InformationWeek
:: analytics

Dec. 5, 2008

Get Ready For 802.11n

As more vendors release products based on the upcoming 802.11n spec, with its increased speed, coverage, and reliability, wireless is becoming a viable platform for mission-critical network connectivity

IN THIS REPORT

United Business Media

InformationWeek
:: analytics

Five Dual-Band Routers Put To The Test

Our reviewer picks the top dual-band 802.11n routers from SMC, Apple, DLink, Linksys, and Netgear

By Bill O'Brien

THE AFRICAN ELEPHANT has one of the longest gestation periods of any mammal: 660 days on average.

The Institute of Electrical and Electronics Engineers has been working on the 802.11n specification for nearly 1,825 days, or five years now, and hopes to have a final version by the end of 2009.

We really could have used an 802.11n router last year, we probably needed them this year, and by the time they show up next year we'll likely need something faster anyway. But that hasn't stopped the presses—or the device manufacturers.

Over the years, router makers have been cobbling together "Pre-N," "Draft-N," and any myriad number of products with names that associate their devices with the 802.11n standard without actually saying they are the standard—because they're not, because there isn't one. They're all based on draft proposals that keep inching closer to what the standard could be. Latest out of the blocks is dual-band 802.11n.

Why have we bothered to wait around for so long? It's because 802.11n is better and faster than 802.11g—the current honest-to-goodness standard. Yes, it really is. Multiple input multiple output, or MIMO, technology, allows a router to send more information over multiple radios at the same time and receive data more reliably, thanks to multiple antennas. Better still, since it can compare the different antennas' data streams, it can fill in any missing data to derive the correct content. Good stuff, huh?

As a side benefit, because it can work with partially corrupted signals, you can squeeze more range out of an 802.11n. In fact, the boast is that it works best with the most reflections. (More fractured data streams mean more signals to compare and integrate.) Enabling mint julep-

sipping out on the veranda while surfing the net is worth the wait!

Until now, however, our Wi-Fi has been wallowing in the doldrums of the 2.4-GHz band. That also happens to be where you'll find your microwave, most cordless phones, some garage door openers, and baby monitors—among other things. You have to deal with all of that—plus all your neighbors' Wi-Fi signals. That's why we're jumping on the 5-GHz band.

Of the 11 Wi-Fi channels in the 2.4-GHz spectrum available in the United States, only three: 1, 6, and 11, don't overlap, based on a 20-MHz wide signal. With 24 channels on 5 GHz, there is more overall bandwidth available to accommodate the use of wider channels, making things faster. In theory, that would increase throughput to 540 Mbps rather than the 135 Mbps on the mandated (2.4-GHz) 20-Mhz signal. But we all know about theory, right? The truth is that most 802.11n product manufacturers don't advertise 540 Mbps. They usually use a number closer to 300 Mbps. The honest truth is that actual throughput can hover around 120 Mbps and that's still quite a bit faster than you'd achieve with 802.11g on its best days.

The way to use dual-band 802.11n correctly is to keep all mundane Internet tasks (mail, Web surfing, etc.) down on 2.4 GHz and throw all your streaming tasks (audio, video, and the like) up on 5 GHz where the lanes are wider and can better handle the load. That's why the latest iteration of 802.11n supports dual-band operation and the latest version will let you use those two bands in the same router simultaneously.

Which brings us to the dual-band routers we've chosen to review.

To establish a baseline, we turned to an SMC Barricade N Pro Wireless Broadband Router. It's a meat-and-potatoes Draft 2.0 router. Apple's Airport Extreme made the cut, as did Netgear's RangeMax Dual Band Wireless-N Router. These are both dual-band but not simultaneous. You can use them on one band or the other, but not both at the same time. D-Link's Xtreme N Duo Media Router and Linksys WRT610N are both simultaneous dual-band routers. These last two are supposed to be the workhorses of the group.

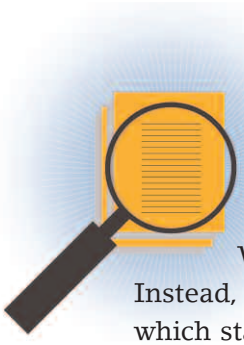
Keep in mind as you go through the reviews that we're only using "802.11n" as a short form. While they are all Draft 2.0 compliant, these routers are "pre-802.11n" until such time as the

The Linksys WRT610N has a slick appearance

specification is a finally ratified. That means they could be subject to change between now and then—as they were between when the plan was first laid out and now. The harsh reality is that if manufacturers are going to spend money developing the specification, they also need to recoup some of that money by selling products—whether they're going to change over time or not. Reality bites.

HOW WE TESTED

There are a myriad number of ways to test routers and other Wi-Fi gear and they're all equally correct and, probably to some extent, equally wrong. Besides, it's already been estab-



lished that 802.11n products—even in Draft form—do produce an empirical increase in throughput and distance.

We're not going to re-invent the wheel. Instead, we chose a very simple approach, which started by optimizing the network topology. If that sounds impressive, it's just taking a close look at what components are in a network and where they are in relation to the router.

In our case, we removed a Linksys WRT600N router from an upstairs room where all computing for our nine PCs had begun and spread downward through the house. We moved that router to the ground floor. Naturally that meant that the upstairs computers needed to be converted to wireless. Computers on the main floor were hardwired into the router and the computers in the basement were configured wirelessly.

The reconfiguration placed the wireless PCs, on average, eight feet above or below the router and no more than 20 feet away laterally. (Feel free to use the hypotenuse of a right triangle formula to figure the exact distance as the Wi-Fi flies.) The places where 802.11g adapters could not be found by the router ("dead zones") were gone.

Technically, that negated the need for the better accuracy and increased distance coverage of 802.11n gear. (And it's something you should consider before you run off with your credit card in hand.)

Our tests started with a simple file-transfer process: copy an 873-MB mpeg video file from a wired PC on the main floor through the router to a wireless PC in the basement. During the file test, we shut down all of the PCs except the single wired computer on the main floor and the one wireless computer in the basement.

Those file transfers were accomplished at each of the bands available from the routers (2.4 GHz and/or 5 GHz). First we used the native equipment (a Linksys router and Linksys Wi-Fi adapter, for example). Then we reconfigured the wireless computer with a Netgear N121T adapter. It's an older 802.11n device and, basically, gives us a reasonable attempt at finding compatibility with the new equipment. After that, we configured a pair of Netgear WNHDE111 high-definition gaming adapters as an access point to the router and as a bridge connected to the basement PC.

If you've never heard of that before, it's pretty slick. The connection between the bridge and the access point is wireless and, for these adapters, uses the 5-GHz band. However, the PC and the router on each end of the setup believe they're wired together, so it totally ignores what might be happening on the router's wireless side. Effectively, if you have a 2.4-GHz router, adding the gaming/media adapters gives you a simultaneous 5-GHz and 2.4-GHz Wi-Fi arrangement. (Even if your original router is a 802.11g.)

