InformationWeek
Research & Reports

WLANs: ONE SIZE DOES NOT FIT ALL

Need the growth potential afforded by wireless? We evaluated six WLANs suitable for small shops and branch offices

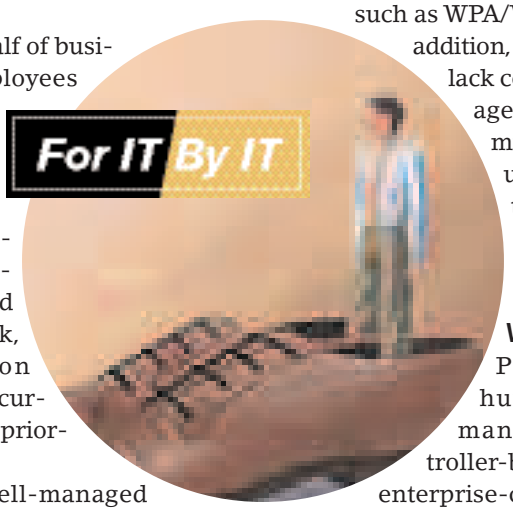
By Jameson Blandford

informationweek.com

Nov. 5, 2007

SMALL AND MIDSIZE ENTERPRISES that investigated Wi-Fi infrastructure gear even a year ago likely came away discouraged. Given a choice between high-priced, complex enterprise systems and bargain-basement standalone access points that your 12-year-old could configure, we don't blame you for figuring the rich get richer, the small get tethered to their desks.

In fact, you're not alone: Only half of businesses with fewer than 100 employees enjoy the benefits of wireless, according to a 2006 Forrester survey, compared with about 70% of companies with 500 to 1,000 workers. That's a competitive disadvantage that's tied to tech budgets. When an already constrained support staff is desktop, network, and application administration rolled into one, building—and securing—a wireless LAN is low on the priority list.



That's unfortunate because well-managed Wi-Fi burnishes your professional image in the eyes of customers and partners. And employees, used to having wireless at home and craving mobility at work, may be tempted to take matters into their own hands, creating security holes by connecting open rogue access points to your network. In addition, as 802.11n takes off, companies that haven't made forays into WLAN deployment will fall behind as the competition increasingly goes wireless.

Our advice: Today's 802.11a/g technology is more than sufficient for most organizations. Get moving, and by the time your bandwidth needs grow or your user base gets dense enough to benefit from 802.11n's throughput enhancements, second-generation, standardized 11n gear will be available. And you'll have a feel for your site and architecture requirements.

Why not save a few bucks and patch together a WLAN from some $100 access points you pick up at Best Buy? Because they don't have features crucial to business, like the ability to create multiple SSIDs on different virtual LANs, robust authentication mechanisms such as WPA/WPA2, and rogue-AP detection. In addition, devices for small and home offices lack centralized configuration and management capabilities, meaning even minor updates will require individual changes to each access point—talk about a management nightmare, especially if you support a few branch offices.

WHEREFORE WI-FI?

Plenty of companies with a few hundred employees want secure, manageable, easy-to-deploy, controller-based WLANs, with a base set of enterprise-class capabilities, at a reasonable price. Is that so much to ask?

To find out, we asked 16 WLAN vendors to send gear to our Syracuse University Real World Labs. Bluesocket submitted its BSC-600, D-Link sent us the DWS-3227P, and Motorola brought its WS5100. Netgear sent the WFS709TP system, Ruckus Wireless entered its ZoneDirector 1000, and 3Com rounded out the field with its 24-port Unified Wireless Switch.

Aerohive, Aruba, Trapeze and Xirrus declined, saying they do not target the SMB market. Cisco Systems, HP and Siemens said their products are currently between development cycles, while Meru pleaded a lack of resources to support the evaluation process. Although Cisco declined for this round, we've made a

few comparisons based on our recent review of its 526 Wireless Express Mobility Controller.

Interestingly, we found that these products come from two distinct backgrounds. Bluesocket and Motorola have long been players in the enterprise WLAN market and have essentially scaled down their enterprise-class systems. Netgear, historically viewed as targeting the consumer/SOHO market, fits into this category as well because its controller is an OEM version of Aruba Networks' 800-series branch office controller. Aruba's position as second in enterprise-class WLAN marketshare is a strong recommendation.

On the other side of the fence, Ruckus Wireless created its WLAN controller from the ground up, while both 3Com and D-Link use third-party controller and AP software from Nexthop Technologies on their respective hardware platforms. Each approach has merits, but we found that products originally focused on the enterprise offer in-depth customization abilities that, while nice to have, may overwhelm an IT staff making its first foray into Wi-Fi.

VAR, OR IS IT ON PAR?

One decision point for an SME looking to deploy its first WLAN: Do you install, configure and maintain the system in-house or rely on a VAR for some or all of those services?

The in-house option offers the ability to customize the design and capabilities of the WLAN to closely to match your needs, though most VARs do offer custom tailoring, for a price. Maintaining the system in-house will ultimately give you more control and flexibility, but that also means training IT staff on yet another technology, possibly straining capacity. If other telecommunications services, such as dial-tone and wired infrastructure, are managed by a VAR, throwing in a WLAN may net cost savings by bundling services. In addition, a VAR may be able to leverage capabilities built into the infrastructure to aid in unifying the wired and wireless networks—especially enticing if voice over Wi-Fi is on your radar.

If in-house staff will be responsible for day-to-day management and security of the WLAN, overall ease of use becomes critical. All the systems we evaluated include automatic channel- and power-adjustment capabilities that allow each AP to periodically change RF parameters to deal with interference or coverage holes. For configuration, management and monitoring, all systems use a Web interface, but some offer a more interactive and real-time experience, especially useful for quickly evaluating the overall health of the wireless network. Ruckus Wireless excels here with simple navigation and a customizable drag-and-drop dashboard view. We also liked Motorola's powerful Java based-GUI and Netgear's configuration wizards geared toward common administration tasks.

Impact Assessment: SME WLAN Infrastructure

	Benefit	Risk
IT organization	Installing a WLAN can result in fewer wired ports to manage, but the Ethernet infrastructure won't disappear just yet.	Maintaining a WLAN is a big paradigm shift from simple Ethernet switches. Without in-house expertise or a VAR's help, problems can sink productivity.
Business organization	If they have access to information resources while on the move, employees can be productive when not at their desks. A plus for visitors and customers as well.	The ability to work anywhere isn't always a good thing. Set ground rules to ensure that employees aren't accessing sensitive data in public areas.
Business competitiveness	WLANs are being adopted by the competition at a rapid pace. If you don't have Wi-Fi, expect to play catch-up, especially in industries such as retail and manufacturing.	Some users will rely on Wi-Fi as their primary access medium, causing productivity to grind to a halt if the system goes down.

