Guide to Deploying 802.11n Wireless LANs

Table of Contents

Overview 2

802.11n Basics

Layer 1 Enhancements 3
- MIMO 3
- Radio Chains 3
- Spatial Multiplexing 4
- Guard Interval 5
- 20 MHz and 40 MHz OFDM Channels 5
- Antenna Diversity 7
- Transmit Beamforming 7

Layer 2 Enhancements 8
- Frame Aggregation 8
- Block ACKs 9

Speeds and Throughputs 10
- Modulation Coding Schemes

Compliance, Design & Integration 11
- Power over Ethernet (PoE) 12
- Existing Infrastructure 14
- 2.4 GHz versus 5 GHz 15
- 20/40 MHz Mode 16
- Backward Compatibility 16
- Clients 17
- VoWiFi 17
- Security 18
- Site Survey 20

Migration & Deployment Strategies 22

Conclusion 25

About the Author 25

Overview

The Institute of Electrical and Electronics Engineers (IEEE) first defined wireless local area networking technology in 1997 in the original 802.11 standard. Wireless LAN (WLAN) networking products supported data rates of 1 and 2 Mbps using the RF technologies of either *Direct Sequencing Spread Spectrum (DSSS)* or *Frequency Hopping Spread Spectrum (FHSS)*. Since 1997, WLAN data rates have gradually increased as the 802.11 standard has been amended to support new technologies. *Orthogonal Frequency Division Multiplexing (ODFM)* technology brought data rates of 6 - 54 Mbps to 5 GHz frequency bands with the ratification of the 802.11a amendment in 1999. In the same year, the 802.11b amendment defined *High-Rate Direct Sequencing Spread Spectrum (HR-DSSS)* mechanisms that brought higher data rates of 5.5 and 11 Mbps to the more commonly used 2.4 GHz frequency band. The IEEE ratified the 802.11g amendment in 2003 which also brought OFDM technology and the data rates of 6 - 54 Mbps to the 2.4 GHz frequency band. Consumers and businesses have long anticipated the ratification of the 802.11n draft amendment which defines the use of *High Throughput (HT)* radios which have the potential to support data rates as high as 600 Mbps. 802.11n technology uses both PHY and MAC layer enhancements to achieve these high data rates.

The 802.11n draft amendment is scheduled to be ratified sometime in 2009. Very often, new 802.11 technologies do not find their way into the enterprise until a year or more after ratification of an 802.11 amendment. However, 802.11n technology is already being deployed in the enterprise prior to ratification of the 802.11n amendment. Most of the major Wi-Fi vendors debuted enterprise 802.11n solutions in 2008 and have already begun to direct their customers to High Throughput (HT) technology. The advent of this new technology also brings new challenges when designing and deploying an 802.11n WLAN. In the past, WLANs were designed to compensate for the negative effects of the RF phenomena of multipath. When designing an 802.11n WLAN, multipath now provides an advantageous effect. 802.11n also presents unique challenges when integrating the technology into a pre-existing wired network infrastructure. Using standard Power over Ethernet (PoE) to remotely power access points may no longer be possible. The increased bandwidth from multiple 802.11n access points might also create backhaul “bottlenecks” anywhere from the access layer to the core layer of the wired network infrastructure. Another design and integration challenge is how the 802.11n radios will affect current 802.11a/b/g transmissions and vice versa. New security considerations may also have to be addressed with *Wireless Intrusion Detection Systems* (WIDS) when monitoring an 802.11n WLAN. This paper will discuss the basics of 802.11n technology as well as all of the unique design and integration challenges. This paper will also outline nine recommendations for deploying and migrating to 802.11n WLANs.

802.11n Basics

Layer 1 Enhancements

802.11n technology uses many PHY layer enhancements to achieve higher data rates and increased data throughput. Some of the physical layer enhancements include:

MIMO - The core components of an 802.11n radio resides in the PHY layer with the use of a technology called *Multiple-Input Multiple-Output (MIMO)*. MIMO transmitters and receivers use multiple radios and antennas, called radio chains. MIMO employs a technology called spatial multiplexing to transmit multiple unique streams of data on the same frequency which increases throughput. MIMO systems can also use multiple antennas to provide for better antenna diversity, which can increase range.

Radio chains - Any single radio along with all of its supporting architecture such as mixers, amplifiers, and analog/digital converters can be defined as *a radio chain*. MIMO systems use multiple radio chains, with each radio chain having its own antenna. Each MIMO system is defined by the number of transmitters and receivers used by the multiple radio chains. The 802.11n draft amendment allows for MIMO 4×4 systems using up to four radio chains. In a MIMO system, the first number always references the transmitters (TX), and the second number references the receivers (RX). For example, a 3×4 MIMO system would consist of four radio chains with three transmitters and four receivers. A 4×4 MIMO system would use four radio chains with four transmitters and four receivers. Each radio chain requires power. A 4×4 MIMO system would require much more of a power draw than a 2×2 MIMO system. Currently, most enterprise WLAN vendors are using 2×3 MIMO radio systems. A dual-frequency access point requires two separate 2x3 MIMO systems for both the 2.4 GHz and 5 GHz frequency bands.

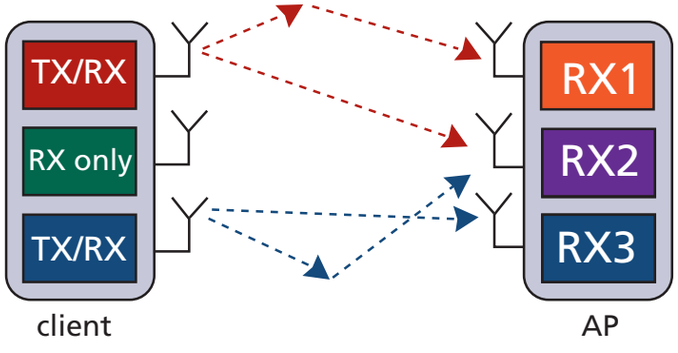


Figure A: 2x3 MIMO radio

MIMO radio spatial multiplexing - In any RF environment, the propagation behaviors of reflection, scattering, diffraction, and refraction will occur. Propagation behaviors such as reflection can cause multiple paths of the same signal. *Multipath* is a propagation phenomenon that results in two or more paths of the same signal arriving at a receiving antenna within nanoseconds of each other. In a traditional WLAN environment the time differential between the multiple paths of the same signal results in data corruption. The data corruption caused by multipath creates the need for layer 2 retransmissions which has an adverse affect on both throughput and latency.

MIMO radios actually transmit multiple radio signals at the same time to take advantage of multipath. Each individual radio signal is transmitted by a unique radio chain and antenna of the MIMO system. As depicted in Figure B, the independent signal is known as a *spatial stream*, and each unique stream will contain different data than the other streams transmitted by one or more of the other radios chains. All the independent data streams travel a different path, because there is at least a half-wavelength of space between the multiple transmitting antennas which is called spatial diversity. Sending multiple unique streams of data using spatial diversity is known as *Spatial Multiplexing (SM)*. Legacy 802.11 a/b/g radios are capable of sending only one stream of data. When a 802.11n 2×3 client station sends two unique data streams to an 802.11n access point that receives both streams, the throughput is effectively doubled. When a 802.11n 3×3 client station sends three unique data streams to an 802.11n access point that receives all three streams, the throughput is tripled.

