

EXECUTIVE BRIEFINGS

EXECUTIVE GUIDES FOR STRATEGIC DECISION-MAKING

Riding the Wireless Wave

Learn how wireless is rapidly evolving into an essential tool for business.

OVERVIEW

Executive Summary2

EMERGING TECHNOLOGIES

Why WiMax?4
Vendors, Carriers Join Intel With WiMax Plans7
Mesh Moves Into the Wireless Office9
Mobile Computing's Energy Crisis12
Case Study: BP's Wireless Sensor Network15

WIRELESS LANS

Evaluate Risk Before Merging Wired and Wireless LANS16
Risk Redux: Common WLAN Vulnerabilities18
Wireless LANS Find Their Voice20

RFID

Early Adopters Send Mixed Messages About RFID22
RFID Moves Beyond Supply Chain Mandates24
Pushing RFID Deeper Into Manufacturing26
Generation 2 RFID and the ROI Challenge28
Case Study: RFID at Philips: Tagged and Tracked29

WIRELESS SECURITY

Wireless Security: The Enemy Is Us31
Wireless Security Requires Integration33
RFID Crack Raises Specter of Weak Encryption35



Executive Summary

YOU'RE GOING wireless. It's no longer a question of "if" — it's how and when. Or, more likely, where do you go from here with your current wireless implementation?

Here are some numbers:

• **60% of enterprises will upgrade or deploy wireless LANs in 2005.**¹

• **By 2007-2008, 65% of enterprises will have wireless applications deployed, with mobile devices outnumbering traditional PCs.**²

• **Total U.S. spending on wireless communications will grow by 9.3% this year, reaching \$158.6 billion. It's predicted to hit \$212.5 billion by 2008, with a 10% compound annual growth rate.**³

• **The use of WLANs will continue to increase in the enterprise through 2006, with voice over WLAN representing a particularly promising area of growth, as use skyrockets from 6% now to 27% by August 2006.**⁴

The biggest obstacle to wireless networking in years past — security — is still formidable, but new standards,

more awareness and new technologies are rapidly addressing that problem. Now IT managers are starting to worry more about implementation and performance.

ROI has been proved. TCO has been mapped. Productivity has been measured. The mandate has been given.

Now it's time to roll up your sleeves and get to work.

Here's a rundown on the current state of affairs in some key segments of the wireless industry and where they might be heading.

WLANs

Recent Wi-Fi standards have addressed security weaknesses and increased options for range, speed and frequency.

On the security front, the Institute of Electrical and Electronics Engineers (IEEE) in June 2004 ratified its 802.11i standard, and a few months later the Wi-Fi Alliance began granting Wi-Fi Protected Access 2 (WPA2) product certifications based on that standard.

WPA2 replaces the notoriously weak Wired Equivalent Privacy standard and the interim Wi-Fi Protected Access that the Wi-Fi Alliance developed to shore up WEP's holes while 802.11i/WPA2 was being developed.

IT managers can now be assured of a variety of secure, interoperable Wi-Fi products.

Know your A, B and Gs

Now attention turns to the more mundane concerns of usability and manageability. The newest Wi-Fi "flavor" is 802.11g. It joins 802.11b and 802.11a. 802.11g operates in the same frequency band as

802.11b (2.4 GHz), so it's interoperable with b devices, but it allows for throughput of 54Mbit/sec. as opposed to b's 11Mbit/sec. (With overhead, interference and attenuation factors, though, actual speeds are usually at least half the claimed peak.)

Meanwhile, 802.11a operates in a higher frequency band (5 GHz) and offers 54Mbit/sec. throughput. Being in a less-crowded spectrum and having more channels available, it's less prone to interference than b and g.

On the downside, it has a shorter range — a drawback of higher frequencies — and a higher cost per device.

The common rule of thumb is to use b/g products where greater coverage is needed and cost is a big factor, and to consider 802.11a devices in small, congested areas where higher throughput is valued more than range.

The most popular devices sold today are b/g combinations, and if you don't mind paying a price premium, you can get devices that support all three flavors.

For the future, the IEEE is working on an 802.11n standard that promises speeds of 100Mbit/sec. It's expected to be ratified near the end of 2006.

In the meantime, several vendors are offering nonstandard, "pre-N" products with higher speeds, if you don't mind going with proprietary technology.

Other standards being developed will address quality of service — important for voice-over-WLAN applications — roaming and other issues.

Computerworld editor in chief **Don Tennant** • Executive briefings editor **Mitch Betts**
 • Designer **Julie Quinn** • Design director **Stephanie Faucher** • Managing editor/production **Michele Lee DeFilippo** • Copy editors **Bob Rawson, Eugene Demaitre, Mike Parent, Monica Sambataro**

Emerging Technologies

WiMax: The highly touted WiMax wireless broadband technology could see partial implementation by the end of 2005. The first part of the standard, IEEE 802.16-2004, will provide fixed 70Mbit/sec.-per-channel network service at up to 31 miles. A second part of the standard, IEEE 802.16e, will address mobile service and is expected no earlier than late 2006 and perhaps not until 2008.

Potential uses are as a Wi-Fi backhaul service, to provide broadband connectivity to small and midsize businesses in sparsely populated areas, and for enterprise disaster recovery.

In a significant push to the industry, Intel Corp. in April 2005 shipped its Rosedale WiMax chip, which conforms to the IEEE 802.16-2004 standard. Products using the new chip are expected to be certified and shipped before the end of 2005.

Mesh: In mesh networking, free-standing, nonwired network nodes communicate with one another and form self-configuring networks, with only one node required to hook into a wired LAN. The other nodes are simply plugged into an electrical outlet, so cabling is much less of an issue.

IT managers again are faced with proprietary, nonstandard mesh products until the IEEE's 802.11s standard is ratified and resulting products are available. The IEEE's mesh group first met in July 2004 and

called for proposals. Industry heavyweight Intel provided its proposals for the standard in early March 2005, and a ratified standard may not come until 2008 or later.

In the meantime, proprietary products offer an alternative to standard WLAN network topologies in certain applications, such as hard-to-wire areas or places where you need quick-and-dirty installations that might change often.

Improved batteries: Increasing laptop capabilities means increasing power consumption, which means decreasing battery life — a big problem for mobile workers. Battery life has been identified as the No. 1 complaint about laptops and one of the top concerns for laptop purchasers.

But there have been no revolutionary breakthroughs in battery technology. Improvements have been incremental. Research for future technologies has centered on fuel cells, but they have many practical disadvantages that have yet to be resolved. Some analysts predict that fuel cells won't make inroads into the laptop battery market before 2010.

So for now, look for small increases in battery life resulting from a combination of improved battery technology and reduced power consumption.

Low-power mobile chips were introduced in 2003 and are now standard. In 2006 Intel is expected to ship a dual-core mobile chip, code-named Yonah, that should lengthen battery life, because two low-

power processors perform better and use less power than one high-power processor. And manufacturers have committed to reducing power consumption of other components, including the display, which draws the most power.

So the goal of a reliable eight hours of use could soon be at hand.

RFID: Having cut its teeth in retail supply-chain applications, this technology is maturing in that market while broadening its scope. More and more businesses are beginning to use RFID technology for business-driven, niche operations outside the supply chain.

That trend should help spur tremendous growth in the industry. In 2004, IDC predicted that the market for RFID technology in the U.S. retail supply chain will rise from \$91.5 million in 2003 to \$1.3 billion in 2008, with even more significant growth possibly following that.

An international RFID standards body, EPCglobal, in late 2004 approved a standard called Class-1, Generation-2. It specifies communications protocols, reduces interference problems, increases tag-reading speed and improves security. Large-scale shipment of standards-based tags are expected in the third quarter of 2005.

Standards-based tags and readers should also eventually cost less, which addresses another impediment to widespread RFID adoption quoted by company executives.

Besides the supply chain, current RFID applications include tracking patients in hospitals, tracking animals on farms, automatically processing toll booth payments and acting as sensors in hazardous areas such as oil wells. In the future, it might be common to track books in libraries, visitors to theme parks and employees in your company. And many more potential uses exist in areas such as the military, law enforcement and security.

Outlook

With the wireless industry in its relative infancy, IT managers need to be cautious in their implementation plans. Important standards are just now coming into place, but companies may not be able to wait for standardized and interoperable products. You may need to go with a proprietary solution now. That will entail a lot of research and consultation to find the best fit for your current needs while keeping your options open for a standardized solution in the future.

Read this Executive Briefing to get prepared for the ride.

FOOTNOTES

¹Forrester Research Inc.

²Meta Group Inc.

³Telecommunications Industry Association

⁴Infonetics Research

Why WiMax?

THE HOT network technology du jour is WiMax, an informal term that covers two emerging broadband wireless standards for metropolitan-area networking. WiMax promises alternate routes to land lines for disaster recovery and relief from the price and service tyranny of the incumbent local-exchange carriers. It also has a compelling high-speed mobile component.

WiMax has the potential for what Carlton O'Neal, vice president of marketing at Tel Aviv-based broadband wireless manufacturer Alvarion Ltd., describes as "high-quality broadband everywhere that mirrors your connectivity experience in the office."

To the casual observer, WiMax backhaul services might not seem substantially different from today's broadband wireless access (BWA) services, though speed and coverage range are expected to improve. However, having standards for non-line-of-sight (NLOS) BWA products will create economies of scale and vendor interoperability, which should help WiMax-based services proliferate beyond the niches where BWA services can currently be found. This means that the benefits of BWA as a land-line alternative

should theoretically become available to more sites and users.

"Fixed" access services and products will emerge in 2006, followed by the mobile flavor a year or so later. There are two corresponding WiMax standards:

IEEE 802.16-2004 for fixed point-to-point and point-to-multipoint wireless access. It's akin to a faster, airborne version of Digital Subscriber Line (DSL) or cable-modem services and became the industry's first NLOS BWA standard last June.

IEEE 802.16e, for mobile wireless access from laptops and handhelds. It's analogous to a faster version of third-generation telecommunications technology. WiMax proponent Intel Corp. has promised 802.16e-enabled laptops by early 2007.

Intel is also involved in the 802.16-2004 standard effort. The vendor says it's providing silicon to Alvarion, Proxim Corp. and Redline Communications Inc., which are manufacturing last-mile fixed products for the carrier market.

The technologies based on the two standards operate in licensed and unlicensed frequency bands below 11 GHz. The standards are being overseen from a market-acceleration standpoint by a 230-company consortium called the WiMax Forum.

Enterprise Impact

WiMax is being deployed from the top down as a carrier technology first, which means that schedules for service availability are dependent on widespread testing and buy-in. WiMax product standards certification and interoperability testing, overseen by the WiMax Forum and to be conducted by independent test lab

Cetecom Spain in Malaga, is slated to begin in 2005.

Once services become available, growing business sites should gain inexpensive broadband access with speeds between T1 and T3 line capabilities. And because they're airborne, these services can be quickly deployed—often in a day's time—and bypass lengthy ILEC lead times.

"Every enterprise struggles with the cost of [local] access, which is often 40%" of a telecommunications bill, says David Willis, an analyst at research firm Meta Group Inc. "The natural monopolies have starved out local competition. But WiMax doesn't require dealing with lobbyists or tariffs."

Adds Alan Menezes, vice president of marketing at Aperto Networks Inc., a maker of BWA products in Milpitas, Calif., "Enterprises gain alternatives to the [regional Bell operating companies] and backups to terrestrial T1 and fiber links that can be cut at the same time." In addition, WiMax comes ready-made with provisions for quality of service, so many prestandard services already support voice over IP, unlike many DSL and cable-modem options.

And standards-based technology should drive down customer premises equipment (CPE) costs for fixed connections, from about \$800 today to \$300 to \$400 in 2006 or 2007, says Bob Egan, president of Mobile Competency Inc., a consultancy in Providence, R.I. Meta Group is even more bullish: Willis says he expects WiMax CPE to drop to \$70 by 2007.