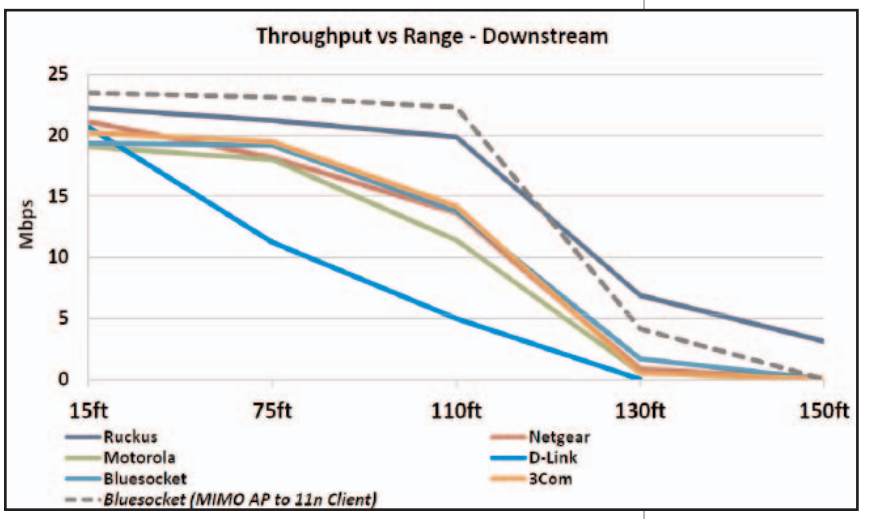
Bottom Line

WLAN infrastructure components based on 802.11a/b/g are fully baked today, and security is much improved. The various automatic adjustment and centralized configuration capabilities of the products we reviewed make deploying a WLAN for data services a low-risk endeavor, even for small shops.

Independent of your choice to self-manage or use a VAR, preinstallation services, such as a site survey, will go a long way toward ensuring your WLAN will be reliable and effective. Because Wi-Fi relies so heavily on proper AP placement and non-overlapping channel assignments, an improperly planned WLAN install can lead to poor user experience and significant troubleshooting overhead. Taking advantage of a VAR or integrator skilled in WLAN design can ensure that your coverage, application and user density requirements are met. Moreover, WLAN tools such as spectrum analyzers and coverage prediction software don't come cheap, so relying on a pro for installation will be less expensive than acquiring the paraphernalia to tackle the task yourself.

KEEP IT SAFE

Ensuring that private data remains private and that only authorized users are on your WLAN requires a base set of important security features that are common across all the products we evaluated.



First, WPA/WPA2 (Wi-Fi Protected Access) support allows full 802.1x authentication to a back-end RADIUS server, which may in turn reference a Microsoft Active Directory or LDAP store. Bluesocket, Motorola, Netgear and Ruckus up the ante by integrating a RADIUS server into the controller itself, a compelling feature for organizations without these servers on their networks. With this feature, IT can leverage an authentication scheme that ties WLAN access to an individual user account without requiring any additional hardware, because the actual user database is housed within the controller.

Although easier-to-configure authentication mechanisms requiring no RADIUS, such as WPA/WPA2-PSK (Pre-shared Key), do provide robust data encryption, they authenticate all users based on possession of a single global passphrase. This means individual user access can't be revoked without changing the passphrase and reconfiguring each WLAN client—a significant burden on IT each time an employee leaves.

Aiming to blend the user-based authentication of 802.1x and the simplicity of WPA-PSK without compromising security, Ruckus Wireless goes above and beyond the competition by offering what it calls "Dynamic PSK." Dynamic PSK provides encryption equivalent to WPA/WPA2-PSK, except the authentication passphrase is unique to each user and WLAN client, while requiring no special software on the client. By pairing this feature with Ruckus' "Zero-IT Activation" a user can simply plug in to the wired infrastructure, download an automatic WLAN provisioning tool from the Ruckus controller that contains her dynamically created passphrase, and voila—the help desk phone remains silent. For access revocation, simply remove the user's Dynamic PSK from the controller.

In addition to providing secure network access for employees, you may want to define a logically separate WLAN to allow visitors to get to public resources, such as the Internet or a corporate information page. All of the systems facilitate this scenario with the ability to tie a specific SSID to a wired VLAN within your network, but Bluesocket, Motorola, Netgear and Ruckus Wireless go one better, offering captive portal authentication designed with guest services in mind. Operating much like a hotspot-style authentication page, a captive portal prohibits users from accessing your network until they provide valid guest credentials or agree to a customizable network access policy. For guest-credential provisioning, vendors use either on-the-fly or bulk account creation that can be delegated, perhaps to a receptionist, to ease guest access distribution. We found Bluesocket's guest services the most well-rounded, including bandwidth throttling and extensive role-based access policies. This came as no surprise given the vendor's historic success in providing WLAN gateways for autonomous APs.

What You Get For The Money

We set up a pricing scenario comprising a single multifloor building requiring a total of 10 access points and one controller. All dollar amounts are list price.

	BLUESOCKET	D-LINK		MOTOROLA		NETGEAR		RUCKUS	3COM	
Supported WLAN standards	11a/g	11a/g	11g	11a/g	11g	11a/g	11g	11g	11a/g	11g or 11a
Controller	$1,995	$4,300	$4,300	$3,778	$3,778	$2,900	$2,900	$2,000	$2,750	$2,750
Max. number of APs	8-12	10	10	10	10	16	16	12	24	24
Per-AP price	$395	$349	$220	$345	$289	$240	$180	$349	$399	$249
Total	$5,945	$7,790	$6,500	$7,228	$6,668	$5,300	$4,700	$5,490	$6,740	$5,240

Worried about an employee punching a security hole in your network by connecting an unsanctioned AP with unauthenticated open access? Then you'll want rogue access point detection capabilities that enable the WLAN infrastructure to periodically search the airwaves for neighboring APs. Although all products present rogue devices in basic list format, Ruckus Wireless and Netgear integrate rogue location, displaying an approximate threat location on a building floor plan. We found these capabilities useful and fairly accurate, depending on the density of AP placement. Similar features are available for an addition fee from Bluesocket, via its BlueView Management System, and Motorola with its RF Management Software.

