CMP
United Business Media

Network Computing

MAY 11, 2006 I WWW.NWC.COM

For IT By IT

WHY NOT CISCO

SOONER OR LATER, A PERVASIVE, MANAGEABLE, SECURE WIRELESS LAN WILL BE TABLE STAKES FOR ENTERPRISES. WHO YA GONNA CALL TO MAKE IT HAPPEN? BY DAVE MOLTA

Ethernet is holding its ground, for now, by virtue of being fast, cheap and relatively secure. But wireless will eventually become the default method of connecting to enterprise networks, and Ethernet will assume a secondary role as a distribution, rather than an access, technology.

When that happens, will Aruba, Symbol, 3Com or any other WLAN player be able to keep Cisco from extending its wireline dominance to wireless?

That depends on whether enterprise IT pros see going with a smaller vendor as a gamble or a smart bet. We have time to contemplate this scenario, of course—the wireless play won't happen overnight. In fact, in our reader poll for this article, only about 8 percent of respondents saw Wi-Fi displacing Ethernet as the most common form of network access during the next three years. But a wise strategist plans five or 10 years ahead, and by then a new generation of Wi-Fi gear will be broadly available, offering 10, even 100 times the performance of today's technologies.

Lots of No-Shows

Although we track developments continually, NETWORK COMPUTING takes an in-depth look at the enterprise WLAN space about once a year. Our evaluation in February 2005 proved interesting because we tested Cisco and Airespace gear side by side and concluded that Airespace had the better offering. Unbeknownst to us, Cisco was performing the same evaluation and agreed with our assessment. By the time our review went to press, Cisco had announced its acquisition of Airespace. Since then, the company has been busy doing what it does best: assimilating superior technology.

When we first embarked on our latest in-depth analysis, we worked with enterprise wireless network managers, vendors, analysts and test-tool makers Azimuth and VeriWave to develop a test plan that covered the full range of issues IT confronts, including product architecture, security, deployment, management, performance and cost. We asked for a significant commitment from vendors in both equipment and support staff. Of the 17 invited to participate, only two—Cisco and Bluesocket—took us up on our offer. Although excuses ran the gamut from a lack of internal resources to concerns that our test plan was too complex, not to mention a little too risky in light of the test platforms' relative immaturity, we concluded that most enterprise WLAN vendors don't want to participate in in-depth product reviews unless they can write the test plan.

Cisco's decision to buck that trend is notable because it has the most to lose from a critical review.

IMPACT ASSESSMENT: ENTERPRISE WIRELESS LANS

	BENEFIT	RISK
IT ORGANIZATION	**The holy grail of Wi-Fi** as the default network connection has the potential to cut cabling costs, and IT staff access to Wi-Fi services can positively impact operational effectiveness. Security features required for wireless can be leveraged to enhance wired network security.	**Wireless networks introduce** significant security risks, their implementation often requires reallocation of IT resources, and rapid evolution of standards means short technology-refresh windows. Still, a failure to implement secure Wi-Fi services leaves the door open to rogues.
BUSINESS ORGANIZATION	**Benefits of Wi-Fi** vary significantly, based primarily on the degree to which internal operational efficiency can be enhanced through mobile information access. Vertical industries can often demonstrate clear ROI; value in carpeted enterprise is generally softer.	**Employees will balk** at a decision not to deploy Wi-Fi services. Attempts to bypass IT policies by implementing personal or departmental Wi-Fi systems introduce significant information security risks.
BUSINESS COMPETITIVENESS	**In business sectors** such as retail, health care and education, wireless is essential to competitiveness. In other businesses, it's all about enhancing personal productivity and shrinking decision windows.	**Mobile information access** can transform business processes in some industries, so ignoring it may not be an option. However, leveraging Wi-Fi for competitive advantage is not easy because the highest return often comes from a pervasive deployment.
BOTTOM LINE	**You can spend a lot of time** developing ROI models to justify an enterprise WLAN, but why bother? This is just something you have to do, unless your shop is hyper-security-sensitive or plans to defy the trends toward increasingly mobile work patterns and notebook computer use. Wi-Fi is built into notebooks, employees have wireless at home, and they want it at work, too. And so do your visitors. Spend your time figuring out how to do it right, with rock-solid security, efficient manageability and capacity for growth.	

After all, it dominates the WLAN market with more than 50 percent share, according to both Synergy Research and Gartner. That got us thinking that maybe the real theme of this article should be, Can anyone beat Cisco? It's a fair question, and one that's on many IT pros' minds. Yes, there are enough ABC ("anybody but Cisco") shops out there to keep at least a few competitors in business, but Cisco's decision to send us a crate full of gear to test shows the company is willing to go head-to-head with any rival, not on the basis of its name, but on its product's merit. Cisco engineers spent several days in our Syracuse University Real-World Labs®, helping us gain a better understanding of its broad and increasingly complex array of WLAN offerings. After they left, we spent about four weeks pressing as many buttons as we could and running a battery of tests. We also appreciate Bluesocket agreeing to participate; we're in the process of testing its gear.

We circled back with vendors that declined to participate and asked them—as well as Bluesocket—to complete an RFI that posed a dozen questions of interest to IT pros and spend a day with us demonstrating their offerings. Aruba Networks, Bluesocket, Colubris Networks, Extreme Networks, Extricom, Meru Networks, Proxim Wireless, Siemens AG, Symbol Technologies, 3Com and Xirrus returned RFIs describing their overall architectural approaches to enterprise WLANs and discussing such ideas as whether enterprises should focus on a single vendor for their wired and wireless networks; use of WPA2, authentication, authorization, monitoring, mobility and endpoint security; guest access; performance and scalability; and cost. Bluesocket, Extricom, Extreme, Meru and Xirrus paid visits to the lab. Our summarized analysis of Bluesocket's response is below. Amazingly, some notable players, including Enterasys Networks, Foundry Networks, Nortel Networks and Trapeze Networks, didn't take the time to respond.

FYI **Full Force:** Large enterprises are more likely to have implemented WLANs than smaller companies: 31 percent of enterprises with more than 20,000 employees have fully deployed WLANs, compared with 22 percent that have 1,000 to 4,999 employees, according to Forrester.

'Marketectural' Trends

It's never easy to mark generational shifts in technology, but it's important to understand WLAN evolution because each successive generation addresses fundamental architectural limitations of the products that came before.

