The future of Wi-Fi in the enterprise

By Monica Paolini

This research was underwritten by Xirrus.

Table of contents

Executive summary

Wi-Fi is the technology that has first brought wireless broadband to the market — both among residential users and in the enterprise. Despite the fast adoption of mobile broadband, Wi-Fi still is the only or predominant wireless access technology today for most of us. Wi-Fi has shown a remarkable ability to evolve, to meet increasingly higher expectations and requirements, and to become pervasively adopted in mobile devices.

The evolution of Wi-Fi continues unabatedly to deliver increased performance, security and reliability in the existing and new license-exempt spectrum bands. It also continues to deliver a more advanced air interface, thanks to a robust ecosystem that staunchly supports standard-based solutions and interoperability among vendors and to an ever-growing range of device form factors that is widening the scope for Wi-Fi applications.

All of these factors are highly prized by the enterprise, public and safety agencies, as well as health and educational institutions that are increasingly deploying larger, high-performance and high-capacity Wi-Fi networks that have become fully integrated within the IT infrastructure. The increased centrality of Wi-Fi has resulted in higher capacity, coverage and security requirements, as well as in the need for Wi-Fi to support more-demanding classes of traffic (e.g., video and voice), a wider range of devices (e.g., tablets) and new applications (e.g., cloud computing, machine-to-machine communications).

This paper follows the ascent of Wi-Fi and looks at how its expanding role within the enterprise — including public or private organizations in the education, health care, government and safety sectors, both to provide access to employees and to support specific enterprise-specific applications that increasingly are machine-to-machine (M2M) — drives more-advanced requirements. We also examine how these requirements will be met by further expansion in the Wi-Fi standards and by a new generation of Wi-Fi equipment and devices. In closing, we discuss how the enterprise

can benefit from the evolution of Wi-Fi by deploying future-proof networks that will organically improve performance.

Introduction

The rapid-fire growth of Wi-Fi over the past decade has been nothing short of extraordinary, but what truly makes Wi-Fi stand out over other wireless technologies is its unremitted capacity to evolve to meet continuously growing requirements from the enterprise and consumer users at the same time.

Designed initially with a very narrow scope — to provide wireless connectivity across computers on Hawaiian islands that lacked wireline links[1] — Wi-Fi, or, more precisely, the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard on which Wi-Fi is based, grew to conquer both the enterprise and the consumer electronics (CE) market by incrementally expanding its role, improving performance and security, adding new functionality, and supporting a wider range of devices and applications.

In the enterprise and other organizations like hospitals, educational institutions or public agencies, Wi-Fi was initially deployed to provide a basic broadband connection to employees' laptops. Today it has become a core part of the information technology (IT) infrastructure that has to meet stringent security, performance and availability requirements and that increasingly is required to carry voice and video communication, in addition to best-efforts data and to support specific applications such as surveillance and monitoring. The explosive growth in device form factors, ranging from smartphones and tablets to sensors and surveillance cameras, that pervasively have Wi-Fi embedded continues to bring further cost savings and productivity gains and to expand the functionality of Wi-Fi within the enterprise.

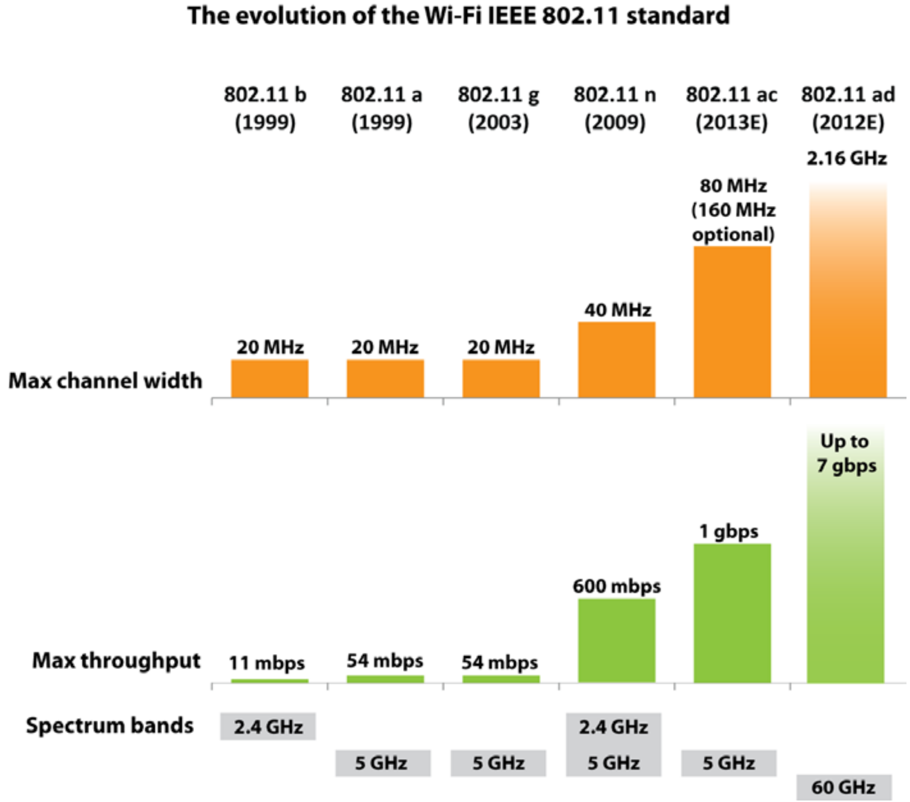
No longer an accessory network designed to cover meeting and public areas, Wi-Fi deployments are increasingly required to provide ubiquitous coverage. This coverage

1 Iljitsch van Beijnum and Jaume Barcelo, "Cutting the cord: how the world's engineers built Wi-Fi"

includes both the enterprise headquarters and remote offices and both the indoor locations and outdoor spaces between them. It also goes beyond offices to cover warehouses, factories, mining grounds, educational campuses, health care facilities and military bases.

