NETWORK AND TELECOM STRATEGIES

802.11n: Enterprise Deployment Considerations

v1, May 16, 2008

AUTHOR:

Paul DeBeasi
(pdedeasi@burtongroup.com)

CONCLUSION:

802.11n has significant advantages over legacy wireless technologies and, with Wi-Fi certification in place since June 2007, is ready for enterprise deployment now. These advantages present the enterprise network manager with important deployment considerations. Managers that take time to evaluate these considerations, within the context of their enterprise needs and constraints, will improve their ability to achieve a successful 802.11n deployment.

BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah · 84047
P 801.566.2880
F 801.566.3611
www.burtongroup.com

Table of Contents

Synopsis

Many enterprises are considering Wi-Fi CERTIFIED™ 802.11n[1] draft 2.0 deployment because it has significant advantages over existing wireless technologies. However, these advantages present the enterprise network manager with important deployment considerations. This paper examines in detail various deployment considerations for 802.11n in the enterprise environment, including operational modes, frequency band selection, power management, the AP wired Ethernet port, use of WLAN controllers, and network management. Considerations on the use of 802.11n as an Ethernet replacement are addressed, and the role of Wi-Fi CERTIFIED as an important purchase criterion is outlined.

Most existing 802.11 devices operate in a single frequency band, (e.g., 2.4 GHz or 5 GHz). 802.11n is different because it is specifically designed to operate in both the 5 GHz and the 2.4 GHz frequency bands. So 802.11n presents an opportunity for enterprises to reconsider which frequency band(s) to use.

Legacy 802.11 access points (APs) have a maximum power draw that is very close to the IEEE 802.3af Power over Ethernet (PoE) maximum of 15.4 watts. However, most 802.11n APs will consume more power than legacy APs. Enterprise AP vendors have addressed this problem in several ways and enterprise IT managers must consider which approach they will select.

802.11b/g/a APs typically use Fast Ethernet ports to forward traffic onto the wired network. Because the 802.11n data rate is designed to exceed the 100 Mbps capacity of Fast Ethernet (especially when using 40 MHz channels), most new APs will use Gigabit Ethernet for wired Ethernet communication. Therefore, some enterprises may choose to upgrade a portion of their wiring closet switches, and possibly their cabling, to provide gigabit Ethernet links to their 802.11n APs.

WLAN controllers that perform the data-forwarding function must backhaul all wireless traffic from hundreds of 802.11n APs, and so each controller will likely need to support several Gigabit Ethernet connections. WLAN controllers that distribute the data-forwarding function to the AP will need only a single Gigabit Ethernet connection.

802.11n presents a new security challenge because existing hardware sensors, without software updates, may not be able to recognize 802.11n APs. Therefore, it is important for enterprise managers to update wireless intrusion detection systems (IDSs), regardless of whether or not they plan to deploy 802.11n.

802.11n will impact network management tools. For example, spectrum analyzers must be able to recognize MIMO spatial streams, and visually communicate network behavior to the user. Therefore, enterprise managers will need to upgrade their network management tools in order to manage 802.11n networks.

[1] Throughout this paper the term "802.11n" explicitly refers to the "IEEE 802.11n draft 2.0 amendment to the 802.11 standard", unless explicitly stated otherwise. 802.11n devices that are currently Wi-Fi CERTIFIED are based upon this draft.

Introduction to 802.11n

802.11n is an emerging amendment of the 802.11 standard that significantly improves throughput and range compared with the existing 802.11 standard. Currently available products are based upon a stable draft version of the amendment (802.11n draft 2.0). The completed version of 802.11n is likely to be ratified in 2009. The Wi-Fi Alliance began certifying products based upon 802.11n draft 2.0 in June 2007, and this has helped align the industry around a set of core features that deliver inter-vendor product interoperability.

802.11n improves the performance of existing wireless applications that currently operate using 802.11a/b/g, and it enables more applications to use a wireless LAN that currently require wired Ethernet. Point of sale transactions, voice over wireless LAN, and Internet browsing will all benefit from the increased performance, coverage, and robustness of 802.11. In addition, 802.11n enables applications such as wireless backup, videoconferencing, and medical imaging to operate over a wireless LAN.