Once all of the file transfers were done, we turned everything on for every computer (nine of them) plus a Roku Netflix player and started having fun playing videos and downloading Instant Play videos from Netflix. Whether it was the overall quality of the new gear or the optimized site topology, everything went smoothly. The only exception was Linksys, which we describe in the detailed review that follows.

SMC BARRICADE N PRO

Setting up the SMC Barricade N Pro Wireless Broadband Router SMCWGBR14-N was like returning to an old friend. After years of testing Draft N equipment, nearly a dozen similar routers lounge around the place. They are all basically big, fat waffles, each with a cadre of antennas poking out into the world. Setup was better

than in the past.

The Barricade worked out of the box: Attach it to the modem, attach your PC, power up the modem, router, and PC (in that order), and Shazaam, it's working! You can stop there if you want, or you can run your browser and reach the router through its address, provided on the quick start sheet. Once you've customized names or passwords or any other parameter you feel needs tweaking, close the browser and you're done.

SMC's USB adapter (SMCWUSB-N) is just a tad more complex—you'll need to run a driver disk. This is single-band equipment so there are no 5-GHz versus 2.4-GHz choices to make. It operates solely at 2.4 GHz and the two SMC components work together in a surprisingly odd manner.

Since we were looking to establish base timings, we weren't expecting all that much from a basic 802.11n unit. (Yes, we're jaded.) We were also correct, of course. Transferring our 873-MB file took 3.5 minutes and that was dead last in

Setting up the SMC Barricade was like returning to an old friend.

the group, tied with D-Link. The Barricade had no problem with our older Netgear N121T USB adapter, punching through the file transfer in a meager 2.2 minutes, tied with Linksys.

When we bypassed the wireless portion of the router and ran the test through our WNHDE111 HD gaming adapters, the transfer time was 2.0 minutes, which was about a half-minute slower than the rest of the group—with the exception of Apple's 1.9-minute time.

All told, this is a great 802.11n single-band starter kit if you're looking to test the waters before 802.11n goes live next year. You can also add 5 GHz to it via the HD gaming adapters so there's no tossing it out as the technology advances.

APPLE AIRPORT EXTREME

A little shorter and all white, Apple's Airport Extreme dual-band router is a good physical match for the similarly square Mac Mini. And if are wondering why an Apple product is included in a router review that's so obviously PC, admit-

SMC's Barricade N Pro

FEATURES:
Dual Band: No
Firewall: Yes
Data Stream Management: Yes
Wi-Fi Protected Setup: Yes
Antennas: 3
Number of Switch Ports: 4
Port Speed:10/100/1000
USB Port: Printer
Dimensions: 7.1 x 4.8 x 1.2 in.

TEST RESULTS (IN MINUTES)
Proprietary 2.4 GHz: 3.5
Proprietary 5 GHz: N/A
Netgear N121T: 2.2
Netgear 5GHz HD: 2.0

tedly Apple came late to the table with its newest incarnation of the Airport Extreme, but it delivered a router that is equally capable under either a Mac or PC environment.

Installation is a snap with the provided disc. It delivers the needed software for either Windows or OS X, depending on what environment it finds itself in. Apple has accomplished a near miracle by making the Airport utility software—the core application from which you customize the router for either 2.4-GHz or 5-GHz operation (it's not simultaneous)—run in relatively plain English. It's a linear progression of option selections that get you from start to finish without having you break a sweat.

In case you hadn't noticed, there aren't many (i.e., none) 802.11n adapter cards available from Apple. Why should there be? Most of the newer Macs and Macbooks are already "n" enabled. There went the portion of our testing scheme that called for file transfers in 5-GHz and 2.4-GHz bands using a proprietary adapter. So we cheated a bit. Instead of using a native adapter, we employed a MacBook as the proprietary hardware for both 5-GHz and 2.4-GHz proprietary transfer tests.

Apple's Airport Extreme

FEATURES:
Dual Band: Either/Or
Firewall: Yes
Data Stream Management: No
Wi-Fi Protected Setup: Yes
Antennas: 3
Number of Switch Ports: 3
Port Speed:10/100/1000
USB Port: Printer/Disk
Dimensions: 6.5 x 6.5 x.1.3 in

TEST RESULTS (IN MINUTES)
Proprietary 2.4 GHz: 2.5
Proprietary 5 GHz: 1.5
Netgear N121T: 2.7
Netgear 5GHz HD: 1.9

Apple's Airport Extreme is equally capable in both Windows or OS X.

Although the testing is not 100% comparable because of differences in hard drive and processor speeds between our PC test and the MacBook, the Airport Extreme did turn in the second-best 2.4-GHz transfer time. The 2.5 minutes it needed to move our 873-MB video file was second only to Netgear's RangeMax Dual Band Wireless-N. Likewise, it took top honors at 5 GHz (by a scant but measurable 0.1 minutes).

Why bother if we can't directly compare? The Airport Extreme can also be used as a bridge, attached to an existing router. If you have an 802.11n single band router or, gasp, an 802.11g router, simply attach the Airport Extreme to it, use the Airport Utility software to set it up for 5 GHz, and you have a simultaneous dual-band router that runs quite rapidly at 5 GHz—1.5 minutes in our testing. You can mix and match your existing Wi-Fi gear to it, or be exclusive and just hang any new Apple 802.11n equipment on it and leave your old PC gear to your old router.

Perhaps surprisingly, the Airport Extreme evolved into one of our favorite routers during the testing. It's not cheap by any means, but its performance and flexibility is worth the price of admission.

NETGEAR RANGEMAX DUAL BAND WIRELESS-N

Looking not a lot different than a rectangular

alien spaceship flashing bright blue LEDs under a clear dome on top, Netgear's RangeMax Dual Band Wireless-N Router WNDR3300 is possibility one of the most annoying routers you'd ever not want to look at. Then again, an appreciation for eye-searing blue pulses over my preference for the twinkle of amber and green LEDs (which it also has) could be an acquired taste.

As with Apple's Airport Extreme, Netgear's WNDR3300 is not a simultaneous dual-band model. You can, however, use its browser-based interface to switch among several modes—some of which might give you pause, literally.

- Up to 270 Mbps at 2.4GHz
- Up to 270 Mbps at 5 GHz & 54 Mbps at 2.4 GHz
- Up to 130 Mbps at 2.4 GHz
- Up to 130 Mbps at 5 GHz & 54 Mbps at 2.4 GHz

The default is "Up to 270 Mbps at 2.4 GHz", which allows all 11b/11g and 802.11n wireless stations to peacefully co-exist at 2.4 GHz at a reasonable speed. If you want 5 GHz, the second and fourth options will allow it but you're driving everything else (basically, any 802.11g legacy adapters you might be using) way down to 54 Mbps and disallowing any 2.4-GHz 802.11n adapters you might be using, unless they also support 802.11g fallback.

