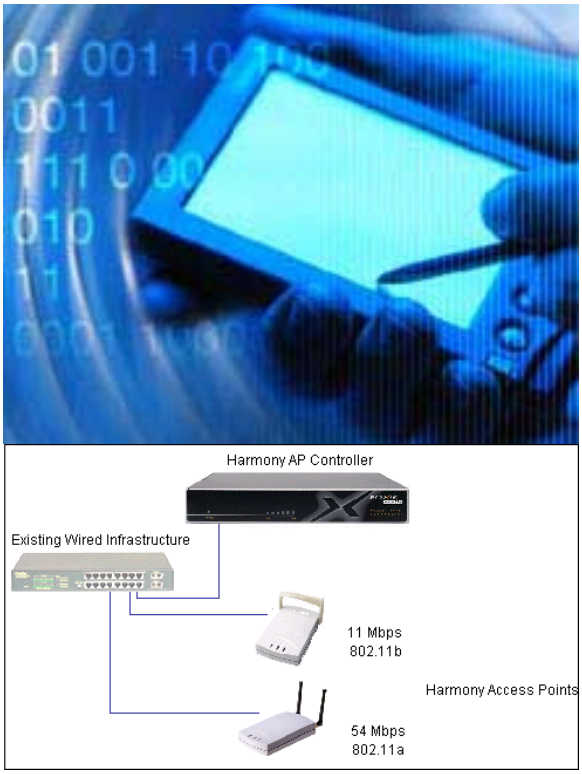
Emerging Wireless Technologies

High-Speed Wireless LANs and Internet Protocols of Tomorrow

Foreword: The Public Safety Wireless Network (PSWN) Program is conducting an ongoing assessment of advancements in the wireless communications industry. The scope of this assessment is to identify emerging wireless services and technologies for potential public safety use in the near future and beyond. This document is the third in a series of studies on emerging wireless technologies. This particular study primarily concentrates on tomorrow's wireless local area network (LAN) standards (802.11a) and Internet protocols (IPv6).



This document introduces two specific elements of wireless data networks, to be deployed in the near future, that will have great impact on all wireless data system users: the Institute of Electrical and Electronics Engineers (IEEE) 802.11a standard and Internet Protocol version 6 (IPv6). Both elements are believed to be the springboards for supporting the next great wireless LAN and Internet solutions.

IEEE introduced a set of standards addressing wireless LAN technology as the 802.11 suite of standards. This suite has thus far been broken into two segments, which can best be differentiated by the frequency band in which their respective technologies are (or will be) implemented. The 802.11b segment (the first segment widely developed) covers the 2.4 gigahertz (GHz) band, and the 802.11a segment (discussed in this document) covers the 5 GHz band. With the acceptance of the IEEE 802.11b standard, a number of products and vendors entered the market with wireless access point products as the enterprise. Widespread adoption of the IEEE 802.11b standard resulted in wireless LAN systems with performance deemed acceptable for today's typical office applications, with adequate levels of reliability. As with most communications technologies, manufacturers are looking ahead to making improvements. Several wireless LAN suppliers are planning to introduce new products within the next 12 months based on a new standard, IEEE 802.11a.

In addition, it is anticipated that an emerging Internet protocol will impact the Internet and its users tremendously. Currently, the Transmission Control Protocol/Internet Protocol (TCP/IP) suite is the fundamental basis of the Internet. All Internet data communications among companies and individuals today are based on TCP/IP, including Web browsers, e-mail, file transfers, and remote logins.

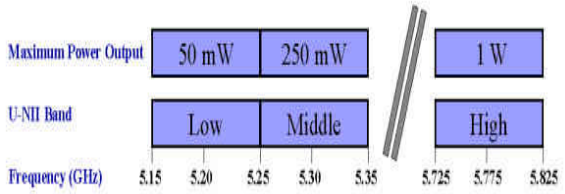
In the coming years, the Internet will face an important transition, enabling it to grow beyond its current limitations. Some of these limitations include a shrinking number of available Internet Protocol (IP) addresses and a lack of static IP addresses (i.e., IP addresses that do not change with each login of the same user). A transition will be made to a newer, more reliable version of IP, namely IPv6, which will change the IP portion of the TCP/IP protocol

suite. The changes IPv6 will introduce are discussed in depth later in this document.

