Whitepaper | AirMagnet | August 05, 2008

802.11n Primer

The 802.11n standard promises to extend today's most popular WLAN standard by significantly increasing reach, reliability, and throughput. The final standard, predicted to be ratified in this year, is expected to trigger broad-scale deployment of bigger, better, faster networks.

The time has come for businesses to take advantage of 802.11n. Some will get their feet wet with draft 2.0 products, using firmware updates to apply the minor tweaks likely in the final standard. Others will await ratification before purchasing products that implement the final IEEE Standard 802.11n-2008. In both cases, network planners and administrators need to understand the business benefits and technical challenges posed by 802.11n. This paper explains the essential new technologies used by 802.11n and their impact on network planning, installation, and operation.

AIRMAGNET®
Wireless Network Assurance

AIRMAGNET®
Wireless Network Assurance

Table of Contents

Understanding 802.11n concepts

The 802.11n amendment includes many enhancements that improve WLAN range, reliability, and throughput. At the physical (PHY) layer, advanced signal processing and modulation techniques have been added to exploit multiple antennas and wider channels. At the Media Access Control (MAC) layer, protocol extensions make more efficient use of available bandwidth. Together, these High Throughput (HT) enhancements can boost data rates up to 600 Mbps – more than a ten-fold improvement over 54 Mbps 802.11a/g (now considered to be legacy devices).

However, real-world WLAN performance is always impacted by numerous variables, from the surrounding RF environment to product selection, placement, and configuration. When deploying 802.11n, it is critically important to understand what these High Throughput enhancements actually do, how they impact and coexist with legacy 802.11a/g WLANs, and which of the many optional "n" features your new products actually support.

Multiple Input Multiple Output (MIMO)

Behind most 802.11n enhancements lies the ability to receive and/or transmit simultaneously through multiple antennas. 802.11n defines many "M x N" antenna configurations, ranging from "1 x 1" to "4 x 4". This refers to the number of transmit (M) and receive (N) antennas – for example, an AP with two transmit and three receive antennas is a "2 x 3" MIMO device.

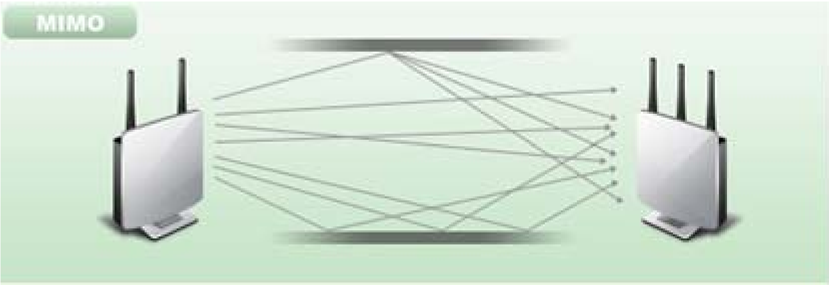

Figure 1. Multiple Input Multiple Output

In general, the more antennas an 802.11n device uses simultaneously, the higher its maximum data rate. However, multiple antennas do not by themselves increase data rate or range. Those improvements come from how the MIMO device actually *uses* its multiple antennas – that is, the advanced signal processing techniques introduced by 802.11n (Figure 2.)