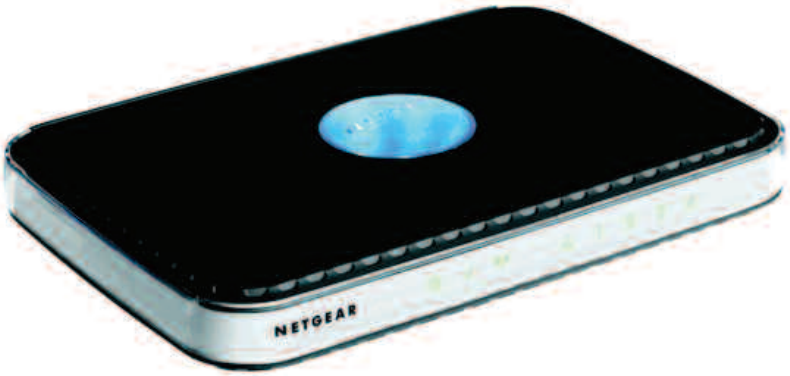
Netgear's WNDR330

FEATURES:
Dual Band: Either/Or
Firewall: Yes
Data Stream Management: Yes
Wi-Fi Protected Setup: Yes
Antennas: 8
Number of Switch Ports: 4
Port Speed:10/100
USB Port: No
Dimensions: 8.8 x 6.0 x 1.2 in

TEST RESULTS (IN MINUTES)
Proprietary 2.4 GHz: 1.9 | 2.0 | N/A
Proprietary 5 GHz: 5 GHz: N/A | N/A | 2.3
Netgear N121T: 3.0 | 2.3 | 4.3
Netgear 5GHz HD: 1.5 | 1.5 | 1.5

Note: Test results reported as follows: 270 Mbps @ 2.4 GHz | 130 Mbps @ 2.4 GHz | 270 Mbps @ 5GHz/54 Mbps @ 2.4 GHz

Netgear's WNDR3300 isn't as solid a 802.11n router as we hoped to see.

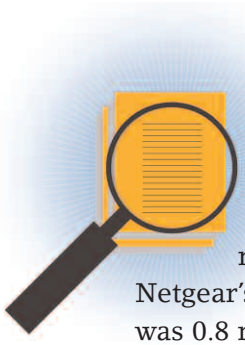


Although security typically means remembering annoying passwords, Netgear supports Wi-Fi protected setup—which it calls "Push 'N' Connect." Basically, press the button on the router, then press the WPS (or would that be "P'N'C"?) button on the adapter—if it has one. The two devices will talk it over as the router configures the adapter to work correctly.

Of course, if you have a wireless adapter like Netgear's WNDA3100 USB device that doesn't have a WPS button, you'll need to follow along with the installation wizard you'll find on the provided disc—and you'll also need to remember the annoying password—at least once. Other than that, the whole process is simplicity itself.

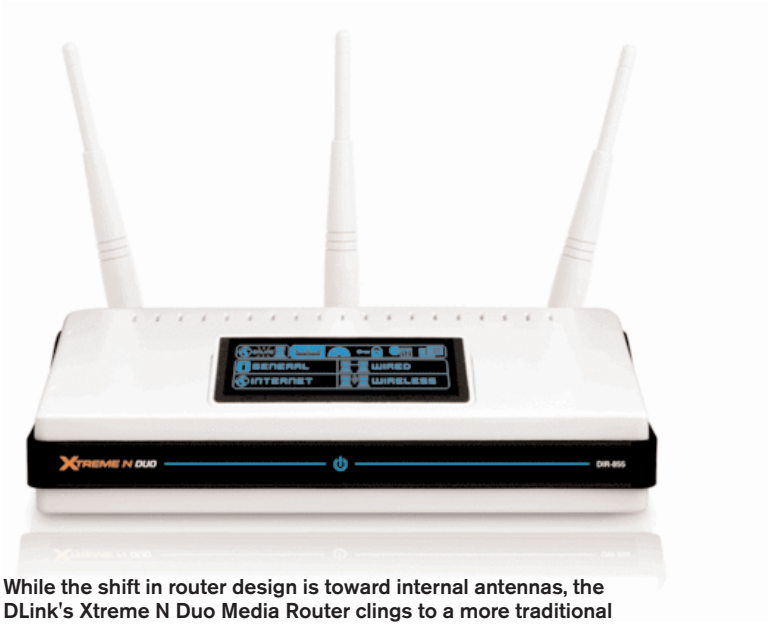
All of the possible connectivity options made the WNDR3300 a bear to test. In fact, we ran it through the mill three times, once at 270 Mbps @ 2.4 GHz, once 130 Mbps @ 2.4 GHz, and finally 270 Mbps @ 5GHz/54 Mbps @ 2.4 GHz.

Its most impressive performances were in the



2.4-GHz band, where it transferred our 873-MB test file in 1.9 minutes and two minutes at a rated 270 Mbps and 130 Mbps, respectively. It was not noteworthy in any other testing venue. Netgear's own WNHDE111 gaming AP/bridge was 0.8 minutes faster at 5 GHz.

If experience is any teacher, at some point between now and when 80.11n is finally ratified, Netgear will release a rock-solid router with all the expected bells and whistles. The WNDR3300 isn't it.



While the shift in router design is toward internal antennas, the DLink's Xtreme N Duo Media Router clings to a more traditional design with three external antennas.

D-LINK XTREME N DUO MEDIA ROUTER

D-Link offers a simultaneous dual-band router called the Xtreme N Duo Media Router DIR-855. "Simultaneous," of course, means that you can access both bands at the same time—effectively setting up a situation where you can use the 2.4-GHz band for your usual data files and tap into the less crowded 5-GHz band for your media needs. That's the theory.

D-Link's installation software is plain English, question and answer, and so meticulous to detail that it's almost tediously annoying. When it's done, especially if you also agree to use the trial version of Network Magic, you're not only up and running but you're also monitoring your network's performance via daily e-mail reports. (For the geekier among us, you can access all of the router's features via a browser-based based interface. As you might suspect, that approach offers access to a somewhat more comprehensive feature set.)

On the hardware end, the rectangular white box lies flat by design. The network activity display would be otherwise difficult to read if the router was set up sideways on blocks. That display provides an easily readable status panel for the router, but you may never have a need for it after the initial installation (although maybe not even then) and doubly so if you're using Network Magic.

While the shift seems to be toward internal antennas, the Xtreme N Duo Media Router clings to a more traditional design of three external antennas. The plus factor to the arrangement is that they are removable and can be replaced with range-increasing alternatives. The minus is that they tend to crowd the back panel connectors somewhat for those who are proud to be ham-handed.

