

Enterprise



**Unwiring the Enterprise:
A Fresh Look at the Risks and Rewards of
Abandoning Wired Access for Wi-Fi**

Austin Hawthorne

Introduction

In the past five years, there has been an enormous and irreversible shift toward workplace mobility. Today, only around 20% of the workforce is deskbound. There is a significant percentage of workers who spend the majority of their time on the road (i.e., “road warriors”), and a much larger percentage that has a need to move about the building, the campus, or even between sites to perform their jobs (i.e., “corridor warriors”). To be maximally effective and productive, these mobile workers require portable technology in the form of laptops, PDAs and mobile phones, along with specialized mobile applications and a corresponding network capable of supporting this mobility. Wireless LAN (WLAN) technology, commonly referred to as Wi-Fi, was developed to do just that.

WLANs are no longer a novelty for tech savvy home users. In recent years, there have been major developments targeted at making WiFi applicable to the corporate world; most notably in the areas of security, speed, interoperability, and QoS. Due to recent IEEE standards such as 802.11i (wireless security), 802.11e (QoS), and 802.11a/g (bandwidth, stability and scale), Wi-Fi is now a more mature technology, able to solve enterprise mobility requirements and offer significant cost savings.

In the enterprise, certain vertical markets have seen faster uptake of Wi-Fi, driven by specific applications and competitive requirements. These industries and key applications include:

- ❖ Healthcare – Bedside care, E-prescriptions, Electronic Medical Records (EMRs), and voice
- ❖ Education – Learning management and student information systems, student demand for wireless Internet access
- ❖ Retail – Inventory tracking (RFID), mobile Point-of-Sale (POS)
- ❖ Manufacturing – Inventory management, work-in-progress tracking, wireless production lines
- ❖ Hospitality – Guest Internet access, maintenance and housekeeping response management, voice

Mainstream enterprises have taken a more gradual and deliberate approach to WLAN deployment. They first used the technology for limited purposes such as guest and common area access. WLAN technology has evolved and matured, and enterprises are now broadening their deployments to support general purpose business applications—email, Internet, server access and instant messaging—to increase the productivity of the mobile workforce.

By definition, the existing fixed, or wired, network cannot meet the need for mobility. It is inflexible. More significantly, the wired network has no visibility into who or what is plugging into it, and it cannot follow a user to deliver consistent user experience and security policies. As workforce mobility continues to grow, the

expectation is that the edge of the network will become predominantly wireless. That is, by and large, workers will not connect to a cable; they will connect to the network through the air.

Issues on the Wire

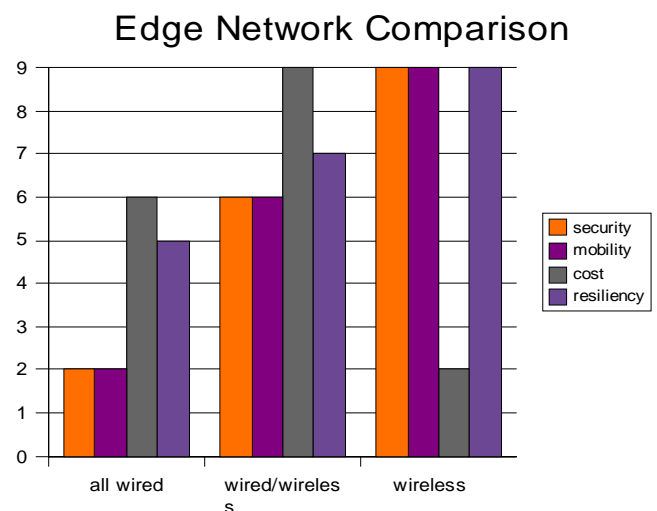
Why consider removing the wire? Because mobility and wireless deliver numerous benefits to the enterprise ranging from cost savings to productivity gains to competitive advantage enabled through applications that mandate mobility. But before considering these benefits, it's worth looking at some of the costs and issues associated with fixed networks, especially in light of mobility trends.

