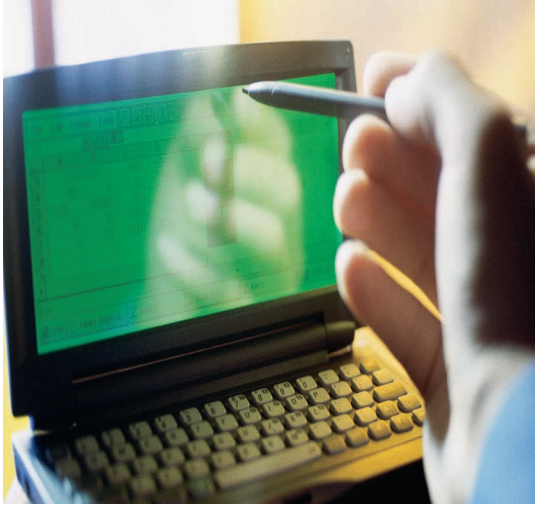

IEEE 802.11 continues to expand. It's time to look at what this alphabet soup of a standard is all about.

William Stallings

IEEE 802.11: Wireless LANs from a to n

From its inception in 1980, the IEEE 802 committee has led the way in developing LAN (local area network) standards. The committee's work on wireless LANs (WLANs) began in 1987 within the IEEE 802.4 working group. Developing an ISM (industrial, scientific, and medical)-based WLAN using the equivalent of a token-passing bus media access control (MAC) protocol was the committee's initial goal. After some work, the committee decided that a token-bus-controlled radio medium would cause inefficient use of the radio frequency spectrum. In 1990, the committee formed a new working group, IEEE 802.11, specifically devoted to WLANs, with a charter to develop a MAC protocol and physical-medium specification.

Since then, demand for WLANs, at different frequencies and data rates, has exploded. Keeping pace with this demand, the IEEE 802.11 working group has issued an ever-expanding list of standards.

IEEE 802.11 PROTOCOL ARCHITECTURE

IEEE 802.11 is defined within the protocol architecture developed as an IEEE 802 standard, consisting of three layers: logical link control (LLC), media access control (MAC), and physical, as Figure 1 illustrates. The LLC layer provides an interface to higher layers and performs basic link layer functions such as error control and flow control. Every LAN consists of devices that must share its transmission capacity. Thus, an individual LAN needs some way to control access to the transmission medium so that devices will use that capacity in an orderly and efficient manner. This responsibility falls to the MAC protocol, which ensures that all the devices on a LAN cooperate. The MAC protocol requires that only one mobile device transmit at a time, and it specifies that data be transmitted in blocks, or MAC frames. Each frame includes user data, a destination and source address, error-detection code, and MAC control bits. Each mobile device monitors the shared medium for frames with a destination address that matches its address, and copies frames addressed to itself. For IEEE 802.11, the MAC layer has two sublayers. The lower one is the distributed coordination function, which uses an Ethernet-style contention algorithm that provides access to all traffic. Ordinary asynchronous traffic uses this coordination function. The upper MAC sublayer is the point coordination function, a centralized MAC algorithm that provides contention-free service by polling mobile devices in turn. Higher-priority traffic—traffic with greater timing requirements—uses this coordination function. The physical layer defines the frequency band, data rate, and other details of the actual radio transmission.

PHYSICAL-LAYER STANDARDS

Within IEEE 802.11's layered protocol architecture, the physical layer describes the frequency band, data rate, and encoding technique. Table 1

Inside

Resources

Published by the IEEE Computer Society

1520-9202/04/$20.00 © 2004 IEEE

provides some details about each physical-layer standard.

The original standard, known simply as IEEE 802.11, defined the MAC layer and three physical layers. The three physical media that the original 802.11 standard defined are the following:

- *Direct-sequence spread spectrum (DSSS).* The standard defines this medium as operating in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps. In the US, the Federal Communications Commission (FCC) requires no licensing to use this band. The total number of available channels depends on the bandwidth that the various national regulatory agencies allocate. This ranges from 13 in most European countries to just one available channel in Japan.
- *Frequency-hopping spread spectrum (FHSS).* The standard also defines this medium operating in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps. The number of channels available ranges from 23 in Japan to 70 in the US.
- *Infrared.* At 1 Mbps and 2 Mbps, operating at a wavelength between 850 and 950 nm, this option never gained market support because it requires unobstructed line-of-sight and because the available data rates are limited.

