What's what in wireless?

PDF e-mail it!

Surveying the wireless landscape

L Victor Marks (lvmarks@us.ibm.com)
Software engineer, IBM
May 2001

Need a quick overview of the current and emerging wireless standards? This article conveniently brings together the basics of many standards into one discussion -- personal area networking, wireless LAN, wireless WAN technologies, and RF data.

Contents:
Bluetooth, the Viking
IEEE 802.11b
IEEE 802.11a
Foreign competition-HiperLAN/2 for Europe
Ahhh, refreshing 5-UP!
Resources
About the author
Rate this article

This article explores the most popular current and emerging standards on the wireless landscape. While I won't go into complete detail or cover all the standards that have been written, I will, instead, introduce the big picture, and leave the rest to be covered in more detail in the upcoming articles on specific technologies.

Wireless technologies are currently being employed for personal, home, local, and wide area networks. I'll discuss the wireless standards in these arenas covering such information as frequency bandwidth, data bandwidth, range, and the implemented security solutions, if any. Wireless is primarily, but not limited to, transmitting Internet/e-mail and voice information.

Let's get personal

Personal area networks, or PANs, consist of devices that operate within a small range, and may or may not be traditional computing devices.

Bluetooth, the Viking

Bluetooth, named for the Viking, Harald Bluetooth, is the prevailing standard in this space so far, and the first device revealed for the standard is a hands-free headset for a cell phone that networks with an attachment to the cell phone, by Ericsson (see Resources). This device shows some of the potential for Bluetooth as more than just another way to bring the Internet to a mobile device.

Standard	Bluetooth
Frequency wavelength	2.4GHz (2.400-2.4835*)
Data bandwidth	v1.1 - 721Kbps, v1.2 - 10Mbps
Security measures	Public address which is unique for each user, two secret keys, and a random number which is different for each new transaction.
Optimum operating range	10 meters, or 30 ft.

Don't interfere!
Bluetooth, IEEE 802.11b, HomeRF, cordless phones, and microwave ovens all emit RF in the unlicensed 2.4GHz band. Because Bluetooth is intended for small range PANs, it could be commonplace to have a PAN in the same physical area as a Wireless LAN. This is a real problem, because the signals used by both standards occupy the same wavelength and conflict, making networking difficult. Nuking that leftover pizza is going to cause packet loss -- such is life.

Fortunately, solutions are being implemented to allow Bluetooth and IEEE 802.11b

Best suited for a specific purpose or device type	Phone hands-free headset, stereo headphones, laptops, PDA devices
Devices currently using the standard	Ericsson HDH-10 hands-free headset, Widcomm Handspring Springboard module

* Each country assigns radio frequencies differently, so in France Bluetooth operates on 2.4465GHz - 2.4835GHz.

This means that Bluetooth products sold in one country probably won't interoperate with products distributed in another country.

Currently, 115 products are approved by the Bluetooth special interest group, several of which are development tools, or components, with which other products can be created. Interesting consumer applications that have been approved fall into categories such as Bluetooth-enabled cell phones, PCMCIA, USB, and PCI host adapters for desktop computers, base stations, modem access points, and a Bluetooth-enabled laptop PC.

The application to which a standard is applied is every bit as important as the standard itself. Bluetooth has been poked fun at as the technology that will be used to put Web-enabled tablets in every kitchen device. I don't really need my toaster to talk to my blender and 'fridge -- they'd probably gang up on me; but Bluetooth seems to be perfect for the PDA wearer who wants the PDA to synchronize from his pocket, or the cell-phone-to-wireless-headset combination. Back in the Web-enabled kitchen, when the oven gets a virus, I'm the one who gets burned.

Security is a subject that can't be emphasized enough, even in an ad-hoc network where devices are allowed to connect at leisure. Even in such a free environment, data transmitted between devices should be secure between both the sending and the receiving device. The Bluetooth device address is the 48-bit IEEE address, and is unique for each Bluetooth unit. The Bluetooth addresses are publicly known, and can be obtained via MMI interactions, or automatically via an inquiry routine by a Bluetooth unit.

The transmission of data is then key-encrypted. The secret keys are generated during initialization and are never disclosed. Normally, the encryption key is derived from the authentication key during the authentication process. For the authentication algorithm, the size of the key used is always 128 bits. For the encryption algorithm, the key size might vary between 1 and 16 octets (8 - 128 bits). The key size is user-configurable, which has the advantage of allowing the user to be as paranoid as he wants to be. Also important to the user is the trade-off between speed and security; the greater bit-length of encryption slows down the speed at which data packets are transmitted.

to coexist. First of all, IEEE 802.11b performance suffers more from Bluetooth activity than Bluetooth suffers from IEEE 802.11b; that's because 802.11b is a wireless version of Ethernet, which listens before broadcasting. Wireless Ethernet also has to have each received packet acknowledged. If a packet is sent, but receipt isn't acknowledged, it backs off and tries to send again. This works great when the interference is caused by another 802.11b station or access point, but not so great when it's caused by Bluetooth. The effects of the interference diminish as the Bluetooth device is further from the 802.11b device, with the least amount of interference at 2 meters distance from the 802.11b device.

