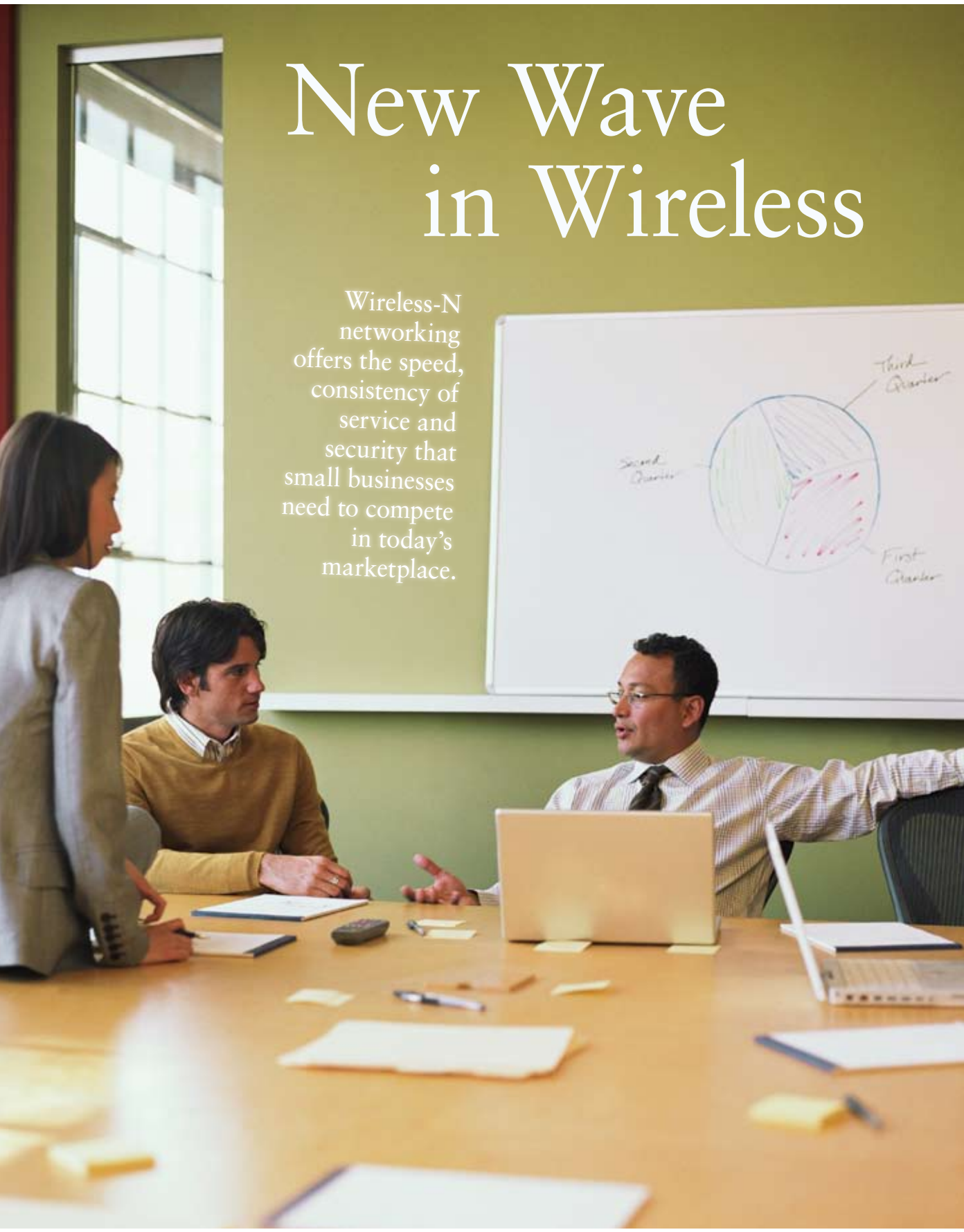
New Wave in Wireless

Wireless-N networking offers the speed, consistency of service and security that small businesses need to compete in today's marketplace.



Some small businesses have taken it slow in adopting wireless, and for a number of good reasons. The problem has traditionally been that there can be dead spots — areas where coverage just isn't reliable, like in the breakroom or conference room. And there are the issues of implementing, maintaining and securing a wireless network with minimal IT staff.

New advances in the way the Wireless-N standard works, as well as in the tools used to manage it, should lay those concerns to rest. It is now entirely within the grasp of most small businesses to run a highly efficient and secure high-speed wireless network — without spending a fortune.

Wireless-N offers a number of technical improvements over previous iterations of the wireless standard. First and foremost, it's fast — really fast. With typical throughputs in the 200 to 300 megabits per second range, and a theoretical limit of up to 600Mbps, a strong Wireless-N connection can outpace even wired 10/100 Ethernet systems.

But speed is only one of Wireless-N's advantages. The greater range of 802.11n provides a stronger signal over a wider range than possible with earlier standards. Plus, Wireless-N handles interference better. This is partly because it employs the less-used 5-gigahertz frequency and partly because of its multiple-input, multiple-output architecture. MIMO uses multiple transmitters and receivers simultaneously.

