

Wireless Broadband:

Next Wi-Fi Standard Delayed

The IEEE 802.11n task group can't decide on a draft standard. What happens next?

By Steven S. Ross ■ *Editor-in-Chief*

How many engineers does it take to approve a draft standard? In Australia in mid-May, 300 couldn't do it. The engineers, called together every two months by the IEEE, split between two proposals, one by TGn Sync and one by the World Wide Spectrum Efficiency (WWiSE) consortium, for a draft of the next big Wi-Fi standard, 802.11n. The 11n standard would raise Wi-Fi bandwidth to 100 Mbps immediately and to as much as 300 Mbps in a few years. It offers a clue into the speeds the equipment vendors think will be necessary, both in commercial networks and in the much larger consumer home market. Both groups have numerous high-powered corporations behind them (see box).

The TGn Sync group proposal for an 801.11n draft standard had pushed ahead in the March voting, garnering 57 percent of the vote. But the IEEE process requires 75 percent in favor for a draft. In the May voting, support for TGn Sync dropped to 49 percent. TGn Sync supporters knew the fall was coming. They tried (unsuccessfully) to cancel the voting. TGn Sync support is still far stronger than support for WWiSE but far short of the near-consensus required for a draft standard.

But "pre-11n" wireless routers are already being sold. Should you jump in? The short answer for consumers and for systems operators is, "probably yes." But to really understand what your hard-earned cash will buy, you have to understand how the standards-setting process works, the time frames involved, the competing standards (especially WiMAX) and what happens if (!) there never is a draft standard.

Is Standards Compromise Possible?

Everyone seems to say compromise is possible, but "compromise" can mean different things to different people. The standards are actually quite different on a key point, channel bonding. You either have it, or you don't. If history is any guide, any likely "compromise" would simply combine almost everything that's different in the two competing standards proposals. But the bonding issue is tricky. TGn Sync allows channels 40 MHz wide; 802.11g and 11a use channels 20 MHz wide, and most countries do not allow use of all the channels that are available in the standard itself (11 that

overlap in 802.11b, which would allow just three 20 MHz channels there). Most 11g implementations include circuitry for 11a compatibility as well, so this article discusses 11g as if 11a compatibility were part of the standard.

The "Pre-n" equipment being sold now uses the main feature that is common to both proposals, multiple-input/multiple-output (MIMO). MIMO splits the transmission into two or more data streams within a single channel. Each stream is sent, and received, by a separate antenna. Even if only one end of a link uses MIMO, transmission is faster than if neither the router nor the Wi-Fi card

TGn Sync Member Companies

Agere Systems Inc.
 Atheros Communications Inc.
 C-cation, Inc.
 Cisco Systems, Inc.
 Infineon
 InfoComm
 Intel Corporation
 InterDigital Communications Corporation
 Marvell Semiconductor, Inc.
 MetaLink
 Mitsubishi Electric Co.
 Nortel Networks Corporation
 Panasonic (Matsushita Electric Industrial Co. Ltd.)
 Qualcomm Inc.
 Royal Philips Electronics N.V.
 Samsung Electronics Co. Ltd.
 SANYO Electric Co. Ltd.
 Sharp Corporation
 Sony Corporation
 Toshiba Corporation
 ATcrc/Wavebreaker
 Wavion Networks

on the device being networked uses it. Think of the Pre-n devices as 11g with better antennas. If your system allows it, then, why not use Pre-n nodes to replace or supplement 11g nodes you already have? By the way, the pronunciation of MIMO has been standardized by IEEE vote as “MyMoe.”

Also WiMax, the popular name for IEEE 802.16, is coming. With it, roving computer devices and phones would use the same nodes, probably through small antennas in a “distributed antenna system,” such as described in the article by Allen Dixon in this issue. So 11n or Pre-n systems will be upgraded, supplemented, or replaced entirely in the years ahead anyway.

The IEEE Process

Standards at the Institute for Electrical and Electronics engineers are written by task groups. There are many, many task groups in the 802.11 (Wi-Fi) universe. Welcome to Task Group N.

Task Group N met for the first time in Vancouver in January 2004, after two years of quiet preparation. The goal was to come up with a Wi-Fi standard that would be faster and more reliable – and that would not promise more than it could deliver. The slowest but most commonly used Wi-Fi flavor, the 802.11b standard, promises 11 Mbps but actually delivers about half that bandwidth in a typical installation. The rarely used 802.11a standard and the increasingly common 802.11g promise a peak throughput of 54 Mbps but rarely deliver more than 24 Mbps. The 802.11n goal is 100 Mbps at first, growing to 300 Mbps in later iterations. But the 100 Mbps would be measured where it counts, as more “real” throughput.

Engineers think of networks in terms of layers - a physical layer and six “logical” layers of increasing specificity. The “physical” (PHY) layer throughput is the bigger number, the way 802.11 devices are defined now. But 802.11n would measure the rate between the media access control layer (MAC, the first layer above the physical) and higher layers. Thus, the real throughput promised is a four- to six-fold improvement over 11g. It was promised for the end of 2005, but 2007 now looks more likely. Will WiMAX pass it by?

