

I. Wherever, Whenever: The WiFi Promise

WiFi technology promises to cut the tethers binding users to the wall and allow free roaming in an expanded digital landscape. And that's a promise consumers find very attractive. Furthermore, according to Metcalfe's Law, as the number of users connected to the Internet—or any network—increases, so too does the power of the network. WiFi creates more users, more users create better networks, better networks attract more users, and so on. The dream of the Internet is open access to a vast amount of information wherever and whenever the need arises, and WiFi delivers that experience to a degree that wired systems simply cannot.

Despite growing consumer demand, the WiFi promise would remain the stuff of science fiction without the infrastructure to deliver it. And industry and regulators have given WiFi several significant benefits that are driving the current boom.



First, WiFi technology has a low cost of entry, which has made home users some of the earliest adopters of wireless networks. These users buy inexpensive access points for their homes and set up their own networks to create a broadband connection throughout the house. As these home users become accustomed to the convenience of WiFi, they begin to expect it in enterprise and other situations, as well.

Second, standardized WiFi protocols across the industry allow interoperability among devices and platforms. Anyone with a laptop NIC (network interface card) can access a wireless signal at work, at home, or on the road, regardless of the hardware at each end of the connection.

Third, WiFi operates in a special unlicensed band. This means that anyone can put up a WiFi wireless network, without having to be a carrier and without having to apply for an auction to buy spectrum.

However, this use of unlicensed band has some inherent risks as well. Regulators have adopted a hands-off approach to managing this free wireless spectrum. The Technological Advisory Council (TAC) is a federal advisory committee that provides recommendations to the United States Federal Communications Commission (FCC) concerning developments in the communications industry. Here's a quote from a December 2000 TAC Meeting Report: "We are about to have an unplanned real-time experiment on the consequences of uncoordinated spectral sharing . . . using incompatible etiquette rules." With regulators standing on the sidelines, it becomes incumbent on industry to identify and communicate the pitfalls and possibilities of unlicensed band usage as they occur.

II. Lessons Learned

The unlicensed spectrum experiment is ongoing, but some of the salient data is in and there are important lessons to be learned.

Lesson 1: Many Unlicensed Devices

The unlicensed spectrum is spurring the creation of new types of wireless devices and applications, from WiFi to Bluetooth, RFID, cordless phones, and other applications like wireless video game controllers, security cameras, and more. From a market perspective, the tremendous variety of wireless devices indicates the unlicensed experiment has been a success.

And the raw numbers of these devices in use is growing, too. About 250 million WiFi devices will be sold this year. Factor in anticipated sales of Bluetooth devices, cordless phones, and all the miscellaneous gadgets and devices on the market and the figure quickly reaches more than a billion unlicensed wireless devices.



Also consider the fact that a good percentage of cellular phones come with an internal Bluetooth radio for use with a wireless headset. So we have one unlicensed radio and one licensed radio in each cellular device. And a smaller but growing percentage of cellular handsets now have a WiFi radio, as well. Soon a cellular handset will feature two unlicensed radios and only one licensed radio. This provides an idea why the growth curve for unlicensed devices is much larger than that for cellular.

Lesson 2: Enterprise depends on WiFi

Most enterprises originally deployed WiFi networks on their premises to support casual and sporadic usage. However, whenever a WiFi network is deployed, users will put it to work in unanticipated ways. What begins as a convenience for a small number of staff quickly becomes a platform for more business-centric applications, including the overlaying of real-time, performance-sensitive services over the WiFi network, such as voice and video transmissions. In other words, users come to expect the same quality of service from both wired and wireless networks. And because users want equivalent performance, they expect their IT department to service both kinds of networks equally well. Cost savings may dictate that eventually the enterprise migrate entirely to a wireless networks. Thus, the secure, reliable functioning of the wireless network is no longer a convenience—it's mission critical.

Lesson 3: Wireless networks introduce new security threats

Wireless networks open the door to a whole new set of protocol threats and require a new class of wireless intrusion detection systems (WIDS). Some of these security issues, especially at the RF level, aren't often discussed.

For example, jammer attacks can bring a network down simply by spraying noise throughout the spectrum. WiFi and non-WiFi rogue devices also pose threats to network security. A user may set up a Bluetooth access point, for example an Anycom access point, and plug it into a network. This is a serious security threat because it's difficult to detect. There's also concern about back-door attacks. Many devices speak multiple wireless protocols. If a user has a laptop with an unsecured Bluetooth connection, there's the possibility of an unsecured data connection regardless of whether the laptop is plugged into the wired or WiFi network -- someone could attack the laptop device and bridge onto the network.

Such RF security issues are real, and as the number of mission critical functions migrating to WiFi increases, so too will the impacts of breached network security be magnified.

Lesson 4: Devices jam other devices

Almost every wireless device brought into a wireless environment presents an interference threat to your WiFi network. Cordless phones, cell phones with Bluetooth, wireless keyboards and mice, and even non-wireless devices like microwave ovens—all of them have potentially devastating effects on WiFi performance and security. Why does this happen?