Far from having exhausted its growth capabilities, Wi-Fi keeps growing, with a promise to move past the gigabit throughput threshold to expand to new spectrum bands, provide increased capacity and better coverage, and improve support for real-time traffic, such as voice and video.

Figure 1. The evolution of the Wi-Fi IEEE 802.11 standard



Source: GigaOM Pro

Wi-Fi performance has steadily improved from the initial 11 Mbps peak throughput supported by IEEE 802.11b in 1999, initially limited to the 2.4 GHz band, to the current 600 Mbps by 802.11n, due to the use of wider channels in the 5 GHz band and a more advanced over-the-air interface that uses multiple-in multiple-out (MIMO) technology. Future versions of Wi-Fi further expand channel widths and take Wi-Fi to the license-exempt 60 GHz millimeter band, and they promise throughputs of over 1 Gbps (Figure 1).

With the transition from Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access 2 (WPA2) in 2004, security came of age in Wi-Fi networks, and WPA2 has been a crucial tool for the technology to gain full acceptance within the enterprise. Support for more-advanced applications with real-time requirements (e.g., those involving voice or

video) has been introduced with Wi-Fi Multimedia (WMM) that supports quality of service (QoS) functionality.

The expanding presence of Wi-Fi within the enterprise

The rise to prominence of Wi-Fi in the enterprise has been an atypical one for a wireless technology, as it was to a large extent driven by employees rather than by the organizations they were working for — although, interestingly, it is a pattern that has also been followed by the iPhone and tablets. Initially developed with the enterprise and educational environment in mind, it quickly gained an enthusiastic following among residential users, and that popularity in many cases drove the initial enterprise deployments. As employees started to surreptitiously bring their Wi-Fi access points (APs) to their offices to get local wireless connectivity for their laptops and to share it with their colleagues, many enterprises realized the value that Wi-Fi brings to the workplace. They were also quick to see the security implications of unsecured employee-controlled APs linked to their corporate networks.

Instead of fighting unauthorized Wi-Fi APs, most enterprises decided to embrace Wi-Fi and to take control of the Wi-Fi infrastructure. They built campus-wide networks that provided secure connectivity to all staff. This has been a successful strategy that has brought wireless broadband to the enterprise way ahead of cellular networks.

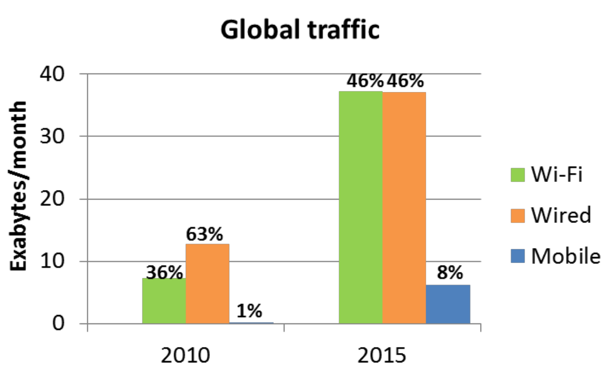
Furthermore, the increasing availability of built-in Wi-Fi at little or no additional cost in laptops first and in mobile phones more recently, as well as the wide availability of home and public Wi-Fi networks, has allowed enterprises to benefit from Wi-Fi well beyond their footprints. Employees can use the same devices and the same applications to continue their work or check their email from wherever they are — home, at their local coffee shop or while traveling. From the enterprise perspective, this means higher productivity and efficiency and lower costs.

Aided by harmonized spectrum allocations across the world and by a highly respected certification program established by the Wi-Fi Alliance, the Wi-Fi ecosystem's staunch support for interoperability has made it possible for Wi-Fi to spread worldwide. We

may now take for granted that any Wi-Fi device we buy will work pretty seamlessly in any network, but this degree of interoperability was initially — and probably still is — unparalleled among wireless technologies.

The increasing availability of Wi-Fi networks and the pervasiveness of Wi-Fi devices have steadily increased the share of data traffic over Wi-Fi. Wi-Fi accounted for 36 percent of global IP traffic in 2010, and it is expected to reach the amount of wired IP traffic by 2015, according to Cisco's Visual Networking Index (VNI) (Figure 2). Wi-Fi traffic in mobile devices is even more prominent. Juniper Research[2] predicts that by 2015, 57 percent of the data traffic over mobile phones and tablets will be carried over Wi-Fi, up from 42 percent in 2010. Similarly, comScore reports that Wi-Fi accounts for 37.2 percent of mobile phone access, at over 90 percent of tablets and other wireless devices (Figure 3).

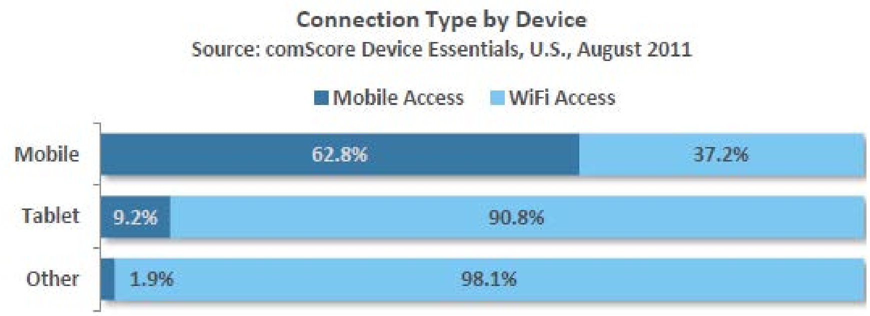
Figure 2. Wired, Wi-Fi and mobile IP global traffic



Source: VNI, Cisco

[2] Juniper Research, "Mobile Data Offload & Onload," March 2011

Figure 3. Wi-Fi as a percentage of traffic in mobile devices



Source: comScore

The increase in Wi-Fi traffic has been accompanied — or it may have contributed to causing — the emergence of a wireless office environment. In this environment, employees are free to move within the workplace while staying seamlessly connected within their corporate network; they can also keep their applications active without worrying about security. In many enterprises, this has created a more flexible work environment that encourages interaction among employees and increases efficiency.

