

# NetworkWorld®

EXECUTIVE GUIDE

# Getting Wireless RIGHT

Wireless LANs move beyond **data**  
to **voice** and **video**

COMPLIMENTS OF



## — Table of Contents —

---

[Introduction: Wireless LANs aren't just for data anymore.....](#)3

### **Trends in wireless LANs**

---

[Wireless wake-up call .....](#)4

[WLAN standards alphabet keeps growing .....](#)7

[Benefits of running thin clients over WLANs .....](#)9

[Municipal WLAN plans draw mixed reaction .....](#)11

[Deploying 802.11i for WLAN security .....](#)12

### **Voice over Wi-Fi**

---

[WLAN-based phones off to a good start .....](#)15

[Mobile VoIP set to roam even wider .....](#)15

[When Wi-Fi meets cellular .....](#)17

### **WLAN testing**

---

[Clear Choice Test of voice over wireless LAN gear .....](#)19

[QoS enforcement: What happened? .....](#)25

[Wireless voice architectures remain diverse .....](#)26

### **Case Studies**

---

[Wireless to take off an Las Vegas airport .....](#)27

[Dartmouth retools for Wi-Fi video .....](#)29

# Introduction

## GETTING WIRELESS RIGHT

James Wiedel, director of networking at the University of Southern California's information services unit, treats his wireless network just like his wired network. "Both nets require registration and both nets need to know who you are, where you are and how you are accessing them," he says. "We have cable, we have fiber or glass, and now we have air. It's just another method of transport."

Wiedel assigns users at USC's Los Angeles campus an ID and password, which they need to log onto either the wired or wireless networks. As an additional level of security, wireless traffic must go through a VPN tunnel. "We have encryption in both directions and authentication," he says.

When Wiedel jumped into wireless networking, the standards were still evolving and many IT professionals shied away from wireless because of security concerns. Today, however, most everyone agrees that with new standards and new tools, airtight wireless security is getting easier to accomplish.

For example, experts recommend that if you're starting from scratch today, your best bet for wireless LAN (WLAN) security is to deploy gear that supports WPA (Wi-Fi Protected Access) or WPA2 for encryption and 802.1X for authentication. Long term, you should be looking to migrate to 802.11i when products based on that encryption standard become widely available.

Also known as Robust Security Networking, 802.11i is the next big thing in WLANs. This 200-page standard replaces the 10-page Wired Equivalent Privacy (WEP) standard and calls for use of the state of the art Advanced Encryption Standard (AES) and 802.1X authentication, giving buyers the best of both worlds.

Of course, there are other tricks of the wireless security trade that are being used to enhance current security methods, such as creating separate virtual LANs (VLAN) for different types of traffic. For example, Children's Hospital Central California, a 255-bed pediatric hospital in Madera, runs voice traffic on its 802.11b network on a separate VLAN. Similarly, at Indiana Heart Hospital in Indianapolis, data is supported by an 802.11a wireless network while wireless voice traffic is handled by a separate 802.11b VLAN.

If you are looking for other tools to keep your WLAN secure, there are specific tools that detect rogue access points, as well as more general purpose tools from both established network/systems management vendors and wireless-focused start-ups that offer policy enforcement, performance management, security and reporting.

### Alphabet soup

The WLAN alphabet is constantly growing, as standards setting bodies develop new protocols and technologies that will transform wireless networks.

For example, 802.11k will deal with management issues, 802.11d handles multi-country roaming, 802.11r is for fast roaming, and 802.11s deals with wireless mesh networks.

The latest buzz is about 802.11n, also known as MIMO, which stands for multiple-input/multiple-output. The technology promises to enable WLANs to support speeds in excess of 100M bit/sec by enabling data streams to follow multiple wireless paths to their destination. Besides promising to boost performance, MIMO will greatly extend the range of WLANs. The 802.11n products are just starting to ship.

A major trend in wireless is voice over Wi-Fi (VoWi-Fi). Overlake Hospital Medical Center in Bellevue, Wash., for example, uses VoWi-Fi so nurses can keep in contact with doctors and other nurses without having to search for a landline.

UC-Davis Medical Center in Sacramento is moving to WLANs as a way to simplify and improve communications. The hospital is replacing a hodge-podge of voice mail, e-mail, individual pagers, group pagers, overhead pagers, intercoms, radios, cell phones, fax and text messaging with multi-service handsets that can roam between cellular and Wi-Fi networks.

But deploying VoWi-Fi won't be easy. That's the inside scoop based on Network World's latest testing. We found that when voice traffic runs on the same WLAN as data traffic, call quality drops considerably, even if QoS is deployed.

Detailed analysis on this groundbreaking test, plus behind-the-scenes looks at what cutting-edge users are doing and the latest information on wireless security trends are featured in this Network World executive guide.

# Trends in Wireless LANs

## WIRELESS WAKE-UP CALL

■ By Jim Geier

Cisco's recent purchase of Airespace could kick-start the wireless LAN market, creating new options for enterprise customers, particularly Cisco shops that were reluctant to pay a premium for Cisco gear, but which were also skittish about going with a WLAN switch start-up.

Cisco initially will offer Airespace WLAN switches and thin access points under the Cisco name alongside Cisco's Aironet fat access points, which are part of its Structured Wireless-Aware Network (SWAN) product line.

The Airespace WLAN switch offers superb security and management features at a much lower total cost of ownership than an Aironet rollout. As a result, it's likely that many customers that shied away from Cisco's

higher-priced offerings will move forward with the Cisco-Airespace product.

Cisco plans to integrate Airespace switches with SWAN, but there is no clear definition of how Cisco will make this integration work. It's likely Cisco will interface Aironet access points to Airespace WLAN switches. This will let Cisco customers with Aironet access points migrate to a wireless switched network.

Cisco's purchase of Airespace is seen as validation of the thin access point approach to WLANs, an approach taken by the start-ups such as Trapeze Networks, Aruba Wireless Networks and Airespace. Cisco followed the more traditional approach of deploying fat access points and connecting to current Ethernet switches. In Cisco's case, the company created a WLAN blade for the Catalyst 6500 switch.

### A switch in time

Cisco's move also reflects an acknowledgement that the future belongs to the Airespace model. According to Infonetics, Cisco is No. 1 in WLAN revenue, with 17% market share, followed by Linksys (owned by Cisco), D-Link Systems and Netgear. But Infonetics reports that fierce pressure is severely impacting revenue – in 2004 worldwide units sold increased 51% but revenue only increased 15%.

Synergy Research predicts that worldwide revenue from traditional access points will drop 2% in 2005, 35% in 2006 and 11% in 2007. On the other hand, sales of WLAN switches will grow 150% in 2005, 53% in 2006 and 59% in 2007, according to Synergy.

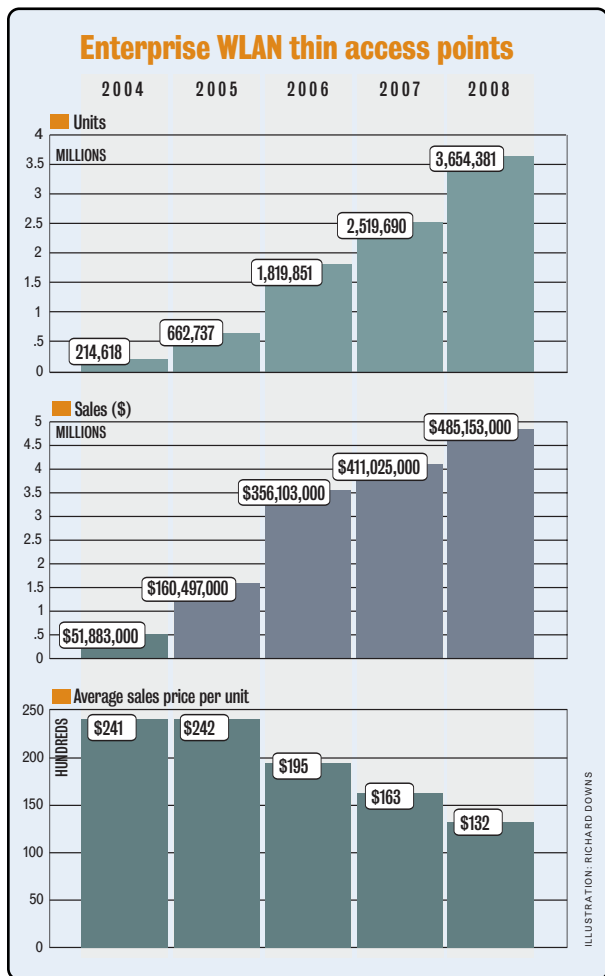
In the fat access point scenario, access points such as Cisco's Aironet provide radio-based connections in addition to security, management and performance enhancements. The advantage is that you easily can make use of your Ethernet infrastructure, but the downsides are that the access points are relatively expensive and difficult to manage.

With the thin access point model, wireless switches provide those security, performance and management features. The thin access points then can concentrate on what they're intended for – reliable, high-performance radio technology.

### WLAN switches offer benefits

Beyond the cost savings, there are a number of technical reasons, including security, performance and ease of management, which make WLAN switching the way to go.

Security is a major concern for IT executives deploying WLANs. Unfortunately, WLAN standards cover encryption between user and access points, but not authentication,



## Trends in Wireless LANs

intrusion detection and rogue access point control.

For example, a hacker could try to compromise security by attaching a rogue access point to the wired network. Unless the company implements careful Ethernet switch port control, the rogue access point could gain access to the corporate network wirelessly from a nearby car.

Likewise, an employee might purchase an access point from an office supply store and connect it to the corporate network without setting acceptable security controls, which inadvertently leaves an opening for a mischievous person to exploit.

However, a wireless switch authenticates and configures each access point based on the company's security policies. An employee or hacker might plug the access point into the network, but the wireless switch will disable the connection if the access point is not able to authenticate or configure correctly.

Additionally, a wireless switch ensures that all authorized access points comply with security policies. Access points can be configured to only allow policy changes from the wireless switch, which precludes a hacker from plugging a laptop into the access point via a console cable and change configurations that make the network insecure.

The wireless switch can be kept inside a locked room and out of hackers' reach. If a hacker attempts to disconnect a legitimate access point and plug in a rogue, the switch will notice what's going on and physically disable the rogue's access to the corporate network.

### Higher performance

A fairly common issue with WLANs is that coverage holes - areas with low signal strength - often exist. This occurs because of poor placement of access points and the dynamics of the environment. After the initial installation of access points, for example, a company might add walls to create new offices or move large machinery. This affects the propagation of radio waves, which leads to lower and sometimes inadequate signal strength in parts of the building.

Some applications, such as e-mail and Web browsing, hold up pretty well as users roam through coverage holes. At least a user can read e-mails or view Web pages in cache on the mobile device while on route to a covered area.

However, a warehouse inventory management application commonly requires a constant connection between the terminal (mobile device) and the host (application server). If the wireless connection is temporarily lost, the

user usually must log back on to the system. Sometimes this can even cause errors on the server if the loss of connection occurs in the middle of a transaction.

WLAN switches can compensate for the periodic disconnected state of mobile devices as users roam through coverage holes. The switch is smart enough to know that a mobile device no longer has a wireless connection to the access point. The switch continues to maintain the applicable connection with the application server. The worst case is users might experience application delays, but the application remains available and ready to start where it left off.

Another issue is that voice-over-WLAN (VoWLAN) phones will drop calls as users walk through areas where signal strength is too low. Cisco publishes stringent guidelines for deploying

WLANs that enable effective VoWLAN operation, but most traditional thick access point WLAN installations don't come close to offering the coverage and speedy handoffs between access points that VoWLAN applications require.

Wireless switches, though, are designed to provide adequate handoffs between access points and intelligently restarts to avoid dropped calls.

### Improved management

Often, the costs associated with ongoing operational support of a WLAN becomes higher than the initial cost of hardware and software, unless you ensure that effective management tools and support methods are in place. WLAN switches are designed to offer effective, centralized support necessary to realize an expected ROI. Centralized management is possible with wireless switches, which can configure, monitor and upgrade multiple access points automatically.

For instance, a company can interface an access point into a WLAN switch, and the switch automatically configures the access point. This saves the time and potential human error of having an administrator perform the configuration. Also, the wireless switch immediately can detect a failed access point and alert appropriate staff.

Also, network managers might not have much experience with radio-based systems. An important aspect of wireless switches is that they offer a layer of management that reduces the need to understand radio waves. The automated switch functions, such as intelligently restarting applications when connections are lost and rogue access point control, compensate for lack of wireless network skills.

Because a wireless switch houses most of the intelligence of the WLAN, the access points can focus on radio

**Often, the costs associated with ongoing operational support of a WLAN becomes higher than the initial cost of hardware and software, unless you ensure that effective management tools and support methods are in place.**

Trends in Wireless LANs

connectivity, which usually keeps the prices of thin access points considerably lower than the thick access point counterparts. As a result, a company with thin access points can migrate to newer technologies at lower costs. The corresponding changes to the rest of the network can be done through software upgrades on the switches.

While it might be tempting to use the current wired Ethernet network to interconnect access points, the improvements in security, performance and management when deploying a wireless switch likely will make the ROI much better in the long run.