Finally, businesses can buy WiMax-certified products to install in their campus-area networks as alternatives to private fiber connections and

QoS Advantage

A big WiMax selling point is that it comes with quality of service built in. Struggles with standardizing QoS have been a downfall of WiMax's cousin, 802.11 wireless LAN technology, or Wi-Fi, whose 802.11e QoS standard extension seems perennially six months away from being ratified.

What's actually described in the WiMax specification are four types of scheduling services for polling client devices about whether they have packets to send.

Here are the basics of the four scheduled services specified by WiMax (in all cases, the base station controls scheduling):

1) Unsolicited Grant Service (UGS) will support VoIP without silence suppression to support a continuous packet stream.

2) Real-Time Polling Service (rtPS) will support VoIP with silence suppression (supporting packets sent only when a person is talking) and MPEG video.

3) Non-Real-Time Polling Service (nrtPS) involves polling devices periodically to maintain a minimum data rate for applications such as file transfers.

4) Best Effort means that there are no guarantees of service quality. But the speed and bandwidth provided by WiMax make it a good best-effort bet.

more-complex wireless bridging options.

Disaster Recovery Shoo-in

According to vendors, service providers and analysts, starting in 2007, an important 802.16-2004 application for enterprises will be disaster recovery—whereby the wireless link serves as either the primary or the backup connection. The reason is that two terrestrial links are likely to be cut simultaneously.

"It's hard for a backhoe to cut packets flying through the

air," says Brian Chernish, network operations director at Western States Insurance, a 27-site company in Missoula, Mont. For about three years, Western States has been using pre-WiMax BWA services from TransAria Inc., a managed data services provider covering six states in the northwestern U.S. TransAria says 70% of its customer base is using "WiMax-class" services deployed with Aperto equipment.

"There's a cost advantage to me already with wireless: I'm paying about one-third the cost for a broadband wireless link as I would for a comparable wired T1," says Chernish. When the mobile version of WiMax emerges, "I should be able to drive around with a broadband VPN for voice and data procured from a single provider," he adds.

"Prior to 2001, no one had a serious disaster recovery budget," says Egan. "Alternative backhaul and disaster recovery should be the primary things about WiMax on enterprise minds now."

For example, WiMax-bound TowerStream Corp., a BWA provider operating in five large U.S. markets, offers a pre-WiMax disaster recovery service, whereby a full T1's worth of bandwidth sits available for \$175 per month as a backup in case a primary link should fail. The Waltham, Mass.-based company, which plans to expand into 10 U.S. markets, also offers its customers the option of turning up their wireless speeds over the weekend for data backups, for which they pay a temporary premium, says Jeff Thompson, the carrier's chief operating officer.

Regional and local service providers can look forward to the benefits of WiMax, if they are delivered as promised in infrastructure equipment.

"We have more customers than we have bandwidth available," says Rod Mitchell, general manager of broadband

WiMax Basics

There are two versions: **802.16-2004** for "fixed" access, **802.16e** for mobile access.

QoS requirements are specified in the standard.

Security (DES, 3DES and AES encryption) is specified in the standard.

WiMax supports IP and traditional TDMA (circuit-switched) applications.

Licensed spectrum is preferred for carrier-class WiMax service offerings. Early U.S. services are being developed for 5.8-GHz (unlicensed) band, because many regional carriers committed to WiMax don't hold licenses in the 2.5-GHz band, also approved for WiMax use in the U.S. Outside the U.S., licensed 3.5-GHz bands will support WiMax. U.S. approval for 3.5-GHz WiMax usage is expected eventually.

services at Midwest Wireless LLC, a broadband wireless and cellular service provider in Mankato, Minn., that serves Minnesota, Iowa and parts of Wisconsin and South Dakota using an Alvarion BWA infrastructure.

"Enterprises are using more bandwidth everyday," says Mitchell. "Instead of selling a 512Kbit/1Mbit/sec. pipe [upstream/downstream, respectively], I should be able to offer 2Mbit, 4Mbit and more than 15Mbit/sec. symmetrical speeds" with WiMax, he says.

But WiMax services aren't necessarily a slam-dunk. "If it delivers all that's promised, I'm for it," says Todd Graetz, chief technology officer and vice president of operations at TransAria in Bozeman, Mont. Those promises include lower subscriber-unit costs, 40% to 50% extended-coverage ranges, depending on the frequency used, and faster speeds. Graetz says he hopes for "an order of magnitude" improvement over his current 40Mbit to 60Mbit/sec. Aperto products. "If I see enough of those items, I'll put WiMax on the network," he says.

Since businesses shy away from multiple carrier relationships, which are complex to support both from a technical support and a billing standpoint, regional carriers such as TransAria and TowerStream have begun entering into wholesale and aggregator part-

nerships. Through the partnerships, customers can use all their services through a single provider.

Traditional big-name carriers which own spectrum in the 2.5-GHz licensed band (one of the U.S.-sanctioned frequencies for BWA traffic such as WiMax) are starting to commit to WiMax. Sprint Corp. and Intel have announced plans to collaborate on WiMax technical specifications, perform equipment trials, and conduct interoperability testing.

Verizon Communications Inc. is focusing most of its last-mile efforts on a well-publicized fiber-to-the-home effort in 11 states. However, "we're always evaluating a number of trials of different wireless-access technologies," says spokesman Mark Marchand.

For its part, Verizon Wireless prefers to concentrate on "selling bananas from the banana truck; that is, promoting the service offerings we have today"—namely, CDMA 1xEV-DO 3G technology—rather than "blowing forth on technology that's so far out," says spokesman Jeffrey Nelson.

Reviving Competition

Given that the Federal Communications Commission ruled in December to largely free telecommunications incumbents from their unbundling obligations to competitive local exchange carriers (CLEC), WiMax is perhaps

one of the last-gasp hopes for getting better local-loop services faster at better prices.

Chernish reported waiting several weeks for his incumbent operator to install a T1 as a backup redundant link to his wireless link in a critical location. Chernish says he would “love to see the incumbents

get taken out of the picture.”

“And alternative operators, such as cable operators, might play in the WiMax space,” suggests Egan.

Graetz says that wireless allows his company to “bypass the incumbent switched network and control the last-mile and overall experience for the

customer.”

He observes that earlier CLECs raised funding to just resell incumbent services. “They didn’t succeed, because their entire business plan was dependent on their sworn enemy,” in that they required cooperation in using some or all of the incumbents’ network el-

ements to provide service, Graetz says.

Willis is predicting “early adoption in rural markets and wireless backhaul within the carrier networks” but says the industry won’t see broad adoption of WiMax until 2009, when economies of scale are likely to kick in.

Vendors, Carriers Join Intel with WiMax Plans

WIMAX broadband wireless technology has received a major boost from Intel, which is now producing volume shipments of its Rosedale chip for the wireless broadband technology.

The Intel Pro/Wireless 5116 chip, formerly code-named Rosedale, is based on the IEEE 802.16-2004 specification and designed for wireless services comparable to DSL (digital subscriber line) or cable modem offerings. Support for traditional TDM (time-division multiplexing) telephone service also is built in to the chip, according to Intel. The chip, announced last year and now available in volume, is priced at about \$45 each in quantities of 1,000 and is expected to go into consumer or business on-site devices priced from \$250 to \$550, according to Intel.

WiMax is the commercial name of the network technology based on IEEE 802.16-2004, which allows for wireless data and voice system over a range of several miles. WiMax is expected to be deployed in most cases by service providers using licensed spectrum. The WiMax Forum will soon begin certifying products to carry the WiMax name.

Vendors and others backing WiMax are counting on the standard to allow for interoperability and the high volumes of manufacturing that typically drive electronics prices down.

Vendors developing gear based on the chip include Alvarion Ltd., Aperto Networks Inc., Proxim Corp., Redline Communications Inc., Siemens AG, and China's Huawei Technologies Co. Ltd. and ZTE Corp. Carriers planning trials include heavy hitters AT&T Corp., BT Group PLC, Brasil Telecom SA, Qwest Communications International Inc. and Teléfonos de México SA de CV.

Intel is not the first chip-maker to announce WiMax silicon, but it carries a lot of weight as both a high-volume chip leader and the rich uncle of the WiMax family, ready to put marketing dollars behind the technology. Rosedale hitting the market marks a significant moment for WiMax, according to Michael Cai, an analyst at Parks Associates, in Dallas.

"The industry is really looking at Intel, because it's been positioned as the leader in the WiMax space," Cai said.

The next major step for WiMax will be product certifi-

cation and interoperability testing by the WiMax Forum, the industry body moving to commercialize 802.16 technology.

Rosedale is a "system on a chip" for customer premises devices that would send and receive data from a base station that could be several miles away. The chip includes a MAC (media access control) component for the IEEE 802.16-2004 standard, a "phy" (physical interface) element that uses OFDM (orthogonal frequency division multiplexing), an integrated 10/100M bps (bit-per-second) Ethernet MAC for a home or office LAN, and a TDM (time-division multiplexing) controller interface to support voice and streaming data, according to Intel.

Intel integrated all those components on the chip as part of its focus on low-cost equipment that it believes will make wireless broadband a success. Some earlier wireless broadband technologies have stalled because of the cost of proprietary equipment and the need for engineers to set up a "line-of-sight" connection for each customer's antenna.

However, opinions are mixed on the potential for fixed WiMax, which in many parts of the world will compete against well-established DSL (digital subscriber line) and cable modem services. Even Intel has said the larger opportunity lies in IEEE 802.16e, a standard still under development that will allow for WiMax services to mobile devices such as notebook PCs. That technology is expected to hit the market in 2007 or 2008.

For fixed WiMax customer devices such as those based on Rosedale to take off in the market, they will first have to go below \$200 in total cost,

"The industry is really looking at Intel, because it's been positioned as the leader in the WiMax space."

**MICHAEL CAI, ANALYST,
PARKS ASSOCIATES**

said Philip Solis, an analyst at ABI Research, in Oyster Bay, New York. That isn't likely to happen for two to three years, in his view. However, service providers could shield subscribers from some or all of that cost through subsidies, he said.

The fixed WiMax that

Rosedale supports may be relegated to filling in where other broadband is not available in Western Europe and North America, according to some analysts, but it could have greater potential in less developed areas.

ZiMax, a subsidiary of Shenzhen, China-based ZTE Corp.,

expects initial response to its products to be strongest in China, Southeast Asia and Eastern Europe, according to James Jiang, general manager at ZiMax, which is based in San Diego. Analysts said countries such as India and China, which have dense populations and less broadband infrastruc-

ture in place, may be ripe for fixed WiMax. It's likely to show up in metropolitan areas first, but could extend out to rural villages if governments mandate widespread broadband coverage, said Parks Associates' Cai.

Mesh Moves Into The Wireless Office

A COSTLY and complex aspect of today's wireless networks can sometimes be the very component they're supposed to eliminate: cabling. Emerging 802.11-based mesh networks attempt to resolve this irony by using more radio spectrum and less wire in the form of Ethernet cabling than traditional wireless LANs.

These are early days for WLAN meshes, but proprietary infrastructure products are commercially available. Organizations with difficult-to-cable environments and those that frequently move their WLAN nodes are among mesh's early adopters.

A wireless mesh infrastructure is, in effect, a router network minus the cabling between nodes—with the inherent rerouting for fault tolerance that such networks deliver. It's built of peer radio devices that don't each have to be cabled to a wired port like traditional WLAN access points (AP) do. Rather, each simply plugs into an AC power supply. It automatically self-configures and communicates with other nodes over the air to determine the most efficient multihop transmission path.

Today, the way these functions work is unique to each vendor. So enterprises that build mesh networks will likely use one vendor for a few

years until standards are in place.

"Mesh is a reasonably important enterprise architecture going forward, because it dramatically simplifies installation," says Craig Mathias, a principal at Farpoint Group, a consulting firm in Ashland, Mass. "You take a node out of the box, plug it into the wall—end of discussion."