Rogue containment, albeit offering a proactive solution to the rogue problem, is a double-edged sword because it uses denial-of-service techniques to boot clients off the rogue. If improperly configured, this functionality may DoS not only rogues, but also any neighboring WLAN in your vicinity, so activate with caution lest your neighbors come knocking. Only Ruckus Wireless and Motorola don't include rogue containment, but a partnership between Motorola and AirDefense offers advanced WLAN IDS/IPS capabilities for an additional fee.

HARD DIFFERENCES

We asked vendors to send systems that use centralized controllers to configure and manage multiple APs, which should support power over Ethernet. In terms of physical hardware, the controllers varied significantly, from 3Com's and D-Link's devices featuring 24 PoE, Gigabit Ethernet ports plus managed wired capabilities worthy of an edge switch, to Bluesocket and Netgear with four and eight PoE ports, respectively. By building PoE ports into the controller, vendors can neutralize the cost of the multiple PoE injectors needed for APs to be functional via a single Ethernet cable. Although we highly recommend PoE, it is not required; most APs support standard AC power.

On the other end of the controller spectrum, Ruckus Wireless and Motorola sport dual Gigabit Ethernet interfaces with failover, representing a pure overlay setup similar in design to Cisco's SME WLAN offering. Notable extras include D-Link's 10Gig Ethernet XFP slot and stacking capabilities. That kind of bandwidth may be overkill, but it's comforting to know it's there.

In terms of AP hardware, common traits such as a Fast Ethernet PoE port and an 802.11b/g radio are available across the board. For more capacity, all vendors except Ruckus Wireless (and Cisco's current SME-class portfolio) offer dual-band 802.11a/b/g APs—but remember, per unit cost is directly related to the number of integrated radios, as is reflected in our pricing chart, above. If possible, splurge for dual-band. It essentially doubles your per-AP capacity, provided most WLAN clients are relatively recent.

In addition, all vendors support the external antennas used to provide coverage in challenging conditions, such as warehouses and industrial environments. Ruckus Wireless offered basic mesh capabilities, useful for situations where wired cable runs aren't feasible. Currently, Bluesocket is the only entrant to support a shipping pre-802.11n/MIMO access point, in the form of its pricy $795 BSAP-1700 with Gigabit Ethernet for extra bandwidth. All other vendors except Netgear pointed to rough late-2007 to mid-2008 timeframes for 802.11n capabilities, and we expect all to have something available before the currently in-draft 802.11n standard is ratified. Do make sure you discuss controller upgradeability before purchase.

Arguably the most important aspect of a WLAN in-

frastructure is performance, by which we mean high throughput, predictable coverage and reliable connections. Although intuitive administrative interfaces, bulletproof security and low prices are also important, of course, they're ultimately useless if the WLAN can't deliver the services and applications required by the business. To quantify this aspect of each product, we performed throughput testing in both RF-shielded and open-air environments to assess the close- and long-range WLAN performance of each device; for more information see "How We Tested SMB WLAN Infrastructures."

At close range, 5 feet to 15 feet, we found little differentiation; all systems delivered close to 20 Mbps aggregate throughput. More interestingly, we found substantial variations in performance when the distance between WLAN client and AP increased. At medium range, 75 feet to 110 feet, average throughput fell, hitting 18 Mbps to 13 Mbps, with D-Link's system performing as much as 50% below par. At long- and extreme-range conditions, 130 feet to 150 feet with numerous intervening concrete walls heavily attenuating Wi-Fi signals, averages were .5 Mbps to 2 Mbps—when a link could be established at all.

Ruckus Wireless set the bar at nearly every test location but really excelled at extreme range, delivering multi-megabit connectivity in conditions where all others could not even establish connections with the client. Pretty impressive. Leveraging this increased per-AP coverage footprint, a small shop deploying Ruckus can spend less to cover the same area. However, if you have high-bandwidth applications or a dense user environment in your cards, every vendor allows for a microcellular design, trading range for capacity by deploying more APs in closer proximity at reduced output power.

All products support QoS features, such as WMM (Wi-Fi Multimedia) and 802.1p priority tags to appropriately place real-time traffic, such as voice and video, above data traffic. However, historically, most WLANs have been deployed with data services in mind, only later adding wireless VoIP services if required by the business. In terms of mobility, every vendor supports AP-to-AP (Layer 2) roaming, but 3Com and Ruckus Wireless forego mechanisms to aid in situations where

How We Tested: SMB WLAN Infrastructures

Throughout our evaluation process, our entire test setup was interconnected via a 24-port Cisco 3750G switch, which provided PoE and Gigabit connectivity to each vendor's controller and access point(s). We used Ixia's Chariot 5.0 for traffic generation, utilizi ng the unidirectional TCP 'Throughput.scr' script, which repeatedly sends a 500 KB file using the maximum permitted payload size until the test interval is over. Each test interval consisted of a one minute period where traffic was transmitted, either upstream or downstream, to a single client. In every case, the other traffic endpoint was a Compaq Pentium 4 2.4GHz tower with a PCI Intel PRO S 10/100 Ethernet adapter.

The most basic test we performed took place in a 'perfect' RF-shielded environment, a 13 foot by 15 foot Faraday Cage, allowing products to operate at full tilt without worry of interference. On the client side we used an IBM T43 laptop and two Dell D610 notebooks, all containing internal Intel 2915ABG WLAN chipsets. Each AP under test was configured on 802.11b/g channel 1, and all 3 clients were associated. Unidirectional throughput was measured on each client simultaneously and aggregated for total cell capacity.

To assess the range of these WLAN infrastructures, we performed open-air testing in Syracuse University's 50,000 square foot physical plant headquarters. The building is laid out much like an industrial warehouse, consisting of concrete walls and metal roofing supports with a few sections of drywall-separated office space. We verified that the testing environment was free of neighboring WLANs and sources of interference using Cognio's Spectrum Expert 3.1 and AirMagnet's Laptop Analyzer 7.0. The AP under test was configured on 802.11b/g channel 1 at maximum transmit power and placed 8 feet above the floor, remaining stationary for the duration of the test.

We selected five client locations, starting at 15 feet away from the AP with no intervening walls and progressing to more difficult scenarios. Subsequent locations included 75 feet with one concrete wall, 110 feet with two concrete walls, 130 feet with four concrete walls and 150 feet with five concrete walls. For clients, we used an IBM T43 with an internal Intel 2915ABG chipset (version 9.0.4.36) and a Fujitsu LifeBook E8410 with an internal Intel 4965AGN (version 11.1.1.11) chipset. Each client was placed on a wooden platform affixed to a Sherline Products digitally controlled turntable located at desk height (36 inches) above the floor. The turntable allowed us to test performance using all possible antenna orientations by rotating each notebook computer at a speed of one RPM for the duration of the test. The screen angle between the keyboard and the LCD was kept at 120 degrees for the duration of each test, and the starting physical orientation was the same for each system. In addition, any power management features were disabled in the WLAN client's utility.

clients are forced to roam among subnets (Layer 3). Although a must for large campus environments, Layer 3 mobility is not a requirement within a single building.