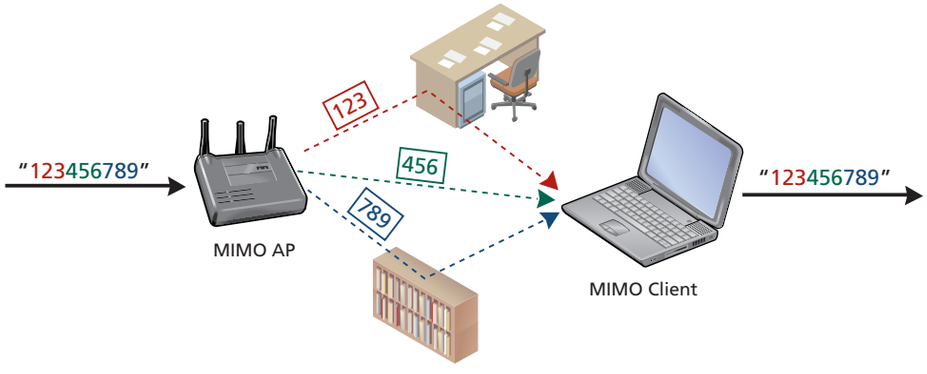


Figure B: Spatial multiplexing

Guard Interval - Data is modulated onto the carrier signal in sequences of bits called symbols. In multipath conditions, symbols travel distinct paths, and therefore some symbols arrive later. Because of the different paths, a symbol of data may arrive at a receiver before an earlier symbol has been completely received. This multipath behavior is called *InterSymbol Interference (ISI)* which culminates in the data corruption described earlier. The time differential between multiple paths of the same signal is known as the *delay spread*. Intersymbol interference is the result of symbol corruption due to a low delay spread tolerance. Normal delay spread is 50–100 nanoseconds, and a maximum delay spread is about 200 nanoseconds.

802.11 radios utilize a buffer for the delay spread called the *guard interval (GI)*. The guard interval is a period of time between symbols that accommodates for the late arrival of symbols over long paths. Typically, the guard interval should be two to four times the length of the delay spread. Legacy 802.11a/g radios use an 800-nanosecond guard interval between OFDM symbols. 802.11n radios have the optional capability of using a 400-nanosecond guard interval. A shorter guard interval can increase data rates by about 10 percent. When the shorter 400-nanosecond guard interval is used with an 802.11n radio, throughput will increase, however, the odds of data corruption due to intersymbol interference increases. The optional 400-nanosecond guard interval should be used in only when good RF conditions exist.

20 MHz and 40 MHz OFDM channels - As pictured in Figure C, a legacy 802.11a/g radio transmits on channel which occupies 20 MHz of frequency bandwidth. Each 20 MHz OFDM channel uses 52 sub-carriers with 48 sub-carriers that transport data. The remaining four sub-carriers are used as pilot tones for dynamic calibration between the transmitter and receiver. 802.11n HT radios have the capability to also transmit on 20 MHz channels, however, the 802.11n radios transmit on four 4 extra sub-carriers which can carry a little more data in the same frequency space. Another unique capability of 802.11n radios is the ability to transmit and receive on 40 MHz wide OFDM channels. As shown in Figure D, a 40 MHz channel doubles the frequency bandwidth available for data transmissions. Each 40 MHz channel uses 114 OFDM sub-carriers of which 108 transport data within the entire channel which significantly increases throughput The 40 MHz channel size is accomplished by using *channel bonding* which will in more detail later in this paper.