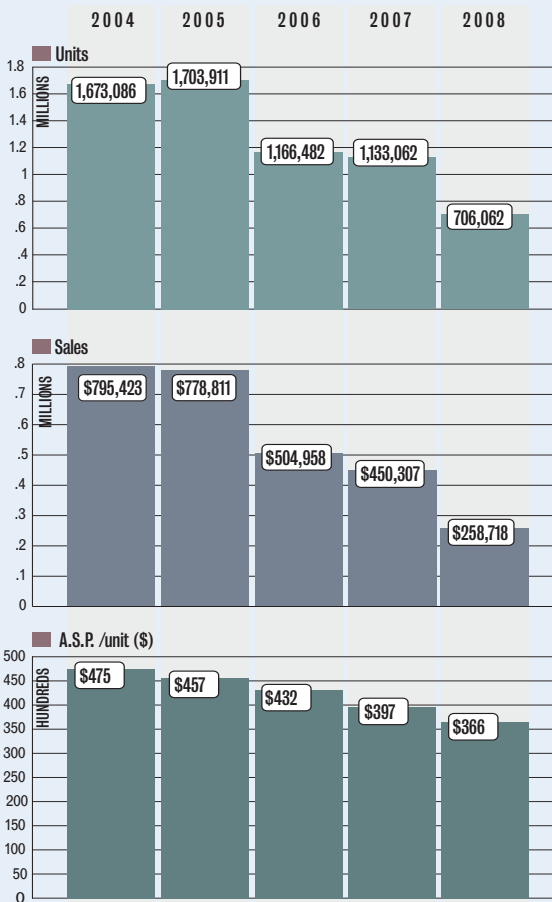
Just keep in mind that you probably won't be able to use third-party access points and still realize all the benefits touted by the wireless switch maker.

That's not too much of a problem for Cisco shops because they can choose Airespace and still be within the realm of Cisco for their entire network. But companies with non-Cisco infrastructures probably will need to use access points from the wireless switch vendor, which probably will be different from the vendor of the wired network.

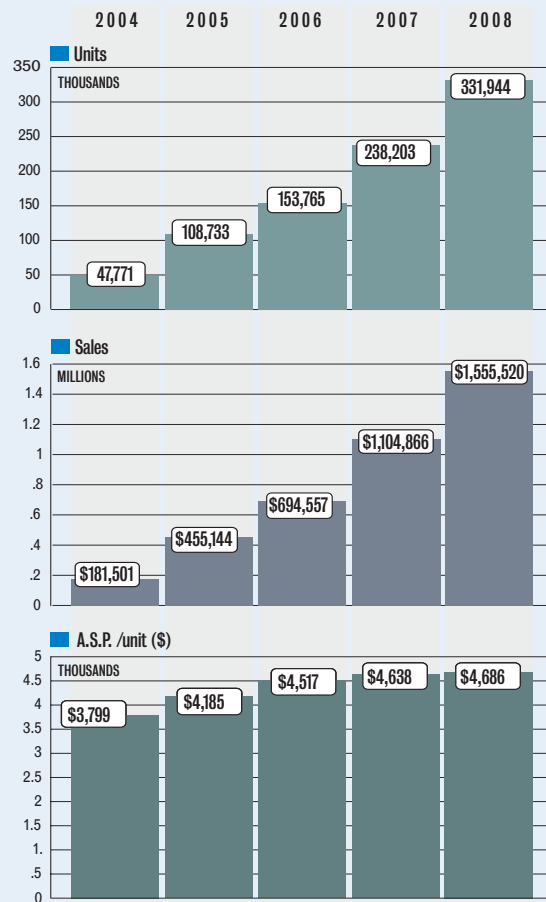
*Geier is the founder and principal consultant of Wireless-Nets, (www.wireless-nets.com), a consulting firm focusing on the implementation of wireless mobile solutions and training. He is the author of the books Wireless LANs and Wireless Networks - First Step.*

**Thin is in** While Cisco is currently the market leader in wireless LANs with its thick access point architecture, the future belongs to the thin AP/WLAN switch model, according to Synergy Research.

Enterprise WLAN traditional access points



Enterprise WLAN switches/controllers



## Trends in Wireless LANs

## THE WLAN STANDARDS ALPHABET KEEPS GROWING

■ By John Cox

The bad news is the alphabet of IEEE standards for wireless LANs keeps expanding. The good news is you can ignore a lot of it, at least until the new technology starts showing up in actual WLAN products.

Some projects in the 802.11 Working Group, which oversees wireless-LAN standards, are nearing completion. Other groups, such as those working on mesh networks and for fast roaming, are just starting up.

Most network executives will never have to worry about the fine print in these technical standards, which cover things such as modulation schemes, access protocols and authentication, or whether to transmit power in the Layer 1, or physical layer.

Most of the worrying is done by wireless chip makers, WLAN product manufacturers and software engineers.

Of course the standards are only one part of the decision making involved in deploying an enterprise WLAN. Corporate suppliers might swear they support 802.11i, the recently completed standard that fixes many weak points in WLAN security.

"But that's almost a meaningless statement," says Sheung Li, product line manager and 802.11 liaison for wireless chip maker Atheros Communications. "The question is, what is the vendor actually offering in terms of capabilities and tools for a full security implementation?"

After all, standards rarely introduce a new technology. Instead, they create common ways for a WLAN to be created, monitored and managed. Vendors use the standards as a foundation and add unique or at least distinguishing features and functions atop the standard. In many cases, vendors will have their own code to do a given WLAN function and then replace it when an 802.11 standard is ratified. For example, Airespace has written its own code for radio resource measurement and management in its WLAN switch product line; when the 802.11k standard is ratified, the vendor will upgrade its products with code based on that.

Most vendors have at least one person who tracks or participates in these IEEE groups. They should be able to give customers a road map of their implementation plans.

The Wi-Fi Alliance, an industry trade group promoting 802.11 WLANs, is taking on an expanding role in creating certification tests for WLAN products as new IEEE stan-

dards are ratified. The alliance is finalizing test programs for the 802.11d and h standards and has plans to introduce others next year.

The alliance also has a role in refusing to sanction new WLAN features that vendors introduce ahead of final IEEE ratification. A few vendors, mainly in the consumer sector, have just started introducing WLAN access points that use multiple antennas and special algorithms to boost throughput. This technology, called multiple input multiple output, is a likely candidate for the 802.11n standard. But that work has only just begun.

"We want to discourage any use of terms suggesting that [802.11n] is real and that products can be 'compliant'" at this stage, says Frank Hanzlik, the alliance's managing director.

Meanwhile, the starring role in 802.11 standards surely goes to the recently formed 802.11n Task Group, which is charged with creating a standard for WLANs with at least 100M bit/sec throughput, compared with 20M to 25M bit/sec today. The group is sifting through scores of technical proposals. Don't expect a final standard until sometime in 2007.

But there are plenty of other WLAN advances completed or in the works. Some of the lesser-known or more recent standards work on 802.11 are:

- **802.11d, multi-country roaming:** Old by WLAN standards, the working group finalized 802.11d in 2001. It's a way for WLAN access points to broadcast what country they're in and what country-specific rules client network interface cards have to follow. You can fly from New York to Rome, walk into your office or hotel, fire up your wireless laptop and expect to connect with whatever WLAN is open.

- **802.11F, inter-access point protocol:** The capital "F" designates a "recommended practice" not a formal standard in IEEE parlance. The basic idea was to create a way for access points to talk among themselves and to transfer data associated with a connection quickly from one access point to another. But WLAN vendors already have figured out how to do this on their own for their own access points. The document was published in mid-2003, but so far is not being embraced. "There are a set of technical issues that make this [hand-off] difficult," says Andrew Myles, manager of wireless standards for Cisco's Wireless Networking Business Unit. "As far as I know at this point, no one is planning to support it."

- **802.11h, dynamic frequency selection, and transmission power control:** the original idea for

The good news is you can ignore a lot of it, at least until the new technology starts showing up in actual WLAN products.

## Trends in Wireless LANs

802.11h was to create a set of management messages for access points and clients in the European 5-GHz band to coordinate efforts to avoid interfering with radar and satellite communications in the same band, Atheros' Li says. The WLAN devices select another channel and adjust power output if needed. But these same actions can be used to improve WLAN efficiency, quite apart from any specific regulatory rules, according to Li, as more countries open more 5-GHz bandwidth for use by 802.11a WLANs. The standard was final in September 2003. Products with some of these features might start appearing soon. Some elements of this work are being carried into another standard, 802.11k. The Wi-Fi Alliance will have certification testing for both 11d and 11h in 2005, according to Cisco's Myles.

- **802.11j, use of the 4.9- to 5-GHz spectrum in Japan:** Originally, this group's work was focused on making changes to the 802.11 media access control and 802.11a PHY layers to gain Japanese regulatory approval in this band. But Li points out that the FCC recently allocated this same band for licensed spectrum set aside solely for public safety and homeland security. The 802.11j work on how to use this spectrum could prove useful in the U.S. as vendors introduce products for public safety networks in this band.

- **802.11k, radio resource management:** Launched in late 2002, this project will standardize an array of radio measurements, dealing with roaming requests, an array of data about the radio channel and

data about the client devices. In addition, this data can be made available to higher-level WLAN management applications, where the information can be used in tasks such as optimizing performance and balancing traffic loads. Task Group K is sifting through some 1,000 comments that members submitted on the proposed standard during a recent ballot, says Clint Chaplin, wireless standards lead at Symbol Technologies. Completion is likely in mid-2005.

- **802.11r, fast roaming:** Handing off clients quickly from one access point to another with their authentication and security policies intact becomes critical when clients are moving, such as VoIP calls made with handheld WLAN phones, Chaplin says. This group, launched in 2004, is creating a standard way to make roaming fast, so that users don't have to re-authenticate at each new access point or have their calls disrupted, he says.

- **802.11s, wireless mesh for access points:** Formed in early 2004, this group is creating a standard that will let access points act as routers for wireless data, forwarding traffic to neighboring access points as Internet nodes do today with a series of multi-hop transmissions. Such mesh networks are inherently more reliable because they can route around failed nodes, and can adjust to balance traffic loads and optimize performance. The members still are sorting out their approach and schedule. Symbol's Chaplin says the first call for proposals likely will be next month.

## Wireless timetable

A myriad of wireless standards will be set in the coming years. Here's a look at what's on tap from the IEEE.

**802.11j:**  
Standardizes use of  
5-GHz channels.

**802.11k:** Defines  
WLAN radio  
measurements.

**802.11n:** Defines  
WLAN with at least  
100M bit/sec  
throughput.

**802.11r:**  
Characterizes fast  
roaming between  
access points.

**802.11s:** Sets standard  
for wireless mesh  
topology.

2004

2005

2006

2007

2008

## Trends in Wireless LANs

## THE BENEFITS OF RUNNING THIN CLIENTS OVER WIRELESS LANs

■ By John Cox

Thin clients were once as chained to the corporate desktop as full-blown PCs. But that's changing now as wireless LANs and 3G cellular networks become more common.

Using both types of wireless networks, end users can have a relatively simple, diskless notebook-style or handheld device that connects securely, often via a Web interface, to their full suite of enterprise applications running on centrally managed server farms.

The benefits are extensive:

- Minimal or no application development for mobile computing.
- Data remains on servers, not on clients that can be lost or stolen.
- Software updates are made on a few servers, not on many clients.
- Real-time access to enterprise data for mobile workers.

A number of recent developments, besides better wireless connections, are fueling interest in wireless thin clients. One is the growing use of operating systems tailored for thin-client devices, especially Windows XP Embedded (XPE). But lightweight Linux variants also are cropping up.

Other developments include: the growing sophistication of display technology; the ease with which a growing number of peripherals can be used by thin clients, via USB and other high-performance interfaces; a new breed of thin clients designed for wireless deployments, including products from HP, Maxspeed, Neoware, Wyse Technology and, most recently, Motion Computing.

Motion executives discovered that some of the healthcare customers for the company's line of tablet PCs, running Windows XP Tablet PC Edition, were configuring the devices as thin clients - with no local data storage - linking to Citrix servers.

"The evolution of wireless nets was now allowing the bandwidth for thin-client sessions to work efficiently," says Peter Hunt, vice president of the value-added products division for the Austin, Texas company. "So we thought of using the existing hardware platform but using Windows XP Embedded as the operating system, freezing the software image of the device into a much smaller footprint and using a flash RAM drive instead of a spinning hard drive."

Motion recently released the M1400TC Table Client, priced at about \$1,650. The tablet boasts handwriting support, a wide viewing-angle display screen and a built-in fingerprint reader. It has a 10/100M bit/sec

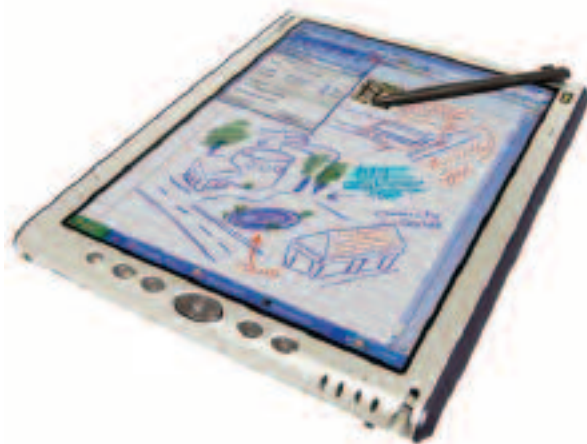
Ethernet interface, a PC Card slot, two USB ports and an 802.11g/b WLAN adapter.

### Familiar middleware

If much of the client technology is new, the core middleware components of a wireless thin-client deployment are not. They're the same as those used in conventional thin-client desktops. Citrix Systems is the leader in this area, with its suite of software built around its MetaFrame server Independent Computing Architecture (ICA) protocol for client-to-server communications. The most recent, and renamed, release is Citrix MetaFrame Presentation Server 3.0. Rivals include Microsoft Windows Server 2003 Terminal Services, Tarantella's Secure Global Desktop, Jetro Platforms' CockpIT and BoostIT, and HOB's HOblink JWT Java software.

