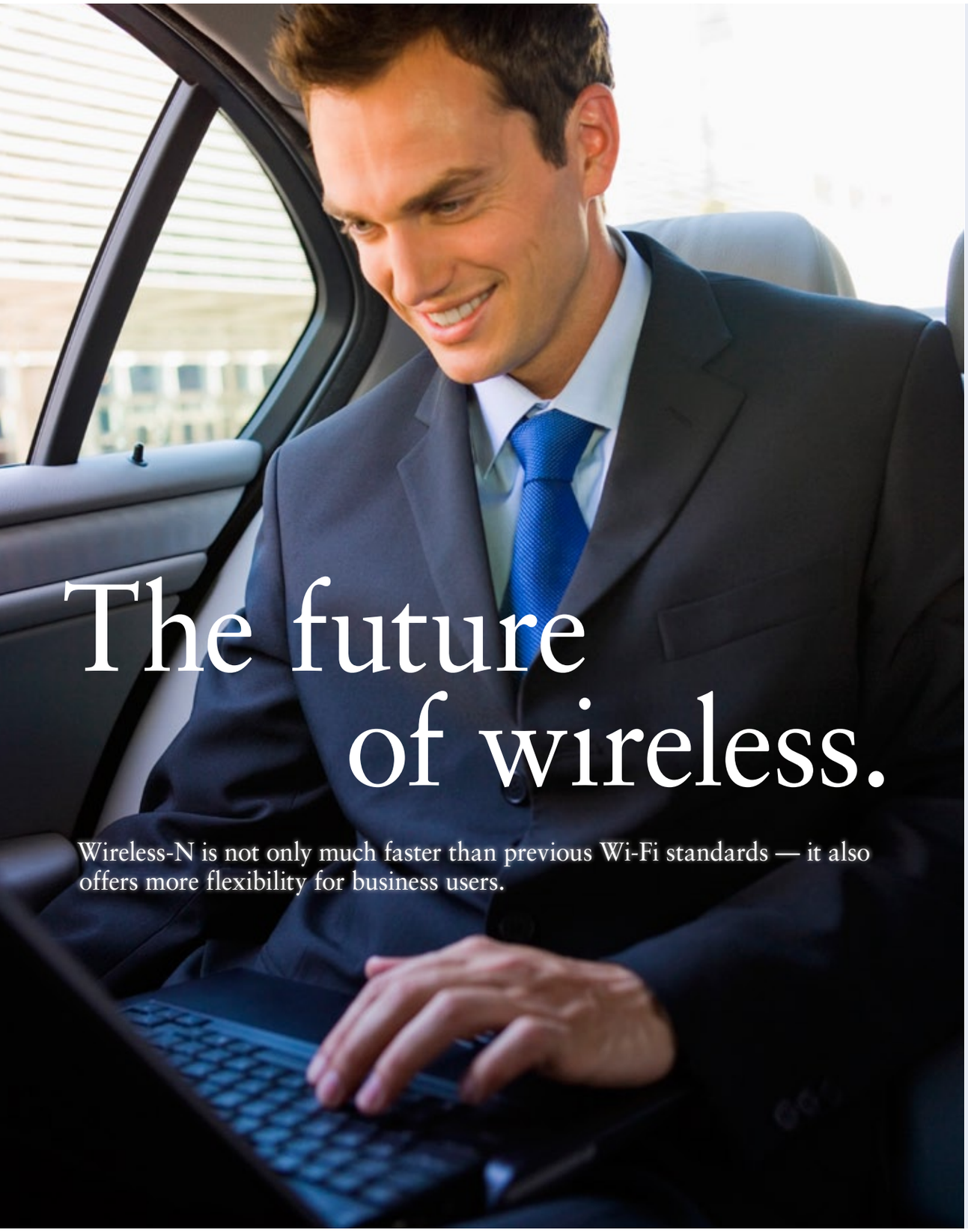

The future of wireless.

Wireless-N is not only much faster than previous Wi-Fi standards — it also offers more flexibility for business users.

The finalization of the 802.11n wireless networking standard at the end of 2009 opened up a world of possibilities for business networking. Not only is 802.11n faster than previous wireless standards and potentially faster than even wired connections, it offers much more flexibility in both deployment and management than earlier wireless technologies.

In fact, for many business uses, 802.11n wireless can effectively replace wired Ethernet. What's more, as the technology improves, the range of situations where this is true will only expand.

Increasing worker mobility and the development of an "always-on" approach to work make 802.11n's power and speed particularly appealing. These factors also look appealing when combining the new wireless standard with video conferencing and voice over IP (VoIP) telephony.