High cost of infrastructure: It is commonplace to run CAT5 for every user and every new networked device. As a rule of thumb, today's network access layer in medium to large enterprises is typically set up with one port for data to each user's PC, one port for voice to each user's fixed VoIP phone, and often, a redundant port for both the data and voice connections. That's up to four ports, and associated cable runs, at each desk.

Spread across a medium to large size enterprise, that requires many ports on many switches, half of which are likely to be unutilized. In addition, more ports in the closet translate into more uplink capacity in the distribution layer, driving higher capacity links and switches in that layer as well. This significantly drives up infrastructure costs. This is a hefty price for dedicated wired access to each desk when the wired network is the primary form of access.

Lack of Redundancy: Cable runs from a given desk are typically all to one switch, and one switch alone. If that switch fails, it is up to the user to move the connection from the PC and VoIP phone to the second available data/voice port, assuming it is available and provisioned to a different switch/IDF. This is not seamless redundancy, and results in lost productivity, and possibly lost revenue. It is ironic how much scrutiny is placed on split second fail-over times between routers given that a single edge switch failure will cause all associated calls to drop and all network-based applications to break.

Lack of Security: Wired network security is set up as a perimeter, protected by a firewall and the physical walls of the building. But how well is a wired LAN typically protected? What happens when a visiting vendor or customer needs Internet access to bring up a WebEx or VPN back to their corporate resources? Port(s) may need to be reconfigured to the guest VLAN to allow that PC to plug in without worry of viruses or worms propagating onto the network. What if a visitor plugs in to the network without the enterprise being aware of it? The wired network is not aware of who or



what is plugging into any given port; it is a fixed infrastructure that requires user intervention to apply the appropriate levels of security to any one port at any given time. This directly results in even more IT man hours required to configure the network. Furthermore, there could be significant costs associated with malicious and unintentional security breaches, both by employees and guest users.

IEEE 802.1x can address some of these security concerns, but is insufficient for complete identity-based security and has proven costly when adapting to an existing wired LAN. Furthermore, 802.1x must be complemented with policy enforcement based on user or device identity so that tiered access is available, where guests are limited to internet access, employees are given access to the whole network, and voice phones are restricted to transmitting voice protocols to a call controller. To enable this level of functionality in a wired LAN would require a patchwork of security systems such as stateful firewalls (possibly even Anti-Virus firewalls to protect against viruses), Layer 7 intrusion detection systems, URL Filters, host integrity checking mechanisms, etc. To make the wired LAN both secure and mobile is just too costly and complex.

Lack of Mobility: The wired network today suffers from insufficient mobility. The port a user plugs into is statically configured for a VLAN that was planned for a particular user or group. There is typically no identity awareness on wired LANs today, and plans for network-wide network access control (NAC) implementations are still a long way off and wrought with complexity and high cost. If a user needs to pick up and move, a whole team of IT engineers must reconfigure the network to have that user's rights (VLAN mapping and associated policies) follow them. If a new user comes on site, the network must be provisioned for that user. Guest users, if allowed on the network, will require additional provisioning. Meeting these requirements in an enterprise is not only time consuming, but costly in terms of IT man-hours to implement change controls and reconfigure the network as well as in hours of lost worker productivity while network connections are moved.

Why Wireless? Why now?

What are the implications of moving to an all-wireless mobile edge? Consider the following five topics often discussed during any consideration of implementing wireless:

1. Reduced capital, operational and management cost
2. Increased security
3. Convergence and voice mobility
4. Greater resiliency and manageability
5. Mobility and increased productivity

Reduced capital, operational and management cost: Looking first at cost, a common starting point, the analysis can be approached from a number of angles. In determining ROI, one can and should consider the increased productivity. However, since that can be difficult to quantify, it's worth looking just at the associated capital, installation and support costs.