Microsoft Terminal Services runs server-based

**This clients go mobile: Broadband wireless links and sophisticated client devices are making thin clients a viable model for wireless deployments. Shown are Sierra Wireless' Aircard 580 for Verizon's EV-DO 3G cellular net, with 300-500K bit/sec bandwidth (right) and Motion Computing's new thin client product, with built-in WLAN adapter (below).**



## Trends in Wireless LANs

Windows applications, sharing them with multiple users. Microsoft offers a less-developed rival to ICA called Remote Data Protocol.

Lexington Medical Center, a 292-bed complex in West Columbia, S.C., has rolled about 60 of an eventual 100-plus thin clients that link over a Cisco 802.11g/b WLAN to a suite of nursing, clinical and physician applications. These run on a group of 15 Citrix servers, based on HP ProLiant servers with Windows 2000 and Service Pack 4.

The initial focus for the thin clients is to let nurses access a Web-based server application via Citrix for administering and monitoring medications given to patients, usually at bedside.

**"Think about that: a whole series of thin-client devices accessing not just [personal information manager] and e-mails like today's BlackBerry, but all of your corporate applications,"**  
**Giobbi says.**

Sixty Wyse Winterm 9455XL thin clients are mounted on mobile carts from Flo Healthcare. The carts, designed for bedside computing, look like pillars mounted on a stable platform of rotating wheels. They are fitted with a flat shelf, with a sealed slotted mount beneath it for the thin-client box, a hidden connection to the WLAN antenna mounted on the rear of the shelf, a slide-out full keyboard, and a 17-inch flat panel display. Lexington Medical chose a sealed lead-acid battery as an alternative to the more expensive nickel metal hydride battery option.

The hospital staff also added to the cart a pistol-like bar-code scanner. Nurses scan their own IDs, the patient IDs and the medications being administered. The application software checks for the "five rights," as they're known: the right patient, medication, time of day, dose and route - the way the drug is given to the patient.

"The nursing staff is really enjoying the system," says Cindy Malphrus, the project manager for the system. "It's preventing errors. We get [application] reports to see how many errors have been prevented. And they think they can actually give meds faster now, although that wasn't a reason for doing this."

By a stroke of good luck, the thin clients were being deployed just as the rest of the IT group completed the hospital-wide WLAN deployment. One goal for the new

WLAN is to support wireless VoIP, using Cisco handsets. "You need to have good WLAN coverage for that," says Jeff Jones, Lexington's network administrator. "By designing the WLAN for optimal phone coverage, it gave us good coverage also for our thin clients."

The rollout went off without a hitch. Training sessions showed nurses how to maneuver and adjust the carts, and cautioned them that the stubby black rod was not a handle but the WLAN antenna.

**3G is key**

One big change in has been the spread of 3G cellular networks that can support data services in the 300K to 500K bit/sec range. Finally catching up were XPE software drivers that would support cellular cards for networks such as Evolution-Data Optimized (EV-DO).

Zumasys is a Lake Forest, Calif., Citrix value-added reseller with more than 70 customers using thin clients on 3G cellular data networks, says Company President Paul Giobbi. He's seeing adoption of diskless, laptop-like thin clients such as Maxspeed's MaxBook married to EV-DO offerings from carriers such as Verizon. "All you need is wireless access to the Internet," he says.

"Think about that: a whole series of thin-client devices accessing not just [personal information manager] and e-mails like today's BlackBerry, but all of your corporate applications," Giobbi says.

One client is Continental Lab Products, a San Diego supplier of laboratory products to life science organizations. The company last year extended its Citrix thin-client deployment by using Panasonic Toughbook laptops and a choice of Sierra Wireless cellular interface cards so sales representatives can access intranet, CRM and ERP applications over Verizon's EV-DO network, BroadbandAccess. Sales representatives can access orders, inventory and other data on the road or at a customer's site. The deployment won best in class recognition in Qualcomm's 2004 3G cdmaA-List awards.

## Trends in Wireless LANs

## MUNICIPAL WLAN PLANS DRAW MIXED REACTIONS

■ By John Cox

A public political spat in Pennsylvania recently threw light on potential issues that might stymie citywide wireless LANs intended to give residents and businesses broadband Internet access.

Such networks are pitting cities such as Philadelphia that want to build their own Wi-Fi networks against carriers such as Verizon. Carriers, which fear losing customers and influence, are lobbying hard for laws that will block cities and towns from building such networks.

It's an issue that has network professionals trying to gauge what effect new Wi-Fi networks could have on their organizations.

"This [kind of network] would be of significant value to our [legal] advocates that do outreach work around the city at community sites and people's homes," says John Greiner, CTO for Legal Services of New York City. "If we had pervasive WLANs across the five boroughs, we could much more cost effectively mobilize our staff."

Greiner says the organization has been experimenting with cellular data services but he finds them too slow, too pricey, with spotty coverage. All these limitations potentially could be overcome with a city WLAN.

"My bet would be that pervasive WLAN will culture all sorts of innovative technology, applications and economic development, similar to the Internet," he says.

The organization's corporate network probably wouldn't change much, he says, unless the city WLAN was able to offer business-class service-level agreements and QoS.

Northern Illinois University has its own WLAN, and so far the neighboring city of DeKalb doesn't have plans for a citywide network. But Walter Czerniak, the school's assistant vice president for IT, says, "A city network would provide access for our students who live off-campus. In that light, we would support [such a net] in any way we could."

But potential problems include unpredictable performance based on user densities, unsolvable interference issues in the increasingly crowded 2.4-GHz band and a greater vulnerability of WLAN users to viruses or other attacks, which then could leak into corporate networks when employees log on.

"802.11b/g/a all ride over unlicensed spectrum, with no rules on what happens when you create channel interference for neighboring access points," says John Halamka, CIO of CareGroup Healthcare Systems in Boston. "As long as your [access point] power settings are within FCC guidelines, it's a Wild West show. There will be plenty of

opportunity for interference."

Outdoor radios from vendors such as Strix Systems use power levels from 100 to 800 milliwatts, two to 16 times as much as is used by indoor WLAN access points.

The chances of such powerful radios being set up outside of corporate offices are growing. Even though Verizon essentially got its way with a bill signed last week by Pennsylvania Gov. Edward Rendell (carriers argue that municipalities creating nets enjoy unfair advantages in the form of taxpayer subsidies and the ability to issue bonds), Philadelphia was granted permission to carry on with its network plan.

These public networks are taking form in all kinds of communities, typically using 802.11-based radios in the unlicensed 2.4- and 5-GHz spectrum bands. A flock of companies, ranging from giants such as Nortel to start-ups such as BelAir, Strix, Tropos and Vivato, offers wireless mesh radios designed for what they see as a market on the verge of exploding. "We're watching this whole development closely," says Doug Huemme, assistant vice president of marketing at Strix.

Generally, these outdoor radio nodes, mounted on utility poles or public buildings, include one or more radios that work like a traditional access point to connect to clients. But they also include one or more radios with special routing software that are dedicated solely to

### Wi-Fi city

**A diverse collection of cities and towns are experimenting with their own 802.11-based wireless LAN services, often to provide residents and businesses broadband access to the Internet.**

**Lompoc, Calif. (pop. 40,000):** Plans to offer fee-based wireless broadband service to residents in 2005.

**Grand Haven, Mich. (pop. 11,000):** Offers WLAN-based Internet access over a 6-square-mile area; currently beta-testing WLAN phones.

**Rio Rancho, N.M. (pop. 52,000):** Relunched a citywide WLAN project to cover 103 square miles via a contract with Ottawa Wireless.

**Granbury, Texas (pop. 6,000):** Deploying a Wi-Fi network via local ISP Frontier Broadband, covering roughly 10 square miles; mixed use network for public access and municipal applications.

**Washington, La. (pop. 1,000):** Installing wireless mesh over 2 square miles for police use, including two wireless IP cameras, and general Internet access; security via digital certificates.

**Los Angeles (pop. 3.6 million):** Mayor Jim Hahn announced creation of a special panel to report on feasibility of a citywide WLAN to extend wireless Internet access to all residents panel to report by April.

SOURCE: MUNIWIRELESS.COM

## Trends in Wireless LANs

high-bandwidth data backhaul.

The result is that nodes can be set up quickly, most of them without any backhaul cabling. Data traffic hops from one node to another, until it finally reaches a wired connection to a telco or service provider.

Not all municipal WLANs are intended for public access, or to replace or compete with broadband offerings from cable companies and service providers. Many are only for municipal employees: police, firefighters, building inspectors, meter readers.

But even in these cases, some officials are looking to extend them for residential and business Internet access.

The city of Hermosa Beach, Calif., launched its Strix-based network first for Internet access and then began adding municipal applications. Another Strix customer, Jersey Village, Texas, took the opposite approach: It installed the network first for employees and now plans to extend it to citizens.

Either approach is fine with Doug Chick, a network manager in the Orlando area for a healthcare company he asked not to name. He also runs thenetworkadministrator.com, a Web site for computer professionals. "Working within and managing an IT department is a 24/7 job, and I need 24/7 access to do my job," he says.

## DEPLOYING 802.11I FOR WIRELESS LAN SECURITY

■ By Kevin Fogarty

Vendors will tell you that upgrading from the interim security standard Wi-Fi Protected Access to the fully baked 802.11i protocol will be fairly simple, straightforward and worth the effort. But analysts and end users warn that there are lots of wrinkles to an 802.11i upgrade, including the fact that you might have to buy new hardware. After analyzing costs and other issues, some users have decided that WPA is good enough for now.

At the very least, moving to 802.11i means managing firmware upgrades on both access points and clients. That's if you have relatively new hardware. If not, you'll have to swap out your old gear for new access points that can handle Advanced Encryption Standard (AES) encryption.

Plus, you'll need to install authentication servers and certificate-authority servers (if you don't already have one in place), and add a whole new protocol to the networks. That's because 802.11i manages the encryption part of wireless LAN security, but you also need authentication, which means implementing 802.1X, another relatively new protocol.

"Anyone who tells you it's simple is not telling you the straight story," says Kenneth Dulaney, an analyst at Gartner. "You're adding two encryption methods and one authentication scheme. That's not simple."

WPA uses temporal key integration protocol (TKIP) encryption, while 802.11i uses AES. Because WPA is a subset of the fuller-featured 802.11i, WPA-enabled access points

usually can support both encryption methods.

"If you have first-generation access points, you've just inherited a doorstep," says Michael Disabato, networking service director at Burton Group. "That's not the worst thing in the world because there are numerous reasons you want the older stuff to go away if you can afford it. The receivers are better, they have better range. Lots of reasons."

What if you can't afford it? Cost is a major reason why the Boston Public Library is holding off on an 802.11i upgrade, according to Systems Officer Carolyn Coulter.

The library provides free wireless access in its public rooms for patrons and staff, so the network has to be pretty open. "We never know what kind of equipment the public is going to walk in with," Coulter says.

Coulter runs Cisco equipment on both wired and wireless networks, but uses a Bluesocket wireless gateway for access control and encryption, rather than WPA.

"We'd like to be as up-to-the-minute as we can with security. But finances are an issue because we're a public entity," she says. Coulter would like to migrate to 802.11i, or add it to her current security options; but without a pressing reason, she's one of a number of network managers who seem comfortable with their present levels of security.

For example, concrete and building-materials conglomerate RMC Group is in the middle of a migration to VoIP; is updating and standardizing its mail servers; and is updating its routers, switches and hubs, according to Dave Miller, project office manager at RMC in Atlanta.

"We'd like to stay as close as possible to the latest security protocols," he says. "We're using [Wired Equivalent Privacy], and we do have some security concerns, but we're focused on these other projects and we're undergo-

**"Anyone who tells you it's simple is not telling you the straight story," says Kenneth Dulaney, an analyst at Gartner. "You're adding two encryption methods and one authentication scheme. That's not simple."**

## Trends in Wireless LANs

ing an acquisition [by Cemex], so we're holding off a little for those reasons."

### 1. Alternatives to 802.11i

Other security approaches might be easier and more cost-effective, according to Chris Cerny, manager of enterprise networking at Community Health Network and the Indiana Heart Hospital in Indianapolis.

Rather than rely on WPA to supply encryption, every approved device has a VPN client that encrypts traffic, handles routing with a DHCP server, then authenticates the user's device and password to a Cisco authentication server.

"At the time we installed this, security wasn't a done deal for wireless, and apparently it's still not," Cerny says. "We figured, whatever the methodology of the day was, we already had a VPN concentrator, [access control list] and Cisco authenticator, and that all works very nicely. Of course, the doctors don't like it because they have to authenticate several times."

Cerny uses 802.11a access points wherever feasible, and uses 802.11b for VoIP phones; the 802.11b access points use a list that contains all the media access control addresses for every phone in the hospital system. "It's a very long list," Cerny says. "But if you're not on it, you don't get on the network."

The system leaves unregulated hot spots in lobbies and elsewhere, but because no unauthorized machines can access the internal network, Cerny's not concerned. "We don't really care if they use your bandwidth to get on the Internet; they can't get to anything inside our network," she says. "It's a very simple deployment; very few hands in the cookie jar."

The Boston Public Library uses a similar setup with a Bluesocket WLAN gateway for the Wi-Fi connections it offers within its main branch, Coulter says. The Bluesocket server handles encryption and access control using both WPA and IPsec encryption. The Bluesocket gear also handles role-based access lists that define access based on a user's role in the organization, broad-based policy management to let network managers reconfigure WLAN access more easily, and QoS. "We do make people download certificates, but otherwise we have to make it as easy for people as we can," Coulter says.

### 2. Look before you LEAP

Interoperability is a potential land mine for users. Dulaney says that while 802.11i encryption protocols are fairly standard, the authentication methods in 802.1X aren't. "The 802.1X spec is not hard and fast, there are interpretations to be made," he says, which means each vendor's version could be slightly different from every other's.

## Wireless by the numbers . . . and letters

**Wired Equivalent Privacy (WEP):** An encryption technique built into 802.11 wireless LANs using 40-bit keys.

**802.1X:** An authentication standard for LANs and WLANs, used to identify users before allowing their traffic onto the network.