PICK AND PLAY

All these vendors deliver a base set of performance, security and ease-of-use features that cater to businesses with one site or a few branch offices. It's advanced features and pricing that separate the offerings; see our Analyst Assessment for use cases.

Although D-Link had problems with WLAN range performance, it does sport 10Gig uplink and stacking capabilities that may appeal to small businesses with a few geographically adjacent but separate buildings, facilitating high-speed interconnections between locations. Bluesocket's role-based access, guest provisioning tools and ability to authenticate clients on legacy autonomous APs cater to those with existing infrastructures or hotspot needs. Motorola supports enterprise-class extras like robust failover, VPN and multi-controller cooperation capabilities that make its gear perfect for remote branches, but its system can be pricey so look into distributor discounts.

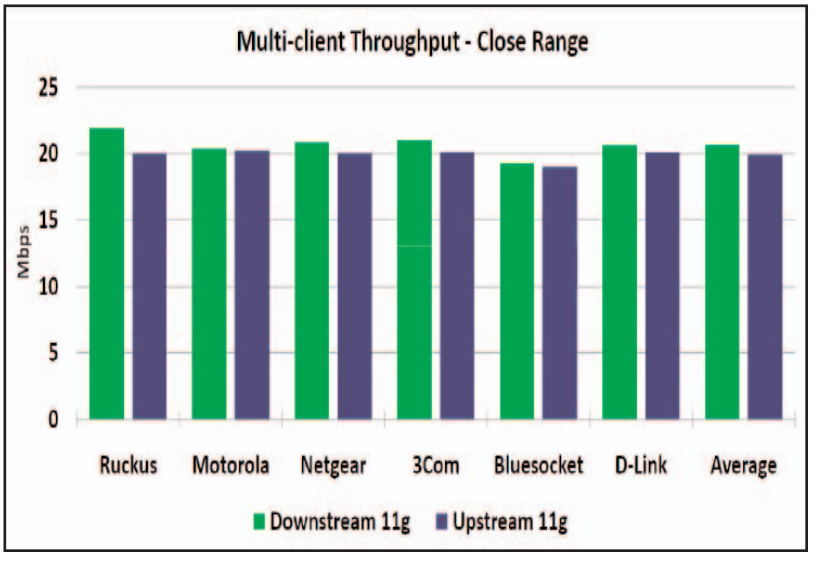
Netgear's extras include a comprehensive role-based stateful packet inspection firewall and the best integrated WLAN coverage-map view of the bunch, but some advanced features are less-than-intuitive to configure. Meanwhile, 3Com offers significant value, bringing all the table-stakes features plus 24 Gigabit PoE ports and a maximum of 24 supported APs at bargain pricing. Ruckus Wireless offered the best performance and compelling ease-of-use features.

SMB WLANs: Product Reviews

3Com Unified Wireless Switch: BEST VALUE, SHORT LIST

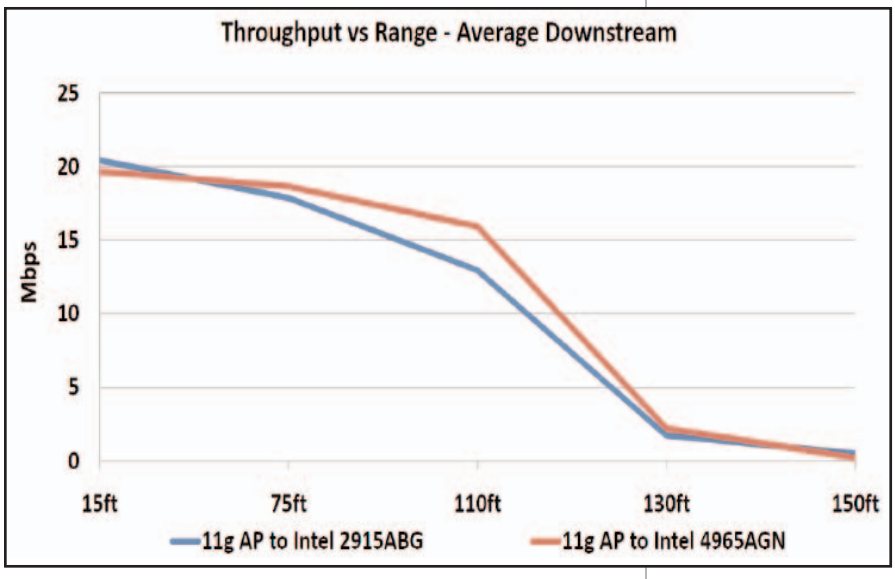
For initial setup 3Com provides a Web-based wizard that handles IP addressing, system information and basic SSID configuration. Each AP, depending on factory configuration, must be placed into "managed mode" via the Web interface, permitting centralized configuration on the controller. Although this seems like a frivolous step, it's necessary because 3Com's APs can also be deployed autonomously, supporting individual management right out of the box. To ease multi-AP controller-based deployments, 3Com's Wireless Infrastructure Device Manager utility automates the managed-mode conversion, even allowing those with compatible legacy 3Com APs to upgrade to a controller-based system. For more routine operations, such as adding a new AP or SSID, we found 3Com's interface adequate and intuitive, though it won't win any awards for looks. In all, 3Com's ease of use was on par with the competition, including all the required elements and forgoing advanced capabilities that often clutter day-to-day management systems.

In terms of security, 3Com includes all expected features, such as WPA/WPA2, rogue AP detection and external RADIUS server support. In addition, wired security is offered via 802.1x authentication on each of the switch's Ethernet ports. Quality of service mechanisms are supported on both the wired and wireless portions of the product, prioritizing traffic based on 802.1p tags and WMM. Other extras include basic AP load balancing and AP-to-AP roaming, but Layer 3 roaming is not currently supported. For those needing more advanced wireless features and scalability, 3Com points to its more expensive enterprise-class WX-series controllers.