	Wired Edge	Wireless Edge
# of Ethernet Switch ports required	100	5
Hardware Cost per port on Switch	\$112	\$112
Support cost per port(10% HW cost/yr)	\$11	\$11
Wired Infrastructure cost	\$12,320	\$616
# of WLAN APs required	0	5
Cost Per AP	0	\$595
support cost per unit(10% HW cost/yr)	0	\$60
Total AP cost	0	\$3,273
# of WLAN controllers	0	1
Cost per controller	0	\$1,750
support cost per unit(10% HW cost/yr)	0	\$175
Total controller cost	0	\$1,925
Wireless Infrastructure cost	0	\$5,198
Data & Voice Cable Pull To Desk (\$500 per pull)	\$50,000	\$-
Cable pull to ceiling (\$300 per pull)	\$-	\$1,500
Site Survey (20 min per AP @ \$100/hr)	\$-	\$170
Install cost per AP (20 min per AP @ \$100/hr)	\$-	\$170
Total Installation Cost	\$50,000	\$1,840
Total COO	\$62,320	\$7,654
% Cost Difference With Wireless Office		88%

Consider a green field deployment in a 25,000 square foot branch office with 100 employees, each requiring voice and data to their desk. The wired plan is straightforward, providing one port to each desk. No redundancy is included as this is a common cost-reduction in a branch office. For wireless, an 802.11a/b/g network is used to provide secure voice and data access for each employee. The network is designed using five dual radio APs, or ten clients/devices per radio.

In addition to the 88% savings on capital and support costs, the cost of moves/adds/changes is virtually eliminated with an all wireless edge as the network seamless supports users who are presumed to be moving continuously.

Increased Security: While security was a weak link in the early days of WLANs, these issues have been addressed so effectively that it could be easily argued that wireless networks are more secure than wired networks. As discussed above, wired network security is set up as a perimeter. Once inside the office, users are wrongly assumed to be “safe” to access the network, and security is applied based on the port into which someone plugs their PC. But mobility breaks this security model as users are not connecting to a specific port.

WLANs are now protected with very strong authentication and encryption technology, and they are able to identify and apply security policies based on who the user is, what type of device it is, how it is

authenticating, when and from where it is connecting, and more. Some mobility controllers integrate policy enforcement firewalls, enabling them to implement role-based access control, tying users to policies and roles defined in directory services.

Whether or not an enterprise chooses to implement wireless, wireless-related threats will exist and must be mitigated. Many of today's centralized WLAN systems incorporate advanced wireless intrusion protection capabilities, able to thwart attacks and protect the network against malicious or inadvertent wireless-based threats such as rogue APs. Some centralized WLAN systems also support client integrity and remediation functions to protect against viruses, worms, and the like. Thus the network is protected against infiltration from the outside and the inside.

Convergence and Voice Mobility: Just as mobile workers want to take their computers with them as they move about, they want their phone “mobilized” as well. Within an enterprise, many workers use and expense their cellphones for this purpose. In doing so, costs are increased and employees “lose” the functionality of the company PBX. Voice over Wi-Fi (Vo-Fi) implementations can deliver both the PBX functionality and user mobility. Standards such as 802.11e and other techniques have been developed to assure Quality of Service (QoS) for latency-sensitive applications. In fact, Vo-Fi is one of the applications accelerating WLAN deployments. Additionally, with the arrival of Fixed-Mobile Convergence (FMC), seamless support for wireless voice-capable devices on both Wi-Fi and cellular networks, will come even greater mobility, cost savings, productivity and convenience.

Greater Resiliency and Manageability: Early WLANs used a distributed architecture with thick access points, APs that include not only the radios, but the security and management functionality as well. However, each AP has to be managed individually, making configuration, management, and upgrades very difficult, time consuming and costly, especially as a network scales.