Key Advantages

802.11n includes many new features that improve throughput, robustness, and range. These include:

- **Frame Aggregation**: The 802.11 standard defines a half-duplex, shared, media access control (MAC) layer. 802.11n boosts MAC layer performance by allowing 802.11n devices to aggregate several packets into a single packet using the two different techniques. The benefit of aggregation is that it avoids the wasted overhead between frames.

- **MIMO**: Multiple input, multiple output (MIMO) is a technology that uses multiple antennas at the transmitter and the receiver. MIMO exploits the fact that radio frequency (RF) signals often reflect off of objects in their path, causing a phenomenon called multipath. MIMO uses a technique called spatial multiplexing that transmits separate data streams at the same frequency but over different spatial channels. In effect, MIMO turns multipath from a signal impairment phenomenon into a signal enhancement technique by making a channel more spectrally efficient by increasing the (baud rate)/(hertz) ratio.

- **Channel bonding:** 802.11a and 802.11g use a single 20 MHz channel, but 802.11n can bond together two channels to form a 40 MHz channel. Channel bonding doubles the channel bandwidth and significantly boosts the maximum throughput.

Throughput and Range

Wireless performance is often characterized using a throughput-versus-range curve. Throughput is usually plotted on the y-axis, and range on the x-axis. As a client moves further away from the AP, the effective throughput typically decreases. As described in the key advantages section, many of the new 802.11n features will improve throughput and range. Equipment manufacturers anticipate that

802.11n throughput will be approximately five times faster than 802.11g at an equivalent distance. Manufactures also anticipate that 802.11n will have approximately 50% better range than 802.11g.

It is very important to note that real-world performance is highly dependent upon many factors, including environmental interference, system design, radio configuration, network design, and building construction. Therefore the performance of an 802.11n network can vary from enterprise to enterprise, building to building, and even floor to floor. Some of the 802.11n-spectifc, performance-limiting factors include:

- **Legacy station support**: Network managers can configure 802.11n access points (APs) to interoperate with legacy 802.11b/g/a devices. However, support for legacy devices may reduce 802.11n performance gains because legacy devices will transmit at a significantly slower rate than that of an 802.11n device. Consequently, legacy devices tend to consume more "air time" and the faster 802.11n stations must wait for the slower legacy stations to complete transmission before they can use the WLAN (see Operational Modes).

- **No multipath reflections**: 802.11n uses MIMO technology and spatial multiplexing to boost aggregate throughput. Environments that cause a lot of multipath reflections make it easier for an 802.11n device to take advantage of spatial multiplexing, whereas environments with little or no multipath reflections reduce 802.11n performance.

- **No channel bonding usage**: As described in the key advantages section, 802.11n devices can bond two 20 MHz wide channels together to form a single 40 MHz wide channel. Channel bonding can significantly boost the performance of an 802.11n transmission compared to a single 20 MHz wide channel. Enterprises will find it easier to take advantage of channel bonding in the 5 GHz band, because the 5 GHz band has significantly more non-overlapping channels than the 2.4 GHz band (See Table 1). In addition, the 5 GHz band tends to be less heavily utilized than the 2.4 GHz band, and thus will likely experience less performance-draining interference. Currently the Wi-Fi Alliance certifies channel bonding in the 5 GHz band only.

Technology Comparison

Table 1 summarizes technical data for each major radio technology standard.

	802.11b	802.11g	802.11a	802.11n draft 2.0
Maximum signaling rate	11 Mbps	54 Mbps	54 Mbps	300 Mbps[1]
Operating frequency band	2.4 GHz	2.4 GHz	5 GHz	2.4 & 5 GHz
Typical range	300 ft/100 m	300 ft/100 m	300 ft/100 m	450 ft/150 m[2]
Non-overlapping channels (varies by country)	3	3	23	3 (2.4 GHz) 23 (5 GHz)
Interference sources	Bluetooth, microwave ovens, baby monitors etc.	Bluetooth, microwave ovens, baby monitors etc.	Cordless phones	Same as 802.11b/g @2.4 GHz Same as 802.11a @5 GHz
Standard approved	Yes	Yes	Yes	2009 expected
Wi-Fi CERTIFIED	Yes	Yes	Yes	Yes (draft 2.0)

