MAKE WI-FI FLY

Wireless-N offers businesses speed, consistency of service and security that previous networking standards can't deliver.

When accessing the Internet, accessibility, bandwidth, security and speed are critical components. From employee productivity to customer satisfaction, the success of a business depends greatly on its wireless service.

Wireless-N, or 802.11n, is faster than previous wireless standards and potentially faster than even wired connections. It also 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 alluring when combining the new wireless standard with video conferencing and Voice over Internet Protocol (VoIP) technology.

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 about 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 (APs) and network interface cards broadcast and receive 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 APs 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 allowing simultaneous reception, thereby 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 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.

802.11n Benefits

Whereas a secured home wireless system's bandwidth might cater to a handful of users, an office setting is required to provide quick accessibility for 20 to 100 people. Some of these individuals may be carrying a number of wireless devices such as smartphones, notebook computers and iPads — which all act as independent APs. With 802.11a, b or g, connectivity could be an issue.

From a performance perspective, businesses can see roughly five times the performance of earlier-generation 802.11a/b/g-compatible wireless systems, says Brian Nicklin, wireless access points product manager for Cisco Systems' small business group. "This equates to increased productivity via faster file transfers and by enabling companies to use high-bandwidth mobile applications."

With high-bandwidth media applications being used and deployed in more businesses, real-time collaboration applications such as voice and video require low-latency wireless connections with high reliability. "Wireless 802.11n provides more consistent signal coverage and throughput," Nicklin adds. "It can yield up to two times greater predictability, which is essential for mobile applications."

Wireless-N benefits are also far-reaching. "802.11n can increase productivity as the wireless network becomes more stable [equaling better connectivity] and with higher speeds," says Bruce Kraemer, chair of IEEE's 802.11 Working Group. "Employees stay connected to all of their assets and applications throughout the office. And who doesn't want better connections and higher speeds?"

Wired networks, once the industry standard for speed and security, have limits on signal strength, thus making systems slower and less productive. Although upgrading to wireless 802.11n requires a moderate investment, wired networks are more difficult to expand and can be more expensive

to reconfigure or upgrade in the long run. On the other hand, as a company grows, a wireless infrastructure reconfiguration is both workable and affordable.

And though analysts and users alike doubted the strength and speed of wireless just a few years ago, the proof is literally in the pudding. "In my own experience, files that used to take five minutes to download on 802.11g now take less than a minute with an 802.11n network," says Peter Newton, director of product marketing at NETGEAR.

"I used to wait to download large files or attachments until I was connected via a wire," Newton adds. "With 802.11n, I can download whatever I need without even thinking about the speed of the network."

802.11n ACCESS POINTS PROVIDE AT LEAST FIVE TIMES AS MUCH BANDWIDTH AS 802.11g.

Cisco's Nicklin notes that the firm has Wireless-N products specifically designed for businesses with fewer than 100 employees. These include Cisco's Small Business Pro AP 541N Wireless Access Points, designed to help enable secure data, guest and multimedia wireless access for any small business.

Gaining Access

The wireless AP, which is the main component in 802.11 wireless LAN platforms, connects an organization's wireless network to its wired network. Small businesses need multiple APs to allow mobility among employees and clients. Typically, APs are either considered thick (also known as "smart") or thin.

Thick APs traditionally offer intelligence capabilities beyond what the 802.11 standard provides. For example, this type of AP may offer enhanced functionality in the areas of security, management and performance. Thin APs minimize the intelligence in the AP and instead centralize the intelligence of the network in the switch.

"A survey of the wireless environment is always important to determine access points," says Joe Melfi, associate director of marketing for D-Link. Surveys should not only include the number of required APs but also power ratings and logistical barriers.

"Engineers can handle the survey," Melfi says. "Or if end users are technology-savvy enough, they could complete a survey." But there are many considerations and the person doing the survey will need to have considerable knowledge of IP and wireless systems.

Thick APs are not as scalable as thin APs. This can cause a problem if a business needs to manage more than roughly five of the devices. Many businesses on the small end of the sub-100-user category will not need as much oversight, Melfi points out.

"There are very few wireless controllers in the sub-100-user market," NETGEAR's Newton says. "So there isn't much discussion of thick versus thin. Almost all sub-100-employee companies are deploying thick (stand-alone) access points."

In larger networks deploying wireless controllers, most are using split architecture: The APs are doing a lot of the data processing locally. And the wireless controller is only performing the management tasks. This means most 802.11n thin APs are acting more as thick APs.