Dlink's Xtreme N Duo

FEATURES:
Dual Band: Simultaneous
Firewall: Yes
Data Stream Management: Yes
Wi-Fi Protected Setup: Yes
Antennas: 3
Number of Switch Ports: 4
Port Speed: 10/100/1000
USB Port: Disk
Dimensions: 4.6 x 7.6 x 1.2 in

TEST RESULTS (IN MINUTES)
Proprietary 2.4 GHz: 3.5
Proprietary 5 GHz: 2.0
Netgear N121T: N/A
Netgear 5GHz HD: 1.6

Performance was a bit scattered for the DIR-855. It did its worst work transferring our 873-MB test file at 2.4 GHz through D-Link's own Xtreme N Dual Band USB Adapter DWA-160. At 5 GHZ, the DIR-855 fell behind leaders Apple and Linksys by almost half a minute. Surprisingly, it and our old Netgear N121T USB adapter refused to talk to each other in any meaningful way. Windows pegged the file-transfer time at greater than 30 minutes and terminated the process after five. It worked well with our pair of Netgear WNHDE111 HD gaming adapters, turning in a 1.6-minute time to transfer our test file, but that was 0.4 minutes faster than this simultaneous router could muster on its own.

We really can't recommend the DIR-855 at this point. The price is close to $300 for just the router (the DWA-160 is about $90 additional) at retail sites recommended by D-Link and there's just not that much here to merit that kind of pricing. If the plain English display was effective for the router's operation, we could understand—and agree—with the pricing. Novelty items are always extra but they should be optional.

LINKSYS WRT610N

It took a few seconds to figure out how to turn off the audio track Linksys uses on the WRT610N product site. A sound-enabling Web page is generally considered a slick feature and, as such, it certainly matches the slick appearance of the router itself—think rear end of a Mitsubishi Eclipse with wrap-around spoiler. The audio track is just oh-so-annoying if you know how to read and prefer to do that instead.

Setup is fairly straightforward and in plain English. When you're done you're up and running with a simultaneous dual-band router—maybe. During our initial testing, file transfer at both 2.4 GHz and 5 GHz lost connection and terminated. Then, after about a half hour, none of the computers we tried could find the 5-GHz band on our first WRT610N. We went through a variety of possible fixes (including a firmware upgrade) with Linksys technical support, but nothing worked. So we had it replaced with another one.

The second WRT610N already had its firmware upgraded and agreed to talk with the

Linksys WRT610N

FEATURES:
Dual Band: Simultaneous
Firewall: Yes
Data Stream Management: Yes
Wi-Fi Protected Setup: Yes
Antennas: 3 per band
Number of Switch Ports: 4
Port Speed: 10/100/1000
USB Port: Disk
Dimensions: 8.9 x 7.1 x 1.48 in

TEST RESULTS (IN MINUTES)
Proprietary 2.4 GHz: 2.6
Proprietary 5 GHz: 1.6
Netgear N121T: 2.2
Netgear 5GHz HD: 1.5

During our initial testing, file transfer using the Linksys WRT610N at both 2.4GHz and 5GHz lost connection and terminated. Things continued to carry on in that manner.

Linksys WUSB600N USB adapter. Unfortunately, when we called up our list of attached computers via the Windows Network icon, the PC that was hard-wired to the router was nowhere to be found in the list. It took another contact with technical support to cure that problem, but then media playback at 5 GHz got splotchy.

Things continued to carry on in that manner, to the point that we finally asked if the router might still be a beta model and not a production unit. We were told that it was definitely a retail product. That wasn't a great answer, considering how it was acting, and, when testing was done, we ran—not walked—to our router closet and re-installed the WRT600N we'd been using for the last seven months or so.

We can't over-emphasize that we have never had problems with any Linksys router similar to the degree we experienced with the WRT610N. When it worked correctly, it proved itself to be one of the top two (tied with Apple's Airport Extreme) devices in performance. But we felt the need to cross our fingers for luck whenever we walked away from it. We just had no confidence that we'd return to the same conditions as when we left.

On the bright side, a pair of Linksys WGA600N dual-band gaming adapters worked perfectly to create a simultaneous dual-band environment with the older WRT600N. They were the equals of the Netgear WNHDE111 devices we've been using.

As with D-Link, it's difficult to recommend the WRT610N at this point. The WGA600N and WUSB600N adapters are champs if you want to add them to and expand your existing network but, as things stand right now, that's just a two-legged simultaneous dual-band Linksys stool.

Dual Band Router Features

	Dual Band	Firewall	Data Stream Management	Wi-Fi Protected Setup (WPS)	Antennas	Number of Switch Ports	Port Speed	USB Port	Dimensions
SMC Barricade	No	Yes	Yes	Yes	3	4	10/100	Printer	7.1 x 4.8 x 1.2 in
Apple Airport Extreme	Either/Or	Yes	No	Yes	3	3	10/100/1000	Printer/Disk	6.5 x 6.5 x 1.3 in
Netgear WNDR3300	Either/Or	Yes	Yes	Yes	8	4	10/100	No	8.8 x 6.0 x 1.2 in
D-Link DIR-855	Simultaneous	Yes	Yes	Yes	3	4	10/100/1000	Disk	4.6 x 7.6 x 1.2 in
Linksys WRT610N	Simultaneous	Yes	Yes	Yes	3 per band	4	10/100/1000	Disk	8.9 x 7.1 x 1.48 in

Dual Band Router Test Results

	SMC	Apple	Netgear	Netgear	Netgear	D-Link	Linksys
Proprietary 2.4 GHz	3.5	2.5	1.9	2.0	N/A	3.5	2.6
Proprietary 5 GHz	N/A	1.5	N/A	N/A	2.3	2.0	1.6
Netgear N121T	2.2	2.7	3.0	2.3	4.3	N/A	2.2
Netgear 5 GHz HD	2.0	1.9	1.5	1.5	1.5	1.6	1.5

All times in minutes at one decimal place

Wireless Mesh

Well-Planned Rollouts Weave Tighter WLANs

By Michael Brandenburg

THE ETHERNET BACKBONE'S DAYS of enterprise dominance may be numbered. Enterprise mesh systems, while not eliminating the need for a wired link, are extending the network infrastructure well beyond Ethernet's reach.

Enterprise mesh's benefit is clear: pervasive connectivity throughout the organization. Unbound by the constraints of copper or fiber, wireless mesh enables enterprises to deliver ubiquitous access and services to parts of their facilities that previously were untouchable by their wired architectures, while managing it as a subset of their overall wireless architecture.

As technologies such as voice over wireless LAN and better handheld devices make their way into enterprises, pervasive wireless coverage, including previously ignored areas such as stairwells and break rooms, will become more business-critical.

Wireless mesh systems also let a network team quickly react to changing business demands with reusable resources. For example, meshed access points can be quickly deployed to provide network access in temporary office space or during special events such as trade shows, and just as easily pulled back when the extra capacity is no longer needed.

So why isn't every corporate net meshed up? Roadblocks remain. First, some WLAN vendors treat enterprise mesh as a premium feature, requiring additional licensing and fees. Second, many vendors limit mesh to specific access point models within their lineups. Typical mesh deployments require a dual-radio access point, with one radio serving clients and the other acting as a wireless backhaul. This is a particularly critical detail in 802.11n deployments, where new wireless devices might be forced onto the same radio frequency as older 802.11b/g clients.