WiFi is a “polite” protocol. It uses an algorithm called “listen before talk” or CSMA (Carrier Sense Multiple Access). As a result, when WiFi perceives a non-WiFi device broadcasting in the environment, it will hold off its own transmission until the other transmission is complete. In another case, WiFi might listen and hear quiet, then go ahead to start transmitting. At the same time, a device that doesn’t follow the same protocol as WiFi might start to transmit in the middle of the WiFi packet. The result is a collision, loss of the WiFi packet, and a need to retransmit. Because of listen-before-talk and collisions, other devices can have a negative impact on the performance users get from their WiFi network.

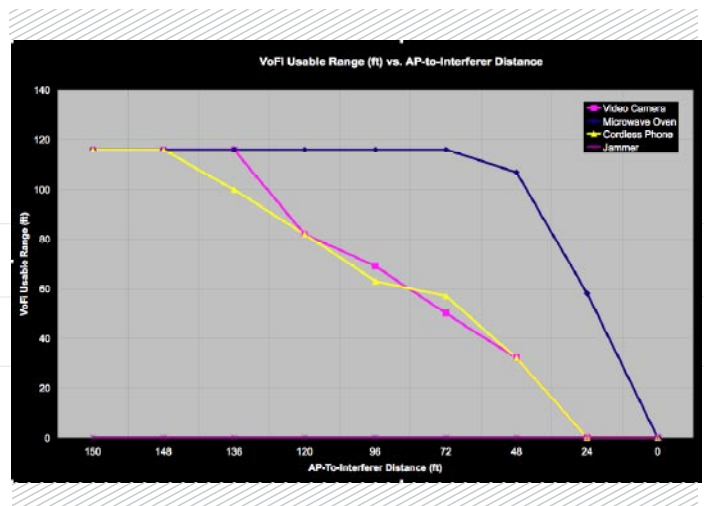
The chart below shows what can happen to WiFi data rates when the spectrum experiences interference from other devices. The vertical axis indicates how much data can get through the given network and connection. The horizontal axis indicates the distance of the interference devices—video camera, microwave oven, cordless phone and jammer—from the Access Point. At the outset, the connection carries 40 Mbps over 802.11g. However, when interference-producing devices are introduced at distances of up to 120 feet from the access point, throughput begins to drop off. At distances of 100 feet or less, this drop off can be dramatic, and as the distance closes, throughput may cease entirely.

In the case of voice over VoWiFi (VoWiFi), the problems presented by interference are especially critical. Where data transmissions may experience decreased throughput due to interference, VoWiFi is typically set not to retransmit packets, so collisions cause lost packets and a reduction in voice quality. In the chart at right the user is 120 feet from the access point, at the outset of a call and experiences acceptable levels of voice quality. However, when a source of interference is introduced to the environment, the range at which the phone can be used starts to decrease. In most cases, An interferer at less than 100 feet from the access point cuts the range at which the VoWiFi phone can be used by half.

Lesson 5: Enterprise RF management is mission-critical

Clearly, as the WiFi world expands, the enterprise faces significant challenges to keeping mission critical wireless services up and running. And the job of meeting those challenges increasingly falls to in-house information technology teams.

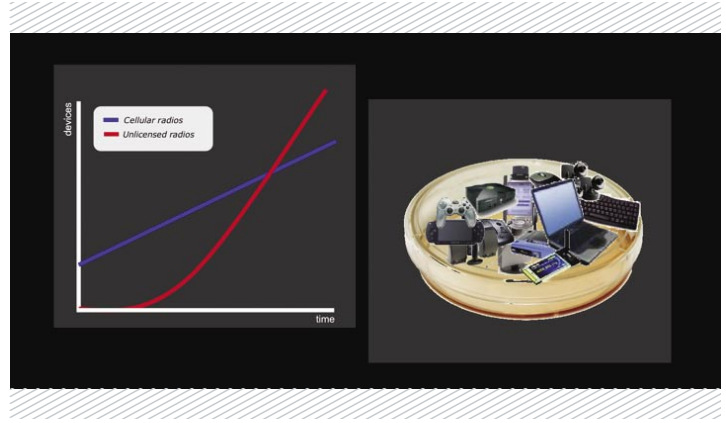
Unfortunately, wireless network management is new territory for many information technology personnel. Before the unlicensed band experiment, RF management was the domain of carriers and some RF specialists. IT managers thus had little incentive to develop RF management skills and instead focused their skill sets on more traditional networking infrastructures. Furthermore, the expense of many spectrum tools provided a further disincentive to enterprise RF management. In many cases, RF consultants fill this gap, as they provide the necessary expertise and tools. However, this level of service comes at a price—a price that quickly multiplies when applied on a per consultancy basis. Because the benefits of wireless networks include their flexibility in scope and context, adjustments do need to be made regularly and in a timely fashion. The increased time-to-repair and cost of service presented by consultant-based RF management both impact the bottom line. As the unlicensed band experiment progresses, IT needs to become self-sufficient in managing enterprise RF issues.