Without going into a lot of detail that belongs in an article unto itself, Bluetooth developers have begun to research several methods for getting around, or at least lessening the worst of the interference. Some of the steps being considered are:

- Driver-level switching
- Adaptive frequency hopping
- MAC-level switching

Mobilian has done a substantial amount of research in this area and has a two-chip product that incorporates both Bluetooth and IEEE 802.11b. If only children on a family road trip got along so well.

And all from the convenience of your own home.
Home networking is currently dominated by 802.11b and HomeRF, with HomeRF running a distant second. These are soon to be joined by 802.11a, HiperLAN/2, and 5-UP. These standards are largely used for Internet and LAN functions that could be accomplished in much the same fashion as wired networks.

HomeRF

Standard	**HomeRF**

Frequency wavelength	2.4GHz
Data bandwidth	10Mbps, 5Mbps, 1.6Mbps, 0.8Mbps (Future plans -- 20Mbps)
Security measures	128-bit encryption, frequency hopping, 48-bit network ID
Optimum operating range	"Covers typical home and yard"
Best suited for a specific purpose or device type	Laptops, gateways, and cable modems with wireless gateways built in
Devices currently using the standard	Cayman Systems, Compaq, Intel, Motorola, Proxim

One advantage of HomeRF is that its main supporter is Intel, a company we won't see dissolving anytime soon. With devices produced by Compaq and Motorola, this is one standard that might last, simply because of the companies supporting it. That said, it's not being marketed well, and the 802.11b products have captured the home consumer's attention as established by Apple, IBM, and others building this functionality into computer offerings.

IEEE 802.11b

802.11b is really the standard that dominates wireless home networking in the public eye, and in the business of selling consumer products, the public eye is everything. This standard was pioneered by Lucent, but is more widely known as Apple Airport. That's really one benefit Apple has; when Apple introduces a product, *everyone* who owns a Macintosh knows about it.

Standard	**802.11b, Wi-Fi**
Frequency wavelength	2.4GHz (2.400-2.4835 in North America)
Data bandwidth	11Mbps, 5Mbps, 2Mpbs, 1Mbps
Security measures	WEP -- Wireless Equivalency Protocol in combination with direct spread spectrum
Optimum operating range	150 ft. indoors, 300 ft. outdoors
Best suited for a specific purpose or device type	Laptops, desktops where running cable is difficult, PDAs
Devices or manufacturers currently using the standard	Apple Airport, Dell TrueMobile, Melco (Buffalo, Techworks.com) AirStation, 3Com, Linsys, D-Link

Security cannot be emphasized enough, and lately the Wi-Fi organization that sponsors the standard has had to respond to reports of insecure transmissions. No one expects to have their e-mail passwords stolen while receiving messages!

Here, in the Wi-Fi group's own words, is their response:

> *"The goal of WEP is to provide an equivalent level of privacy as is ordinarily present with an unsecured wired LAN. Wired LANs such as IEEE 802.3 (Ethernet) do not incorporate encryption at the Physical or Media Access layer, since they are ordinarily protected by physical security mechanisms such as controlled entrances to a building. Wireless LANs are not necessarily protected by this physical security because the radio waves might penetrate the exterior walls of a building. IEEE 802.11 decided to incorporate WEP into the standard to provide an equivalent level of privacy as the wired LAN by encrypting the transmitted data. If this goal were achieved, then higher layer security mechanisms that were developed for*

> *wired LANs would work with no modification on IEEE 802..11 wireless LANs. It is important to emphasize that WEP was never intended to be a complete end-to-end security solution. It protects the wireless link between the client machines and access points. Whenever the value of the data justifies such concern, both wired and wireless LANs should be supplemented with additional higher-level security mechanisms such as access control, end-to-end encryption, password protection, authentication, virtual private networks, or firewalls."*

Now, it's important to remember that the hacks that people have been performing to show how insecure 802.11b might be are not easy. I'm not convinced they're as difficult to perform as the Wi-Fi organization claims, but as Wi-Fi recommends, if you really want to ensure your own security, use some form of encryption. As with the encryption in Bluetooth, the larger the number of bits in the key generated for the encryption, the slower the performance will be. Most people recommend OpenSSH or PGP for encrypting. OpenSSH works as a method for making secure remote logins, like those required for Telnet or FTP services. PGP is a method pioneered by Phillip Zimmerman for strong public key encryption, or as PGP stands for, Pretty Good Privacy. It's worth mentioning that many of the access points and host adapters include at least 64 bit encryption that can be enabled, and some allow for 128 bit encryption, so that the radio signal is encrypted. It certainly doesn't hurt for a user to encrypt the data further.