Kraemer points out that the 802.11n APs would be connected to an Ethernet infrastructure — the same procedure as with 802.11a and 802.11g. "It would be advisable, however, to use an Ethernet port of at least 1 gigabit per second in order to carry the wireless LAN information without introducing delays," he says.

Packing in Power

Power over Ethernet (PoE) is a cabling system that transfers power. It removes the need for power outlets in cumbersome areas such as a drop ceiling. For higher power levels, a CAT 5 cable is required. However, some businesses can get away with CAT 3 cabling, if power levels are low.

PoE technology has been on the market for a number of years. However, it wasn't a viable business application until recently. "Back three or four years ago, products consumed so much power that Power over Ethernet would not work," says Paul DeBeasi, research vice president for the tech analyst firm Gartner. "However, things have changed."

The reason? Manufacturers have improved their product power consumption techniques. The power needs of APs make them well within the limits of PoE, even for hosting video surveillance.

"The advantages of PoE are realized through the ease of installation and the reduction of total cost of ownership [TCO]," Nicklin adds. "APs are often mounted on the ceiling or wall for optimization and security, and PoE reduces the installation costs by not having to run extra AC power to these mounting locations.

"PoE can also help to reduce the overall TCO on a wireless LAN by giving the network administrator more flexibility and control of the switching and wireless infrastructure," he says. For a small business, Cisco's new small business SG300-28P 28-Port Gigabit PoE Managed Switch is an ideal solution.

Where power supply is more of an issue than running Ethernet cable, PoE will let compatible APs draw power directly from the

Tips for 802.11n Migration

802.11n offers the potential to bring revolutionary advances in bandwidth, throughput, security and reliability to wireless LANs. Some even say it will place the WLAN on the same performance level as a wired LAN.

Here are some things to consider when upgrading:

Q. How do 802.11n access points (APs) interface with existing switches?

A. To get the full speed out of clients connected to an 802.11n wireless network, a gigabit switching infrastructure is needed.

Q. How are 802.11n APs powered?

A. They can be powered by a traditional AC adapter or via Power over Ethernet (PoE). Keep in mind, because of power requirements, some 802.11n APs require the 803.3at PoE standard, plus PoE switch or power injector.

Q. What is the impact to the network backbone?

A. Adding an 802.11n AP will most likely add more traffic to the network infrastructure.

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 30 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."

Security Foresight

A few years ago, horror stories depicting thieves sitting in parking lots of businesses stealing information via a notebook computer were common. This was because most wireless systems lacked proper encryption. Today, most businesses have taken measures to secure company information against such threats.

"A lot of lessons were learned in the last few years," says D-Link's Melfi. Businesses are now deploying Wi-Fi Protected Access (WPA and WPA2), which was developed by the Wi-Fi Alliance to indicate compliance with the security protocol to secure wireless computer networks.

There have been other advancements introduced that have further increased security measures, Melfi adds. "Some access points are hyper-intelligent. The normal thinking would be to use a centralized controller to take the intelligence out of the access points." he says. "But what happens is that the environment is such that we want some of the processing to be done at the access point. Therefore, we now have products that provide security for each access point."

Among D-Link's security offerings is the DLF-210 NetDefend Network Security Firewall. Ideal for the small office looking for solid performance and security, it offers numerous flexible features to help manage, monitor and maintain a healthy and secure network. "It works with firewalls, switches and swipes, and can detect rogue APs or someone trying to hack into the system," Melfi notes. "We use our zone defense to cut off the access point and provide real-time notification to the IT department."

Moving forward, businesses should upgrade to WPA2 with the Advanced Encryption Standard (AES) for data encryption. It ensures that the traffic from the client safely travels to the AP and back without anyone being able to see the transmission, NETGEAR's Newton explains. Conversely, using 802.1x as an authentication method is another good way to ensure that only the right people are connecting to the wireless network.

Not ready to deploy WPA just yet? "The easiest way to protect a business is to turn off the service set identifier or SSID broadcast," Newton recommends. "If you disable this, it's difficult for nonemployees to find your network to connect to it." Once you disable SSID, if you want to allow guests to access the Internet via the network, simply set up a separate SSID to act as a guest network and protect it with virtual LANs on the switch infrastructure.

Although it remains true that a business can still operate on 802.11g, the investment in 802.11n greatly outweighs the risk. "The density and dependency of these networks is going up faster than ever," says Gartner's DeBeasi. "The users are getting more comfortable with wireless, which is driving the vendors to make more sophisticated tools." ◊

CDW has the products, services and know-how to help small businesses install a wireless LAN.