On the hardware front, 3Com's controller is integrated into a 1U form-factor, 24-port Gigabit Ethernet switch providing full PoE capabilities across every port. In addition, the inclusion of four SFP ports for fiber runs, full 802.1Q VLAN tagging and a CLI resembling Cisco's IOS make it a credible edge switch, providing fully managed wired and wireless capabilities

that cater to an SME's all-in-one needs. For access points, 3Com's portfolio includes the single-radio 7760-series and the dual-radio 8760-series. Notably, the 7760-series supports 802.11a or 802.11b/g, in contrast to competitors that offer only 802.11b/g on their single-radio APs. We found open-air 802.11b/g range performance to be above the competition average, but only slightly. At close range (15 feet) performance was above 20 Mbps, and at long range (130 feet) only half a megabit—pretty much on par.



3Com's controller is $2,750 and APs are $249 for single-radio and $399 for dual-radio, bringing the system within dollars of the lowest price for our 10-AP scenario. If you splurge for dual-radio a/b/g APs, as we recommend, expect to pay a 60% premium. Also notable: 3Com's controller supports 24 APs with no upgrade fees, giving a small installation room to grow. For the money and situations where dual-radio capacity is not needed, the 3Com system represents the Best Value given its solid wireless capabilities paired with a credible managed 24-port Gigabit switch. 3Com's product also provides unified wired and wireless connectivity, especially useful in a small network.

Bluesocket BSC-600: SHORT LIST

Bluesocket gained success in the early days of WLANs by providing vendor-neutral captive-portal gateway authentication of users and guests. Since then, a majority of those capabilities have been integrated in most vendors' centralized WLAN controllers, and Bluesocket has expanded to compete directly in the enterprise-class WLAN infrastructure market.

We found that Bluesocket's small-scale WLAN offering packed with a variety of powerful enterprise-oriented features; not much of a surprise given that the BSC-600 is actually the branch-office version of the company's enterprise-class controller. With all this power, however, comes great responsibility … not to mention possible confusion if the system is to be supported by an in-house IT staff unaccustomed to wireless. For administration, Bluesocket uses a somewhat cluttered Web interface that often requires a three-tiered, tabbed interface to display all of the options. For situations where configuration and management will primarily be the responsibilities of a VAR, Bluesocket's powerful yet complex user interface becomes much less of a pain point.

On the bright side, Bluesocket's built-in role-based firewall, L2TP/IPSec VPN and integrated RADIUS server supporting PEAP/MS-CHAPv2 and EAP-TTLS authentication allow for granular user-based network access. Coupled with IDS/IPS capabilities such as rogue detection, DoS alerting and rogue containment, Bluesocket's security story is decidedly strong.

For guest access, credential provisioning, bandwidth throttling and captive portal abilities offer more power and customization than competitors' offerings. QoS is provided via WMM prioritization and proprietary vendor protocols such as SpectraLink's SVP. In addition, full Layer 2/3 roaming is supported, and data traffic can be bridged locally at the AP on a per-SSID basis or tunneled centrally to the controller.

In terms of hardware, the BSC-600 controller sports five Gigabit Ethernet ports, supporting POE on four of the interfaces. Bluesocket's AP portfolio includes the dual-radio a/b/g BSAP-1500 and the dual-radio 802.11a/b/g BSAP-1700, which utilizes MIMO technology to increase performance by leveraging RF multipath.

Integrating AirGo's (now owned by Qualcomm) pre-802.11n Draft 2.0 chipset, the BSAP-1700 uses a six-antenna array to increase coverage to even legacy WLAN clients. Although the BSAP-1700 supports other 802.11n capabilities, including double-wide channels and frame aggregation, we did not assess the performance impact given the device's lack of Wi-Fi

Alliance 11n Draft 2.0 certification. Bluesocket's 802.11n roadmap is shooting for Q108 as the timeframe for its 802.11n Draft 2.0 AP release, so production deployments requiring 802.11n throughput should hold off just a bit longer; the forthcoming AP will offer enhanced interoperability over the current BSAP-1700.

We found 802.11b/g performance of the BSAP-1500 on par with the competition, delivering 19 Mbps+ at close range (15 feet) and 1 Mbps to 2 Mbps at long range (130 feet). Our initial performance testing uncovered a rate-adaptation bug (corrected via a firmware update) that, when paired with our Intel 2915ABG client chipset, would cause downstream packets to be sent at a lowly 18 Mbps data rate, resulting in poor throughput.

Performance for the MIMO BSAP-1700 access point was marginally better than the less expensive BSAP-1500 device, but it didn't rival Ruckus Wireless' multi-megabit throughput at a distance of 150 feet. To its credit, Bluesocket stated that the BSAP-1700 is designed to be ceiling mounted upside-down as opposed to our temporary "LED-side-up" deployment, which may lead to increased range depending on environmental conditions.

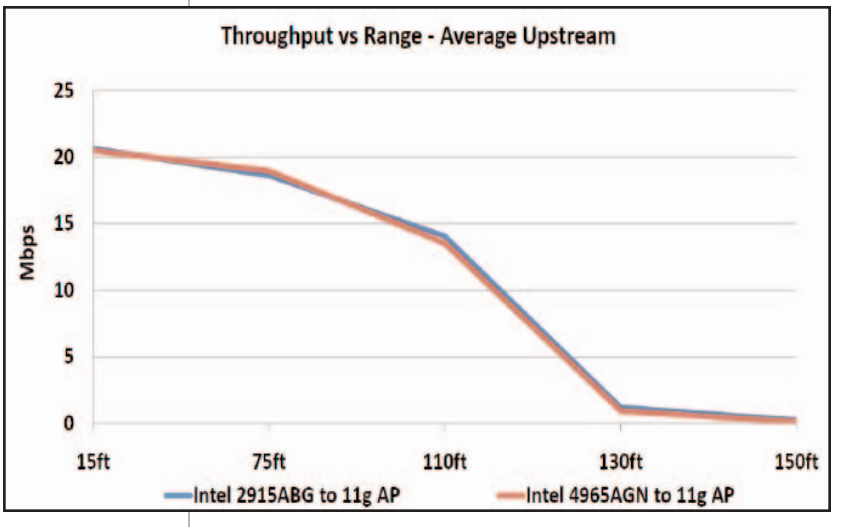
The as-tested cost for Bluesocket's system includes the $1,995 BSC-600 controller and $395 dual-radio AP, resulting in middle-of-the-pack pricing for our scenario.

Supporting a recommended soft limit of eight access points, the BSC-600 can be vertically scaled to support 25 APs via a software license key. For larger installations, Bluesocket's hardware portfolio stretches to a maximum of 300 APs per controller, featuring multi-controller load balancing, configuration replication and failover capabilities.

The optional BlueView Management System appliance provides large-scale centralized management of multiple controllers, useful for a campuswide deployment or multiple regional branch offices. In the future, Bluesocket's recently acquired open-source IP-PBX vendor, Pingtel, may allow for integrated mobility and unified communications services in a single box, an especially attractive proposition for small shops. Given Bluesocket's expansive feature list but steep learning curve, this system is best for experienced WLAN administrators or deployments with VAR-provided support.