802.11b uses the 2.4GHz range. Using this range in certain environments can cause some small problems. 802.11b doesn't work well around operating microwave ovens, 2.4GHz cordless telephones, and Bluetooth devices, but as mentioned in the first sidebar, solutions to this problem are being developed.

One of the interesting things about this protocol is the way it is implemented in access points. The standard says that access points must implement some method of enabling roaming between access points, but leaves the implementation entirely up to the manufacturer. It is certainly possible for one host adapter to work with both an Apple Airport and a Melco AirStation, but since roaming between the two is likely to be implemented differently, I'd have to have my host adapter renew its IP when switching to a new station, assuming I'm using DHCP. I've only used these two products as examples, and while it's likely my example is factual, I haven't tested it in a real world situation or disassembled my AirStation.

Luke: "Can't this THING go any faster?!"
Han:"Flying space ships ain't like dusting crops, boy!"

Bluetooth, IEEE 802.11b, and HomeRF are all fairly slow when it comes to data transfer speeds. As with everything in life, there are trade-offs: When it comes to adding more speed and maintaining the same range, we need more power. Power is a major concern in the design of network devices, considering that most of the wireless applications are produced for devices that are intended to be powered by batteries. Power is essentially proportional to throughput at a given range, so achieving 50 Mbps takes approximately 5 times the power of 10 Mbps. The result is that 54-Mbps, 5-GHz designs must be more power-efficient to achieve similar range or power usage as 11-Mbps, 2.4-GHz designs. In wireless LANs, maximum power is usually consumed while sending data.

IEEE 802.11a
IEEE 802.11a hasn't actually appeared on the market for consumers yet. In many ways it is similar to 802.11b, both being a wireless variation of the Ethernet standard. They both share WEP, although it is being expanded upon for the newer 802.11a. They also share similar software layers. The primary difference lies in the physical layer of the standard, which changes to a different wavelength and higher data bandwidth speeds. Once again, international partitioning of frequency bandwidth causes problems for worldwide interoperability; less bandwidth is permitted for use in Japan, and this standard has to meet more requirements to be passed by ETSI, the European standards board.

Standard	**IEEE 802.11a, WLAN**
Frequency wavelength	5GHz
Data bandwidth	54Mbps, 48Mbps, 36Mbps, 24Mbps, 12Mbps, 6Mbps
Security measures	WEP, OFDM

Optimum operating range	150 ft. indoors, 300 ft. outdoors
Best suited for a specific purpose or device type	Roaming laptops in home or business; computers when wiring is inconvenient
Devices currently using the standard	None for consumers at this time; chipsets made by Atheros and Radiata

Foreign competition- HiperLAN/2 for Europe

Standard	**HiperLAN/2**
Frequency wavelength	5GHz (5.15 - 5.3GHz)
Data bandwidth	6, 9, 12, 18, 27, 36, 54Mbps
Security measures	An encryption-decryption scheme for optional use in the HiperLAN/2
Optimum operating range	150 meters maximum
Best suited for a specific purpose or device type	Packetized voice, video, and Internet communications

The 5GHz band is open in Europe, the United States, and Japan. The current spectrum allocation at 5GHz comprises 455MHz in Europe, 300MHz in the U.S., and 100MHz in Japan.

The HiperLAN/2 network has support for both authentication and encryption.. With authentication, both the AP and the MT can authenticate each other to ensure authorized access to the network (from the AP's point of view), or to ensure access to a valid network operator (from the MT's point of view). Authentication relies on the existence of a supporting function, such as a directory service, but this is outside the scope of HiperLAN/2. The encryption can be used to protect against eavesdropping and man-in-the-middle attacks. In HiperLAN/2, each communicating node is given a HiperLAN/2 ID (HID) and a Node ID (NID). These two IDs uniquely identify any station, and restrict the way in which it can connect to other HiperLAN/2 nodes. All nodes with the same HID can communicate with each other using a dynamic routing mechanism denoted Intra-HiperLAN Forwarding (see Resources).

HiperLAN/2 does permit roaming between access points, making it suitable for a corporate wireless LAN.