The advantages that Wi-Fi has brought to the workplace have also raised the expectations and requirements. Gone are the days when Wi-Fi networks were kept as a stand-alone part of the IT infrastructure to be used basically to check email or browse the Internet. Now the Wi-Fi infrastructure has become an integral part of the overall corporate network, and it has to meet comparable requirements, especially with regard to:

- Security
- Coverage
- Reliability
- Capacity
- Support for best-effort traffic, as well as voice and video
- Features (e.g., support for QoS)

- Interoperability

While it cannot be expected that the throughput over a wireless interface matches that of a fiber connection, it is expected that Wi-Fi networks efficiently and effectively transport the traffic generated by employees and M2M wireless devices, as the wireline infrastructure does.

For a technology like Wi-Fi, these are challenging requirements to meet, as they initially were not included within the scope of the standard. Wi-Fi uses exclusively license-exempt bands, which are subject to interference and stricter transmission power limitations than licensed bands, like those used in mobile networks. Interference can affect performance, reliability, coverage and the overall quality of experience. The collision-avoidance transmission (also known as a “listen-before-you-talk”) algorithm used by Wi-Fi ensures that all devices within a network have equal opportunity to receive and transmit data, and it provides an environment where many devices can receive and transmit at the same time. But it can also limit the ability to actively manage and prioritize traffic, and this can degrade performance in highly loaded networks. Yet the Wi-Fi avoidance of a command-and-control approach has shown a remarkable capability in managing interference and device coexistence in the high-traffic areas where Wi-Fi is most frequently deployed.

Over the years, multiple solutions have been developed to retain the core Wi-Fi features that are behind its success — i.e., the ability to use freely available spectrum as well as interoperability and legacy support for all Wi-Fi devices — while adding support for advanced functionality, through a mix of standards-based enhancements and proprietary extensions. Wi-Fi has been extremely successful in finding the right balance between supporting the existing devices and equipment and aggressively pursuing innovation.

The results have been impressive. On one hand, Wi-Fi is increasingly used outside the enterprise to offload traffic from congested and slower mobile networks or to provide public access to occasional users. In these environments, Wi-Fi has shown to be very

effective at frequently providing a better end-user experience than cellular networks that use licensed spectrum, often in environments with challenging RF and multiple overlapping networks interfering with one another.

On the other hand, virtually all vertical markets have adopted Wi-Fi to support highly demanding or mission-critical applications. Wi-Fi is increasingly used in many military applications, even in those in which security is a paramount concern. Public safety agencies have been at the forefront of Wi-Fi adoption to provide nomadic connectivity to their staff, their vehicles and, increasingly, to support surveillance and remote control applications. More recently, utilities have started to include Wi-Fi as one of their core technologies in smart-grid deployments.

The adoption of Wi-Fi in verticals like the military, public safety and utilities is particularly instructive, because in most countries they have access to reserved spectrum. Yet, in many cases, the license-exempt Wi-Fi bands prove to be the best suited to deliver the performance and functionality required, along with a wide choice of interoperable devices, at the right price point.

A higher performance bar

The increasing reliance on wireless communications is creating an increased sense of urgency in the enterprise to expand and deepen the Wi-Fi footprint and improve its reliability and resiliency, as it provides the preferred wireless access technology. Adoption of Wi-Fi continues to rise both in terms of width — with a higher percentage of enterprises in more vertical sectors deciding to deploy Wi-Fi networks — and in terms of depth — with enterprises expanding their existing deployments, supporting more devices and more applications (Figure 3).

Figure 4. Drivers for the next stage of growth in Wi-Fi in the enterprise

Wi-Fi growth drivers	Implications
Wi-Fi has become the primary access technology for many users, devices and applications. Increased adoption of cloud applications designed to be available across locations and devices confers further value to Wi-Fi, as it provides a preferred, secure conduit to the cloud, which in an enterprise environment typically has a better performance than cellular technologies.	Wi-Fi performance, reliability and coverage have to be comparable to wireline technologies. Advanced security (multiple authentication methods, data encryption, intrusion prevention and detection systems [IDS/IPS]) also has to be available for all devices that connect to the network.
There has been a steep increase in overall data traffic and specifically in wireless and mobile data traffic.	Congestion in cellular networks makes the offload of mobile traffic to Wi-Fi more compelling. In addition to carrier-driven offload data traffic from mobile networks to Wi-Fi, enterprises increasingly strive to keep their employees on their Wi-Fi corporate networks to provide better performance and retain more control over subscribers' quality of experience.
Rapidly growing adoption of a wide range of mobile-only devices. Tablets are rapidly becoming increasingly deployed as they provide a powerful form factor to support core and segment-specific applications.	Enterprise Wi-Fi networks have to provide full, seamless support to new devices. At the same time, the new devices and infrastructure have to coexist with older devices that may lack some of the new product features. The enterprise has to ensure that these legacy devices can coexist within the WLAN (wireless local area

	network) without interfering with the performance of new devices. A high penetration of mobile devices will also harvest the seeds for a pervasive adoption of location-based applications and for the inclusion of location-aware functionality to existing applications.
Mobile operators try to extend Wi-Fi offload to enterprise-controlled zones such as campuses.	Enterprises may open their Wi-Fi infrastructure to mobile carrier offload or allow mobile operators to install their own infrastructure. In the latter case, enterprises and operators have to work together to minimize the impact of interference.
Adoption of M2M applications is expected to grow rapidly over the next few years, driven by increased Wi-Fi coverage and affordability of Wi-Fi modules for M2M sensors, meters, cameras, and other devices.	M2M applications have a huge diversity in requirements. Many require little bandwidth, but high reliability and good coverage. Others require high throughput levels but only at a few locations. In all cases, M2M applications will increase the Wi-Fi network complexity and the number of the devices to be supported. In some networks, this may have a deep impact on h0w the network is managed.

Source: GigaOM Pro

Underlying this growth, there is a clear trend toward tighter integration with the fixed IT infrastructure.