The first two schemes use spread-spectrum approaches. Spread spectrum essentially involves using a much wider bandwidth than is actually necessary to support a given data rate. Using a wider bandwidth minimizes interference and drastically reduces the error rate. FHSS spreads the spectrum by repeatedly jumping from one carrier frequency to another; thus, interference or performance degradation at a given frequency only affects a small fraction of the transmission. DSSS effectively increases a signal's data rate by mapping each data bit into a string of bits, using one string for binary 1 and another for binary 0. The higher data rate uses a greater bandwidth. The effect is to spread each data bit out over time, minimizing the effects of interference and degradation. Most early 802.11 networks employed FHSS, which is somewhat less complex to implement than DSSS. Products using DSSS fol-

Figure 1. IEEE 802.11 protocol architecture.

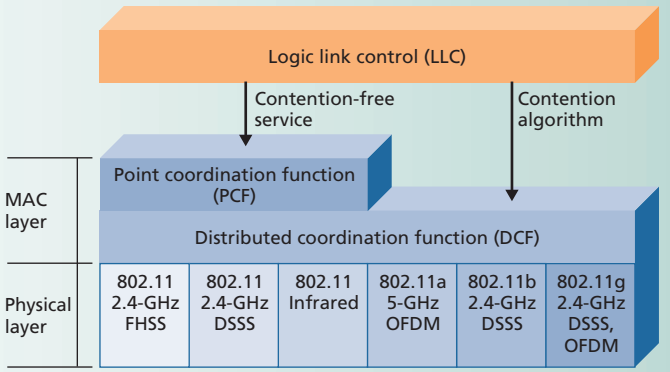

Table 1. IEEE 802.11 physical layer standards.

Standard	Date issued	Available bandwidth (MHz)	Unlicensed frequency of operation (MHz)	No. of nonoverlapping channels *	Data rate per channel (Mbps)	Compatibility
802.11	1997	83.5	2.4 to 2.4835 DSSS, FHSS	3 indoor or outdoor	1, 2	802.11
802.11a	1999	300	5.15 to 5.35 OFDM (orthogonal frequency division multiplexing) 5.725 to 5.825 OFDM	4 indoor 4 indoor or outdoor 4 outdoor	6, 9, 12, 18, 24, 36, 48, and 54	Wi-Fi5
802.11b	1999	83.5	2.4 to 2.4835 DSSS	3 indoor or outdoor	1, 2, 5.5, and 11	Wi-Fi
802.11g	2003	83.5	2. 4 to 2.4835 DSSS, OFDM	3 indoor or outdoor	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54	Wi-Fi at 11 Mbps and below

*Nonoverlapping channels have frequency bands that do not overlap. Their operation can take place in the same area simultaneously.

Table 2. Other IEEE 802.11 standards.

Standard	Date issued	Scope
802.11c	2003	Bridge operation at 802.11 MAC layer
802.11d	2001	Physical layer: Extend operation of 802.11 WLANs to new regulatory domains
802.11e	Ongoing	MAC: Enhance to improve quality of service (QoS) and enhance security mechanisms
802.11f	2003	Recommended practices for multivendor access point interoperability
802.11h	2003	Physical or MAC: Enhance IEEE 802.11a to add indoor and outdoor channel selection and to improve spectrum and transmit power management
802.11i	Ongoing	MAC: Enhance security and authentication mechanisms
802.11j	Ongoing	Physical: Enhance IEEE 802.11a to conform to Japanese requirements
802.11k	Ongoing	Radio resource measurement enhancements to provide interface to higher layers for radio and network measurements
802.11m	Ongoing	Maintenance of IEEE 802.11-1999 standard with technical and editorial corrections
802.11n	Ongoing	Physical or MAC: Enhancements to enable higher throughput

lowed; DSSS is more effective in the 802.11 scheme in terms of resistance to interference. However, all of the original DSSS 802.11 products were of limited use because of their low data rates.

802.11a

The IEEE 802.11a specification uses the 5-GHz band. The working group established this standard so US users could take advantage of a newly allocated unlicensed radio band, the Unlicensed National Information Infrastructure (UNII) band. The FCC created UNII so manufacturers could develop high-speed wireless networks. To find enough bandwidth to meet demand, the FCC established the band at 5 GHz, making it incompatible with 2.4-GHz equipment.