There's no question that wireless networking presents security and management challenges not found in traditional Ethernet deployments. Still, regardless of the standard, the benefits for most businesses make tackling the challenges worthwhile.

A step forward

802.11n represents a significant leap from existing wireless networking standards, resulting in speeds as much as 12 times faster than the 802.11g maximum and up to 70 times faster at range. At 300 feet, 802.11g performance plummets to 1 megabit per second, whereas 802.11n still maintains throughput of up to 70Mbps.

At the core of 802.11n's technological improvement is MIMO: Multiple Input, Multiple Output. Where previous access points and network interface cards broadcast and received on a single antenna, Wireless-N equipment can have up to four antennas for transmitting and four for receiving.

(Keep in mind, at this time, most access points have either two or three antennas for each, with some or all doing double-duty as transmitters and receivers.)

The result is that the signal can be split into several transmissions that can be received simultaneously, doubling or tripling throughput. Multiple antennas also allow Wireless-N equipment to handle interference more gracefully, by prioritizing the antenna with the strongest signal.

Wireless-N also addresses interference by using the 5-gigahertz broadcast frequency, in addition to the 2.4GHz used to maintain backwards compatibility. Both 802.11b and 802.11g devices broadcast at 2.4GHz, a frequency also used by Bluetooth devices, wireless phones, car alarms, wireless video cameras and even microwave ovens — all of which can interfere with a b/g signal.

The 5GHz band is much cleaner, with few devices broadcasting in that range, and it accommodates 12 nonoverlapping channels (23 channels total), as opposed to the three channels available in the 2.4GHz spectrum. Plus, channels can be bonded together to effectively double available bandwidth.

Wireless-N also incorporates technological advances that apply if you think of the standard as a platform, rather than a physical medium. "802.11n is just a starting point," says Michael Tennefoss, head of strategic marketing for Aruba Networks. "The physical layer might be 802.11n, but different things are done on top of that to make the network work correctly."

For example, because many businesses have a range of legacy equipment that is not Wireless-N-enabled, they typically run a mixed network. That requires using the crowded 2.4GHz band, which can slow even 802.11n hardware down to 802.11g speeds, Tennefoss says.

But band steering — which forces capable hardware to use the faster 5GHz frequency — can help preserve the speed of higher-end Wireless-N devices. "Band steering runs above 11n," he points out. >>>

<<< "It's completely compliant with the standard, but it totally changes the way 11n devices are running on the network and the performance you get out of them."

Better business with Wireless-N

The technological improvements in Wireless-N can add up to serious advantages for businesses. First and foremost, the greater speed and throughput of Wireless-N access points let employees work more swiftly and more productively than with earlier wireless standards.

Moving to UC?

Then Move to Wireless-N Too.

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:

- **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 make for fewer and smoother handoffs, preventing interruption to the data stream.

"Wireless networking is a shared medium," says Paul DeBeasi, vice president and research director at Burton Group. "More bandwidth overall means a lot more bandwidth per user." Ten employees sharing a 300Mbps Wireless-N connection can be much more efficient than the same employees sharing a 54Mbps 802.11g access point.

Beyond just speed, though, Wireless-N's multistream technology and extended reach make the signal more predictable and robust than earlier wireless technologies. "Wireless-N opens up opportunities for businesses to be more mobile and allows employees to be more productive by having faster access to information, better real-time communication and more responsiveness to customers," DeBeasi says.

With Wireless-N, employees can also act much more spontaneously. "These days, most people in the workforce have a notebook," explains Joe Melfi, associate director of business solutions marketing at D-Link. "Whatever they need, it's about having the freedom to move anywhere."

Building the business network

In theory, plugging an 802.11n access point into any Ethernet switch creates a Wireless-N network. Although that might be OK for the home user or even in a small office, the management of a Wi-Fi network grows increasingly difficult as more and more access points are brought online.

Off-the-shelf wireless routers need to be configured individually and managed individually, says Salah Nassar, NETGEAR's wireless product line manager. That requires logging into each IP address and accessing the administrative consoles one by one. Just something as seemingly simple as troubleshooting a broken antenna can mean hours or days, or longer, of work, and that's not acceptable in a medium or large enterprise, he points out.

For more demanding business use, then, Wi-Fi systems are deployed using a centralized controller and any number of stripped-down, thin or light access points. Unlike the access points you might find in your local electronics store, the thin access points have little or no software onboard beyond that strictly necessary to move packets to their intended destination.