Wi-Fi deployments initially had tens of APs, which were loosely managed and installed where needed without detailed planning. Today many Wi-Fi deployments include thousands of APs to provide not only wider coverage but also more-consistent

coverage across the footprint and higher throughput. A higher concentration of APs can improve coverage by eliminating islands with no coverage and areas located farther away from the AP or affected by obstruction that have unreliable connectivity and low throughput.

Equally important is the realization that the wireless environment is intrinsically dynamic. Users move across the coverage footprint, and they want to stay seamlessly connected and keep their applications running as their devices detach from AP to associate to the next. But the RF environment also changes over time. New sources of interference may appear, and existing ones may vanish or change. Propagation obstacles may move.

These two factors — fully integrated, larger networks with ubiquitous coverage and operations within a dynamic environment — have a deep impact on how networks are planned and managed, which equipment and architectures are selected, and what security mechanisms are implemented.

While Wi-Fi is becoming increasingly pervasive across vertical markets, the rate of adoption and growth as well as the dominating devices and applications change considerably across different vertical markets beyond enterprise office locations, such as health care, military, public safety, transportation, education, utilities or mining. Enterprise office coverage, educational institutions and public agencies have often been at the forefront of adoption. As Wi-Fi has widened the range of applications that it has supported, a more varied range of vertical segments have joined in. This has led to a much richer choice of Wi-Fi equipment, in terms of APs' form factors (i.e., more ruggedized equipment) and integration of Wi-Fi in a growing range of CPE devices. The usage models are still developing, and many enterprises are actively exploring which applications provide a positive return on investment (ROI) and which ones provide a better fit to their needs.
The health care segment provides a good example of the wide range of wireless applications and devices[3] that Wi-Fi is increasingly called to support (Figure 5).

[3] Wi-Fi Alliance, "Wi-Fi in Healthcare: The solution for growing hospital communication needs," 2011

Figure 5. Wi-Fi in health care: a powerful technology for a challenging environment \

Wi-Fi's role in a hospital	Requirements
Provide wireless connectivity to staff, who often do not work from a fixed office location, using laptops, smartphones, tablets or customized devices for specific applications (e.g., for internal voice communications) and who may need to retain connectivity as they move through the hospital	▪ Provide extended, reliable coverage across the entire hospital ▪ Support a wide range of devices, vendors and form factors. Many devices are exclusively mobile, and some may connect to multiple wireless networks (e.g., smartphone or tablets with a cellular connection) ▪ Enable roaming and session continuity to allow staff to continue working as they move to their next location
Provide a media-rich platform to doctors and other staff for access to medical records, remote consultations, communication among teams and with patients	▪ Provide high levels of security to protect confidentiality of medical records ▪ Meet latency, jitter and packet-loss requirements to support real-time voice and video traffic ▪ Use QoS to prioritize voice and video traffic
Collect data and transmit data to medical equipment that has to be moved to follow patient's location.	▪ Enable high-throughput, secure connections. ▪ Provide robust coverage that can accommodate changes in the RF environment (i.e., changes in levels and sources of interference or in the

	location of obstructions)
Track patient conditions through wearable mobile devices and sensors.	▪ Provide a high-reliability infrastructure, with good coverage to ensure continuous monitoring. ▪ Enable effective management of mobile devices that may use cellular networks as a supplementary interface. ▪ Remain connected as patients move within the hospital. ▪ Maximize battery life for mobile devices.

Source: GigaOM Pro

Moving ahead: Will Wi-Fi keep its performance edge?

The success of Wi-Fi in the enterprise, as well as in the consumer market, was to a large extent driven by the ability of the technology to evolve and improve performance. At this stage, it's worth asking, Can Wi-Fi continue its ride and be able to innovate in response to the new usage models and more-sophisticated requirements driven by new devices, applications and the overall transition to pervasive wireless connectivity? Or has Wi-Fi reached a maturity plateau where there is only scope for incremental improvements? Are there new technologies ready to take its place?

The amount of activity within the IEEE 802.11 group, the Wi-Fi Alliance and the vendor ecosystem, as well as the interest from the enterprise, suggest that there is plenty of life left in Wi-Fi, with evolution in functionality and performance taking place in multiple parallel directions.

Wi-Fi's position as the preferred wireless local area network (WLAN) technology is not challenged by new next-generation technologies. In fact its dominance is becoming more deeply established, as enterprises continue to expand their Wi-Fi networks, leveraging the existing infrastructure — a more cost-effective approach than replacing it with a new technology. For a while, there has been a perceived threat that WiMAX or 3G would present a challenge, but the need for licensed spectrum, which is difficult — if not impossible — for the enterprise to obtain at a justifiable price point, has only strengthened Wi-Fi's position. And to date there are no technologies that could credibly challenge Wi-Fi in the license-exempt band. This is in sharp contrast with the cellular industry, where third-generation (3G) technology is still being actively deployed but there is very limited scope for further evolution, as mobile operators are all converging to fourth-generation technology (4G) for new deployments.

The introduction of IEEE 802.11n[4] in 2009 (Figure 6) marked an important new phase in Wi-Fi growth, bringing an increase of up to 100 percent in coverage and up to 5 to 10 times an increase in throughput over the IEEE 802.11a/b/g versions of the standards (Figure 1). In many deployments, the transition is still ongoing as enterprises gradually upgrade to n as needed. An overall market transition to IEEE 802.11n is clearly taking place, with IEEE 802.11n equipment accounting for 87 percent of overall units sold[5] and 97 percent of enterprise equipment sales[6].