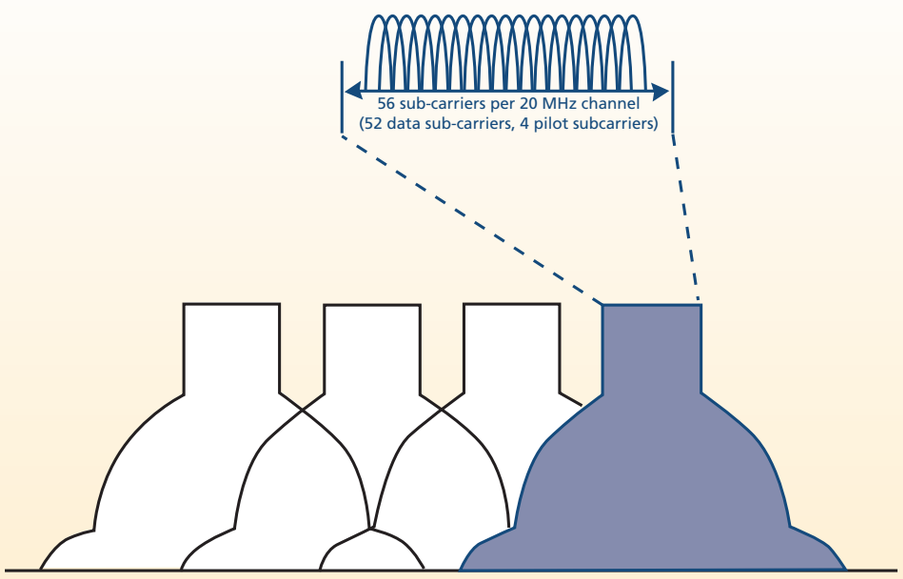


Figure C: 20 MHz OFDM channel

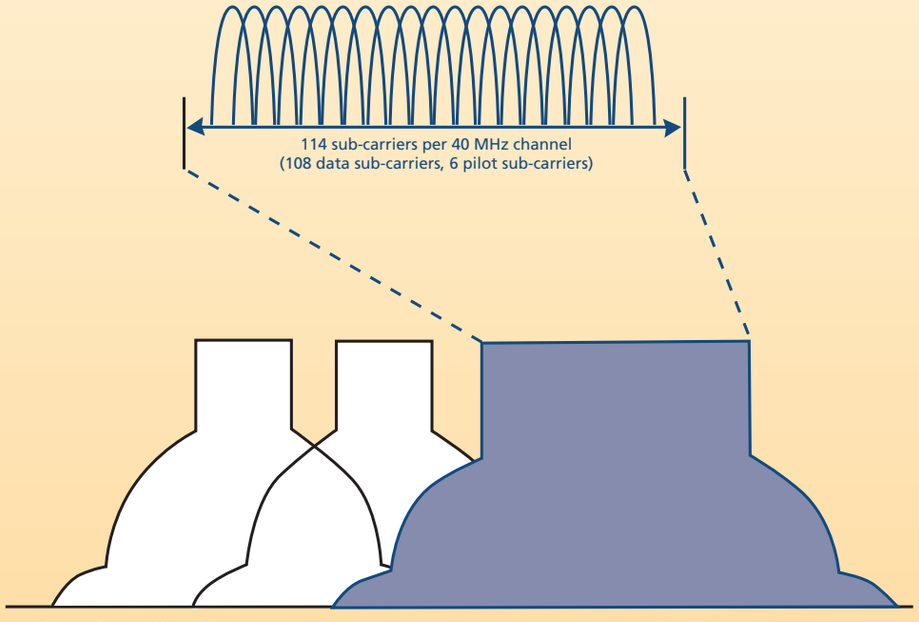


Figure D: 40 MHz OFDM channel

Antenna Diversity - To compensate against the negative effects of multipath, the majority pre-802.11n radios use *switched diversity* antenna systems. When receiving RF signals, switched diversity systems listen with multiple antennas. Multiple copies of the same signal arrive at the receiver antennas with different amplitudes. The signal with the best amplitude is chosen, and the other signals are ignored. Switched diversity is also used while transmitting, however only one antenna is used for transmission. When a mobile client moves further away from an access point, the received signal amplitude decreases and the *signal-to-noise ratio (SNR)* diminishes. A low SNR increases the odds of data corruption. Listening with two antennas increases the odds of hearing at least one uncorrupted signal. MIMO radio systems use more advanced antenna diversity systems. If three or four antennas are listening for the best received signal the odds of hearing signals with stronger amplitudes and uncorrupted data have increased. Instead of having two ears, the radios have three or four ears for listening purposes. MIMO diversity systems also can use a signal processing technique called *maximal ratio combining (MRC)*. Multiple received signals are linearly combined by using MRC algorithms in an optimal method that is additive as opposed to destructive. The MRC capabilities effectively increases the receive sensitivity of the of the receiving 802.11n radio. MIMO diversity systems that deploy three or four antennas will result in increased range for 802.11n compliant clients. MRC is also useful when a non-MIMO radio transmits to a MIMO receiver when multipath occurs.

Transmit beamforming - is an optional smart antenna technology that can be used in MIMO systems to "pinpoint" beams and provide for greater throughput and range. *Transmit beamforming (TxBF)* is a method that allows a MIMO transmitter using multiple antennas to "focus" the transmissions in a coordinated communications between the transmitter and receiver much like radar technology. When multiple copies of the same signal are sent to a receiver, the signals will usually arrive out of phase with each other. If the transmitter (TX) knows about the receiver's location, the phase of the multiple signals sent by a MIMO transmitter can be adjusted. When the multiple signals arrive at the receiver, they are in-phase, resulting in constructive multipath instead of the normal destructive multipath caused by out-of-phase signals. Carefully controlling the phase of the signals transmitted from multiple omni-directional antennas has the effect of emulating a high-gain unidirectional antenna.

As pictured in Figure E, when utilizing transmit beamforming, the transmitter will not be sending multiple unique spatial streams but will instead be sending multiple streams of the same data with the phase adjusted for each RF signal. This results in constructive multipath communication, a higher signal-to-noise ratio and greater received amplitude. Therefore, transmit beamforming will result in greater range for individual clients communicating with an access point. Higher throughput will also be a consequence of TxBF because more data bits can be encoded by more-complex modulation methods because of the higher SNR.

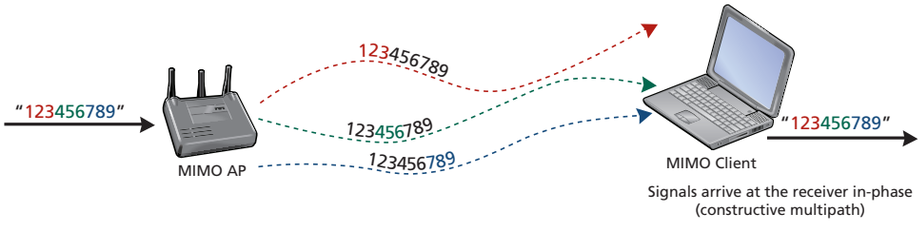


Figure E: Transmit beamforming

So far most of the implementations of transmit beamforming are proprietary and are not standardized as based on the 802.11n draft amendment. Currently, the Wi-Fi® Alliance does not yet test or certify transmit beamforming technology. Once the 802.11n amendment is ratified, more WLAN enterprise vendors may begin to deploy 802.11n radios that use chipsets capable of standardized transmit beamforming,

Layer 2 Enhancements

802.11n technology also uses many enhancements at the MAC sub-layer of the Data-Link layer to achieve higher data rates, increased data throughput and greater reliability. Some of the MAC sub-layer enhancements include:

Frame aggregation - When the Network layer (layer 3) sends data down to the Data-Link layer (layer 2), that data is handed off to the LLC sublayer and becomes known as the *MAC Service Data Unit (MSDU)*. The MSDU contains data from the LLC and layers 3–7. A simple definition of the MSDU is that it is the payload of an 802.11 data frame. The MSDU payload is essentially an IP packet and some LLC data. When the LLC sends the MSDU to the MAC sublayer, the MAC header information is added to the MSDU to identify it. The MSDU is now encapsulated in a *MAC Protocol Data Unit (MPDU)*. A simple definition of an MPDU is that it is an 802.11 frame.

The 802.11n amendment defines two methods of frame aggregation to help reduce the MAC layer overhead and medium contention overhead. Frame aggregation is a mechanism used to combine multiple frames into a single frame transmission. Multiple frame payloads (MSDUs) can be aggregated into a single frame known as an *Aggregate MAC Service Data Unit (A-MSDU)*. As pictured in Figure F, multiple 802.11 frames (MPDUs) can be aggregated into a single frame known as *Aggregate MAC Protocol Data Unit (A-MPDU)*.

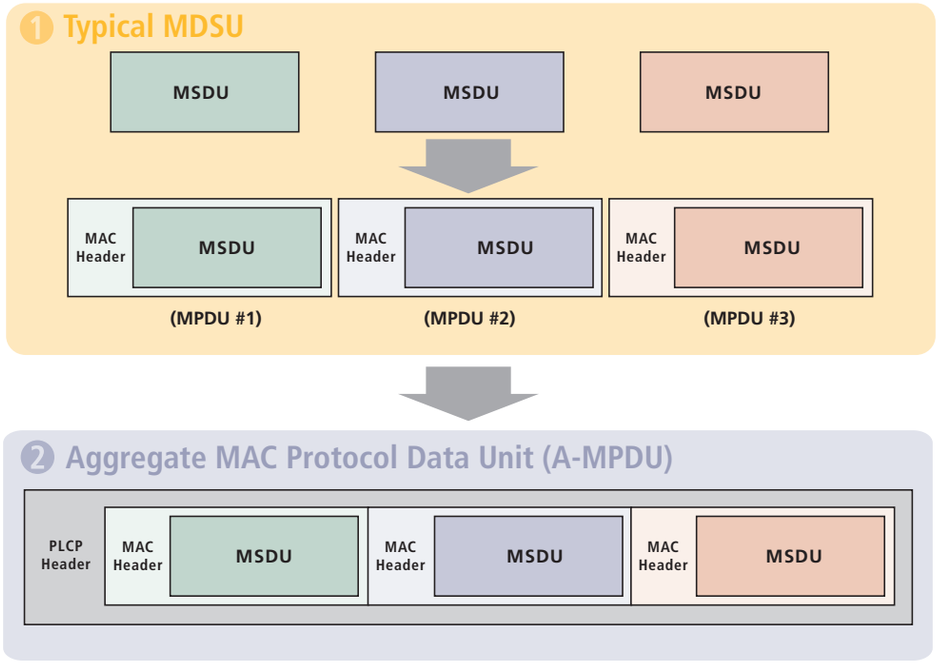


Figure F: Frame Aggregation

Both methods of frame aggregation decrease MAC overhead and medium contention overhead and therefore data throughput also increases. Aggregating small packets into a single frame as opposed to multiple frames increases the reliability of delivery of time-sensitive applications such as VoIP. It should be noted that both methods of aggregation require that the MSDUs/MPDUs be of the same quality-of-service access category. For example voice and non-voice data payloads cannot be mixed within the same aggregated frame. Currently, most enterprise WLAN vendors are using the A-MPDU method.