**Wi-Fi Protected Access (WPA):** An industry standard based on a subset of an early draft of 802.11i. WPA replaces WEP's keying mechanism with a more robust system, called Temporal Key Integrity Protocol (TKIP). WPA adds a strong message-integrity check and allows for authentication using 802.1X.

**802.11i:** In addition to all the features in WPA, 802.11i uses Advanced Encryption Standard (AES) as a replacement for RC4 encryption.

**Advanced Encryption Standard (AES):** AES is the U.S. government standard encryption protocol that replaces Data Encryption Standard.

**Certificate authority:** Independent organizations that verify the identities of internal or external network security servers, and give those servers the ability to do the same for clients that connect to them, using encrypted certificates that are verified by the server every time the client logs on.

**Extensible Authentication Protocol (EAP):** An extension of Point-to-Point Protocol that supports many authentication methods, including Kerberos, public-key authentication and smart cards. In the IEEE's 802.1X, EAP is encapsulated in LAN or WLAN traffic, providing the mechanism for verifying the identity of a user to a RADIUS or other authentication server.

**Lightweight Extensible Authentication Protocol (LEAP):** a proprietary version of EAP that Cisco developed.

**Protected Extensible Authentication Protocol (PEAP):** a proprietary, extended-function version of EAP that Microsoft, Cisco and RSA Security developed.

**EAP-Transport Layer Security (EAP-TLS):** another Microsoft-created proprietary extension, but this one has been accepted by the IETF as a public standard.

**EAP-Tunneled Transport Layer Security (EAP-TTLS),** a proprietary protocol developed by Funk Software and Certicom; under consideration by IETF as a new standard.

**Temporal Key Integrity Protocol (TKIP):** an encryption protocol designed to provide more secure wireless encryption than WEP by making keys more difficult to crack. TKIP is the encryption mechanism for WPA, but is replaced by AES in 802.11i, which is also known as WPA2.

Trends in Wireless LANs

Most vendors use the Extensible Authentication Protocol (EAP) to communicate port-access requests between the client and the access point. But EAP packets only carry the requests; the protocol doesn't include descriptions of how to manage the authentication itself. For that, you have to pick one of several EAP implementations, including Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), any of which are acceptable under the 802.1X framework, but not all of which are interoperable.

Cisco developed Lightweight Extensible Authentication Protocol (LEAP). But testers showed that LEAP could be cracked by a simple dictionary attack, so Cisco is replacing it with a new EAP-FAST (Flexible Authentication via Secure Tunneling).

Yet another twist comes from Microsoft, which developed a Protected EAP (PEAP) with help from Cisco and RSA Security. Unlike EAP-FAST, in which both client and server are issued keys before any communication takes place, PEAP relies on certificates that have to be generated by an authentication server. Microsoft ships PEAP in some versions of Windows XP, providing certificates using its Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) or Cisco's Generic Token Card certificate.

Almost any kind of certificate is allowed under 802.1X as is any authentication protocol, according to Shripati Acharya, director of product management in the wireless networking business unit at Cisco.

The bottom line, according to Dulaney: "Even if you do see 802.11i certification on a product, you probably won't be able to make every product work with every other

product. You have to ask vendors what products they're certified for."

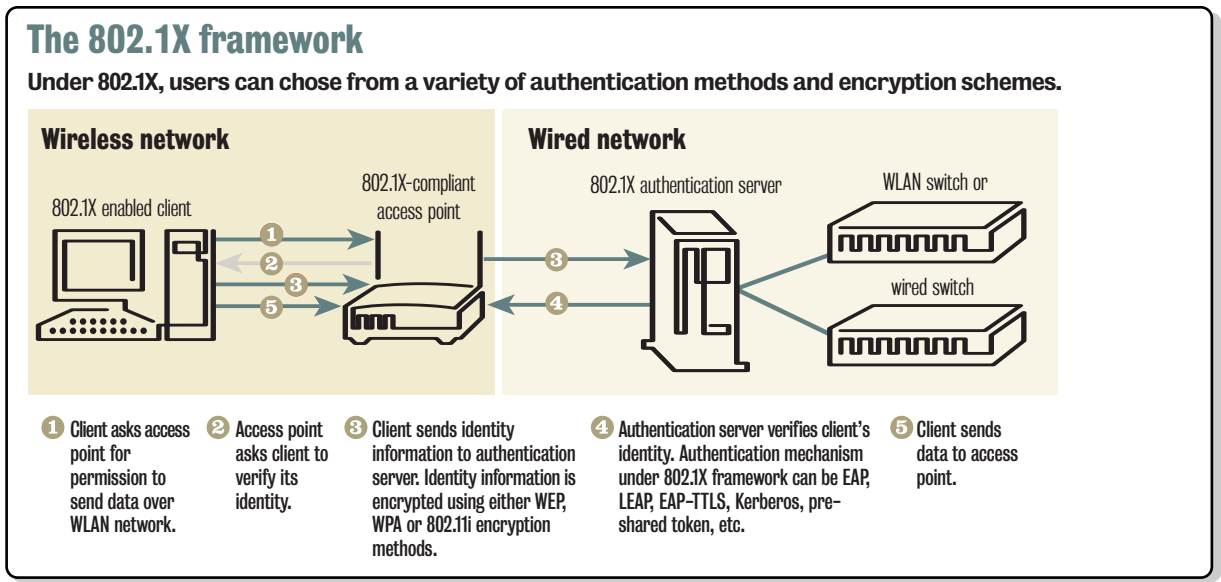
**3. Certification trepidation**

Finally, many end users shy away from using certificate-based systems of any kind, says Jeff Keenan, a principal at integrator Keenan Systems in Hartford, Conn. It's just too complicated to have a certificate server authenticated by an external authority so it can issue certificates, then keep the certificates on servers and mobile clients fully synchronized.

"I only work with two or three companies that have certificates, and at least one has a whole department to manage it. Other companies use RSA, hard tokens or other ways to get around issuing certificates," he says. "It's a big headache even once it's running."

But IT and security professionals realize that they could face even bigger headaches if they don't at some point upgrade to the most advanced wireless security standards.

Disabato says, "There's a lot of regulatory fear out there for people affected by [Health Insurance Portability and Accountability Act], Sarbanes-Oxley, Gramm-Leach Bliley. People are nervous. If you get caught on something under Sarbanes-Oxley, and you have WPA2 running, you can at least say you did the best you could with the technology that was available."



# Voice over Wi-Fi

## WLAN-BASED PHONES OFF TO A GOOD START

■ By Jeff Caruso

Are we all destined to own wireless LAN-based VoIP phones? It would seem that way from a recent study by Infonetics Research, which found that such handsets are already gaining acceptance.

Worldwide sales of WLAN VoIP handsets reached \$45 million last year, and 113,000 units were sold, the research firm says. Deployment of voice over WLANs is expected to steadily increase among enterprise firms through the next several years.

A brand-new segment of that market is dual-mode Wi-Fi/cellular handsets. Revenue in that area hit \$6.6 million last year for more than 8,000 units shipped. Infonetics notes that the latter handsets were only available in the last few

months of the year, so this number represents a strong start for a nascent market.

These dual-mode handsets are likely to become more common and prices are likely to come down, the firm says. The result will be that users will be able to roam across WLANs at home, at work and at public hot spots.

Infonetics says logistics and healthcare are the vertical markets where wireless VoIP handsets stand to gain the most ground early. But as VoIP expands across many more enterprises, wireless handsets are bound to follow.

Consumers could also gravitate toward VoIP over WLANs. Broadband service providers are looking to offer VoIP services and wireless access in a bundle with their broadband offerings.

Next up is wireless Internet calling. QoS issues, which have been discussed at length for years, will crop up - but Infonetics says that, despite those issues, adoption will start to pick up by the middle of next year.

## MOBILE VOIP SET TO ROAM EVEN WIDER

■ By Tim Greene

While mobile VoIP technology is finding a home in hospitals and manufacturing plants where workers need to stay connected as they roam, rollouts still require painstaking work, users say.

At San Antonio Community Hospital in Upland, Calif., VoIP is second on the list of applications being implemented over the facility's Wi-Fi network - right after bedside and operating-room computer access to patient records and X-rays, says Irv Hoff, the hospital's manager of converged networks.

True mobility and cost were major concerns Hoff had to overcome about Wi-Fi, but he is now convinced the technology meets his needs. Still to be worked out: details of deploying VoIP to avoid problems such as calls dropping between access points and barriers within buildings blocking calls. "We want the quality of the call to be equal to what you expect from a wired phone, given that we control the environment," Hoff says.

The problems are complex because VoIP over Wi-Fi combines the issues of wireless LANs (WLAN) with those of IP telephony. As WLANs for data become more and more accepted, so will VoIP over Wi-Fi, says Will Stofega, an analyst with IDC, but the potential problems with VoIP must be dealt with first. "If there is packet delay or loss, you hear it with VoIP," Stofega says. And as Wi-Fi VoIP phones proliferate, phone calls will boost the demand on wireless networks. "If you give people mobility on the LAN, you have

to increase the number of access points," he says.

Despite such issues, Wi-Fi networks are growing, with worldwide sales of wireless mobile network infrastructure gear projected to rise from about \$43 billion last year to \$49 billion by the end of 2008, according to IDC. As network executives get comfortable running data over these networks, they will increasingly add VoIP, Stofega says. At the moment, VoIP over Wi-Fi use is very limited. As the technology advances to make its use easier and to assure voice quality, that use will increase, he says.

Vendors selling access points and switches capable of supporting VoIP include Airespace (which is being bought by Cisco), Aruba Wireless Networks, Cisco, Siemens and Trapeze Networks. According to Siemens, the top users are hospitals, retail stores, manufacturers and warehouses.

### 4. Keys to deployment

For Hoff, the first step is making sure access points in the hospital cover every location an end user might go in the building. Then he has to make sure there are enough overlapping access points to support the likely load of simultaneous users without denying service to any of them. He is using Trapeze gear and a tool the company provides called RingMaster that maps buildings and the effective penetration of Wi-Fi frequencies through walls, floors, doors and windows.

This is a particularly big issue in hospitals, where renovations that change the configuration of walls are common, but also because some of these walls are shielded to block X-rays and are therefore unfriendly to Wi-Fi transmissions, as well. "We do a lot of remodeling - new partitions, new

## Voice over WiFi

offices," Hoff says. It's an ongoing process, so as the hospital makes changes it records them in RingMaster, which identifies new blind spots. Then access points are reconfigured to get around them.

Load balancing among access points is key to efficient distribution of calls, vendors say. Airespace access points, for one, distribute users evenly in environments where they might be within range of several devices at the same time. Without this feature, user gear would vie for entry to the access point with the strongest signal. Siemens says its next round of devices will include this feature.

Assuming there are enough access points to guarantee coverage, network executives have to ensure fast handoffs between devices as callers walk in and out of range of different sites. The switchover has to take less than 50 milliseconds or callers can hear it - this means careful network design is essential. For instance, with voice and data running on the same network, the handoffs can take from a half second to 10 seconds, with the presence or absence of data on the network affecting the time unpredictably, according to Network World Clear Choice testing.

Beyond network performance, any use of VoIP over Wi-Fi should include an evaluation of voice quality. "Do you want to be on a call with a client and barely be able to hear?" Stofega says.

### 5. Future roaming outside

While roaming within a building might be good enough for staff inside a hospital, salespeople that roam the country also can benefit from wireless VoIP phones and save customers money, says Keith Waryas, an analyst with IDC.

Using VoIP wireless phones or even VoIP softphone software on a wireless PC can turn public hot spots into havens where users can avoid dipping into cellular minutes where expensive residential rates might apply, according to Waryas.

"Most business users are getting reimbursed by their companies for use of their personal cell phones," he says. So a company would issue a VoIP wireless phone to roving users and receive fewer expense reports for cell phone reimbursement.

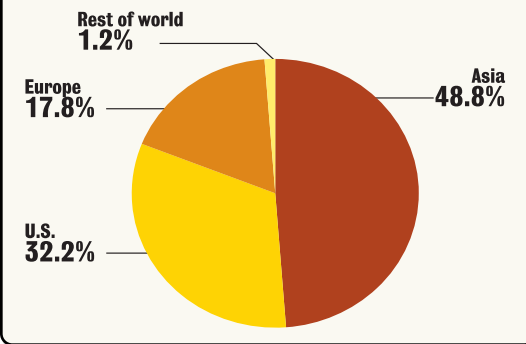
A key limiting factor that remains is the number of public hot spots available, although the number is growing rapidly.

Even when there are enough, corporations would have no control over the design and management of public hot-spot networks, so quality could suffer. Also, users would have to carry around two phones apiece - one for Wi-Fi, the other for cellular if they want to stay in range all the time. Apparently, though, service providers think enough customers will want these Wi-Fi phones to support new services. VoIP service provider Vonage recently announced a service supporting Wi-Fi phones. And Net2Phone is about to market a similar service in the U.S. after initiating it in Canada.

Motorola, in conjunction with partners, is field testing the first dual-mode wireless phones, access points and PBXs that let users make or receive calls on corporate Wi-Fi networks

### What's hot?

By the end of 2007, there will be a total of about 182,000 hot spots worldwide, making use of VoIP wireless phones by mobile workers more likely. The U.S. will have 60,600 of these, according to IDC.



and continue them on GSM networks as they move out of Wi-Fi range.

So a doctor starting a phone conversation in the hospital via Wi-Fi could walk out of the building, get in a car and drive away but continue the call because the network flipped it over to a cellular network.