We think in terms of three distinct eras. Early WLANs, both proprietary and 802.11, were sold primarily into vertical markets like retail, supply chain, health care, manufacturing and education. These WLANs were expensive and, by today's standards, feature-limited. Because the applications didn't require substantial bandwidth, the design goal was to maximize the coverage area of each access point. The number of APs and clients was limited, so management was simple. Some of these legacy systems have been upgraded, and many more will require overhauls in coming years as vendors gradually announce many

RFI Synopsis: Bluesocket

Performance and scalability	Controllers range from 8 to 100 APs, providing flexible deployment sizes
Planning and deployment	Partnered with Motorola/Wireless Valley for its planning tool; management system provides RF coverage heat maps
Monitoring and management	Controller and management system provide two levels of monitoring, with roles determining levels of access; reports can be exported in a variety of formats and run automatically
Security and availability	Controllers support standard 802.11i security mechanisms, the ability to terminate VPN connections, a variety of authentication methods and wireless access policies; partnered with Check Point Software Technologies for integrated, clientless endpoint scanning; controllers offer stateful failover and load-sharing
AP capabilities	APs feature dual radios and internal or external antennas; management system can configure and support autonomous APs from vendors such as 3Com, Cisco and Proxim
Pricing	APs, $450; controllers start at $1,695 for 8 APs and $12,995 for 50 APs; management system, $9,995
Industry penetration	Achieved significant early market penetration, particularly in education, government and health care, by providing flexible security gateways with mobility-enhanced capabilities; has added integrated APs and associated AP management capabilities to that platform
Strengths	Has several years' experience providing secure mobile identity-based WLAN services on large networks, providing it with a large customer base and an understanding of enterprise wireless issues; with its roots as a security-oriented company, Bluesocket has already solved the most difficult problems, but now needs to establish market identity as a total enterprise Wi-Fi system provider
Weaknesses	Transforming itself from a security gateway company to a full integrated WLAN system provider will be challenging, as will hanging on to its existing customers (especially Cisco shops) that now have a broader range of options for deploying a secure enterprise WLAN

For our analysis of RFI responses from Aruba Networks, Bluesocket, Colubris Networks, Extreme Networks, Extricom, Meru Networks, Proxim Wireless, Siemens AG, Symbol Technologies, 3Com and Xirrus, go to *networkcomputing.com/go/1709rd1.jhtml*. Full RFIs are available at *networkcomputing.com/go/1709rd2.jhtml*. For a list of questions we asked WLAN vendors, go to *networkcomputing.com/go/1709rd3/jhtml*.

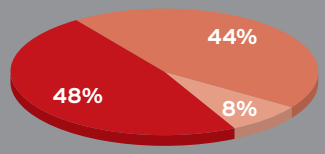
components' end of life.

Second-generation enterprise WLANs supported newer access protocols (802.11a, b and g) on more powerful APs and provided significant functional improvements over first-generation offerings, at a lower cost. But inherent architectural deficiencies prompted the emergence of third-party tools for site design (Ekahau and Wireless Valley, now owned by Motorola) and management (AirWave and Wavelink), as well as security gateways (Bluesocket and AirFortress) and wireless IDSs (AirDefense and AirMagnet).

Third-generation enterprise WLANs are best represented by the Big 3 start-ups—Airespace, Aruba and Trapeze—all of which made market splashes in 2003. Their architectures applied client-server distributed processing principles to wireless LANs, combining so-called "thin" APs and centralized controllers glued together with proprietary protocols that effectively locked customers into using APs and controllers from a single vendor. Initial product offerings were creative but complex, often requiring that APs attach directly to controllers (then called wireless switches) installed at the network edge. By 2004, version 2.x offerings addressed many of the performance, reliabilty, security, integration and management deficiencies plaguing initial products. Cisco took significant steps to add controller capabilities to its highly successful Aironet wireless offerings, while established wireless competitors, like Bluesocket and Colubris, enhanced their systems to compete with the Big 3.

READER POLL

Imagine how your network will look three years from now. Which of the following best represents the relationship between Wi-Fi and Ethernet LANs?



- Wi-Fi will supplement Ethernet LAN services by providing convenient network access in public spaces, like conference rooms and cafeterias
- Wi-Fi will be broadly available throughout our facilities but Ethernet will be the most common form of network access
- Wi-Fi will displace Ethernet as the most common form of network access

Source: NETWORK COMPUTING Reader Poll, 276 respondents

Meanwhile, network gear vendors—namely, Alcatel, Enterasys, Extreme, Foundry, Nortel and 3Com—developed OEM relationships to provide their customer bases with wireless solutions. These were largely me-too offerings that leveraged the channels of established network vendors, but such an approach is much less risky than internal development. And for providers like Trapeze, the OEM channel was a lifesaver, a way to remain profitable in an increasingly competitive market dominated by Cisco. The OEM approach is not a bad strategy per se, but it poses significant risks for enterprise IT, especially in emerging technology markets. Organizations that purchased Nortel WLAN gear when the company had an OEM relationship with Airespace, for example, were forced to migrate when Cisco bought Airespace and Nortel switched to Trapeze as a system provider.

CISCO CCX: ADDED VALUE OR STANDARDS END RUN?

Cisco is walking a fine line with its Cisco Compatible Extensions (CCX) program. The dearth of critical standards-based functionality in areas like mobility and RF management has forced the company to venture into the world of proprietary protocols to meet customer needs. CCX encourages WLAN-client vendors and silicon providers to implement Cisco-specific enhancements and certify those products for compatibility. Although Cisco has encountered challenges along the way, especially in getting vendors to update drivers and utilities for older hardware, most new enterprise-class client hardware includes full support for CCX.

It's ironic that the management team from Airespace used to complain to us that, though Cisco was open in providing CCX implementation details to client vendors, Cisco hardware was required if you wanted to leverage those features. When Cisco relabeled and added the old Airespace controllers and APs to its Unified Network, there was no support for CCX. Version 4.0 of Cisco's WLAN controller software now includes support for a range of CCX functions, including roaming, radio resource management, Cisco discovery protocol and enhanced security.

Eventually, we expect to see standards-based solutions to all the feature voids CCX is designed to address. Cisco's public statements vehemently assert that the company will maintain and promote proprietary capabilities only as long as necessary and that it will be aggressive not only in contributing its intellectual property to standards bodies but also in supporting standards as they emerge. Seasoned IT pros can be forgiven some skepticism—Cisco's track record in this regard is checkered. Yes, the company almost always adds support for standards, but the implementation of those standards sometimes provides customers with subtle encouragement to stick with proprietary features.