Unlike the 2.4-GHz specifications, IEEE 802.11a uses OFDM rather than a spread-spectrum scheme. OFDM, also called multicarrier modulation, uses multiple carrier signals at different frequencies, sending some of the bits on each channel. This is similar to FDM (frequency-division multiplexing), which uses each subchannel for a separate data source. OFDM, however, dedicates all of the subchannels to a single data source. The possible data rates per channel for IEEE 802.11a are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

802.11b

IEEE 802.11b is an extension of the IEEE 802.11 DSSS scheme, providing data rates of 5.5 and 11 Mbps. Each channel requires the same 11-MHz bandwidth as an 802.11 DSSS channel. To achieve a higher data rate in the same bandwidth, the standard employs a modulation scheme called complementary code keying. IEEE 802.11b is currently the most commonly used 802.11 standard in commercial products.

802.11g

IEEE 802.11g extends 802.11b to data rates of 12 to 54 Mbps per channel. IEEE 802.11g is compatible with 802.11b because they both operate in the 2.4-GHz range. The key difference between 802.11b and 802.11g is that the latter uses OFDM and DSSS rather than DSSS only. With this standard, 802.11b devices will work when connected to an 802.11g access point, and 802.11g devices will work when connected to an 802.11b access point, in both cases using the lower 802.11b data rate.

Other IEEE 802.11 standards

The standards discussed so far provide specific physical-layer functionality, but several other 802.11 standards are in place or in development, as Table 2 shows.

IEEE 802.11c covers bridge operation. A bridge is a device that links to LANs with a similar or identical MAC protocol. It performs functions similar to those of an Internet Protocol (IP)-level router, but at the MAC layer. Typically, a bridge is simpler and more efficient than an IP router. In 2003, the 802.11c task group completed its work on this standard, which folded into the IEEE 802.1d standard for LAN bridges.

IEEE 802.11d is a regulatory domain update. It covers issues related to regulatory differences in various countries.

IEEE 802.11e revises the MAC layer to improve QoS and address MAC enhancement. It accommodates time-scheduled and polled communication during null periods when no other data is moving through the system. In addition, IEEE 802.11e improves polling efficiency and channel robustness. These enhancements should provide the quality necessary for services such as IP telephony and video streaming. A QoS station is any base station implementing

802.11e. In a QoS station, a hybrid coordination function (HCF) replaces modules for a distributed coordination function (DCF) and point coordination function (PCF). The HCF consists of enhanced distributed-channel access (EDCA) and HCF-controlled channel access (HCCA). EDCA extends the legacy DCF mechanism to include priorities. As with the PCF, HCCA centrally manages medium access, but does so more efficiently and flexibly.

IEEE 802.11f addresses interoperability among access points from multiple vendors. In addition to providing communication among WLAN stations in its area, an access point can function as a bridge that connects two 802.11 LANs across another type of network, such as an Ethernet LAN or a wide area network. So IEEE 802.11f facilitates the roaming of a device from one access point to another while ensuring transmission continuity.

IEEE 802.11h covers spectrum and power management. The objective is to make 802.11a products compliant with European regulatory requirements. The European Union military uses part of the 5-GHz band for satellite communications. The standard includes a dynamic channel selection mechanism to prevent selection of the frequency band's restricted portion. The standard's transmit-power-control features adjust power to EU requirements.

IEEE 802.11i defines security and authentication mechanisms at the MAC layer. This standard addresses security deficiencies in the Wired Equivalent Privacy (WEP) algorithm originally designed for the MAC layer of 802.11. The 802.11i scheme's stronger encryption and other enhancements improve security.

IEEE 802.11j addresses 4.9- and 5-GHz operation in Japan.

IEEE 802.11k defines enhancements that provide mechanisms available to protocol layers above the physical layer for radio resource measurement. The standard specifies what information should be available to facilitate the management and maintenance of wireless and mobile LANs, including the following:

- To improve roaming decisions, an access point can provide a site report to a mobile device when the access point determines that the mobile device is moving away from it. The site report lists access points—from best to worst service—that a mobile device can use in changing over to another access point.
- An access point can collect channel information from each mobile device on the WLAN. Each mobile device provides a noise histogram that displays all non-802.11 energy on that channel as perceived by the mobile device. The access point also collects statistics on how long a channel is in active use during a given time. This data enable the access point to regulate access to a given channel.
- Access points can query mobile devices to collect statistics, such as retries, packets transmitted, and packets received. This gives the access point a more complete view of network performance.
- 802.11k extends the transmit-power-control procedures (defined in 802.11h) to other regulatory domains and frequency bands, to reduce interference and power consumption, and to provide range control.

