

# White Paper on WLAN

## Introduction

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the face of the earth. Hundreds of millions of people exchange information every day using pagers, cellular telephones, and other wireless communication products. With tremendous success of wireless telephony and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere they venture.

Originally a second-class citizen in terms of transfer speeds, today's 802.11 products, which transmit in the unlicensed spectrum at 2.5GHz, are capable of speeds of up to 11Mbps--more than enough speed to keep up with the average Internet connection.

802.11 Standards

### **802.11a**

**Description:** A physical layer standard for WLANs in the 5GHz radio band. It specifies eight available radio channels (available radio spectrum in some countries would permit the use of 12 channels). Maximum link rate of 54-Mbps per channel, but maximum user data throughput will be approximately half of this and all users of the same radio channel share the throughput. The data rate decreases as the distance between the user and the radio access point increases.

**Comments:** In most offices, the data throughput will be greater than for 11b. Also, the greater number of radio channels (eight as opposed to three) gives better protection against possible interference from neighboring access points. 802.11a-compliant products are available in North America, but there will not be a wide choice of vendors or lower prices until the second half of 2002. Conformance is shown by a Wi-Fi5 mark from WECA.

### **802.11b**

**Description:** A physical layer standard for WLANs in the 2.4GHz radio band. It specifies three available radio channels. Maximum link rate of 11-Mbps per channel, but maximum user throughput will be approximately half of this because all users of the same radio channel share the throughput. The data rate decreases as the distance between the user and the radio access point increases.

**Comments:** Products are in volume production with a wide selection at competitive prices. Installations may suffer from speed restrictions in the future as the numbers of active users increase, and the limit of three radio channels may cause interference from neighboring access points.

When making the decision of whether to go with 802.11a or 802.11b, think about the performance, range, and interoperability issues. Also, here are some general guidelines that will help you make the right decision:

**Consider using 802.11b if:**

1. Range requirements are significant. For larger facilities, such as a warehouse or department store, 802.11b will provide the least costly solution because of fewer access points.
2. You already have a large investment in 802.11b devices. The relatively high costs associated with migrating from a large-scale 802.11b system to 802.11a will be difficult to sell to the company's financial decision makers.
3. End users are sparsely populated. If there are relatively few end users that need to roam throughout the entire facility, then 802.11b will likely meet performance requirements because there are fewer end users competing for each access point's total throughput. Unless there are significant needs for very high performance per end user, then 802.11a would probably be overkill in this situation.

**Consider using 802.11a if:**

1. There's need for much higher performance. By far the top driver for choosing 802.11a is the need to support higher end applications involving video, voice, and the transmission of large images and files. For these applications, 802.11b probably won't be able to keep up.
2. Significant RF interference is present within the 2.4 GHz band. The growing use of 2.4 GHz wireless phones and Bluetooth devices could crowd the radio spectrum within your facility and significantly decrease the performance of 802.11b wireless LANs. The use of 802.11a operating in the 5 GHz band will avoid this interference.
3. End users are densely populated. Places such as computer labs, airports, and convention centers need to support lots of end users in a common area competing for the same access point, with each user sharing the total throughput. The use of 802.11a will handle a higher concentration of end users by offering greater total throughput.

**802.11d**

**Description:** 802.11d is supplementary to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It will allow access points to communicate information on the permissible radio channels with acceptable power levels for user devices. The 802.11 standards cannot legally operate in some countries; the purpose of 11d is to add features and restrictions to allow WLANs to operate within the rules of these countries.

**Comments:** In countries where the physical layer radio requirements are different from those in North America, the use of WLANs is lagging behind. Equipment manufacturers do not want to produce a wide variety of country-specific products and users that travel does not want a bag full of country-specific WLAN PC cards. The outcome will be country-specific firmware solutions.

### **802.11e**

**Description:** Supplementary to the MAC layer to provide QOS support for LAN applications. It will apply to 802.11 physical standards a, b and g. The purpose is to provide classes of service with managed levels of QOS for data, voice and video applications.

**Comments:** 11e should provide some useful features for differentiating data traffic streams. Many WLAN manufacturers have targeted QOS as a feature to differentiate their products, so there will be plenty of proprietary offerings before 11e is complete. However, the successes or failures of these products will determine how eager manufacturers will be to adopt standard 11e features.