D-Link DWS-3227P

D-Link's SMB WLAN offering is a combination of in-house-developed hardware and third-party WLAN mobility software from NextHop, which enables both wired and wireless services to be offered on a single platform. Although 3Com uses NextHop WLAN mobility software as well, differentiation exists between the hardware features of each platform. For administration, D-Link uses a Web-based interface for both wired and wireless management, including all basic options in a simple layout.

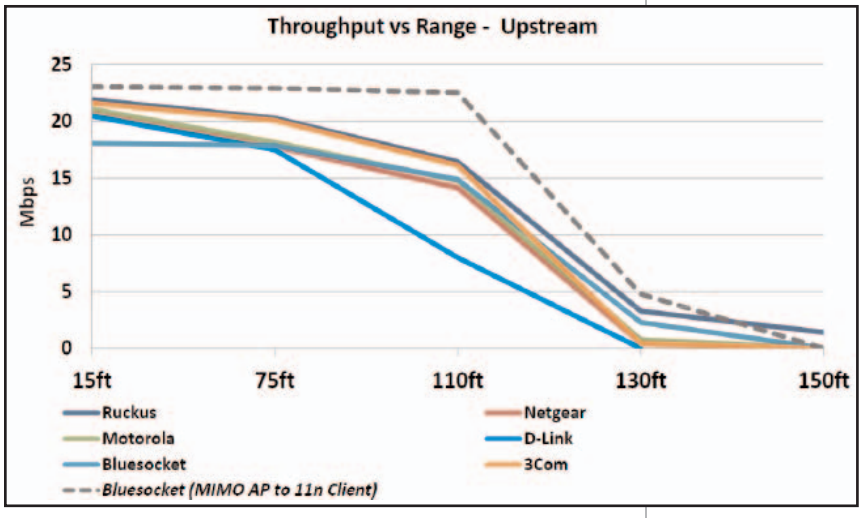


We found initial AP setup less than intuitive until, digging through documentation, we discovered the default "LTK" security key required to associate APs successfully with the controller. The DWS-3227P is easy to use for routine management, supporting all the basics with no complex or confusing extras. For security, D-Link sports all the usual features, from WPA/WPA2 to rogue AP detection and containment. Mobility is enhanced via Layer 2 and Layer 3 roaming, but that's just about the only advanced WLAN functionality you'll find.

D-Link's controller is a 1U form-factor, 24-port 10/100/1000 Ethernet switch with PoE capabilities. In contrast to the competition, 10 Gig XFP uplink and 10 Gig stacking capabilities allow high-bandwidth interconnections between as many as eight switch units. Although not a highly weighted capability in this evaluation, D-Link boasts respectable L2/L3 wired capabilities, making its offering a perfectly capable edge or distribution layer switch as well.

D-Link's AP portfolio includes single-radio 2130/2230-series 802.11b/g units and dual-radio 7130/7230-series 802.11a/b/g APs, each coming in PoE

and non-PoE varieties. We tested the dual-radio DWL-7230AP's 802.11b/g performance and found it delivered 20 Mbps+ throughput at close range (15 feet), on par with the competition. However, when distances between AP and client were increased, performance dropped off considerably, scoring 4 Mbps to 8 Mbps at medium-range (110 feet) locations and unreliable connectivity at long-range (130 feet) locations. Another low point of D-Link's entry is list pricing. At $4,299, its controller is the most expensive of the bunch; at $219 for single-radio and $395 for dual-radio, APs are around average for this market segment. In terms of max AP capacity, the default limit stops at 10 but is upgradeable via software license to a total of 50 per controller.



Although D-Link provides credible wired switch features and OK wireless performance, its above-average costs for both single- and dual-radio deployment scenarios may be a deal breaker.

Motorola WS5100: SHORT LIST

Motorola's SME WLAN offering originates from its acquisition of the company credited with the invention of the wireless switch architecture—Symbol. Note that Symbol and Wireless Valley are currently suing competitor Aruba Networks regarding WLAN patent infringement, but we're going to wait for the legal judgment before making any assumptions.

Motorola's centralized WLAN infrastructure portfolio scales from the WS2000 controller, supporting as many as six access points, to the WS5100, supporting six to 48 APs, all the way up to the large-scale RFS7000, supporting 256 APs per controller. For multi-controller deployments, Motorola's RF Manager permits centralized firmware, configuration and monitoring capabilities, for a price. To aid initial installation, Motorola offers its advanced LANPlanner site survey software for selecting appropriate AP locations based on the building floor plan, but its price may be cost-prohibitive for single-building WLANs that may just use it sparingly after deployment.

During our evaluation, we found the Java-based Web user interface in the WS5100 controller interactive and comprehensive, but less than intuitive at times. Although advanced options in the product may cater to enterprise or niche environments that benefit from extensive WLAN customization, many common management items, such as provisioning a new WLAN, are more complex than with rivals. However, if a VAR or seasoned WLAN administration will be responsible for supporting the system, this gripe essentially becomes a moot point.

Security capabilities include all the usual suspects, ranging from WPA/WPA2 to rogue-AP detection to a built-in SPI firewall. Advanced features like the internal RADIUS server supporting EAP-TTLS and PEAP/MSCHAPv2 and on-the-box IPSec VPN termination provide an all-in-one hardware offering—helpful for installations lacking a comprehensive security infrastructure. Enhanced security features, such as rogue location and containment, are offered for an additional fee via Motorola's W-IPS product, an OEM from wireless IDS/IPS vendor AirDefense that can utilize AP300 access points as dedicated hardware sensors. Real-time applications such as voice and video are appropriately prioritized via WMM and 802.1p packet tagging, and full Layer 2/3 mobility is supported in both single- and multi-controller installations. For guest access, Motorola includes captive portal authentication with useful provisioning and account-expiration capabilities.

The WS5100 controller we reviewed consisted of a 1U appliance with two Gigabit Ethernet ports, but also notable is the smaller WS2000 controller with four built-in PoE ports. Motorola's access point offering is the single- or dual-radio 802.11a/b/g AP300, available in office or industrial/ruggedized form factors and supporting PoE across the board. The main difference between these form factors is inclusion in the industrial version of external antenna connectors, which allow challenging RF environments to be addressed via

directional antennas. We benchmarked 802.11b/g performance of the ruggedized AP300 sporting omni-directional antennas. At close range locations (15 feet) throughput was 19 Mbps to 21 Mbps, dropping to half a megabit at long range (130 feet). That's on par with the competition's showing.