IEEE 802.11a at a Glance

The IEEE has developed 802.11a, a new specification that supports the next generation of wireless LANs. This new wireless standard offers many advantages over the existing standard. Advantages gained with 802.11a include greater scalability, better interference immunity, and significantly higher speed—up to 54 megabits per second (Mbps) and beyond. In comparison, IEEE 802.11b, the current wireless LAN standard, delivers only 11 Mbps. All the advantages of 802.11a will allow for both higher bandwidth applications and more users. In addition to providing a signaling rate of 54 Mbps, the new 802.11a standard promises throughput capabilities in excess of 20 Mbps. Such performance can support, for example, a wireless digital video disk (DVD) quality streaming video sessions with an additional 10 Mbps remaining for file transfers, database access, and other applications. Current applications for 802.11b are mostly file (data) transfers—high-quality streaming video is not applicable at this speed.

802.11a uses 300 megahertz (MHz) of bandwidth in the 5 GHz Unlicensed National Information Infrastructure (U-NII) bands. Although the lower 200 MHz is physically contiguous, the Federal Communications Commission has divided the total 300 MHz into three distinct 100 MHz domains, each with a different legal maximum power output. The low band operates from 5.15–5.25 GHz and has a maximum transmit power output of 50-milliwatts (mW). The middle band is located from 5.25–5.35 GHz, with a maximum of 250-mW. The high band uses 5.725–5.825 GHz, with a maximum of 1 Watt.



802.11a Physical Layer

Because of their higher power output, devices transmitting in the high band will likely be used for building-to-building products. The low and medium bands are more suited to in-building wireless products. One requirement specific to the low band is that all devices must use integrated antennas (i.e., antennas that are internal to the device, with no external protrusion).

Currently, the frequency range for most enterprise-class unlicensed transmission, including 802.11b, is the 2.4 GHz Industrial, Scientific, and Medical (ISM) band. This band is crowded and only offers 83 MHz of spectrum for all wireless traffic. The ISM band is congested with transmissions from many different devices, including cordless phones, building-to-building transmissions, and microwave ovens. This congestion makes the ISM band much more susceptible to interference. Comparatively, the 300 MHz offered in the U-NII band represents a nearly four-fold increase in spectrum, which is very impressive considering the limited wireless traffic currently operating in this band.

802.11a Modulation Scheme

802.11a uses orthogonal frequency division multiplexing (OFDM), a new encoding scheme that offers benefits over spread spectrum in channel availability and data rate. Among these benefits is the ability to carry more data traffic over the same amount of physical spectrum. The high data rate is achieved by combining many lower speed sub-carriers to create one high-speed channel. 802.11a uses OFDM to

define a total of eight, non-overlapping, 20 MHz channels across the two lower bands; each of these channels is divided into 52 sub-carriers, each approximately 300 kilohertz (kHz) wide.

As described above, 802.11a uses channels that are 20 MHz wide, with 52 sub-carriers contained within each channel. The sub-carriers are transmitted in parallel, meaning they are sent and received simultaneously. The receiving device processes these individual signals, each one representing a fraction of the total data that, together, makes up the actual signal. With this number of sub-carriers comprising each channel, a tremendous amount of information can be transmitted at once.

With so much information per transmission, it becomes extremely important to guard against data loss. Forward error correction (FEC) was added to the 802.11a specification for this purpose. (FEC does not exist in 802.11b.) The FEC process consists of imbedding redundant information with the primary information. Then, if part of the primary information is lost, the receiving device can recover all or part of the lost data through sophisticated algorithms. In this way, even if part of the signal is lost, the information can be recovered so the data is received as intended, eliminating the need to retransmit. Because of its high speed, 802.11a can accommodate this overhead with negligible impact on performance.

Another threat to the integrity of the transmission is multipath reflection, also called delay spread. When a radio signal leaves the sending antenna, it radiates outward, spreading as it travels. If the signal reflects off a flat surface, the original signal and the reflected signal may reach the receiving antenna simultaneously. Depending on how the signals overlap, they can either augment or interfere with each other. A baseband processor, or equalizer, unravels the divergent signals. However, if the delay is long enough, the delayed signal spreads into the next transmission. OFDM specifies a slower symbol rate to reduce the chances that a signal will encroach on the following signal and thereby minimize multipath interference.

