

Intel and 802.11

Helping Define 802.11n and other Wireless LAN Standards

IEEE 802.11 wireless local area networks

Intel is working with standards leaders on ratifying 802.11n, a new faster version of the 802.11 standard. Ratification is expected in December 2009 and publication in early 2010. Products are already on the market adhering to the Wi-Fi Alliance's 802.11n draft 2.0 certification, demonstrating the wellspring of support for this upcoming standard.

Did You Know?

The term "Wi-Fi" was the invention of what is now called the Wi-Fi Alliance (WFA—formerly known as the Wireless Ethernet Compatibility Alliance). The WFA decided the term "IEEE 802.11b-compliant" was too long and hard for consumers looking for certified products to remember. "Wi-Fi" meant nothing at the time, but sounded like "hi-fi," a familiar term to consumers. Later on, the meaning "wireless fidelity" was attached to "Wi-Fi."

802.11 is a group of specifications developed by the Institute of Electrical and Electronics Engineers Inc. (IEEE) for wireless local area networks (WLANs). These specifications define an over-the-air interface between a wireless client and a base station (or access point), or between two or more wireless clients.

Known more popularly as Wi-Fi*, 802.11 has taken the world by storm. According to data released by the Wi-Fi Alliance and In-Stat, Wi-Fi chipset sales were estimated at 300 million units for 2007¹. This milestone represents a 41 percent growth rate from 2006, in which 213 million chipsets were shipped². In-Stat predicts that by 2011 approximately 700 million devices will ship with Wi-Fi on board³. Nearly 50 percent of the chipsets sold in 2008 are predicted to adhere to the 802.11n draft standard⁴. ABI research forecasts that by 2013 more than 90 percent of Wi-Fi products will support 802.11n⁵.

"Wi-Fi Certified 802.11n will eventually surpass wired Ethernet as the dominant enterprise LAN access technology."

– Paul DeBeasi, senior analyst at the Burton Group (a research firm focused on in-depth analysis of enterprise technologies).

Intel employees continue to play a key role in the IEEE and Wi-Fi Alliance in shepherding this new wireless LAN standard. Intel sees 802.11n as vital for redefining the wireless experience by enabling multiple HDTV and digital video streams in the home and advanced applications in enterprise networks. Products based on the IEEE 802.11n draft 2.0 deliver up to five times the throughput of previous 802.11 standards, as well as improved range±. This new standard will support consumer electronics, PC and handheld platforms at speeds potentially up to 600 Mbps◇ (over-the-air throughput with maximum bandwidth channels and multiple antenna configurations). Businesses see 802.11n as a way to free them from the burden of laying and maintaining Ethernet cabling. It will also help them handle more clients and increase the range and performance of hotspots.

To better understand the significance of where 802.11 is going, let's look at how it began.

A short history of 802.11

Wi-Fi sprang into existence as a result of a decision in 1985 by the United States Federal Communications Commission (FCC) to open several bands of the wireless spectrum for use without a government license. These so-called "garbage bands" were already allocated to equipment such as microwave ovens that use radio waves to heat food. To operate in these bands though, devices would be required to use "spread spectrum" technology. This technology spreads a radio signal out over a wide range of frequencies making the signal less susceptible to interference and difficult to intercept.

"Wi-Fi technology is clearly poised to experience strong growth in China over the next few years," says Kevin Li, telecom research director at In-Stat China. "While about 20 percent of Internet households use Wi-Fi today, 67 percent of Internet households that plan to install networks soon plan to use Wi-Fi. What's

more, there is keen interest in the next generation of Wi-Fi applications and devices. About half of Chinese Wi-Fi hotspot users have adopted Wi-Fi enabled handsets and 58 percent of cellular users in China want Wi-Fi on their next handset." (Source: Wi-Fi Alliance press release, July 14, 2008)

In 1990, a new IEEE committee called 802.11 was set up to look into getting a standard started. It wasn't until 1997 though, some 8 or 9 years later, that this new standard was published (though pre-standard devices were already shipping).

Two variants were ratified over the next two years — 802.11b which operates in the industrial, medical and scientific (ISM) band of 2.4 GHz and 802.11a which operates in the bands of 5.3 GHz and 5.8 GHz.