Today's WLANs are usually built using a centralized architecture comprising a mobility controller and thin APs. Thin APs simply provide Wi-Fi access and monitor the air for intrusion; all the intelligence and security is offloaded to the mobility controller. The entire WLAN can be managed from a single mobility controller. Consequently, WLANs with numerous controllers and thousands of APs can be managed with a small staff.

Planning, implementation and management of the WLAN is also greatly facilitated through integrated RF management functions. The network, coordinated by the mobility controller, has the ability to optimize itself and self-heal around AP failures, dynamically adjusting channel settings and power levels. In fact, in most cases, an AP failure would not even be noticed by the user, and the data session or voice call would not be affected. A wired connection from a PC to the closet switch simply cannot provide an equivalent level of resiliency.

Mobility and Increased Productivity: Finally, and most significantly, an all-wireless edge enables mobility. This applies not only within the walls of a single building or across a campus, but extends to branch offices, workers' homes, and other locations across the WAN and the Internet as well. Users are provided with a consistent user experience and secure access to voice and data resources no matter where they need them. The wireless edge significantly boosts employee productivity and enables a wide range of applications that are simply not possible on a wired network edge.

Common Objections to Wireless

Because the concept of deploying Wi-Fi as the primary access medium is relatively new, there have been challenges. Fortunately, with the maturity of new WLAN offerings, these challenges can be overcome through proper design and implementation.

Bandwidth Concerns: Bandwidth is the most common objection raised when considering removing the wire. Wired access is typically dedicated 100Mbps full duplex, while wireless is shared 54Mbps. Common perception is that wireless bandwidth is insufficient, but a quick calculation shows that bandwidth per user is actually far less than expected for voice, web, email, file sharing, etc. Many studies show that the typical employee uses roughly ~2.2Mbps on average. The 100Mbps Full-Duplex link is, in most cases, severely under utilized. Vendors of wired switches have been pushing gigabit Ethernet to the desktop as a hard requirement, but most organizations have pushed back, demanding mobility over bandwidth. While 802.11a/b/g cannot currently meet the pure throughput of a dedicated 100Mbps link, it can provide a desktop like experience to the end user with proper design and traffic engineering. By placing enough APs in the environment with a proper channel plan, user load can be distributed equally among the available APs so as to reduce the maximum number of clients per AP, providing bandwidth much greater than or equal to the current requirement of ~2.2Mbps per user. To meet more bandwidth hungry applications, the industry is responding with the IEEE 802.11n standard, with pre-standard certification due in 2007 and full ratification of the standard expected in early 2008. 802.11n will raise WLAN performance to approximately 100Mbps.

Security Fears: Many continue to be concerned with the security of WLANs, arguing that RF leaks can allow would-be hackers or war drivers to initiate attacks. This is where properly implemented security plays an important role. RF simply cannot be contained within a physical boundary such as a building and security policies must be defined accordingly. With the advent of IEEE 802.11i and mobility controllers that support identity-based policy enforcement, strong encryption, authentication, and mobile access control, policies can be easily deployed and managed throughout the enterprise. Using industry best-practices can actually protect a network better than the wired network.

An All-Wireless Edge: The Clear Choice

WLANs have reached a critical maturity level, enabling enterprises to finally make the transition from wired access to a wireless mobile edge. A move to an all-wireless edge brings numerous benefits:

- ❖ Radically enhance the economics of networks by lowering both capital and operational costs
- ❖ Provide a security approach that is designed for mobile enterprises and more secure than traditional fixed network methods
- ❖ Quickly, easily, and economically adds converged voice services demanded by both users and corporate management
- ❖ Integrates seamlessly into existing infrastructure, and keeps it stable and secure
- ❖ Provides a strong and flexible foundation for future growth of mobile applications and users

About Aruba Networks, Inc.

Aruba Networks provides an enterprise mobility solution that enables secure access to data, voice and video. Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

© 2007 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. All rights reserved. Specifications are subject to change without notice.

WP_UNWIR_US_071217



1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>