Motorola's 802.11n support is slated for the first half of 2008; to be accompanied by a software update that allows access points to perform data forwarding at the edge instead of tunneling through the controller—a distributed data-plane architecture that we expect to become more common in the industry as 11n takes off. List pricing for Motorola's WS5100 controller is $3,778, with single-radio APs costing $259 and dual-radio APs priced at $345, a little high compared with the competition, but look for distributor discounts to ease the pain. Given that Motorola's WS5100 controller sports enterprise-class features with an enterprise-oriented interface, it's a good fit for branch offices or VAR-supported deployments. Motorola's smaller WS2000 controller boasts a simpler interface and built-in wired WAN NAT capabilities that are appealing for SMEs looking for an all-in-one, small-scale network system.

Netgear WFS709TP: SHORT LIST

Netgear's entrance into the SMB market is via a rebranded OEM version of Aruba Network's 800-series

WLAN Features

	BlueSocket	D-Link	Motorola
	BSC-600	DWS-3227P	WS5100
Access Point Specifications			
802.11b/g	Y	Y	Y
802.11a/b/g	Y	Y	Y
802.11n Draft / MIMO	Q1 08 / Y	N	1H 08
External Antenna Connector	Y	Y	Y
QOS Support	WMM	WMM	WMM
Auto Channel / Auto Power	Y / Y	Y / Y	Y / Y
Multiple SSID support	Y	Y	Y
Controller Specifications			
Administrative Interface	Web, CLI, SNMP	Web, CLI, SNMP	Web Java-UI, CLI, SNMP
Standard / Maximum # of APs	8 / 25	10 / 50	6 / 48
# of Gigabit Ports	5	24	2
# of POE Ports	4	24	-
Additional Ports	1x Fail-Over	4x SFP, 1x XFP	-
Multiple VLANs	Y	Y	Y
Layer 2 / Layer 3 Roaming	Y / Y	Y / Y	Y / Y
Distributed Data Plane Architecture	Y (per SSID)	N	N
Security Features			
WPA/WPA2 Pre-shared Key	Y	Y	Y
WPA/WPA2 Enterprise	Y	Y	Y
Integrated RADIUS Server (EAP-types)	Y (PEAPv0, TTLS)	N	Y (PEAPv0, TTLS, TLS)
Captive Portal Authentication	Y	N	Y
Rogue Detection / Containment	Y / Y	Y / Y	Y / Y*
Advanced Features			
Mesh	N	N	N (Standalone APs Only)
WLAN Coverage Mapping	Y*	N	Y*
Integrated SPI firewall	Y	N	Y
Guest Access Bandwidth Limiting	Y	N	N

* Available through add-on application, for an additional fee.

controller paired with Netgear's own lightweight-series access points. Given Aruba's second place share of the enterprise WLAN market and the fact that a majority of Netgear's controller 'smarts' are identical, the Netgear system is an enterprise-class offering at bargain pricing. After initial installation, a Web-based wizard helps configure controller network parameters, and APs automatically search for the controller on boot up. Other wizards are on call for common operations, such as provisioning a new AP, SSID or VLAN. On the monitoring and logging side, Netgear supports extensive statistical and on-demand reporting capabilities. For more advanced configuration options, the interface can feel slightly cluttered with powerful yet complex parameters. Given the slight learning curve, Netgear's system should be supported by a trained IT staff or managed by a VAR.

For security, Netgear supports all the basics plus more, from an integrated RADIUS server supporting PEAP/MSCHAPv2 and PEAP/GTC to rogue-AP location capabilities. The integrated role-based SPI firewall provides powerful network segmentation and user authentication. Quality of service is supported via 802.1p tagging, WMM and automatic voice flow classification for VoIP protocols including SIP, SpectraLink's SVP, Cisco's SCCP and Vocera. Other advanced features include Layer 2/3 roaming, integrated captive portal authentication and a useful WLAN coverage map view.

Netgear's hardware includes a 1U form-factor con-

WLAN Features

	Netgear	Ruckus	3Com
	WFS709TP	ZoneDirector 1000	Unified Switch
Access Point Specifications			
802.11b/g	Y	Y	Y
802.11a/b/g	Y	N	Y
802.11n Draft / MIMO	N	Q4 07	1H 08
External Antenna Connector	Y	Y	Y
QOS Support	WMM	WMM	WMM
Auto Channel / Auto Power	Y / Y	Y	Y / Y
Multiple SSID support	Y	Y	Y
Controller Specifications			
Administrative Interface	Web, CLI, SNMP	Web, CLI, SNMP	Web, CLI, SNMP
Standard / Maximum # of APs	16 / 16	6 / 25	24 / 24
# of Gigabit Ports	1	2	24
# of POE Ports	8	-	24
Additional Ports	N/A	-	4x SFP
Multiple VLANs	Y	Y	Y
Layer 2 / Layer 3 Roaming	Y / Y	Y / N	Y / N
Distributed Data Plane Architecture	N	Y	Y (per SSID)
Security Features			
WPA/WPA2 Pre-shared Key	Y	Y	Y
WPA/WPA2 Enterprise	Y	Y	Y
Integrated RADIUS Server (EAP-types)	Y (PEAPv0, PEAPv1)	Y (PEAPv0)	N
Captive Portal Authentication	Y	Y	N
Rogue Detection / Containment	Y / Y	Y / N	Y / Y
Advanced Features			
Mesh	N	Y	N
WLAN Coverage Mapping	Y	Y	N
Integrated SPI firewall	Y	N	N
Guest Access Bandwidth Limiting	N	N	N

* Available through add-on application, for an additional fee.

troller sporting eight Fast Ethernet PoE ports and a single Gigabit uplink. Netgear's 802.11b/g WGL102 and 802.11a/b/g WAGL102 access points are compact and capable, with high-gain 5dBi detachable antennas and PoE support. We found throughput on par with rivals at close and far distances. From 15 feet away, Netgear delivered 20 Mbps+ performance, and at far range (130 feet) roughly half a megabit. In terms of 802.11n-readiness, Netgear currently forwards all data traffic through the controller, placing unnecessary strain on the core wired infrastructure. Although this architecture is adequate for today's 802.11a/b/g throughput requirements, it won't support more than a few 802.11n APs, each pushing 100Mbps+ at full utilization.

