



The Case for an Untethered Enterprise





Introduction

In the beginning, there were wires. The traditional wired local area network included a separate voice and data wire for each user, and lots of switches all over the place.

Next came wireless LANs, along with the wireless networking technology known as Wi-Fi. Initially, WLANs were comprised of “thick,” individually managed access points, providing limited coverage areas within the enterprise.

Then came WLAN switches, which simplified network management by enabling centralized control. This lowered the total cost of ownership and increased the security of the WLAN, increasing the popularity of Wi-Fi among corporate enterprises.

Today, most enterprises are running two separate networks – one wired, and one wireless. Most enterprises have treated Wi-Fi as an ancillary tool, meant to complement, but not replace, a company’s wired Ethernet network.

However, several new technological advancements and trends are encouraging IT administrators to rethink their network strategies. In this respect, Wi-Fi has grown up a lot in the past decade.

Once a luxury reserved for curious corporate executives and engineering labs, Wi-Fi is now an invaluable tool for any modern office whose employees use notebooks or handheld computers. Wi-Fi unshackles employees from their desktop computers, whether they are attending a meeting down the hall or visiting the company’s manufacturing floor. The majority of PCs and handheld computers now come equipped with a Wi-Fi connection.

Meanwhile, the Institute of Electrical and Electronics Engineers (IEEE) is set to ratify a highly-anticipated Wi-Fi standard called 802.11n, which promises data speeds that rival and often surpass wired network connections. The advent of 802.11n is a milestone in the evolution of the Wireless Enterprise.

Furthermore, wireless technology has evolved to include mesh networking. In a wireless mesh, the network dynamically routes packets from access point to access point. A few nodes have to be

connected directly to an Ethernet port, but the rest share a connection with one another over the air. This negates the seemingly contradictory need to distribute wires for a wireless network.

The time has come for IT administrators to consider deploying office networks that run entirely on Wi-Fi technology.

A Wireless Enterprise Promises a Lower Cost of Ownership

Anyone who has overseen the deployment of a corporate network knows that wired LANs are very expensive. It can cost nearly \$250 to wire a single Ethernet port. The cost of running a cable between two buildings on a corporate campus can exceed \$10,000. A completely wireless network, on the other hand, eliminates cabling costs. In addition, the wired LAN limits the flexibility in the initial configuration of the office environment, as well making adjustments to accommodate changing business needs — once walls, offices, and cubes are in place, reconfiguration is often cumbersome and expensive. And finally, desktop computers, wired phones and wired networks tether employees to the desk.

A completely wireless network, on the other hand, eliminates cabling costs and unshackles employees from their desks. Such moving issues are moot in a wireless enterprise. Further, a recent analysis conducted by Motorola shows that the cost of a wireless LAN deployment is generally 1/10 to 1/5 that of the cost of a wired LAN, depending on the size and nature of the deployment. See Figure 1 for a sample cost savings analysis of a 5000 employee facility. Further, maintaining a wireless network is more economical. Maintenance costs are based on the number of access points which serve many users, while wired maintenance costs are computed on a per user Ethernet port basis.

Wired networks are also more difficult to deploy than wireless networks, not to mention more time-consuming. In addition to being expensive, wires are messy. Traditional LANs require separate voice and data wires for each user and networked switches all over the building. Deploying and maintaining such networks can be a huge headache for IT administrators. Wireless networks can be deployed quickly, and with much less pain. Consider the case

What about ROI?

ROI of "All Wireless" Enterprise for a 5000 Employee Facility

Wireless Network Considerations

- Eliminate cabling costs
- Reduced number of access switches
- Reduced support & Maintenance costs

First Year cost for a WLAN deployment

Total hardware costs	\$ 140,100
Total installation costs	\$ 75,857
Total support & maintenance costs	\$ 15,862
Total	\$ 231,820

Recurring annual per user cost

Per user hardware cost	\$ 9.00
Per user support cost	\$ 3.00
Total	\$ 12.51

Wired Network Considerations

- Cost of running cables to user locations
- Access switches to supply 2 ports per user
- Support & Maintenance costs