### **802.11f**

**Description:** This is a "recommended practice" document that aims to achieve radio access point interoperability within a multivendor WLAN network. The standard defines the registration of access points within a network and the interchange of information between access points when a user is handed over from one access point to another.

**Comments:** 802.11f will reduce vendor lock-in and allow Multi Vendor infrastructures.

### **802.11g**

**Description:** A physical layer standard for WLANs in the 2.4GHz and 5GHz radio band. It specifies three available radio channels. The maximum link rate is 54-Mbps per channel--compared with 11 Mbps for 11b. The 802.11g standard uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 11b, it also supports complementary code keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation.

**Comments:** Speeds similar to 11a and backward compatibility may appear attractive but there are modulation issues: Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group compromised by including both types of modulation in the draft standard. With the addition of support for 11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late and too complex compared with 11a. However, there are advantages for vendors looking to supply dual-mode 2.4GHz and 5GHz products, in that using OFDM for both modes will reduce silicon cost. If 802.11h fails to obtain pan-European approval by the second half of 2003, then 11g will become the high-speed WLAN of choice in Europe.

### **802.11h**

**Description:** This standard is supplementary to the MAC layer to comply with European regulations for 5GHz WLANs. European radio regulations for the 5GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest

user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar.

**Comments:** Completion of 11h will provide better acceptability within Europe for IEEE-compliant 5GHz WLAN products. A fast-dwindling group will continue to support the alternative Hyper LAN standard defined by ETSI. Although European countries such as the Netherlands and the United Kingdom are likely to allow the use of 5GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003, possibly longer.

### **802.11i**

**Description:** Supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1x forms a key part of 802.11i.

**Comments:** Security is a major weakness of WLANs. Vendors have not improved matters by shipping products without setting default security features. In addition, the WEP algorithm weaknesses have been exposed. The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2002. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility.

### **Applications for Wireless LANs**

Wireless LANs frequently augment rather than replace wired LAN networks-often providing the final few meters of connectivity between a backbone network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- Doctors and nurses in hospitals are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- Consulting or accounting audit engagement teams or small workgroups increase productivity with quick network setup.
- Network managers in dynamic environments minimize the overhead of moves, adds, and changes with wireless LANs, thereby reducing the cost of LAN ownership.
- Training sites at corporations and students at universities use wireless connectivity to facilitate access to information, information exchanges, and learning.

- Network managers installing networked computers in older buildings find that wireless LANs are a cost-effective network infrastructure solution.
- Retail storeowners use wireless networks to simplify frequent network reconfiguration.
- Trade show and branch office workers minimize setup requirements by installing preconfigured wireless LANs needing no local MIS support.
- Warehouse workers use wireless LANs to exchange information with central databases and increase their productivity.
- Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.
- Senior executives in conference rooms make quicker decisions because they have real-time information at their fingertips.

### **Benefits of WLANs**

The widespread strategic reliance on networking among competitive businesses and the meteoric growth of the Internet and online services are strong testimonies to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug in, and network managers can set up or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

**Mobility**-Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.

**Installation Speed and Simplicity**-Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

**Installation Flexibility**-Wireless technology allows the network to go where wire cannot go.

**Reduced Cost-of-Ownership**-While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds, and changes.

**Scalability**-Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allow roaming over a broad area.

## **Site Survey**

Before setting up a WLAN, professional site survey is better as it takes the risk out of wireless LAN setup. The following are the steps to be followed for a site survey.

- A site survey team has to define the installation to the customer and this includes identifying the space to be covered, devices to be used and the interface between wired and the wireless.
- Another important issue is the placement of access points and antennas that will maintain maximum amount of coverage and signal strength for optimal performance. Locate Access points towards the center of the building rather than near windows. Plan coverage to radiate out to the windows, but not beyond. If the access points are located near the windows, a stronger signal will be radiated outside our building making it easier for people to find us.
- Care has to be taken about all the different hidden things that cause degradation in a wireless network setup. For example if we have to shoot down an RF signal down an aisle then we can put up a directional antenna that doesn't interfere with everything else.
- Last leg of installation is the interface between WLAN and the wired. A couple of key considerations are the amount of broadcast traffic and bandwidth utilization on the existing network. Unnecessary flooding of broadcast traffic through the radio reduces wireless performance. If network utilization is already high then we are going to cause nothing but problems by adding devices to an already unstable network.

An important issue that has to be addressed is Roaming. Some times if the access points are not setup properly then the network may fail to recognize when devices roam and a dropped network connection may occur. We can use IP Tunneling to avoid this issue.

