Five Myths of Wireless Networks

IT professionals who have resisted deploying pervasive wireless networks based on earlier assessments need to revisit their decisions in light of a new generation of standards, technologies, and products.

The primary reasons IT professionals cite for not adopting pervasive wireless are:

- The benefits of a wireless network versus a wired network are not clear.
- There are security threats to wireless networks.
- The complexity of wireless networks—and the resources required to deploy and support them—are too costly.
- Wireless technology is still not mature.
- Aside from data mobility, the business value of wireless networks isn't evident.

This white paper addresses the top concerns of IT professionals who resist the deployment of pervasive, enterprise-wide wireless networks. It identifies these reservations based on the experience of Cisco Systems® and Intel Corporation in leading new efforts in wireless standards and working with enterprise customers. By presenting advances in wireless technologies, products, and standards, this paper challenges the outdated perceptions that currently prevent many businesses from capturing the tangible benefits of pervasive wireless networks.

> **"As organizations embrace wireless and mobility to increase productivity, enhance collaboration, and improve business flow, a unified wireless and wired network provides the high levels of security, scalability, and resiliency required of today's business-critical applications."**
>
> — **Brett Galloway**
> VP and GM, Wireless Networking
> Cisco Systems

Myth #1: Wireless networks provide limited benefits compared with wired networks

Many IT professionals do not see the business case for wireless networks given the wired Ethernet infrastructure that is currently in place. While wired networks offer a more deterministic medium for data transfer, they cannot offer the pervasive connectivity inherent in wireless networks, which are designed for today's mobile computing environment.

A key driver for pervasive wireless connectivity is the increase in the number of mobile devices capable of connecting to the network. As client devices expand in form factor and functionality, the benefit of wireless connectivity grows. Analyst firms confirm that for the first time ever, the shipment of notebook computers has surpassed desktops. An estimated 95 percent of those notebook computers have embedded Wi-Fi. And the growth of mobile wireless notebook computers shows no sign of slowing. Notebook computers in the enterprise are expected to grow at a compounded annual growth rate (CAGR) of 18 percent between 2005 and 2010. This is a significant trend for IT departments because the

desktop CAGR for the same period is expected to grow by only 3 percent. To respond to this market transition, IT must be proactive or risk losing to more tech-savvy competitors.

The preference for mobility within the enterprise can be seen by IT departments from both top down (upper management) and bottom up (department users). Upper management wants to improve their company's competitive edge through faster decision-making, better access to information, and improved accuracy for employees. Users want to work more effectively from any location, whether they are at their desks, at any place within the enterprise environment, at home, or on the road.

The drive for mobility in the enterprise, coupled with dramatic improvements in wireless networking technology, is reshaping the work habits and productivity of workers. IT departments are being asked to embrace the mobile wireless usage model to respond to the demands of both management and users.

The benefits of wireless networking go beyond simply providing data transfer to mobile devices. Productivity has long been singled out by wireless advocates as being the primary reason for adopting wireless technology. Several studies quantify productivity gains from wireless networks. For example, a study completed in 2003 by NOP World Technology showed the average time saved per day as a result of wireless connectivity was 1.3 hours. An internal study conducted by the Cisco IT department, indicated that 95 percent of employees gained at least one hour per week of additional productive time.

As the pervasiveness of wireless networking within the enterprise increases, so do the benefits. In addition to productivity gains, enterprises can take advantage of a variety of new mobility services—such as location, voice, guest access, and enhanced security—that allow businesses to reap additional benefits from the network by adding a mobility element to existing (and new) business applications.

Thanks to the availability of these services, businesses can calculate a tangible return on investment (ROI) for each wireless application enabled by the network. For example, a business may implement an asset tracking application based on active Wi-Fi asset tags to decrease the cost and time associated with looking for and replacing high-value assets. Or a business deploying an in-building voice over wireless LAN service can decrease its dependency and the costs of cellular voice services for calls originating from the enterprise.

Cisco and Intel Alliance

The strong Cisco Systems and Intel partnership focuses on improving the business impact of technology. The Cisco Intel Alliance (www.ciscointelalliance.com) is the vehicle for both companies to collaborate in specific technology areas for the benefit of their mutual customers. The alliance provides:

- Tangible business value for technology adoption
- Business-class wireless networking solutions that seamlessly combine Intel® Centrino® mobile technology clients with the Cisco Unified Wireless Network
- Lower complexity of deployment and total cost of ownership (TCO) for businesses implementing and managing a pervasive wireless network

Myth #2: Wireless networks are not secure

Inadequate security has consistently been one of the biggest concerns IT departments raise about wireless networking. Wireless security has made great advances over the past few years thanks to the efforts of the IEEE and the Wi-Fi Alliance. New security standards like IEEE 802.11i and the Wi-Fi Alliance Wi-Fi Protected Access 2 (WPA2) have emerged to match the robust protection previously found on wired networks.