We hope this isn't the path Cisco takes with CCX, and in the end, it's up to network managers to drive Cisco's direction. If you express satisfaction with proprietary capabilities, there will be little motivation to standardize. Sometimes, solving problems in your own organization takes precedence over doing what's best for the industry as a whole. But at the least, you should let Cisco know that you believe in open industry standards and will make future purchasing decisions with that ideal in mind.

Although notable differences in features and functionality exist among established WLAN controller vendors, all their offerings are more feature-rich and polished than they were a year ago. But the most interesting development since our last look at enterprise WLAN systems has been the emergence of new architectures from Extricom, Meru and Xirrus. The last is addressing deployment and scalability challenges by integrating as many as 16 radios and a controller into a single AP and using sectorized antennas to support narrow pie-slice-shaped cells, an approach resembling that taken by cellular providers. Extricom and Meru have adopted a more revolutionary tactic, eschewing conventional channel-planning design in favor of a single-channel architecture with the goal of addressing interference and roaming problems.

For organizations contemplating the rollout of simultaneous VoIP and data services over a single WLAN infrastructure in the 2.4-GHz band—and for those that just don't want to deal with the hassle of multichannel RF design—the approach taken by Extricom and Meru may offer significant benefits over more conventional architectures. Although equipment from both vendors operates with standard 802.11 clients, their controllers play a more significant role in regulating access to the airwaves, which allows for a more deterministic form of network access. And because the WLAN appears to clients as a single AP operating on one channel, rather than multiple APs operating on different channels, as is the case with older designs, roaming is extremely fast.

Although the single-channel architecture offers benefits, the problems associated with more conventional multichannel systems may be mitigated by several key developments. First, increasing numbers of enterprises are smartly supporting dual-band (2.4-GHz and 5-GHz) infrastructures, meaning contention issues are somewhat mitigated as clients are spread across a larger number of channels. Second, the emergence of ultra-high-speed 802.11n will make performance and capacity problems less of a long-term concern. And finally, if standards-based solutions to client-radio-management problems and secure, fast roaming make their way from the IEEE into products, the benefits of Extricom's and Meru's scheduled-access designs don't look quite so compelling.

There's a strong chance all this will happen during the next two years. Still, Extricom and Meru are making important technical contributions that could significantly enhance enterprise WLAN performance, and we wouldn't be surprised to see other vendors adopt some of these capabilities.

LAB TESTED: CISCO UNIFIED WIRELESS NETWORK

Cisco Systems sent key elements of its UWN to our Syracuse University Real-World Labs®. These appliances, controllers and APs blur the lines between Cisco's market-leading wired network gear and the enterprise WLAN. (See "Picking the Pieces," page 7, for a rundown of components.)

The UWN is based on the products and technologies Cisco picked up when it acquired Airespace. Cisco says standalone IOS-based APs will still be supported, but companies looking for superior management tools and advanced functionality, such as fast roaming, mesh services and location capabilities, should consider phasing in UWN devices.

Those planning new Cisco controller-based networks, or expanding existing ones, will need the WCS (Wireless Control System). For testing, we entered a floor plan of our lab with an aerial map view, specified the type of APs and antennas we wanted, whether to optimize for coverage or capacity, and our throughput expectations. While WCS provided an educated guess at how many APs we should deploy, its features are not as comprehensive as those found in some third-party planning tools.

We also evaluated WCS' monitoring and reporting capabilities. We quickly saw an aggregate view of network health from a dashboard that provides data on controllers, APs, rogue APs and client activity, and we could drill down to specific devices and events. We generated canned reports on items including client counts, transmit power and channel and AP activity, based on historical data from the previous seven days. While the reports are elementary, they provide trend information. Overall, the built-in security-monitoring and reporting capabilities will meet the basic needs of enterprises without specific compliance or regulatory requirements; others may want to consider a wireless IDS/IPS system.

We also investigated the UWN's location-tracking, guest-access capabilities and the ability of the architecture to serve enterprises with branch-office locations. We were impressed with location tracking, and Cisco's upcoming 4.0 software and hardware release should ease the creation of guest credentials. A wide range of AP and controller choices provides flexibility in configuring remote locations.

Growth Industry

Tracking enterprise WLAN market trends requires a fair amount of subjective interpretation. Fourth-quarter 2005 enterprise WLAN shipments worldwide were up 29 percent over the same period in 2004, according to Dell'Oro Group. For the year, sales were up 20 percent, making enterprise WLANs a billion-dollar market. Still, the enterprise market is about half the size of the more consumer-oriented small office/home office space, and other research firms put enterprise WLAN numbers slightly lower. Synergy Research pegs Q4 2005 enterprise WLAN growth at 5 percent year over year. Likewise, it reports overall 2005 enterprise WLAN sales of about $1.3 billion, up 5 percent from 2004.

To some degree, reductions in the per-unit cost of APs mask the true expansion. However, the positive cost impact of commodity-priced APs is offset by a steady enterprise migration from second-generation smart-AP system architectures to newer designs that leverage WLAN switches or controllers. These systems have considerably higher profit margins for vendors—and they significantly increase capital expenditures for enterprises. Synergy estimates almost 30 percent of enterprise WLAN purchases in Q4 were for controller-based architectures, and sales of controller-based systems grew 76 percent in the same quarter, year over year. Clearly, there's a trend toward newer architectures, especially for green-field installations, and even those who prefer more conventional smart APs recognize they'll eventually need to change their designs to leverage emerging features and services, like better roaming, enhanced security, location and mesh back-

FYI **Slainte-d Adoption:** Almost 30 percent of enterprises in the United Kingdom and Ireland have deployed WLANs, surpassing North America, with 24 percent adoption, according to Forrester.

Picking the Pieces

A number of components fall under the heading of Cisco's Unified Wireless Network, but you don't have to buy one of each to put it all together. That said, it's always helpful to understand what each piece does and its pricing.