Block ACKs – For delivery verification purposes, the 802.11 standard requires that all 802.11 unicast frames be followed by an ACK frame. Block ACKs are used by Wi-Fi Multimedia (WMM) compliant radios as a method of acknowledging multiple individual 802.11 frames during a frame burst. Block acknowledgments are also needed to verify the delivery of the multiple MPDUs that are aggregated inside a single A-MPDU transmission. When using the A-MPDU frame aggregation method each A-MPDU contains multiple frames, and each of the individual MPDUs must be acknowledged. This is accomplished by using a *multiple traffic ID block acknowledgment (MTBA)* frame. The use of block acknowledgements decreases MAC layer overhead and thus increases throughput and reliability.

Speeds and Throughput

Modulation Coding Schemes – 802.11a/g radios use OFDM technology capable of data rates of 6 Mbps to 54 Mbps based on the modulation in use. 802.11n radios, however, define data rates based on numerous factors including modulation, the number of spatial streams, channel size, and the guard interval. A combination of these multiple factors is known as a *Modulation and Coding Scheme* (MCS). Each modulation coding scheme is a variation of these multiple factors. Seventy-seven modulation coding schemes exist for both 20 MHz HT channels and 40 MHz HT channels. As pictured in Table A, the 802.11n amendment defines eight mandatory modulation and coding schemes for 20 MHz HT channels. The eight mandatory MCSs for 20 MHz channels are comparable to basic (required) rates.

Table A: Mandatory Modulation and Coding Schemes – 20 MHz Channel

MCS Index	Modulation	Spatial Streams	Data Rates	
			800 NS Guard Interval	400 NS Guard Interval
0	BPSK	1	6.5 Mbps	7.2 Mbps
1	QPSK	1	13.0 Mbps	14.4 Mbps
2	QPSK	1	19.5 Mbps	21.7 Mbps
3	16-QAM	1	26.0 Mbps	28.9 Mbps
4	16-QAM	1	39.0 Mbps	43.3 Mbps
5	64-QAM	1	52.0 Mbps	57.8 Mbps
6	64-QAM	1	58.5 Mbps	65.0 Mbps
7	64-QAM	1	65.0 Mbps	72.2 Mbps

As pictured in Table B, data rates increase significantly as higher modulation rates are combined with more spatial streams in a 40 MHz channel while using the short guard interval. Most current 802.11n products can transmit at data rates up to 300 Mbps using two or three spatial streams in a 40 MHz channel. The use of multiple streams and 40 MHz channels is optional.

Table B: Modulation and Coding Schemes —40 MHz Channel, Three Spatial Streams

MCS Index	Modulation	Spatial Streams	DATA RATES	
			800 NS Guard Interval	400 NS Guard Interval
16	BPSK	3	40.5 Mbps	45.0 Mbps
17	QPSK	3	81.0 Mbps	90.0 Mbps
18	QPSK	3	121.5 Mbps	135.0 Mbps
19	16-QAM	3	162.0 Mbps	180.0 Mbps
20	16-QAM	3	243.0 Mbps	270.0 Mbps
21	64-QAM	3	324.0 Mbps	360.0 Mbps
22	64-QAM	3	364.5 Mbps	405.0 Mbps
23	64-QAM	3	405.0 Mbps	450.0 Mbps

It should be understood that a data rate is not the same as throughput. 802.11 technology uses a media access method called *Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)* which can add 50 percent or more overhead. For example, a modulation and coding scheme (MCS) with a data rate of 120 Mbps might only achieve actual throughput of 60 Mbps due to medium contention overhead. Other factors can also affect throughput including the protection mechanisms for legacy 802.11a/b/g devices. It should also be understood that throughput is aggregate meaning that 802.11 is a shared medium. If multiple 802.11n devices within a WLAN coverage cell are all communicating at a data rate of 120 Mbps, the total aggregate throughput of 60 Mbps is shared between all those devices.

Compliance, Design and Integration

Wi-Fi Alliance™ – The Wi-Fi Alliance maintains a vendor certification program called Wi-Fi CERTIFIED™ 802.11n draft 2.0. Because 802.11n technology is already being sold and deployed, this certification program currently tests many of the 802.11n capabilities that will eventually be seen in the final ratified 802.11n amendment. The goal of the Wi-Fi CERTIFIED™ 802.11n draft 2.0 certification is for current products to be software-upgradeable and be compliant when the final 802.11n amendment is ratified.

The Wi-Fi Alliance tests 802.11n products for both mandatory and optional baseline capabilities, as depicted in Table C. It should also be noted that all certified 802.11n products must also support both *Wi-Fi Multimedia* (WMM) quality-of-service mechanisms and WPA/WPA2 security mechanisms. Before the Wi-Fi CERTIFIED 802.11n draft 2.0 certification program existed, many WLAN vendors offered *pre-802.11n* products in the SOHO marketplace. Most of these products are not compatible with certified Wi-Fi Alliance products and are not interoperable with other vendors' products. The pre-802.11n products were never meant for deployment in the enterprise.

Table C: Baseline Requirements of the Wi-Fi CERTIFIED 802.11n draft 2.0 certification

802.11N Feature	Explanation	Mandatory/Optional
Support for two spatial streams in transmit mode	Required for an AP device.	Mandatory
Support for two spatial streams in receive mode	Required for an AP and a client device, except for handheld devices.	Mandatory
Support for A-MPDU and A-MSDU	Required for all devices.	Mandatory
Support for block ACK	Required for all devices.	Mandatory
2.4 GHz operation	Devices can be 2.4 GHz only, 5 GHz only, or dual-band. For this reason, both frequency bands are listed as optional.	Optional – tested if implemented
5 GHz operation		Optional – tested if implemented
40 MHz channels in the 5 GHz band	40 MHz operation is supported by the Wi-Fi Alliance in only the 5 GHz band. Operation of 40 MHz channels in the 2.4 GHz band is still being debated by the IEEE and may be supported by the Wi-Fi Alliance at a later time.	Optional – tested if implemented
Greenfield preamble	Greenfield preamble cannot be interpreted by legacy stations. The Greenfield preamble improves efficiency of the 802.11n networks with no legacy devices.	Optional – tested if implemented
Short guard interval (short GI), 20 and 40 MHz	Short GI is 400 nanoseconds vs. the traditional GI of 800 nanoseconds.	Optional – tested if implemented
Concurrent operation in 2.4 and 5 GHz bands	This mode is tested for APs only.	Optional – tested if implemented

PoE – Because access points are usually installed in the ceiling and other hard to reach places, the majority of APs are powered using *Power over Ethernet (PoE)*. By providing power to the APs via the same Ethernet cable that provides the data, a single low-voltage cable is all that is necessary to install a networked access point. PoE eliminates the need to run electrical cables and outlets to every AP. This greatly reduces the cost of installing access points and provides more flexibility in terms of where the APs can be mounted. The current 802.3af standard for PoE defines the capability of providing a maximum of 15.4 watts via the Ethernet cable to an access point capable of a maximum power draw of 12.95 watts.