Wi-Fi's popularity took off with the growth of high-speed broadband Internet access in the home. It was and remains the easiest way to share a broadband link between several computers located in various parts of a home. The growth of hotspots, free and fee-based public access points, have added to Wi-Fi's popularity. A third variant, 802.11g was ratified in June 2003. Like 802.11a, it uses a more advanced form of modulation called orthogonal frequency-division multiplexing (OFDM). Using the 2.4 GHz band, 802.11g can achieve speeds of up to 54 Mbps. Other amendments have been approved since then, such as 802.11i for security, but until now, none targeting performance.

Where 802.11a, b and g fall short

Today 802.11 is rapidly proliferating all over the planet. Nonetheless, it still faces a number of technological challenges. A major one is throughput. As today's multimedia needs grow, particularly video and voice, the shortcomings of 802.11a, b and g in terms of data throughput speeds become more apparent. Other issues needing more attention include security, roaming and quality of service (QoS) enhancements. Through a variety of wireless LAN standards (such as 802.11n, 802.11w, 802.11r and 802.11aa), Intel and the industry are working on these and other 802.11 issues.

802.11n: the logical next step for 802.11

Wireless LAN Throughput by IEEE Standard

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps

802.11n	Up to 600 Mbps‡	Up to 400 Mbpsθ
---------	--------------------	--------------------

With 802.11n, the industry has an excellent solution for increasing data throughput speed and potentially range. While 802.11a/b/g WLANs provide adequate performance for today's networking applications where the convenience of a wireless connection is the chief value, next generation wireless applications require higher WLAN data throughput. For this reason, Intel product groups and Intel research and development employees have played and continue to play major roles in both the IEEE 802.11n Task Group and the Wi-Fi Alliance.

A major part of this work has been helping the task group define modifications to the Physical Layer and Media Access Control Layer (PHY/MAC) to deliver a minimum of 100 Mbps throughput at the MAC service access point (SAP). This minimum throughput requirement approximately quadruples WLAN throughput performance compared to today's 802.11a/g networks. Over-the-air throughput is targeted to exceed 200 Mbps to meet the 100 Mbps MAC SAP throughput requirement. Other improvements attributable to the support for multiple antennas include better range at given throughputs and improved, more uniform service within the coverage of an access point (Basic Service Set - BSS). Wider bandwidth channels and multiple antenna configurations could eventually lead to data rates of 600 Mbps.

The 802.11n standard will also ensure a smooth transition by requiring backward compatibility with existing IEEE WLAN legacy solutions (802.11a/b/g). As for security amendments, 802.11n is fully compatible with 802.11i (data protection), 802.11r (secure inter-access point roaming), and 802.11w (management frame protection).

Intel has contributed to the development of the 802.11n standard in many ways. At the formative stages of the process, an Intel employee chaired the task group committee responsible for the core documents being used to guide the group's development of the 802.11n standard. As part of the task group, Intel employees contributed to the development of channel models, usage models, functional requirements, and comparison criteria. Intel employees have provided technical submissions on MAC and PHY technologies, performance measurement methodologies, and simulation methodologies. Intel was also a founder member of a group of companies that formed a special interest group (SIG), known as the Enhanced Wireless Consortium, to accelerate convergence on a widely supported proposal. After selection and approval of the proposal, Intel supported the lengthy fine-tuning process (known as comment resolution) by providing the task group's technical editor and one of its technical group leaders. For the Wi-Fi Alliance, Intel helped coauthor this certification group's marketing requirements document (MRD) for High Throughput WLANs (802.11n).

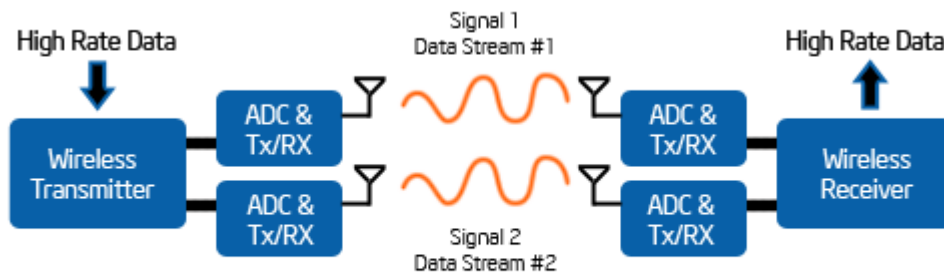
Increasing throughput with multiple antenna systems

One approach to increasing the physical transfer rate of 802.11 wireless systems is using multiple antenna systems for both the transmitter and the receiver. This technology is referred to as multiple-input multiple-output (MIMO), or smart antenna systems. MIMO technology plays an important role in achieving the 802.11n goals, and Intel has contributed much research to MIMO.