Cisco and Intel continue to take the lead in these security standards bodies to focus on delivering a wireless solution that is as secure as the wired network, as well as to provide products designed to protect the enterprise against wireless security threats. Cisco delivered the Cisco Compatible Extensions program, of which Intel is a lead collaborator. Cisco Compatible Extensions incorporates the latest security standards and innovative security solutions, including authentication protocols like Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST).

The end result has been to dramatically improve the ability of the network to automatically identify, prevent, and adapt to security threats. Every device in the network—from clients to access points to wireless controllers and the management system—plays a part in securing the wireless network environment through a distributed defense.

A multilayered approach to security is required to provide protection to any mobile solution. The following is a five-step approach for mitigating risks to the network from wireless threats:

1. Create a WLAN security policy.
2. Secure the WLAN.
3. Secure the wired (Ethernet) network against wireless threats.
4. Defend the organization from external threats.
5. Enlist employees in safeguarding the network.

"Intel and Cisco have delivered industry-leading, standards- based wireless security solutions, making the wireless network more secure than the wired."

— **Pat Calhoun**
CTO Wireless Networking
Cisco Systems

Secure network communications entail both encryption of data and authentication of users to the network. In a wireless network, much like a wired network, these two components do not have to be combined, but for most networks it is recommended to use both. Exceptions might include hotspot or guest networks. In addition, the unique characteristics of the wireless network require adoption of other security techniques to defend the network, including:

- Using strong encryption
- Deploying mutual authentication between the client and the network
- Modifying the Secure Set Service Identifier (SSID)
- Using identity-based networking to segment users to appropriate resources
- Ensuring management ports are secure

To protect the wired network from wireless threats, IT must also consider threat control and containment. Wireless threat control and containment are vitally important, especially in an era in which lack of threat control can lead to violations of regulatory controls or legal statutes. Even a "no Wi-Fi" policy is no guarantee of security against these threats without a comprehensive RF monitoring solution. For example, rogue access points can be brought in by employees, and notebook computers with embedded Wi-Fi can connect to neighboring networks, which can create security holes.

By working together, both Intel and Cisco address such security vulnerabilities—for example, by utilizing roaming profile rules for the Cisco Unified Wireless Network as well as the Intel® Centrino® mobile technology client. Wireless network security is dramatically enhanced when both the access point infrastructure and the client are locked down. The last thing IT wants to worry about is clients roaming to rogue access points or a user setting up their own ad hoc network to some other notebook computer or device.

Based on a multilayered approach to securing wireless networks, IT directors can have confidence when deploying production-scale networks. Such an approach ensures the integrity of the information passed over the wireless network and maintains adequate barriers to protect internal resources.

Cisco and Intel Enhance Security

Cisco Systems and Intel have worked extensively to improve both the robustness and manageability of wireless security. Both companies have:

- Taken a leading role in the standards bodies
- Delivered the Cisco Compatible Extensions program to bring the latest Wi-Fi security standards to Wi-Fi devices
- Provided customers with security standards such as WPA2 and EAP-FAST
- Committed to delivering improved security features such as management frame protection

Myth #3: Wireless networks are complex to deploy and support

One of biggest changes in deploying wireless networks has been in client management. The mobility of wireless clients presents IT departments with increased complexity of managing clients to maintain the integrity and support of the enterprise network. Intel® Centrino® mobile technology overcomes these barriers.

Intel® Centrino® mobile technology includes built-in remote management capabilities and powerful tools for IT departments to deploy and manage wireless clients in the enterprise. By centrally managing end user wireless configurations, IT departments minimize TCO and strengthen corporate wireless security policies. And because of tested interoperability between Intel® Centrino® mobile technology clients and the Cisco Unified Wireless Network, wireless clients seamlessly integrate into existing enterprise infrastructures.

Using the Intel® PRO/Wireless Administrator Tool, IT departments can create profiles with all the network access and enterprise-class security (WPA2, 802.11i and Cisco LEAP authentication protocol) requirements to fully control wireless clients within their environments. These advanced client profiles ensure wireless clients comply with corporate policies when accessing the corporate network. For wireless network users, the Intel® Centrino® mobile technology client experience is secure and seamless. Wireless network connectivity is streamlined with profiles that automatically connect to specified in-range networks.