Systems involving Motorola hybrid phones require use of Avaya PBXs and Proxim access points to coordinate the handoff of calls, and are touted as a way for businesses to save on cellular costs. Businesses would buy the phones and set up corporate cellular accounts, which would let them negotiate lower cellular rates than their employees would individually.

The phones can only tap into specific Wi-Fi networks that must include Motorola presence servers that keep track of where users are.

Service providers could offer a managed service based on this technology. Waryas says he expects at least one major U.S. carrier to announce one by summer. This could give users seamless transition from cellular to Wi-Fi at public hot spots.

One hospital telecom manager, who would speak only if he was not identified, is considering the technology and had a concern about billing. He says he'd want to know how the network decides which mode to use and whether there would be a fee for calls received on the Wi-Fi network.

Advocates of this type of service say businesses will be able to negotiate good cellular deals because they will need large buckets of calling minutes. Waryas says he thinks such services will allow for setting up least-cost routing to keep the cost down.

If billing isn't a problem, these dual-mode services could relieve some of the Wi-Fi coverage issues within buildings, Waryas adds. If a user wandered into a dead spot within a building, the call would continue as a cell call rather than drop, he says.

## Voice over WiFi

**WHEN WI-FI MEETS CELLULAR**

■ By Jeff Vance

Wouldn't it be nice if you had a dual-mode phone that let you talk via voice over Wi-Fi when you're in the office, warehouse or hospital, and then seamlessly switched over to cellular when you were outside the coverage area of your wireless LAN.

That's the promise of new converged or hybrid services that will become available sooner than you think. The benefits are increased mobility, productivity and convenience, not to mention some cost savings.

Of course, there are trade-offs. This hybrid service means replacing a public switched telephone network (PSTN) service with a VoIP service running over a broadband Internet connection.

Compared with VoIP, reliability and call quality are both superior on the PSTN, while the calls are fairly inexpensive. Moreover, indoor coverage can be spotty, making many users wary of abandoning that fixed-line phone altogether.

And without a reliable system for LAN to WAN handoffs, many calls initiated on the cellular network will remain on that network for the call's duration, regardless of whether there is a better WLAN signal available.

The question for the IT executive is whether it's in the company's best interest to trade away some degree of reliability and call quality for cost savings and mobility. For now, it's a tough call, but as VoIP becomes more reliable and as the bridging technology between these networks becomes more sophisticated, the scales will tip in favor of converged services.

**The future isn't that far away**

Although most carriers have shown interest in fixed-mobile convergence, one carrier actually has begun deployments.

T-Mobile offers the dual-mode iPaq H6315, which lets users switch between GSM/General Packet Radio Service (GPRS) and Wi-Fi networks as they travel. "The device automatically notifies you as you enter a Wi-Fi hot spot and switches to the fastest network available, allowing you to maintain your Internet session as you travel from your home, to Starbucks, to the airport, to a business meeting and to your hotel," says Todd Achilles, director of handset product management at T-Mobile.

According to Achilles, the current GSM/GPRS network provides wide-area coverage for applications to which customers want constant access, such as e-mail and calendar, while users can turn to broadband hot spots when they

need to access larger data files.

On an even more ambitious scale, Avaya recently teamed with Motorola and Proxim to develop a fixed-mobile offering targeted at corporations. All you need is a dual-mode phone from Motorola, Session Initiation Protocol (SIP)-enabled IP telephony software from Avaya, and a voice-enabled WLAN infrastructure from Proxim. Trials are underway.

Within the enterprise, Motorola's dual-mode phone connects with a Proxim WLAN access point and functions as a VoIP phone. As a user moves out of the office, the phone acts as a GSM cell phone. A wireless gateway jointly developed by Proxim and Avaya manages the handoff between the two networks, while Avaya's SIP-based IP telephony software pushes features commonly associated with desk phones, such as conferencing, out to the mobile handset. The handset also can access data applications on both networks.

According to Frank Lovasco, mobility solutions practice leader at Avaya, cost savings will exist, but cost won't be the biggest draw initially. "In terms of what will motivate an enterprise to make this switch, you have to think in terms of business continuity," he says.

Early adopters will be high-value users such as executives, doctors, lawyers and salespeople. Saving airtime minutes isn't a big deal to them - they already buy big buckets of minutes - but having a single point of contact is a big deal. Added to that is a converged service that pushes important features such as conference calling from the

desk to the mobile phone, meaning that these users are more productive when on the move.

The new service "allows you to access all of your important applications, be they voice or data, from a single device," he says, noting that Avaya's SIP-based software adds features such as presence while simplifying a user's life beyond just the subtraction of devices. "You now have one point of contact, one phone number where you can be reached all of the time, as well as a single voice mail box," he says.

**The seams are still visible**

These two early offerings still have some wrinkles to be worked out.

As of now, billing is not centralized. Users still would pay a carrier for the cellular plan, while the VoIP calls within the company would be rolled in with the corporation's telephony plan.

Also, these services don't shield users from the underlying networks. In other words, while T-Mobile's service informs you when a new network is available, you must fin-

**"You now have one point of contact, one phone number where you can be reached all of the time, as well as a single voice mail box," he says.**

## Voice over WiFi

ish your session and reconnect with the new network. With the Avaya/Proxim/Motorola offerings, the corporate network is the only network where you get guaranteed Wi-Fi connectivity. Currently, the solution does not integrate hot-spot access.

For fixed-mobile convergence to really fly, it needs is the seamless handoff between various Wi-Fi networks and cellular networks, with users maintaining their sessions and with the underlying networks essentially invisible to them.

"There is still a lot of work to be done to improve the handoff capabilities," says Phil Solis, a senior analyst at ABI Research. Unlicensed Mobile Access (UMA) "could help, but in the end what networks you can roam to might be determined by your carrier and the bundle you sign up for."

UMA technology is a set of specifications for linking cellular networks and unlicensed spectrums such as 802.11 and Bluetooth.

**Start-ups push middleware products**

A number of start-ups have emerged to tackle the issues involved with linking these divergent networks. BridgePort Networks, Kineto Wireless, IBiS Telecom and LongBoard all intend to bring products to market that enable fixed-mobile convergence.

These products reside in the core of the carrier network, and bridge mobile and IP networks. To link networks, these products typically use a roaming technology that extends a user's mobile-phone identity over an IP network, translating from Signaling System 7 on one end to SIP on the other. All the products are designed to extend a user's mobile identity to IP networks, so a user's phone number and session remain the same, regardless of location. These start-ups also focus on additional features, such as session persistence and single sign-on authentication.

Executives at BridgePort emphasize the benefits of a single subscriber identity. "Today's highly mobile professional has several different points of contact, a desk phone, a mobile phone and maybe a couple of e-mail addresses," says Sanjay Jhawar, BridgePort's senior vice president of marketing and business development. "With fixed-mobile convergence, not only do you converge the networks, but you also converge the points of contact for the individuals you serve. In certain verticals, such as healthcare, this is a very valuable service.

"A fixed-mobile solution also needs to extend services from one network to the other, such as enabling [Short Messaging Service] on Wi-Fi," says Steven Shaw, director of marketing for Kineto Wireless. "Users need to have the same access to applications and the same user features as they had before, or they won't be satisfied."

However, the bridging technology is only one piece of the puzzle. Another must-have is the dual-mode handset that switches seamlessly between networks. "For broad

handset support, the industry first needed an appropriate standard for fixed-mobile convergence," Shaw says.

This is where UMA comes in. It will be part of Release 6 of 3rd Generation Partnership Program, and as a result handset manufacturers now have specifications to build to. On the heels of these developments, ABI Research predicts that there will be more than 50 million dual-mode handsets worldwide by the end of 2009.

**What's the benefit to IT?**

The most immediate benefit to an IT staff will be cost. However, quantifying actual cost savings is something that carriers, vendors and even analysts seem reluctant to do. Although, the basic logic goes something like this: A large number of mobile calls placed within the corporation are actually intra-enterprise calls. With a converged service, those calls would be free. Mobile calls placed within a corporation but going to the outside world also would be less expensive going over the Internet than over the cellular network.

"Already you have large enterprises playing hardball with carriers," BridgePort's Jhawar says. "Certain large enterprises are telling the telcos that they will no longer pay for on-campus-to-on-campus calls." If this is true, it means that convergence ultimately will benefit the carrier - which in essence is able to extend its network without adding capacity.

"Basically, increased mobility equals increased productivity," Kineto's Shaw says. "The user experience of data applications on phones is also greatly improved when you have broadband."

"A converged solution is a more secure solution," Avaya's Lovasco says. "With convergence, enterprises are able to regain control of their mobile user base."

**When will we see converged services?**

That depends on what you mean by "converged." T-Mobile provides a dual-mode service, although it lacks session persistence. BridgePort and Kineto have both been in trials with carriers - BridgePort with Bell Canada and Kineto with AT&T Wireless. The Avaya/Proxim/Motorola offering is due out soon.

As for carrier offerings, timetables are still up in the air. "Actually, the cable operators may be the first movers in this space," Jhawar says. "Many are looking to partner with [mobile virtual network operators], as evidenced by the recent announcement between EarthLink Wireless and SK Telecom. Convergence is perfect for [mobile virtual network operators]. They're not responsible for maintaining networks, so they are freer to focus on convergence and the benefits that come with it."

*Vance is a freelance technology writer and president of Sandstorm Media ([www.sandstormmedia.net](http://www.sandstormmedia.net)). He can be reached at [jeff@sandstormmedia.net](mailto:jeff@sandstormmedia.net).*

# Wireless LAN product Testing

## VOICE OVER WIRELESS LAN

■ By David Newman

VoIP should be an easy fit for wireless LANs, but mixing the two technologies today is difficult. Despite VoIP's low-bandwidth profile, even a small amount of data traffic on the same network can lead to seriously degraded audio quality and dropped calls, even with QoS features enabled.

That's the major conclusion of our first-ever assessment of VoIP capability in WLAN systems. Over the course of three months we tested WLAN switches and access points from Aruba Wireless Networks, Chantry Networks (now Siemens), Cisco and Colubris Networks in terms of audio quality, QoS enforcement, roaming capabilities, and system features. Other vendors, including Airespace, Meru Networks and Trapeze Networks, declined to participate.

Among our major findings:

- With QoS enforcement enabled, the products delivered near-toll-quality audio, provided only voice traffic is active. This is fine as long as the wireless network carries voice traffic only, but that's not likely as companies move toward converged voice-data networks.

- When voice traffic had to contend for bandwidth (even with a little data traffic), dropped calls were common and audio quality on the remaining calls was poor in many cases - and this was with QoS enforcement enabled.

- With data traffic present, roaming from one access point to another took anywhere from 0.5 to 10 seconds - in cases where roaming succeeded at all. These long delays and dropped calls made roaming practically impossible with some vendors' gear.

While some products struggled mightily in our tests, Aruba's A2400 and A800 switches and A61 access points were consistently strong performers. The Aruba products posted generally excellent numbers, regardless of how much voice or data traffic was thrown at them. Aruba's gear just

worked, earning it the Clear Choice Award.

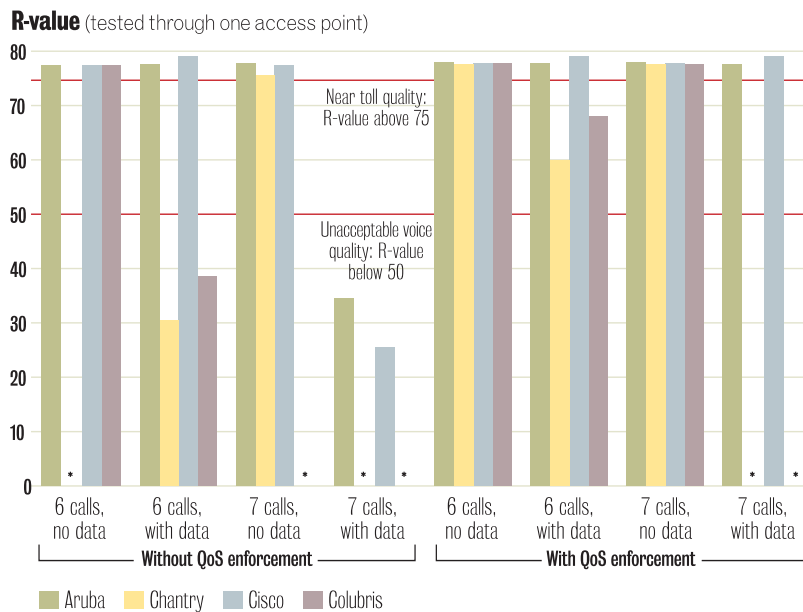
Two issues confounded other vendors. First, when handling voice and data traffic on the same network, vendors need to pay attention to metrics such as delay and jitter rather than forwarding rates.

Many vendors are only just beginning to tune their products for voice/data convergence, even though some have touted that capability for 18 months or more. However, it's still relatively early days for VoIP over WLANs. Test tools that accurately measure these metrics on WLANs (such as the VeriWave instruments we used) are only just beginning to appear, and this test is among the first to measure audio quality, delay and jitter in a methodical way.

Second, the emerging 802.11e standard for QoS on WLANs might bring some relief. The 802.11e specification wasn't yet ratified when we began this project, so by definition all QoS methods were nonstandard.

### Voice quality with and without QoS

Tests with six and seven concurrent calls make clear why QoS enforcement is a must when handling VoIP traffic on WLANs. Even with QoS enabled, audio quality (R-value) suffered when VoIP traffic had to share bandwidth with data traffic.



All systems also delivered R-values around 78 for a single call, but because all systems also put up comparable scores for one call even without QoS, we omitted the single-call comparison here.

\* N/A: Calls dropped, could not measure R-value.

## Wireless LAN Product Testing

**R-value ratings**

An ITU specification that determines call quality, R-value measures packet loss, jitter and delay.