MIMO exploits the use of multiple signals transmitted into the wireless medium and multiple signals received from the wireless medium to improve wireless performance. Employing multiple diverse antennas tuned to the same channel, each transmitting with different spatial characteristics, MIMO uses spectrum more efficiently without sacrificing reliability. Every receiver listens for signals from every transmitter, enabling path diversity where multi-path reflections (normally disruptive to signal recovery) may be recombined to enhance the desired signals.

Another valuable benefit MIMO technology provides is Spatial Division Multiplexing (SDM). SDM spatially multiplexes multiple independent data streams (essentially virtual channels) simultaneously within one spectral channel of bandwidth. In essence, multiple antennas send different flows of individually encoded signals (spatial streams) over the air in parallel to shove more data through a given channel. At the receiving end, each antenna sees a different mix of the signal streams and the device "demultiplexes" them to use them. MIMO SDM can significantly increase data throughput as the number of resolved spatial data

streams is increased. Each spatial stream requires its own transmit/receive (TX/RX) antenna pair at each end of the transmission.



How a Smart Antenna (MIMO) System Works

It is important to understand that MIMO technology requires a separate radio frequency (RF) chain and analog-to-digital converter (ADC) for each MIMO antenna. Implementations requiring more than two RF antenna chains need to be carefully architected to keep costs down while maintaining performance expectations. Intel has already shown this can be done and introduced an Intel® Centrino® 2 platform with a wireless adapter (the Intel WiFi Link 5300) featuring support for three antennas running three spatial streams.

Meeting throughput demands by combining MIMO with wide bandwidth channels

An important tool for increasing the physical transfer rate is wider bandwidth spectral channels. Using a wider channel bandwidth with orthogonal frequency division multiplexing (OFDM) offers significant advantages when maximizing performance. (OFDM is a multi-carrier transmission technique that has been recently recognized as an excellent method for high speed bi-directional wireless data communication.) Wider bandwidth channels are cost effective and easily accomplished with moderate increases in digital signal processing (DSP). If properly implemented, doubling the legacy bandwidth of 802.11 20 MHz channels to 40 MHz can provide greater than two times the usable channel bandwidth used presently. Coupling MIMO architecture with wider bandwidth channels offers the opportunity of very powerful, yet cost effective approaches for increasing the physical transfer rate.

"The promise of 11n is more than simply going faster," says Phil Belanger, managing director for Novarum. "The increased range of 11n will make it more practical to deploy large systems using the 5-GHz band, which has many more channels than the 2.4-GHz and has not been used very much to date. That, in turn, will enable much higher capacity wireless LANs. For many enterprises, a wireless network that delivers hundreds of megabits of capacity everywhere will be good enough to be the only network." (Source: Network World, "Wireless Networks: The Burning Questions," June 11, 2007)

MIMO approaches that use only 20 MHz channels will require higher implementation costs to meet the Task Group n requirement of 100 Mbps throughput at the MAC SAP. Meeting the IEEE Task Group n requirement with only 20 MHz channels would require at least three antenna analog front ends at both the transmitter and receiver. At the same time, a 20 MHz approach will struggle to provide a robust experience with applications that demand higher throughput in real user environments.

Intel believes both MIMO technology and wider bandwidth channels will be required to reliably satisfy the higher throughput demands of consumer electronics applications. This will become increasingly true as BSS environments need to service multiple high throughput applications simultaneously, especially where servicing networking applications is also required. Choosing conservative increases in channel bandwidth, combined with conservative approaches in MIMO technology, will enable cost effective solutions that meet the high demands of these types of applications. This combined approach, employing MIMO and 40 MHz channels will enable the IEEE 802.11n technology to reach even higher performance as Moore's Law and CMOS process technology improvements advance DSP capabilities.

