Guide to IEEE 802.11 Wireless LAN Standards

by Larry Mittag
CTO/Chief Technologist
Zaxis Corporation
ESC-305

Introduction

The IEEE standards sometimes seem like a force of nature. They define how things are to work in meticulous detail that only an engineer could love, but their force is such that they are regularly featured in the marketing materials of a number of complex devices like the Good Housekeeping Seal of Approval.

This has certainly been true in terms of wireless LANs. The IEEE 802.11b standard has achieved a level of support and customer acceptance that is truly the envy of other standards in that space such as HomeRF. Customers have learned that things from different manufacturers that are compatible with this standard really do in fact interoperate, and more to the point they operate well.

But beneath the surface there are problems brewing. Security has already been identified as a concern with 802.11b, and there are other nagging issues as well. Can it handle multimedia? If it does, will it guarantee Quality of Service (QoS)? Is 802.11a really the next generation, and if it is why does the standard appear to move backwards (from ‘ b’ to ‘a’)?

This paper will explore The IEEE standards that relate to wireless communication and provide a glimpse at how these standards are created. We will also look at what is in store from IEEE in the future regarding a number of types of wireless computing.

What is the IEEE?

The IEEE in human (non-acronym) speak is the Institute of Electrical and Electronics Engineers. This trade organization currently has over 350,000 individual members in 150 countries around the world. Their mission is to advance the cause of engineering in any way they can, including lobbying on behalf of the membership on issues in which there are technical ramifications and publishing a variety of materials containing technical content. Much of this publication is in the form of magazines and books, but they also define and publish a set of standards that define how a number of systems and industry best practices should be done. One subset of these standards is computer networking under the 802 standards, and a further subset of this defines various

flavors of wireless communication as it pertains to networking. The best known of these are the 802.11 standards regarding wireless LANs, but there are also wireless networking standards regarding Personal Area Networks (PANs) and fixed location Wide Area Networks (WANs).

The primary reason that IEEE publishes these standards is to promote interoperability. They act as a neutral third party that knows enough about the technology to create a standard that is reliable and capable of being the basis for the creation of products that are deployable by customers. The major advantage is that if products from multiple vendors adhere to an IEEE standard then they will interoperate among themselves. This promotes the growth of technology in general and acts as a rising tide lifting all ships.

It should be noted that there are costs involved in the creation and publication of these standards. The IEEE charges for copies of the standards to help them recoup those costs, which works against their wide dissemination. This has been a sticking point in the past, so they have set up a program where corporate sponsorships help them cover the cost so that they can distribute free electronic copies of any of the 802 standards after it has been published for six months. The assumption is that the OEMs that will make money from products based on the standards have to pay to get them as soon as possible, while students and others on limited budgets can still get access to the documents after they have been published for a while.

The Major Wireless Groups

As mentioned earlier, there are actually three subgroups under the 802 standards that pertain to wireless data networking. This was done for the obvious reason that there are different concerns in wireless communication between a small battery-powered device that wants to communicate within a room and large fixed installations that want to send data across a metropolitan area.

In general the standards are created and numbered as someone comes up with the idea. Most of the time this is a fairly harmless identification scheme, but as we will see there are ramifications at least in terms of 802.11b/802.11a.

The 802.11 Hierarchy

Wireless LANs are in some ways the easiest type of wireless data to do. There are no requirements to send data over miles of countryside, and there are also no tremendously strong restrictions as far as the battery power of the mobile devices. This is probably why this was the first IEEE committee to get started. That has enabled this market segment to also become the first of the three that has really taken off as a result.

One confusing aspect of this group is that the first standard was defined at the top of the hierarchy. Again, that is one of those issues that should affect only a handful of people that should know enough to not be bothered by it, but the public dissemination of IEEE ‘stamps of approval’ on products has created some confusion.

802.11 – The Root Standard

The 802.11 standard was the first attempt to define how wireless data from a network should be sent, and it shows the scars from being in that position. The standard defines operation and interfaces at the MAC (Media Access Control) and PHY (Physical interface) levels in a TCP/IP network. There is extensive analysis in the standard on the nuts and bolts of communicating with mobile systems. Even with that, the definition of mobility is somewhat limited compared to how we are beginning to define that term today. The assumption was that mobile users would stay pretty much in one place, although that one place might be anywhere within the covered space.

The biggest area of uncertainty in the 802.11 standard is in the PHY layer interfaces. There are three of them defined, and the three do not interoperate. One of them is based on infrared communications, but that one never really did generate much interest. The other two are both RF spread-spectrum interfaces, but one utilizes Frequency-Hopping Spread Spectrum (FHSS) and the other used Direct Sequence Spread Spectrum (DSSS).

From an engineering point of view this was not a major problem. Engineers debated heavily the relative merits of the two. But when it came down to creating products based on this standard there was certainly no guarantee that a FHSS product would interface with a DSSS product. Attempts to define the differences in the product packaging frightened customers away in droves.