MAC Layer

802.11a uses the same media access control (MAC) layer technology as 802.11b—carrier sense multiple access with collision avoidance (CSMA-CA). CSMA-CA is a basic protocol used to prevent signals from colliding and canceling each other out. It works by requesting authorization to transmit for a specific amount of time prior to sending information. The sending device broadcasts a request-to-send (RTS) frame, with information on the length of the signal. If the receiving device permits it at that moment, the receiving device then broadcasts a clear-to-send (CTS) frame. Once the CTS goes out, the sending machine transmits its information. Any other sending devices in the area "hearing" the CTS detect that another device will be transmitting and allow that signal to go out unimpeded.

Comparisons Between 802.11a and 802.11b

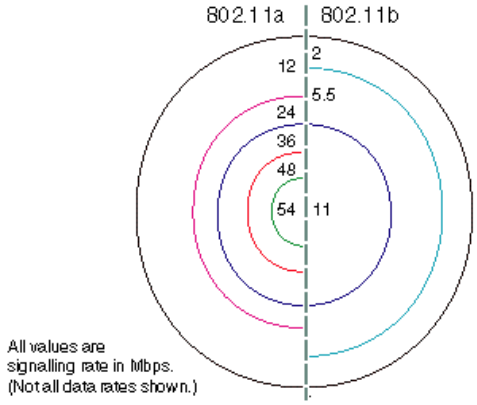
Today's 802.11b wireless LAN systems provide mobile access to typical enterprise applications, such as e-mail, Web browsing, and Enterprise Resource Planning (ERP) systems, at speeds roughly equivalent to a 10-Mbps desktop, wired Ethernet. The 802.11b standard will remain viable for such applications for the foreseeable future.

However, the mobility aspect of wireless data communications is driving the development of unique applications, such as remote observation, untethered access to maintenance resources, and distributed training. Video is key to many of these emerging applications.

The throughput required for real-time wireless video distribution could exceed 10 Mbps, which demands an over-the-air signaling rate of more than 20 Mbps. (User throughput efficiency of wireless systems is approximately 50 percent of the radio signaling rate.) Today's 11-Mbps (signaling rate) 802.11b products cannot deliver the throughput required for high-quality video-based applications. In addition, the ever-increasing need for any network, wired or wireless, to support larger, faster file transfers, and higher user densities, demands the highest throughput available. As stated earlier, the new 802.11a standard promises transmission speeds of up to 54 Mbps, while delivering user throughput in excess of 20 Mbps. Such performance will support DVD-quality streaming video sessions with additional speed and bandwidth to support other applications.

The range of a typical 2.4 GHz 802.11b access point in an indoor office environment is 150 feet at best, at the highest data rate of 11 Mbps. Systems based on the 5 GHz 802.11a standard will likely achieve a range of approximately 50 feet in the same environment at the highest 802.11a data rate of 54 Mbps (as shown in the figure below). This means that covering the same area with the highest speed available from each technology will require more 802.11a access points. Both technologies will support lower data rates as distance from the access point increases, and the relative 802.11a data rate will be consistently much higher than 802.11b at all ranges. For full coverage at the highest speed available, however, a higher quantity of 802.11a access points will be required for the same area. Overall, 802.11a offers many benefits over current (802.11b) wireless LAN technologies, including:

- Increased wireless networking speeds, up to 54 Mbps
- Greater capacity for large-scale deployments
- Less interference from other wireless devices.



802.11a is always faster than 802.11b at any range

The plot above shows that there are two access points located in the center, 820.11a on the left and 802.11b on the right. The plot demonstrates the differences between 802.11a and 802.11b with respect to data rate versus distance. Each circle represents a defined distance away from the access point, and the numbers represent the data rate in Mbps. The numbers 54 and 11 represent the maximum data rate that one can achieve when positioned closely to each access point.

As shown above (and according to Proxim, a wireless LAN vendor who tested the two technologies) when the distance from the access point increases, there is a loss in data rate. However, when comparing 802.11a and 802.11b, 802.11a supported a larger coverage area because it supports a higher data rate, even when considering the increased distance.

Compatibility with 802.11b

While 802.11a and 802.11b share the same MAC layer technology, there are significant differences at the physical layer. 802.11b, using the ISM band, transmits in the 2.4 GHz range, while 802.11a, using the U-NII band, transmits in the 5 GHz range. Because their signals travel in different frequency bands, one significant benefit is

that they will not interfere with each other. A related consequence, however, is that the two technologies are not compatible. Consequently, there are various strategies for migrating from 802.11b to 802.11a, or even using both on the same network concurrently.

