put in place that allow network administrators to control network traffic and bandwidth usage both at the controller plane and *points of access* and productivity at the very edges of the wireless network.

Other points to consider in planning for combined 802.11 a/b/g and 802.11n networks are ease of deployment and use, quality of service (QoS), flexibility, and scalability of the entire WLAN infrastructure.

Due to the higher bandwidth capabilities of 802.11n systems (even when integrated with conventional Wi-Fi networks) , it is advisable to have on-demand as opposed to automatic control of activities and the traffic that flow through conventional and higher-bandwidth APs, since this affords a greater degree of management at these edge points and throughout the wireless network.

While some vendors tackle the issue of control in an intensified-bandwidth environment with a solution based on increasing the gigabit capabilities at the controller, this is generally viewed as a temporary solution – especially as wireless network demands increased over time and 802.11n systems dominate or replace current 802.11 a/b/g equipment. Back-end controllers can be installed to support the primary controller plane, although this adds an extra layer of gates to the network and may create latency problems.

The optimal solution then, is to provide technology and software support at the edge devices, by deploying flexible and intelligent APs that can be adapted for changing user and applications demands.

Network administrators charged with supporting or developing enterprise 802.11 networks should take a hard look at channel management, applications demands and usage loads in planning new wireless networks or for future systems expansion – especially when gradually introducing 802.11n equipment into the mix.

In deploying higher-bandwidth-capable systems, administrators should also consider the impact more robust technology will have the network environment (particularly with the use of less APs as edge managers), the potential problems created by signal overlap, and the flexibility of the system to adapt to changes in design and demand as network needs escalate.

With all this in mind, the most important aspect of mixed 802.11n and 802.11 a/b/g or pure 802.11n networks is flexible and user-definable control over what happens at the controller plane, within the network itself, and at the edge points, which are the final gateways to user access.