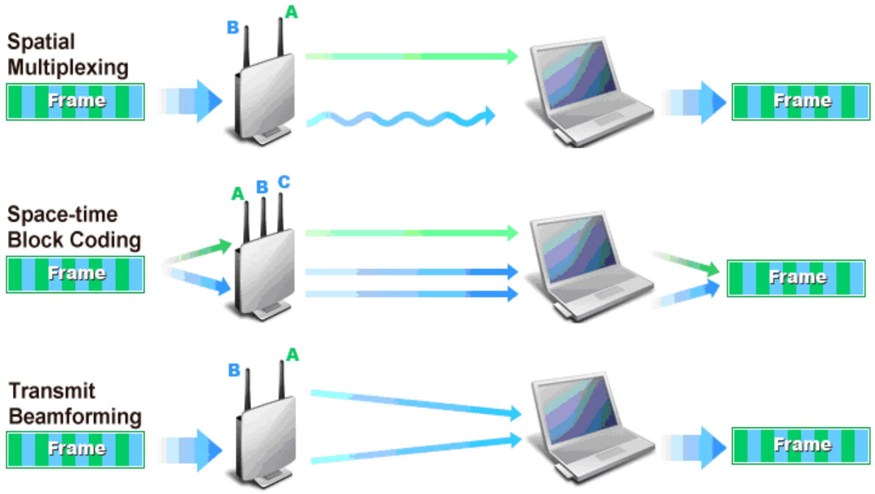

Figure 2. 802.11n Signal Processing Techniques that use MIMO Antennas

Spatial Multiplexing (SM) subdivides an outgoing signal stream into multiple pieces, transmitted through different antennas. Because each transmission propagates along a different path, those pieces – called *spatial streams* – arrive with different strengths and delays. Provided the individual streams arrive at the receiver with sufficiently distinct spatial signatures, an SM enabled receiver is able to reassemble them back into the original signal stream. Multiplexing two spatial streams onto a single channel (radio frequency) effectively doubles capacity and thus maximizes data rate. All 802.11n APs must implement at least two spatial streams, up to a maximum of four. 802.11n stations can implement as few as one spatial stream.

Space-Time Block Coding (STBC) sends an outgoing signal stream redundantly, using up to four differently-coded spatial streams, each transmitted through a different antenna. By comparing arriving spatial streams, the receiver has a better chance of accurately determining the original signal stream in the presence of RF interference and distortion. That is, STBC improves reliability by reducing the error rate experienced at a given Signal to Noise Ratio (SNR). This optional 802.11n feature may be combined with SM, but can only be used when the number of transmit antennas exceeds the number of receive antennas.

Transmit Beamforming (TxBF) steers an outgoing signal stream towards the intended receiver by concentrating transmitted RF energy in a given direction. This technique leverages additive and destructive environmental impacts, exploiting RF phenomena like signal reflection and multipath to *improve* received signal strength and sustain higher data rates. To steer signal in the best direction, the transmitter needs to know how that signal will likely be received. This "channel knowledge" can be obtained implicitly (by assuming that propagation is identical in both directions) or explicitly (by obtaining feedback from the receiver). This optional 802.11n feature is not yet widely implemented.

The multiple antennas and spatial streams supported by all 802.11n APs are responsible for much of the throughput and range increase vs. legacy APs. The number of antennas and spatial streams vary, as do support for STBC and TxBF options. But only 802.11n stations can reap the benefit of High Throughput data rates.

40 MHz Channel Bandwidth

Another optional 802.11n feature that only benefits new devices are 40 MHz channels that use twice as much bandwidth to double throughput (Figure 2).

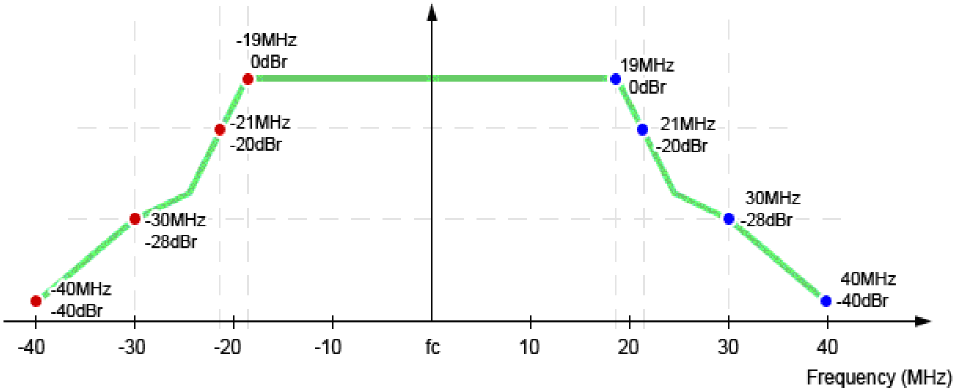

Figure 3. Spectrum Mask for 40 MHz Channel used by 802.11n

Legacy 802.11 products use channels that are approximately 20 MHz wide. In the US, 802.11b/g radios use one of 11 20 MHz channels (three non-overlapping: 1, 6, 11) within the 2.4 GHz ISM frequency band. 802.11a radios use one of 12 non-overlapping 20 MHz channels in the 5 GHz UNII band.

New 802.11n products can use 20 or 40 MHz wide channels in either the ISM or UNII band. In other words, they are allowed to use a bigger patch of bandwidth to boost throughput.