This standard was published in 1999 and is freely available from www.ieee.org to anyone willing to register their interest.

802.11b – The Current Champ

The 802.11b committee was not the first subgroup of 802.11 to get started, but so far they are certainly the ones that have become the most famous. This group got a number of things right, including a speed that was fast enough to do useful things (11 Mbps), agreement on a single PHY layer (DSSS), and a catchier name for the standard (WiFi).

This combination, along with an organization that was tasked to ensure interoperability (WECA, the Wireless Ethernet Compatibility Alliance, www.wi-fi.org) combined to allow the interest in wireless computing to really take off. A large percentage of companies worldwide have begun experimenting with wireless additions to their inhouse LANs.

But this committee didn't get everything right. In particular, there are weaknesses in the security algorithms that are specified in the 802.11b standard. This is the primary reason that companies are experimenting rather than deploying on a wide scale.

This standard is in many ways a direct descendent of the original 802.11 specification. In fact, it is described as a speed enhancement to 802.11 networks, a "high

data rate" version of 802.11. The good news is that they also took the opportunity to fix other problems in the specification.

The 802.11b standard was published in late 1999 and is available currently for free download.

802.11g – The Heir Apparent

Shortly after the 802.11b standard was published a group got together and decided that the speed of 802.11b could be increased even more. The original specifications that came from Texas Instruments described improvements in the coding algorithms that would double the speed to 22 Mbps in a way that could be made downwardly compatible with 802.11b. This generated enough interest that the 802.11g committee was formed and began working.

Unfortunately, this group fell prey to internal squabbling. The TI technology was challenged by technology from Intersil. Neither technology was able to gain majority approval among the voting membership, so this standard struggled for a long time. It has only been recently (late 2001) that enough of a consensus could be reached to allow the group to define technical specifications and move onward to create a formal specification.

As tends to happen, life went on while all this was going on. As a result, the next full generation of wireless networks is ready and being released to market before this one has even made it out of the starting gate. This has forced the 802.11g group to increase their target to 54 Mbps to match the throughput of 802.11a.

The 802.11g standard has come on strong over the last year or so. It still is not as ubiquitous as 802.11b, but most new equipment installations (save the lowest end hardware) include this option.

802.11a – The Young Upstart

The plan was that 802.11g would be the midlife kicker that would enable wireless networking in the 2.4 GHz spectrum to maintain improvements until a relatively blue sky technology could be brought into place. The change in spectrum meant that there would be little point in attempting to maintain backward compatibility, so this group worked relatively independently. In fact, this specification was ratified at the same time that the 802.11b standard became official, September of 1999.

The higher frequencies that 802.11a required were expected to be quite challenging to chip vendors, so the expectation was that 802.11a networking would be quite expensive when it was released. Likewise, the OFDM (Orthogonal Frequency Division Multiplexing) coding scheme was expected to take some time to work out. As it turned out, all of this common sense was simply wrong.

A small company named Atheros pretty much made hash of all of these expectations. They released a chipset in late 2001 that was created out of CMOS, a very familiar (and therefore cheap to produce) technology. It is possible that there will be interoperability problems someday, but that is irrelevant at the moment because they are the only ones out there. This chip has been built into products from a number of vendors, including Intel, Proxim, IBM, and others.

This is where things are getting confusing for customers. They were just getting used to 802.11b/WiFi when suddenly there is the New and Improved 802.11a. The fact that this group got their paperwork in earlier is confusing both vendors and customers. WECA is attempting to ease the confusion by dubbing this WiFi5, highlighting the fact that it works in the 5 GHz space.

We will discuss the ramifications of this in more detail in a later section. The 802.11a standard was published in Sept. 1999 and is freely available.

802.11c – Access Point Bridging

Not all of the IEEE groups create separate standards. For example, there was a need perceived to use 802.11 access points to bridge across networks within relatively short distances from each other. For example, this could be used where there was a solid wall dividing a wired network.

The 802.11c working group defined the protocols and procedures necessary to do this. The results were a modification to the 802.1d standard rather than as a separate document.

802.11d – Internationalization

One of the bothersome details about wireless communications is that the use of spectrum differs significantly from one country to another. Even when spectrum is available there may be issues as to the details of the allowed use of that spectrum.

That is what the 802.11d working group is all about. Specifically, they are working on issues and procedures to allow 802.11b to be used legally in specific parts of Europe. This standard was published on 25 September 2001.

802.11e – QoS Extensions

The 802.11 standards are very much out of the data networking world. As a result, they are not well adapted to the requirements for streaming audio or video via a preallocated dependable portion of the bandwidth.

The 802.11e group is defining a series of extensions to 802.11 networking to allow for QoS operation. These will be published in the form of amendments to the pertinent documents to allow additional modes of operation.

