From: www.cio.com

802.11n: How Best to Use It and When

– Karen D. Schwartz, CIO

October 02, 2008

If your company has traveling employees, bandwidth-hogging applications, a need for speed or just a desire to keep pace with technology, you're probably thinking about moving to an 802.11n-based wireless networking infrastructure, at least at the network's perimeter.

It's inevitable, experts say, and the numbers bear it out. ABI Research, an Oyster Bay, NY, market research firm, finds that while 802.11n has only a 2.3 percent penetration rate in North America today, that number will grow exponentially, reaching 19 percent by next year. In large part, that's because the technology is mature, costs have decreased, and it has the flexibility that wireless can't compete with, says Stan Schatt, vice president and research director for wireless connectivity at ABI Research.

Although the standard isn't fully approved—it's expected to be available by 3Q09 at the latest—it's finished, for all intents and purposes, he says, and most major vendors have 802.11n products ready to go.

With products already available and companies hungry for the throughput and flexibility 802.11n will provide, the only decisions left involve how to choose and implement the technology most effectively and efficiently.

The first step is performing a thorough site survey, evaluating your current technology infrastructure and future needs.

"Now is the time to spend the money and time to look at your needs," says Lisa A. Phifer, vice president of Core Competence Inc., a Chester Springs, Penn., network and security consultancy. "You have an opportunity to start with a clean slate with a brand new set of products and do it right the first time. You'll spend less money in the long run."

Once you know what you need, the next step is choosing a product and a vendor, which is more difficult than it may seem. There are major differences in terms of robustness, capacity, flexibility and manageability.

"You have to consider everything. For example, what if your controller goes down? Some access points are capable of going into independent mode and some aren't," says Schatt. "And there are significant differences in antenna technology; some companies like Motorola and Ruckus have put a lot of effort into their antennae to accentuate the advantage of the MIMO (multiple input/multiple output), while others haven't."

Don't be afraid to ask vendors the tough questions, especially about features that are important but don't get much airtime in websites and collateral, adds Michael Fineran, a principal at dBrn Associates, a consultancy in Hewlett Neck, NY.

For example, few vendors mention how many transmit chains their products provide. That's important, because while 802.11n provides the ability to send multiple signals at the same time in the same frequency band, two chains would provide twice the transmission capacity of one chain. "That's not something they tell you, so you have to ask," Fineran says.

Another important factor is maximum transmission rate. Although all vendors quote one, they often don't say whether it's 20MHz or 40MHz. It's an important consideration, he adds, because that determines the bandwidth and the number of available channels.

There also is a major difference in the type of management software different vendors provide, and depending on your needs, it could drive your decision.

"Some have really good site survey tools or planning tools, while others will have really good interfaces to external management systems. Still others can manage multiple vendor environments or widely distributed geographical environments," says Craig Mathias, a principal at Farpoint Group, an Ashland, Mass.-based consultancy.

Sometimes, the management tools that come with the system might not be enough, but the rest of the product might fit your needs. In that case, consider augmenting with third-party tools, such as wireless LAN assurance tools from companies like AirMagnet and AeroPeak that verify that the network is actually doing what you think it's doing, Mathias advises. Third-party tools also are recommended for intrusion detection of wireless networks.

Implementing an 802.11n network also means shoring up your security infrastructure. For example, few wireless intrusion detection systems today detect 802.11n, because they were designed for 802.11a, b and g. That means organizations installing 802.11n have to upgrade those systems immediately to detect N-based networks, to better monitor for rogue access points and ad hoc networks.

The next step is readying your existing wired network to work with 802.11n. Consider power sources carefully, Fineran says, because whereas other network access points run over Power over Ethernet (PoE), saving money, most 11n access points today don't. That's slowly changing; Siemens now has an N access point running on standard PoE and others are on the way, but check carefully, he advises.

Also consider capacity. Most access points today are connected on a 100MB Ethernet connection, but 802.11n runs faster than that, which means your existing access points will probably have to be upgraded to 802.11g Ethernet connections. Without a doubt, you'll probably be upgrading portions of your network to Gigabit Ethernet or even 2G Ethernet in some cases, Schatt says.

And when it comes to your migration strategy, don't forget the laptops.

"Part of the growth of 802.11 is predicated on how quickly companies upgrade their laptops, and when they upgrade, they won't have N automatically installed on their laptops," Schatt says. "That means they may have to buy some external adapters in the meantime, which CIOs hate to do because they are hard to keep track of and break easily."

If issues like reliability and speed are an issue with your current network, or if you have specific issues with 2.4GHz interference, it's probably worth biting the bullet and upgrading your network to 802.11n today. Similarly, if your network is running mainly productivity applications and you have sufficient bandwidth, or if your infrastructure changes would be extremely expensive, it's fine to wait; the technology will only get better and cheaper, says Schatt.

It's also reasonable to upgrade to 802.11n in a piecemeal fashion. In fact, it can often be the best move.

"If you can identify specific segments of your network that need what 802.11n offers, like a bandwidth-intensive video application, you can identify those specific network segments so you only have to upgrade part of it today," Schatt says. "That can make a lot of sense, both economically and for the business."