4 Wi-Fi Alliance, "Wi-Fi CERTIFIED n: Longer-Range, Faster-Throughput, Multimedia-Grade Wi-Fi Networks," 2009

5 In-Stat, "Q2'11 Wi-Fi Network Equipment Database: By Region, Form Factor, Technology, and Vendor," 2011 (www.instat.com)

6 Dell'Oro, WLAN quarterly report, 2011

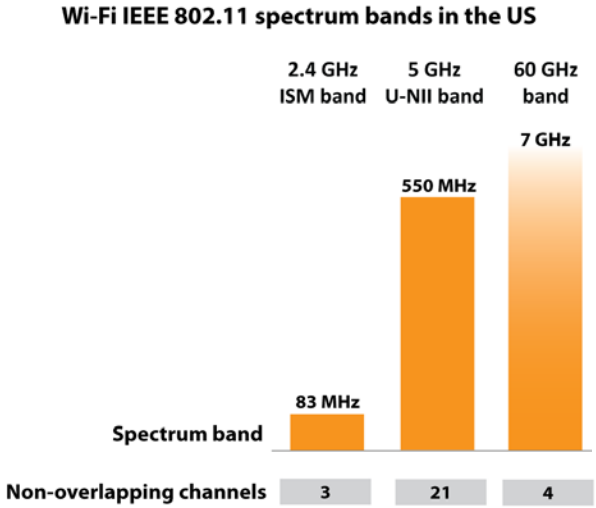
Figure 6. Certification logo for IEEE 802.11n-based equipment

Source: Wi-Fi Alliance

MIMO was at the core of the increased throughput and improved coverage in IEEE 802.11n in 2009 (Figure 1). Now widely used in 3G and 4G cellular networks, MIMO's first adoption in a mass-market technology was in Wi-Fi, and indeed there was initially substantial uncertainty as to whether MIMO was effective in improving performance and whether it was affordable. MIMO uses spatial multiplexing to send concurrent data streams transmitted over multiple antennas. Initial MIMO equipment had a 2x2 configuration, with two antennas in the AP and two antennas in the user device; MIMO equipment can now support 3x3 and 4x4 configurations as well. The signal is decomposed before transmission and then reconstructed by the receiving terminal. As a result, with MIMO, Wi-Fi can pack more traffic in the same amount of spectrum. Moreover, MIMO can use multipath due to reflections from objects within the coverage area of the AP to its advantage, as the temporal delay introduced by multipath is used to segregate data streams. This offers an additional improvement in coverage in non-line-of-sight environments. IEEE 802.11n also improves performance by using frame aggregation to reduce overhead and by supporting wider channels, from 20 MHz to 40 MHz.

IEEE 802.11n has also had the side advantage of encouraging the utilization of the wider 5 GHz band (21 nonoverlapping 20 MHz channels, versus 3 in the 2.4 GHz band in most countries) (Figure 7), which is less heavily used, even though it has been supported by the standard since 1999. While IEEE 802.11n operates in both the 2.4 GHz and in the 5 GHz band, the wider 40 MHz channels in the 5 GHz band are better suited to support the highest throughput rates. The 2.4 GHz band has been the one initially used by Wi-Fi equipment, and it was preferred because of the better propagation. With the increased traffic levels (and, hence, interference) and the need for additional throughput, the migration to the 5 GHz band has become imperative.

Figure 7. Wi-Fi IEEE 802.11 spectrum bands in the U.S.



In the U.S., Wi-Fi can also be used in the lightly regulated 3.65 GHz band (IEEE 802.11y). Wi-Fi adoption in this band is still limited and is mostly used in niche vertical applications.
ISM band: Industrial, scientific and medical band
U-NII band: Unlicensed national information infrastructure band

Source: Wi-Fi Alliance, GigaOM Pro

Among the ongoing IEEE activity to enhance the 802.11 standard, there are two initiatives that will provide impressive performance enhancement to Wi-Fi: IEEE 802.11ac (or Very High Throughput [VHT] <6 GHz) and IEEE 802.1ad (VHT 60 GHz). Furthermore, Super Wi-Fi, based on IEEE 802.11af, will enable Wi-Fi to use promising sub-1-GHz white space spectrum.

IEEE 802.11ac operates in the same 5 GHz band as IEEE 802.11n, but it is expected to provide up to 1 Gbps throughput by increasing spectrum channel widths to 80 MHz (with optional support for 160 MHz channels) (Figure 1), more MIMO streams (8, up from 4 in IEEE 802.11n), multiuser MIMO, and improved modulation (from 64-quadrature amplitude modulation [QAM] in IEEE 802.11n to 256-QAM). The standard amendment is expected to be finalized at the end of 2012 and approved by 2013. IEEE 802.11ac will continue to support devices using legacy Wi-Fi (i.e., IEEE 802.11a/b/g/n) and narrower channels.

While IEEE 802.11ac will increase spectrum efficiency in the 5 GHz band, it still uses the same spectrum resources as IEEE 802.11n, so there is only an incremental capacity enhancement. IEEE 802.11ad introduces a much more innovative development in Wi-Fi that is likely to have a deeper impact on how Wi-Fi will be deployed in the future. The Wireless Gigabit Alliance (WiGig) released the initial specifications in 2010 and contributed them to the IEEE to become part of the IEEE 802.11ad standardization process. The WiGig and the Wi-Fi Alliance are working together to complete the IEEE 802.11ad standardization process, and the Wi-Fi Alliance will establish a certification program for IEEE 802.11ad equipment. The IEEE 802.11ad amendment is expected to be ratified in 2012.

IEEE 802.11ad[7] uses the 60 GHz millimeter band. Like the 2.4 GHz and the 5 GHz bands, it is a license-exempt band that is free for the enterprise to use. But it is a much wider band: While the existing Wi-Fi bands combined have an allocation of less than 700 MHz in most countries, the 60 GHz band ranges from 5 to 9 GHz (Figure 8). The introduction of IEEE 802.11ad will add a further 7 Mbps to Wi-Fi networks while continuing to support the 2.4 GHz and 5 GHz devices.