Compare those channels and APs to lanes and toll booths on a highway. Each old booth (802.11b/g AP) received cars from just one lane (20 MHz channel), while new booths (802.11n APs) can service two adjacent lanes (40 MHz channel). A new booth could handle twice as many vehicles per hour.

But the 2.4 and 5 GHz *frequency bands* did not get any bigger. That 2.4 GHz highway still has three lanes, so it can only utilize one double-wide booth. The third lane leaves room for just one legacy booth. However, the 12 lane 5 GHz highway can take far better advantage of double-wide booths while also accommodating more legacy booths. This is why most 802.11n WLANs will end up using 40 MHz channels only in the 5 GHz UNII band.

ISM use is further complicated by 802.11b/g channel overlap. When an 802.11b/g radio transmits, the modulated signal is designed to fall +/- 11 MHz from the channel center frequency. But some RF energy ends up "bleeding" into frequencies up to 30 MHz from channel center. As a result, each 802.11b/g AP actually consumes 5 overlapping channels. For example, an AP using channel 6 causes significant interference on channels 5 and 7, and some interference on channels 4 and 8. That leaves just 3 non-overlapping (simultaneously usable) 20 MHz channels: 1, 6, and 11.

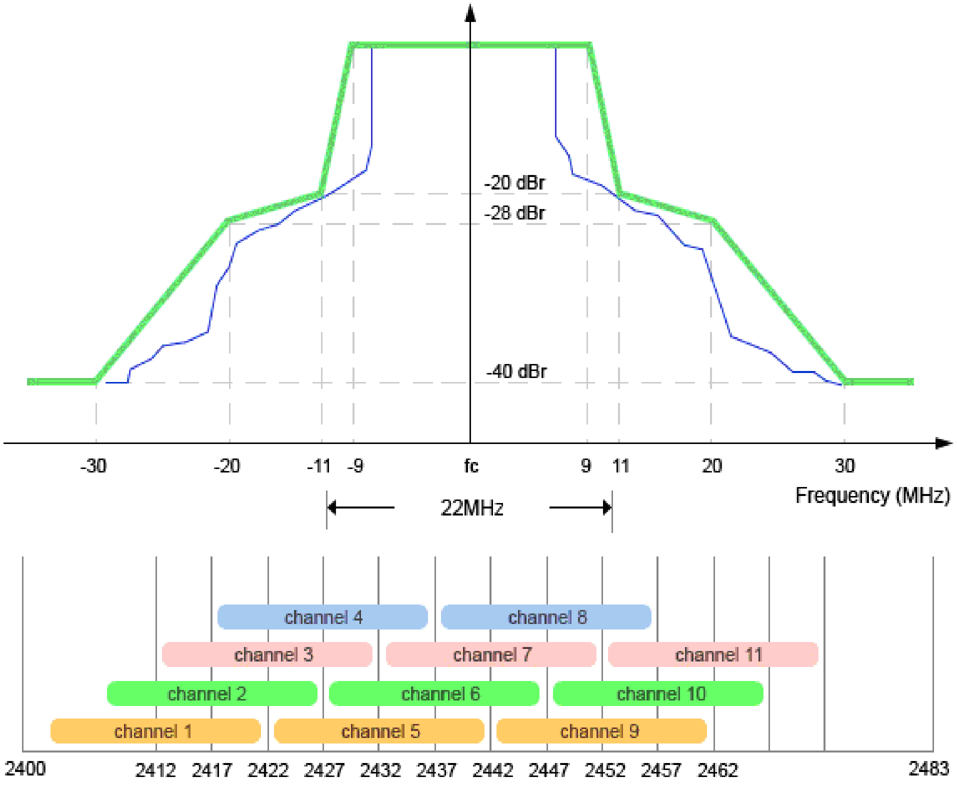

Figure 4. 20 MHz Channels used by 802.11g in ISM Band

Transmitting on a 40 MHz 802.11n channel in the ISM band would exacerbate this scarcity by consuming 9 channels: the center frequency plus four channels on the left and four on the right. Finding these many adjacent unused channels in the congested ISM band is rare; thus, 40 MHz 802.11n operation would very likely interfere with existing 802.11b/g APs. To mitigate this, 802.11n APs using 40 MHz channels are required to listen for legacy (or other non-40 MHz HT) devices and provide coexistence mechanisms (see later section).