Supplying power to a mesh node can still be problematic. However, electrical outlets are usually far more abundant in buildings than Ethernet ports are, Mathias notes.

Only devices at the very edge of the wireless mesh hit wire—either to connect to a network switch or to stand-alone cabled devices such as printers and video cameras.

A design goal is to minimize the number of those wired devices and allow network managers to easily move wireless nodes as needed for capacity and coverage.

In a wireless mesh network, as devices are added and moved, the network automatically discovers topology changes and adjusts traffic-forwarding paths to optimize throughput.

Urology Clinics of North Texas replaced a traditional WLAN with a meshed Access/One system from Strix Systems Inc. in Calabasas, Calif., for just this reason. "We had intermittent problems

with interference and shifting coverage holes," explains Kyle Nash, IT manager at the Dallas-based facility. This required him to frequently move APs to tune the network, which was laborious and time-consuming because cabling ran from each AP to an Ethernet switch.

"Now I just move APs on the fly. This means the network is up longer. It will also make things much easier as our network continues to expand," says Nash, whose goal is for the five-office, 200-plus user facility to eventually be about 90% wireless.

Early Players and Users

The flexibility provided by mesh networks is particularly helpful over large geographies and in hard-to-wire buildings. Cisco Systems Inc., for one, says it helped kick off the effort to develop the IEEE 802.11s mesh networking standard when it discovered that some of its customers were running Cisco Aironet APs in "repeater mode," whereby one AP backhauls packets to another.

"This was happening in large warehouses where customers either couldn't get to a location or were running into Ethernet's 100-meter cabling limitation," says Jon Leary, product line manager in Cisco's wireless networking business unit.

Similarly, consider hospitals using the services of Shared P.E.T. Imaging LLC in Canton, Ohio. The company offers mobile positron emission tomography (PET) diagnostic medical imaging services to facilities that can't support the service full time in-house.

Mobile scanning labs are equipped with an \$800 Firetide Inc. 802.11b HotPoint mesh router attached to a PET

Standards on the way . . . in 2007

THE IEEE 802.11 Task Group S met in September to begin developing a standard for interoperable wireless LAN mesh infrastructures. There are at least two items that the standard will likely define:

- n How a packet selects its multihop path across the wireless mesh. Today, this is the secret sauce giving early vendors their value-add. Best-path selection is analogous to traditional Layer 3 wired routing protocols, such as Open Shortest Path First, or OSPF. In wireless configurations, though, the algorithm must be tightly coupled with Layer 1 radio metrics, accounting for physical-layer issues such as signal strength and interference when selecting a path.

- n Authentication and security extensions for mesh. Part of the standard's scope is still to be decided, says Steven Conner, wireless network architect at Intel Corp.'s Communications Technology Lab and technical editor for the IEEE 802.11 Task Group S. For example, he speculates that the standard could include the way a node selects a channel and what transmission power to use.

Conner predicts that proposals will be received during the first half of 2005 and that the standard will be complete sometime in 2007.

scanner. The router in the mobile coach communicates images to another router inside the hospital, where they are relayed to a reader, says Marc Simms, director of IT at Shared P.E.T. Previously, the company dragged Category 5 Ethernet cabling outdoors after drilling a hole in the building.

Simms describes the cabling as "flaky and susceptible to weather." In one instance, cabling beyond the 100-meter Ethernet limit required the installation of more-costly fiber optics.

Simms says that before the company took the wireless mesh approach, an installation with a new customer took four to eight weeks and cost \$2,000 to \$4,000—or \$10,000, if fiber was involved. "Now, setup time is about an hour," he says.

Strix and Los Gatos, Calif.-based Firetide are the two mesh vendors that have made the greatest enterprise inroads. Firetide focuses strictly on wireless backbone applications - the company added 54Mbit/sec. 802.11a nodes to its portfolio—while Strix builds nodes that perform double duty as wireless backbone routers and traditional WLAN APs.

Strix supports 802.11a/b/g in a modular, stackable mode that costs \$800 to \$900. It also uses the faster, shared 54Mbit/sec. 802.11a or g for backhaul and 802.11b for user access. In addition, Strix says it can use the proprietary 802.11g channel-bonding mode supported in some WLAN chips to achieve 108Mbit/sec. optimum-shared bandwidth.

Like Strix and Firetide, Tropo Networks Inc. in San Mateo, Calif., makes both indoor and outdoor Wi-Fi mesh products that could be used by enterprises or public network operators. To date, though, Tropo products have been installed in metropolitan applications, such as citywide 802.11 hot-spot networks.

Similarly, Nortel Networks Corp., which began shipping mesh products last month along with BelAir Networks Inc. and RoamAD, focuses on outdoor applications such as municipal and campus backbones. Like Strix, Nortel mesh nodes also support traditional AP access, and Kanata, Ontario-based BelAir's products offer indoor coverage from the same, outdoor-mounted node. Nortel provides indoor WLANs via a product line from Airespace Inc., which it resells.

The enterprise applications

for mesh are fairly targeted, given the relatively low speeds of Wi-Fi networks compared with gigabit-speed cabled Ethernet backbones. The actual throughput speeds of Wi-Fi are about one-half to two-thirds of their stated optimum bandwidth because of wireless overhead and interference.

Generally, adding more mesh nodes increases capacity. However, Wi-Fi bandwidth is shared, and while both Strix and Firetide cite per-hop latency of less than 5 msec., this could add up as meshes scale, particularly as voice applications emerge and more hops eat into the total voice-latency budget.

Throughput Considerations

"The concept of sustained [wireless mesh] backbone bandwidth is not applicable," says Sunil Dhar, director of product management at Firetide. "End-to-end throughput is determined by the number of wireless hops required to traverse the mesh, the density of the mesh deployment and the amount of interference."

"For backhaul, you're going to pay, performance-wise," says Yuval Goren, a wireless

consultant at Goren International in Saratoga, Calif. "Mesh is for applications where you can't get access wherever you want, such as temporary applications where it makes no sense to pay thousands of dollars to run cables."

The Computer History Museum in Mountain View, Calif., has such an application. When the previous occupant vacated the building a few years ago, it cut much of the Ethernet cabling out of the 120,000-square-foot building.

So the museum is using Firetide nodes for temporary exhibits and outdoor events, where generator power is used, and in small, inaccessible areas indoors, according to Mike Walton, the museum's director of IT.

The Computer History Museum runs a Hewlett-Packard Co. AP infrastructure hanging off the Firetide 11Mbit/sec. backbone, which serves places such as the lobby for event registration.

"The lobby had no options for an Ethernet drop. Now, if I want registration computers, all I have to do is plug a [Firetide] node into an electrical outlet," Walton says.

Similarly, The Science Place,

Municipal Hot Zones

ONE LEADING-EDGE technology being deployed in U.S. cities is known as municipal wireless mesh hot zones. Based on the concept of Wi-Fi hot zones, they cover broader areas than the Wi-Fi hot spots in shopping malls and airports.

Some cities are building these hot zones for public safety needs. Others have gone further and are offering fast wireless connections to homeowners and businesses to replace cable modem and DSL services sold by the private sector.

Tropo Networks Inc. in Sunnyvale, Calif., has sold its Wi-Fi mesh routers to 125 cities, according to CEO Ron Sege. The devices are deployed from city street lamps in a mesh design of about 10 routers

- per square mile, giving 1Mbit/sec. connectivity using the 802.11 specification, he says. "It's quite a phenomenon, and the demand is increasing rapidly," Sege says, noting that Dallas and Philadelphia have deployed some of the routers, and other large cities, including Boston, Houston and New York, are in the early stages of considering the technology.

- In some cases, Wi-Fi hot zones can generate revenue for cities, putting CIOs and their IT shops in the unusual role of profit center rather than cost center. "CIOs are excited to be doing something so visible in the community," Sege says. "They are out of the engine room and into the wheel house."

an interactive museum in Dallas, has exhibits requiring both LAN and Internet access that are frequently moved. The 38,000-square-foot, two-building facility has 20-foot ceilings, 6-foot limestone walls and strict laws about what can be done to the building, says Michael Wright, director of IT.

The Strix network runs through both buildings “without having to string wires across the floor,” Wright says. However, the organization re-

tains a wired Fast Ethernet backbone with 10Mbit/sec. throughput to the desktop for permanent administrative uses.

Jose Villarreal, director of technical marketing at Strix, counters that it won’t be long before wireless is on par with wired speeds. “Some seriously smart engineers used to say we would never be able to deliver broadband over twisted pair. How many DSL deployments are being done each day now?”

Mobile Computing's Energy Crisis

WHEN Dave Saltzman prepares for a business trip, he charges up the main battery in his notebook computer, removes the CD-ROM drive and fills the bay with a second battery, and then packs a third one in his bag. That's sufficient for long trips, says Saltzman, systems manager at United Parcel Service Inc. in Atlanta.

Like many users, Saltzman wants to be able to work continuously during extended flights, but he also wants to use power-hungry features such as wireless networking while traveling. These changing usage patterns and the demand for faster notebooks have created a power gap between what batteries can provide and what systems can deliver.

While notebooks continue to benefit from Moore's Law, batteries haven't kept up. The future of disconnected computing depends on century-old electrochemical technology that has improved only gradually.

It's not that batteries haven't gotten better. "If we were to put today's battery on a notebook built five years ago, you'd get eight hours of battery life," says Carl Pinto, director of product development for notebooks at Toshiba Corp. in Irvine, Calif. The problem is that mobile devices are demanding more power, he says.

Until recently, investment in battery technology has been relatively small. "In the last 100 years, there hasn't been enough work put into batteries. It's just not exciting stuff," says Rob Enderle, an analyst at Enderle Group in San Jose.

But battery life has risen to become one of the top three purchase criteria for notebook computers, says Mike Trainor, chief mobile technology strategist at Intel Corp., which produces logic boards and chip sets used by the majority of notebook makers. "IT shops want more performance, more wireless and slimmer systems, which cuts down the room for batteries," he says.

Power Gap For Notebook Computers

Improvements in the traditional six-cell lithium ion battery pack are projected to fall short of notebook requirements, so vendors are turning to new battery chemistries to improve energy density. Longer term, fuel cells are expected to take power densities well beyond what batteries can offer and will allow virtually unlimited operating time to be extended by refueling the system with a replaceable methanol cartridge or refillable tank.

Intel's Centrino mobile chip set has reduced power consumption, extending projected operating times from two to three hours into the five-hour range, which is still short of the all-day battery users want. Eight hours of life would require 100 watt hours (Wh) of power, but the best available battery technology—lithium ion—delivers less than 60Wh.

Trainor is confident that Intel can "give Moore's Law's worth of features" through the end of the decade while keeping consumption at the 100Wh mark. But that still leaves a power gap. "The other side of the equation has become equally important: How do we get more energy into the system?" he says.

Vendors have recently awakened to the problem, but government and private research and development dollars have poured into fuel-cell research rather than into basic battery designs. The direction of investment away from batteries has contributed to today's power gap, contends Donald Sadoway, a professor of materials engineering at MIT.

"They put all of their eggs in one basket. Here we are, seven or eight years later, and fuel-cell applications are nowhere near to realization," he says.

Users are feeling the pain. Tony Scott, chief technology officer at General Motors Corp., says Centrino-based notebooks have improved battery efficiency 20% to 30%, but actual operating times remain under three hours. That's not always enough when people bring such computers to meetings, says Scott.

"If you get two back-to-back one-hour meetings and you're making any significant use of the machine at all, you can start running into problems. And three meetings in a row—

forget it," he says. "We need eight-plus hours of use, and that's a struggle with a lot of the devices we have today."

For Saltzman, the battery issue goes beyond notebooks. He manages 200,000 battery-powered devices at UPS, including radio-enabled handhelds used in delivery trucks. The batteries don't charge well in hot or cold weather, so charging must be done at the dispatching location. And because drivers are on the road for up to 10 hours, UPS must use bigger batteries, which adds weight to the devices. Saltzman would like to see higher energy densities to reduce weight.