Complete client installation packages that include connection profiles, driver and application software, security settings and more can be seamlessly distributed using existing network software distribution tools. Using different profiles, users also have the flexibility to connect to wireless networks outside the enterprise using the free administrator tool provided with Intel PROSET/Wireless Software.

“Lights-out” remote management support built into Intel® Centrino® mobile technology notebook computers enable WLAN connections to be maintained even when no user is logged in. Combined with Wake on WLAN (WoWLAN) support that allows remote wake up of notebook computers, administrators can push critical security updates and other software to keep clients in compliance with corporate network policies.

The Cisco Unified Wireless Network provides a variety of features to decrease the complexity of wireless deployment and management. As enterprises strive to decrease the complexity of management, having a unified management view across all domains enhances the ability to maintain unified network policies and detect and respond to alerts more quickly. A centralized management solution reduces training costs and allows IT administrators to be more flexible when managing Internetworking issues.

The wireless RF domain has a special set of characteristics that make managing it more challenging than managing the wired network. These challenges relate to the ever-changing nature of the RF environment and the fact that most enterprises lack in-house RF expertise. The Cisco Unified Wireless Network takes the complexity out of RF management by supporting a variety of RF-specific management tools such as dynamic channel assignment, RF interference mitigation, client load balancing, and power transmit control. These tools provide visibility into the wireless network. Using these tools, network managers can view performance, usage, availability, and reliability statistics from a single interface across wired and wireless networks. The combination of these features supports ongoing and automated site survey services to help ensure that the wireless network provides optimal coverage and capacity.

Cisco and Intel Lower Complexity

Cisco and Intel understand the complexities involved in deploying and managing a business-class wireless network. The two companies have worked together on the following solutions:

- The Cisco Compatible Extensions program to provide simple interoperability between wireless clients and infrastructure
- A strong focus on quality assurance and testing to ensure stable and highly available products
- Automated configuration and deployment services such as RF site surveying and client configuration for lower total cost of ownership

Myth #4: Wireless networks are immature

Thanks to Cisco and Intel collaboration, mature IEEE wireless networking standards, and third-party vendor support, wireless networks deliver a mature networking solution and provide a platform for enhanced value-added services to extract additional return from wireless networks.

Intel Cisco Business Class Wireless Suite

The Intel-Cisco strategic alliance, based on a technology collaboration called Business Class Wireless Suite ensures full capability between Intel® Centrino® Duo mobile technology and Cisco Unified Wireless Network products. Business Class Wireless Suite contains innovative wireless features that provide customers who use products from both Intel and Cisco with additional interoperability. Business Class Wireless Suite Version 1.0 focuses on two core areas: enhanced wireless VoIP support and smart access point selection technology.

> **"Our employees enjoy the freedom of working anywhere—conference rooms, common areas, cafeterias—just as productively as if they were at their desks."**
>
> — **Sylvia Stump**
> Wireless Program Manager
> Intel IT

Wireless VoIP

Market estimates show voice over IP (VoIP) clients are expected to grow 70 to 80 percent per year, while VoIP use over wireless LAN is expected to grow 300 percent by 2007. Working together and with third-party VoIP soft phone vendors, Intel and Cisco deliver optimized mobile VoIP experiences with higher audio fidelity and improved roaming capability during phone calls. By building specific capabilities into the Intel® PROSet/Wireless driver such as wide-band codec support and enhanced Cisco WLAN statistic support, the improved VoIP experience is seamless to the end user. The unique APIs added to the Intel® PROSet/Wireless driver relay enhanced WLAN statistics from the Cisco Unified Wireless Network to the third-party soft phone software. Enhanced WLAN statistics give soft phone software greater flexibility in determining audio codec and roaming decisions, resulting in a higher quality VoIP experience within an enterprise environment.

Smart Access Point Selection

Another key feature of Business Class Wireless Suite v1.0 is the ability to provide client and access point load balancing. Load balancing using Business Class Wireless Suite improves client throughput and packet reliability, and optimizes WLAN infrastructure investments. Clients typically associate with an access point that has the strongest radio signal without regard to the current access point (AP) throughput or packet retries. With Business Class Wireless Suite Smart AP Selection technology, the client periodically gathers statistics from the Cisco WLAN infrastructure to determine if a better connection with another access point would increase throughput or reliability or both. For example, a tight grouping of clients may all associate to the closest access point, even if the access point is overwhelmed with network traffic. With Business Class Wireless Suite, an Intel® Centrino® Duo mobile technology notebook computer could see that more distant access point would give better throughput based upon the statistics received from the Cisco WLAN infrastructure.