## **WLAN Customer Considerations**

### **Range/Coverage**

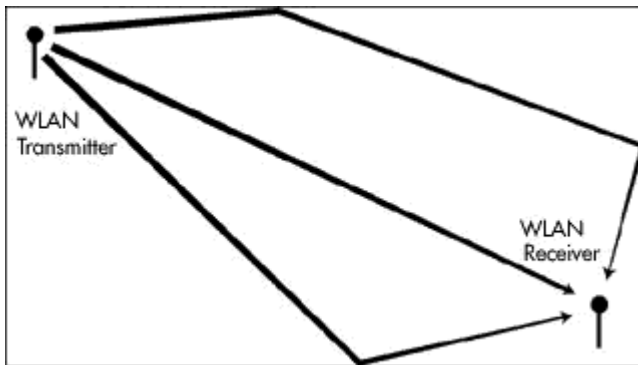
The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Most wireless LAN systems use RF because radio waves can penetrate many indoor walls and surfaces. The range (or radius of coverage) for typical WLAN systems varies from under 100 feet to more than 500 feet. Coverage can be extended, and true freedom of mobility via roaming, provided through micro cells.

### **Throughput**

As with wired LAN systems, actual throughput in wireless LANs is dependent upon the product and how it is configured. Factors that affect throughput include airwave congestion (number of users), propagation factors such as range and multipath, the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the WLAN. Typical data rates range from 1 to 11 Mbps.

### **Multipath Effects**

As Figure 9 shows, a radio signal can take multiple paths from a transmitter to a receiver, an attribute called multipath. Reflections of the signals can cause them to become stronger or weaker, which can affect data throughput. Affects of multipath depend on the number of reflective surfaces in the environment, the distance from the transmitter to the receiver, the product design and the radio technology.



**Figure 9. Radio Signals Traveling over Multiple Paths**

### **Integrity**

Wireless data technologies have been proven through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the workplace. Robust designs of WLAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

### **Interoperability with Wired Infrastructure**

Most wireless LAN systems provide industry standard interconnection with wired systems including Ethernet (802.3) and Token Ring (802.5). Standards based interoperability makes the wireless portion of the network completely transparent to the rest of the network. Wireless LAN nodes are supported by network operating systems (NOS) in the same way any other LAN node via network device drivers. Once installed, the NOS treats wireless nodes like any other component of the network.

### **Interoperability with Wireless Infrastructure**

There are several types of interoperability that are possible between wireless LANs. This will depend both on technology choice and on the specific vendor's implementation. Products from different vendors employing the same technology and the same implementation typically allow for the interchange of adapters and access points. An eventual goal of the IEEE 802.11 specification, currently being drafted by a committee of WLAN vendors and users, is to allow compliant products to interoperate without explicit collaboration between vendors.

### **Interference and Coexistence**

The unlicensed nature of radio-based wireless LANs means that other products that

transmit energy in the same frequency spectrum can potentially provide some measure of interference to a WLAN system. Microwave ovens are a potential concern, but most WLAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple WLAN systems. While co-located WLANs from different vendors may interfere with each other, others coexist without interference. This issue is best addressed directly with the appropriate vendors.

### **Simplicity/Ease of Use**

Users need very little new information to take advantage of wireless LANs. WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools. WLANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on WLANs. Finally, the portable nature of WLANs lets network managers pre-configure and troubleshoot entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.

### **Security**

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

### **Cost**

A wireless LAN implementation includes both infrastructure costs for the wireless access points and user costs for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed; access points range in price from \$800.00 to \$2,000.00. The number of access points typically depends on the required coverage region and/or the number and types of users to be serviced. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms, and range in price from \$200.00 to \$700.00. The cost of installing and maintaining a wireless LAN is generally lower than the cost of installing and maintaining a wired LAN for two reasons. First, a WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because WLANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead.

### **Scalability**

Wireless networks can be designed to be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

### **Battery Life for Mobile Platforms**

End-user wireless products are capable of being completely untethered, and run off the battery power from their host notebook or hand-held computer. WLAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.

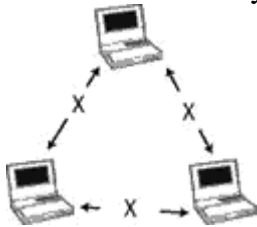
### **Safety**

The output power of wireless LAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health affects have ever been attributed to wireless LANs.