Extending the Batteries

Battery manufacturers have made incremental improvements in lithium ion batteries since they were introduced in the early '90s, says Kurt Kelty, director of business development at Panasonic Energy Solutions Lab, a unit of Princeton, N.J.-based Panasonic Technologies Inc. Over the past five years, lithium ion batteries have replaced nickel cadmium (NiCd) and nickel metal hydride (NiMH) technology in mobile computing devices. Lithium ion offers a higher volumetric energy density. It also doesn't suffer from the memory effects that shorten the life span of NiCd batteries. And it's environmentally superior to NiCd, which faces a gradual phaseout because cadmium is toxic, making it a hazard in the waste stream.

While nickel-based chemistry has reached its capacity limit, lithium ion continues to make small gains. In recent years, capacity has increased at a rate of about 10% per year, while competition has reduced prices at 10% to 20% annually, Kelty says.

Although lithium ion hasn't yet hit the theoretical capacity limit, the industry consensus is that future gains will be unlikely to close the power gap.

Battery Timeline

1802: First electric battery capable of being mass produced

1859: Rechargeable lead acid battery

1888: Dry cell battery

1899: Nickel cadmium (NiCd) battery

1947: Sealed NiCd battery

1960: Union Carbide creates alkaline battery

1990: Nickel metal hydride (NiMH) battery

1992: Reusable alkaline battery

1999: Lithium ion polymer battery

2002: Early proton exchange membrane (PEM) fuel cells developed for vehicles

2004: Early trials of direct methanol fuel cells for mobile computing/portable electronics

2010: Wide commercial adoption of direct methanol fuel cells (DMFC) predicted

SOURCE: CADEX ELECTRONICS INC., ABI RESEARCH.

That conclusion has spurred renewed interest in battery research.

Companies such as Mississauga, Ontario-based Electrovaya Inc. use lithium ion polymer, which uses a gel-like electrolyte. Despite early promise, the technology remains more expensive than lithium ion and hasn't improved energy density. But it does have one advantage: Polymer-based cells can be formed into flat shapes that fit into small devices, while lithium ion is limited to cylindrical cell designs.

Pionics Co. in Shiga, Japan, has shown a prototype battery with an energy density of 600Wh/liter. Most of today's lithium ion batteries fall into the 200Wh to 250Wh/liter range, says Atakan Ozbek, principal analyst at ABI Research in Oyster Bay, N.Y. Still

other vendors are working on designs based on materials such as lithium sulfur and lithium phosphate.

Even the traditional alkaline battery may get back into the game. With zinc-based alkaline batteries, it has been difficult to get more than 10 recharge cycles, says Robert Zeiler, president of Zinc Matrix Power Inc. in Santa Barbara, Calif. The company has replaced the alkaline battery's traditional electrolyte solution with a polymer-based formula that extends the number of recharge cycles. "We can get hundreds of cycles," with an energy density of 600Wh/liter, he says. The company has an agreement with Intel and says it will have a commercial notebook battery in production by 2006. While Intel has invested in the more promising companies, Trainor is realistic about early claims. "What we have not seen is anyone manufacture these cells in high volume," he says.

Fuel-Cell Frenzy

For the long term, most vendors have pinned their futures on fuel cells. Government and private investments in fuel-cell research have been substantial, and more than 60 companies are working on designs to power electronics, says Jim Balcom, president and CEO of PolyFuel Inc. in Mountain View, Calif.

Fuel cells combine a fuel such as hydrogen or methanol with oxygen in an electrochemical reaction. The most popular design, the direct methanol cell, uses methanol or a methanol/water mix. Fuel cells show promise in delivering dramatically higher energy densities, and the ability to swap out fuel cartridges could guarantee a virtually endless power supply. As little as 1cc of fuel can generate 1Wh of electricity—enough to power a cell phone for about two hours, says Alan Soucy, chief operating officer at MTI MicroFuel

Cells Inc. in Albany, N.Y.

But the technology faces several challenges. Fuel-cell systems are complex, requiring an engine, or "stack"; tiny pumps, sensors and other electronics; a venting system; and a fuel tank. Squeezing them into something the size of a notebook battery that can be sold at a reasonable price and that works reliably is a major engineering hurdle.

Fuel cells are also relatively inefficient—turning 70% of the energy they produce into waste heat vs. 10% for batteries—which is a problem for notebook designers, who are already facing thermal challenges. And the systems vent small amounts of carbon dioxide and water vapor.

Fuel cells also don't respond well to sudden spikes in power demand, so early designs, such as Intermec Technologies Corp.'s fuel-cell-powered IP3 radio frequency identification (RFID) reader prototype, are coupled with a lithium ion battery. The IP3 fuel cell, an MTI design, trickle-charges the battery in addition to directly powering the RFID reader. The unit runs for 30 hours on a 55cc fuel cartridge compared with about 10 hours for a traditional battery. Other vendors are experimenting with ultracapacitors, solid-state devices that can deliver short bursts of supplemental power to handle peak loads.

"Toshiba's big investment is in fuel cells," says Pinto. Toshiba, Hitachi Ltd. and NEC Corp. have shown prototype "swap bay" designs that attach to a notebook or handheld, with internal units to follow. But real products won't come until standards are ironed out. A standard fuel mix and cartridge design is needed for broad acceptance, and regulators still need to approve its safety and use, particularly on airplanes. Getting Federal Aviation Administration approval to carry the flammable methane tanks onboard com-

mercial flights may not be easy, given the agency's recent ban on butane lighters.

ABI Research's Ozbek says fuel-cell makers have made significant strides in the past six months, reducing the pack-

age size by 50% while surpassing the energy density of lithium ion in test units. Early fuel-cell power packs will ship this year and next, ramping up to a few thousand units in 2007. "Then it's going to be millions

by 2010," he says.

In the interim, users will have to make do by dimming screens and using the power-saving features available to them. Those features can help, says GM's Scott.

But power-saving designs alone aren't going to close the power gap, he adds. "Batteries have been the boat anchor in terms of real progress."

CASE STUDY:

BP's Wireless Sensor Networks

BP PLC's wireless sensor network program began with a two-day technology immersion session for the company's top executives in May 2003. Less than two years later, these sophisticated networks are one of the oil and gas giant's cornerstone strategies for transforming business processes, from increasing supply chain visibility and inventory control to monitoring sensitive pumps and compressors on oil tankers plying the North Sea.

"The idea was to open their minds to possibilities," says Chief Technology Officer Phiroz "Daru" Darukhanavala of the technology sessions for BP's top brass. "Once you open the right executives' minds to possibilities, they tend to grab on to an idea and move it along more than IT could ever push it along."

Consider BP's liquefied petroleum gas (LPG) business, which is pilot testing RFID sensors to track the whereabouts and condition of some 35,000 refillable cylinders of gas used for domestic cooking by customers in Denmark. By the end of this year, a Europe-wide rollout is slated to begin, with RFID-tagged cylinders becoming mainstream throughout BP's worldwide LPG business.

The London-based company is also remotely monitoring its industrial customers' LPG tank fill levels, using battery-powered ultrasonic sensors that transmit information by radio signal to a low Earth orbit satellite, which relays the data to BP for timely deliveries. The technology, co-developed with Londonderry, Northern Ireland-based Andronics Ltd., is operational on about 200 tanks in England and is being deployed across Europe.

Previously, neither customers nor BP had an accurate way to gauge how much LPG remained in one of the large tanks, and BP would receive lots of last-minute panic calls from customers who had run out unexpectedly. Using the sensor network, the LPG business has improved delivery efficiency by over 33%, according to Ken Douglas, director of technology and sensory networks.

"You need to work the pilot and build confidence and assure yourself that the benefits are really there."

PHIROZ DARUKHANAVALA, CHIEF TECHNOLOGY OFFICER, BP

Sensors are also helping BP track the whereabouts and condition of its railroad tanker cars, which transport some 45,000 chemical shipments annually—each valued at about \$100,000. In a pilot test in 2004, BP attached a black box with sensors and a GPS transponder to 21 tanker rail cars in North America. The system captures data on the car's location and temperature, and whether it has been tampered with. The information is transmitted via satellite to a control center, where it can be accessed via the Internet by BP and its customers. The system will eventually include 500 rail cars.

"We always do a pilot, because in virtually all of these cases, we're breaking new ground," Darukhanavala says. "You need to work the pilot and build confidence and assure yourself that the benefits are really there."

Another tip: "It is absolutely necessary that you use an ecosystem of suppliers because no one is smart enough to do it all," he says.

BP's network supplier "ecosystem" includes some 60 companies, each with a different specialty. "What my [internal IT] team does is nurture the executives' ideas forward and help to bring the ecosystem together. It's a technology-transfer function," Darukhanavala says.

There is no question that BP is way ahead of the curve, says Marlene Bourne, an analyst at In-Stat/MDR, a high-tech research firm. "Other [sensor] applications are definitely showing signs of progress, but it will be several years before we see ubiquitous commercial applications," she says.

Evaluate Risk Before Merging Wired and Wireless LANs

COMPANIES need to do their homework before merging the security and management of their wireless and wired networks, according to industry analysts.

The first step should be a risk analysis of the security and management issues for the unified wireless and the wired networks, according to Michael Disabato, director of wireless security at Burton Group in Midvale, Utah. A key objective should be “to determine a common set of authentication, access and authorization policies for all users,” he said.

The impetus to merge wireless and wired networks into a common security and management infrastructure “began in an effort to secure WLANs from the unique threats posed to mobile users accessing the flexible and wide-open wireless hot spots,” Disabato said. “Strong authentication has long been a requirement for wireless LANs because of the threats to wireless sessions. Now this strong authentication, as well as management for it, is being extended to the wired LAN side.”

Merging the two LAN architectures gives users a cost-effective means to secure and manage two vastly different infrastructures, Disabato said. A predictable ROI will be pivotal in driving the exploding growth in wireless networking.

Marketplace numbers tell the story of exploding WLAN

growth. Sales of Wi-Fi clients—mobile PCs, PDAs and phones—grew 66% in 2004, according to In-Stat/MDR in Scottsdale, Ariz. Wi-Fi hardware—access points and switches—will surpass \$6 billion in annual sales in 2005, and 90% of laptop PCs now are shipped with WLAN cards, In-Stat reports. Meanwhile, the number of VoIP users leaped by a factor of eight to more than 1 million users by the end of 2004.

Common security and management architecture is still a work in progress for managing VoIP calls over WLANs, according to Abner Germanow, a wireless analyst at IDC in Framingham, Mass. “Many WLAN vendors are presenting VLANs [virtual LANS] as a

solution of choice for VoIP traffic,” he said. VLANs enable network engineers to segregate traffic so users on a given VLAN see only the traffic on that VLAN.

VLANs are a good interim solution for creating subnets to segment certain types of LAN traffic, such as VoIP, Germanow said, “because you don’t have tons and tons of devices on the network, and it’s all just getting started. But at some point, the VLAN runway runs out and an enterprise will need to look at other options.”

Chief among the options for a unified management and security framework is providing better access control to sensitive applications and data, Germanow said. “Every switch and access-point vendor has a security strategy that accounts for access and identity management,” he said.

Germanow cited Cisco’s Network Admission Control program, announced in 2004, as an effort to integrate security and configuration management information from WLAN vendors. “They’re creating an umbrella security architecture for both wired and wireless networks that can provide the level of controls needed for compliance,” Germanow said.

Burton’s Disabato echoed Germanow’s caution on VLANs. “Enterprises should be careful to not get too granular with VLAN deployments,” Disabato said. “Going to one VLAN per department gets counterproductive. It will put great management burdens on the network and have diminishing returns for security.

“VLANs are a good technical solution once you determine your business requirements. The cost of VLANs as a security solution needs to be weighted against the benefits it provides. You shouldn’t be

“Strong authentication has long been a requirement for wireless LANs because of the threats to wireless sessions. Now this strong authentication, as well as management for it, is being extended to the wired LAN side.”