[1]Assumes 40 MHz channel and 2x2 MIMO
[2]Assumes 50% range improvement over 802.11g/a

Table 1: *WLAN Radio Technologies*

Deployment Considerations

Many enterprises are now considering 802.11n deployment. 802.11n has many advantages over legacy wireless technologies. However these advantages provide the enterprise network manager with more deployment choices. This section describes the major deployment choices enterprises that must consider and makes specific recommendations.

Certification and Interoperability

The goal of the Wi-Fi Alliance is to help ensure multivendor interoperability by verifying that systems from different manufacturers can be used within the same wireless infrastructure. The effectiveness and wide industry adoption of its certification program has enabled network administrators to deploy WLAN products in their organizations without being locked into a single-vendor solution. Enterprises must ensure that they purchase only Wi-Fi CERTIFIED products.

The Wi-Fi Alliance is currently certifying products based upon draft 2.0 of the 802.11n amendment. Some enterprises may be hesitant to deploy draft standard products because they perceive such action represents an unacceptable risk. However there are three important factors that greatly diminish this

risk. First, draft 2.0 includes virtually all of the major features expected in the final standard. Secondly, draft 2.0 features are very unlikely to change in a way that threatens interoperability. Lastly, all of the major enterprise vendors are committed to maintaining interoperability between draft 2.0 and the final standard. Therefore, the risk associated with deployment of draft 2.0 products is very low. A current list of Wi-Fi CERTIFIED products is available at www.wi-fi.org.

Operational Modes

Most enterprise equipment vendors will allow their 802.11n APs to operate in several different operational modes. Although the implementation details vary from vendor to vendor, the operational modes are broadly defined below. Recommendations in the next section (Frequency Band Selection) will refer to these operational modes.

Mixed Mode: This mode enables 802.11n devices to co-exist and interoperate with legacy 802.11b/g/a devices on the same wireless LAN. Most enterprise WLAN equipment will use mixed mode by default, to ensure legacy compatibility. This is because most enterprises will concurrently use legacy and 802.11n devices far into the foreseeable future.

Legacy Mode: Many enterprise equipment vendors will allow their access points to operate as legacy access points. In this mode, the AP behaves like an 802.11g/a AP with improved performance, due to the fact that it utilizes some of the 802.11n physical layer enhancements. This configuration could be used when an enterprise buys new 802.11n APs but does not yet want to enable 802.11n operation.

802.11n Mode[2]: Some enterprise equipment vendors will allow their access points to be configured such that they accept association requests from only other 802.11n devices. Some enterprises may choose this configuration in order to achieve the best possible throughput for 802.11n devices because legacy 802.11b/g/a devices tend to consume more "air time" than 802.11n devices (See Legacy station support).

Frequency Band Selection

The installed base of 802.11b clients drove many enterprises to select 802.11g to ensure interoperability with their previous investment. Therefore, many enterprises today use the 2.4 GHz band. However, 802.11n is designed to operate in both the 5 GHz and the 2.4 GHz frequency bands so enterprises that deploy 802.11n must decide which frequency band and channels to use. See Table 2 for a summary of the key frequency band considerations.

[2] This mode is sometimes imprecisely referred to as "Greenfield Mode". The term Greenfield is a very specific term in the 802.11n standard and refers to the Greenfield preamble. Most enterprises will rarely, if ever, use the Greenfield preamble. Therefore, in order to avoid confusion, this paper does not use the term Greenfield Mode.