Product name	Description	List price
4400 Series Wireless LAN Controller	This wireless controller is designed to sit in the distribution-layer data closets throughout your infrastructure. The 4400 Series has several models, with capacities of 12, 25, 50 and 100 APs.	Starts at $9,995
2000 Series Wireless LAN Controller	This controller is designed for branch-office use and currently supports six APs. The product is also available as a module for the Cisco Integrated Services Router, dubbed the Wireless LAN Controller Module, or WLCM.	$3,250
Catalyst 6500 Series Wireless Services Module (WiSM)	The WiSM blade, designed for the Catalyst 6500 Series switch, supports as many as 300 APs per module. This product is good for shops that want to centralize controllers within the network core or at large distribution blocks.	$45,995
Catalyst 3750 Integrated Wireless LAN Controller	This new product, included with Cisco's 4.0 release, delivers the form factor the industry has been expecting—an Ethernet switch and wireless controller rolled into a 2U device. The product contains all the functionality of a Catalyst 3750 switch and supports as many as 50 APs.	$TKTK
Wireless Control System (WCS)	The WCS is the software platform that ties together the Unified Wireless Network, providing a single point for WLAN planning, multiple controller management and aggregate network monitoring. Currently, WCS is limited to 1500 APs and 50 controllers, but the next release is slated to scale to 2,500 APs and 250 controllers. If your network exceeds these proportions, you can set up another WCS, but you'll have to manage each independently.	Starts at $3,995
2700 Series Wireless Location Appliance	The WCS uses the capabilities of this appliance to track the locations of as many as 10,000 devices on the wireless network in near-real-time.	$14,995
Aironet 1000 Series Access Point	Available in a/b/g and b/g-only versions, the 1000 Series AP contains several models designed to meet a variety of needs, from basic carpeted-office access to the Aironet 1030, which can serve as a remote edge AP (REAP) for wireless backhaul, and as a point-to-point and point-to-multipoint bridge.	Starts at $599
Aironet 1100 Series Access Point	This AP series has been around for a while as a carpeted office-focused autonomous AP that supports b/g through internal antennas. The company hasn't made many changes, except to add a lightweight version.	$599
Aironet 1130 Series Access Point	The 1130, supporting a/b/g, is also designed for the carpeted office, with an internal omnidirectional antenna and no external connectors; it's capable of serving as a hybrid remote edge AP (HREAP).	$699
Aironet 1200 Series Access Point	The 1200, like the 1100, is not new, but has been made LWAPP-capable. This ruggedized AP supports b/g out of the box and has a modular slot for 802.11a support.	Starts at $750
Aironet 1240 Series Access Point	The 1240 is a ruggedized version of the 1130, with no internal antenna, just connectors for external 2.4-GHz and 5-GHz antennas. It also can serve as a repeater, a bridge and in HREAP mode.	$899
Aironet 1300 Series Access Point	The b/g-only 1300 provides for outdoor AP and bridge capabilities, for enterprises that want to put their toes in the water for open-air services.	$1,299
Aironet 1500 Series Access Point	Enterprises ready to jump into wireless may prefer the new 1500 mesh APs.	$3,999

haul. The hope, from a budget perspective, is that enhanced operational efficiency of these new designs will offset higher acquisition and vendor maintenance costs. Whether this will pan out is a complex issue. In large installations, some centralized management capabilities are critical, but there are many variables that must be considered before spending extra money on hardware and software in hopes of reducing staff costs. These factors include the quality of management capabilities, the number and variety of users and the type of applications they're running, the available skill sets of technical staff, discounts provided by vendors, and internal budget policies that compare current and future costs.

As noted earlier, Cisco dominates in market share, controlling more than half of enterprise sales. Just how much more is a good question. If you zero in on the so-called "carpeted enterprise" market and exclude Symbol, and if you focus exclusively on WLAN infrastructure rather than supporting products like wireless VoIP, that number sneaks closer to 65 percent. By any measure, Cisco is doing well. Although Synergy has the

Emerging Standards

IEEE Task Group	Task group title	Summary	Status/expected ratification	Comments
802.11e	Quality of service enhancements	Defines MAC procedures to support LAN applications with QoS requirements, including the transport of voice, streaming audio and video over IEEE 802.11 WLANs.	Ratified	No 802.11e-compliant client devices are available. Many client vendors, including VoIP phone vendors, are supporting the Wi-Fi Alliance's WMM (wireless multimedia) spec, which includes a subset of 802.11e features.
802.11k	Radio resource management (RRM)	Working to define radio resource measurement enhancements to improve the capability, reliability and maintainability of WLANs. Key goals include enabling better diagnostics, improving dynamic frequency planning, optimizing network performance and enabling new services like voice/video over IP and location-based services.	Projected ratification: October 2006	802.11k is a key element of many vendors' WLAN plans because it will allow client radio parameters to be centrally managed, a process expected to enhance performance in small-cell dense deployments. Cisco is a big backer of 802.11k and includes some of this functionality in CCX.
802.11n	Higher data rates and throughput	New MAC and PHY technologies to expand the throughput of 802.11 WLANs to 100-Mbps+ throughput speeds	Projected ratification: September 2007	The 802.11n standard, based on MIMO technology pioneered by Airgo Networks, is one of the most highly anticipated developments in wireless networking in recent years. After an intense battle between two consortia (TGnSync and WWISE), the new Enhanced Wireless Consortium (EWC) emerged earlier this year, with backing by Cisco and most leading wireless silicon vendors. However, while pre-N and EWC-compliant products are emerging, there's no guarantee these products will be upgradable to support the final standard.
802.11r	Fast roaming	The 802.11i task group, which developed a new security architecture for WLANs based on 802.1X, EAP and AES, was not able to agree on a standard for secure fast roaming in a timely manner. This job was given to the 802.11r task group. The standard is designed to let clients move from one AP to another and quickly re-establish both security and QoS state without introducing security vulnerabilities.	Projected ratification: March, 2007; but the 11r proposal has just been recirculated, so late 2007 seems more likely.	Several vendors have prestandard fast-roaming solutions. Cisco has two: Cisco Centralized Key Management (CCKM) and Pro-active Key Caching (PKC), which was an Airespace proposal.
802.11v	Wireless network management	Provides enhancements to the 802.11 MAC, extending other amendments to add client diagnostics and client-reporting capabilities.	Projected ratification: September 2008; IEEE publish: October 2008	While 802.11k is important because it standardizes the information collected across a wireless network, 802.11v will be required to use this information in a meaningful way. Cisco and others are pushing to make this happen because 11v is crucial for efficient operation of densely deployed wireless networks. Further, 11v may let customers move away from proprietary client software (Cisco CCX enhancements and third-party wireless supplicants).
802.11w	Management frame protection	11w is an attempt to close a gap in the 802.11 standard, which defines protection for data frames, but not management frames. Unprotected management frames leave systems vulnerable to denial of service, device impersonation and information falsification.	Projected ratification: March 2008; IEEE publish: April 2008	Cisco has been pushing 11w, actively working through 802.11 but also moving ahead with its own management frame protection—aptly named MFP—which is a prestandard version of 11w, in conjunction with CCX.