Coexistence with legacy devices

There has been some concern about potential coexistence problems with other devices – such as existing 802.11a/b/g devices and those using Bluetooth* technology – when using 40 MHz in the 2.4 GHz band. To address this issue, the 802.11n draft includes a variety of solutions. One mechanism specifically designed to protect legacy networks from possible disruption by 802.11n traffic is called non-high throughput (non-HT) duplicate mode. Prior to a device using 802.11n-specific protocols, this mechanism sends two packets on both halves of the 40 MHz channel that announce the network allocation vector (NAV). This lets legacy stations know how long to stay off the air. Following the non-HT duplicate mode NAV message, the 802.11n protocol can be used for the announced duration of time without disturbing legacy networks.

Another mechanism, designed to protect Bluetooth devices is a means of signaling that the wireless network should not use the wider (40 MHz) channel width. An 802.11n device that knows of potential interference with Bluetooth (e.g. a laptop with both 11n and BT) can force its BSS and neighboring BSS's to stop transmitting 40 MHz. This reduces any potential impact on these devices to the same level as existing 802.11b/g devices.

Whenever 802.11 stations or access points detect the presence of legacy devices or nearby networks, they are required to use protection protocols, such as non-HT duplicate mode, or respond in other defined ways. This ensures that 802.11n draft 2.0-certified devices can be gradually deployed within legacy networks or side-by-side with legacy networks without the need to upgrade the entire network to 802.11n.

Enabling next generation digital media through QoS

While data and audio transferring have long been the primary attractions for most Wi-Fi users, streaming video is a large part of the action today. Witness the fast rise and popularity of YouTube and movie downloads. In the past, quality of service issues with 802.11a/b/g have hurt performance, making streaming video difficult and unsatisfying. Video images could be jittery and halt when the network gets overloaded.

Wi-Fi hotspots are continuing their torrid growth in 2008. According to ABI Research's WI-FI Hotspots Forecasts, by the end of this year global hotspots will grow by 40 percent over 2007. The greatest growth and the largest number of hotspots continue to be found in Europe. While the UK has long led in European Wi-Fi hotspots, there is also marked growth in France, Germany, and Russia.

To improve video streams, Wi-Fi certified 802.11n draft 2.0 products are required to pass the Wi-Fi WMM (Wi-Fi Multimedia) QoS certification based on the 802.11e draft standard. This brings prioritization to latency-sensitive streams like voice and video to help avoid performance degradation. The high bandwidth and QoS of Wi-Fi certified 802.11n draft 2.0 systems is also designed to help ensure that an Internet connection can be reliably shared by the increasing number and type of Wi-Fi enabled devices in a home or office without degradation of service. The higher data rates of 802.11n also increase the throughput capacity of overlapping Wi-Fi networks.

An amendment improves Wi-Fi roaming experiences and enables new secure and QoS-enhanced Voice-over-WLAN usages in the enterprise and public hotspots. The 802.11r (Fast BSS Transition) amendment allows a roaming user device to procure QoS parameters at a new access point before making a transition away from the original access points. This solves a handover delay problem formerly experienced with 802.11 devices that frequently caused lost connections and voice quality degradation.

Getting the hop on mesh networking

Mesh networking, also known as "multi-hop" networking, is a flexible architecture for moving data efficiently between wireless devices. Mesh technology expands the reach of wireless networks by allowing signals to be passed from one wireless router to another. By placing wireless routers every few hundred feet, signals can be beamed for miles. Mesh networking is being used to enable Wi-Fi access for residents in metropolitan areas such as Minneapolis, Minnesota, Singapore, and Fulham, West London, for emergency response services in cities like Beijing, and for surveillance in cities like Chicago. Mesh networking can also be used on a smaller scale in settings such as the home. Every radio-enabled device in a home can be designed to assume one of three roles: client, router, or proxy. Devices can self-organize into temporary, ad hoc networks that emerge and disband in response to user needs.

Mesh networking is a key aspect of ongoing efforts in both 802.11 and 802.16 (WiMAX) standards. A key benefit of 802.11n is that high-speed core networks built from a mesh of intercommunicating Draft 2.0 802.11n nodes can alleviate the need to cable every wireless LAN access point to an Ethernet switch. Intel is contributing to mesh networking standards through employee participation in IEEE and other industry groups, as well as doing research of its own into architectures for interconnecting wireless devices of all kinds.