Consideration	Explanation
Regulatory constraints	Some regional authorities regulate the 2.4 GHz and 5 GHz bands and may therefore constraint frequency band usage.
Radio frequency interference	802.11n competes with many technologies in the 2.4 GHz band (e.g., microwave ovens, portable phones) whereas the 5 GHz band is less prone to interference.
Use of non-overlapping channels	The 2.4 GHz band has only three non-overlapping channels whereas the 5 GHz band has up to 23. It is therefore easier to find an interference-free channel when using the 5 GHz band.
Use of 40 MHz channels (i.e., channel bonding)	The 5 GHz band can support up to 11, 40 MHz channels whereas the 2.4 GHz band can accommodate only 1. Therefore there is more aggregate bandwidth in the 5 GHz band. (Note: The Wi-Fi Alliance does not currently certify 40 MHz channels in the 2.4 GHz band).

Table 2: *Key Frequency Band Considerations*

Virtually all enterprise WLAN vendors offer dual-radio 802.11n APs (and some offer three or more radios per AP). The Burton Group recommendations listed below assume that APs contain 2 or more radios.

1. **Purchase dual-band devices.** Enterprises should purchase dual-band (2.4 GHz and 5 GHz) 802.11n devices in order to have the greatest deployment flexibility.

2. **Use the 5 GHz band when possible.** The 5 GHz band enables 802.11n to achieve the best possible wireless network throughput, albeit with somewhat decreased range compared to 802.11n at 2.4 GHz. The large number of non-overlapping channels in the 5 GHz band enables enterprises to take full advantage of channel bonding.

3. **Preferentially balance load across the 5 GHz band.** Enterprises that utilize both bands may want to configure their load balancing system to preferentially move stations to the 5 GHz band because this band has more non-overlapping channels and may experience less interference than the 2.4 GHz WLAN.

4. **Operate 802.11n APs in mixed mode when few 802.11n stations exist.** For many enterprises, the number of legacy stations will far exceed the number of 802.11n stations. In this situation, 802.11n APs should be configured for mixed mode operation in order to provide the greatest coverage and performance for legacy stations.

5. **Operate 802.11n APs according to Table 3 when the number of 802.11n stations exceeds legacy stations.** As the number of 802.11n stations grows and exceeds the number of legacy stations, enterprises may want to configure one of the radios in their 802.11n APs for 802.11n mode operation in order to provide the greatest performance for 802.11n stations while maintaining broad coverage for legacy devices. In this situation, refer to Table 3.

Scenario[1]	Is support for these clients required?		Configure the AP as shown below			
			Radio A		Radio B	
	802.11b/g	802.11a	Band	Mode	Band	Mode
1	No	No	5[2]	802.11n	5	802.11n
2	No	Yes	5[2]	Mixed	5	802.11n
3	Yes	No	2.4	Mixed	5	802.11n
4	Yes	Yes	2.4	Mixed	5	Mixed

[1] All scenarios assume that the wireless LAN must support 802.11n stations

[2] If 802.11n stations do not support 5 GHz then configure AP to use 2.4 GHz.

Table 3: *Frequency band and operational mode recommendations*

Power Consumption

WLAN APs require a stable power source to operate and are typically installed in ceiling areas or high up on walls, where power outlets are not generally located. To facilitate these installations, the IEEE has developed 802.3af, a standard that specifies Power over Ethernet (PoE). Wired switches that provide this capability (and APs that accept PoE) simplify the installation process throughout the enterprise.

Many 802.11n APs with all features enabled will likely exceed the power rating of 802.3af PoE equipment, and thus enterprises must consider how they will supply power to 802.11n APs. In addition, peak power consumption is highly correlated to traffic rate. The more traffic an AP transmits and receives, the more power the device consumes.

Enterprise AP vendors have addressed this problem in several ways and enterprise IT managers must consider which approach they will select. First, all vendors will support use of wall-outlet-powered APs, and thus will be able to draw all the power they need. Second, some vendors will design their 802.11n APs with multiple Ethernet connections, thus enabling the AP to be powered by two PoE connections. Third, many PoE-powered 802.11n APs will continue to operate—albeit with degraded functionality—in order to stay within the PoE power budget. An example of degraded functionality is the use of a single transmitter rather than multiple transmitters, resulting in reduced system throughput. Fourth, some vendors will provide support for PoE Plus (i.e., IEEE 802.3at) either through the use of power injectors or via circuitry inside Ethernet switches. Finally, some vendors have figured out how to engineer products that they do not exceed the PoE power limits.