### **WLAN Configurations**

#### **Independent WLANs**

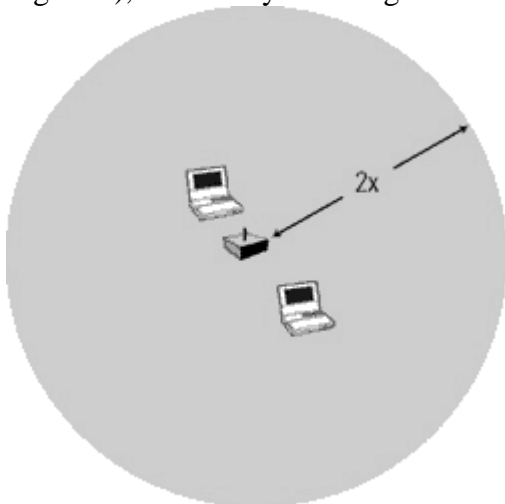
The simplest WLAN configuration is an independent (or peer-to-peer) WLAN that connects a set of PCs with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network (Figure 3). These on-demand networks typically require no administration or preconfiguration.



**Figure 3.**

Independent WLAN

Access points can extend the range of independent WLANs by acting as a repeater (see Figure 4), effectively doubling the distance between wireless PCs.



**Figure 4. Extended-Range Independent WLAN Using Access Point as Repeater**

### Infrastructure WLANs

In infrastructure WLANs, multiple access points link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus.

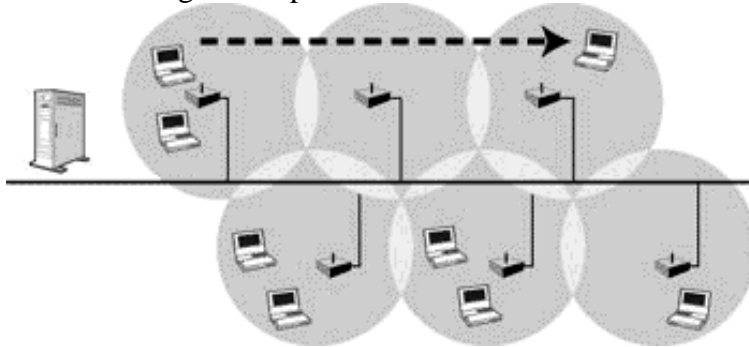
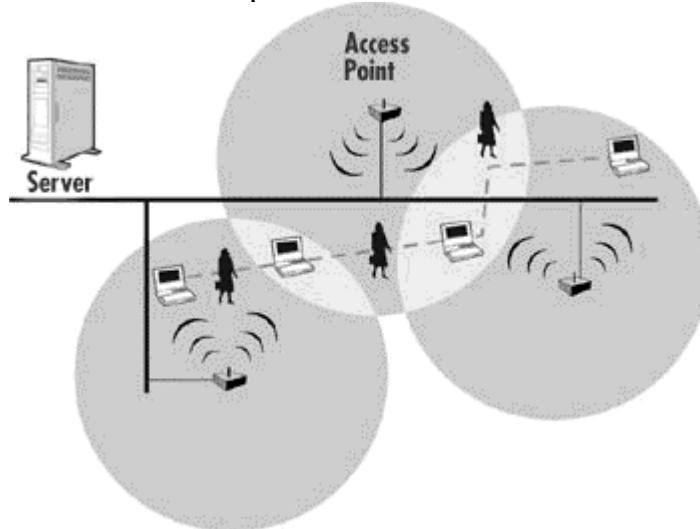


Figure 5. Infrastructure WLAN

### Microcells and Roaming

Wireless communication is limited by how far signals carry for given power output. WLANs use cells, called microcells, similar to the cellular telephone system to extend the range of wireless connectivity. At any point in time, a mobile PC equipped with a WLAN adapter is associated with a single access point and its microcell, or area of coverage. Individual microcells overlap to allow continuous communication within a wireless



network.

Figure 6. Handing off the WLAN Connection Between Access Points

### Keeping Your Wireless Network Safe

1. Enable WEP. Yes, WEP isn't secure as by now virtually everyone knows, but at least it's a first barrier. And best of all, it's free. Nearly all Wi-Fi certified products ship with basic encryption capabilities. (40-bit key WEP). If it's disabled then it's an invitation for someone to pay you a visit anytime.