Modulation and Coding Schemes

802.11n APs and stations need to negotiate capabilities like the number of spatial streams and channel width. They also must agree upon the type of RF modulation, coding rate, and guard interval to be used. The combination of all these factors determines the actual PHY data rate, ranging from a minimum 6.5 Mbps to a maximum 600 Mbps (achieved by leveraging all possible 802.11n options).

Because 802.11n defines 77 possible permutations of the factors that determine data rate, a clear and efficient way is needed to communicate them. The 802.11n standard defines Modulation and Coding Scheme (MCS) – a simple integer assigned to every permutation of modulation, coding rate, guard interval, channel width, and number of spatial streams. Some broadly supported 802.11n MCS values are illustrated in Table 1 (see next page).

MCS Index	Type	Coding Rate	Spatial Streams	Data Rate (Mbps) with 20 MHz CH		Data Rate (Mbps) with 40 MHz CH	
				800 ns	400 ns (SGI)	800 ns	400 ns (SGI)
0	BPSK	1 / 2	1	6.50	7.20	13.50	15.00
1	QPSK	1 / 2	1	13.00	14.40	27.00	30.00
2	QPSK	3 / 4	1	19.50	21.70	40.50	45.00
3	16-QAM	1 / 2	1	26.00	28.90	54.00	60.00
4	16-QAM	3 / 4	1	39.00	43.30	81.00	90.00
5	64-QAM	2 / 3	1	52.00	57.80	108.00	120.00
6	64-QAM	3 / 4	1	58.50	65.00	121.50	135.00
7	64-QAM	5 / 6	1	65.00	72.20	135.00	150.00
8	BPSK	1 / 2	2	13.00	14.40	27.00	30.00
9	QPSK	1 / 2	2	26.00	28.90	54.00	60.00
10	QPSK	3 / 4	2	39.00	43.30	81.00	90.00
11	16-QAM	1 / 2	2	52.00	57.80	108.00	120.00
12	16-QAM	3 / 4	2	78.00	86.70	162.00	180.00
13	64-QAM	2 / 3	2	104.00	115.60	216.00	240.00
14	64-QAM	3 / 4	2	117.00	130.00	243.00	270.00
15	64-QAM	5 / 6	2	130.00	144.40	270.00	300.00
16	BPSK	1 / 2	3	19.50	21.70	40.50	45.00
...	...	...	...	...	...	...	...
31	64-QAM	5 / 6	4	260.00	288.90	540.00	600.00

Table 1. Some 802.11n MCS Values

- **Modulation and Coding Rate** determines how data is sent over the air. For example, Binary Phase Shift Keying (BPSK) was included in by the original 802.11 standard, while Quadrature Amplitude Modulation (QAM) was added by 802.11a. Newer modulation methods and coding rates are generally more efficient and sustain higher data rates, but older methods and rates are still supported for backwards compatibility.
- **Guard Interval** is the time between transmitted symbols (the smallest unit of data sent at once). This Guard Interval is necessary to offset the effects of multipath that would otherwise cause Inter-Symbol Interference (ISI). Guard interval is like pausing between words spoken into a megaphone to overcome echo (sound wave reflection). Legacy 802.11a/g devices use an 800 ns guard interval, but 802.11n devices have the option of pausing just 400 ns. Shorter Guard Intervals would lead to more interference and reduced throughput, while a longer Guard Interval would lead to unwanted idle time in the wireless environment. A Short Guard Interval (SGI) boosts data rate by 11 percent while maintaining symbol separation sufficient for most environments.

- **Unequal Modulation** refers to using a different modulation type and coding rate on each spatial stream. MCS values 0 through 31 define the same modulation and coding will be used on all streams, while MCS values 32 through 77 describe mixed combinations that can be used to modulate two to four streams. For example, MCS 33 refers to using 16-QAM on spatial stream #1 and QPSK on stream #2, while MCS 77 refers to using 64-QAM on streams #1-3 with 16-QAM on stream #4.

802.11n APs are required to support at least MCS values 0 through 15, while 802.11n stations must support MCS values 0 through 7. All other MCS values, including those associated with 40 MHz channels, SGI, and unequal modulation, are optional. Identifying the MCS values supported in common by all of your 802.11n devices is a good way to determine the set of data rates that can actually be utilized by your WLAN.