Access Points

Implementing Wireless-N in a small business can be as simple as plugging a wireless access point into a network switch and turning it on. In fact, for the smallest businesses, off-the-shelf consumer products such as Apple's AirPort Extreme Base Station might even be adequate.

Keep in mind, because wireless bandwidth is shared among everyone connected to an access point, you'll come up against the limitations of consumer hardware pretty quickly. In fact, once you add more than 10 devices to your network — or once the space you need to cover starts to approach 150 feet or more — you're going to want to add more access points.

Consumer-grade access points — dubbed fat or smart access points — have all the software and processing power needed to operate independently, which is fine for small networks. But that can become a chore for larger networks because each has to be configured and maintained separately. For small businesses with limited IT staff, dealing with just routine networking tasks, let alone dealing with problems such as a failed access point, can quickly outstrip resources.

"Management for wireless is an ongoing task," says Salah Nassar, product line manager for wireless and accessories at NETGEAR. "A work environment changes and has a lot of interference. If there are wireless problems, it is difficult to see where the problem is."

To manage wireless networks and identify problems, business-grade networking typically uses a central controller and so-called thin or light access points. Thin access points contain only the basic hardware and software needed to receive and transmit signals back and forth from the controller which handles the processing.

A systems administrator can visualize and configure the network as a whole through the controller. It then passes encryption keys, service set identifiers (SSIDs) and other information on to the access points automatically.

For example, the NETGEAR ProSafe WMS105 Wireless Management Software and WMS5316 Wireless Management System controllers support up to five and 16 access points, respectively. Both will provide plenty of coverage for a fair-sized office space, retail outlet or warehouse.

NETGEAR's Wireless Management Solution Network handles management and automation. "The software will automatically do the channel selection, power selection and load balancing between access points, and then put it in a centralized view so you can see any problems," Nassar says. >>>>

Multimedia and Wireless-N: Perfect Partners

The right time to implement Wireless-N technology is when a company is getting ready to deploy Voice over IP and unified communications systems. That's the recommendation of the Burton Group. There are many factors that make 802.11n ideal for streaming audio and video applications, says Paul DeBeasi, research director at Burton Group. These include:

- **Bandwidth and speed:** Obviously, having a fast, wide pipe for transmitting data is essential for real-time audio and video transmission.
- **Good-enough latency and jitter:** Although no wireless technology can match Ethernet's lack of latency (the lag between sending and receiving data) and jitter (slower packets that hold up the processing of faster packets), Wireless-N provides latency and jitter rates far below the usability threshold for audio and video streaming.
- **Airtime fairness:** Slower equipment or demanding tasks that come online, while a video or audio transmission is occurring, can draw off enough bandwidth to degrade the existing stream. Airtime fairness ensures that bandwidth is reserved for high-priority uses such as e-mail communications.
- **Load balancing:** Similarly, an overworked access point is no good for critical communications. Most wireless management systems automatically increase the power of nearby access points to more evenly distribute the load when one access point is being used heavily.
- **Signal handoff:** Mobile phone users who move from place to place in the building will need to be shifted from one access point to the next as they move. 802.11n's longer broadcast range and sophisticated signal processing makes for fewer and smoother handoffs, preventing interruption to the data stream.

Mixed Standards

The combination of a controller and thin access points helps to deal with legacy hardware. Wireless-N is entirely backward compatible with 802.11a/b/g systems. However, unless managed correctly, an entire network will drop down to its oldest devices' speed. Chances are, a business has notebooks, smartphones, inventory scanners, printers and other equipment supporting 802.11g or b connectivity that's not ready for a refresh.

"The problem for businesses is, 'How do I pull all those together?'" says Michael Tennefoss, Aruba Networks' head of strategic marketing. "Plus, the business needs something that looks like a seamless system that can be managed from a single tool."

Both Aruba and Cisco Systems make products to help manage mixed networks: Cisco ClientLink and Aruba Airwave. Cisco's ClientLink offers uplink improvements as well as downlink communication from access point to client.

This is significant because the majority of daily communication on the WLAN such as web browsing, e-mail and file downloads occur in the downlink direction. Improving the downlink throughput of the slowest clients improves the experience not only for the clients, but also for all other clients on the network. The result is a more reliable roaming experience and increased capacity of the network.

Airwave offers a unique multivendor network management tool that can handle equipment made by 16 vendors, using tricks such as band-steering and splitting the Wireless-N signal to maintain separation between the 2.4GHz and 5GHz streams so that slower legacy hardware doesn't interfere with faster Wireless-N data transfer.

Because of the separation of functions between the controller and the access point, and network management tools such as Airwave, "Businesses with older wireless systems don't need to do a 'forklift upgrade' of everything all at once," says Tennefoss.

Updating to Wireless-N can occur gradually by swapping out 802.11g access points as they reach their end of lifecycle and replacing them with 802.11n devices. Alternately, a business could add an up-to-date controller to an existing network.