WLAN vendors such as Aruba Networks, Cisco, Meru Networks, and Trapeze Networks take a structured approach in their mesh offerings. Under these plans, both indoor and outdoor access points can be defined and configured as mesh nodes within the network planning tools. With the Ethernet port on the access point now available, a node can serve wireless clients and bridge wired networks. Mesh allows an organization to manage the entire wireless network as a single entity.

Some vendors, notably Motorola and startup Aerohive Networks, offer a dynamic approach focused on wireless network resiliency and connectivity options. Access points from these vendors automatically provision a mesh network in the event of wired switch failure, delivering data through another access point to maintain the connection, without administrator intervention. Aerohive and Motorola access points have this adaptive capability built in—thus making it a standard feature. Both companies are betting that a no-cost wireless mesh option will give them a competitive advantage, as well as drive greater adoption of the technology.

THE LOWDOWN

›› THE PROMISE Wireless mesh systems are no longer the sole domain of wireless ISPs and municipal Wi-Fi projects, but are now in reach of the enterprise. Mesh will extend enterprise wireless LANs to areas previously unreachable and can build resiliency and failover into the corporate wireless network.

›› THE PLAYERS Almost all the wireless vendors, including Aruba, Cisco, Meru, and Motorola, have built some level of enterprise mesh into their WLAN offerings, as have startups such as Aerohive. Enterprise mesh is well on its way to being a standard option available on enterprise WLAN solutions—for a price.

›› THE PROSPECTS Enterprise mesh is an excellent addition for any wireless engineer's toolbox. By extending the WLAN beyond the reach of Ethernet cabling, as well as building resiliency and flexibility into 802.11 solutions, mesh opens the door to truly pervasive wireless coverage in the enterprise and offers the flexibility to adapt to changing business environments.

Cut The Cord

Get Ready For A Wire-Free Enterprise

By Frank Bulk

IT'S AN OVERSIMPLIFICATION to say that 802.11n heralds the era of the wire-free office—though with top speeds of up to 300 Mbps, it's clearly a catalyst for cutting the cords that tether users to their desks. Yet there's no question that within a few years, Wi-Fi will become the new network edge for companies interested in saving money, attracting top

talent, and increasing security.

Of course, pure-play wireless LAN vendors have been saying for a while now that wired Ethernet to the desktop is dead, despite lingering concerns about reliability, the suitability of WLANs for telephony, the complexity of managing mixed wireless and wired networks, branch office and teleworker support … and, oh yeah, the fact that the legacy infrastructure is chugging along just fine.

Business technology managers have long weighed these factors against the most touted benefit of Wi-Fi: increased productivity. The efficiency studies are many and the refrain generally the same: Wireless keeps information at employees' fingertips, enables quicker decision making, reduces downtime, and enables collaboration. But in today's tight economic environment, the savings picture is just as compelling. Intel estimates—and we agree—that moving to a largely wireless network can reduce capital costs 40% to 50% and operational costs 20% to 30%. Luc Roy, VP of enterprise mobility at Siemens Enterprise Communications, cites a Canadian government customer that's saving $500 per event for moves, additions, and changes.

With the rising price of all modes of travel, teleworking is looking mighty attractive as well, and IT can now extend wireless to remote sites. Aruba Networks recently announced an access point, developed with Avaya and called the

Impact Assessment: 802.11n And The Wire-Free Office

	Benefit	Risk
IT organization	802.11n delivers speeds that exceed 100 Mbps to the desktop while enhancing reliability and coverage. Capital and operational savings over wired connections if the legacy infrastructure is fully depreciated and can be mostly turned off.	The 802.11n standard has not yet been ratified by the IEEE; moving early may mean higher prices and immature chipsets. Because wired networks are not going away anytime soon, it's another set of equipment to manage.
Business organization	Unchaining an end user's tools (laptop and phone) from her desk should increase productivity by enabling anyplace access.	A poorly functioning wireless network can lead to user frustration. Some employees may feel uncomfortable taking communication tools out of offices and won't readily change work patterns.
Business competitiveness	Companies are all about doing more with less. A wire-free office based on 802.11n will cost less than a comparable wired LAN, freeing up cash. Security is improved as well.	Offices with WLANs for primary network access are relatively rare, and productivity increases aren't guaranteed. This is one competitive difference that can be easily duplicated.

Bottom Line

While the 802.11n standard isn't yet ratified, the Wi-Fi Alliance's certification should put most worries to rest. Because the 802.11n market is so nascent, businesses can gain a first-mover advantage thanks to operational savings. Still, Wi-Fi is still more a black art than wired Ethernet. That said, the productivity, cost savings, and flexibility benefits are compelling.

Mobile Remote Access Point, that can use any broadband connection to provide secure access to business resources for both data and voice. All the employee needs is a single- or dual-mode phone, or a softphone on a wireless laptop. Remote and branch offices also are obvious places to take advantage of all-wireless access, especially as management tools emerge for monitoring mixed-vendor WLANs (see story, p. 20).

Cisco Systems, Motorola, and others now offer 3G interfaces that can provide backups for branch offices and locations with minimal WAN connectivity, or for failover of critical applications. And WLAN security can beat that of most wired LANs—yes, you read that right. Sites looking into desktop virtualization should do fine on an all-Wi-Fi network as well, thanks to the small packet sizes inherent in virtual desktop infrastructures.

Motorola sees 802.11n as an inflection point in the industry and has adopted the slogan "Wireless by default and wired by exception." It and other vendors are practicing what they preach, deploying ubiquitous WLANs in their own offices.

SHOULD YOU FOLLOW SUIT?

Although wireless vendors such as Motorola are happy to promote the wire-free office concept, Ethernet switch sellers, including Cisco and Hewlett-Packard, approach the concept with caution. That's not surprising: Switch vendors stand to lose big money as we move away from Ethernet to the desktop. Even if companies pay the manufacturer's suggested retail price for enterprise-class 802.11n gear, it's still much less expensive per user than a new 10/100/1,000-Mbps switch deployment with $250-per-drop wiring costs.

CAREFUL STEPS

But don't feel too bad for Cisco—no enterprise WLAN vendor is claiming to replace wire at the core or distribution layers, and besides its wire-side dominance, Cisco owns more than half of

Copper Costs Lots Of Pretty Pennies

IN A REPORT LAST YEAR, Gartner analyst Ken Dulaney predicted that by the end of 2011, 70% of all new worldwide voice and data client-to-LAN connections will be wireless. The firm also estimated that $100 billion will be wasted over the coming five years following outdated network design principles.

Included in that figure is Gigabit Ethernet to the desktop.