Migration Issues for 802.11b to 802.11a

Wireless LAN manufacturers that have announced plans for 802.11a products have taken significantly different approaches in addressing the migration issue. The first approach uses an 802.11a version of a traditional access point, in which each self-contained unit includes the radio, bridging circuitry, processors and memory required to deliver and manage all wireless-to-wired networking functionality.

In this case, 802.11a access points will likely be priced equivalent to or greater than traditional 802.11b access points. Incorporating traditional-style 802.11a access points into an existing 802.11b installation will more than double the cost of the complete wireless infrastructure, particularly because more 802.11a access points will be required to cover the same area at the highest data rate.

A second approach, which was also attempted in the migration from 2-Mbps 802.11 radios to 11-Mbps 802.11b radios, is based on access points with a slotted architecture. These access points have a slot (or sometimes two slots) into which the radio, in the form of a standard PC card, is inserted. This approach would seem to offer advantages for upgrading from one radio technology to the next by simply unplugging the 802.11b PC card and replacing it with a new 802.11a PC card. With the two-slot versions of these access points, the implication is that one can install the two radio types, 802.11b and 802.11a, side-by-side within the same unit.

What is IPv6?

With high-speed wireless LAN technology development moving at a very fast pace, 802.11a is just one of the protocols that will emerge within the next few years. A new, critically needed upgrade to today's Internet is Internet Protocol version 6 (IPv6). IPv6 is the next-generation Internet protocol, designed as a successor to the currently used IP version 4 (IPv4).

The Internet Engineering Task Force (IETF) assigned IP version 5 (Ipv5) to identify an experimental non-IP real-time stream protocol called Scheduled Transfer (ST). Although ST was never widely used, the decision was made not to reassign the number 5. This is the reason that Ipv6 is replacing Ipv4. It is generally accepted that further iterations of IP will use even numbered versions from this point forward.

IPv4 currently serves the Internet and many enterprise networks. As with all legacy technologies, there are certain limits to its capabilities. To overcome the limitations of IPv4, the industry recognized the need to move from IPv4 to IPv6. IPv6 uses an address scheme based on a unique Internet address of 128 bits, as opposed to the 32 bits of IPv4. IPv6 was designed to enable a high-performance, scalable Internet address space. This goal was achieved by overcoming many of the weaknesses of IPv4 protocols and by adding several new features.

Why IPv6 Now?

The Internet is growing at an incredible rate. This growth, with its anticipated future requirement for more IP addresses, is a major factor driving the need for a new IP version. With the current IP, the number of possible unique Internet addresses is in the range of 4 billion. However, this is a theoretical limit, actually

constrained by several factors to a number on the order of "only" a few hundred million addresses. Currently, with more than 100 million computers connected to the Internet and an estimated annual connection growth rate of 65 percent, it is projected that unique IPv4 addresses will be completely depleted by 2004.

There are also general limitations to IPv4. Developed in the early 1980s, the IPv4 protocol was designed for the applications and environment envisioned at that time. The Internet was originally set up as a research network, for use by very few users, for transporting mainly ASCII files. Now, however, it has transitioned to an essential commercial and business tool, running mission-critical applications, transporting real-time multimedia files. Instead of the few users originally envisioned for the Internet, millions of people access the Internet—and those numbers are growing on a daily basis.

As the Internet grew, new requirements and applications were created, and ingenious solutions were developed to make IPv4 work. These ingenious solutions were merely patches to force IPv4 to perform as needed. However, as the Internet continues to grow at a surprising rate, additional, more demanding applications are being deployed. Although the patch approach to modifying IPv4 was ingenious, it now appears less appropriate and might impede further growth of the Internet. Additional limitations of IPv4 include complex host and router configurations, non-hierarchical addressing, difficulty in re-numbering addresses, large routing tables, non-trivial implementations in providing quality of service (QoS), and mobility to name a few. Quality of service is important because it allows network administrators to use their existing resources efficiently, guaranteeing that critical applications receive high-quality service without having to expand very quickly.

The emerging IPv6 Internet will have several advantages over the current IPv4 Internet. A nearly infinite number of IP addresses will be available. This will enable constant connection of millions of data phones, handheld personal digital assistant (PDA) type devices, Web pads, and home appliances to the Internet—all with the possibility of having unique IP addresses. With IPv6 implemented, globally unique and permanent IP addresses will make peer-to-peer computing and multicast applications much easier to implement.