"The controller is the centralized brain," Nassar says. "Everything comes back to the controller, which does all the routing."

NETGEAR's ProSafe WMS-5316 Wireless Management System supports up to 16 access points and 50 to 100 users. It offers automation and network management for midsize organizations.

"The functionality of the controller is that it does automatic power as well as channel selection," Nassar says. "This ensures that access points are not on the same channel, and the power is balanced to avoid interference."

Big business wireless

Larger businesses might have far more than 16 access points to manage, which brings new challenges. For instance, thousands of workers moving about from place to place with their wireless gear means thousands of network handoffs, as wireless devices move away from one access point and into range of another.

The multiplication of workers and roles also brings a multiplication of types of data streams. These can range from file transfers to live video streaming, each with different power and bandwidth needs.

Enterprise-level networks, such as those produced by Aruba, Cisco and D-Link, have to take into account the complexity of wireless traffic over the network. One significant issue is integrating legacy hardware into the new network because most companies still have thousands of notebook PCs, smartphones and other equipment that run 802.11g.

"How do I pull all of those together into what looks like a seamless system that can be managed from a single tool?" asks Tennefoss.

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

Aruba addresses that problem with a unique multivendor network management tool that can handle equipment made by 16 vendors.

The function uses networking tricks, such as band steering and splitting the Wireless-N signal to maintain separation between the 2.4GHz and 5GHz streams. The idea is to keep slower legacy hardware from interfering with faster Wireless-N data transfers.

Another challenge is ensuring the reliable provisioning of bandwidth to critical tasks such as video streaming and VoIP, instead of less time- or latency-sensitive tasks such as transferring documents. Airtime fairness policies, a set of policies for prioritizing traffic on the WLAN, can help by making sure that lower-priority tasks don't nab bandwidth from higher priority tasks.

Tools such as Aruba's Policy Enforcement Firewall can also help. It's designed to reserve a fixed amount of bandwidth on a per-application basis. In that way, each application functions as it if were on its own private network.

Installing Wireless-N systems, as with any other wireless technology, requires special attention to the corporate geography — the structural elements that might block the signal, sources of potential interference and so on. Still, 802.11n hardware offers several features that allow for greater flexibility than previous-generation systems.

In areas where it would be impractical to pull cable for each access point, for example, the gear can be run in mesh mode with each access point passing the other access points' signals along to and from the central controller. For more specialized deployments, such as connecting two buildings, directional access points like D-Link's AirPremier N Dual Band DAP 3520 can create a virtual bridge and eliminate the need for new wiring.

Where power supply is more of an issue than running Ethernet cable, Power over Ethernet will let compatible access points draw power directly from the Ethernet cable. The older 802.3af PoE standard provides about 14 to 15 watts of electricity. A newer standard, 802.3at (PoE Plus) can provide up to 54 watts.

"Vendors have worked hard to reduce power consumption," DeBeasi points out. "So many 802.11n access points today can run with 802.3af's 14 watts."

Keeping it safe

An important concern in any wireless deployment is network security and integrity. Unlike wired networks, which require physical access to the hardware to intercept the signal, wireless networks can transmit over wide ranges, often through exterior walls and into the surrounding terrain.

This is a crucial security concern for Wireless-N because it can broadcast a usable signal as far as 450 feet. Without proper safeguards, an attacker could park in the corporate lot or even on the street and gain access to the network.

Fortunately, well-understood best practices for wireless security can ensure adequate protection against signal leakage. "11n has much better security than 11g," says D-Link's Melfi. "Almost surely, you can have better corporate security."

The foundation of security on Wireless-N networks is Wi-Fi Protected Access 2 encryption and 802.1x authentication. "WPA2 is a very secure, uncrackable technology when used with strong passwords," says Nassar. "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 the companywide passphrase."

Protecting the wireless signal defends against outside attackers but not against a determined attacker with access to the network itself. "For instance," explains DeBeasi, "an employee could install an extra wireless router to broadcast without encryption.

"Fortunately, virtually every WMS [wireless management system] has a wireless intrusion protection system, which can detect rogue access points, ad hoc connections and other breaches of the network," he adds. Of course, the WMS itself needs to be protected, but traditional best practices for wired Ethernet systems, such as changing default settings, are already well understood and common.

"When implemented properly, Wireless-N is so advanced it can actually be more secure than a wired network," says Nassar. Security concerns shouldn't be a reason to avoid implementing wireless — the benefits of a Wireless-N network are too great and will become more and more essential as time goes on, and the security issues are well understood. ◊