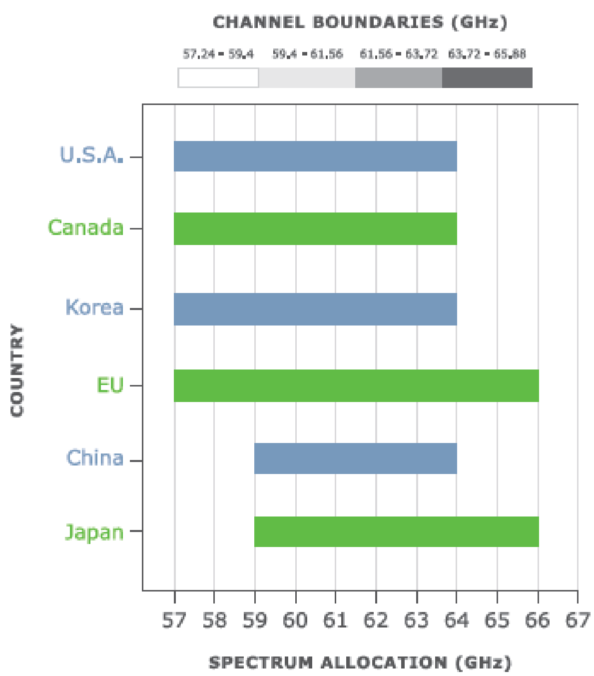
At the same time, the 60 GHz band provides more-limited coverage, with the subscriber devices required to be within line-of-sight (LOS) of the AP. In dense deployments with limited obstructions, the propagation limitations of the 60 GHz band may often be successfully managed by careful RF planning or by leveraging the other spectrum bands for edge users. For deployments that do not require a high-capacity density and, therefore, do not require a dense network of APs, the use of the 60 GHz band will typically require more APs to cover the same area than other bands.

To mitigate the impact of propagation loss in the 60 GHz band, IEEE 802.11ad supports adaptive beamforming, which uses directional antennas to dynamically direct a narrow transmission beam toward the location of user devices, extending the coverage area beyond ten meters and enabling some degree of non-line-of-sight

[7] Wireless Gigabit Alliance, "Defining the Future of Multi-Gigabit Wireless Communications," 2010

(NLOS) connectivity. Designed primarily for high-resolution video applications, IEEE 802.11ad will support low-power user mobile devices. This can be advantageous for many enterprise applications as well that may require high throughput to and from mobile devices (e.g., wireless displays when using real-time video streaming or remote video cameras for surveillance) or a high number of mobile devices within a small area.

Figure 8. Global availability of spectrum in the 60 GHz millimeter band



Source: Wireless Gigabit Alliance

Super Wi-Fi is based on IEEE 802.11af, a version of the 802.11 standard that expands the scope of Wi-Fi to include about 300 MHz of sub-1-GHz spectrum, to be used in a noninterfering basis, in the gaps between VHF and UHF channels used for TV broadcast, which were previously used for analog broadcast. Because of the advantageous propagation characteristics of sub-1-GHz bands, Super Wi-Fi can be used in outdoor environments with a radius of 100 km when higher power is used and in indoor environments when the low-power version can be used.

Outdoor deployments are more likely to be concentrated in rural areas, as those are the areas where white space spectrum is mostly available. Indoor Super Wi-Fi can be deployed and used in a way similar to other Wi-Fi interfaces in the 2.4 GHz and 5 GHz bands. Indoor Super Wi-Fi can have better in-building penetration characteristics than Wi-Fi, but as a result, self-interference may limit the usefulness of Super Wi-Fi to provide enterprise coverage. The specification is expected to be ratified into the IEEE 8021.11 standard in 2012. Afterward, the Wi-Fi Alliance plans to launch a certification program to test adherence to the standard and interoperability among vendors.

Spectrum availability imposes major limitations in the use of white spaces. Technologies such as Super Wi-Fi can only be used in the channels that are not being used by broadcasters to avoid interference with the TV signal. In practice this results in very limited spectrum availability in metropolitan areas, where most enterprises are located.

Channel size is another limitation of Super Wi-Fi, as individual channels are limited to 6 GHz. MIMO and channel bonding are expected to improve performance, but as the channels that can be bonded vary through time and location, channel bonding may prove to be challenging.

Competing with Super Wi-Fi is the IEEE 802.22 standard (published in July 2011) for wireless regional area network, which uses cognitive radio to dynamically select the spectrum channels that are available. The standard is primarily aimed at the rural underserved market, where there is no direct competition with Wi-Fi. An amendment to the standard, IEEE P802.22.1, has been developed for low-power, shorter-range devices that can be deployed as an alternative to Wi-Fi. In this context, Super Wi-Fi has the advantage of being a mature, well-understood and widely used technology that, like IEEE 802.22, incorporates cognitive radio and may become the dominant technology.

Wi-Fi innovation from standards to the market

Standards are the foundations that enable the development of products and applications for technologies and of the ecosystem that supports it. Yet much of the innovation is tied to incremental enhancements that are added to the specifications enshrined in the standards.

In Wi-Fi, a competitive and fast-moving ecosystem with a large number of players, a widely accepted IEEE standard and the recognition that interoperability is necessary to ensure adoption have created a dynamic vendor environment that ranges from low-cost, no-frills vendors that offer basic products at unbeatable prices to technologically sophisticated vendors with a tight focus on a market, application or technology niche that provide optimized performance and higher reliability.

For enterprise users, this high level of competition and choice can be confusing at times. At the same time, the high number of vendors gives enterprises — long used to much more expensive and slowly innovating proprietary products — the freedom to pick the vendor they want, a greater flexibility in innovating their network incrementally and the confidence that Wi-Fi will be around for a long time and that they are not tied to a single vendor. For instance, a company may decide to move to a new architecture (e.g., to a mesh network or from a centralized to a distributed network), but it may still be able to keep some of the existing equipment within its network, even if choosing a different vendor, or to retain two coexisting networks. In any case, all the devices can still access the network. In fact, users may not even notice they have moved from one network to another. To make use of new functionality that the old network did not support, new devices may have to be introduced (e.g., devices have to support WMM to use standards-based Wi-Fi QoS functionality), but at the same time they will be able to use the old network for basic connectivity.

Among mobile devices, Wi-Fi modules are pervasive and inexpensive. In the future, further growth in volumes and maturity of the technology will increase the percentage of devices with built-in Wi-Fi or that are ready to connect to Wi-Fi through a dongle.