Most enterprise 802.11n access points use 2x3 MIMO radios and are dual-frequency capable. In other words, an enterprise dual-frequency 802.11n AP has a total of six radio chains that require power. In most cases, 15.4 watts will be insufficient to power a dual-frequency 2x3 MIMO access point. When 4x4 MIMO access points become more commonplace, the power needs for the 802.11n APs will be even greater. The IEEE has a proposed draft amendment (802.3at) that enhances PoE capabilities and defines the capability of providing 30 watts or greater via Ethernet cable. 802.3at is sometimes referred to as "PoE Plus" but it has yet to be ratified. In the meantime, enterprise vendors have come up with different options to provide the needed power to 802.11n access points:

- **Proprietary PoE** – Pre-802.3 PoE solutions already exist that allow for 30 watt capability. Some 802.11n access points are equipped with 802.3at Ethernet ports that can take advantage of this technology. Keep in mind that PoE Plus technology is not yet standardized.
- **Dual 802.3af Ethernet ports** – Many vendors simply use two Ethernet ports that provide double the power using standard 802.3af ports. A downside to this solution is that dual cable runs are also needed.
- **Downgrade MIMO capability** – Some 802.11n access points with 3x3 or 4x4 multiple transmitter capability might only use a single transmitter when using standard PoE and therefore conserve power. The downside is that not all of the MIMO transmitter capabilities are being used.
- **Power outlets** – Most 802.11n access points also allow for full-power when plugged into an available power outlet. The downside is that most access points are deployed in areas where a power outlet does not exist.

It should also be noted that some of the enterprise vendors currently offer 802.11n access points with minimal circuitry that can be powered by the standard PoE capability of 15.4 watts. Careful consideration should be given when choosing an 802.11n vendor and the method they use to power the 802.11n access points. Please understand that 802.11n access points will be a huge drain on the overall power budget of power sourcing equipment (PSE). The endpoint or midspan

Detect and measure PoE voltage with EtherScope™

The EtherScope Network Assistant can detect and measure voltage on an 802.3af Power over Ethernet (PoE) enabled port, usually an access layer switch or an in-line powering sourcing device (PSE). When you enable the PoE test on the EtherScope, the EtherScope will mimic a PoE-powered device and signal the PSE to supply power. The EtherScope will measure and report the DC voltage and the polarity on each pin of the cable.

Certify 802.11n uplinks to ensure Gig Throughput using the DTX CableAnalyzer™

The only way to know if your existing cabling will support 1 Gigabit Ethernet traffic is to certify it. Certification is an exhaustive series of tests that ensure the cable, the connectors and the associated workmanship meets recognized standards. The DTX CableAnalyzer from Fluke Networks can certify a Cat 6 link in 9 seconds, ensuring that WiFi traffic will be successfully backhauled to the wired network.

power sourcing equipment might not be able to provide enough power for all the 802.11n access points as well as for other remote devices such as desktop VoIP phones and video cameras that require PoE. Careful PoE power budget planning will always be a necessity when deploying 802.11n access points.

Existing Infrastructure – Because current 802.11n access points are already capable of data rates of 300 Mbps, the bandwidth provided by the wireless medium exceeds the capacity of 10/100 Mbps Fast Ethernet. If multiple 802.11n APs are deployed, it is possible that bottlenecks might occur within the wired infrastructure. For this reason, the wired network infrastructure may eventually need to be upgraded to provide faster bandwidth connections. Access layer switches providing downlinks to many 802.11n access points will most likely need multiple Gigabit Ethernet or larger pipes for uplinks to the core layer of the network.

Most Ethernet switches deployed in the access layer are only 10/100 capable and theoretically the data flow from a single 802.11n AP with multiple radios could overwhelm a 10/100 bps Ethernet link. In reality, current data applications used over enterprise 802.11n wireless networks are not overwhelming the wired network. However as 802.11n grows in popularity, bandwidth-intensive enterprise applications, including video, will become commonplace over WiFi. Most 802.11n access points already have Gigabit Ethernet uplink ports and upgrading the wired infrastructure in anticipation of these applications is a recommended practice. Another reason to upgrade to Gigabit Ethernet at the access layer is Distributed Data Forwarding (DDF). Most WLAN architectures use thin access points that forward 802.11 frames through an IP-encapsulated tunnel to a centralized WLAN controller where the data is then forwarded to network resources. However, some WLAN architectures bypass the controller entirely and the APs handle the data forwarding at the access layer to the final destination.

Because 802.11n access points with multiple radios will make Gigabit Ethernet an eventual necessity, upgrading to better quality cabling is also a recommended practice. Although Gigabit Ethernet may be possible with Category 5e cabling, an upgrade to Cat6 cabling should be considered. As with any wired network, all the cabling should be certified and tested so that throughput and latency is not negatively affected.

2.4 GHz versus 5 GHz – As pictured in Figure G, the 40 MHz channels used by HT radios are essentially two 20 MHz OFDM channels that are bonded together. Each 40 MHz channel consists of a primary and secondary 20 MHz channel. The primary and secondary 20 MHz channels must be adjacent 20 MHz channels in the frequency in which they operate.

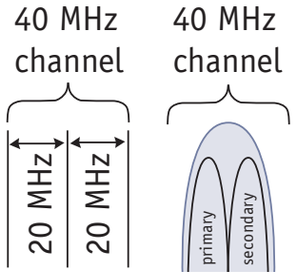


Figure G: Channel Bonding

When deploying at 2.4 GHz, most WLAN vendors use multiple channel architecture (MCA) design. As pictured in Figure H, MCA design uses a channel reuse pattern of 20 MHz channels 1, 6 and 11 which have non-overlapping frequency space. The channel reuse pattern is needed to prevent overlapping frequency interference that will cause layer 2 retransmissions that negatively affect throughput and latency. The Wi-Fi Alliance only supports 40 MHz channels in the 5 GHz bands for a good reason; 40 MHz channels cannot scale within a 2.4 GHz multiple channel architecture because there will always be frequency overlap as pictured in Figure I. The 5 GHz band has much more frequency space and using a channel reuse pattern of multiple 40 MHz channels that do not interfere with each other in the 5 GHz bands is a reality.