SOURCE: Network Computing reporting. IEEE data at *www.ieee802.org/11/*. Updated projected ratification dates at *grouper.ieee.org/groups/802/11/802.11_Timelines.htm*.

overall enterprise WLAN market growing by 5 percent in Q4 2005, it gauges Cisco's growth at 18 percent. Impressive, especially when you consider that the company was busy absorbing Airespace during 2005, an activity that undoubtedly convinced some Cisco customers to take a wait-and-see attitude regarding new acquisitions.

What's Next

One of the most significant decisions for IT managers relates to the integration of conventional Ethernet and Wi-Fi LAN services. One school of thought is that Ethernet and Wi-Fi are complementary LAN access alternatives that demand tight service, security and policy integration. For example, many organizations with large 802.11 deployments are implementing 802.1X authentication and privacy services. Although 802.1X has long been available for Ethernet networks, few organizations have taken advantage because the cost often exceeded the benefits. However, once an 802.1X infrastructure is developed to support 802.11, the incremental effort associated with adding wired Ethernet to the mix is relatively modest. Vendors that embrace this view seek to leverage existing Ethernet infrastructures by adding wireless functionality. The most notable examples include Cisco's plan to add Wi-Fi controllers to its Catalyst 6500 and 3750 products.

A counterpoint position asserts that these technologies are sufficiently unique in design and capabilities to be treated separately. Does it make sense to upgrade an established Ethernet infrastructure solely to support enhanced wireless functionality? After all, it's common for Cisco shops to run older, more stable IOS code in their switches and routers. Vendors that champion the overlay strategy assert that the Wi-Fi infrastructure should be logically distinct, though dependent on, a robust Ethernet environment. They further warn that, though a vendor may offer the appearance of wired/wireless integration by physically embedding wireless controller capabilities into a switch, such an approach may offer only a minor level of true integration. And the risks associated with early adoption are real, despite vendor efforts to test all permutations.

From a practical perspective, Cisco has embarked on a concerted effort to integrate wired Ethernet and wireless 802.11 services, but its most ambitious goals are still found in PowerPoint slide decks rather than in real products. Still, we predict Cisco will continue its push in that direction, providing rational incentives for its Ethernet customers to remain loyal when it comes to wireless.

For other purveyors of wired and wireless gear, including Enterasys, Extreme, Foundry, Hewlett-Packard and 3Com, all of which partner with third parties for WLAN services, the level of integration is thin at this point. The reason for this goes beyond the challenges associated with integrating wired and wireless to reflect the complexity that's still associated with delivering enterprise-class wireless.

For technology professionals looking at wireless as a tactical service, either approach will likely meet your needs. For more strategic, pervasive deployments, the level of integration required will vary depending on your security policies and the nature of your wireless applications. Delivering enterprise hotspot service is getting a lot easier; implementing pervasive wireless VoIP, location services and granular multilayer security is not.

Last but not least, don't discount the very real possibility of finger-pointing between wired and wireless vendors when things go wrong. Purchasing best-of-breed technology for every network application sounds great in principle, but minimizing the number of vendors you deal with to maintain adequate service levels almost always simplifies operations. That puts Cisco in a clear position of market leadership. Yes, its gear may cost a little more, and you may need to navigate through the complexities of a mega-company for support. But when it comes to wireless, it's a safe bet you won't be giving up much for this added level of comfort. NWC

HAVE WI-FI, WILL WORK WHILE TRAVELING?

Does your company provide accounts for mobile employees to access wireless hotspots? Here's what Gartner found when it surveyed more than 2,000 business travelers in the United States and Britain:

25%
U.S. respondents who use hotspots while traveling on business, compared with 17 percent of U.K. respondents

4 of 5
Laptop PCs that will have native Wi-Fi capabilities by the end of 2008

16%
Respondents who say they're worried about security

1 in 10
Respondents who think Wi-Fi hotspot access is too expensive

$29.99
Per-month cost of unlimited access to T-Mobile's HotSpot locations in U.S., with a 12-month commitment

37%
U.S. Wi-Fi users who connect to hotspots more than 10 times a year. For U.K. users, it's 33 percent

Source: Gartner Dataquest, NETWORK COMPUTING

DAVE MOLTA is a NETWORK COMPUTING senior technology editor. He is also assistant dean for technology at the School of Information Studies and director of the Center for Emerging Network Technologies at Syracuse University. Write to him at *dmolta@nwc.com*.

Wireless, Wireline Come Closer

We put elements of Cisco's Unified Wireless Network initiative to the test and were impressed, not only with how well it's assimilated Airespace's technology but with integration across the entire enterprise network

BY DAN RENFROE

To say that Cisco Systems' WLAN infrastructure offering is comprehensive is like saying the Grand Canyon is big—the scope just doesn't come across. Cisco's Unified Wireless Network blurs the line between the company's traditional wired network hardware and the appliances, controllers and APs that make up the UWN. Although you don't need one of each UWN product, our testing of the crates of gear Cisco sent to our Syracuse University Real World Lab® shows the company has worked hard to integrate all of the elements to extend the capabilities of your WLAN.

Once we got all the gear sorted out, we explored Cisco's UWN package with an eye toward how IT groups would use it to plan, deploy, manage, secure and monitor enterprise WLAN services. Note that we primarily tested hardware running version 3.2 operating code, but Cisco briefed us on some of the new features and hardware that will be available with its 4.0 release, due out in early May.

The UWN is largely based on the product line and technologies the company got in its Airespace acquisition, leaving owners of stand-alone Cisco IOS-based APs—what Cisco calls "autonomous APs"—asking, "What about me?" In discussions with Cisco, it became clear to us that the company doesn't see these autonomous APs as going away, nor does it see them as being in conflict with the controller-based system. Still, the reality is that autonomous APs provide fairly baseline WLAN services; customers desiring advanced functionality, like fast roaming, mesh services and location capabilities, will need to upgrade.

More important for enterprise IT, the management tools for the UWN are superior to Cisco's tool for autonomous AP management, the Wireless LAN Solution Engine, or WLSE. Existing customers need not fear, though; Cisco has developed a number of updates to enable autonomous AP customers to upgrade while still protecting their hardware investments.

Planning Your Implementation

If you're planning a new Cisco controller-based network or expanding an existing one, you'll start with the WCS (Wireless Control System), a soft appliance that runs under Windows or Linux and provides WLAN planning, deployment, management and reporting capabilities.