Deployment of IPv6 is not going to happen overnight..

Migration from IPv4 to IPv6

Deployment of IPv6 is not going to happen over night, and it must follow a defined migration strategy. An important note is that the operator will not have to change or upgrade any of the existing network elements, and it is fairly certain that IPv6 will coexist with IPv4 for a long time. Both mobile and subscriber units, configured with IPv4, will continue to be used and continue to grow in number before IPv6 implementation gains enough momentum to begin replacing IPv4. Initially, IPv6 network elements will be deployed in parallel with the IPv4 networks to support new mobile units. Thus, coexistence between these two elements will ensure smooth interoperability.

Impact of IPv6 on Wireless

Some researchers of IPv6, say that wireless communications will be an essential application. Major vendors, such as Sun, Microsoft, and IBM, expect the proliferation of Internet-enabled mobile telephones and handheld computers to propel IPv6 into the core of the Internet. As a result, the mobile and wireless

communications community heavily supports IPv6, largely because it anticipates needing a billion IP addresses for mobile devices within the next decade. Networks comprised of these types of devices will likely become IPv6 islands, with gateways to the Internet, as the next-generation wireless services are rolled out.

802.11a and IPv6 – Impacts on Public Safety

With both of these new standards, technology development will press forward with new and exciting applications. Many of these applications, while mostly targeted toward the commercial and enterprise markets, will have considerable impact on public safety operations.

In fact, many of the applications of both 802.11a and IPv6 that are in development can be directly applied to public safety. One such application is mobile computing. Although the public safety community already has mobile computing in selected vehicles, these new standards will allow for mobile computing to handheld devices. This will enable officers to access databases from outside their vehicles to obtain crucial information such as criminal records, wants and warrants, etc.

Among the limitations that the public safety community must be aware of regarding mobile computing are security and processor capability. Many of the databases that the public safety community accesses contain confidential information that must be protected from unauthorized viewing and use. Many application developers are working to improve wireless security so that when these new technologies become available, the public safety community can use them knowing that the information it accesses will not be intercepted by unauthorized personnel.

Similarly, as mobile computing becomes ubiquitous, devices will require more processing power and better power consumption capabilities. These issues will affect all entities that use these new technologies. However, because of the criticality of the operational missions of the public safety community, particular attention must be paid to the development and use of reliable hardware.

In Summary

802.11a represents the next generation of enterprise-class wireless LAN technology, with many advantages over current options. At speeds of 54 Mbps and greater, it is faster than any other unlicensed solution. As opposed to 802.11b, 802.11a provides a higher speed throughout the entire coverage area, but some vendors claim that both technologies have similar range. The 5 GHz band in which it operates is not crowded, so there is less congestion to cause interference or signal contention.

The eight non-overlapping channels of 802.11a allow for a highly scalable and flexible installation. Thus, 802.11a is the most reliable and efficient medium for accommodating high-bandwidth applications for numerous users. In addition, 802.11a's speed, scalability, and interference immunity also make it the highest performing solution.

Likewise, IPv6 is a new technology that will replace an existing legacy technology. Currently, IPv4 serves the Internet and many enterprise networks. The limitations of IPv4 have been identified, and a need for migration to an improved IP is currently being addressed. IPv6 promises to overcome all the current limitations of IPv4 and thereby satisfy many of the growing needs of technology and a greatly expanded Internet.

Both 802.11a and IPv6 will enhance wireless communications immensely. As applications are developed, the commercial, enterprise, and public safety communities will benefit greatly. The possibilities are

endless—limited only by the imaginations of the developers and end users.

Postscript: The purpose of this article is to further educate the reader regarding advancements in wireless LAN and wireless Internet standards and their impacts to public safety. In upcoming articles, other developments in emerging wireless technologies (e.g., ultra-wideband, wireless security) will be presented.

References:

http://www.atheros.com/products/5_up.html
http://www.cnn.com/2001/TECH/internet/07/12/wireless.government.idg/index.html
http://www.nokia.com/ipv6/faq.html
http://www.nortelnetworks.com/corporate/technology/ipv6/faqs.html
http://www.nwfusion.com/news/2001/0406hslans.html
http://www.nwfusion.com/reviews/2000/0925rev.html
http://www.planetanalog.com/story/OEG20001002s005
http://www.proxim.com
http://www.proxim.com/products/harmony/whitepapers/802.11a.html