This accelerates Wi-Fi adoption in vertical applications that may use remote sensors, cameras or low-cost consumer mobile devices that can be customized to run specific vertical applications.

The crucial wave of innovation in wireless connectivity was brought by smartphones. They now have become easy to use and powerful enough that in some environments they can substitute laptops or desktops or work alongside them.

The most recent wave, still in its early infancy, is generated by tablets. While designed primarily for the residential subscriber, the tablet has been successfully introduced to enterprise environments. It is valuable for the enterprise because it supports applications that require a bigger screen but do not require the power of a laptop, as well as light and low-power devices.

The Wi-Fi infrastructure equipment market is a diversified ecosystem in which many vendors have carved niches that allow them to meet the specific requirements of the enterprise. From the air-interface perspective, vendors have embraced MIMO, initially in 2x2 configurations and now increasingly with a high number of streams, and they have also launched products that use advanced antenna technologies such as multiple flavors of beamforming. Omnidirectional antennas are still prevalent, but vendors are increasingly focusing on multisector APs, directional antennas, distributed antenna systems (DAS) and point-to-point (PTP) links.

Vendors also support different topologies that have evolved a long way from the initial mesh architectures that imposed a substantial latency penalty. As Wi-Fi networks become bigger and denser and require higher reliability, we expect network topology to become a more prominent decision factor during network planning, as it enables enterprises to optimize performance.

More-advanced topologies and larger networks, in turn, increase the relevance of network management in the smooth and seamless performance of the network. Multiple approaches to network management have emerged, ranging from highly

centralized platforms, which allow the enterprise to tightly control all network elements and their interfaces to the IT network, to distributed platforms, which push network intelligence to the edge to limit the impact of bottlenecks or failures to a contained part of the network.

Another area of intense innovation for enterprise Wi-Fi is traffic management. Initially this was a weak area for Wi-Fi, because license-exempt spectrum limits the ability to prioritize traffic, especially in environments with high interference levels. The introduction of WMM provided the basis for a standards-based implementation of QoS, to which vendors often add increasing functionality, especially to improve performance and to enable more-granular traffic prioritization for voice and video traffic. As mobile devices become more widely used in enterprise networks, the mobility management is also gaining traction, as it enables Wi-Fi networks to support handovers between Wi-Fi APs and session continuity. Moving forward, it may expand to include seamless handovers to cellular networks for both data and voice. This allows the enterprise to fully — and finally — benefit from a full integration between voice and data applications.

In the future, especially with the availability of Wi-Fi equipment in the 60 GHz band and with the increased coverage and throughput requirements, we expect to see advanced products that offer better performance and coverage, higher reliability and more-powerful interference-avoidance tools to gain market share and become more widely deployed. This will initially occur in larger corporations and for highly demanding applications but eventually within a much broader customer base.

The adoption of more-sophisticated products, however, will also force a transition to a more complex Wi-Fi network architecture that, although transparent to the end user, will require more careful network planning, monitoring and management from IT teams. The increase in complexity runs in parallel with what we see in other wireless technologies — for instance in cellular networks with the move from homogeneous cellular networks to multilayer networks, which has started with the well-established macro level to include small cells, femtocells and Wi-Fi offload.

Planning for a future-proof network

The enterprise can choose among a wide range of solutions and equipment functionality to deploy a Wi-Fi network, but ultimately the ability of the network to meet current requirements and to organically evolve as these requirements grow and more-powerful solutions become available rests on how the network is designed and how well the selected elements provide sufficient flexibility to create a future-proof infrastructure. A future-proof infrastructure would be one that can organically evolve with equipment availability and enterprise needs and that does not require expensive and time-consuming forklift upgrades.

The next phase of Wi-Fi deployments will see larger networks with higher density and wider coverage that can support heavier traffic loads. There will be many fixed and mobile device types, and the deployments will be tightly integrated within the larger IT infrastructure.

As we transition, there are multiple dimensions that will shape the ability of the enterprise to fully benefit from innovation and to leverage innovation in Wi-Fi to meet its rapidly evolving needs.

Scalability. Larger networks do not simply mean more APs. The overall approach to planning and selection of a solution often has to deeply change as networks grow, and it needs to take into account:

- Larger traffic loads, with the consequent ability to backhaul this traffic
- Better coverage, which also entails stronger interference management
- Higher complexity in managing the network infrastructure and traffic, as well as in integrating it within the overall IT infrastructure
- Need for tighter security

Coverage requirements. As Wi-Fi increasingly becomes an integral part of the IT infrastructure, it has to be available everywhere within the enterprise. It is no longer acceptable to tell employees to move closer to the AP or to the meeting room to get wireless connectivity. Wi-Fi has to follow them where they go and provide reliable, high-throughput, continuous or near-continuous coverage. Good coverage is challenging for Wi-Fi. In the 2.4 GHz band, it can be difficult to achieve it in areas with high levels of interference. In the 5 GHz band, propagation limitations require a higher density of APs to ensure the same coverage that can be achieved in the 2.4 GHz band. At the same time, the 5 GHz band is highly preferable to the 2.4 GHz band, because it is less heavily used and has more spectrum (Figure 7). To optimize coverage, the enterprise can use multiple tools, including directional antennas, multisector APs, or beamforming. The predeployment RF analysis and ongoing RF monitoring of the infrastructure are also needed to extract the best performance from the selected equipment, and careful power-level tuning is needed to balance the trade-off between coverage (more power, better coverage) and interference management (less power, less interference).

Capacity requirements. More users, more devices, more applications and a heavier reliance on wireless connectivity clearly converge to higher traffic loads. Improvements in performance and coverage also contribute to traffic increase, as users get to use the infrastructure more intensively. Instead of waiting for a big file to download, they can move on to download the next one. Instead of waiting to be within the area covered by Wi-Fi, they can join the conference call in video mode now. While the new generation of Wi-Fi equipment supports higher throughput and, consequently, capacity density (i.e., network capacity per square mile), there are trade-offs between throughput and range that need to be considered when planning for a network.