**MICHAEL DISABATO,
DIRECTOR OF WIRELESS
SECURITY, BURTON GROUP**

buying technology until you've done your homework and planned the relationship of the technology to the business environment," he added.

Disabato also advocates identity as the unified security and management solution. "Once you determine who's going to be allowed on the network, how are we going to provision and control them?" he asked. The ideal security solu-

tion for a unified wired/wireless architecture, Disabato said, will include "some form of user policy management" that controls access and authorizations for regulatory compliance and can be extended to give granular authorization for VoIP.

"Some combination of role-based and rule-based security" would be the best approach, he said. "VLANS alone are a role-

based approach" that should be augmented by rules for the different levels of permissions allowed between wired and wireless users, he noted.

Identity management is forecast to soar from \$738 million worldwide in 2004 to \$10.2 billion by 2008, according to The Radicati Group Inc. in Palo Alto, Calif.

VLANs do provide effective countermeasures against

rogue access points and session spoofing, two WLAN security threats. VLANs centrally control 802.1X authentication and prevent a rogue access point from masquerading as an authorized WLAN on-ramp. VLANs also can thwart session spoofing with encrypted tunnels secured by the client and server both authenticating themselves with hashed values.

RISK REDUX: Common WLAN Vulnerabilities

THE BENEFITS of wireless LANs are undeniable, but the risks introduced by them are increasing exponentially. According to In-Stat/MDR, more than 75 million Wi-Fi devices have been deployed worldwide, and another 4 million new WLAN devices are being shipped per month.

Some organizations think their investments in firewalls and virtual private networks will protect them from the risks of WLANs. However, they don't realize that the WLAN signal bypasses all wired-side security and opens a back door for an intruder. Simply banning WLANs isn't an option, either, because most

laptops are shipped with built-in wireless cards. If companies were to ban wireless networks, they would need to ban the use of laptops, which is an impractical solution.

The fact is, any wireless device connected to a wired network essentially broadcasts an Ethernet connection and an on-ramp to the entire enterprise network. Unless properly secured and monitored across the global enterprise, these self-deploying, transient wireless devices and networks are dangerous to all organizations. Intruders and hackers will use an unsecured WLAN to break into corporate networks and compromise the integrity of financial data, customer information or even trade secrets.

No longer should the security of wireless networks be a peripheral thought.

The Difficulties of Securing the Air

To understand the risk of WLANs, one must first understand the security vulnerabilities of all WLANs. WLANs face all of the security challenges of any wired network. In addition, risks are introduced by the nature of wireless technology.

First, the medium in which a WLAN operates is the air, an uncontrollable space. In addition, wireless devices self-deploy and have the capability to connect to strangers. Due to the growth of WLAN-enabled laptops and the increasingly wireless-friendly Windows XP operating system, laptops in the default setting automatically search for an access point (AP) to connect with. Lastly, wireless devices are transient in the way they connect. If a wireless device picks up a strong signal, it may connect with the new AP even if the AP is the laptop of an intruder in the parking lot.

There are many ways in which WLANs can be compromised:

ROGUE ACCESS POINTS

A rogue WLAN has traditionally been thought of as a physical AP unsanctioned by network administrators. Today, rogue WLANs are further defined as laptops, handhelds with wireless cards, bar code scanners, printers, copiers or any WLAN device. These devices have little to no security built in, making it easy for intruders to find an entry point. Rogue APs could be maliciously placed by intruders to hack into a corporation, or they can be innocently deployed by employees for easy wireless access.

What is at Risk?

WLANs provide an easy open door to the wired network. Through unintentional associations and ad hoc networks, unsecured wireless networks can be sniffed, acting as a launch pad to the wired network and an organization's corporate backbone.

Once accessed, an unsecured WLAN can compromise the following:

- **Financial data**, leading to financial loss
- **Reputation**, damaging the efforts spent building the brand

- **Proprietary information**, leaking trade secrets or patents
 - **Regulatory information**, foregoing customer privacy or ignoring government mandates
- All of these scenarios could have legal ramifications. As wireless networks become ubiquitous extensions of wired networks, the threat of intruders becomes more pervasive. Organizations need to look beyond local APs and think globally to secure the air across the entire enterprise.

SOFT APs

While hardware APs have been the focus of security concerns, wireless-enabled laptops are easily configured to function as APs with commonly available freeware such as HostAP or software from PC-Tel Inc. Known as “soft APs,” these laptops are harder to detect than rogue APs and are quite dangerous because they appear as user stations to all wire-side network scans.

ACCIDENTAL ASSOCIATIONS

Accidental associations are created when an AP across the street or on adjacent floors of a building bleeds over into another organization’s airspace,

triggering its wireless devices to connect. Once those devices connect with the neighboring network, the neighbor has access back into the organization. Accidental associations between a station and a neighboring WLAN are now being recognized as a security concern.

MALICIOUS ASSOCIATIONS

A malicious association is when a company laptop is induced to connect with a malicious device such as a soft AP or laptop. The scenario also exists when a malicious laptop connects with a sanctioned AP. Once the association has been made, a hacker can use the

wireless device to attack servers and other systems on the corporate network.

AD HOC NETWORKS

Ad hoc wireless networks, or peer-to-peer networking between two computers without connection to an access point, represent another major concern for WLAN security. These ad hoc networks can be self-deploying or intentional. In addition, such networks have little security in terms of authentication and encryption. Therefore, it’s easy for an intruder to connect to innocent users’ computers and copy private documents or sensitive information.

Wireless LANs Find Their Voice

THE combination of wireless LANs and IP-based telephony has forever changed the definition of mobile phones and how they're used in the enterprise.

Today, a wireless voice-over-IP (VoIP) phone operating over a WLAN can look much like a typical cordless phone. And thanks to accelerated hardware and software development, these phones are morphing into wireless IP headsets and Star Trek-like voice-activated communicators and software phones, also known as softphones, that are just another program on a laptop or handheld computer.

This hardware and software was designed to piggyback on proliferating enterprise WLANs, including new voice-grade WLAN software, access points and switches from a growing number of manufacturers.

These developments have transformed WLAN VoIP from a bleeding-edge technology in 2001 to a technology close to maturity today, says Shawn Wilde, director of worldwide operations at Trimble Navigation Ltd., a Sunnyvale, Calif.-based manufacturer of Global Positioning System receivers. Trimble began using wireless IP phones globally in 2003.

As WLAN VoIP technology

has matured, the number of vendors that offer mobile VoIP phones and the WLAN infrastructure designed to support them has increased. Cisco Systems Inc. in 2003 introduced its first VoIP handset and additions to its Internetworking Operating System designed to support WLAN IP voice systems.

In early March, Alcatel in Paris and Nortel Networks Ltd. in Brampton, Ontario, entered the market. Both companies will base handsets on technology developed by industry pioneer SpectraLink Corp. in Boulder, Colo. Both will resell WLAN switches and access points from San Jose-based Airespace Inc.

Market Heats Up

Airespace is one of a handful of start-ups that, along with established companies such as Cisco, Symbol Technologies Inc. and Proxim Corp., are vying to provide the quality of service and roaming infrastructure needed to support VoIP in the enterprise WLAN environment.

Chris Kozup, an analyst at Meta Group Inc., cautions that supporting VoIP calls over a WLAN presents a far bigger challenge than providing wireless data services, especially when users roam and their calls need to be handed off

from one subnetwork to another. This requires the handset or softphone to obtain a new dynamic IP address, which must happen in 100 milliseconds or less, or the call is dropped.

Some companies, such as Cisco, have developed proprietary fast-roaming protocols, but Ritch Watson, director of VoIP at Holtsville, N.Y.-based Symbol, says the first industry-wide meeting to discuss roaming standards was just held in March.

Despite this challenge, early enterprise adopters of WLAN VoIP say the technology delivers bottom-line savings and increases mobility in ways they couldn't have imagined.

St. Agnes HealthCare, a 299-bed hospital in Baltimore, deployed WLAN VoIP communicators from Vocera Communications Inc. in Cupertino, Calif., in lieu of installing a new paging or nurse-call system. The hospital equipped nurses, nurse technicians and care-unit secretaries with Vocera hardware and realized dramatic improvements in productivity, says William Greskovich, St. Agnes' CIO and vice president of operations.

The Vocera system consists of 2-oz. voice-activated VoIP communications badges. Voice traffic is directed by the system software, which runs on an Intel-based server at St. Agnes. The badges can be clipped to a shirt pocket or collar to provide a hands-free communications system, Greskovich says.

Nurses and other employees log in via a voice-recognition system with their badges and can call other employees by saying their names. The system also tracks users based on their proximity to 120 Cisco access points in the hospital,

Greskovich says. To locate one another, nurses speak a simple voice command to find "Nurse X." The system responds, "Nurse X is on the fifth floor," and another command connects the nurses.

The hospital's phone directory is loaded into Vocera's software, making a hands-free call quick and easy, Greskovich says. To call the blood bank or pharmacy, nurses say the department's name and are connected. Staffers can make outside calls by saying the number, and they are then connected through a Vocera interface to the hospital's private branch exchange (PBX), he says.

St. Agnes commissioned First Consulting Group Inc. in Long Beach, Calif., in December to assess the Vocera system's effect on workflow and nurses' satisfaction. The study found that the system saves unit secretaries 1,446 hours, nurses 1,146 hours and nurse technicians 626 hours each year.

That works out to about 1.7 full-time equivalents per unit, or a savings of \$74,000 per unit each year, Greskovich says. The system cost about \$200,000 for the server software and \$300 per badge for each of the 350 badges.

Greskovich says the Vocera system has also reduced intercom voice pages, which can be annoying to patients and staff alike. He said he believes that the Vocera system will help St. Agnes cut more hours and improve workflow this year as staffers such as maintenance

personnel and security guards are added to the system.

Always On, Anywhere

Trimble Navigation has deployed a more conventional IP system: 40 of Cisco's 7920 wireless IP phones plus 20 Cisco softphones, all of which work over the company's global Internet-based virtual private network. Wilde says Trimble initially deployed the devices to IT staffers who aren't tethered to their desks.

The IP phones provide easy global connectivity, he adds. When Wilde travels to Trimble's research and development facility in New Zealand, for example, he takes his 7920 with him. When Wilde turns on the phone in New Zealand, it connects through a WLAN to Trimble's global network with the same number he uses in Sunnyvale.

The same thing happens when Wilde uses his 7920 in the company's plant in Germany, making it easier for anyone at Trimble to track him down using his standard office phone number, rather than trying to determine which country he's in and then dialing a long international phone number.

When Wilde makes an outgoing call from New Zealand, the device places the call through the PBX in Sunnyvale. Using the 7920 overseas "has definitely chipped away at my cell phone bill," he says.

Besides giving the 7920s to the IT staff and department managers, Trimble has also de-

ployed them to workers in shipping facilities who aren't near a desk phone. The device gives these workers the connectivity and functionality of a desk phone while allowing them to be mobile, Wilde says.

Wilde adds that he wants to deploy IP phones to office and plant staff but plans to wait until he can assess the price versus performance and capabilities of combined cellular and IP phones. Such models are expected from both Motorola Inc. and Nokia Corp. later this year.

Student Body in Motion

Dartmouth College in Hanover N.H., plans to use its WLAN infrastructure to fulfill all of its students' and staffers' voice, data and video needs, according to Brad Noblet, the college's director of technical services.

Dartmouth has already deployed a wide range of VoIP clients, including 80 Cisco 7920 phones, 1,000 Cisco softphones and 100 Vocera badges. Noblet says Dartmouth also has a contract with TeleSym Inc. in Bellevue, Wash., for 600 of its SymPhone clients.

These clients operate over 500 Cisco access points, including some installed specifically to serve maintenance staff, such as in the extensive network of steam tunnels throughout the campus.