In a controller-based environment, you might have APs in the same building, even on the same floor, that communicate with different controllers for load-balancing or redundancy reasons. Thus, viewing APs based on controller won't always provide an accurate geographical view of a wireless network. That's where building maps and floor plans come in—representing a WLAN based on physical deployment areas provides administrators with comprehensive pictures of their networks. Maps are a critical part of any planning tool, and WCS is no exception. WCS differs, though, in its ability to use these maps for planning versus management and location tracking. We'll focus on planning capabilities for now, reserving management and location tracking for later sections.

The planning capabilities of WCS are designed to give users a ballpark idea of how many APs to deploy and where they should be located. Utilizing the map features of WCS, we re-created a section of our campus complete with an aerial map view (handy if we were doing outdoor coverage) and floor plans of the building where our labs are located. In planning mode, we specified the types of APs and antennas we wanted, whether to optimize for coverage or capacity, and our throughput expectations. The system then recommended AP placement, and we were able to adjust its suggestions based on our knowledge of the building and re-calculate coverage areas. The tool also contains a map editor that allowed us to draw in walls and architectural features that might impede RF propagation, such as elevator shafts or concrete walls.

Those who have already deployed WCS and placed APs on maps can pull existing AP data for a floor into planning mode and adjust AP location and antenna type, as well as add or remove APs, to visualize what those changes will do to WLAN coverage. One of our biggest frustrations with the planning capabilities of WCS, though, is the disconnect between planning maps and deployment maps. If we chose to deploy our APs in the same locations we had placed them in planning mode, we couldn't just import that placement data from planning mode; we had to manually place the APs on deployment maps all over again.

We feel that WCS' planning capabilities provide an educated guess at how many APs a company should deploy, but the features are not as comprehensive as those found in some third-party tools—enterprises with complex RF environments or expansive reporting capabilities will want to invest in a separate planning utility, like the predictive modelers by Ekahau, Motorola/Wireless Valley and others. Some WLAN vendors, including Bluesocket, Colubris Networks and Xirrus, see the value in these tools and have partnered with third-party vendors to provide these capabilities.

Putting It All in Place

Cisco's UWN takes a layered approach to deployment and management. APs, once deployed, discover and communicate directly with controllers. Controllers, in addition to managing and coordinating APs, can communicate with one another. Although we could manage individual controllers directly, it may be cumbersome to keep everything up-to-date if you've got more than two or three. In addition, the monitoring capabilities of individual controllers are fairly basic. That's where WCS steps in, providing a way to manage multiple controllers and deploy your wireless network.

We were impressed with the relatively straightfor-

ward deployment options. After some initial CLI configuration, we were able to easily manage our controllers through their internal Web interfaces or using WCS. While we could manually copy configurations from one controller to another, a better route is to use the template capabilities built into WCS. WCS has a number of templates for groups of settings, like SSIDs; radio parameters; and management configurations. Once created, those templates can be pushed out to all controllers or any subset thereof. The same thing goes for APs: We created templates for controller order, AP mode, location and more, and pushed them out to subsets of the AP population.

In addition to mass configuration, we used WCS to change configurations on select controllers; anything we could do on the APs' Web configuration interfaces, we could do from WCS. Of course, just because you *can* do something doesn't mean you should. We think it would be pretty easy to get far down the rabbit hole by making a number of indi-

UNIFIED WIRELESS NETWORK ARCHITECTURAL BASICS

The controller-based architecture of Cisco's Unified Wireless Network is a definite shift from the autonomous-AP mindset, where access points serve as the ingress/egress points for network data destined for wireless clients. Not so with lightweight APs in a controller architecture, where client data is tunneled back to the controller.

We thought it might be useful to discuss the underlying architecture for the Unified Wireless Network, with an emphasis on the role of Cisco's proprietary LWAPP (Light Weight Access Point Protocol). LWAPP is the protocol Cisco APs use to communicate with controllers and is the secret sauce behind light-touch AP provisioning.

Although LWAPP is a proprietary protocol, it also serves as the basis for the current draft of the CAPWAP (Control and Provisioning of Wireless Access Points) specification the IETF is developing. Cisco is not the only company to espouse a thin-AP architecture—most vendors with switch-based architectures have developed a similar method for AP-to-controller communications. Still, though these architectures are similar, don't expect cross-vendor interoperability anytime soon, even after the CAPWAP specification is approved and implemented by vendors. The Cisco architecture provides one example of why this is: APs and controllers conduct mutual authentication through factory-installed X.509 certificates; maintaining that level of security with products from multiple makers poses challenges that many vendors (and enterprises) will be reticent to tackle.

When a lightweight AP is connected to the network, it attempts to find a controller IP address through a variety of means; these discovery requests include IP broadcast, DHCP options and over-the-air provisioning through neighbor messages from other APs. Once the AP finds a controller, it sends a join request to that controller; the controller then identifies the AP and determines whether it should let the AP join, or should point it to another controller based on the preference settings configured by the network administrator. Once the AP is joined to the appropriate controller, it downloads the correct AP operating code version from the controller; using this method ensures all APs will have the proper code to communicate with the controller.

Communication between AP and controller occurs within a UDP tunnel that secures device communications and also provides heartbeat functionality. Every 30 seconds, the AP sends a heartbeat message to the controller to verify connectivity; if this process doesn't receive a reply, the AP disjoins from the controller and searches for a new controller, providing a good failover mechanism.

Roaming, especially across subnets, is a critical capability, especially for voice deployments. In some cases, roams may occur across controllers, which is where the rubber meets the road in terms of technical complexity. It just wouldn't be a "unified" network if the system broke down here. Cisco has developed a solution that we feel places less strain on applications during roams across subnets: When a client roams from an AP on a controller connected to one subnet to an AP on a different controller connected to another subnet, the client ends up with dual-citizenship—it maintains its client record on the first controller and its IP address from the initial subnet, but it also has a client record on the second controller, marked as its foreign "home." Outbound data from the client is sent through the IP subnet that the controller is connected to, but incoming data is sent to the original controller, where it is tunneled back to the foreign controller via Ethernet in an IP tunnel.

Inter-controller communications, for roaming and other activities, relies heavily on an element Cisco calls Mobility Groups. Administrators can designate as many as 24 controllers as members of a Mobility Group, enabling information sharing among them. For example, controllers within the same group automatically share information to facilitate inter-controller roaming, AP load balancing and controller redundancy. These groups are usually created if it's possible for a client to roam from AP on one controller to an AP on another. Say you have a WLAN across two large office buildings, but it's impossible to roam between the two; you might create separate Mobility Groups for the controllers in each building.

vidual configuration changes that could get out of sync with the other controllers. Although WCS will tell you if a controller is out of sync, there's no method to enforce a particular template. Enterprises can manually conduct version control by creating active and backup templates for rollback if there are issues, but the software doesn't have enforcement built in. We raised this issue with Cisco, and its position is that organizations with WCS tend to use templates and not make individual controller changes; if they do tweak, it's for a good reason.