The takeaway is that all organizations need to ask a fundamental question: "What is our strategic platform for network access connectivity?" If the answer isn't "wireless," you need to take a hard look at up-front and ongoing costs—and possibly reconsider your stance. In our experience, wiring Ethernet commonly hovers around $250 per drop, though site-specific considerations such as a historical building or union labor can double or triple that cost. Once you've paid for the copper wire, there are edge Ethernet switches to consider at anywhere from $50 to $100 per port.

According to Motorola, which admittedly has a stake in this game, a wired network costs $88 per user per year for maintenance and support, compared with $12.51 for a WLAN. While that might be a bit optimistic, there's no way around the fact that purposing a single wired Ethernet port and cable to serve many clients via an access point does in fact translate to significant savings.

While you'll still pay a premium for 802.11n APs—Cisco's new 11n 1250 AP was priced at $1,299 for the dual-radio version we tested recently—we expect prices to drop over the coming year.

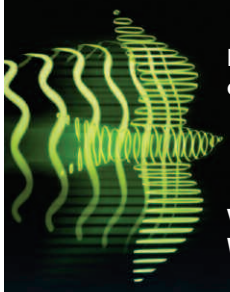
the enterprise WLAN market with its wireless gear set, originally from Aironet and later supplemented with its Airespace acquisition. Chris Kozup, manager for mobility solutions at Cisco, emphasizes that the company is making the most of its leadership in both wired and wireless with a "unified" network approach that blankets the office with Wi-Fi while keeping a few wired ports at every workstation. Nice if you can afford it. Cisco is clearly cautious in its pronouncements regarding the all-wireless office. Don't look to the WLAN gear leader to be in front of this charge.

No. 2 switch vendor HP, which mixes some of its own Wi-Fi gear with licensed technology, is also approaching the all-wireless office carefully. Andre Kindness, Americas security and mobility solution manager for ProCurve networking, says HP's customers are driving that stance. Companies are looking to reduce their operational costs through a consistent management system that covers both wireline and wireless and provides product longevity, Kindness says. However, such management does not yet exist. Cisco talks about a unified network, but it's not yet providing integrated management. HP openly discussed the problem of inconsistent management tools between wired and wireless networks, and we see it making the most credible progress of any of the "we do both wired and wireless" players. Other vendors looking to cover these bases include Nortel Networks, which says it's developing its own 802.11n gear—essentially shunning its OEM partner, Trapeze Networks—and Enterasys, Extreme Networks, Foundry Networks, and Juniper Networks, all of which are OEMs or resell wireless products.

Meanwhile, overlay vendors such as Aruba, Motorola, and Trapeze treat the wired network as more or less a dumb transport for their wireless traffic. It makes for easier sales to the wireless-oriented parties in IT organizations, but this stance leaves those who must manage both with a less-than-easy feeling.

Another angle enterprise switch vendors play is to suggest that all-wireless is a better fit for the remote or branch office, rather than main sites, appealing to interest in this architecture while protecting their wire-side revenue. Most also deliver some variation on the message that IT should be about "providing flexibility to the business"—in other words, preserving wired connectivity where it exists and delivering wireless where it's wanted. Tim Purves, CTO of

Voice Options For The Wire-Free Office



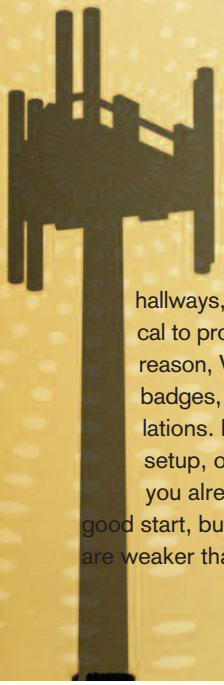
	PROS	CONS
Softphone on laptop	Works anywhere with wired or wireless connection; wide PBX support	Laptop must be on to take a call; requires headset or earpiece
Mobile cellular phone	Form factor and experience well-understood by users; variety of providers and pricing plans	Indoor coverage typically challenging; no PBX integration; may not be acceptable for regulated industries
Voice-over-Wi-Fi handset	Truly portable voice option; coverage wherever your WLAN reaches	Few PBX vendors offer Vo-Fi systems; requires strict attention to RF design
e-FMC phone that supports cellular and Wi-Fi	Best of both worlds	Usually requires integration and sophisticated handsets; nascent market

the Henry Ford Health System in Detroit, says it's his department's aim to "align technology with business workflow processes." While that's a familiar mantra, if those processes are tied to immobile approaches that ignore the productivity increases and workflow improvements possible via a pervasive wireless network, IT must step up and champion a new way forward.

Talk Vo-Fi To Me

VOICE SERVICES ARE A SIGNIFICANT sticking point for companies considering an all-wireless office. Voice over Wi-Fi is still in its infancy. Fixed-mobile convergence using a dual-mode handset is another approach, but that technology and market are no more mature than Vo-Fi. Standardizing on cellular voice services is also a possibility, but that requires good in-building coverage, something rarely found in North America without investing in special gear, such as femtocells.

Until the voice question is definitively answered, organizations have good reason to be cautious.



Even if Vo-Fi isn't yet on your radar, your WLAN needs to be designed to support quality of service and multiple applications (data, voice, and video). While wired networks need the same type of planning, the added latency of the air and that fact that Wi-Fi is a shared medium require specific attention. And QoS won't help you if the radio in the employee's Vo-Fi phone can't connect. Building the wireless network to saturate all locations, including hallways, elevators, stairwells, and utility closets, is critical to providing complete in-building coverage. For that reason, Vocera, well known for its *Star Trek*-like voice badges, uses AirMagnet's VoFi Analyzer in all its installations. Depending on your building's location and setup, outdoor coverage may be required as well. If you already perform post-installation surveys, that's a good start, but remember that the radios in Vo-Fi phones are weaker than the clients built into most laptops.

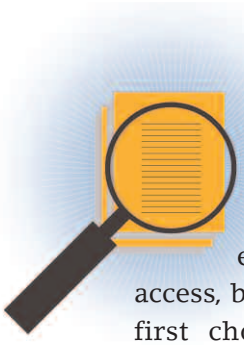
—FRANK BULK

Fortunately, not all enterprise switch vendors are stonewalling. Trent Waterhouse, VP of marketing for Enterasys, says his company sees wireless as a strategic component of its business and is evaluating WLAN players with an eye toward an acquisition. Juniper is shopping around, too; it was spurned by Meru Networks, which also acts as an OEM for Foundry, on at least one occasion, say industry sources. No matter—Aerohive, Bluesocket, Colubris, and Xirrus stand out as attractive acquisition targets for enterprise switch vendors that lack their own wireless products. Trapeze might be a good fit for Nortel, if it decides to turn to its former OEM partner rather than build its own 802.11n gear.

MAKE THE MOVE

Truly transforming the workspace extends beyond installing access points and providing laptops, to physical reconfiguration. Take Capital One's Future of Work program. The financial services firm's 360-acre, eight-building campus almost doubled the number of employees it could house, from 650 to 1,100, by adopting the concept of hoteling. Rather than being assigned a specific location, employees who participate in this optional program have access to a generic cubicle, as well as conference rooms and open areas. Space is essentially overbooked. Each employee is assigned a telephone number that flows to a Cisco voice-over-IP phone and/or BlackBerry. The WLAN is the primary medium for network access.