Noblet says he decided to build Dartmouth's network infrastructure around WLANs rather than wired networks because a college campus is "one

of the most mobile environments," with students in constant motion between dorms, classrooms, dining halls and the library.

Noblet has bold plans to beef up the campus WLAN infrastructure to support all 4,000 students with their own softphones integrated into laptops or handheld computers. Currently, faculty, administrators and support staffers are the primary users of the VoIP hardware, he adds.

Noblet says he plans to boost bandwidth and coverage over the next 18 months, with 1,500 access points supported by the Cisco infrastructure as well as new wireless switches and low-cost access points from Aruba Wireless Networks Inc. in San Jose. When it's complete, the campus WLAN will support the majority of voice, data and video services and be one of the first and largest converged networks of its kind in the U.S., he says.

This grand vision may take longer to achieve in traditional office-based environments, according to vendors and analysts. Bill Rossi, vice president of Cisco's wireless networking business unit, says demand for WLANs and wireless VoIP still remains low in what he calls the "carpeted office."

Kozup agrees, saying that in the near future, WLAN VoIP will follow the path blazed by data WLAN installations. Users in health care, higher education and retail will be the most likely early adopters, he says.

Early Adopters Send Mixed Messages About RFID

COMPANIES preparing to test or evaluate radio frequency identification technology are excited about RFID's potential, but worried about cost and other issues.

Some consumer goods manufacturers are facing RFID compliance deadlines from retailers such as Wal-Mart Stores Inc. and Target Corp. They are keen on the potential benefits, such as the ability to track inventory with greater precision and to keep products in stock and on store shelves.

But some of those same early adopters say they are still trying to nail down business cases, that the technology isn't mature and that RFID standards remain a work in progress. In addition, the cost of RFID tags and readers has yet to drop to price levels that will help users achieve returns on their investments.

"It's going to be pure cost at the beginning. That's a concern, because it cuts into our profitability," says Richard Siegfried, manager of global data synchronization efforts at Binney & Smith Inc., a subsidiary of Hallmark Cards Inc. in Easton, Pa., which makes crayons and other products.

At the same time, Siegfried notes that he's optimistic about the long-term ROI potential from an increased flow of information, which is expected to help his company improve forecasting and planning with its suppliers.

Efrain Barreiro, director of

ty to press a button and get an accurate inventory count would provide great benefits.

High Tag Costs

But Barreiro notes that as much as 70% of Elan-Polo's shoe business involves high-volume, low-price products. When he runs the numbers, he needs 5-cent tags to make the RFID investment pay off. RFID tags are still selling for several times that amount.

In many ways, the pros and cons of adopting RFID haven't changed substantially since the technology became a hot-button issue in 2003, when Wal-Mart directed that its top 100 suppliers begin tagging pallets and cases.

"The faster payback is really going to be upstream, in working with our raw materials and finishing-goods suppliers and looking at how we manage our materials within our operations," says Mike O'Shea, director of corporate RFID strategies and technology at Kimberly-Clark Corp., which started conducting RFID field trials in 2002.

But an ROI isn't expected for a few years. First the Irving, Texas-based company has to do the business process re-engineering necessary for it to take advantage of the information gathered through RFID technology, according to O'Shea. He says that in the near term, Kimberly-Clark views its RFID work as a research and development effort with no immediate payback.

Jim Flannery, director of global customer development at Cincinnati-based Procter & Gamble Co., another early adopter of RFID, says the company is still figuring out which business processes to change.

"We're working with our trading partners, trying to figure out where to get value," he

Five Other Uses for RFID

Highway Tolls. California's FasTrak, Illinois' I-Pass, New York's EZPass and Massachusetts' FastLane let commuters pay tolls by driving through special lanes at toll plazas.

Cash Transactions. In some parts of the world, cards with RFID chips let consumers buy goods and transit tickets.

Prisons. Some inmates have been issued RFID bracelets that let administrators track their movements in prison facilities.

Animal Tracking. Implanted RFID chips can help reunite lost pets with their owners.

Implanted Humans. In pilot programs, people have been implanted with RFID chips to let doctors access medical records, allow access to buildings and even let police officers access sensitive law enforcement databases.

operations at Elan-Polo Inc. in Nashville, says the footwear maker and distributor faces a January 2006 deadline to comply with a directive from Wal-Mart to put RFID tags on pallets and cases shipped to the retailer's Dallas-area distribution centers. He says the abili-

says. "What's clear is that the business cases are going to be different based on different [product] categories."

Flannery says the justification is more apparent in P&G's pharmaceutical business, where RFID is viewed as a technology that can help curb counterfeit drugs and bolster consumer safety. But in product categories that are optimized around bar-code technology, there's more work to do, Flannery says.

Despite the encouragement of early adopters, launching RFID pilot projects isn't always possible. Greg Vick, director of distribution systems and Web development at Unified Western Grocers Inc., a Commerce, Calif.-based food wholesaler and cooperative, describes an attempt to find a manufacturing partner with which to pilot RFID technology. But he found no takers.

"The reaction was, 'No, we're not going to do this because it costs a lot of money,'

"The faster payback is really going to be upstream, in working with our raw materials and finishing-goods suppliers and looking at how we manage our materials within our operations."

MIKE O'SHEA, DIRECTOR OF CORPORATE RFID STRATEGIES AND TECHNOLOGY AT KIMBERLY-CLARK CORP.

and 'We're only doing it because we have to,' " Vick said. "I understand the tags are expensive. But there's a lot of talk here that 'we don't want to do slap and ship. We want to look upstream. We want to find that value.' But people aren't ready to act yet."

RFID Moves Beyond Supply Chain Mandates

THE SUPPLY CHAIN continues to be a driving factor for the momentum in RFID. However, companies also are looking to use RFID in more focused applications where incremental returns on investment may be obtained.

While supply chain tends to be far-ranging and disparate (open loop), focused, localized applications (closed loop) can provide such incremental justification for the RFID investment. These applications include warehousing, theft detection, asset location/tracking, people location, mobile payments, in-process inventory tracking, repair and maintenance, and luggage tracking.

Yet another change has been the remarkable interest in this technology by enterprises that

weren't affected by any of the mandates — these organizations are rapidly educating themselves on using RFID to gain a competitive edge or for solving a business problem. For them, the excitement stemming from the rapid reduction in RFID tag and reader prices—along with standardization—provides justification in trying out limited pilot studies.

The applications in which companies are inserting RFID are typically niche-oriented with limited budget needs as opposed to a mandated supply chain. They are typically closed-loop, can have measurable results in the short term and can be deployed in phases.

For example, equipment renters are looking to perform check-in, check-out and security functions with RFID technology to reduce labor costs.

Hospitals are investigating pilot studies on tracking of staff and patients to better utilize their resources and reduce incorrect medication administration.

Airports and airlines are tracking baggage with tags to reduce losses associated with lost baggage.

Some aerospace companies have started to tag and track high-value components of their aircraft.

Companies are starting to use writable RFID tags for automatic tracking of maintenance status on products to reduce human errors in data entry. Warehouses are piloting RFID-based solutions to monitor, track and find warehoused goods. A common challenge reported by these companies is justifying the business case for RFID.

This optimism isn't without caution, however.

Concerns about privacy and security persist. Privacy becomes important if a customer's information is stored on the tag. Today, this issue is alleviated by having the tag contain no data other than an ID and a pointer to a secured firewalled database containing information about the item tagged.

Security concerns revolve around the ability to spoof tags to overwrite the data in tags, overwrite the tag ID or sniff/modify data while it's in transit through the air. These concerns are alleviated by controlling the physical environment so that malicious users can't access the tags. This is relatively easy in closed-loop situations.

In open-loop situations such as a supply chain, the tags are typically moved along with the products all through the supply chain, requiring higher levels of security. As with the Internet, security is a moving target. Security needs to be handled on a case-by-case basis. For instance, having trusted shippers of goods helps alleviate some security concerns.

There are three critical components to an RFID system deployment:

TECHNOLOGY DECISION: Decision on RFID technology that includes hardware, middleware and application software.

Types of Tags

RFID TAGS are categorized according to frequency (low, high, UHF, microwave, etc.) but can also be grouped according to power usage.

Active RFID tags contain their own power supplies, which increase range, and sometimes allow for the information on the tags to be updated. A typical example is the transponder some motorists

use to pay highway tolls.

Passive RFID tags do not use embedded power supplies, and therefore have a shorter range and a more limited set of users. However, passive tags are smaller, cheaper and easier to manufacture. An example is the company-issued ID card, which an employee can wave in front of a reader to gain access to company facilities.

ENGINEERING PRACTICE UNDERSTANDING AND MODIFICATION:

An understanding of how the technology will work in the enterprise's engineering setting and how insertion of the RFID technology into the engineering practice will be accompanied by changes both to the technology as well as to the engineering practice itself.

BUSINESS PROCESS UNDERSTANDING AND MODIFICATION:

This involves understanding and justifying insertion of RFID into the business process, which may also need to be changed, including how the RFID investment is justified in the modified business process.

Involving as many different organizations in the corpora-

tion upfront in the decision-making process allows for better and more informed decisions and also allows for a somewhat longer-term planned vision and strategy for the insertion of RFID into the enterprise's functions.

Since RFID is a horizontal technology that could help different organizations in their business functions, getting

broad involvement upfront allows for spreading the cost and the risk of the project deployment.

Eventually, it's the combination of technology, engineering and business decisions that will allow smooth and successful deployment of RFID in the enterprise

Pushing RFID Deeper Into Manufacturing

AS MANUFACTURERS rush to implement radio frequency identification (RFID) technologies, pushed by the likes of Wal-Mart Stores Inc. and regulatory mandates, don't be surprised if they start asking about what's in it for them. With much of the value appearing to benefit distribution-intensive suppliers such as Wal-Mart, some manufacturers are wondering what they can do to find some value from their RFID implementations that will benefit their operations. The good news is they don't have far to look. The answer lies in all that RFID data.

RFID's ability to provide volumes of data to help manufacturers track products through their factories has been recognized by asset-intensive manufacturers for years. Industries such as semiconductor manufacturing are old hands at this, having architected their application environments to help them manage the complex processes and high volumes of work in progress (WIP) moving through their multibillion-dollar factories.

Now that distribution-intensive companies are recognizing that RFID can help optimize the flow of products from their suppliers directly to the retail shelf, the attention is

turning to the node in the middle, those material-intensive manufacturers that purchase products from the asset-intensive companies (such as chip makers) and then struggle to produce exactly the right number of the right product at exactly the right time that their customers expect. It's here that RFID can help manufacturers find value.

To help manage the hugely complex semiconductor manufacturing process, chip makers have settled on a relatively consistent application stack. At the lowest level is the instrumentation layer, which ensures that the machines that control the physics and chemistry involved in constructing a chip's circuitry behave according to a proscribed process recipe.

The next level in the application stack is a controls layer, which includes RFID technology, obtains data and assigns unique identifiers to the material so it can be easily tracked through the manufacturing process.

The third level is the manufacturing execution layer that tracks WIP and controls numerous rules-based functions such as ensuring that the right process recipe is downloaded to the right process tool when an RFID-tagged lot of wafers arrives.

The fourth level is a temporal historian that keeps a time-stamped picture of the shop floor in its database. The historian allows manufacturers to make "what next," "where next" and "when next" decisions, but it can also include decisions such as "how much" or "how often."

The final level is the workflow layer that choreographs the decision-making between the applications, allowing manufacturers to execute their

plans in real time.

What's remarkable about the application stack described above is its similarity to the RFID application environment defined by EPCglobal Inc., the organization chartered with driving the adoption of global RFID implementation standards. Its RFID application stack includes a data collection layer (i.e., readers and middleware), an execution layer (serving up the RFID-tagged data to the manufacturing execution applications for WIP tracking), a temporal historian for real-time decision-making and a workflow manager to broker activity between all the applications.