Wireless-N can be a boon for small businesses occupying older spaces. Here infrastructure upgrades may not be possible or practical. Or perhaps the budget for running cable or power lines does not exist.

If pulling cable to each access point is impractical, one option is to run the devices in mesh mode. Each access point then passes the other access points' signals along to and from the central controller. This means you don't need to run Ethernet cable to each device.

For more specialized problem spots — connecting two buildings, for instance — directional access points such as D-Link's AirPremier N Dual Band Exterior PoE Access Point DAP 3520 can create a bridge. This eliminates the need to pull cabling between the sites.

Where power supply is an issue, Power over Ethernet (PoE) allows compatible access points to draw their power directly from the Ethernet cable. The older

802.3af PoE standard provides about 14 to 15 watts of electricity; the newer 802.3at, or PoE Plus, can provide up to 54 watts.

"Vendors have worked hard to reduce power consumption," says Paul DeBeasi, research director at Burton Group. "So many 802.11n access points today can run on 802.3af's 14 watts."

Cisco's AP 541N, for instance, is compatible with the lower-power 802.3af standard so it can be installed in places where adding new outlets proves a challenge, such as above a drop ceiling. The AP 541N also combines the controller in the access point so that several can be clustered to share the configuration automatically as new access points are added.

"With the clustering technology, you just buy the access point and then if you add another one, they automatically sync up," DeBeasi says. "This simplifies the deployment while at the same time you're not making the upfront investment."

Safety First, Middle and Last

Small companies have always been a little afraid of wireless because of security. These fears are reasonable, given a lack of specialized IT teams to manage network security. But the same tools that help small businesses manage configuration can also help manage security.

The heart of wireless security is Wi-Fi Protected Access 2 encryption, which protects the broadcast signal using the 256-bit Advanced Encryption Standard (AES). "WPA2 is a very secure, uncrackable technology when used with strong passwords," NETGEAR's Nassar says. "And implementation is fairly simple. You can create a single profile and push it out through the wireless management system, with each client system using a companywide passphrase."

For an additional level of security, access to the network can be channeled through an 802.1x authentication server built into access points such as Cisco's AP 541N and NETGEAR's ProSafe WNDAP350. 802.1x passes an authentication token, such as an encrypted certificate installed onto authorized notebooks, smartphones and other machines, to a central server for confirmation. If authentication fails, the network denies the machine access.

These measures offer a powerful first line of defense against unauthorized access. But a determined attacker, such as a deceptive employee who surreptitiously installs an unprotected access point on the network, can often find other ways in. That's another reason why controller-client architecture is useful.

A centralized console provides much greater control over the network. Today, every wireless management system has a range of security features built in, such as intrusion detection software that can easily detect an unauthorized access point being inserted into the network.

Business Benefits

Wireless-N offers a lot. Consider the technological advances represented by the 802.11n standard, the attention to security and the ease of use that Wi-Fi equipment manufacturers have integrated into their systems. Now there are no good reasons for small businesses not to consider implementing wireless networking — and plenty of reasons they should.

Contact CDW for the products, services and know-how needed to install a wireless LAN.

"The edge of the network is migrating," says DeBeasi. Doing business effectively expands far beyond the employees' desks. Whether those employees simply need the freedom to roam from office to office within the building or need to log sales from halfway around the world, mobility is a fundamental competitive need. "Employees today accept that the companies they work for will have Wi-Fi," he says.

Wireless gives employees the flexibility to innovate and collaborate freely. "These days, most people in the workforce have a laptop," says Joe Melfi, associate director of business solutions marketing at D-Link. "They can pull it into a conference room and have a meeting, take it home with them, go into a lab and do some work, go out to the warehouse and do inventory, whatever they need. It's about having the freedom to move anywhere."

Wireless-N satisfies more traditional notions of good business as well. Because its backward compatibility allows piecemeal upgrades over time, Wireless-N can be implemented as the business grows and the budget allows. And because the reach of Wireless-N gear extends much further than older 802.11a, b and g devices, a company can cover the same area with less equipment.

"Fewer access points can lower the total cost of ownership while giving a more consistent user experience than you get with 802.11g," points out Brad Sakai, Cisco's small business technology group manager.

Finally, advances in security models and deployment can actually improve security. "When implemented properly," says Nassar, "Wireless-N is so advanced it can actually be more secure than a wired network." Powerful encryption, authorization and intrusion protection rival anything available for traditional Ethernet.

"The biggest barriers to wireless deployment these days are not security or reliability, they are really the complexity of the wireless network itself," Nassar says. But with ever-better tools and equipment, that complexity should no longer be a barrier for most businesses seeking to deploy — and enjoy the benefits of — a high-speed wireless network. ◊

Comparison of wireless standards

	802.11a	802.11b	802.11g	802.11n
Maximum speed	54Mbps	11Mbps	54Mbps	300Mbps (up to 600)
Maximum range	300 feet	300 feet	300 feet	450 feet
Frequency	5GHz	2.4GHz	2.4GHz	2.4 and 5GHz
Channels	23	3	3	3 (at 2.4GHz), 23 (at 5GHz)

SOURCE: Burton Group