OFDM
Wideband Orthogonal Frequency Division Multiplexing (W-OFDM) is a transmission scheme that enables data to be encoded on multiple high-speed radio frequencies concurrently. This allows for greater security, increased amounts of data being sent, and is claimed to be the industry's most efficient use of bandwidth.

W-OFDM tries to solve the problem that Bluetooth and 802.11b networks have when operating in the same frequency range. It enables the implementation of low power multipoint RF networks that minimize interference with adjacent networks. This reduced interference enables independent channels to operate within the same band allowing multipoint networks and point-to-point backbone systems to be overlaid in the same frequency band.

A series of articles could be devoted to OFDM technologies alone, but for now, know that it's a way of arranging the signal to reduce interference and to keep the speed of transmission high. Combined with Direct Spread Spectrum, and WEP, this signal is fairly complex to try and spy on. Again, security is not a passive practice, and users should supplement wireless communications with as much encryption as deemed necessary.

What's really intriguing about HiperLAN/2 is it's implementation of convergence layers in the MAC. It allows for HiperLAN/2 to adapt service requests from higher layers to the services offered by the data link control layer (DLC), and for converting the higher layer packets with fixed or variable sizes into fixed-size DLC Service Data Units that are used within the DLC. Convergence layers have been developed for Ethernet (IP-based) applications, cell based core networks such as ATM, and for IEEE 1394 protocols and applications. In addition, it is scheduled to define access interfaces to the third-generation mobile in cooperation with the ETSI Project UMTS and 3GPP. This means that HiperLAN/2 can carry ATM and FireWire over wireless links. As more convergence layers are introduced it will be interesting to see what new uses can be made of this standard.

Ahhh, refreshing 5-UP!
Atheros isn't taking any chances, and is producing parts for competing European standards as well. From their products Web site:

> Both the international IEEE 802.11a and European ETSI HiperLAN/2 specifications are for high-speed local area networks operating in the 5.15- to 5.35-GHz band. At this time, no products are shipping in accordance with these new specifications. Atheros' proposal is to enhance these protocols and provide backward interoperability to products that comply only with the specifications as they exist, while also enabling new capabilities, hence the name 5-UP, from 5GHz Unified Protocol.

Atheros' goal is to produce a standard that is compatible with both HiperLAN/2 *and* IEEE 802.11a while enabling 108Mbps maximum.

Standard	**5-UP**
Frequency wavelength	5GHz
Data bandwidth	128Kbps to 108Mbps, scaling

5-UP has been submitted to the IEEE and ETSI, but hasn't been approved. No reference designs are readily available at this time. 5-UP sounds promising, especially because of its interoperability, but it's hard to pass judgement on a standard with so few documents available for public perusal.

Be sure to tune in next time for part 2, which will cover Wide Area Wireless Networking -- cell phone and cell phone-like technologies, such as:

- TDMA, CDMA, GSM, Mobitex, Motient, CDPD (Ricochet)
- GPRS, PHS, EDGE (expansion on GRPS), UMTS

Resources

- The WebSphere Everyplace Suite SDK allows you to create and test wireless applications.
- Visit the IBM pervasive/wireless home page for links to wireless development solutions.
- Visit the Wireless Ethernet Compatability Alliance.
- Check out details on a hands-free headset for a cell phone that networks with an attachment to the cell phone, by Ericsson
- Peruse research into the coexistence of Bluetooth and 802.11b networks in the 2.4GHz band
- Visit the Bluetooth interest group member site
- Read the Bluetooth public site technical specifications
- Portable Design has a great Bluetooth article by Anita S. Becker (*Wave of Bluetooth components crests*. Portable Design, February 2001, p.40. PennWell Corp., ATD Publishing : Nasua, NH)
- See The HomeRF specification
- For more information on HiperLAN/2, see this paper at the technical committee RES10 Web site.
- Apple has good resources on their 802.11b products, designing AirPort networks, and on wireless networking
- See the Ambicon FAQ about 802.11b
- See also the Commnet article on 802.11a
- Chipcenter.com hosts articles on the chips by Radiata and Atheros
- Read up on the HiperLAN/2 spec
- Check out this well-written essay on HiperLAN/2 by Janne Korhonen
- Read Atheros' 5-UP proposal

About the author

L Victor Marks works at IBM, and enjoys hands-on experiences with wireless technologies. He is currently using an 802.11b network at home and looking to introduce Bluetooth and other emerging technologies. He spends the rest of his time restoring a 1962 Chevrolet Impala. He happily responds to e-mail at lvmarks@us.ibm.com.

PDF e-mail it!

What do you think of this article?

○ Killer! (5) ○ Good stuff (4) ○ So-so; not bad (3) ○ Needs work (2) ○ Lame! (1)

Comments?

Submit feedback

About IBM | Privacy | Legal | Contact