Manufacturers should take a look at their application environment to see if all the tagged RFID data they are starting to collect can be leveraged to improve productivity and efficiency, providing a real return on their RFID investment. The real value lies at the top of the application stack. Investing in RFID readers and middleware software allows companies to obtain the data. Mining that data for real business value will only occur if it can be turned into increased visibility to shop-floor events that allow manufacturers to make better business decisions in real time. This is where the temporal historian and workflow management software come in.

As manufacturing shifts from forecast-based planning to demand-based planning, companies are being driven to rethink how their manufacturing applications connect with other enterprise systems such as ERP and supply chain systems.

If a large distributor signals a demand change for a particular product, manufacturing must be able to adapt and respond in real time to change

production schedules and product mix to meet the new requirement. Providing greater visibility of real-time demand signals directly to the shop floor allows business managers to make more informed decisions.

RFID is a powerful, enabling technology that helps manufacturers achieve this goal, but only if they move beyond the data-collection stage.

Generation 2 RFID and the ROI Challenge

AN EMERGING generation of radio frequency identification tags promises reduced costs for manufacturers that have to put RFID labels on pallets and cases for retailers such as Wal-Mart Stores Inc. and Target Corp.

But that can't happen soon enough for many suppliers. Some IT executives have been studying business cases and exploring ways to use RFID data, and they have concluded that benefits won't materialize until tag costs dip below 10 cents.

"What Gen 2 is going to do, hopefully, is get everybody to use the same standard and consequently drive down the costs," says Gary Cooper, chief technology officer at Tyson Foods Inc. "I need the cost to really drop because we're moving hundreds of millions of cases a year and we're a fairly low-margin business. Just do the math: 20 cents times hundreds of millions."

Return on Investment

Cooper says that about 90% of the pallets and cases Tyson ships to Wal-Mart's Dallas-area distribution centers are now tagged. He adds that

Springdale, Ark.-based Tyson has developed business-case models showing a payoff from RFID by late next year or, more probably, in 2007. But tag costs have to hit the single digits for the company to see a return on investment, he says.

EPCglobal Inc., a not-for-profit organization that establishes and promotes RFID technology standards, finalized the UHF Generation 2 standard in December 2004, and the new tags are expected to become available in late 2005. Tag makers, consultants and retail IT analysts say it could take anywhere from one to five years for the cost of Gen 2 tags to drop to 10 cents each.

Edwin Matthews, director of information services at Pacific Cycle LLC in Madison, Wis., says that if tag costs don't drop to 7 cents within the next 18 to 24 months, he will need to "have discussions" with the retailers that are requesting usage of RFID technology.

Matthews says that he has

"I need the cost to really drop because we're moving hundreds of millions of cases a year and we're a fairly low-margin business. Just do the math: 20 cents times hundreds of millions."

GARY COOPER, CHIEF TECHNOLOGY OFFICER, TYSON FOODS INC.

no quibble with the mandates and hopes more retailers hop on the RFID bandwagon to help drive up volume and lower the price of tags. "The cost," he notes, "truly is the tags."

Business Cases Solidify

Jeff Woods, an analyst at Gartner Inc., says tag cost has become a much bigger issue now that some suppliers have developed potentially solid business cases for RFID.

"Six to nine months ago, the business cases were hope and faith," Woods says. "Today, we've got some reasonable leads on what the business cases would be, but they don't have a chance of clearing the existing tag costs."

For suppliers that ship only a small percentage of tagged pallets and cases to Wal-Mart, the payoff is farther away.

"There's not much use to the data until we can get to higher volumes," says an RFID project manager at a large maker of consumer products that is shipping only a limited amount of tagged cases and pallets to Wal-Mart. But large volumes won't be feasible until tag prices sink to the single digits, says the project manager, who asked not to be identified.

"This is the ultimate chicken-and-egg scenario," says Dennis Gaughan, an analyst at AMR Research Inc. in Boston. "More people won't do RFID until the tag costs come down, but the tag costs won't come down until more people do it. These guys are in a bad situation."

RFID at Philips: Tagged And Tracked

FOR ROYAL PHILIPS Electronics, RFID is transforming its Asian shipping operations.

In early 2005, it unveiled its RFID implementation, known as the STAR Project. Using RFID, Philips is able to tag and track goods between its manufacturing facility in Kaoshiung, Taiwan, and its Asia-Pacific distribution center in Hong Kong.

The project started in June 2003 as a Philips initiative to convince its client of the value of RFID. Since Philips is a component supplier of RFID, the firm decided to apply the technology itself, said Mathieu Clerkx, CIO and senior vice president, supply chain management, Philips Semiconductor.

The company started in Asia because the region holds a large number of semiconductor manufacturers. "We decided to start the project between our Kaoshiung assembly plant and Hong Kong distribution center, because it's a very significant route," he says.

The project was supported by IBM on the overall system integration, as well as by Smartag and Tasy's in delivering the labels and readers, and Zebra in providing the printers. Although Philips did not reveal the project investment, Clerkx said the ROI was prom-

ising.

"The major benefit with RFID is to match the information flow with the physical flow [of the goods]," he said. "We can now simplify the [distribution] process tremendously in the receiving warehouse."

Within the project, RFID tags are being placed in three levels of packages, ranging from the palette, to carton boxes, to the individual packing quantity (PQ). Using these tags, when a palette of goods arrived at the distribution center in Hong Kong, the employees no longer have to unwrap them to count and verify the actual shipment, says Clerkx.

He said that previously, a receipt process required employees to unwrap the palette and the carton boxes to tally the PQ. With RFID, as the palettes pass through the reader gate, the total number of carton boxes and PQs will be tallied electronically.

As workers no longer have to unwrap the palette, the

technology has tremendously shortened the receipt process by 400 percent and the redistribution cycle time by 50 percent, from two days to within a day, says Clerkx.

"This is a very significant cost saving for us," he said. "Especially when both labor and rental costs in Hong Kong are so high, RFID has helped to reduce operational costs at the distribution center."

In addition, the technology has also increased the utilization of storage space, according to Clerkx.

Tag it right

For Philips the STAR project was a learning experience as the firm had a dearth of successful RFID precedent cases. Clerkx noted the project was more than merely bringing in some new chips, but also involved a lot of process re-engineering.

Within a supply chain environment, the ability of the RFID system to match the actual physical shipment with the information within the system is critical.

"As long as there's a single doubt about the RFID reading, the technology investment is wasted," he says. "Therefore, quite a lot of effort within the project goes to ensure a 100 percent readability of the tags."

Achieving 100 percent readability was particularly challenging since the product and packing involves a lot of aluminum, which interferes with radio frequency readings, notes Brian Eccles, managing consultant, RFID at IBM Global Services.

He explains that placement of tags is critical in the process. When the tags are placed on boxes, it is important to ensure that when the boxes pile up, tags are not too

"Although Philips is a global company, the process to handle goods varies between each location. The RFID technology will standardize the operation, bringing much easier management of the supply chain management."

MATHIEU CLERKX, CIO AND SENIOR VICE PRESIDENT, SUPPLY CHAIN MANAGEMENT, PHILIPS SEMICONDUCTOR

close to each other and are not blocked as they pass through the reading gate.

“It is a very challenging product and environment,” says Eccles. “But with proper design of the process and placement of the tags, we can achieve a successful operation.”

Clerkx adds the process design involved not only the study of tag placement, but also ensuring the tagged items are piled in a precise direction on the palette.

Integrating Hardware And Software

Besides process re-engineering, the project also required adjustments within the IT systems. The major adjustment was the warehouse management system, notes Eccles. Besides tag placement, the system has also added measures to ensure no double-counts as the palette goes through the reader gate twice.

Although there were no major changes within the ERP system, there were adjust-

“When both labor and rental costs in Hong Kong are so high, RFID has helped reduce operational costs at the distribution center.”

MATHIEU CLERKX, CIO AND SENIOR VICE PRESIDENT, SUPPLY CHAIN MANAGEMENT, PHILIPS SEMICONDUCTOR

ments in the middleware and database to handle the additional information captured from the RFID system. He adds the development time was about three months, much shorter than the time spent in developing the business case and re-designing the supply chain process.

Philips began the project by spending two months to develop a business case with IBM. “The business case looked very promising on paper,” says Clerkx. “Based on that, we de-

ecided to start making the engagement for the project.”

Following that, he notes almost 10 weeks was spent on process design and vendor selection before the actual development work began.

Copying the concept

Building on the success of its first RFID implementation, Clerkx notes Philips plans to expand the technology in other areas.

“It is very easy to expand the same operational process to other locations,” he says. “This is like a ‘cut-and-paste’ of the operation.” The company is planning to expand the RFID technology to its five other chip set assembly plants in Asia and other regions.

The global expansion of RFID usage not only allows other warehouses to enjoy the same efficiency as Hong Kong, but is also an important initiative to standardize processes among its global operations.

“Although Philips is a global company, the process to handle goods varies between each

location,” Clerkx says. “The RFID technology will standardize the operation, bringing much easier management of the supply chain management.”

Apart from internal operations, Clerkx noted the next step is to make use of RFID to better serve its customers. The company has begun the process by using RFID to track its green products—semiconductors produced under an environmental-friendly process.

He explained that green products are often indicated with a green label. Using RFID, the warehouse can easily track the number of green products being delivered, without counting the green labels.

“This is just the beginning of our expanded use of RFID,” Clerkx says. “As the system allows the company to capture and share a lot more information, there’s still much that can be done to make full use of the technology.”

Wireless Security: The Enemy Is Us

IN A PERFECT WORLD of wireless security, no data ever lies exposed on the disks of mobile clients. There's never a possibility of rogue access points (AP) hijacking critical log-in data. All wireless datagrams are encrypted to stymie those sniffing sessions out of thin air. This perfect world evaporates with users, the weak link in wireless security.

"The biggest problem with securing mobile devices is the behavior of the end users," said Michael Disabato, vice president and service director of the Burton Group, a wireless security industry analyst company in Midvale, Utah.

IT needs to analyze wireless vulnerabilities and threats "just like any other type of security," Disabato said, starting with users and their mobile devices. IT needs to start planning for working outside the corporate firewall," he said, adding that the old "M&M security model," with a hard exterior and soft interior, "is dead and gone."

"Now we're on to the Swiss cheese model because people are opening up firewalls to accommodate new services. So network and IT managers and security people need to understand they've now got thousands of perimeters with a lot more problems, in addition to Port 80 [Web] and 443 [Secure

Sockets Layer] problems," he said.

Wireless users, like users everywhere, don't care about underlying security or connections so long as they work and are unobtrusive, Disabato said. "Users will always be the critical link in the security chain," he added. "Technologists must remember that users want IT to perform an assigned task. Anything IT does that interferes with that task will get bypassed."

Hot Growth Market

Strong and friendly mobile-client security is a hot growth market experiencing double-digit sales jumps year over year and jockeying among a slew of established and start-up vendors for position in services, platforms and security. IBM Global Services offers a suite of desktop security services, and start-up Buffalo Technology (USA) Inc., a division of Japan-based peripheral vendor Melco Holdings Inc., has a line of wireless routers and access points that can enforce security policies.

But don't look to Wi-Fi (802.11 wireless data network) service providers to secure users and the wireless links between mobile devices and APs anytime soon, according to John Barrett, director of research at Parks Associates, a Dallas-based company focused

on digital consumer technologies.

"With Wi-Fi, you're introducing a link between the source device and the applications that the carrier can't control," Barrett said. "Carriers now are dealing with a new level of risk and uncertainty brought by the client Wi-Fi wireless links to applications they don't control."

Network service providers do a good job of securing end-to-end access on their Global System for Mobile Communications and Code Division Multiple Access cellular wireless networks, he said, because they exercise end-to-end control. This also applies to cellular data applications and emerging voice over IP via Wi-Fi networks.

Authenticating and authorizing users is the cornerstone of remote mobile access, said Disabato. Cellular providers were early adopters of device authentication to thwart fraud. They also have been enthusiastic backers of emerging identity management standards from standards-setting bodies such as the Organization for the Advancement of Structured Information Standards and the Liberty Alliance.