2. Change the default SSID of the product but not to an SSID that reflects company's main names, divisions, or products. It just makes you too easy to target.
3. If your access point supports it, disable "broadcast SSID". As you take your access point out of the box, broadcast SSID is enabled which means that it will accept *any* SSID. By disabling that feature, the SSID configured in the client must match the SSID of the access point.
4. As a network administrator, you should periodically survey your site using a tool like NetStumbler to see if any "rogue" access points pop up. With the declining pricing of access points, it's not hard to imagine that a department might run out to Best Buy, buy a couple of NICs and an AP, and plug it into your corporate network. All of your hard work to "harden" your wireless network could be wasted if a rogue AP were plugged into you network behind your firewall.
5. Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it. If the MAC address of your NIC isn't in the table of the access point, you won't associate with it. And while it's true that there are ways of spoofing a MAC address that's been sniffed out of the air, it takes an additional level of sophistication to spoof a MAC address. The downside of deploying MAC address tables is that if you have a lot of access points, maintaining the tables in each access point could be time consuming. Some higher-end, enterprise-level access points have mechanisms for updating these tables across multiple access points of the same brand.
6. Consider using an additional level of authentication, such as RADIUS, before you permit an association with your access points. While it's not part of the 802.11b standard, a number of companies are optionally including some provision for RADIUS authentication. Intermec access points include a built-in RADIUS server for up to 128 MAC addresses.
7. If you're deploying a wireless router, think about assigning static IP addresses for your wireless NICs and turn off DHCP. It's true that it's more of an administrative overhead to manage, but we found a number of wireless networks that passed out IP addresses to us once we associated with the AP. Although a wireless sniffer could easily pick out IP addresses, by not passing them out, it just adds another barrier. It makes it tougher for the casual "drive by" to use your network.
8. If you're using a wireless router and have decided to turn off DHCP, also consider changing the IP subnet. Many wireless routers default to the 192.168.1.0 network and use 192.168.1.1 as the default router. We discovered one network that didn't give us an IP address, but we assumed that they were using the defaults. We were right. We configured our notebook with an IP address in the 192.168.1.0 network using 192.168.1.1 as the router address, and we had access to the Internet through their network.

9. Don't buy access points or NICs that only support 64-bit WEP. Some low-end products only support 64-bit (40 bit key) WEP, and as you know by now, even 128-bit WEP is universally considered not very secure. Note that some NICs may only require a driver upgrade to attain 128-bit WEP capability.
10. Only purchase access points that have flashable firmware. There are a number of security enhancements that are being developed, and you want to be sure that you can upgrade your access point.

### **Hackers Delight**

The specifications for 802.11 came under fire last year as encryption experts exposed flaws in its built-in security technology, Wired Equivalent Privacy. The flaws make networks using 802.11b (or its newer, faster, 54-mbps sibling, 802.11a) vulnerable to hackers located within range of these networks.

The 802.11i draft now circulating is for a security algorithm called Temporal Key Integrity Protocol. Developed with the help of some of the encryption experts that exposed WEP's vulnerabilities, TKIP, like WEP, is based on RC4 encryption--but implemented in a different way that addresses those vulnerabilities, Eaton says. Among other things it generates new encryption keys for every 10 kilobytes of data transmitted. Most, if not all, current Wi-Fi-certified products should be upgradeable to TKIP, Eaton adds. Those that can't be upgraded will still interoperate with products that use TKIP--but only using WEP for security.

### **Beyond TKIP**

The IEEE does not view TKIP as a long-term solution for wireless Ethernet security, however. Also in the works is a draft spec for an algorithm based on AES encryption. Considered more robust than TKIP, the AES algorithm would replace WEP and RC4. It would involve hardware optimization; so older 802.11x hardware will not be upgradeable in many cases.

The AES spec is primarily intended for newer hardware. Devices using the AES algorithm would still be able to interoperate with the older devices, but using the weaker security technologies.

### **Why it will work**

WLAN has all the makings of a disruptive and explosive technology: huge growth, a strong value proposition, multiple and expanding uses, industry standardization, and global standardization. There are flaws, but none is insurmountable, and none is nearly large enough to be anything more than a speed bump with respect to the billions of dollars of research and development already pointed into this space.

Lastly and most importantly, there is plenty of running room as we move from the corporation to the home to the campus to the airport to the hotel and potentially to a carrier-class level.

This truly is the next big thing.