The same is true when choosing among solutions with substantial differences in performance. These differences are often dependent on the specific environment in which the network is deployed. As throughput to individual users declines as the distance from the AP increases (or the path becomes more obstructed), the overall

capacity of an AP depends on the distribution of users' locations. As a result, maximizing coverage may lead to lower capacity density, and, vice versa, maximizing capacity density is likely to reduce range. Equipment that supports MIMO, directional antennas or beamforming can provide both improved coverage and higher capacity, but the trade-offs between the two need to be carefully evaluated to extract the desired capacity and range mix. In an office environment with a high number of users generating high traffic volumes, increasing capacity is much more important than expanding coverage. In fact, increasing coverage would result in higher interference. In a mining field or in a farm, where traffic levels are lower but the area to cover is larger, to some extent capacity can be sacrificed to increase the reach of APs.

Reliability and redundancy. As an increasing percentage of enterprise data and voice traffic is transported over Wi-Fi networks, the requirements for reliability are bound to become more stringent. As users are increasingly working away from the office or do not have a fixed office location, they often do not have the option or a device to connect to the wireline network. Without wireless connectivity they are unable to do their work. In this context reliability becomes paramount, and some level redundancy is often required. At the AP level, redundancy can be achieved by deploying standby equipment to be activated when a failure occurs, by providing some coverage overlap, or by dynamically reconfiguring AP coverage in response to outages. Network management, traffic management and security mechanisms also need to be designed to provide the required reliability levels to ensure that they do not become bottlenecks.

Dynamic RF environment and mobility support. Employees are increasingly moving within the enterprise footprint and taking their mobile Wi-Fi devices with them. But the overall RF environment is also changing as goods, materials, furniture and other potentially obstructing objects move. Of course, this is nothing new, but as Wi-Fi networks move from meeting rooms and corporate headquarters to hospitals, warehouses and factories, environments with a changing RF profile are increasingly common — and challenging, as the initial RF survey becomes less informative. In addition, the distribution of demand changes more rapidly as employees have devices

that offer better support for mobility. When laptops were the only Wi-Fi devices in the enterprise, sitting areas were almost exclusively used for access. This is rapidly changing as employees increase their use of smartphones, tablets or other mobile devices designed to be used while conducting some task (e.g., visiting a patient) and as sensors and other devices that are attached to objects (i.e., testing instruments) or individuals (i.e., patients) that move are adopted. In addition to changing the traffic distribution within the single AP coverage area, these new devices also create a stronger case for supporting seamless handovers and session continuity as devices move and connect to new APs. The increased dynamic nature of the RF environment and traffic distribution has to be taken into account when assessing the provisioning requirements and when determining the network management approach and functionality needed.

Voice and video support. We are in the middle of a clear transition toward data traffic like voice and video that has higher latency, packet loss and jitter requirements. It is matched by increasingly high expectations from users that video and voice delivered through Wi-Fi matches in quality wired Internet and copper phone lines. While best-efforts data is likely to remain the core of Wi-Fi traffic in the enterprise, real-time traffic like voice and video is much more difficult to manage, especially when the traffic load is high. Enterprises that expect to have heavy voice and video traffic should plan ahead to deploy network architectures that are well suited for it. For instance, a network with good coverage but limited edge throughput may result in edge users' being unable to use voice and video services.

Concluding remarks: a bright future for Wi-Fi

Unlike many technologies that with maturity appear to exhaust the scope of innovation, Wi-Fi has managed to strike an effective balance between support for the existing networks and innovation to support the growing needs and expectations of the enterprise.

Backed by standards highly respected across the globe, a supportive and powerful ecosystem, and a steady increase in demand for wireless connectivity in the enterprise, Wi-Fi has established itself as the dominant wireless technology in the enterprise and has vastly expanded its role from an accessory access network that provided basic broadband connectivity to a few laptop users to a pervasive technology that allows an increasing range of smartphones, tablets, sensors, cameras and other fixed or mobile devices to connect to a fully integrated, wireless and wireline IT network.

As the role of wireless connectivity and, specifically, of Wi-Fi within the enterprise continues to expand, so are the demands placed on its performance, coverage and reliability. Innovation within the standards and the vendor ecosystem indicates that Wi-Fi is ready to take on the challenge of heavier traffic loads, increased impact of voice and video applications, and a more dynamic RF environment. The Wi-Fi of the future will still support legacy equipment, enabling enterprises to organically transition to new solutions and capability at their own pace while retaining their existing devices. At the same time, it will continue to enhance its air interface, network and traffic management, and it will improve the support for vertical-specific applications.

Wi-Fi evolution toward greater performance, reliability and scalability closely matches the rapid ongoing changes in the enterprise toward increased mobility of office-free employees, the adoption of cloud-based applications and the expansion of M2M communications. Moving forward, expect the ties of the enterprise to Wi-Fi to deepen, as wireless connectivity is slated to become the primary-access modality for voice, video and data.

About Monica Paolini

Monica Paolini is the founder and president of Senza Fili Consulting. She is an expert in wireless technologies and has helped clients worldwide to understand technology and customer requirements, evaluate business plan opportunities, market their services and products, and estimate the market size and revenue opportunity of new and established wireless technologies. She has frequently been invited to give presentations at conferences and has written several reports on wireless broadband technologies.

She holds a Ph.D. in cognitive science from the University of California, San Diego; an MBA from the University of Oxford; and a BA/MA in philosophy from the University of Bologna.

Contact Monica Paolini at: monica.paolini@senzafiliconsulting.com

About GigaOM Pro

GigaOM Pro gives you insider access to expert industry insights on emerging markets. Focused on delivering highly relevant and timely research to the people who need it most, our analysis, reports and original research come from the most respected voices in the industry. Whether you're beginning to learn about a new market or are an industry insider, GigaOM Pro addresses the need for relevant, illuminating insights into the industry's most dynamic markets.

Visit us at: http://pro.gigaom.com

Want more information?

Contact Monica Paolini, the author of this report,

or any of the other experts at GigaOM Pro.

Discuss this report online.

Suggest a research topic.