The 802.11e group has approved this standard..

802.11f – Intervendor Access Point Handoffs

As the definition of mobility is extended to include constant operation while the mobile terminal is actually moving new problems begin to appear. Specifically, one of the basic assumptions of the IP addressing system of TCP/IP is that computers stay in one place physically and in the network map. The concept of handoffs is a very familiar one to cell phones, but it has not been nearly as familiar to the data networking environment. This group is working on a set of standards to enable these handoffs to be done in such a way as to work across access points from a number of vendors. This group anticipates creating a new standard that defines these parameters. This standard was approved and published in June of 2003.

802.11h – Power Control for 5 GHz Region

This group is looking into the tradeoffs involved in creating reduced-power transmission modes for networking in the 5 GHz space that would be compatible with spectrum usage laws in Europe. Potentially, this would allow 802.11a to be used by handheld computers and other devices with limited battery power available to them, and these devices would be usable in both the US and Europe.

There are a number of issues involved in this effort. They are also examining the possibility of allowing access points to reduce power to shape the geometry of a wireless network and reduce interference outside of the desired influence of such a network.

Preliminary versions of this standard caused a bit of a stir in Europe among those that are still trying to promote the European HiperLan standards. There were some fairly heated editorials about how the arrogant yanks were at it again.

This group plans on publishing the results as an amendment to the 802.11 family of specifications. I would expect that the major changes would come in the 802.11a document. These changes were approved in June of 2003.

802.11i – Enhanced Security

As mentioned earlier, there are problems in the security of 802.11 networks. This group is tasked with improving the PHY-level security that is used on these networks.

The whole question of security in wireless data networks is interesting. From one point of view it does not make much sense to worry about building default encryption in at the PHY layer. After all, Ethernet has no such capability and that doesn't seem to create much of a problem.

This is exactly the problem this group is facing. Even if they do their job perfectly, the best that can be achieved is security at the device level. If someone finds a device lying in the street, they can become whoever used to own it as far as the device and an associated wireless communications network is concerned.

I will discuss a more robust security proposal in a later section that may very well make the primary mission of this group moot. The group is planning to publish an amendment to the relevant 802.11 family of documents. This should be done by December of 2003.

802.11j – Adaptation to Japanese Wireless Requirements

The 802.11j committee has a mission very similar to that of the 802.11h one, but their target is Japan. As with that group, most of the attention is on the 5 GHz region rather than prior versions.

This group is too early in the process to be able to predict an approval date.

802.11k – Interface to Provide Power Metrics

One of the advantages of the 802.11 protocol stacks is strict adherence to appropriate levels of that protocol stack. All details of the radio interface are handled at the MAC and PHY level, and higher levels do not need to worry about these details.

But this can be a problem for some applications. For example, there may be two WLANs available, one with a weak signal and one that is stronger. Protocols such as Mobile IP would really like to be able to pick up differences like this to facilitate smooth handovers between networks. This is the information that the 802.11k standard will provide.

Again, this group is in the early stages of development and it is too soon to tell when they will publish. The result will most likely be a modification of current standards rather than a new document.

The New 802.15 Standards

The Bluetooth protocol has largely been identified very strongly with PANs. In a very real sense Bluetooth has defined the PAN. This is a problem for IEEE, considering that Bluetooth is not an IEEE standard.

This was a conscious decision by the companies that defined the Bluetooth specification. They wanted to bring this standard to market quickly, and the extended revision and approval cycles of the IEEE committees do not lend themselves well to speed of execution.

This has led to some problems. There was a significant flap last year about how Bluetooth was going to interfere destructively with 802.11 networks, since they both were operating in the 2.4 GHz spectrum. As it turned out, the interference is minimal, but the flap was more of a public relations event than a technical discussion anyway.

The two sides are attempting to come to an accord. The 802.15 standards are essentially the IEEE's attempt to coordinate PAN networking with the standards it has created or is creating for LAN and WAN networking.

802.15.1 PAN Network Definition

This standard was meant to be the base document, the way that the 802.11 standard is within that hierarchy. Unfortunately, Bluetooth already owns that space. As a result, the committee course was changed in December of 2001 and they quickly resolved to accept Bluetooth as the base PAN standard for the 802.15 groups, which was approved in March of 2002.

802.15.2 Wireless Coexistence

This committee is tasked with coordinating the 802.15.1 specification with "…other selected wireless devices…". In other words, Bluetooth.

This part of their task obviously depends on the existence of an IEEE specification with which to coordinate, but it also is responsible for coordinating other IEEE specifications with these existing devices. In other words, they are looking at how 802.11 and Bluetooth interact.

This document is now an Approved Publication..