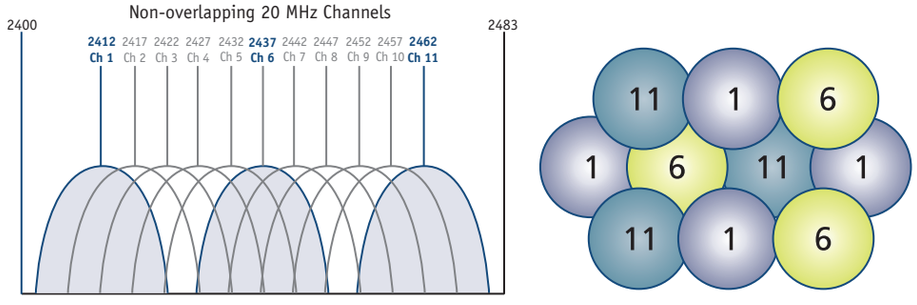


Figure H: 2.4 GHz non-overlapping 20 MHz channels

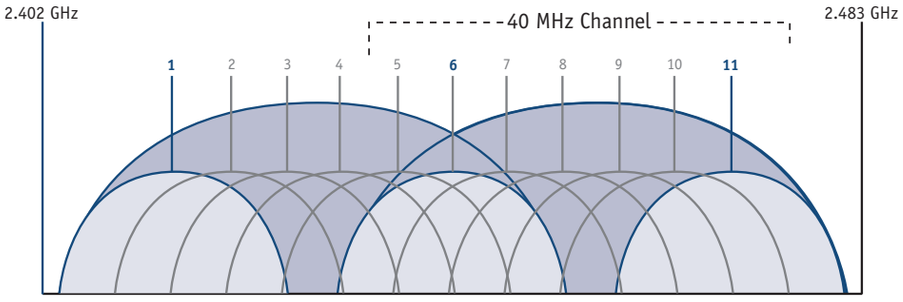


Figure I: 2.4 GHz frequency overlap of 40 MHz channels

In order to fully maximize the 40 MHz bandwidth capabilities of 802.11n, it is a highly recommended practice to deploy enterprise 802.11n at 5 GHz. If 802.11n technology is to be used at 2.4 GHz, smaller 20 MHz channels will have to be used. There are however always exceptions to the rules. Some vendors offer proprietary *single channel architecture (SCA)* solutions where deploying a single 40 MHz channel solution with multiple access points at 2.4 GHz is possible.

20/40 MHz Mode – 20 MHz 802.11a/g clients and 20 MHz 802.11n clients can still operate within the same coverage cell along with 40 MHz 802.11n client stations. The majority of 802.11n access points will operate in a 20/40 MHz mode that allows for both 20 MHz and 40 MHz channel transmissions. Access points and client stations tell each other whether they are 20 MHz or 40 MHz capable using 802.11 management frames. Typically the 20 MHz transmissions will occur on the primary channel of a bonded 40 MHz channel. Once again, in order to fully maximize the 40 MHz bandwidth capabilities of 802.11n, it is a highly recommended practice to deploy enterprise 802.11n in the 5 GHz bands.

Backward Compatibility – 802.11n radios are required to be backward compatible with 802.11a, 802.11b and 802.11g radios. However, backward compatibility will have a negative affect on the 802.11n WLAN throughput capabilities. Many people are already familiar with the protection mechanisms introduced by 802.11g amendment. 802.11g radios using OFDM technology are required to be backward compatible with 802.11b radios that use a different radio technology called *High Rate direct sequencing spread spectrum (HR-DSSS)*. The 802.11g amendment defines RTS/CTS mechanisms to allow these two technologies to co-exist within the same coverage cell. The problem is that the protection mechanisms create excessive MAC layer overhead in a 2.4 GHz 802.11g WLAN environment and has a negative affect on overall throughput. In the past, 5 GHz 802.11 WLAN's did not require a protection mechanism because only OFDM technology was used.

Because 802.11n radios are required to be backward compatible with legacy 802.11a/b/g radios, protection mechanisms are also needed. The 802.11n amendment defines four different protection mechanism modes that trigger a variety of MAC layer protection methods. The problem with 802.11n protection mechanisms is that they also create excessive MAC layer overhead. It should be noted that a legacy 802.11a client can now trigger 802.11n protection in the 5 GHz band. It should also be noted that any nearby legacy 802.11a/b/g client or legacy 802.11a/b/g AP can trigger these mechanisms.

Clients – Most companies already have numerous 802.11a/b/g client devices within their organization and 802.11n backward compatibility most likely will be a necessity. It should however be understood that there will a price to be paid in overall capacity due to the overhead caused by the 802.11n protection methods. The 802.11n standard does define a *Greenfield* 802.11n frame format that is not backward compatible with legacy 802.11a/b/g radios. A greenfield 802.11n WLAN would consist of an environment where only 802.11n access points and 802.11n clients are used within any coverage cell. Because only 802.11n radios are being used, no protection mechanisms are needed and throughput is therefore maximized.

In reality, it will be very hard for organizations to deploy "pure" 802.11n WLANS because of all the pre-existing legacy 802.11a/b/g clients. However, because many companies have so far only deployed 2.4 GHz WLANs, it might be possible to mandate an "802.11n-only" policy in the 5 GHz band and still support legacy 802.11b/g clients at 2.4 GHz. The problem is that many companies have begun to use 5 GHz 802.11a VoWiFi telephones and many laptops are now also 5 GHz capable. Protection modes will be needed at 5 GHz if any 802.11a VoWiFi phones or clients are deployed. However, one complicated strategy might be used to deploy 802.11a and 802.11n 5 GHz WLANs in the same physical space. Some of the 5 GHz channels can be designated for an 802.11a channel reuse pattern while a different channel reuse pattern is used for the 802.11n access points. For example, the upper band frequency channels of 149, 153, 157, and 161 could be used for 20 MHz, 802.11a channel reuse pattern. The 5 GHz lower and middle bands would be used for an 802.11n deployment using 40 MHz channels. Even though they operate in the same physical space, the 802.11n and 802.11a deployments will not interfere with each other because they will be transmitting in different frequency bands at 5 GHz.

VoWiFi – Does 802.11n technology improve *Voice over WiFi (VoWiFi)* communications? The main goal of 802.11n HT technology is to increase throughput via PHY and MAC layer enhancements. Throughput is not an issue with applications such as voice and whose data payloads are carried in very small IP packets. However, VoIP does depend on the timely and consistent delivery of the IP packet. Excessive layer 2 retransmissions usually result in latency and jitter problems for time-sensitive applications such as voice. Increased latency of a VoIP packet due to layer 2 retransmissions can result in echo problems. A high variance in the latency (jitter) is the more common result of 802.11 layer 2 retransmissions. Jitter will result in choppy audio communications and reduced battery life for VoWiFi phones.

Quickly identify and locate rogue devices

Fluke Networks EtherScope Network Assistant and OptiView Integrated Network Analyzers help you address wireless security vulnerabilities. Walk your site to detect and identify unauthorized rogue devices and unprotected access points, then use the locate feature to hunt them down. Periodically survey the network for changes that could indicate a security breach. These portable analyzers discover active networks, mobile clients and access points. Drill down into devices to see configuration details. Troubleshoot WLAN connectivity, authentication and performance issues.