Monitoring Activity and Security

The current generation of Cisco's UWN has solid capabilities for monitoring active network events, with a focus on security-centric happenings. WCS' first screen provides an aggregate view of network health from a dashboard that provides quick data on controllers, access points, rogue APs and client activity. From there, we drilled down to specific controllers and other wireless devices and accessed detailed information on security events, network alarms or critical events on the network.

WCS' security event tracking is not limited to rogue APs. Through signature-based tracking we found that WCS monitors wireless attacks, like deauth floods, as well as NetStumbler usage that might indicate suspicious activity. The system also checks for AP attacks, like AP impersonation, and client security events, such as WEP decrypt errors and IPSec failures.

The alarms and events track a variety of network activities, including security events, controller and AP messages, and location server notifications. Each item is designated with a specific priority level, ranging from informational to critical, and we were able to assign events for follow-up and add annotations. We could also configure the system to notify us of specific event types.

From WCS, we generated canned reports, including client counts, transmit power, and channel and AP activity, all based on historical data from the previous seven days. While reports are fairly basic, they provide decent trend information for the reporting period.

Overall, we felt that the monitoring and reporting capabilities built in to WCS provide a baseline for the metrics an administrator needs to keep tabs on a wireless network. In the future, though, we'd like to see Cisco add capabilities for reporting and trending for longer periods, and hopefully much of the information in WCS will eventually be able to migrate upstream to a broader network monitoring system, not just one solely focused on the wireless network. The missing integration at this level made us question how "unified" the Cisco solution is, but given that Cisco is early in this endeavor, we're willing to wait and see.

We believe WCS' wireless security monitoring capabilities will meet the basic needs of most enterprises now, and Cisco is working to improve in that area; for example, a number of the company's CCX initiatives, such as NAC (Network Admission Control) and MFP (Management Frame Protection), are aimed squarely at security. That said, enterprises with specific compliance or regulatory requirements need to look beyond the basics toward Cisco's IDS product or the wireless IDS/IPS systems offered by vendors like AirDefense, AirMagnet, AirTight Neworks and Network Chemistry.

Rounding out the Feature Set

Cisco is betting that location tracking is going to be one of the next killer apps, and its efforts in that arena should stand up to the test if that wager pays off. While many verticals, like healthcare and manufacturing, do require location tracking capabilities, we're unsure how critical it will be for the typical carpeted enterprise to have real-time tracking of Wi-Fi devices.

Nonetheless, we're definitely impressed with Cisco's location tracking. Using WCS paired with a Cisco 2700 Series Location Appliance, we were able to view a variety of Wi-Fi devices on the floor plans we had imported into WCS. Devices were separated into typical categories, including clients, 802.11 asset tags and rogue APs. Word to the wise: Achieving solid accuracy with location requires a dense deployment of APs in order to adequately triangulate the signal.

A more critical feature for many enterprises is the ability to facilitate guest access to the wireless network, but this poses challenges for administrators. The first issue is limiting or prohibiting access to corporate resources—you want to provide Internet access so visitors can check their e-mail, not give them a peek at your ERP system. In most enterprise WLANs, setting up separate SSIDs, often tagged to a separate VLAN, is an effective way to segregate guest traffic. WCS also allowed us to tunnel guest traffic back to a controller housed in the DMZ, terminating all guest traffic outside our firewall—a handy trick.

The real sticky issue with guests, however, is how

to authenticate them. The most common method is to use a captive portal system, but then you've got to set up their credentials first, a problem because IT may know little to nothing about guests before they arrive. Cisco's upcoming 4.0 software and hardware releases add a number of capabilities to facilitate creation of guest credentials, including automatic generation of guest user IDs and passwords, and also create a handy role that Cisco calls the "Lobby Ambassador." This role would enable, say, a receptionist to create time-limited guest accounts. We think this is a great idea, and many of Cisco's competitors agree—we've seen similar features cropping up in other WLAN offerings.

We also examined Cisco's UWN architecture with an eye toward branch- and remote-office wireless services and found solutions to meet different needs. For larger branch offices, Cisco offers several controllers, the 2000 series and the Wireless LAN Controller Module for the Cisco ISR, that can support as many as six APs.

However, enterprises with multiple, smaller branch offices that need only one or two APs may not want to invest in controllers for each site. It is possible to deploy only APs at small locations, but because LWAPP data is tunneled back to the controller, there is the issue of WAN survivability and increased utilization on those WAN links. This may not be a big deal if your application traffic already traverses that link, but Cisco also addresses the issue with its Aironet 1030 AP, which can operate in REAP (Remote Edge Access Point) mode. REAP splits the data and control planes for APs by bridging data traffic locally at the AP while still tunneling LWAPP control data back to the controller. Unfortunately, REAP mode does not have visibility into 802.1q VLAN tagging, making it necessary to bridge all data traffic locally at the AP. This may be a problem for some enterprises; for example, you may want to tunnel all guest traffic back to a controller in the corporate DMZ, which is not possible with REAP.

Enter HREAP (Hybrid REAP) mode, which will be supported on Aironet 1130 and 1240 APs with Cisco's newest software release, due out about the same time as this article. HREAP supports visibility into VLAN tagging, providing enterprises with the flexibility to determine which SSIDs will have data bridged locally and which will have data tunneled back to a controller. HREAP is a definite improvement over REAP and will be attractive to enterprises looking to provide small-scale wireless services for a multitude of branch offices. And did we mention there's no extra charge?

Get What You Pay For

Speaking of price, enterprises that have implemented traditional autonomous AP networks, especially installations with 100 or more APs, are going to experience sticker shock when they start looking at controller-based systems, regardless of vendor. Given that controller hardware bumps up costs, we asked Cisco to supply us with pricing information on the UWN components we tested, so that we could provide a ballpark cost estimate.

HAVE NO FEAR, UPGRADES ARE HERE

When a vendor makes major architectural shifts in its product line, and especially when shifts are due to acquisitions, current customers often feel confused and left behind. One of Cisco's major challenges in rolling out the Unified Wireless Network will be to assure customers that have invested in Aironet APs and WLSE appliances that they won't be left out in the cold.