One reason for the difference is that networks have a lot of overhead - the headers that define data packets, the separating and sorting of data from multiple transmitting computers and multiple receivers, calls to resend bad data, and so forth. In the wired world, for instance, plain-vanilla 100Base-T Ethernet rarely delivers data at anywhere near the 100 Mbps promised. Wireless networks have more juggling to do because the transmission medium - the air - is not as error-free as fiber or coax. Traditionally, as promised data rates have increased, so has the gap between the promise and what is actually delivered.

There’s another constraint in the open-standard network world: In general, new network standards in a given standards area like 802.11 are all supposed to be backwards-compatible at the physical layer unless there’s a clear reason for them NOT to be. That is, an 802.11g card in a laptop will connect, albeit more slowly, with an older 802.11b router. If you are creating a wireless mesh network to cover a large area of a downtown or even an entire municipality, you have to look at this requirement carefully. It does not mean that your network has to be backwards-compatible with very old equipment. The presence of an 11b client on an 11g network, for instance,

slows the whole system down for everybody because the node has to operate in 11b mode.

You can choose to “allow” users of very old network cards to connect, or not. The standard just means that the equipment is capable of such connections. In the 802.11 world, for example, there are legacy standards for 1 and 2 Mbps equipment. Allowing them would slow the network for everyone else. So most networks are not set up to allow them, even though the hardware capability is there. Well, in truth the signal-processing logic is there. But the original 802.11 standard from 1997 specifies data transmission by infrared as well as the 2.4 GHz. Band. No one ever sold equipment for infrared Wi-Fi.

For network engineers, the problem is generally stated as one of shrinking data packets while overhead remains the same. For 11n overhead would actually increase. One reason: A need for better security. The security issues are being handled by another task group, for 802.11i. The existing 802.11 Wi-Fi standards started by using a security protocol called WEP. It’s weak, because it uses a static, unchanging “key” to encrypt the network traffic. All users on the same network must use the same key. In theory, if your traffic is monitored enough, the key can be calculated from outside.

WWiSE Member Companies

Airgo
Broadcom
Buffalo Technology
Conexant
Electronics and Telecommunications Research Institute (Korea)
France Telecom
Hughes Network Systems
ITRI CCL
Motorola
Nokia
NTT
Ralink Technology Corp.
Realtek
STMicroelectronics
Texas Instruments
TrellisWare Technologies
Winbond Electronics Corp.

Remember, though, that an encryption standard that is weak for one purpose is probably fine for others; it is a matter of matching security strength against the likelihood that someone would take the time to peak. I work within range of 20 other detectable Wi-Fi networks. If I can see them, they can see me. My router can handle 256-bit WEP but the network card in my PDA can only handle 128. So I use a 128-bit key for all my connections. Every few months I change the key. Manually. In six different devices. Each computer in my network has its own firewall, so that a casual snoop who has the key can't easily see them. That means, of course, that I can't share data on one computer from another because the machines on my own network can't see each other either!

Yes, most of my network traffic is encrypted another way as well, using Secure Socket Layer. The SSL public key encryption is built into Web browsers and most e-mail clients such as Microsoft Outlook. But I'm lucky; most of the servers I communicate with allow SSL. Good thing. At a public hotspot, I can't use WEP. So only my laptop or PDA's firewall and

SSL stand between my data and people who might find my data useful.

This security is fine for my needs. But what if I were a bank or high-tech firm dealing with sensitive, valuable data that a competitor or an identify thief would like to have? At the very least, I'd need AES - Advanced Encryption Standard. It's more usable in a public hotspot, and much harder to crack. The new wireless protocols allow AES (called WPA2 by the industry). But again, the person receiving your message has to be similarly equipped.

The Technology

Getting the extra throughput without using more spectrum requires a stronger signal, more efficient use of the existing bandwidth by changing the signal logic and the overhead, and maybe faster, more efficient electronics. The TGn Sync group would gain throughput under some circumstances by combining ("bonding") two 20 MHz channels in the 2.4 GHz band. This does not, however, add to the total bandwidth available to all users on the network, and is opposed by the

WWiSE group. The 40 MHz requirement has been misread by the technical press as more-or-less required, but the actual standard calls for its use only when contention by users for the bandwidth is low enough to "steal" a 20 MHz channel and combine it with another. Even so, the bandwidth allocations in some countries, including Japan, would require that this feature be disabled entirely. There would be no worldwide 11n standard equipment that allowed 40 MHz channels.