First Year cost for a new wired network

Total hardware costs	
(Including support & maintenance)	\$ 1,320,000
Total installation cost	\$ 2,500,000
Total	\$ 3,820,000

Recurring annual per user cost

Total hardware costs	
(Including support & maintenance)	\$ 88.00
Total	\$ 88.00

1/5th to 1/10th the Cost of Wired Equivalent

Figure 1

of Kilkenny Castle, a historic castle in Kilkenny, Ireland. Until recently, the castle's Internet access was limited to a dial-up connection. The IT project manager was assigned the task of networking the castle without compromising its structural integrity. To mitigate ugly wires and holes in the 12th century walls, Kilkenny decided to deploy a completely wireless solution, using wireless networking equipment from Motorola. The installation took only four days.

A wireless LAN cannot only replace wired networks within a building, but also replace the connection between buildings on a corporate campus. Instead of leasing expensive T1/E1 or T3 lines to bridge

the network connections between buildings, enterprises can bridge the connections wirelessly – using point-to-point or point-to-multipoint wireless Ethernet bridges. By avoiding a monthly leasing fee, enterprises can see a return on investment in as few as six months.

Furthermore, industry trends show most enterprises will be deploying and supporting wireless networks anyway, whether or not they already run a wired LAN. The technology consultancy Gartner predicts that by 2011, 70 percent of new voice and data connections to the LAN will be wireless connections. Not only will notebook computer shipments exceed desktop computer sales, but 35 percent of mobile

phones will be equipped with Wi-Fi by 2011. In an age when so many employees expect and need a wireless Internet connection, it just makes sense to eschew wired Ethernet connections in favor of deploying a network entirely based on Wi-Fi.

Once-valid concerns about wireless technology are now obsolete

Historically, some enterprises have avoided ubiquitous Wi-Fi deployments, mainly because network administrators had concerns about network security, performance, and reliability. They deployed Wi-Fi grudgingly and cautiously, and that too, as an overlay. Traditionally, these concerns were valid. Ten years ago, wireless LAN encryption standards were weak, data rates were slow, and wireless access points and routers were relatively difficult to manage and maintain.

Today, however, technological advances have rendered those problems obsolete. In fact, today's wireless LANs can be as secure, as reliable, and just as fast as wired networks – if not more so.

- **Performance:** The original 802.11 wireless LAN standard (ratified in 1997) offered maximum transfer rates of only 2 Mb per second, which was sufficient for basic data transfers, but not nearly fast enough for video.

Wireless data rates have come a long way since then. 802.11n, the latest Wi-Fi standard, uses multiple input/multiple output (MIMO) technology, which can simultaneously transmit three data streams. 802.11n is very fast, offering throughput rates close to 248 Mbps in a clean environment and around 150 Mbps in real-world conditions; these rates are significantly faster than a wired Fast Ethernet connection. Such rates are more than sufficient for high-bandwidth audio and video applications. Data also travels a long way with 802.11n – around 70 meters indoors and 250 meters outdoors.

- **Security:** In the past, the security mechanisms available for wireless LANs were insufficient for the privacy needs of a corporate enterprise. An encryption protocol known as “Wired Equivalent Privacy” (WEP) received a great deal of bad

publicity in 2001 when cryptography experts exposed its vulnerabilities. WEP, they said, was easy for experts to crack. That led to widespread concerns about wireless security in general. But just as Wi-Fi speed has come a long way, so has Wi-Fi security.

Today, it's safe to say a good Wi-Fi network can be as safe as, if not safer than, a wired network because the wireless industry offers myriad mechanisms for protecting a wireless LAN. Wired networks can provide a false sense of security, but are also prone to attack. Recently an international bank discovered a network intrusion as untold sums of funds were disappearing from accounts. After an exhaustive analysis, the IT staff discovered the culprit, a wireless access point plugged into an Ethernet port in the wiring closet that the thief used to gain access to the network.

WPA2 (Wi-Fi Protected Access), based on the IEEE 802.11i security standard, uses algorithms based on AES (the advanced encryption standard). As the name suggests, it provides highly advanced key encryption.