Securing users on Wi-Fi networks today beyond the control of the service provider's APs usually begins with the 802.1x secure authentication standard, which centralizes authentication for a local Wi-Fi AP with passwords entered onto a remote Radius server.

Access Provided, But Bring Your Own Security

Austin-based Wayport Inc. is a privately held leader in providing Wi-Fi connectivity. According to Dan Lowden, vice president of marketing, Wayport has Wi-Fi APs in the common areas of almost 800 ho-

tels, terminals and gates in six airports, plus wireless business centers in an additional six U.S. airports. Wayport also has ventures to provide APs in McDonald's Corp. restaurants in the U.S. and more than 3,000 United Parcel Service Inc. stores.

Users need to bring their own security for the link between their mobile devices and Wayport's Wi-Fi APs, Lowden said. "We're trying to educate our customers that there's things you as a user need to do to make the connection as secure as possible. We encourage the use of personal firewalls and VPNs" after users log into Wayport's APs, he said, a policy echoed in the security policy and disclaimer on the company's Web site.

"We know a good number of our users are doing that [launching encrypted virtual private network tunnels after the AP log-in], but we don't have statistics," he said, adding that VPN usage statistics are planned for future customer surveys.

Lowden said Wayport installs a network management server at each Wi-Fi AP to monitor and control traffic and to supervise credit card authorizations.

"Our system is set up to block and adapt to attacks as they happen," Lowden said, referring to the Wayport wireless network upstream from the APs. "And if we need to do

Three Steps For Stronger Wi-Fi Security

1 Secure your access point log-in: Check for encrypted log-in fields for passwords and personal information. Minimal 802.1x authentication doesn't require encrypted fields. The more authentication, especially using methods that can't be compromised by a "man-in-the-middle," the better.

2 Secure your session: There's no substitute for a client firewall and VPN tunnel to secure your data after logging into the access point.

3 Know your service provider's security policies: How much security does your Wi-Fi service company provide for thwarting man-in-the middle attacks or detecting rogue access points?

something, we can send a patch remotely to all our locations instantaneously. There's tremendous risk for abuse if we just provide the service. We need to protect users and the access point venue," he said.

Cometa Networks Inc. is a privately held Wi-Fi provider founded by IBM, AT&T Corp.

and Intel Corp. Cometa also uses the 802.1x wireless secure authentication to centrally manage and secure authentication for their APs.

Jim Szafranski, Cometa's vice president of product management, said the company adds a few extra security steps to secure clients, such as encrypting all log-in data entry fields for personal information and passwords. "We do some other things to secure our APs, such as securing them so users can't see other users and their disks," he said.

Schaumburg, Ill.-based Cometa also has intrusion-detection and network defenses to thwart unauthorized usage.

"We've generally had a very well-behaved user set. People are finding value in using our Wi-Fi as a productivity tool, [so] we haven't had a lot of bad user behavior."

Szafranski added that newer technologies, such as Wireless Protected Access and the new 802.11i strong encryption standard, will give service providers the means to do end-to-end integrated security from the client.

"We don't support WEP [Wireless Equivalent Protocol] because of its weaknesses, and we absolutely will support WPA when it's practical," he said. "You'll start to see the gap widening between carrier-class Wi-Fi networks such as Cometa and generic free wireless hot spots."

Wireless Security Requires Integration

CORPORATIONS should think of wireless security as an add-on to their existing security architecture, not as a separate entity. IT managers should either integrate the new wireless piece into the overall company security policy, if one already exists, or take the opportunity to create a plan for the entire IT infrastructure.

Instead of considering wireless security in isolation, technology managers should think of defending their existing wired network against a new set of threats that emanate from the wireless world, says Craig Mathias, principal at advisory and systems integration company Farpoint Group, based in Ashland, Massachusetts.

It used to be the case that corporations weren't embracing wireless technology because of security concerns. Now, however, the leading barrier to adoption is the perceived complexity of wireless security, according to Lisa Phifer, vice president of consulting firm Core Competence Inc. in Chester Springs, Pennsylvania.

Farpoint's Mathias agrees. "Most security solutions are much too difficult for most people to use and understand," he said. "Too often end users are required to be their own security systems integrators," buying a firewall from one

vendor, a VPN (virtual private network) from another and trying to make all the products interoperate.

The situation is beginning to change, as vendors build more functionality into wireless LAN switches. Additionally, some companies are working on the ease of use issue. Mathias points to Ann Arbor, Michigan-based Interlink Networks Inc.'s LucidLink, an enterprise-level wireless security application designed to be easily deployed by small business and home office users. "It's a step in the right direction," he says. "Down the road, the industrial-strength security products will also go this route."

Mathias stresses that wireless will likely form only a small piece of a company's security policy, mostly in terms of specifying which mobile devices and intermediary networks for remote access meet desirable corporate security standards. Companies need to keep updating their security policy and verify the solutions

they have in place to counter attacks are doing their job.

In a large company, IT managers can establish a security operations center (SOC) where people watch out for any violations and attacks. Over time, Mathias expects to see automated tools aimed at smaller companies fulfilling the same functions as a staffed SOC.

How a company thinks about security evolves over time. Rob Kermode, general manager, managed wireless services at Sprint Business Solutions, based in Kansas City, Kansas, points to his own company's experience. Eight months ago, the mobile communications firm considered wireless e-mail to be "very benign," he says, but all that changed with the December 2004 announcement of a planned merger with Nextel Communications Inc.

Suddenly, wireless e-mail became a cause for concern, given the potential for possible leaks of sensitive financial information relating to the planned tie-up with Nextel. Thus far, Sprint hasn't done anything specifically to address the issue, according to Kermode. Like any large company, "we're slow to move," he says. "We're trying to place one bet in security and live with it. We'll research it fully and then do something."

Ultimately, any company needs to be aware that there's no such thing as absolute security and there never will be, in part due to the human element.

"We have a saying that if you could just get rid of the end users, you could have perfect security," quips Jim Burns, senior software developer at Portsmouth, New Hampshire-based network authentication software developer Meeting-

"Most security solutions are much too difficult for most people to use and understand."

**CRAIG MATHIAS, PRINCIPAL,
FARPOINT GROUP**

house Inc.

What's needed is for companies to establish a "culture of security," according to Farpoint's Mathias, and to provide training and support to their users so that employees understand how to use wireless technologies safely.

RFID Crack Raises Specter of Weak Encryption

WITH A LITTLE bit of technical acumen and a few hundred dollars, enterprising

thieves can walk away with some late-model cars and gas them up for free to boot, according to research published by computer security experts at the Johns Hopkins University in Baltimore and RSA Security Inc.'s RSA Laboratories in Bedford, Mass.

In January, the researchers published the results of a technical analysis of a kind of secure radio frequency identification (RFID) technology called Digital Signature Transponder (DST) from Texas Instruments Inc., which is widely used to secure newer-generation automobiles and electronic payment systems like Exxon Mobil Corp.'s Speedpass. The work revealed serious weaknesses in the cryptographic security used to protect data sent back and forth, and shines a light on the problem of security systems that rely on aging or inadequate cryptography, according to experts.

The team of researchers included staff from Johns Hopkins' Information Security Institute such as Avi Rubin, the institute's technical director, who gained fame for his analysis of flawed electronic voting technology from Diebold Inc.

Rubin and a team of three graduate students, along with

cryptography experts from RSA, used reverse-engineering techniques and custom-designed tools to crack the cryptographic keys used to secure the systems and simulate both the RFID DST tags and readers. The hack allowed researchers to disable a vehicle immobilizer in a 2005 Ford automobile using a specially equipped laptop computer, and purchase gas at a number of Exxon Mobil locations with a homemade Speedpass device, according to a copy of their findings posted online.

The TI technology is vulnerable to attack because it uses a decade-old, 40-bit cryptographic key to encrypt communications between the RFID DST tags and readers, the researchers found. TI also used an unknown and proprietary encryption algorithm on its DST devices. But Rubin's team reverse-engineered the secret algorithm by observing how DST tags responded to specially crafted challenges. Once they guessed the algorithm, researchers created a software program that could be used in so-called brute-force attacks on DST devices to recover the secret cryptographic keys, Rubin said.

The researchers worked for two months to break the TI algorithm, but once it was

cracked, they made short work of the rest of TI's product, designing tools that guessed the encryption keys on five TI gas Speedpasses in two hours, Rubin said.

Other commercial security systems also use the DST technology, including card-key access systems for buildings and livestock tracking products, he said.

Tony Sabetti, global business manager for TI's RFID Systems, said that Rubin's team broke only one element of the system's security and that successful thieves would need to defeat more security features to carry out a crime. For example, even crooks who could disable the vehicle immobilization feature would still have to find a way to start the car. And, for the Speedpass payment system, TI has other security features in place to stop fraudulent purchases that the company cannot discuss, he said.

Sabetti said TI does sell updated versions of the RFID technology that use more advanced, 128-bit encryption algorithms. TI will also begin ramping up production of the 128-bit RFID chips, which have been available since 2003, the company said in a statement.

But Sabetti questioned whether the older technology is even seriously at risk.

Johns Hopkins' "methods are wildly beyond the reach of most researchers," he said. "JHU is not painting an accurate picture of the risk for consumers. We recommend that customers apply the level of security they need for the application, and we're vigilant in making sure the systems are secure. I don't see any reason to change this approach."

TI also said it would be difficult for attackers to read RFID tags so that they could

"When you're talking about snooping transactions out of someone's pocket, one would have to ask 'What are the odds of that?'"

**TONY SABETTI, GLOBAL
BUSINESS MANAGER FOR
RFID SYSTEMS,
TEXAS INSTRUMENTS INC.**

then clone them, or intercept communications, noting that the equipment Rubín's team designed to do just that was "complex, expensive and cumbersome."

"When you're talking about snooping [RFID] transactions out of someone's pocket, one would have to ask 'What are the odds of that?'" Sabetti said.

But Rubín said that motivated thieves, such as organized crime groups, could have the desire and resources to carry out similar attacks, and noted that his group did simulate (and videotape) a successful attack in which the signal from an RFID Speedpass was captured. Assuming that the technology is too hard to crack is a mistake, he said.

"People build systems and

"People build systems and underestimate what an attacker could do to take advantage of them."

AVI RUBIN, TECHNICAL DIRECTOR, INFORMATION SECURITY INSTITUTE, JOHNS HOPKINS UNIVERSITY

underestimate what an attacker could do to take advantage of them," he said.

Unlike voting machine maker Diebold, TI paid attention to security when it designed the DST system, Rubín said. But the product needs to be

updated with stronger encryption, or an alternative system for authenticating users. The Johns Hopkins hack also calls attention to a more widespread lack of security in consumer software and other products.

"There are a lot of consumer products out there that don't have adequate security," he said.

Bruce Schneier at Counterpane Internet Security Inc. agreed, saying that it's common for consumer systems to have inadequate security. "The number of lousy encryption systems out there is amazing ... even to me," he wrote in an e-mail.

Still, companies must weigh the cost of implementing stronger security against the

cost of fraud, Schneier said. "If a company is losing \$1 million a year to fraud, and fixing the security costs \$2 million a year, then it would be foolish for it to fix the system," he said.

However, the question of adequate versus inadequate security on systems like Speedpass and auto antitheft devices becomes more complicated when consumers, not companies, pay the cost of fraud.

"My worry is when a company implements poor security, and then the users suffer losses because of it," Schneier said. "If TI's customers are losing money because of bad TI security, then TI has both a moral and legal obligation to either inform its customers or fix the system."

© Copyright 2005, Computerworld Inc., Framingham, Mass.

See our full selection of Executive Briefings at the Computerworld Store.

<https://store.computerworld.com>

Computerworld has Executive Briefings on many subjects including Outsourcing, Wireless, Storage, ROI and Security.