IEEE 802.11m is an ongoing task group activity to correct editorial and technical issues in the 802.11 standard. The other task groups generate documents, and the 802.11m task group reviews those documents to locate and correct inconsistencies and errors in the 802.11 standard and its approved amendments.

The IEEE 802.11n task group is studying various enhancements to the physical and MAC layers to improve throughput. These enhancements include such items as multiple antennas, smart antennas, changes to signal encoding schemes, and changes to MAC protocols. The task group's current objective is a data rate of at least 100 Mbps, as measured at the interface between the 802.11 MAC layer and higher layers. In contrast, the 802.11 phys-

Resources

Web Sites

- **IEEE 802.11 Wireless LAN Working Group (http://grouper.ieee.org/groups/802/11/index.html): Contains working group documents plus discussion archives.**
- **Wi-Fi Alliance (http://www.wi-fi.org/OpenSection/index.asp): Industry group promotes the interoperability of 802.11 products.**
- **Wireless LAN Association (http://www.wlana.org): In addition to an introduction to the technology, this site includes user case studies and a discussion of implementation considerations.**

Books

- ***802.11 Wireless LAN Fundamentals*, Pejman Roshan and Jonathan Leary, Cisco Press, 2004: This book covers IEEE 802.11 standards in detail.**
- ***Wireless Communications and Networks*, 2nd ed., William Stallings, Prentice Hall, 2004: Available in November 2004, this edition contains detailed technical coverage of wireless LANs and all IEEE 802.11 standards.**

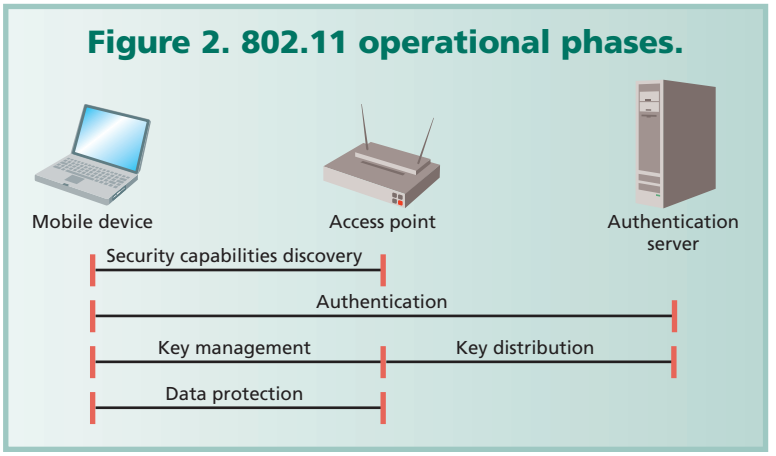

Figure 2. 802.11 operational phases.

ical-layer standards listed in Table 1 measure data rate at the physical interface to the wireless medium. The motivation for measuring at the upper interface to the MAC layer is that a user can experience a data rate significantly less than that of the physical layer. Overhead includes packet preambles, acknowledgments, contention windows, and various interface spacing parameters. The result is that the data rate coming out of the MAC layer could be about one-half of the physical-layer data rate. In addition to improving throughput, 802.11n addresses other performance-related requirements, including improved range at existing throughputs, increased resistance to interference, and more uniform coverage within an area. An approved standard by the end of 2005 is the current goal.

WI-FI ALLIANCE

Shortly after 802.11b approval, many vendors adopted it for their WLAN products. Although these new products are all based on the same standard, there is always concern about whether products from different vendors will interoperate. To meet this concern, the Wireless Ethernet Compatibility Alliance (WECA, http://www.wi-fi.org), an industry consortium, formed in 1999. The consortium, subsequently renamed the Wi-Fi (wireless fidelity) Alliance, created a test suite to certify 802.11b product interoperability. As of October 2004, this group had certified products from 142 vendors. Wi-Fi is the term for certified 802.11b products. Wi-Fi certification has extended to 802.11g products, and 86 vendors have thus far qualified. The Wi-Fi Alliance has also developed a certification process for 802.11a products, called Wi-Fi5. So far, 47 vendors have qualified for Wi-Fi5 certification.

The Wi-Fi Alliance focuses on various market areas for WLANs, including enterprise, home, and hot spots.