R-value	Mean opinion score	User satisfaction
90 or higher	4.34 or higher	All users very satisfied
80 or higher	4.03 or higher	All users satisfied
70 or higher	3.60 or higher	Some users dissatisfied
60 or higher	3.10 or higher	Many users dissatisfied
50 or higher	2.58 or higher	Nearly all users dissatisfied

Companies might want to wait until the new 802.11e specification and products based on it are more mature and fully tested.

**Measuring voice quality over wireless**

Our tests sought to answer a simple question: How does a VoIP over WLAN system sound?

To find out, we worked with VeriWave, a start-up that makes WLAN test and measurement equipment. VeriWave developed a new application, the VoIP over WLAN Analysis Test Suite, especially for our test.

In addition to collecting delay and jitter statistics, VeriWave's test suite and TestPoint hardware let us measure R-value, an ITU specification (G.107) for determining call quality. R-value is an objective measurement, computed directly from measurements of packet loss, jitter and delay. While R-value is objective, it has a strong correlation to the subjective Mean opinion score method in ITU standard P80 (see R-value ratings).

We measured voice call quality with up to 14 handsets and an H.323 call server from SpectraLink, a maker of 802.11 handsets. We measured audio quality with up to seven concurrent calls, and in some events configured the VeriWave TestPoint boxes to offer background data. For each system tested, we checked call quality with QoS disabled, then enabled.

**Audio quality without QoS**

With QoS disabled, we started by routing all calls through one access point. Because all the vendors recommend enabling QoS for voice traffic, this baseline test gave us a "before" picture to demonstrate the need for voice traffic prioritization.

With QoS turned off, all four systems tested did fine with only a single call active, with R-values hovering around 78. That is about as good as it gets with VoIP over wireless. The threshold for near-toll-quality voice is generally considered to be around 75, meaning the systems delivered good audio quality for a single call.

Performance for all systems changed across the board when we placed six or seven calls through a single access point and switch, especially when data traffic was active. Yet even without background data, we could not test the

Colubris system with seven calls active and QoS disabled - all the calls dropped.

When we configured the TestPoints to offer background data (a stream of User Datagram Protocol [UDP] packets at 1M bit/sec), the results were positively awful without QoS. With only six concurrent calls, R-values for all systems (except Aruba) were generally at or below the point where voice signals were unintelligible or calls were dropped. Sound quality through Aruba's system

remained high, roughly the same as with no data, even without QoS.

The Chantry and Colubris systems could not perform the background data test with seven calls (QoS disabled). All calls failed as soon as the VeriWave box began offering background data.

All vendors recommend the use of QoS mechanisms for handling voice traffic, even when no data traffic exists. QoS is a must when handling VoIP traffic over a WLAN.

**Adding QoS to the mix**

We reran the same five test configurations as in the non-QoS cases: We measured one call with no background data, and six and seven calls with and without the 1M bit/sec background UDP traffic.

We expected much-improved results once we enabled QoS, but only Aruba's system put up consistently excellent results in all the tests with QoS enforcement. Even in the most stressful case (seven calls plus background data), the Aruba system delivered near-toll-quality. With QoS enabled on the Aruba equipment, there was little difference between the least and most stressful test scenarios.

Other vendors' QoS mechanisms did little to protect call quality when background data was present. On the plus side, QoS mechanisms generally did an excellent job when only voice traffic was present.

Audio quality improved for all systems in cases where we used only voice traffic. In tests with six and seven calls (no background data), all systems delivered near-toll-quality results with QoS enabled.

That changed when we added the background data. With six calls and data active, R-values fell below 70 for the Colubris CN1250, meaning that "some users [would be] dissatisfied" according to the ITU R-value specification. The R-value was about 60 for the Chantry switch ("many users dissatisfied").

Beyond the objective R-value scores, we did some subjective spot-checking of call quality when data was present. Sure enough, we heard echoes, dropouts and generally poor voice quality whenever the TestPoints offered a datastream.

Things got worse for Chantry, Cisco and Colubris when

Wireless LAN Product Testing

we tried seven calls plus data. Chantry's BeaconMaster couldn't handle this test case; all seven calls failed when we added data. Cisco's WLSM posted an R-value of about 50, the bare minimum level at which calls are intelligible. Further, three of seven calls dropped during this test on Cisco's gear. The Colubris CN1250 completed the test, but didn't forward enough voice frames for the test equipment to compute an R-value score. R-value scores for this test were only computed for the calls that remained active during the 30-second test (so in Cisco's case, it was on four calls instead of seven).

SpectraLink generally recommends a maximum of six concurrent calls per access point, not the seven we used in our tests. Thus, vendors might complain that our seven-call scenario was an overload test case. That is valid, but only up to a point. First, the Chantry and Colubris systems had trouble even with the recommended maximum of six calls with data. Second, Aruba's system could handle the seven calls with data scenario. Third, our most stressful test came nowhere near overloading the wireless medium. We offered 3M bit/sec of traffic or less in all tests, including voice and data. That's not even near the amount needed to saturate the wireless channel (see story on wireless architecture remaining diverse).

It's possible to run each access point with seven calls and data, provided the system is designed for it. But doing so requires careful attention to timing (see story).

**Delay and jitter measurements**

Delay and jitter are critical metrics for any application, but are especially important when dealing with voice or video. When delay or jitter rises to 50 to 70 millisecond, voice quality starts to degrade (see graphic). With six calls and background data, the average delay measured below 50 millisecond for all vendors, but maximum delay and jitter shot up to much higher levels, topping out at more than 250 millisecond in tests of Cisco (six calls) and Colubris gear (seven calls).

An analysis of the logs produced by the TestPoints found several reasons for the voice quality degradation. Anytime jitter exceeds 60 millisecond, audio quality begins to suffer. As the maximum delay and jitter numbers rose, R-

values fell - and that's for the calls that survived the 30-second test. When delay and jitter rose too high, the calls simply dropped.

**Doubling the access points**

So would throwing more access points at the problem help? We re-ran all our tests on two access points, with half the phones associated to each access point.

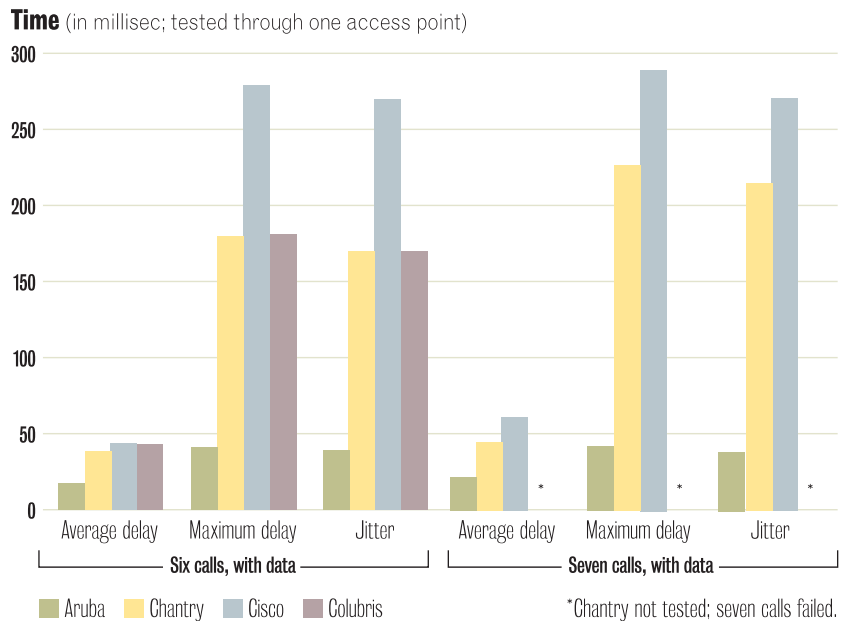
With two access points, the R-values were generally much higher. That wasn't surprising, considering each access point does half the work as in the first set of tests. Average delay also increased, which was expected given the additional component in the traffic path.

While this suggests performance can improve with more access points, it also raises several concerns. Cost goes up, even with thin access points. Second, wireless spectrum is limited, and depending on placement, too many access points will interfere with one another. Third, performance still was not perfect with two access points; we had some dropped calls in the presence of background data.

With a mobile workforce you can't predict how many users will try to associate with a given access point at a

**Delay and jitter with QoS**

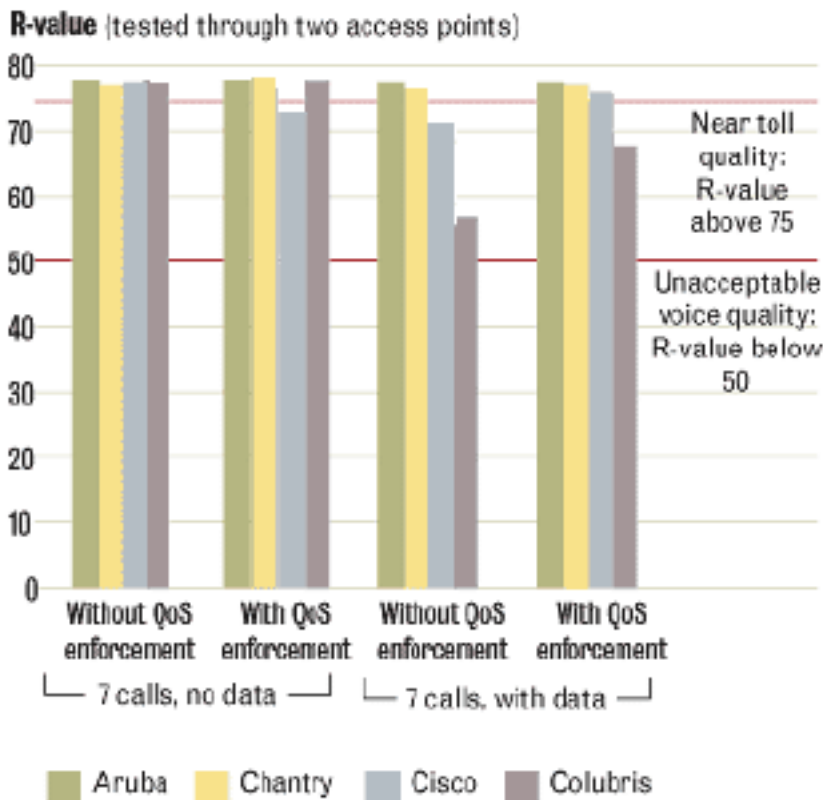
**Delay and jitter are the critical metrics for VoIP traffic. While all systems kept average delay relatively low, the big spikes in maximum delay and jitter translated directly into poor voice quality or even dropped calls.**



Wireless LAN Product Testing

**Voice quality through two access points**

Audio quality improved dramatically when we routed calls through two access points. That's hardly surprising, given that each access point does only half the work of the single-access-point test case. However, adding access points to improve voice quality isn't always economically or technically feasible.



given time. Every access point has a saturation point, and our results suggest that point is relatively low when voice is added.

**Roam if you dare**

Mobility for voice is a major driver for a WLAN deployment. Just as cellular phone users move from one coverage area to another, so too will WLAN handset users.

We measured the time needed for a call to migrate from one access point to another, with both access points attached to the same switch. We also tracked R-value, delay and jitter.

To force the handsets to roam, we powered off the first access point. This drew objections from two vendors -

Chantry and Colubris. Chantry says its roaming capabilities are designed for the case where a user physically moves from one location to another, not when there's a power loss to a given access point.

While it is desirable to test roaming under this condition, we could not put enough space between access points in our 1,200-square-foot lab for this approach to be practical. We considered using the VeriWave TestPoint as a noise generator, but rejected that option because it was no more representative of physical mobility than the power-off test. Also, loss of power is a real (if uncommon) occurrence; if the access point goes away for whatever reason, a WLAN system needs to seamlessly migrate associated users to a nearby alternative.

The Colubris CN1250 could not be tested by turning it off. The vendor handles mobility through Mobile IP, which requires a home agent - the station where a client first learns its IP credentials - to remain active. If the access point that hosts the home agent goes down, so does the ability to roam. Cisco also supports Mobile IP, but did not use that technology in our tests.

Instead of pulling the plug on the CN1250, we tested roaming by disabling the radio on the first access point. This had the same effect of forcing the clients to roam.

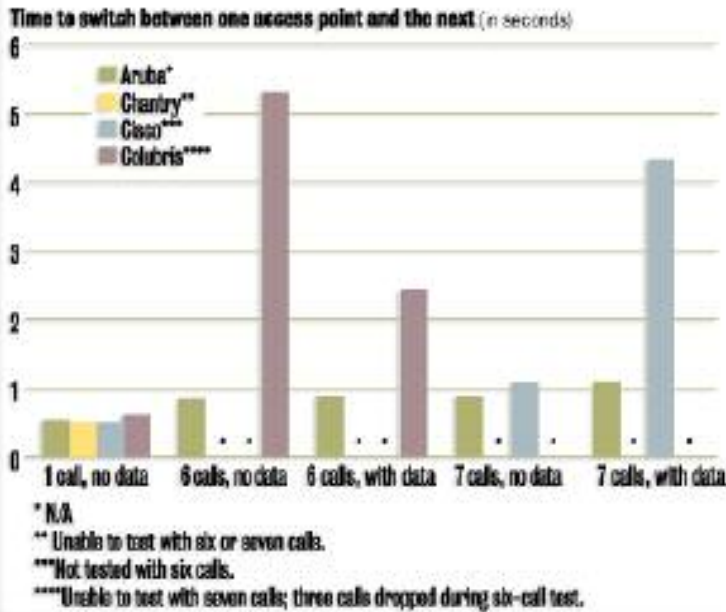
Colubris also requires a third access point to function as a foreign agent, which relays information about clients that roamed back to the home agent. For this purpose, we used a third Colubris CN1250 with its antennas removed; there is no requirement that the foreign agent needs wireless connectivity.