Wireless intrusion protection systems enable IT to automatically detect and locate rogue devices, prevent intrusions to a WLAN, and protect the network against denial-of-service attacks.

Various techniques such as “geofencing” enable network administrators to provide access based on location of wireless devices, adding physical security to wireless access.

- **Reliability:** In the past, a corporate wireless LAN comprised a series of autonomous access points, scattered throughout an office or a building. Garnering an effective radio signal was a matter of trial and error. Since there was no central management, the administrator often wouldn't know if an access point had failed until someone complained.

Today, the best Wi-Fi networks are very reliable. They are managed from a central switch, with a graphical interface that shows the location and performance of every access point and user on the network. This enables network administrators to spot potential problems and make proactive adjustments to prevent actual problems.

Today's corporate Wi-Fi networks are extremely resilient and, in many cases, self-healing. If one access point fails, a neighboring access points takes over. If the central wireless switch loses power, a redundant switch will take over.

When running in conjunction with a wired Ethernet network, wireless access points can keep going (and take over) when a wired switch fails. Thanks to the advent of mesh networks, it's

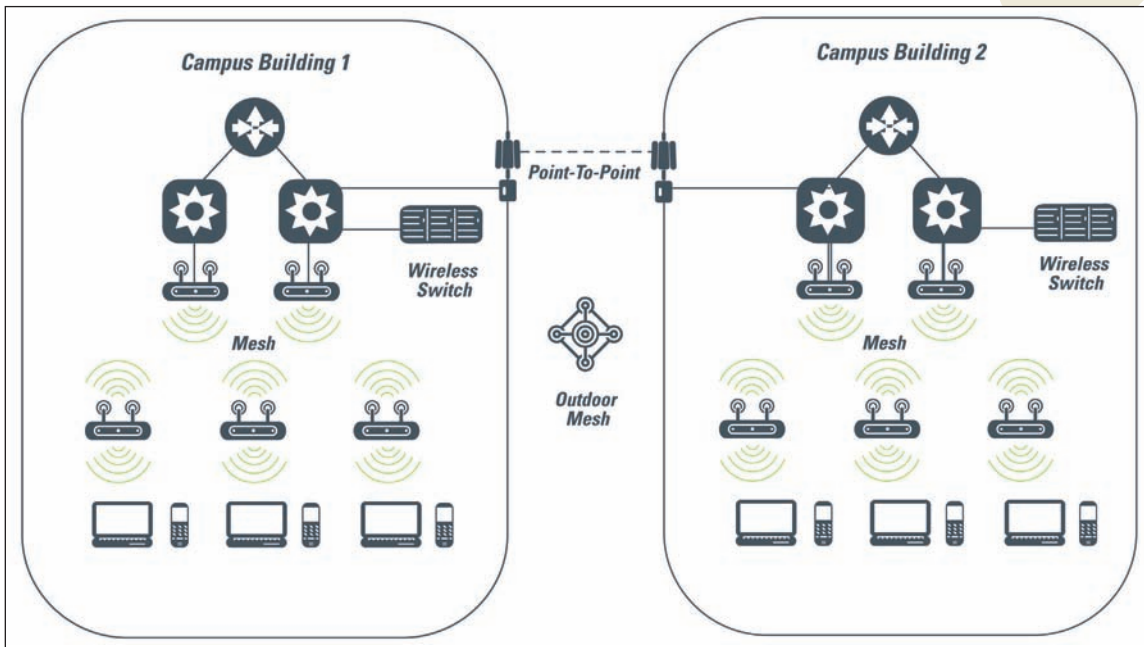
possible for access points to communicate with each other without the switch.


Similarly, access points can take over when a company's wide area network (WAN) link fails, enabling continued communication and (business uptime) within offices and facilities. Wired networks have multiple points of possible failure – from ports to hubs to switches. In many ways, a wireless network provides better resilience than a wired network.