Intel Wireless Campus Case Study

Many enterprise employees already use Wi-Fi within their own homes and other hotspot locations. Wi-Fi delivers more freedom and flexibility. It's a natural extension for users to use Wi-Fi in the workplace. When Intel employees walk through the doors of the Jones Farm campus, in Hillsboro, Oregon, their Intel® Centrino® mobile technology notebook computers detect the Cisco primary WLAN and are automatically logged on to the network. Employees open and log into their notebook computers—and are immediately connected.

With nearly 6000 employees, the Intel Jones Farm campus has adopted wireless as its primary method of network access on a wide scale. The Intel IT group accomplished the engineering feat using Cisco Business Class Wireless Suite, which combines the Cisco Unified Wireless Architecture and Intel® Centrino® mobile technology notebook computers.

The idea of using wireless for primary access arose when the Intel IT wireless team began investigating ways to increase employee productivity and reduce network costs. In 2004, Intel IT was managing three separate networks—LAN, WLAN, and telephony—which essentially tripled operational costs. The new wireless deployment converges data, voice, and video all on the same wireless LAN reducing capital expenses for cabling while at the same time satisfying employee preference for mobility.

Security, reliability, performance, and mobility are at the forefront of the business units within Intel's Jones Farm Campus which includes a wide variety of disciplines such as marketing, engineering, test validation, legal, R&D etc. Intel expects that when the deployment is complete in 2006, 75 percent of campus employees will use the primary wireless network exclusively.

Myth #5: Wireless provides no business value beyond mobile data

Wireless technology is credited with improving the flow of information unfettered by the constraints of location or time. The impact of this has been improved productivity and faster and more effective decision making. Businesses are embracing the promise of wireless with the expectation that the technology will enable its employees to perform better. While several studies (and common sense) confirm that there is a relationship between pervasive business wireless deployments and improved employee productivity, wireless brings broader benefits to business. Using mobility, the business can become more agile and efficient by morphing traditional business applications to be mobility-aware.

Cisco and Intel Deliver Mature Wireless

- Cisco and Intel have combined their efforts to bring wireless technology from early adoption to maturation. Examples of this focus include:
- Founding members of the Wi-Fi Alliance to drive interoperability and increase market adoption of wireless networking.
- Relentless focus on standards development to deliver enhancements in wireless network features such as security, management, quality of service and throughput.

However, wireless networks alone are not what allow businesses to achieve these benefits. Mobility services enabled by the wireless LAN are the missing middle layer that connects the wireless network to business applications. Through mobility services, the wireless network not only improves employee productivity, but also creates new ways of doing business, improves efficiencies, and opens doors for expanded revenue generation.

Wireless LAN Mobility Services

Wireless LAN mobility services are the interface between the wireless network and business applications. Services that are currently providing businesses with the most value include location, voice, guest access, and security services. They are defined as follows:

- **Location services**—Locate any Wi-Fi device quickly to support enhanced network security, management, and troubleshooting, as well as to enable location-based applications through a rich, open API.
- **Voice services**—Extend the seamless mobility of the Cisco Unified Wireless Network to enable business communications using Wi-Fi clients with end-to-end quality of service (QoS) and manageability.
- **Guest access services**—Allow customers, vendors, and other non-employees to wirelessly access network resources, with privileges based on user type and physical location, without compromising the enterprise security.
- **Security services**—Unify wired and wireless security and ensure network information integrity by enabling location-based authentication and precise detection, identification, and prevention of wireless threats.

The integration of wireless LAN mobility services into business logic significantly increases the value of the wireless network. The following are examples of emerging applications and benefits enabled by wireless LAN mobility services.

Location Services

- **Asset tracking**—The business uses active RFID tags to quickly and accurately locate important assets. The types of assets to be tracked vary based on the industry. Examples of such tracked assets include heart monitors in hospitals, handheld scanners in retail locations, servers in data centers, and work-in-progress in manufacturing.
- **Presence**—Presence allows the network to adjust the delivery of its services based on the location and availability of the user. As an example, the network may elect to contact a user in a conference by text message instead of by calling in order to avoid disruption.