MAC Layer Overhead Reduction

The PHY enhancements described thus far increase maximum PHY data rate, but would make very inefficient use of the airwaves without the following MAC layer enhancements also utilized by 802.11n.

- **Block Acknowledgement** reduces the number of ACKs that a receiver must send to a transmitter to confirm frame delivery. Legacy 802.11a/g transmitters expect an (almost immediate) ACK for each non-multicast/broadcast frame. But 802.11n transmitters also accept Block ACKs which confirm receipt of multiple unicast frames. For example, instead of sending 9 legacy ACKs to confirm frames 1 through 8 and 10, an 802.11n receiver can say the same thing with just one Block ACK.
- **Frame Aggregation** increases the payload that can be conveyed by each 802.11 frame, reducing MAC layer overhead from a whopping 83 % to as little as 58 % (using A-MSDU) and 14 % (when using A-MPDU). Legacy 802.11a/g devices can send no more than 2304 payload bytes per frame. But new 802.11n devices have the option of bundling frames together for transmission, increasing payload size to reduce the significance of the fixed overhead caused by inter-frame spacing and preamble. There are two aggregation options:
    - **MAC Service Data Unit Aggregation (A-MSDU)** groups logical link control packets (MSDUs) with the same 802.11e Quality of Service, independent of source or destination. The resulting MAC frame contains one MAC header, followed by up to 7935 MSDU bytes.
    - **MAC Protocol Data Unit Aggregation (A-MPDU)** occurs later, after MAC headers are added to each MSDU. Complete MAC frames (MPDUs) are then grouped into PHY payloads up to 65535 bytes.

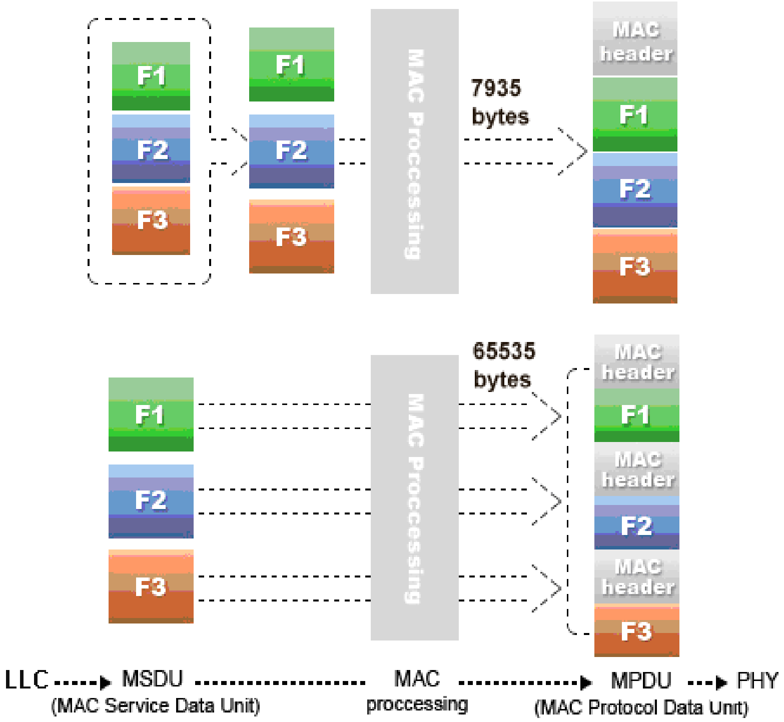

Figure 4. Using Frame Aggregation to cut 802.11 MAC Overhead

These protocol extensions increase throughput by taking better advantage of higher PHY data rates, but can only be used when communicating with other 802.11n devices. Legacy ACKs can be used to confirm Aggregated MSDUs, but Block ACKs must be used to confirm Aggregated MPDUs.

802.11n interoperability and coexistence

Given the fact that millions of legacy 802.11a/b/g devices have been deployed to date, and that those devices operate in the same frequency bands used by 802.11n, enabling coexistence is critical.

Over time, older devices will be retired. But consumers and businesses will not stop using legacy devices overnight. In fact, many businesses still use embedded 802.11b devices, even though 802.11a/g products have been available for years. 802.11n deployments must therefore be able to "play nicely" with 802.11a/b/g, both by limiting 802.11n impact on nearby legacy WLANs and by enabling communication with legacy stations. These goals are accomplished using HT Protection and Coexistence mechanisms.