Motorola's Wireless Networking Portfolio Enables a Truly Wireless Enterprise

In committing to wireless technology, network administrators must ensure every piece of the wireless LAN is both reliable and compatible with the other pieces of the network. The best way to ensure compatibility, is to find an equipment provider offering a broad range of wireless networking gear. With the industry's broadest wireless portfolio, and a long history of delivering business critical wireless connectivity, Motorola offers all the pieces necessary to deploy a wireless enterprise. Not only does the company offer indoor networking equipment, it also provides the tools necessary for wirelessly connecting multiple buildings on a corporate campus. See Figure 2.

Figure 2: The Truly Wireless Enterprise





And yes, Motorola's portfolio supports the latest draft of the 802.11n:

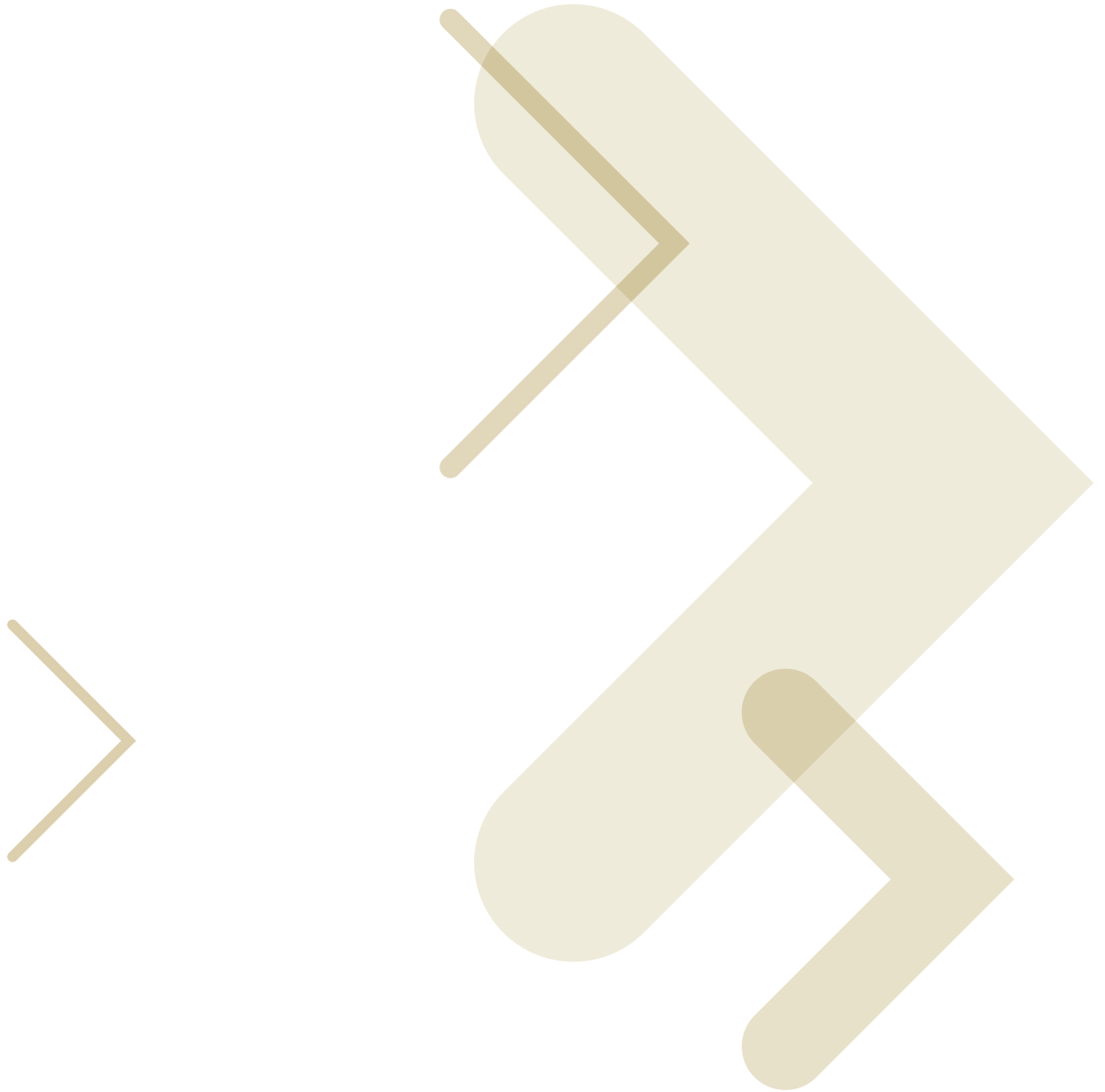
- **Wireless switches:** Motorola offers a broad range of wireless switches acting as the nerve center of the wireless LAN. The company's veteran large enterprise switch, the RFS7000 now supports 802.11n. The company's newest wireless switch, the RFS6000, extends 802.11n capabilities to mid-sized deployments. The RFS6000 provides failover capabilities, ensuring high availability and reliability. The switch also offers comprehensive support for voice services on the wireless LAN, enabling advanced voice applications such as push-to-talk for both indoor and outdoor deployments. Furthermore, the switch includes the ExpressCard™ Slot expansion port, which enables a wireless WAN backhaul connection – supporting current and next-generation WAN technologies such as EVDO, HSDPA, and WiMax. This provides network resiliency for remote and branch offices, in the event of wired backhaul failure, or the absence thereof.
- **802.11 Wireless access points:** Motorola also offers a broad range of wireless access points for both indoor and outdoor deployments. The latest of these is the AP-7131, which offers three radios and includes support for 802.11n. The unique tri radio design of the AP-7131 integrates three 802.11n draft 2.0 radios that deliver high speed client access, mesh backhaul and dedicated dual band IPS functionality simultaneously. The AP-7131 integrates its third radio in an expansion slot which can in future be field upgraded to enable next generation data and non data applications like WiMax and Cellular backhails.
- **Mesh access points:** For many enterprises, business is not limited to inside of four walls; their operations extend outdoors into remote and sometimes harsh environments. To mitigate wiring and to enable outdoor network connections, many enterprises are deploying wireless mesh networks. In a wireless mesh network, the network dynamically routes packets from access point to access point to enable the extension of enterprise WLAN coverage to areas where Ethernet or fiber cabling is cost-prohibitive.