III. The Way Forward

What do these lessons mean? Is WiFi in trouble? Will the unlicensed band experiment fall victim to its own success? The phrase “tragedy of the commons” refers to the depletion of shared, finite resources through overcrowding and overuse. If no steps were being taken to expand and control our wireless commons, a tragedy might well ensue.

However, recent developments in a number of areas are showing that the challenges posed by RF management are by no means insurmountable. Innovation and responsiveness to user demands are the foundations of the wireless experience, and these qualities will continue to sustain and expand that experience as the industry moves forward. In fact, there are currently three trends that point to an increasingly robust wireless future for home users and enterprise alike.



Trend 1: Enhanced capabilities

The next generation of WiFi technologies are evolving and maturing, and as they come to market, users may at last have wireless options that meet or exceed the speed and reliability of traditional wired networks.

One of the most promising ways forward is in the development of next-generation WiFi standards. Currently, there is great excitement over the development of a new 802.11n wireless standard. Through the use of multiple input, multiple output (MIMO) technology, which uses multiple antenna paths to achieve higher throughput and expanded range, 802.11n has the ability to provide significantly greater capacity and reliability than previous WiFi standards. This additional capacity will remove some of the pressures of bottlenecks and interference caused by increasing WiFi traffic and deliver an enhanced wireless experience.

One of the ways 802.11n achieves increased performance is through “beam forming,” a signal processing technique that directs transmissions between two communicating devices. One of the benefits of beam forming is its ability to overcome, to some degree, interference in the environment; the interference has to be closer to the access point or client before it becomes a problem. In this way 802.11n provides improved resilience to interference.

Along with the 802.11n standard, government regulators are increasing the amount of unlicensed spectrum. This increased spectrum will increase capacity and provide fewer opportunities for interference among competing devices.

Trend 2: Better spectrum tools

As WiFi infrastructures evolve, so too do spectrum tools for RF management. Industry is responding to the problems posed by increased WiFi usage with better spectrum tools to help IT managers debug tricky RF problems, without having to be RF gurus.

For example, next-generation spectrum analytics software performs troubleshooting at the physical level. Managers can use the software to take the interference temperature of their wireless environments on a regular basis, helping them to determine any changes or trends. The software also promotes ease of use for IT managers and quick resolution of individual incidents by locating the source of an interference problem in the building and naming the trouble device. This is especially important as more and more devices are added to the wireless environment.

Trend 3: Spectrum integration

As better spectrum tools become available, WiFi network administrators will increasingly demand fuller integration of these tools with their infrastructure equipment. Already, the equipment is getting smarter by providing a wider, deeper range of RF management tools, right out of the box. As this process accelerates, WiFi users are bound to experience a number of real benefits.

First, the integration of monitoring tools as part of WiFi infrastructure provides a full-time, real-time line of defense against interference, dropouts, and security attacks. It's on the job, scanning for problems twenty-four hours a day, seven days a week.

Second, when 24x7 monitoring is coupled with intelligent software, systems will have the ability to automatically mitigate RF issues the moment they occur. The system can change channels, alter network parameters, shift users to a different access point, or take other measures to address the problem, all without the intervention of IT staff.

Third, the data and resources offered by these tools allow network administrators to act on their system needs more intelligently. If one understands the nature of the interference that one is dealing with, then the response to that interference can be more intelligent. If voice traffic is a concern, one can schedule it around the interference in such a way that the voice quality stays better in the face of the interference.

Finally, taken together, the integration of automated monitoring and mitigation tools into WiFi equipment will provide enhanced quality of service by removing the human element from the situation as much as possible. In other words, as spectrum integration accelerates it will make possible a new level of WiFi security, reliability, and management efficiency.

In a few short years, the unlicensed band experiment has changed the face of telecommunications. Consumer demand for WiFi and other wireless technologies is growing and will soon surpass cellular as the wireless option of choice. New applications and capabilities are pushing the technology into new areas and driving further innovation. Of course, such rapid expansion does not come without growing pains. There is much work to be done if industry is to develop effective technical solutions to the problems of shared, unlicensed spectrum, and home users and enterprise alike will have to grow smarter about managing their share of the unlicensed spectrum. Nevertheless, it's a wireless world, and will continue to be so for the foreseeable future.

About the Author

Neil Diener has 20 years of experience in the architecture and design of reliable communication systems and embedded software. At Cognio, he is responsible for leading the company's technology and product strategy. Prior to becoming CTO, Neil was Director of Software Technology. Before joining Cognio, he held a series of director level positions at companies including Telogy/Motorola, Sun Microsystems, Xerox, and Ask Jeeves. Neil holds a BS in Electrical Engineering from MIT and an MS in Computer Engineering from USC.



About COGNIO

Founded in 2001, Cognio is the leading innovator of cognitive spectrum-analysis products. Cognio's technology monitors wireless networks and solves wireless network problems. Cognio's products are applicable to a wide range of bands, including 802.11. Cognio is headquartered in the greater Washington, DC area, and is privately held with venture investments from Avansis Ventures, ABS Ventures and North Bridge Venture Partners.

Additional information is available on the Web at <http://www.cognio.com>