802.15.3 High Data Rate for PANs

This group is the equivalent of the 802.11b group in that hierarchy. The goal is to improve whatever the 802.15.2 group comes up with to move it up to a data rate around 20 Mbps. They anticipate the creation of a new standard.

802.15.3a

Things are changing in this space very quickly. Just as the 802.15.3 group was getting going several companies announced development of PAN technology based on Ultra WideBand (UWB) technology. This essentially redefined the term "High Data Rate" and forced creation of a group that will concentrate on this technology for PAN applications. This group expected six or seven technology submissions. They received 29. As with the others, it is too early to tell when they will come out with a standard.

802.15.4 Low Speed and Complexity PANs

This group is going in the opposite direction of the previous one. The idea here is to standardize the small, cheap networking devices that are around such as toys and garage door openers. The concept is to standardize the protocols and make them as cheap as possible and supporting a standard set of protocols and data rates. They have published the results in a new standard.

Fixed Wireless 802.16 Standards

There is one more group in the IEEE hierarchy that pertains to wireless communications. This is the 802.16 group that concentrates on fixed wireless systems.

This is a relatively new group, but the work is potentially very important to the future deployment of wireless infrastructure systems.

The main concentration of this group is the spectrum between 10 and 66 GHz, with a specific concentration around 30 GHz. On the other hand, they are also examining the 802.11a protocols as a potential area of interest. This reflects the fact that wireless systems are not as cleanly divided as the WAN/LAN/PAN categories would make you think. Already there are efforts underway to extend 802.11b networks across metropolitan areas, and the faster throughput and cleaner bandwidth of 802.11a systems will only encourage that.

802.1x Impacts on Wireless

There is one more standard that could have a very significant impact on wireless networks. That is the 802.1x standard, which defines port-level security for networks based on the RADIUS/Kerberos protocols. There is work underway right now to extend those protocols into wireless LANs. The advantage here is that it would extend authentication capability to these networks via secure protocols.

This is exactly why security is not a crippling concern for Ethernet, in spite of the lack of PHY-level encryption. These protocols allow the creation of secure sessions based on authentication from a central server within the corporation. In essence, with this in place wireless LANs would become even more of simply a wireless extension of the corporate network. As such, it is much easier for companies to deal with them. This is a good thing for wireless computing.

It is worthwhile to note, however, that this will not help the home user that doesn't have an IT department. Maintaining a password server is not something that will be undertaken lightly in most homes. As a result, home wireless networks will still have security concerns.

My expectation is that this will not be a major concern. The range of wireless LANs is limited enough that they are not conducive to widespread hacking, and there are already more serious security concerns in most home systems. This is not the most serious problem they have.

The 802.11a/802.11g Controversy

There is serious confusion beginning to appear regarding the conflict between 802.11a and 802.11g. I have heard propaganda from a number of players on this issue, and some of it they ought to just be ashamed of. There is the shadow of obsolescence that is beginning to fall on 802.11b just as it was beginning to gain market acceptance. There is also the fact that 802.11a requires replacing or at least adding to the new access points and PC cards that just got bought. There is also the fact that many equipment manufacturers were just poised to build 802.11b into laptops and handheld computers. Now they are waiting to see which way they should go.

The companies that have heavy vested interests in 802.11b are pushing for people to wait for 802.11g as a 'logical' upgrade path. Chip manufacturers are rushing to complete designs that can handle combinations of these protocols. All in all, I have great sympathy for anyone trying to make a clear choice in this area.

As it turns out, the decision has gone pretty much to 802.11g for now. There are multi-protocol chipsets available that enable all three protocols, but the overwhelming majority of new installations are for 802.11b/g these days.

New things coming

Wireless data is becoming a busy field. As with most busy fields, there is confusion and shifting definitions. Looming over all of this discussion is a new technology called Ultra Wideband (UWB) that promises to rewrite the rules on wireless data transmission before the ink has a chance to dry.

This technology broadcasts data across a very wide spectrum at very low power, which means it should simply appear to be noise to any other users of the spectrum. Unfortunately, the FCC rules still don't take kindly to transmissions in restricted spectrum. This and other factors will probably force them to rewrite the rules on how spectrum is allocated. This certainly has interesting ramifications for wireless data transmission

Conclusion

Wireless data is a real opportunity for embedded systems. There has been an increase in the number of connected systems as LAN technology has become widespread, but there is still that nasty fact of life that is wires. Wireless communications promises to remove that tether once and for all.

The IEEE way of creating standards for this space is tedious, political, and in many ways pretty ugly. On the other hand, it is also the best one that I know of. The Bluetooth group sidestepped it because they couldn't afford to wait. In the end, it still took them just as long (if not longer) to get products to market and they still have the problem ahead of them of integrating it into the other IEEE standards.

If you have a deep interest in any of the standards described here or an interest in creating new standards I would encourage you to get involved in the process of creating them at IEEE. If you are not a member, I would encourage you to join.