The Wi-Fi Alliance requires that all certified 802.11n products must support Wi-Fi Multimedia (WMM) quality-of-service mechanisms. WMM defines a high priority for transmission of VoIP traffic. In addition, the PHY and MAC layer enhancements defined by 802.11n should provide for more reliable delivery of frames with a VoIP payload and decrease the need for layer 2 retransmissions.

One of the biggest challenges with VoWiFi telephones is battery life. The battery of a VoWiFi telephone needs to last at least one eight hour work shift. MIMO systems that use multiple radio chains will drain a telephone battery in a very short time. For that reason, the major VoWiFi vendors currently do not offer phones with 802.11n chip-sets. More than likely the first VoWiFi telephones using an 802.11n chipset will only be 1x1 MIMO radios. 2x3, 3x3 and 4x4 MIMO systems with multiple radio chains will be too much of a drain on battery life.

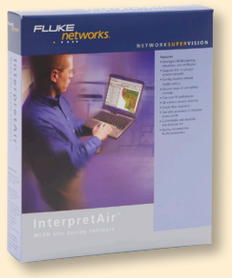
The 802.11n amendment does define enhanced power management capabilities such as *spatial multiplexing power save (SM Power Save)* which allows MIMO client stations to power down all the client's radios except for one single radio. Should VoWiFi vendors ever offer 802.11n VoWiFi phones with multiple radio chains, SM Power Save capabilities will be a necessity to conserve power and save battery life.

Security – New issues arise in regards to security when 802.11n technology is deployed. Traditional *wireless intrusion prevention systems (WIPS)* will detect 802.11n radios as long as they are communicating on a 20 MHz primary or secondary channel and using an 802.11 frame format that the legacy sensors can understand. All 802.11n radio transmissions use a physical layer header with training symbols that provide the initial synchronization with receiving 802.11 radios. 802.11n supports three frame formats:

- **Non-HT (Legacy)** – This format uses the legacy PHY header that is used by 802.11a and 802.11g radios.
- **Mixed Format** – This format uses a PHY header that can be interpreted by both legacy 802.11a/g radios and 802.11n High Throughput (HT) radios.
- **HT Greenfield** – As mentioned earlier, the Greenfield PHY header not backward compatible with legacy 802.11a/g radios and can only be interpreted by 802.11n radios

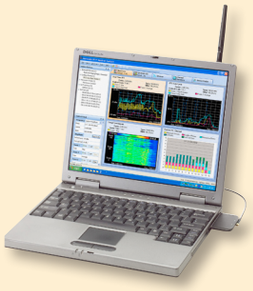
Most of the current WIPS sensors only have 802.11a/g radios. An 802.11a/g sensor will be able to detect an 802.11n transmitter using a 20 MHz channel and using either the Non-HT or Mixed frame formats. However, a legacy 802.11a/g sensor will not be able to decipher any transmissions on 40 MHz channels and will not be able to understand any transmissions using the HT Greenfield frame format. An attacker could potentially install a rogue 802.11n AP transmitting using HT Greenfield frame format and go undetected by the wireless intrusion prevention system that is using 802.11a/g sensors. The solution to this problem is to upgrade the WIPS solution with new sensors that also have 802.11n MIMO radios.

An 802.11n deployment effectively doubles the amount of channels that must be monitored for IDS purposes. The WIPS solution must listen for attacks on both the 20 MHz and 40 MHz OFDM channels. Some WLAN vendors use an integrated WIPS solution where access points perform off-channel scanning and are used as part-time WIPS sensors. Access points spending too much time listening off-channel will cause latency/jitter issues with VoWiFi solutions. Because more channels must be monitoring, the potential of unheard attacks increases. Too little time spent listening off-channel can also expose the WLAN to potential unheard attacks. If an integrated IDS solution is being used, is a highly recommend practice to convert a number of the access points into *full-time* WIPS sensors that are constantly scanning all channels



Visualize coverage and optimize performance with InterpretAir™

InterpretAir WLAN site survey software helps you to plan, deploy, verify, and expand your wireless LAN network. InterpretAir enables you to visualize multiple RF performance characteristics over a floor plan of your building, and provides for access point simulation to help you with planning to fill coverage gaps. InterpretAir automatically generates comprehensive performance documentation for historical reference and reporting. The network health feature lets you define your own baseline for WLAN performance and shows you where your WLAN meets or does not meet your network performance requirements, enabling faster analysis and decision making.



Solve RF interference problems with AnalyzeAir™

Gets instant vision into the hidden world of RF, allowing you to see the spectrum in a visible and intelligent format using Fluke Networks AnalyzeAir™ Wi-Fi Spectrum Analyzers. AnalyzeAir software lets you see, monitor, analyze, and manage all RF sources and wireless devices that influence your Wi-Fi network's performance and security – even visibility of unauthorized or transient devices.

AnalyzeAir software takes the cost and complexity out of spectrum analysis. Unlike single-function RF analyzers or expensive tools that provide RF information without device identification and location, AnalyzeAir provides an easy-to-understand, fast-start solution, allowing you to quickly resolve RF problems that prevent WLAN connectivity and impact performance.

As new technologies are deployed, new attacks always follow. Currently there is already a *denial of service (DoS)* attack that exploits the 802.11n Block Acks. There will probably be more new layer 2 DoS attacks against 802.11n deployments in the future. The answer to this problem is to make sure that the deployed WIPS can detect these new attacks and to update the WIPS signature files on a regular basis.

Site Survey – When performing an 802.11n site survey, careful consideration should be always be given to the type of clients that are deployed in the enterprise. If only 802.11n clients are being used, all of the access points should be deployed in areas to take advantage of multipath. However, high multipath environments will still have a negative affect for legacy 802.11a/b/g clients. If a legacy client population is prevalent, using unidirectional antennas to cut down on reflections and lower the multipath environment is still recommended. A lowest common denominator strategy is often needed for the site survey as long as legacy clients exist. Another example is range. If only 802.11n MIMO clients are used, the 802.11n APs can be placed further apart because of the increased range capabilities that MIMO provides. However, if many legacy clients still exist, the APs will need to be closer together.

Site survey hardware and software solutions will need to be upgraded so that it supports 802.11n technology. Predictive analysis software will have to drastically change due to the new coverage and capacity capabilities of 802.11n technology. It is always a highly recommended practice to also perform a manual site survey to determine coverage areas and analyze the environment. If 802.11n clients are to be deployed, measurements should be taken using an 802.11n client radio. If legacy clients will still be deployed, measurements should be taken using a legacy 802.11a/b/g client radio.

The major types of manual coverage analysis site surveys are generally performed when determining coverage cell boundaries. During a passive manual site survey, the client device just measures received signal strength (dBm) and the signal-to-noise ratio (SNR). During an active manual site survey, the client radio is associated to the access point. In addition to RF measurements, information such as packet loss and layer 2 retransmission percentages are measured while the client card is associated the AP. When performing an 802.11n site survey, the need for active survey is more important due to the fact that the multipath environment is different in both directions between the client and access point.

As with any manual site survey, a spectrum analysis survey must also be performed to determine if there are any potential sources of RF interference such as microwave ovens or cordless phones.