Pricing for Netgear's single radio system was the lowest of the competition thanks to its $2,900 controller and $180 802.11g access points. For more capacity, deploying 802.11a/b/g APs, at $240 per unit, is also the least pricey dual-band option of the bunch. The maximum number of APs per controller is 16, and additional controllers can scale the maximum to 48 (32 with failover capabilities enabled). In comparison with the competition, Netgear exhibited on-par performance, advanced features and good value, making it a must for any SMB WLAN shortlist.

Real-World Analyst Assessment SME WLAN Infrastructure

UNACCEPTABLE ← ● ● ● ● ● → IDEAL

	BlueSocket	D-Link	Motorola	Netgear	Ruckus Wireless	3Com
Short List ✔, Editor's Choice ☆, Best Value $	✔		✔	✔	✔	$✔
Performance/range Open-air and RF-shielded throughput tests using industry-standard test tools.	●	●	●	●	●	●
Security 802.1x (WPA/WPA2) support and rogue detection musts. Advanced features such as an internal RADIUS server.	●	●	●	●	●	●
Ease of configuration, monitoring, management	●	●	●	●	●	●
Extras Includes WMM/QoS for supporting voice over Wi-Fi, mesh, guest bandwidth limiting, integrated firewall, WLAN coverage prediction	●	●	●	●	●	●
Price List to cover a single multifloor building requiring a total of 10 access points and one controller	●	●	●	●	●	●

Bluesocket BSC-600: Advanced role-based access, guest provisioning tools and the ability to authenticate clients on legacy autonomous APs cater to those with existing infrastructures or hotspot requirements.

D-Link DWS-3227P: A 24-port Gigabit Ethernet, PoE wireless offering that provides value through an all-in-one package. Although D-Link had problems at long-range locations, it does have unique 10Gig uplink and stacking capabilities.

Motorola WS5100: Enterprise-class extras like robust failover, VPN and multi-controller cooperation capabilities make the WS5100 perfect for multiple remote branch offices. List pricing is on the high end of the spectrum, but distributor discounts can offset this.

Netgear WFS709TP: Essentially an enterprise-class system at SME pricing, the WFS709TP is a strong entry with an attendant learning curve. Extras include a comprehensive role-based firewall, but be aware that some advanced features are less-than-intuitive to configure.

Ruckus Wireless ZoneDirector 1000: Offering the best performance of the competition and compelling ease-of-use features, the ZoneDirector is a solid all-around choice.

3Com Unified Wireless Switch: The best value of the bunch, 3Com brings all of the basic features you'll need plus 24 Gigabit PoE ports and support for 24 APs per controller.

Ruckus Wireless ZoneDirector 1000:

SHORT LIST

Ruckus Wireless is the only entrant with an SMB-class offering that is not based on OEM, third-party software (3Com and D-Link via NextHop) or a remarketed enterprise-class branch office controller. The result is a system with all the essential centralized WLAN features plus a few extras—and without all of the customizable bells and whistles that find little use in small-scale deployments. We found ZoneDirector intuitive and simple to configure thanks to its interactive and modern Web-based administration interface. Sporting a WLAN dashboard view with drag-and-drop modules and searchable and clickable device lists, the user interface has a definite Web 2.0 feel to it. Although seasoned administrators will notice the lack of advanced RF, WLAN and network parameters, Ruckus included the most important and common options catering to installations that put ease of use at the top of their lists.

The Ruckus Wireless system consists of a small two-port ZoneDirector controller supporting Gigabit Ethernet and single-radio ZoneFlex 2942 APs offering the best 802.11b/g coverage range we've tested to date. Utilizing a pure overlay architecture, each AP relies on network connectivity and power via existing PoE edge switches (or AC power if an outlet is close by). Inside each AP lies an appropriately named "Tomahawk" WLAN antenna array, which provides highly directional gain adjusted in real-time to provide the best coverage pattern on a per client (and packet) basis. This array, besides being responsible for the AP's dome-like form-factor, sports a total of 12 antennas, each vertically or horizontally polarized.

Using the array and smart-diversity capabilities, roughly 4,000 unique antenna patterns can be selected, allowing more RF energy to be focused to the current physical location of the client. In contrast to commonly used 2-5dBi omnidirectional antennas that emit power over 360 degrees, Ruckus's 2942 APs use directional antennas with a 90-degree beam width, providing 7dBi gain and powerful interference rejection.

For 802.11n support, Ruckus pointed to a Q407 timeframe and said its initial offering will be a single-radio 802.11b/g/n access point. In the future we'd expect Ruckus to offer a dual-band AP making use of the nearly vacant 5GHz spectrum for increased capacity. Also notable is Ruckus' distributed WLAN data-forwarding architecture, designed with 802.11n in mind, that allows traffic to be bridged locally at the access point instead of centrally at the controller.

Ruckus Wireless has all the required security features plus a few extras that cater to environments where ease of use is critical. The integrated RADIUS server provides on-the-box termination of WPA2 (PEAP/MSCHAPv2) authentication, which is natively supported by a variety of modern WLAN clients. For an even easier solution, the unique "Dynamic PSK" feature combines the simplicity of deploying WPA2-PSK with the security of user-based authentication, since each client uses a unique PSK. Deployment is additionally eased by a "Zero-IT Activation" capability that uses a Web-based portal for automatic WLAN client profile provisioning (Windows XP SP2 only). Other extras include rogue AP location capabilities and an integrated guest access captive portal.

Quality of service for real-time applications is handled via WMM and SmartCast, Ruckus' traffic flow classification software. Basic WLAN mesh capability is also supported today, permitting Ruckus' ZoneFlex 2925 Lite Mesh Gateway to backhaul network access via a ZoneFlex AP, useful for situations where Ethernet cable runs are too costly or unacceptable, such as in antique buildings lacking structured wiring.

Performance for Ruckus Wireless was on par with the competition, but when distance was increased, the benefits of the antenna array clearly showed. At close range performance was 21 Mbps+, and at long range we saw an impressive 3 Mbps to 6 Mbps. At extreme range (150 feet), Ruckus ZoneDirector was the only product to deliver an astonishing 1 Mbps to 3 Mbps where all others failed to even maintain a reliable connection.

All this performance doesn't come cheap—each $349 single-radio Ruckus AP costs as much as most competitors' dual-radio APs. But in situations where high-bandwidth applications or dense user environments are not present, Ruckus' system can be deployed using fewer APs per given area because of their impressive coverage footprint. Controller pricing starts at $1,200 for six APs, $2,000 for 12 APs and $3,500 for 25 APs, allowing IT to start small but expand as needed. Delivering excellent performance, intuitive configuration and useful, unique features with room to grow, Ruckus' ZoneDirector is a strong choice for SMEs and branch offices.

Write to Jameson Blandford at jblandford@nwc.com.