High Throughput (Greenfield) Mode

There are three 802.11n operating modes: HT, Non-HT, and HT Mixed. An 802.11n AP using High Throughput (HT) mode – also known as Greenfield mode – assumes that there are no nearby legacy stations using the same frequency band. If legacy stations do exist, they cannot communicate with the 802.11n AP. HT mode is optional.

Non-HT (Legacy) Mode

An 802.11n AP using Non-HT mode sends all frames in the old 802.11a/g format so that legacy stations can understand them. That AP must use 20 MHz channels and none of the new HT features described in this paper. All products must support this mode to ensure backward compatibility, but an 802.11n AP using Non-HT delivers no better performance than 802.11a/g.

HT Mixed Mode

The mandatory HT Mixed mode will be the most common 802.11n AP operating mode for the next year or so. In this mode, HT enhancements can be used simultaneously with HT Protection mechanisms that permit communication with legacy stations. HT Mixed mode provides backwards compatibility, but 802.11n devices pay significant throughput penalties as compared to Greenfield mode.

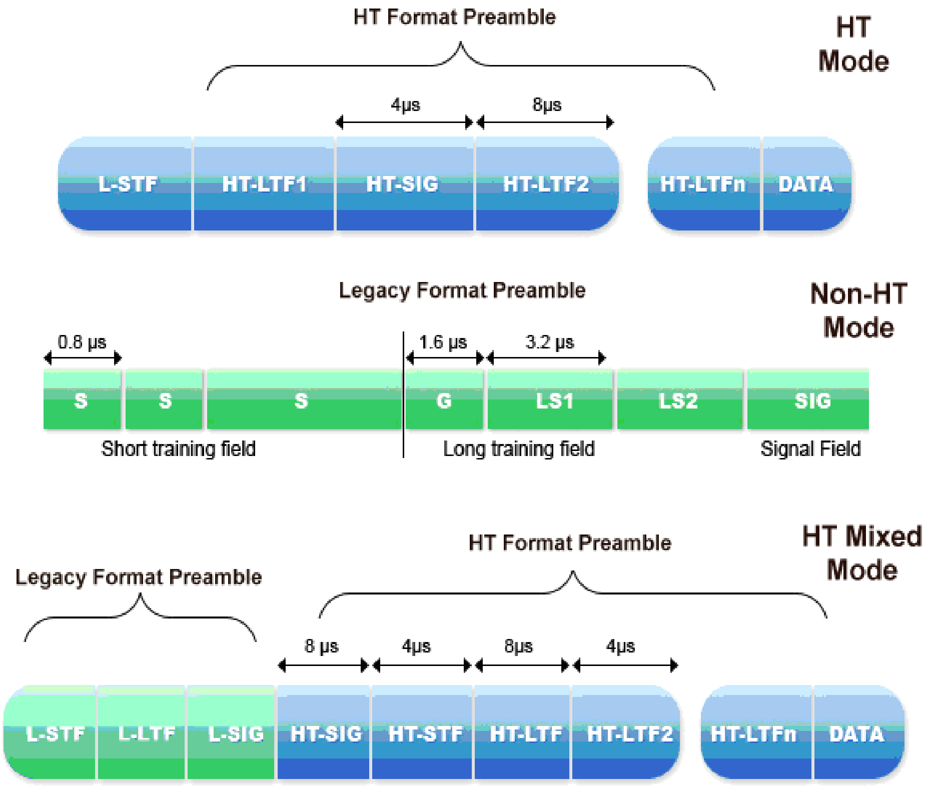

Figure 5. 802.11n Preambles

At the PHY layer, HT Protection requires 802.11n devices to transmit a legacy format preamble, followed by an HT format preamble. A preamble is a bit sequence that receivers watch for to lock onto the rest of the transmission. The legacy preamble makes it possible for 802.11a/g stations to avoid transmitting over the HT frames sent to and from 802.11n stations. That double preamble adds overhead, reducing throughput, but 802.11n stations can still take advantage of HT features.