Burton Group expects that this problem will be temporary and that, due to competitive dynamics, most enterprise AP vendors will be able to operate their APs using a single PoE connection without any degraded functionality by 2009.

AP Wired Ethernet Port

Legacy 802.11b/g/a APs used Fast Ethernet ports to forward traffic onto the wired network. Because the 802.11n data rate will exceed the 100 Mbps capacity of Fast Ethernet (especially when using 40 MHz channels), most new APs will provide Gigabit Ethernet as an alternative to 100 Mbps Fast Ethernet. Gigabit Ethernet provides more bandwidth than any 802.11n AP can generate over a wired Ethernet connection. Therefore, some enterprises may choose to upgrade a portion of their wiring closet switches, and possibly their cabling (if less than Cat5e), to provide Gigabit Ethernet links to their 802.11n APs.

WLAN Controllers

The term WLAN controller is used to represent any device that implements centralized management and control of multiple lightweight APs. The primary benefit of a controller is improved manageability, because the controller provides a management focal point for hundreds of individual APs. Many enterprises now recognize the value of WLAN controllers, and have migrated their networks to use controller-based architectures.

Vendor solutions that centralize the data-forwarding function in the controller must backhaul all wireless traffic to the controller, where it can make forwarding decisions, perform quality of service (QoS) queuing, and perform virtual LAN (VLAN) tagging. Vendor solutions that distribute the data-forwarding function to the AP, perform these functions in the AP and therefore do not backhaul the traffic to the controller.

WLAN controllers that perform the data-forwarding function will receive traffic from hundreds of 802.11n APs, and so each controller will likely need to support several gigabit Ethernet connections. It should be noted that some enterprises might need to purchase new switches (and possibly new cabling, e.g., Cat6A) if their networks do not support 10 GB Ethernet connections. Vendor solutions that distributed the data-forwarding function to the AP, need only a single Gigabit Ethernet connection.

Intrusion Detection

To monitor the WLAN for security violations, many enterprises have deployed wireless intrusion detection systems (WIDSs). These tools use hardware sensors to capture data from the RF link, perform analysis on that data in a central server, and provide alerts and reporting in a portal or console view. Monitoring for rogue APs and unauthorized devices, maintaining policy adherence in

the air and on the APs, and looking for anomalous or unexpected behavior on the WLAN are a few of the services a WIDS offers.

Rogue APs can attempt to join the network, lure unsuspecting users to their own network, disrupt traffic, or interfere with the RF signal. 802.11n presents a new challenge because existing hardware sensors, without software updates, may not be able to recognize rogue or permitted 802.11n APs. In addition, an 802.11n device could be used to launch a denial of service (DoS) attack on legacy 802.11 networks. Therefore, it is important for an enterprise to update its wireless IDS, regardless of whether or not it plans to deploy 802.11n.

Network Management

The 802.11 MAC layer is a shared, half-duplex connection and the three-dimensional (3D) nature of RF allows the signal to pass through walls and ceilings, rendering it susceptible to interception, interference, and unpredictable performance. Given the increasing deployment of WLANs, network managers have found a way to address these differences using a variety of network management tools (e.g., spectrum analyzers, WLAN monitors, site planning, and configuration management tools).

802.11n introduces enhancements at the physical (PHY) and media access control (MAC) layers that impact all of these tools. For example, spectrum analyzers must be able to recognize MIMO spatial streams, and visually communicate network behavior to the user. WLAN monitors need to be able to perform packet capture at much higher speeds, and must be able to decode MAC layer frame aggregation. In addition, configuration management tools need to be able to manage the many new features in 802.11n. Therefore, enterprise IT managers will need to upgrade their network management tools in order to manage 802.11n networks.

802.11n versus Wired Ethernet

It is likely that wireless and wired LANs will coexist far into the foreseeable future. However, the significant advantages that 802.11 provides over legacy wireless standards will cause some enterprise IT managers to consider deploying 802.11n instead of wired Ethernet for network access. Burton Group recommends that enterprises deploy wired Ethernet instead of a wireless LAN in the following situations:

- Enterprises that need the highest level of network reliability and predictability. Although 802.11n reliability and predictability is significantly better than 802.11g, it is not as good as wired Ethernet.