As before, we measured roaming in configurations involving one, six and seven calls, with and without our background data. Cisco has bragging rights in the single-call case, with a roaming time of 0.433 seconds, and all systems roamed one call in about 0.5 seconds (see graphic). A half-second gap is noticeable to the human ear - as is any gap of around 70 millisc or more - but except for this dropout audio quality was generally high.

Wireless LAN Product Testing

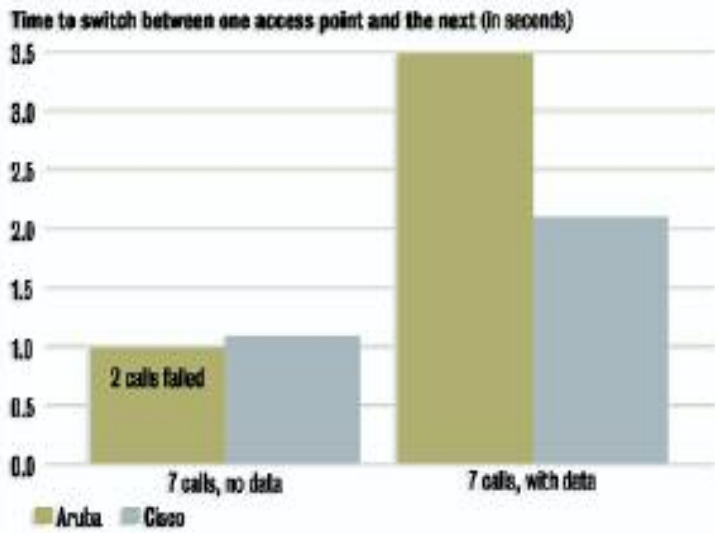
**Local roaming with QoS**

Ideally, roaming time should remain the same regardless of the number of calls or the presence of background data. No system met that ideal; increased roaming times and dropped calls were common.



**Remote roaming with QoS**

A key challenge for WLAN switches that manage remote access points is to deliver roaming times roughly comparable to those for locally attached access points.



Aruba excelled in the roaming tests. Its average handoff times ranged from about a half-second for one call, to just more than 1 second for the seven-calls-with-data scenario. While that kind of delay will be noticeable to callers, it was still by far the fastest roaming performance of any product.

In Cisco's case, we could perform seven-call roaming tests, but not six-call tests because of time constraints. Average roaming times doubled from 0.433 seconds with one call, up to 1.053 seconds with seven calls - and then it leapt to 4.324 seconds with seven calls and background data.

Colubris could roam with six calls, but not seven. In the seven-call case, we could not prevent some phones from "pre-roaming" to the second access point before our test, which invalidated the results. We also had similar issues in testing with six calls, but the handsets stayed associated long enough for us to record the results, with and without background data. Even so, the results are counterintuitive - roaming took an average of more than 5 seconds without data, vs. about 2 seconds with data.

Chantry's BeaconMaster couldn't perform the roaming test with six or seven calls, even without background data present. Calls would drop rather than roam in those configurations. In troubleshooting the problem, we reduced the number of calls to see if it was a load problem. It was: In our power-off scenario, the highest number of calls that could roam through the BeaconMaster was only two. Two-call roaming times were similar to the one-call case, but we're not presenting those numbers because of the much-lower call count than the other vendors.

VeriWave's new test gear helped us contrast roaming at the 802.11 link layer and at the application layer, and the results were startling. In many cases, delays of even a few dozen milliseconds in link-layer 802.11 roaming led to delays of 10 seconds or longer at the application layer. Even vendors' engineers were surprised at the enormous disconnect between Layer 2 and Layer 7 measurements. The fact that even minor issues at the link layer had a major effect at the application layer underscores the need for well-behaved 802.11 implementations.

Wireless LAN Product Testing

Remote roaming

Because WLAN switches can manage access points at remote locations, we wanted to know whether roaming times and call quality would be affected if the access points are in different locations than the switch. For example, would roaming times differ if the WLAN switch was in Boston and a user roamed between two access points in Los Angeles?

We re-ran the roaming tests, this time using an AX/4000 traffic generator/analyzer from Spirent Communications to inject a 100-millisecond, round-trip delay. This is roughly the delay that traffic would experience going between Boston and Los Angeles.

We completed this test with only Aruba and Cisco. Chantry's BeaconMaster couldn't sustain six or seven concurrent calls. Colubris consists of an access point but no switch, ruling out remote roaming tests. For remote roaming, we tested with seven calls (time constraints prevented us from testing Cisco's gear with six calls).

Without data, local and remote roaming times were essentially identical for both vendors (see graphic). With data present, Aruba's roaming times rose from about 1 second in the local case, to about 3.5 seconds in the remote scenario. Cisco's remote roaming time was actually lower than the local test, which is counterintuitive. We cannot explain this result, but at least it validates Cisco's claim that access points can "pre-authenticate" clients, resulting in no performance penalty for remote access points.

So what now?

It's possible that products supporting 802.11e QoS will do better at prioritizing traffic than our results indicated. All the vendors said it was early in the evolution of VoIP over wireless, and our test results show there is certainly room for improvement. For network managers looking to deploy VoIP on WLANs in the near future, there are three choices: make very few calls; don't ever send data; or look for equipment - such as Aruba's - that handles time-sensitive traffic in a timely way.

Acknowledgements

Network World gratefully thanks VeriWave for its support on this test. The company supplied its TestPoint instruments and developed the VoIP over WLAN Analysis Test Suite especially for this project. Further, company CTO Tom Alexander spent many weeks camped out in the Network Test lab while we ran these benchmarks. Thanks also to SpectraLink, which supplied WLAN handsets and its SVP Server call server; and to Spirent Communications, which supplied an AX/4000 analyzer with Genie impairment software for use in the remote roaming tests.

Net Results

Aruba A2400, A800 switches, A61 access point

OVERALL RATING  
**4.58**

Company: Aruba Networks. Cost: \$8,780 as tested. Pros: Outstanding voice prioritization capabilities; rich set of QoS and radio frequency management features. Con: Some call drops in most stressful test case.



Cisco WLSM

OVERALL RATING  
**3.53**

Company: Cisco. Cost: \$51,978 as tested. Pros: Highly scalable, rich set of routing and switching functions. Cons: Doesn't protect voice traffic under most stressful test case; doesn't dynamically adjust to changes in radio frequency environment; pricey.

Colubris CN1250

OVERALL RATING  
**3.0**

Company: Colubris Networks. Cost: \$1,800 as tested; access point, \$500. Pro: Powerful and intuitive user interface. Con: Limited prioritization of voice traffic.

Chantry BeaconMaster

OVERALL RATING  
**2.4**

Company: Chantry Networks (recently purchased by Siemens). Cost: \$9,180 as tested. Pro: Supports Open Shortest Path First routing. Cons: Dropped calls in six- and seven-call cases; poor voice quality in the presence of data; no contingency for the loss of power.

The breakdown

	Aruba	Cisco	Colubris	Chantry
QoS enforcement for VoIP traffic 25%	5	5	5	5
QoS enforcement for VoIP and data traffic 25%	4.5	1.5	1	1
Roaming 20%	4	4	2	1
Features 20%	5	4.5	3	2
Price 10%	4	2	5	3
<b>TOTAL SCORE</b>	<b>4.58</b>	<b>3.53</b>	<b>3.0</b>	<b>2.4</b>

Scoring Key: 5: Exceptional; 4: Very good; 3: Average; 2: Below average; 1: Consistently subpar

## Wireless LAN Product Testing

### QoS ENFORCEMENT: WHAT HAPPENED?

■ By David Newman

Three of four vendors in this test failed to protect voice traffic in the presence of data, even using QoS mechanisms specifically intended to do so. Why did these QoS mechanisms fail, even with the vendors' best experts configuring them?

There are a number of factors that might explain our results.

Timing is everything. The importance of keeping delay and jitter low can't be overemphasized when it comes to voice traffic. Some QoS mechanisms work in terms of bandwidth and frame loss; if a given traffic class consumes more than a set amount of bandwidth, packets belonging to that class get dropped. That's not sufficient for voice. Even "strict priority" mechanisms, which always service a given traffic class first regardless of the consequences for other classes, only work properly if they receive high-priority packets in the first place. That's not so easy to do with 802.11 traffic. The IEEE protocols involve large amounts of management traffic and also require that every data frame

be acknowledged. At the same time, the SpectraLink phones send out one frame about every 30 millisecond and seem to falter anytime four or five packets in a row are dropped. These twin constraints make it critical that wireless LAN (WLAN) systems nail down the timely delivery of as much traffic as possible. In our tests, only the Aruba system did that.

It's not about the bandwidth. At most, we threw less than 3M bit/sec of traffic at each system - and that includes both voice and data. Given that four vendors cracked the 6M bit/sec mark in last year's tests, the initial suspicions of some vendors that we simply overloaded the systems with data doesn't hold up. This test emphasized timely servicing of high-priority traffic, not high data rates.

Access points aren't hot rods. The typical "thin access point" consists of a relatively modest CPU, a limited amount of RAM and firmware. By itself, those components aren't enough to ensure timely traffic delivery. Instead, vendors must rely on precise scheduling mechanisms in their switches (as Aruba does); reduce the number of concurrent calls (which improves performance, as we will discuss in covering tests with two access points); or deploy voice-only WLANs and don't allow data clients (not a practical alternative for most corporations).

## Wireless LAN Product Testing

**WIRELESS ARCHITECTURES  
REMAIN DIVERSE**

■ By Jim Geier

Although wireless LAN systems with voice support have been available for nearly two years, this is still an emerging market. As in our previous test of WLAN switches, there are huge differences in architectures and features.

The Aruba, Chantry and Cisco products are "wireless LAN switches." User authentication and spectrum management decisions are made by a wired Ethernet switch (the brains, handling user authentication and radio frequency management), not the access points. The switch not only controls access to the wired network, but also dynamically adjusts wireless radio signal strength in response to changes in the RF environment.

Cisco's Wireless LAN Services Module (WLSM) blade for the Catalyst 6500 switch is essentially a WLAN switch within a switch. It offers the same access control as the Aruba and Chantry devices, plus switching, routing, security and content management functions from other Catalyst blades. Not surprising, the WLSM is also stronger on IP routing support than the other entrants. While Chantry supports Open Shortest Path First and Colubris supports Routing Information Protocol, the Cisco offering supports virtually every major routing protocol available.

The Colubris CN1250 is a stand-alone access point with VPN features. Multiple CN1250s can be monitored and configured through the vendor's management software (not supplied for our test; instead, we configured each access point through its Web user interface). Colubris relies on third-party switches or routers to attach to the wired network.

**The biggest architectural difference was in the methods used to shuttle traffic between access points and switches.**

None of the switches tested require direct attachment to its access points. A company can use one WLAN switch to manage dozens, or even hundreds, of access points scattered throughout the corporation, including at different physical locations. Aruba claims support for 50 access points on its A2400 switch (and 256 access points on the larger A5000, not tested). Chantry claims support for up to 200 access points, and Cisco claims support for up to 300 access points with a single WLSM blade.

The biggest architectural difference was in the methods used to shuttle traffic between access points and switches. Aruba and Cisco products set up Generic Routing Encapsulation tunnels between the access points and switches, but each system uses different structures within the GRE tunnel. For example, a protocol analyzer that decodes Aruba's traffic will not read Cisco's traffic. Chantry's BeaconMaster encapsulates traffic using IP-in-IP encapsulation. The Colubris CN1250, because it is a stand-alone access point, does not encapsulate traffic.

**The varying transport methods raise interoperability and performance issues.**

The varying transport methods raise interoperability and performance issues. Aruba and Chantry say their switches interoperate with third-party access points, but they may not offer all the same features as their own gear. Also, encapsulation adds some overhead, which reduces performance and may introduce packet fragmentation. But encapsulation can be very useful to manage client roaming because it lets clients keep the same credentials and IP address as clients move from one access point to another.

For QoS enforcement, the vendors tested (except Chantry) say they now support the emerging 802.11e Wireless Media Enhancements protocol. The IEEE hasn't yet ratified 802.11e, and thus all Wi-Fi QoS mechanisms today are by definition proprietary. Judging from some of our results, companies may want to wait until the standard is ratified and products fully implement it—something we hope to show in future tests.

All the products tested (except Colubris CN1250) can allocate bandwidth to a given workgroup. This is useful in distinguishing between employees and guests associated with the enterprise network. Aruba and Cisco products also can allocate bandwidth on a per-user basis.

Price is a major difference among the products tested, but can be misleading. At less than \$2,000, Colubris by far had the lowest price, but that does not factor in the required third-party switch or router. Aruba and Chantry were both about \$9,000 as tested. Cisco's entry came in at more than \$50,000 as tested, but it also includes an enterprise backbone-class chassis and management module. Cisco's rationale for bringing in such a large system is that companies already use the market-leading Catalyst 6500 at the core of the network, and it also makes a logical place to manage wireless attachments. Even so, Cisco's solution comes at a price: The WLSM blade alone costs more than twice as much as any other system tested.

# Case Studies

## WIRELESS TO TAKE OFF AT VEGAS AIRPORT

■ By John Cox

Between the wireless LAN switches and the radio frequency identification system, McCarran International Airport in Las Vegas is spending serious money to go wireless. And that's not even counting what it paid for used luggage.

The switches are for the airport's recently unveiled no-charge wireless Internet access services for passengers. The luggage was used early this year to run an extensive battery of tests on the first part of a \$120 million baggage system that exploits RFID tags and will boast 4 miles of conveyor belts.

"We bought just about every piece of used luggage we could find at Salvation Army stores and other places," says Samuel Ingalls, McCarran's assistant director of aviation, information services. "We cleaned them out."