At the MAC layer, HT Protection requires 802.11n devices to announce their intent to transmit by sending legacy format CTS-to-self or RTS/CTS (Request to Send/Clear to Send) frames. These frames let nearby 802.11a/g devices – including those not connected to your AP – sense when the channel is in use to avoid collisions. Even though RTS/CTS frames are short, it takes more time to transmit them at the legacy rate of 6 Mbps than it does to transmit 500 bytes of data at 600 Mbps. HT Protection significantly reduces an 802.11n WLAN's overall throughput.

20/40 MHz Channels and Coexistence

APs and stations must exchange information about the channels they will use to communicate. In 802.11n, this is done by sending HT Information and Capabilities Elements to indicate channel width (20 or 40 MHz), primary channel number, and 40 MHz secondary channel offset. To promote peaceful coexistence, an 802.11n AP can automatically move to another channel or switch to 20 MHz operation if another AP starts operating in either half of the designated 40 MHz channel.

Phased Coexistence Operation (PCO) is an option in which an 802.11n AP alternates between using 20 MHz and 40 MHz channels. Before it uses a 40 MHz channel, the AP reserves both adjacent 20 MHz channels. This makes an 802.11n AP more tolerant of a nearby legacy AP operating on overlapping channels. But once again, this option reduces throughput.

Migration Strategies

These 802.11n mechanisms are intended to enable interoperability and reduce interference with legacy APs and stations. It is better to avoid these problems altogether. WLAN planners should carefully consider how they will use the 2.4 and 5 GHz bands.

For example, some may use the uncrowded 5 GHz band for high-speed 802.11n AP-to-AP backhaul over 40 MHz channels. These 802.11n APs can even use HT mode if no legacy 802.11a devices were ever deployed. Many will find it necessary to use the busy 2.4 GHz band for AP-station communication, given the many 802.11b/g chipsets embedded in notebooks and handsets. One strategy is to deploy 802.11n in HT Mixed mode using 20 MHz channels in the 2.4 GHz band just to support those legacy stations. New 802.11n stations could be given the option of connecting to 802.11n APs in the 5 GHz band, using performance improvement to encourage equipment upgrade. Dual-radio 802.11n APs could even be deployed to support 2.4 and 5 GHz stations simultaneously.

These are just a few possible strategies for transitioning a WLAN to 802.11n. Applications, QoS, and user density must also be considered.

802.11n deployment challenges

WLAN administrators will find 802.11n familiar in many ways. Association flows and link security measures remain the same, as do many provisioning, management, and monitoring processes. However, the new 802.11n data rates, PHY techniques, MAC formats will impact network infrastructure, WLAN tools, and how they should be used.

Infrastructure Upgrades

The higher data rates and throughput delivered by 802.11n APs increase the demands placed on upstream wireless and wired network infrastructure. If you upgraded half of your 802.11g APs to 802.11n, your WLAN Controller could be required to handle up to 5 times as many packets. If half that traffic heads to your wired network, backhaul Ethernet switches could experience two to three fold growth. As legacy stations are retired, 802.11n throughput will further increase. Clearly, network infrastructure upgrades will (eventually) be needed to handle this load, and so capacity planning must be part of any 802.11n deployment.

Those new 802.11n APs also require more power than legacy APs. Draft 2.0 802.11n APs require up to twice the 12.95W that can be delivered via 802.3af Power over Ethernet (PoE). Future 802.11n chipsets will be more power-efficient and the emerging 802.3at PoE standard will be able to deliver 30W. Until then, workarounds must be considered (e.g., AC, dual PoE terminations, mid-span injectors). If you use PoE to power legacy APs, you should plan to upgrade your PoE switches or injectors to support 802.11n.

RF Planning & Site Surveying

RF planning will play a pivotal role in 802.11n deployment. 802.11a/g AP coverage was relatively easy to predict based on signal strength. Because 802.11n PHY techniques exploit RF phenomena like multipath to great benefit, ad hoc "rule of thumb" AP placement based on signal strength alone is no longer sufficient. RF modeling and survey tools must be upgraded to help analyze the many possible 802.11n modulation type, coding rate, guard interval, channel width, and spatial stream permutations.

As always, best practices dictate the use of active site surveys (where survey applications associate to deployed enterprise APs to verify and refine planning predictions). These active surveys let you make final deployment decisions based on real-world 802.11n PHY speed (the rate at which data is transferred over the wireless communications medium), packet loss and packet retry measurements. Active surveys also take into account the real-world impact of beam-forming (if implemented) and multi-path encountered at each individual location.