Migration and Deployment Strategies

The best case scenario for deploying 802.11n is when a pre-existing WLAN never existed and a Greenfield 802.11n WLAN deployment is planned. As mentioned earlier using 40 MHz channels in the 5 GHz bands with only 802.11n clients and no legacy client support is the best case scenario. However most enterprise have already deployed a 802.11b/g WLAN at 2.4 GHz and might already have an 802.11a WLAN operating at 5 GHz. We suggest the following nine recommendations for both 802.11n Greenfield deployments and for migrating from legacy WLANs to 802.11n technology:

1. **Verify Wi-Fi Alliance 802.11n draft 2.0 compliance** – Even though the IEEE has yet to ratify the 802.11n amendment, a high priority should be given to only deploying 802.11n access points and client cards that meet the current Wi-Fi CERTIFIED™ 802.11n draft 2.0 certification baselines. Understand that some optional 802.11n capabilities such as transmit beamforming that might get wider use in the future, may also require a different chipset and therefore require a hardware upgrade.

2. **Review WLAN vendor migration and deployment recommendations** – Although standardization is important, each WLAN vendor has unique capabilities that distinguish their solution from the competition. Reviewing the vendor deployment guide and migration documentation is highly recommended. One major exception is that some vendors actually recommend simply swapping legacy access points with new 802.11n access points as a migration strategy. That recommendation is usually unacceptable because of the radical differences in how MIMO radios operate. A new 802.11n site survey is always the preferred method. Consideration should also be given to allocating proper training for the IT staff that will be responsible for the 802.11n network. The majority of the major WLAN vendors all recommend the vendor-neutral CWNP training classes (**www.cwnp.com**). All of the major vendors also offer training classes for their specific WLAN solution.

3. **Invest in tools that speed deployment and troubleshooting** – The wireless lifecycle involves distinct and interrelated phases: pre-deployment and expansion planning, installation and verification, troubleshooting, and management and optimization. To navigate through each of these phases successfully and efficiently, a network manager needs tools that provide features and functions specific to the unique requirements of each phase of this wireless lifecycle. Fluke Networks offers a suite of 802.11 a/b/g/n wireless solutions that deliver complete network visibility to help you successfully manage your network's wireless lifecycle. Having the right tool reduces deployment time, minimizes re-work, and reduces overall deployment and implementation costs.

4. **Perform an 802.11n site survey** – Every building is different and a proper site survey should always be executed. All site survey hardware and software will need to be 802.11n capable and an active manual site survey is highly advisable. A lowest common denominator strategy is often needed for the site survey as long as there is a legacy client population.

5. **Choose a PoE solution** – Careful consideration will have to be given to how 802.11n access points with multiple radio chains will be powered. Most vendors are implementing proprietary PoE solutions until 802.3at (PoE Plus) is standardized. Keep in mind that some proprietary PoE solutions may not be compliant with the future ratified 802.3at higher power solutions.

6. **Upgrade wired infrastructure to meet data flow needs** – Ideally the wired infrastructure should be upgraded to Gigabit Ethernet when the 802.11n access points are deployed. Cabling upgrades may also be necessary. In reality, current data applications used over 802.11n wireless networks are not currently overwhelming the wired network. However upgrading to Gigabit Ethernet at the access layer will eventually be a necessity as more 802.11n APs are deployed and as more bandwidth-intensive applications are put into use. Edge switches providing downlinks to many 802.11n access points will most likely need multiple Gigabit Ethernet or larger pipes for trunked uplinks to the core layer.

7. **Upgrade clients prior to access points** – Even though backward compatibility is a requirement of 802.11n technology, upgrading as many of the laptops and other client devices should begin prior to installation of the 802.11n access points. If legacy clients are a necessity, consider a deployment strategy that still supports legacy 802.11b/g clients at 2.4 GHz, but mandates 802.11n only clients at 5 GHz. A Greenfield 802.11n WLAN can be deployed at 5 GHz without the throughput reductions that result from protection mechanisms.

Complete WLAN Visibility in one tool

Fluke Networks award-winning OptiView Integrated Network Analyzer provides the visibility you need to manage and troubleshoot both sides of the access point –for both 802.11 a/b /g/n wireless and 10/100/1000 Ethernet copper and fiber wired networks. With Wi-Fi detection, verification and troubleshooting, and the ability to run InterpretAir Site Survey and AnalyzeAir RF Spectrum Analyzer all on the same platform – no other tool offers this much vision and all-in-one capability to help you manage and analyze your wired and wireless network.

8. **Deploy new 802.11n access points** – Once the proper coverage analysis has been completed during the site survey, the 802.11n access points should be deployed. Spot checks should always be performed to validate coverage. Stick with one enterprise vendor when deploying WLAN controllers and APs. Use 40 MHz channels in the 5 GHz bands but only use 20 MHz channels in the 2.4 GHz band.

9. **Upgrade monitoring capabilities** – As soon as possible, all WIPS sensors should be replaced with sensors with 802.11n MIMO radios. Even if an 802.11n WLAN is not being deployed, consideration should be given to upgrading the WIPS sensors so as to properly detect unauthorized 802.11n clients and APs. If an integrated WIPS solution is being used, be sure to dedicate a certain number of APs as full-time sensors. Update the WIPS signature files as they become available. Wireless network monitoring servers (WNMS) that are used for performance monitoring should also be upgraded to support 802.11n capabilities. Any 802.11 frame analysis software that is used for troubleshooting will also have to have 802.11n capabilities.

Conclusion

The bottom line is that organizations should take a structured project based approach to 802.11n deployment, skipping or short cutting these steps can put the project and future performance at risk. Taking a lifecycle approach from pre-deployment planning to installation verification, troubleshooting to performance optimization, will ensure you get optimal performance out of your 802.11n WLAN.

Additional Recommended Reading

- *CWNA: Certified Wireless Network Administrator Official Study Guide:* (Exam PW0-104) by David D. Coleman and David A. Westcott - Sybex Publishing - ISBN# 0470438908
- *Wi-Fi CERTIFIED™ 802.11n draft 2.0: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks* – **www.wi-fi.org**
- *The Promise and Pitfalls of 802.11n* – **www.flukenetworks.com/11n**

About the Author

David Coleman is a wireless security/networking trainer and consultant. His company, AirSpy Networks (www.airspy.com), specializes in corporate training and has worked in the past with Avaya®, Nortel®, Polycom®, and Siemens®. He has trained numerous computer security employees from various law enforcement agencies, the U.S. Marines, the U.S. Army, the U.S. Navy, the U.S. Air Force, and other federal and state government agencies. David is the co-author of Sybex Publishing's "CWNA Study Guide" - ISBN# 0470438908. David Coleman is CWNE #4 and can be reached via email at **david@airspy.com**.

FLUKE networks

NETWORKSUPERVISION

Fluke Networks
P.O. Box 777, Everett, WA USA 98206-0777

Fluke Networks operates in more than 50 countries worldwide. To find your local office contact details, go to **www.flukenetworks.com/contact**.

Printed in U.S.A. 8/2009 3520118A