"Today, work is what you do, not a place you go," says Rob Alexander, Capital One's CIO. "The wireless and mobile technologies we provide through our Future of Work environment provide our associates greater flexibility in how and where they work, which in turn improves collaboration and productivity." Employees are happy, and the company saves big on facilities.



Intel takes a similar approach at its Jones Farm, Ore., campus. This location serves almost 6,000 employees using Cisco wireless gear. Intel started with an overlay network for wireless access, but as Wi-Fi caught on, it's become the first choice for employees. In addition to Centrino-based laptops (of course), Intel also uses Cisco Wi-Fi phones for voice services, as well as softphones and dual-mode devices.

Cisco has its own initiative, called the Connected Workspace. In line with its preferred converged approach, wireless is deployed everywhere, but wired ports for high-bandwidth communications needs, such as backups and video streaming, also are available. Still, the company has cut its need for copper by 60%. "The Connected Workspace encourages collaboration and reduces real estate and infrastructure costs, while accommodating different work styles," Cisco's Kozup says.

Aruba and Motorola have been the most vocal vendor supporters of the wire-free office. With no wired revenue to lose, they can only gain by stealing away dollars that would normally be spent on their competitors' Ethernet switches. With 802.11n offering comparable performance to a wired network, but with added mobility, they have a strong argument.

Of course, the wireless office is like the paperless office—though electronic documents and e-mail have become the main forms of information storage and redistribution, there's still paper exchanged in the postal mail. In the same way, wireless will become the primary connection only at the access layer. "'All wireless' is a bit of a misnomer," says Kozup. There will still be cables, but they'll reside predominately in the distribution and core layers of the network, unseen by the average user.

SECURITY MATTERS

The security breach at TJ Maxx parent TJX, where attackers took advantage of a wireless connection secured only with Wired Equivalent Privacy to capture credit card information on tens of millions of the retailer's customers, remains fresh in many CIOs' minds. The fact that the key element in that equation is "secured only with WEP" is a detail easily ignored by the security paranoid.

Done right, Wi-Fi can be deployed with greater security than wired networks, which often leave ports unprotected in cubicles and conference rooms. Because security concerns have long been a drag on WLAN adoption rates, it's now standard form to use 802.1X to ascertain a connection's user credentials and the Advanced Encryption Standard to encrypt traffic until it reaches a wireless controller in the data center or at the network edge. Those still using a VPN overlay on an open wireless network, take note: Unless you have specific application requirements or hardware limitations, now is the time to move to 802.1X with AES.

A wireless network's greatest vulnerability is in performance-degrading interference or denial-of-service techniques, some facilitated by options in the 802.11n standard. Your wireless infrastructure management system may be able to pinpoint the source of malicious traffic, or else a product from an overlay wireless intrusion-prevention system vendor like AirDefense, AirMagnet, or AirTight can do that and more. Work on the 802.11w standard is progressing to offer management frame protection, among other capabilities, to fill gaps.

PEOPLE, GET READY

If you have some sentimental attachment to the copper feeding your desktop, consider that your future workforce has spent the past four years

in a wireless oasis. Most colleges and universities provide Wi-Fi in a substantial portion of their classrooms and public spaces, some in their dorms. Freshly minted graduates expect mobility when they step into the workforce, and that starts with Wi-Fi access in the office.

If businesses want to attract young talent, staying on the cutting edge isn't optional. To see how close we can come to going wire-free, we broke down wireless communication into three areas: data, voice, and video.

Conventional office applications account for the majority of data access. Whether e-mail, productivity suites, or line-of-business applications, data apps consume the largest amount of a knowledge worker's time and have been successfully mobilized, in and out of the office.

Wireless voice is often thought of in terms of cellular services, but voice over Wi-Fi, or Vo-Fi, increasingly is considered a key application for wireless networks. CIOs are generally cautious about running voice over their enterprise WLANs, for good reason: Unless the wireless network was engineered with voice in mind, whether it be first- or third-generation gear, poorly implemented quality-of-service functions and a weak signal will lead to disappointed users. All the major WLAN infrastructure vendors have spent considerable time working with enterprise-class Vo-Fi providers, such as Cisco, Polycom (formerly SpectraLink), and Vocera, developing deployment guides to assist VARs and IT groups with configuring the WLAN for QoS.

Wireless video, which generates much higher traffic volumes than voice, requires special consideration as well. Although we don't see enterprises deploying Cisco's TelePresence over Wi-Fi anytime soon, video-based corporate training and closed-circuit television for both inside cameras and those mounted in the parking lot are here now.

Not all apps can be neatly siloed into voice, video, and data. Environmental controls and security monitoring can also be performed wirelessly, eliminating time-consuming and expensive installations. Services such as location and presence increase productivity and security. We're in the midst of a Rolling Review covering location systems, and we like what we see; check out our findings at informationweek.com/rollingreviews.

NEED FOR SPEED

Throughput is the first consideration when it comes to network connectivity, and 802.11n delivers: Both vendor and independent tests have shown that peak rates upward of 130 Mbps are achievable in good conditions. Advanced antenna designs, spatial streams, and multiple input/multiple output (MIMO) technology mean 11n also offers better coverage and improved radio frequency reliability and consistency. Access points can be spaced farther apart, if desired, but the better signal may more effectively be used to achieve higher access rates. Multipath, which previously degraded signal quality, is now used to good effect by MIMO to reduce the effects of fading and interference.

There are other benefits of 802.11n. First, it's essentially the fourth generation of the 802.11 standard, yet despite the evolution, each revision is backward compatible on both clients and access points, albeit at lowest common denominator rates. Companies can upgrade gradually because 802.11n clients work with 802.11a/b/g APs, and vice versa.

Second, as the market developed, amendments have been added to address deficiencies in the original 802.11 specification. The most significant are 802.11i, which deals with security, and 802.11e, which introduced quality-of-service features. Architectural approaches also have broadened. First-generation access points were standalone, with little to assist IT in terms of scalability, RF management, and Layer 3 roaming. Startups generally swung to the opposite extreme and centralized everything, leading to what pundits called "thin" APs.

With development of 802.11n and its higher traffic rates, a more sensible distributed approach, first used by Colubris in 2005, has evolved. The management plane remains centralized, as is common in any enterprise service framework, but the control and data planes can be placed at the core, edge switch, or access point. Motorola calls this "adaptive AP," while Trapeze has taken the moniker "Smart Mobile." Even Aruba, with its emphasis on centralized data flows, provides flexibility as described earlier with its Mobile Remote Access Point. Even if the WAN link is interrupted, connections stay up and local traffic will continue to be switched locally.