Improving security

A major problem for all wireless LANs (and for that matter all LANs) is security. As anyone who uses the Internet knows, security is a difficult issue requiring constant attention.

"The biggest threat is people who use open Wi-Fi access points and don't use encryption or VPNs," says David Kotz, Dartmouth professor of computer science. "They trust some random hot spot operator or open access point somewhere with their personal or professional data. People are careless."

From the very beginning, wireless LANs proved tricky to secure. Hackers easily cracked such initial efforts as the Wired Equivalent Privacy (WEP), an early security protocol. This left some companies hesitant to adopt wireless technology for fear that the data transmitted between a wireless device and an access point could be intercepted and decrypted.

To shore up a battered security model that was slowing wireless adoption in the enterprise and making home users nervous, IEEE 802.11 initiated work in the 802.11i Task Group. This group was tasked with building a comprehensive security model for providing 128-bit AES encryption and authentication for data protection. An Intel employee led the specification development as the Technical Editor of 802.11i. The Wi-Fi Alliance introduced its own interim version of the 802.11i security specification: Wi-Fi Protected Access (WPA). WPA combined several technologies to address known 802.11 WEP security vulnerabilities. It provided strong user-based authentication through the use of the 802.1X standard (a mutual authentication framework designed to provide controlled port access between wireless client devices, access points, and authentication servers) and the Extensible Authentication Protocol (EAP). WPA provided interim enhancements to the WEP encryption engine through 128-bit encryption keys and the use of the Temporal Key Integrity Protocol (TKIP). A message integrity check (MIC) prevented attackers from capturing and altering or forging data packets. This combination of technologies protected the confidentiality and integrity of WLAN transmissions while helping to ensure through security access control that only authorized users gained access to the network. WPA further enhanced security and access control for clients by creating a fresh, unique master key between each user device and access point, providing session authentication and fresh random key generation, and unique, per-packet encryption keys.

The IEEE standard, 802.11i, ratified in June 2004, strongly enhanced many of the features already in practice through WPA. The WiFi Alliance incorporated these security enhancements in its WPA2 program, making WPA2-enhanced 802.11 ready for widespread enterprise and high-security zone deployments. Some substantial 802.11i (WPA2) changes over WPA involve use of the 128-bit Advanced Encryption Standard (AES). WPA2 uses AES in Counter with CBC-MAC mode (a mode of operation for a block cipher that enables a single key to be used for both encryption and authentication) to provide data confidentiality, authentication, integrity, and replay protection. The 802.11i standard also offers key caching and pre-authentication to streamline user authentication to an access point. With 802.11i, the entire security chain for logging in, exchanging credentials, authenticating, and encryption becomes much more robust and effective in protecting against both non-targeted and targeted attacks. WPA2 allows multiple credentials for authentication, which enables a WLAN administrator to refocus from worrying about security to managing operations and devices. Both 802.11i and 802.11w security mechanisms protect 802.11n networks.

Wireless LAN standards and amendments in which Intel is participating or has participated.

802.11 The original WLAN Standard. Supports

1 Mbps to 2 Mbps.

- 802.11a High speed WLAN standard for 5 GHz band. Supports 54 Mbps.
- 802.11b WLAN standard for 2.4 GHz band. Supports 11 Mbps.
- 802.11d International roaming — automatically configures devices to meet local RF regulations
- 802.11e Addresses quality of service requirements for all IEEE WLAN radio interfaces.
- 802.11f Defines inter-access point communications to facilitate multiple vendor-distributed WLAN networks.
- 802.11g Establishes an additional modulation technique for 2.4 GHz band. Supports speeds up to 54 Mbps.
- 802.11h Defines the spectrum management of the 5 GHz band.
- 802.11k Defines and exposes radio and network

information to facilitate radio resource management of a mobile Wireless LAN.

802.11n Provides higher throughput improvements. Intended to provide speeds up to 500 Mbps.

802.11s Defines how wireless devices can interconnect to create an ad-hoc (mesh) network.

802.11r Provides fast (<50 millisecond), secure and QoS-enabled inter-access point roaming protocol for clients.

802.11u Adds features to improve interworking with external (non-802) networks where the user is not pre-authorized for access.

802.11v Enhances client manageability, infrastructure assisted roaming management, and filtering services.