A number of existing Aironet products and design models will be going into maintenance mode, meaning that you won't see a lot of new feature releases, but the company isn't going to be announcing end-of-life or forcing customers to migrate to the new architecture. To that end, expect to see a decreased emphasis on the Structured Wireless-Aware Network (SWAN) and products like the Wireless LAN Services Module (WLSM) for the Catalyst 6500 switch and the Wireless LAN Solution Engine (WLSE), a management tool for autonomous APs.

Cisco is doing a number of things to ease the pain for customers that have invested in these products. The company has buy-back and trade-in programs to help you recoup purchase costs, for example. Options also exist for customers that want to run their existing WLAN hardware alongside the new products; for instance, a Catalyst 6500 will support WLSM blades and WiSM blades simultaneously.

The big deal as far as we're concerned, though, is the ability to upgrade many existing products to work in a controller-based architecture. By the 4.0 software release, due out about the same time as you read this article, Cisco says customers will be able to upgrade the majority of legacy APs to communicate with controllers. Upgradable models include the Aironet 1100, 1130, 1200, 1240 and 1300 Series APs, though there are some specific early revisions of those devices that may not be included. Cisco hasn't forgotten about customers who have invested in the WLSE management appliance, either; a utility to upgrade your WLSE to a WCS is due out with the 4.0 release in early May.

Certainly, Cisco is not going after extremely cost-conscious shops with its WLAN products, but the list prices it supplied were fairly reasonable when compared with competitors based on their RFI responses. Cisco APs, which start at $599 for the 1000 Series and $699 for other models, are middle-of-the-road in terms of AP pricing. Controllers are difficult to compare in an apples-to-apples fashion because quantity of APs supported and extra licensing options vary among vendors. That said, Cisco's 4400 Series Controller starts at $9,995, which we find comparable to many rivals. The price does increase, however, based on the number of APs supported, as it does with just about every WLAN vendor.

The real budget cruncher comes when you start bundling pricey extras, like the Wireless Services Module (WiSM) for the Catalyst 6500 Series switch. When WiSM is bundled with the 6500 chassis, Supervisor 720 module and redundant power supplies, the package starts at $86,995 list. This supports 300 APs and has room to grow, with space for more WiSM modules, making it possible to increase capacity within the chassis.

All prices listed here are MSRP, a point from which to negotiate downward. Some colleagues at higher education institutions cite discount levels up to 40 percent off of list; large organizations should be able to expect similar deals.

Performance

We conducted a number of performance tests in an effort to gain a better understanding of how the Cisco UWN performs in a lab environment. A bit of a caveat before we dig in, though: We realize that benchmark feeds and speeds recorded in our labs may more accurately simulate theoretical maximum capabilities than real-world conditions. For instance, several of the test tools that we use to simulate multiple clients do so with a single radio, eliminating the bottlenecks that contention places on the wireless medium. Moreover, without other systems to compare to, it's tough to cull a lot of meaning from the data.

Using the Azimuth Systems 800W test chassis, we evaluated the call capacity and quality capabilities of an Aironet 1240 AP connected to a 4400 Series WLC. In running as many as 18 simulated calls with varying levels of TCP background traffic, we found that the system performed admirably. In instances of no background traffic and up to 5 Mbps of background traffic, we got Mean Opinion Score (MOS) values hovering around 4.3 and 4.4. Even after increasing the background traffic to 10 Mbps, our downstream MOS stayed at around 4.3 and 4.4, although the upstream MOS was a little lower, at an average of 4.07, but still very respectable. For comparison, most cell phones provide a minimum MOS of 3.5, although some scale up to 4.3. Five is the highest attainable MOS, but anything above 4 should be acceptable to users.

We also tested the association capacity of the Cisco system. We were able to associate 127 simulated clients using the Azimuth system in open, WPA-PSK and WPA2 with RADIUS, so there are definitely no issues with AP capacity as far as clients are concerned. The final evaluation we performed with the Azimuth was a failover roaming test to determine how a client would behave if the AP it was connected to failed. Using an Intel 2915ABG client card, we saw average failover roam times of 2.5 seconds in open authentication and three seconds in WPA2, which is reasonable for most applications, although latency- and connectivity-sensitive apps would be temporarily hampered.

In addition, we conducted a number of tests with the VeriWave WaveTest 90 connected to eight Aironet 1240 APs and a Cisco 4400 Series WLC. We evaluated aggregate throughput of the system across a number of frame sizes, ranging from 82 to 1400 octets, and found respectable throughput for each size in the range. At 1400 octets we were pushing approximately 167.48 Mbps across all eight APs; at 82 octets we measured about 26.45 Mbps, both reasonable by our standards. We also tested the latency of the system at load, measuring latency at the observed throughput of the previous frame-size ranges. Average latency ranged from 3 ms to 6 ms, with maximum latency running between 55 ms and 85 ms. These figures, especially the average latency, are sufficient for most enterprise applications. At maximum latency you might have brief effects on VoIP traffic, but because average latency is much lower, we don't think those effects will cause much of an issue for users.

As for the ability of the system to handle 81 clients of different security configurations (open, WPA-PSK and WPA2-PSK) roaming among all eight APs, we measured an average roam delay of 37 ms for clients in open mode, and 94 and 96 ms for clients using WPA-PSK and WPA2-PSK, respectively. These numbers were marginally higher than we expected, but in our discussions with VeriWave and Cisco we came to realize that those results are attributable to the unique way the VeriWave system measures roam delay—this test measures the end-to-end roam, including any delay inserted by the controller, rather than just measuring the delay in associating with a different AP.

Putting It All Together

The final burning question on our minds—and yours too, we suspect—is whether the controllers you buy today will support 802.11n, the forthcoming standard from the IEEE to update the 802.11 MAC and PHY layers to achieve higher throughput. Cisco told us that it's still too early in the standards process for it to commit to an answer one way or another. Because the standard is still in draft form, and because of the uncertain nature of the changes to the MAC and the PHY, we'd be suspicious of any vendor that was willing to make a lot of promises with respect to 802.11n support.

We believe that Cisco has a solid offering with the Unified Wireless Network, and the strides that the company has made toward integrating the Airespace technology make its wireless story fairly compelling for Cisco shops. We agree that putting the WiSM module in the Catalyst 6500 platform isn't new to those familiar with the older Wireless LAN Services Module (WLSM); products like the new Catalyst 3750 Integrated Wireless LAN Controller Ethernet switch/wireless controller, on the other hand, indicate the company's commitment to a tighter integration between wired and wireless networks. NWC

DAN RENFROE is a technology associate focusing on wireless and mobile technologies with the Center for Emerging Network Technologies at Syracuse University. Write to him at *drenfroe@nwc.com*.