With 802.11n just around the corner, early adopters whose 802.11b/g gear is nearing end of life face a conundrum: Pay top dollar for 802.11n, stick with b/g, or add 802.11a support to their access points by buying new gear or moving to a different vendor. While 802.11a buys some advantages, at this point we recommend sitting tight until prices, AP maturity, and/or standard adoption are such that you feel comfortable upgrading to 802.11n. In fact, Aruba has a new marketing pitch: Buy its 802.11a/b/g APs today, and buy a key later to activate 802.11n. This approach helps customers split their costs over time—and assures Aruba market share.

It doesn't help purchasing decisions that the 802.11n standard isn't complete. Working group approval is tentatively scheduled for March 2009, many months past predictions. Vendor adoption of the draft 2.0 spec, along with all the pre-standard chipsets already in use, make it highly unlikely that a final standard that's incompatible with existing products will be adopted. Nevertheless, we can't argue the logic of waiting. Second-generation standards-based 802.11n products, even if functionality equivalent, will have many of the bugs and kinks—for example, 802.3af Power over Ethernet support—worked out. Prices will drop, and processes regarding site planning, installation, and maintenance will be better defined.

Enterprise network administrators also are concerned about reliability. Will that unforgiving terminal session or enterprise application drop every time the microwave goes on in the cafeteria? There remain a plethora of wireless supplicants, and connectivity is still not as certain as with Ethernet. With proper device selection and configuration, connectivity bugs can be minimized, but there's still room for improvement. Most users will trade a few connectivity blips for mobility. Some won't.

GOTCHAS REMAIN

Despite all the performance and other benefits of 802.11n, there are still questions about reliability, performance, legacy devices, integration into the existing wire-centric infrastructure, and market dynamics.

RF remains a black art, and although MIMO makes Wi-Fi more reliable, it's still no guarantee that interference won't interrupt. For starters, good planning is required, perhaps using a

tool such as Cisco's Spectrum Expert (formerly Cognio), which identifies possible sources of interference. There are also architectural approaches to address the reliability problem. Meru's newest 802.11n access point, the AP400, was designed for robustness. Its four built-in radios can operate simultaneously, on different channels; interference on one channel or band doesn't prevent a client from roaming to another radio. Another approach, used by Ruckus Wireless and Xirrus, is to employ directional antennas. These approaches are still considered a bit unconventional, but they're worth watching.

If aggregate performance is a key issue, legacy clients that operate only in 802.11b mode may need to be replaced or upgraded. That's not always possible with older Vo-Fi handsets, portable scanners, and other application-specific devices. In these cases, moving nonlegacy clients to the 5-GHz band, where there's great channel selection and support for multiple 40-MHz channels, may be prudent. That way, the legacy clients won't impact the peak-performance capabilities of the 802.11n-capable gear.

The challenge of consistent network management between wired and wireless networks is also vexing. Even Cisco, which leads in market share in both segments, doesn't have a management interface between both platforms. As HP points out, enterprises aren't eager to layer on a different set of intrusion-detection and -prevention systems, security, and network-access control tools for the wireless environment. For now, you will need different sets of tools for managing wired and wireless networks, so for organizations that do both, back-end support costs will rise, not fall.

Mixed WLANs

AirWave Provides The Management Tools

By Lee Badman

THE WIRELESS NETWORKING MARKET is changing at a dizzying pace, with once-cutting-edge hardware sets becoming legacy gear in the blink of an eye. The result: Many companies—especially those working toward all-wireless offices—find themselves proud owners of mixed-vendor wireless LANs.

To address management of these networks, AirWave, which was acquired by Aruba Networks in January for $37 million, brings a new mix of tools to version 6.0 of its multivendor Wireless Management Suite, or AWMS. While the suite doesn't have all the pieces required to completely replace vendor-specific tools, it's the closest we've seen to a heterogeneous WLAN management product.

We tested a beta version of AWMS 6.0 at our Syracuse University Real-World Labs. The new code handled a fair portion of the campus' Lightweight

Access Point Protocol (LWAPP)-based production AirOrange Network. With AWMS 6.0 managing or monitoring IOS-based point-to-point bridges, LWAPP and Aruba 802.11n access points, Radius servers, a Cisco Wireless LAN Solution Engine, a variety of network switches, and hundreds of clients, it didn't take long to see the value proposition. We also gave the product full configuration control over several test devices in a nonproduction lab environment. AWMS supports new 802.11n access points from Cisco Systems and Aruba, and support for 802.11n gear from Meru and others is due soon. As in previous AWMS versions, the complete list of wireless products supported reads like a who's who in the wireless industry, including mesh and WiMax product sets from 3Com, Tropos, and almost everyone in between.

RIGHT ON SCHEDULE

One of the most valuable features in any wireless management system is the ability to schedule tasks. In this regard, AWMS shines. New to 6.0 is the ability to specify standard date/time formats, and we found greater flexibility in planning downtime, a must-have capability given that most production WLANs have become critical resources.

Also new in Wireless Management Suite 6.0, AirWave provides help-desk functionality to go with its hardware management capabilities. For example, if a wireless user can't authenticate to a secure wireless network segment, first-level responders with role-appropriate AWMS access can capture symptoms and feedback with screen shots and annotations that can be integrated with systems like Remedy Service Desk or used within AWMS.

When we induced failures during testing, AWMS revealed a wealth of information, enabling better and quicker escalation. And for large companies with several wireless networks spread out across multiple geographic areas, enhancements made to the Master Console architecture allow distributed AWMS systems to be controlled from a central location.

AWMS 5.0's VisualRF module was quite clunky. In 6.0, VisualRF has improved; for example, the SVG format has given way to Flash for expanded browser compatibility. AirWave also heeded the call for easier floor-plan imports by adding native support for bulk import of CAD files, and AP placement may be carried over if provisioned properly.

AirWave provides robust client location services, and recognizing increased use of radio frequency identification, the Wireless Management Suite now supports tracking of AeroScout RFID tags when used with Cisco LWAPP controllers.

As with other network management tools, bringing AWMS to a functional state requires discovering devices and building profiles, policies, and the general management framework for a given environment. AWMS is fairly intuitive in this regard, and it was a swift process getting our devices found and managed.

Still, while AirWave has made great strides with Wireless Management Suite 6.0, it isn't yet a full replacement for vendor-specific management platforms. Searching for a client device in AWMS is just as easy as doing it in Cisco's Wireless Control System—but if you need to push a configuration template to an LWAPP controller that's denying the client WLAN access, AWMS can't help. Same with configuring access control lists available through Wireless Control System's proprietary mechanisms—AWMS isn't there yet.

That said, for networks that use multiple wireless systems, and for those who aren't satisfied with the management products offered by their WLAN vendors, AirWave's Wireless Management Suite 6.0 provides an attractive alternative. The Professional Edition license lists for $36,995 and supports as many as 1,000 devices, including APs, controllers, routers, and switches. The master console is an additional $14,995.