- No mobile applications are in use and future use of such applications is not anticipated. An example is a call center where users remain at their desks and do not use mobile devices.

- When even a small risk of DoS attack is unacceptable. An example is a highly sensitive government facility.

- Enterprise users need Gigabit Ethernet performance. For example, computer-aided design (CAD) users that frequently move large files need high-performance connections.

In all other situations, Burton Group recommends that enterprises deploy a wireless LAN. Employees want the convenience of being un-tethered, as exhibited by the fact that laptops now outsell desktop devices. A WLAN is preferred over a wired Ethernet LAN for network access in all other cases because wireless technology enables pervasive mobility while wired Ethernet doesn't. Pervasive mobility is the ability of workers to remain connected to the LAN regardless of where they are located within the enterprise. One can analyze the differences between 802.11 and Ethernet with respect to performance, security, manageability, cost and impact on staff. However, the unalterable competitive advantage that 802.11n has over wired Ethernet is the ability to provide pervasive mobility.

Conclusion

802.11n has significant advantages over legacy wireless technologies and, with Wi-Fi certification in place since June 2007, is ready for enterprise deployment now. These advantages present the enterprise network manager with important deployment considerations. Managers that take time to evaluate these considerations, within the context of their enterprise needs and constraints, will improve their ability to achieve a successful 802.11n deployment.

Further Reading

Wi-Fi Alliance. "Wi-Fi CERTIFIED™ 802.11n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi® Networks." *Wi-Fi.org*. Jun 2007

Wi-Fi Alliance. "Wi-Fi CERTIFIED Makes it Wi-Fi: An Overview of the Wi-Fi Alliance Approach to Certification." *Wi-Fi.org*. 2006

Paul DeBeasi. "802.11n: Beyond the Hype." *BurtonGroup.com*. 5 Jul 2007

Paul DeBeasi. "802.11n: The End of Ethernet?" *BurtonGroup.com*. 28 Aug 2007

Paul DeBeasi. "Securing WLANs in the Enterprise." *BurtonGroup.com*. 18 Dec 2007

Paul DeBeasi. "Wireless Local Area Networks." *BurtonGroup.com*. Apr 2008

Author Bio

Paul DeBeasi is a senior analyst at Burton Group and has more than 25 years of experience in the networking industry. Before joining Burton Group, Paul founded ClearChoice Advisors, a wireless consulting firm, and was vice president of product marketing at Legra Systems, a wireless-switch innovator. Prior to Legra, Paul was VP of product marketing at startups IPHighway and ONEX Communications, and was also the Frame Relay product line manager for Cascade Communications. Paul began his career developing networking systems as a senior engineer at Bell Laboratories, Prime Computer, and Chipcom Corporation. Paul holds a bachelor's of science degree in systems engineering from Boston University and a master's degree in electrical engineering from Cornell University.

About the Wi-Fi Alliance

The Wi-Fi Alliance is a global, non-profit industry association of more than 300 member companies devoted to promoting the growth of wireless Local Area Networks (WLANs). With the aim of enhancing the user experience for wireless portable, mobile, and home entertainment devices, the Wi-Fi Alliance's testing and certification programs help ensure the interoperability of WLAN products based on the IEEE 802.11 specification. Since the introduction of the Wi-Fi Alliance's certification program in March 2000, more than 4,500 products have been designated as Wi-Fi CERTIFIED™, encouraging the expanded use of Wi-Fi products and services across the consumer and enterprise markets.

Wi-Fi®, Wi-Fi Alliance®, WMM®, the Wi-Fi CERTIFIED logo, the Wi-Fi logo, and the Wi-Fi ZONE logo are registered trademarks of the Wi-Fi Alliance; Wi-Fi CERTIFIED™, Wi-Fi Protected Setup™, Wi-Fi Protected Access (WPA™), Wi-Fi Multimedia™, and the Wi-Fi Alliance logo are trademarks of the Wi-Fi Alliance.