The luggage was hauled to the Air Cargo Terminal, chosen to be the first site for what eventually will be an airport-wide automated system to collect, screen and

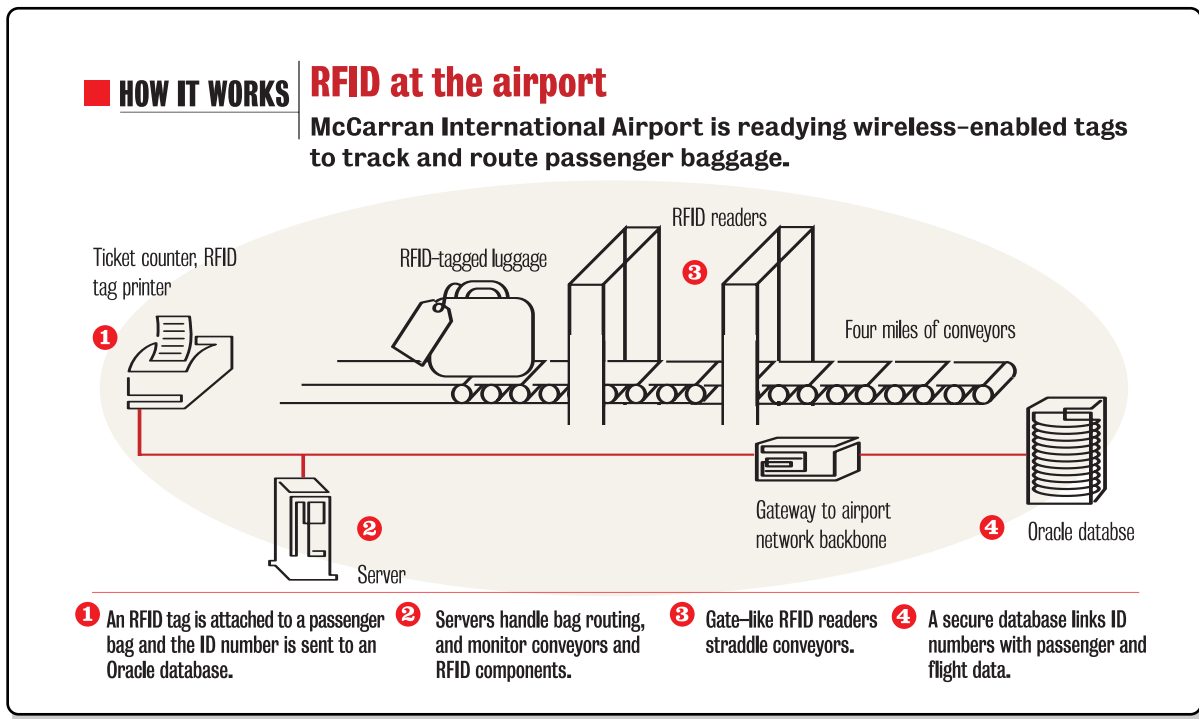
X-ray luggage, and then parcel it out on time to the gates to load onto jets. The Air Cargo site also will be used to screen luggage checked in from offsite locations such as hotels and resorts. Later this year, bags from those sites will arrive at this terminal, run through screening and then pass along the conveyor system being built at the other terminals.

### Early tests look good

The RFID tests at the terminal have been impressive, Ingalls says.

Bags with read-only RFID tags pass along the conveyors through gate-like RFID readers. A radio chip in each tag sends out a signal that is picked up by the gate's antenna array. The tags transmit a unique 10-digit ID number, which is forwarded along with a time stamp to a secure Oracle database that associates the information with passengers' personal data and flight information.

Until now, each airline at McCarran had its own tagging system based on bar codes, which have to be read by a laser scanner. The scanner must have a clear line of sight to the tag. But scans can fail to register because of dust on scanning heads, inclement weather



## Case Studies

in areas near jets or misaligned print heads that smear part or all of the bar-code label.

"Their read rates vary from about 80% to 90% accurate in most systems," Ingalls says. "Unless the tag can be clearly seen by the scanner, it won't be read."

Ingalls' goal for the RFID system was a read accuracy rate of 99.8%. In the tests earlier this year at the Air Cargo Terminal, using all those thousands of Salvation Army suitcases, backpacks and duffel bags, the lowest rate was 99.89%. "In one test with 3,000 bags, we had one misread," Ingalls says.

McCarran on average handles 65,000 outbound bags per day. If 10% of those were misread, the airport would have to have a process to handle some 6,500 bags manually, at least for part of the process. Every time a bag has to be touched between a ticket counter and a jet's cargo bay, it costs time and money.

Lost or late bags cost even more. According to data from SITA, a Geneva IT services company owned by airlines and other air transport industry companies, mishandled baggage cost airlines \$1 billion per year. The company estimates it costs an airline an average of nearly \$90 when a bag doesn't show up on time. In 2004, the number of mishandled bags in the U.S. jumped 20% over the 2003 figure, SITA says.

That's a big incentive for McCarran and its airlines to bring the RFID system online, on schedule. The plan is to have conveyors in place, with RFID readers, RFID printers at the ticket counters in the main terminal and two new security scanning sites, all operational by mid-year, with the remaining sites in the months following. The first RFID printers are due to arrive in the next week or so.

The entire project - which includes conveyor installation, construction of what amounts to six multi-story buildings, IT spending, the RFID components and tags — will cost \$125 million. That includes a 5-year \$20 million contract for 100 million RFID tags.

FKI Logistex, a St. Louis company that specializes in automated materials handling, is building the new baggage system. The RFID components are from Symbol Technologies, which last fall acquired Matrics, the RFID company originally working on the project.

Most passengers will never notice this system, though they might notice that they no longer have to schlep their bags over to the X-ray machines after checking in. This should give passengers whose computers are outfitted with a WLAN card more time to use McCarran's free wireless Internet access system.

### Wireless 'Net access

The \$75,000 WLAN system went live in January with 20 Aruba Wireless Networks access points - now up to 30. The airport plans to add another 30 over time to support more users, enable load balancing among

access points and dedicate some as radio monitors, says Gerard Hughes, airport network manager.

The access points were installed easily. The IS group mounted them on pillars supporting the ubiquitous video screens known as FIDS, for Flight Information Display System, which show flight arrival and departure information throughout the terminals. These pillars

**Roughly 200 to 300 people use the system daily.**

**A few times there were about 500 concurrent users, with no impact on performance.**

already were wired for electricity and a link to the airport's fiber backbone. The access points connect back to one of Aruba's high-end Model 5000 switches in the main terminal's data center.

"We liked the idea of the access point as a dumb radio, with the intelligence on the switch," Hughes says.

It's a stand-alone WLAN, running separately from the airport's backbone. Internet access is via a 3M bit/sec DSL pipe.

Roughly 200 to 300 people use the system daily. During the recent heavily attended Consumer Electronics Show, the number jumped to 900 to 1,200. A few times there were about 500 concurrent users, with no impact on performance.

The one unknown was customer support: how to handle the inevitable calls about connection problems or other glitches. The IS group chose simple Service Set Identifier, and put together an easy-to-read-and-use brochure that's distributed throughout the airport. It seems to be working: The help desk gets four or five calls a day about the WLAN. "So we think it's been pretty easy for people to get online," Hughes says.

Recently, one airport tenant, which offers wheelchair services for passengers, began running its VPN over the WLAN so staff with wireless handhelds can schedule services while on the move.

Over time, Hughes expects other tenants and the airport itself to add applications to the network, using Aruba's virtual LAN tagging support to keep them separate.

Case Studies

**DARTMOUTH RETOOLS FOR WI-FI VIDEO**

■ By Tim Greene

Dartmouth College has embraced Wi-Fi for data so enthusiastically that the school's IT chief is leaping into voice and video over Wi-Fi. A venture that calls for tripling the number of access points on campus, swapping out old wireless gear for smarter equipment and partnering with a start-up that is still putting the finishing touches on its technology.

With video set to go into production soon, the Hanover, N.H., school is beefing up its Wi-Fi network to support four channels of educational video, says Brad Noblet, director of technical services for the college. "We have a little over 600 access points today covering 150 buildings in a mile square. I'm going to come close to tripling that in order to increase the amount of bandwidth so I can deliver video and handle a number of concurrent VoIP telephone conversations."

The current Wi-Fi network, based on Cisco gear, is used primarily for e-mail, instant messaging and Web surfing, he says, but the school has greater needs.

"A lot of the faculty feel like to capture the attention of their students, they have to do more than just stand there and talk," he says. That means adding video presentations as part of the curriculum.

Ideally that would mean student laptop access to audio, video and data in classrooms, but that would require an Ethernet jack at each desk, a huge infrastructure upgrade. "We want to take four channels for teaching and learning and make those available on wireless as well as wired so we can again have this mobile classroom effect," Noblet says. "You don't need a smart classroom." The new wireless gear will support existing data applications and Internet access.

The school has teamed up with Video Furnace, a start-up that multicasts video to laptops using client software agents downloaded to PCs when users select the encrypted

videostreams they want. The company supports Macintosh, Linux and Windows operating systems, all of which are used on campus. In addition to supporting the educational streams, Video Furnace also will deliver commercial cable TV to the campus over Dartmouth's converged wired IP network, Noblet says.

Because each computer needs 400K to 2M bit/sec of bandwidth to screen video content (depending on screen size and resolution), efficient use of bandwidth is key.

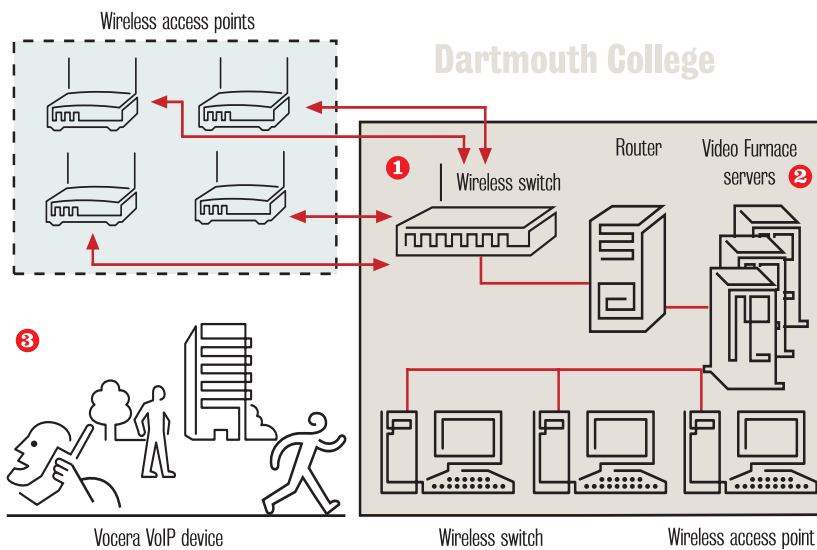
Bandwidth for 802.11a is provided at 55M bit/sec using its own radio frequency. 802.11b supports 11M bit/sec, and 802.11g supports 55M bit/sec, but 802.11b and 802.11g share the same frequency. If an 802.11b device associates with an access point, the access point drops down to 11M bit/sec for 802.11g users.

That led Noblet to choose 802.11a. "I'm going to be able to get on the order of 20 to 25 streams per access point," he says.

Noblet is packing access points in high density for areas such as dorms that are likely to have large numbers of users, to ensure coverage during peak times. He is swapping

**Video strains Wi-Fi**

Dartmouth College is tripling the density of its Wi-Fi access points to support video, and it is installing smart switches that load balance access and adjust signals to maximize coverage area.



- 1 Aruba switches in high-use areas such as dorms load balance access requests to make the most efficient use of access points and adjust transmission power to maximize coverage area.
- 2 Video Furnace servers download client software to PCs that have authenticated and multicast video.
- 3 The locations of users with Vocera VoIP devices can be determined via the wireless switches. In the future, servers will be able to send users information, such as when not to use equipment located in a given room.

## Case Studies

out Cisco access points for Aruba Wireless Networks access points because Aruba supports intelligent switching. "Cisco was not in that game" when he started the project, he says.

The intelligence he wants includes Aruba wireless switches' ability to load balance requests from laptops. In an area with overlapping access points, the switches send messages that force laptops to less-busy access points to maximize the number of users associated with the wireless network.

The switches also adjust power of access point transmissions to maximize the area in which wireless devices can get a signal.

The intelligent switches, in combination with mapping tools, also make it easier to install access points effectively. "The wireless switch can force access points to signal one another so they can get an indication of who can hear who and develop a coverage map that gets plotted graphically on a screen," Noblet says. Using that map, technicians installing access points can see where more access points are needed. "When we put up the original 600 access points, it damn near killed us to do it manually," he says.

The tool plots Wi-Fi coverage on architectural drawings of buildings. "So I can see how's my coverage in this given building and be able to pinpoint where I need to move an

access point or maybe I need to add an additional access point," he says.

Noblet spent a lot of time with Aruba developing location-sensing tools to go along with the switches. Now the switches can tell him the rough location of a wireless device associated with the network, and this can help run the campus more efficiently.

For instance, a student on an unstaffed floor of the library who is wearing a VoIP communicator badge made by Vocera could ask, "Where are the Shakespeare folios located?" Voice recognition software would translate the question and deliver an automated voice response to tell the student where the folios are in relation to where the questioner is standing.

Similarly, students with laptops in a lab could query a server how to use the piece of lab gear sitting in front of them, and the server could respond with a Web page containing a user manual.

The video project should also increase use of VoIP over Wi-Fi. Most Wi-Fi VoIP phones employ 802.11b, which supports only eight concurrent VoIP calls. More access points means support for more VoIP, Noblet says, which should help accelerate the college's migration to VoIP. So far about 4,000 of 7,000 phone lines have been converted to VoIP, but only a few hundred of those today are Wi-Fi, he says.