HIGH-SPEED WLAN CHOICES

For high-speed WLAN capability, users now have two standardized choices: 802.11a and 802.11g. The 802.11g standard ensures high data rates while maintaining backward compatibility with existing 802.11b equipment. At data rates up to 11 Mbps, 802.11g uses the same DSSS modulation scheme as 802.11b, and provides full interoperability within the 2.4-GHz band. Thus, 802.11g is attractive for use with an installed base of 802.11b equipment. The drawback is that its total capacity is lower than 802.11a. The 802.11a scheme, operating in the 5-GHz band, has a total bandwidth of 300 MHz, compared to only 83.5 MHz for 802.11g. This bandwidth translates into eight simultaneous channels for 802.11a, compared to three channels for 802.11g.

Another consideration is interference. In the 2.4-GHz band, 802.11g must contend with interference from satellites, microwave ovens, and high-end wireless phones, resulting in lower throughput and shorter range. The 5-GHz band of 802.11a deals with much less interference; in the US, this band will likely stay free of most other types of radio frequency devices.

A factor in user choice is that many vendors will likely offer combination chips that support both standards at a modest cost increase over a single-standard chip.

WLAN SECURITY

Two characteristics of a wired LAN are not inherent in a WLAN. First, to transmit over a wired LAN, you must physically connect a mobile device to the LAN. On the other hand, with a WLAN, any mobile device within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, for two reasons. First, some positive and presumably observable action is necessary to connect a mobile device to a wired LAN—that is, someone will see you connecting to the LAN. Second, to receive a transmission from a mobile device on a wired LAN, the receiving mobile device must also connect to the wired LAN. On the other hand, with a WLAN, any mobile device within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting the reception of data to mobile devices connected to the LAN.

Accordingly, the original 802.11 specification included security features for privacy and authentication, which were unfortunately quite weak. For privacy, 802.11 defined the WEP algorithm. WEP uses a 40-bit key based on the RC4 encryption algorithm. A later revision enables the use of a 104-bit key. For authentication, 802.11 requires that the two parties share a secret key that no other party shares, and defines a protocol by which the two parties can use this key for mutual authentication.

The privacy portion of the 802.11 standard contained major weaknesses. The 40-bit key is woefully inadequate. Even the 104-bit key proved vulnerable because of various weaknesses internal and external to the protocol supporting WEP. These vulnerabilities include the heavy reuse of keys, the ease of data access in a wireless network, and

the lack of any key management within the protocol. Similarly, the shared-key authentication scheme has several problems, such as the use of the weak keys just mentioned and the fact that authentication is in one direction only (only the initiator of an exchange is authenticated).

The 802.11i task group has developed capabilities to address the WLAN security issues. To accelerate the introduction of strong security into WLANs, the Wi-Fi Alliance declared Wi-Fi Protected Access (WPA) as a Wi-Fi standard. WPA is a set of security mechanisms that eliminates most 802.11 security issues and was based on the current state of the 802.11i standard. As 802.11i evolves, WPA will evolve to maintain compatibility.

IEEE 802.11i addresses three main security areas: authentication, key management, and data transfer privacy. To improve authentication, 802.11i requires an authentication server and defines a more robust authentication protocol. The authentication server also plays a role in key distribution. For privacy, 802.11i provides three different encryption schemes. The scheme that provides a long-term solution uses the Advanced Encryption Standard (AES) with 128-bit keys. However, because AES use would require expensive upgrades to existing equipment, 802.11i also defines alternative schemes based on 104-bit RC4.

Figure 2 presents a general overview of 802.11i operation. First, an exchange between a mobile device and an access point enables the two to agree on a set of security capabilities to use. Then, an exchange involving the authentication server and the mobile device ensures secure authentication. The authentication server is responsible for key distribution to the access point, which in turn manages and distributes keys to mobile devices. Finally, the mobile device and the access point use strong encryption to protect the data transfer between them.

As of this writing, several other task groups are in the early planning stages. IEEE 802.11r is looking at the concept of fast roaming. IEEE 802.11s is concerned with mesh networking, which deals with interconnection of multiple 802.11 WLANs. IEEE 802.11t deals with performance prediction. Issues for 802.11t include performance metrics and application-level testing for evaluating wireless performance. ■

William Stallings *is a consultant, lecturer, and author of more than a dozen professional reference books and textbooks on data communications and computer networking. Contact him at ws@shore.net or at http://www.WilliamStallings.com.*

For further information on this or any other computing topic, visit our Digital Library at http://computer.org/publications/dlib.