July 26, 2007

start:Taming the Beast: 802.11n Coexistence with legacy networks

Without protection protocols, 802.11n devices can hamper the performance of legacy networks, particularly in the 2.4GHz band

By Fanny Mlinarsky, octoScope

Since testing began on June 25 2007, the Wi-Fi Alliance has been certifying 802.11n draft 2.0 devices for interoperability and backwards compatibility. As of this writing, the number of certified products is 14 and counting[1].

Will these devices disrupt legacy networks? Will 802.11n-based video streaming applications operating in the double-width 40 MHz channels squeeze out low data rate applications such as VoIP and remote control?

802.11n coexistence issues and protection mode

The emerging 802.11n specification is more than just a new physical layer (PHY) for 802.11. It is a whole new standard with efficiency improvements at the MAC (medium access control) and PHY.

These improvements bring impressive range and throughput performance to new generation Wi-Fi networks promising streaming video in the home and support for mission critical applications in the office with throughput approaching that of Ethernet.

However, without proper protection protocols, 802.11n devices have the potential of hampering the performance of legacy networks.

To achieve backwards compatibility and coexistence with legacy networks, 802.11n has to pay special attention to the 802.11 collision avoidance protocol. Collision avoidance is central to all 802.11 networks and lets multiple stations share the airlink efficiently.

Without collision avoidance, stations are unable to get on and off the air in an orderly way and may disrupt each other's access to the airlink, drastically reducing aggregate throughput of the network.

For collision avoidance to work, all stations must be able to interpret each other's packets and exchange information on how long each station intends to occupy the medium.

With major changes to the 802.11 PHY and MAC layers, native 802.11n transmissions cannot be interpreted by the legacy 802.11 a/b/g stations and have the potential of disrupting the collision avoidance protocol for these networks. 802.11n transmissions may appear to legacy stations as strong and pervasive interference—packets that legacy stations are unable to interpret.

Footnotes:

[1] 801.11n draft 2.0 certified products are listed at http://certifications.wi-fi.org/wbcs_certified_products.php?.

Draft IEEE 802.11n specification is based on MIMO (multiple-input multiple-output) radio technology. MIMO is a major innovation in wireless data transmission and a technology that is being adapted by other standards, including WiMAX and LTE (long term evolution), the emerging standard for 4G cellular.

MIMO uses *spatial multiplexing* to transport two or more data streams simultaneously in the same frequency channel. When two spatial streams are transmitted, spatial multiplexing can double the throughput of a wireless channel.

While legacy 802.11 a/b/g networks operate in 20 MHz channels, 802.11n can use 20 or 40 MHz channels with up to 4 spatial streams per channel. With 4 spatial streams in a 40 MHz channel the maximum transmission data rate is 600 Mbps. Current products can transmit at up to 300 Mbps using 2 spatial streams in a 40 MHz channel.

In addition to spatial multiplexing, PHY improvements include more efficient OFDM and short GI (guard interval)[2]. With 52 data sub-carriers, the highest data rate per stream of 802.11n is 65 Mbps vs. 54 Mbps for the 48 data sub-carrier legacy technology.

Legacy 802.11a/b/g devices use 800ns GI, while 802.11n devices can optionally use GI of 400ns shortening the OFDM symbol by 400 ns. Short GI reduces the symbol time from 4 microseconds for legacy networks to 3.6 microseconds for 802.11n thereby increasing the symbol rate by 10%.

To reduce the protocol overhead at the MAC layer, 802.11n has introduced *frame aggregation* and *block acknowledgement* mechanisms. Frame aggregation is the method of combining several frames into one, thereby reducing the number of inter-frame gaps and acknowledgement (ACK) frames, which take up a significant percentage of the airlink capacity.

Aggregate frames called A-MPDUs (aggregate MAC protocol data units) can reach the length of 64k bytes and be composed of multiple traditional frames that can range in size from 52 bytes to 2304 bytes.

Block ACK is the method of sending a single acknowledgement packet to confirm receipt of multiple frames. Block ACK improves protocol efficiency by removing the need to transmit an ACK frame for every data frame on the airlink as is done in the legacy 802.11 networks.

While the block ACK protocol exists in the current 802.11 standard, it isn't widely deployed. 802.11n has shortened the block ACK frame from the legacy 128 bytes to 8 bytes to improve airlink efficiency.

Footnotes:
[2] GI (guard interval) is a time period at the end of each OFDM symbol introduced to let multipath reflections settle prior to transmitting the next symbol.

Collision avoidance
NAV (network allocation vector) is the main mechanism of collision avoidance in 802.11 networks. NAV is the indicator of time kept by each station when transmission onto the wireless medium cannot be initiated. NAV information is derived by each station from the announcements by other stations of how long they intend to occupy the medium.

The new 802.11n protocols, such as more efficient OFDM, short GI, aggregate frames and block ACK, cannot be interpreted by the legacy devices and this can pose a serious disruption to the legacy networks that wouldn't know how to predict the duration of such traffic on the airlink and thus wouldn't be able to avoid colliding with it.

To address this issue, the 802.11n draft incorporates a protocol designed to protect legacy networks from the potential disruption by 802.11n traffic. This *protection protocol* is called *Non-HT* (High Throughput) *duplicate mode.*

In non-HT mode, prior to the use of 802.11n protocols, two packets are sent on both halves of the 40 MHz channel simultaneously announcing the NAV to let the legacy stations know how long to stay off the air. Following the non-HT duplicate mode NAV message, the legacy stations make no attempt to interpret any transmissions and keep themselves off the air for the announced duration of time while the 802.11n stations communicate with each other using native 802.11n protocols and taking advantage of new throughput enhancements.

Perils of 40 MHz operation in the 2.4 GHz band
Since only 70 MHz is available in the 2.4 GHz band already crowded with 802.11b and g networks, 40 MHz operation of 802.11n has a good chance of overlapping in frequency with existing networks.

The issue of 40 MHz operation in the 2.4 GHz band has been contentious at IEEE and is addressed in draft 2.0 by new coexistence protocols. Coexistence includes methodology for detecting WLAN activity in the band and for switching channels when necessary to avoid interference.

These are complex protocols requiring coordinated periodic scanning of all available channels by multiple stations in the network. In the 2.4 GHz band, where channels are defined on a 5 MHz boundary, there are 11 possible overlapping channels that all have to be scanned to detect legacy interference.

Due to the complexity of managing 40 MHz operation in the 2.4 GHz band, the Wi-Fi Alliance certification only allows the use of 40 MHz channels in the 5 GHz band. Coexistence is less of a concern in the 5 GHz band where more spectrum is available and where the channels are on a 20 MHz boundary making detection and avoidance of adjacent services easier.

Summary
Draft 802.11n equipment compliant with the Wi-Fi Alliance 802.11n certification is expected to be aware of and interoperate with the legacy equipment.

When 802.11 stations or APs detect the presence of legacy devices or nearby networks, they are required to use protection protocols such as Non-HT duplicate mode.

The issue of 40 MHz channels in the 2.4 MHz band remains a concern with the protocol for interference avoidance still unsettled in the 802.11n draft.

About the author
Fanny Mlinarsky *is an expert in wireless and RF data communications. She has served in key technology roles at Agilent, Azimuth and octoScope (www.octoscope.com), a Boston area consulting company.*