Voice Services

- **Cost avoidance**—Cisco customers' claim that as many as 50 to 80 percent of corporate cellular calls are made between employees located within the same campus. Wireless voice over IP allows the business to route these calls over the internal Wi-Fi network and avoid the cellular carrier rate charges.

- **Universal telephony**—Many companies have locations in which voice services are not currently available for all employees, such as retail stores, distribution centers, warehouses, and manufacturing floors. By deploying wireless voice over IP, the business can provide voice services, including a direct dial extension and individual voicemail to every employee. Mobile telephony improves productivity by increasing call completion and reducing the time spent accessing voicemail.

Guest Access Services

- **Decreased support costs**—Traditionally, non-employees who visit the business either go without network access or rely on the IT department to securely configure their PCs to work on the network. By providing wireless guest access, the business can significantly reduce the cost of providing network access to guests and contractors and do it in a secure and manageable way.
- **Partner services**—Guest services are ideal as a single network platform for offering secure network access to multiple constituents. Locations such as factories, retail stores, and airports often require a single infrastructure for multiple companies. Using guest access, a business can provide its partners with wireless network access without the need for each partner to individually deploy their own.

> **"The contractors and partners that come to our offices arrive expecting an outlet to the internet. Without this access, most meetings or projects are delayed as we work to find ways around the access issue."**
>
> — **Chris S. Thomas**
> Chief Strategist
> Intel

Security Services

- **Physical security**—The pervasiveness of the wireless network lends itself to physical security applications such as video surveillance and facility control (for example, badge reading). While these are not new applications, physical security can be delivered in a more cost-effective and pervasive manner than previously possible.
- **Rogue network containment**—Businesses continue to struggle with the containment of rogue wireless networks because of the ease with which users can purchase and deploy consumer-grade Wi-Fi access points. Integrated RF monitoring capabilities allow the wireless system to detect the presence of rogue activity and contain it. By combining RF monitoring with location services, the network can provide precise location details on where the rogue activity is occurring so that it can be physically removed.

Pervasive wireless deployments are providing business benefits far beyond productivity improvements. With wireless LAN mobility services, businesses can now deploy innovative applications to change business processes and provide new avenues for revenue growth and potential competitive advantage. As the adoption of wireless and mobile solutions expands, businesses will derive greater benefit from their infrastructure.

VoIP over Wi-Fi Case Study

Voice over IP has seen steady growth in the enterprise, with corporations taking advantage of the convergence of voice on their LAN or WAN infrastructure. With the same advantages of VoIP on wired networks in the enterprise, corporations are extending VoIP over Wi-Fi to reduce costs and improve communication efficiencies.

For many businesses, making voice calls by telephone is crucial for communicating in a timely manner with customers and staff and between offices. By providing the underlying technologies for security, quality of service, and improved voice codecs, Cisco and Intel help IT departments leverage their mobile users' unique working environments to aggressively compete in today's marketplace.

In August 2005, Shanghai GM deployed Intel® Centrino® mobile technology notebook computers with the Cisco IP Communicator soft phone application running in a wireless network environment. With the Cisco and Intel solution, Shanghai General Motors achieved communication goals that included the reduction of operating expenses and the improvement of seamless communications to gain a competitive advantage through faster response to market changes.

Cisco, Intel, and the Business Value of Wireless

Cisco and Intel recognize that technology adoption must be driven by a tangible business case. The following are examples of how the two companies have worked to increase the business relevance of wireless and mobility:

- Joint research initiatives with leading industry analyst firms to define ROI models for pervasive wireless adoption and the use of mobility services.
- A focus on delivering solutions capable of supporting mission critical business application

Conclusion

The new generation of standards, technologies and products are busting the outdated myths that have kept IT from deploying pervasive, enterprise-wide wireless networks. Cisco Systems and Intel are at the forefront of building solutions that deliver business value, while at the same time eliminating the remaining barriers to adoption. As a result, adopters of wireless technologies are experiencing tangible improvements in productivity that is delivering a quantifiable return on investment. The impact of issues such as security and management is being dramatically reduced through a continued focus on delivering standards-based improvements. New technology architectures have decreased the complexity of deployment and ongoing support, which in turn decreases the resources required to maintain a pervasive wireless network.

These improvements, in combination with exciting new wireless LAN mobility services like voice, location, guest access, and advanced security, derive even more value from a wireless solution. Only through a pervasive wireless deployment can business equip itself with the tools required to continue to increase productivity, retain customers and employees, and drive incremental value, revenue growth, and competitive advantage.

For more information, visit: www.ciscointelalliance.com

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
www.cisco.com

www.intel.com