The AP-5131, AP-5181 & AP-7131 (11n) access points all support fast self-assembling and self-healing mesh capabilities.

- **Point to Point and Point to Multipoint:** Many corporate enterprise campuses sport multiple buildings, and they require network connections between those buildings. Motorola's PTP and Point to Multipoint line of wireless Ethernet bridges provide highly reliable connections between buildings – even in high-interference or obstructed environments. Unlike competing solutions, the PTP bridges do not require a direct line of sight between nearby buildings. Motorola also offers bridges that provide long-range connections of up to hundreds of miles – including links over large bodies of water.
- **Centralized Management:** A full suite of RF Management software for simplified and accurate site design and modeling, around-the-clock protection against attacks and unauthorized access, and day-to-day management of your entire mobility solution — from your wireless infrastructure to mobile devices and wireless applications — inside and out.

Conclusion

While once considered a luxury, Wi-Fi connectivity is now an integral part of the modern enterprise. To that end, most corporate IT administrators are expected to deploy wireless LANs. Until recently, most enterprises have chosen to deploy Wi-Fi in addition to a wired network. But with the introduction of 802.11n, which will typically require a costly upgrade to the wired network as well, enterprises can save significant capital and feel confident in the decision to go completely wireless. Wireless technologies now match or exceed the performance of wired networks – at a significantly lower cost and a significantly higher ease of installation. And with a broad portfolio of indoor and outdoor wireless networking equipment, Motorola offers all the tools necessary to create a wireless enterprise – including wireless connections between buildings on a large corporate campus. The Wireless Enterprise is all about “getting rid of the wires, inside and out.”



MOTOROLA

motorola.com

Part number WP_eWLAN. Printed in USA 06/08. MOTOROLA and the Stylized M Logo and Symbol and the Symbol Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners. ©2008 Motorola, Inc. All rights reserved. For system, product or services availability and specific information within your country, please contact your local Motorola office or Business Partner. Specifications are subject to change without notice.