Updated RF planning tools are needed, not only to recommend optimal 802.11n AP placement and configuration, but to assist with legacy AP/station coexistence planning and channel assignment. Although WLAN infrastructure may assume responsibility for making as-needed channel and transmit power adjustments, you must make those critical decisions regarding frequency band use and 802.11n AP operating mode.

WLAN Security

802.11n employs the very same 802.11i (WPA2) security measures used by legacy 802.11a/g devices. VPNs can still be used to protect 802.11n frames, although VPN gateways will need to deliver higher encrypted throughput.

New Wireless IPS alerts and reports are needed, even in legacy WLANs, to spot and react to 802.11n rogue APs. Note that legacy WIPS sensors can detect the presence of 802.11n devices operating in Non-HT or HT Mixed mode, but not in HT (Greenfield) mode. When rolling out 802.11n, plan to deploy new 802.11n-capable sensors and leverage the integrated RF monitoring capabilities found in some new 802.11n APs.

The latter can be particularly helpful for accurate locationing, given that 802.11n increases in range make it possible for intruders and accidental associations to occur at greater distances. Over time, it is also likely that new attacks will be developed to exploit 802.11n PHY and MAC extensions, requiring further WIPS signature and alert upgrades.

Troubleshooting and Tuning

802.11n signal processing techniques let APs adapt themselves to changing RF conditions. However, visibility into 802.11n WLAN operation and performance is still critical. Given the number of possible configurations, this is quite possibly even more important than ever before. Wireless traffic monitoring and diagnostic tools must be updated to recognize new 802.11n devices, 40 MHz channels, HT frame formats, and protocol fields.

- WLAN analyzers must be able to capture and decode 802.11n traffic. They should also be able to determine the various 802.11n features configured on each observed AP and station.
- Spectrum analyzers must recognize the spectral usage patterns associated with 802.11n APs – including Greenfield mode.
- Connection diagnostic tools will require the ability to connect to 802.11n APs using any supported MCS value.
- WLAN analyzers must help 802.11n users overcome their potentially inability to achieve high throughput, due to presence of legacy devices, implementation of protection mechanisms, etc.
- WLAN analyzers must help administrators understand the real-world overhead incurred when supporting legacy devices.
- WIPS alerts and reports must be extended to analyze 802.11n PHY and MAC extensions and their impact on WLAN operation and performance.
- Integration between WIPS and WLAN management systems can help administrators better understand the long-term impact of real-time dynamic channel adjustments caused by 802.11n APs and controllers.

Conclusion

Enterprises have much to gain by upgrading to 802.11n. 802.11n can leverage advanced signal processing techniques like spatial multiplexing transmit beamforming and MAC efficiency improvements to significantly boost your WLAN's range, throughput, and reliability. However, the sheer number of possible 802.11n configurations and the myriad of ways in which 802.11n can impact legacy 802.11a/g requires deployment planning to maximize the benefits while minimizing disruption and cost. 802.11n draft 2.0 products are already here; ratified standard products will ship very soon. There's no time like the present to start getting your network ready for this next generation of more robust and reliable WLAN products.

About AirMagnet

AirMagnet Inc. is the leader in security, performance and compliance solutions for wireless LANs. The company's innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet WiFi Analyzer – which is known as the "de facto tool for wireless LAN troubleshooting and analysis." Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over Wi-Fi analysis solution. AirMagnet has more than 7,500 customers worldwide, including 75 of the Fortune 100.

AirMagnet WiFi Analyzer, known as the de facto standard for WLAN troubleshooting and analysis, also is the industry's first mobile monitoring tool specifically designed for wireless "N" networks. WiFi Analyzer helps IT staff make sense of end-user complaints to quickly resolve performance problems, while automatically detecting security threats and other network vulnerabilities. Although compact, WiFi Analyzer has many of the feature-rich qualities of a dedicated, policy-driven wireless LAN monitoring system.

Corporate Headquarters
830 E. Arques Ave.
Sunnyvale, CA 94085
United States
Tel: +1 408.400.1200
Fax: +1 408.744.1250
www.airmagnet.com

EMEA Headquarters
St Mary's Court The Broadway
Amersham
Buckinghamshire, HP7 0UT
United Kingdom
Tel: +44 1494 582 023
Fax: +44 870 139 5156