802.11z Creates tunnel direct link setup between clients to improve peer-peer

video throughput.

**Robust video
802.11aa transport
streaming.**

Intel employees worked closely with Cisco and other members of the 802.11 community to develop the aforementioned 802.11r, the secure, QoS-enhanced inter-access point roaming protocol amendment in 802.11. The 802.11r amendment, ratified in July 2008, builds upon the 802.11i security by providing faster (sub-50 millisecond) and secure key hierarchy-based handoffs when a user roams between access points. 802.11r enables user-undetectable inter-access point roaming for Multimedia-over-Wi-Fi applications, access point load balancing, and salt-and-pepper (dual-grid) usages in enterprises, healthcare, and operator deployments. 802.11r is fully compatible with 802.11a/b/g/n.

An Intel employee is Chair of the 802.11w Task Group for security enhancements. This group's charter is to extend 802.11i data frames protection schemes to a critical subset of 802.11 management frames. 802.11w brings management frames security on par with data frames security (802.11i) by securing 802.11 management frames against illegal eavesdropping, in-flight illegal modifications, unauthorized replays, and providing source authentication.

What lies ahead

Obviously, the wireless broadband vision of freedom from wired Internet connections is becoming a reality in many parts of the world. What's driven this success is having a standard. Like the Ethernet standard has been to networking, 802.11 has been to wireless communications. The standard has been crucial to industry innovation and acceptance of 802.11 products. Because of it, customers enjoy the ability to buy 802.11 devices with assurance of the interoperability, and the Wi-Fi industry has profited from the fast growth spawned by having an open standard.

802.11n is just now showing its promise. Other wireless technologies, such as [WiMAX](#), which is based on the IEEE 802.16 standard, will have much to add as well. IEEE 802.16 is a wide area wireless technology that supports full mobility of users and offers optimal spectral efficiency. The combination of outdoor WiMAX and indoor Wi-Fi provides ubiquitous and cost-effective mobile Internet to the mass market.

Intel is currently working on another promising wireless technology for the Very High Throughput (VHT) study group. This is an effort to create a gigabit (Gbit) version of Wi-Fi running at 60GHz for increasing the speed of existing wireless LAN applications and meeting the needs of new applications such as wireless interconnections for home audio-visual equipment via wireless. The goal is to pump data at several Gbits per second (Gbps). This will only work for short distances (a few meters, or perhaps as much as 10 meters with beamforming – a signal processing technique used in sensor arrays for directional signal transmission or reception), but would be perfect in home environments. Current ideas call for it to let users quickly fallback from 60GHz to 5GHz or 2.4GHz 802.11n networks when needed. It will also support compatibility with the existing 802.11 services, access points and base stations as well as its management features such as association, authentication and security. The 802.11 Working Group is considering an IEEE Project Authorization Request (PAR) for VHT at 60 GHz.

Intel is committed to 802.11 in all its "flavors" and will continue to drive the industry standards, ecosystem development and end-user awareness necessary for the broad proliferation of broadband wireless. The innovation that has led to 802.11's success will continue as wireless networking is adapted to touch every facet of our lives, from homes and cars to office buildings, factories, and health care institutions.

Learn more

Visit the [802.11 Working Group](http://grouper.ieee.org/groups/802/11/) (<http://grouper.ieee.org/groups/802/11/>) site and the [Wi-Fi Alliance](http://www.wi-fi.org/) (<http://www.wi-fi.org/>) site.

The links on this page will take you from the Intel Web site. Intel does not control the content on these Web sites.

¹ "Wi-Fi Industry to Ship 300 Million Chipsets in 2007," Wi-Fi Alliance press release, December 3, 2007.

² Ibid.

³ Ibid.

§ "802.11n Equipment Sales Show Continued Momentum One Year After Wi-Fi Alliance Certification Program Begins," Wi-Fi Alliance press release, June 23, 2008.

° Ibid.

± Ibid.

◇ "Wi-Fi CERTIFIED™ 802.11n draft 2.0: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks," Wi-Fi Alliance white paper, 2007.

‡ Conversation with Eldad Perahia, author with Robert Stacey of "Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n," Cambridge University Press, 2008. These figures are best case, with all efficiency techniques implemented.

θ Ibid.