In contrast, the old 802.11b standard uses 14 channels whose center frequencies are 5 MHz apart. This does not mean the channels are "5 MHz wide" because the signal strength at the edge of a channel is lower than at the center, but far from zero. So the network professionals tend to talk about widely separated channels (1, 6 and 11 for instance) as being non-overlapping. Even that is not entirely true, because a very strong signal on channel 6 may trump a very weak signal on channel 1 or 11. The standard for 802.11b is that the signal must be at least 30 dB below its peak at 11 MHz from the channel's center frequency and

What the numbers mean at IEEE 801.11

802.11 - Original 1 Mbps and 2 Mbps, 2.4 GHz RF and IR standard

802.11a - 54 Mbps, 5 GHz standard

802.11b - 5.5 and 11 Mbps, 2.4 GHz standard

802.11d - International (country-to-country) roaming extensions

802.11e - QoS, including packet bursting

802.11f - Inter-Access Point Protocol (IAPP)

802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b)

802.11h - 5 GHz spectrum, Dynamic Channel/Frequency Selection (DCS/DFS) and Transmit Power Control (TPC) for European compatibility

802.11i - Enhanced security

802.11j - Extensions for Japan

802.11k - Radio resource measurements

802.11n - Higher throughput improvements

802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)

802.11r - Fast roaming

802.11s - Wireless mesh networking

802.11t - Wireless Performance Prediction (WPP) - test methods and metrics

802.11u - Interworking with non-802 networks (e.g., cellular)

802.11v - Wireless network management

50 dB below at 22 MHz (more than four channel-widths!) from the center. Also, not all of the 14 channels are available in all countries.

The 802.11a and 11g equipment (when no 11b equipment is within range and the equipment can default to 11a-mode, as some implementations do) use a wider channel (11a at 5 GHz). At the 2.4 GHz band of 11b, 11g uses a different signal logic, OFDM, which splits the spectrum into three 20 MHz channels, each with 52 data-carrying subchannels and four pilot channels, each carried by a specific frequency or “tone” so that signal overlaps don’t matter as much. This requires a lot of extra circuitry to generate and decode tones, but everything ends up on one chip anyway so the extra cost is small.

The new 11n standard would keep all that and add more. The competing groups agree that the antenna will change to at least MIMO with two input and two output antennas. More antennas could be an option.

WWiSE defines a new peak modulation rate of 135 Mbps, with burst transmission and block acknowledgements. That is, three 4K data frames can be burst-transmitted as a single block that requires less overhead. For 100 Mbps throughput, that means the 12K must be transmitted in 960 microseconds; the 135 Mbps modulation can do it in 711 microseconds. The extra time can be used for backwards-compatibility, the space between frames that the MAC layer needs, and the receiver’s acknowledgement that it got a clean transmission.

WWiSE would use the 20 MHz channels a bit differently from the standard in 11g – 56 data carrier subchannels instead of 54, with two “pilot” subcarriers instead of four. WWiSE also has a new error-correcting code. All in all, this makes it fairly easy to accommodate existing standards in WWiSE circuitry.

TGn Sync uses 140 Mbps modulation and another trick, MIMO Spatial Division Multiplexing, to promise up to 315 Mbps with two antennas and twice that with extra antennas. The channel width would “scale,” or adjust to signal needs, going as wide as 40 MHz. It has TRMS (Timed Receive Mode Switch-

ing) and MRA (Multiple Receiver Addressing) to reduce power requirements – great for portable equipment. TGn Sync also calls for worldwide commonality of equipment, using internal logic to adjust to different countries’ regulatory requirements automatically.

This is not entirely new. There is a proprietary “Super G” Wi-Fi used in some wireless hotspots that allows 108 Mbps with channel bonding. It can interfere with other networks and is incompatible with some laptop 11g cards.

Wi-Fi Alliance

Engineers on IEEE committees write the standards but they don’t test for compliance. The Wi-Fi Alliance, a trade association made up of all vendors who make 802.11 equipment, monitors that. The alliance owns the “Wi-Fi” trademark, and applies it to 802.11a, b, g and i (the 802.11i security standard is called WPA2). The Wi-Fi Alliance is no stranger to draft standards. In fact, it supported an interim security protocol, Wi-Fi Protected Access (WPA), which was based on the draft standard from 802.11i. The final standard, dubbed WPA2, is what is supported now. (It uses AES instead of RC4, which was used in WEP and WPA; there’s a good white paper on data security for public Wi-Fi networks at http://www.wi-fi.org/membersonly/getfile.asp?f=WPA_for_Public_Access_Final.pdf.)

But the Wi-Fi Alliance has been upset at “Pre-n” products, which are not based on even a draft standard. The alliance says it will not certify Pre-n products and will in fact strip certification claims from companies that claim 802.11n compatibility but whose products impede the performance of other Wi-Fi equipment. This is a first for the Alliance.

The next meeting of the 802.11 Working Group and the 11n Task Group will be July 18-22 in San Francisco. The fate of 802.11n could be decided there. ♦

About the Author

Steve Ross is Editor-in-Chief at Broadband Properties. As an ASTM member for more than 30 years, he’s no stranger to standards-setting. He can be reached by email at steve@broadbandproperties.com.

4COM

Committed to providing the most knowledgeable service and efficient access to cable television programming.

800-737-0852
www.4com.com

teleguide

Get closer to your customers with **TeleGuide.**



The **TV Listings Channel** displays two hours of current and upcoming programming.



CTV provides a place to post community information, notices and ads.

800-737-0852
www.teleguide.tv