Although the IEEE 802.11 standard has been around since 1997, work continues to make it more adaptable to the demand for higher data rates and true wireless flexibility.

William Stallings

IEEE 802.11: Moving Closer to Practical Wireless LANs

Wireless LANs have quickly become a significant niche in the LAN market. As adjuncts to traditional wired LANs, they satisfy mobility, relocation, and ad hoc networking requirements and provide a way to cover locations that are difficult to wire.

As the name suggests, a wireless LAN uses a wireless transmission medium. Until relatively recently, few organizations used wireless LANs because they cost too much, their data rates were too low, they posed occupational safety problems because of concerns about the health effects of electromagnetic radiation, and the spectrum used required a license. Today, however, these problems have largely diminished, and wireless LAN popularity is skyrocketing.

WHEN WIRELESS LANs MAKE SENSE

Wireless LAN products first appeared in the late 1980s, marketed as substitutes for traditional wired LANs. The idea was to use a wireless LAN to avoid the cost of installing LAN cabling and ease the task of relocating or otherwise modifying the network's structure.

As events unfolded, however, organizations began to rethink this substitution strategy. LANs had become more popular, and architects were designing new buildings to include extensive prewiring for data applications. Also, as data transmission technology advanced, organizations began relying more on inexpensive twisted-pair cabling for LANs—in particular Category 3 and Category 5 unshielded twisted pair. Category 3 wiring is the traditional telephone wiring found in every office building; category 5 wiring is higher-performance wiring able to carry higher data rates. Many older buildings are prewired with an abundance of Category 3 cable, and many newer buildings are prewired with Category 5. Thus, there was little motivation to replace wired LANs with wireless.

This is not true of all environments, however. For some, the motivation to use wireless LANs is much higher. Buildings with large open areas, such as manufacturing plants, stock exchange trading floors, and warehouses, make wired LANs awkward to install because of limited choices for cable placement. Historical buildings often have insufficient twisted-pair cabling and prohibit drilling holes for new wiring. Finally, small offices often find it uneconomical to install and maintain wired LANs.

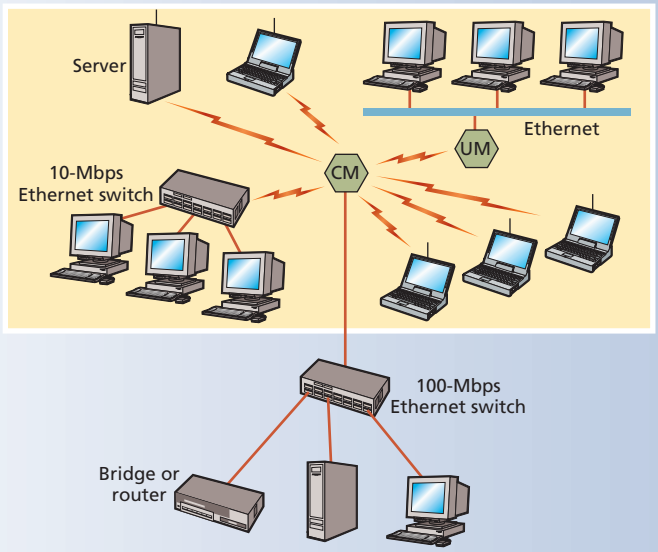
POSSIBLE CONFIGURATIONS

In most cases, an organization already has a wired LAN to support servers and some stationary workstations. For example, a manufacturing facility typically has an office area that is physically separate from the factory floor but must be linked to it for networking. Therefore, organizations will commonly link a wireless LAN into a wired LAN on the same premises. This kind of application, or *LAN extension*, can take several forms.

Inside

1520-9202/01/$10.00 © 2001 IEEE

Figure 1. Single-cell wireless LAN configuration.



A backbone wired LAN, such as Ethernet, supports servers, workstations, and one or more bridges or routers to link with other networks. A control module (CM) acts as an interface to a wireless LAN. The module includes either bridge or router functionality to link the wireless LAN to the backbone and some sort of access control logic, such as a polling or token-passing scheme, to regulate access from the end systems. Some of the end systems are stand-alone devices, such as a workstation or a server. Hubs or other user modules (UMs) that control several stations off a wired LAN may also be part of the configuration.

Single and multiple cells

Figure 1 shows the single-cell configuration—a simple wireless LAN strategy typical of many environments. It is so named because all the wireless end systems are within range of a single control module. Another common configuration is a multiple-cell wireless LAN, in which a wired LAN connects multiple control modules. Each control module supports wireless end systems within its transmission range. An infrared LAN, for example, limits transmission to a single room, so each room in an office building would need one cell.

Nomadic access

In this configuration, the wireless LAN links a LAN hub and a mobile data terminal equipped with an antenna, such as a laptop or notepad computer. Thus, for example, an employee returning from a trip can transfer data from a personal portable computer to an office server. Nomadic access is also useful in an extended environment such as a campus or a business operating from a cluster of buildings. In both cases, users can move around with their portable computers and access the servers on a wired LAN from various locations.

Ad hoc network

This network is set up temporarily to meet some immediate need. It has no centralized server. Thus, in meetings, a group of employees, each with a laptop or palmtop computer, can link their computers in a network that lasts just as long as the meeting.

WIRELESS LAN REQUIREMENTS

As these configurations show, wireless LANs must meet requirements typical of any LAN, including high capacity, ability to cover short distances, full connectivity among attached stations, and broadcast capability. They must also meet requirements specific to their intended environment.

- **Throughput.** The medium access control (MAC) protocol should use the wireless medium as efficiently as possible to maximize capacity. The "What is the MAC Protocol?" sidebar describes this protocol in more detail.
- **Number of nodes.** Wireless LANs may need to support hundreds of nodes across multiple cells.
- **Connection to backbone LAN.** Most applications require interconnection with stations on a wired backbone LAN. Wireless LANs easily satisfy this requirement by using control modules that connect to both types of LANs. Applications may also require accommodating mobile users and ad hoc wireless networks.
- **Service area.** A typical coverage area for a wireless LAN has a diameter of 100 to 300 meters.
- **Battery life.** Mobile workers use battery-powered workstations that must have a long battery life when used with wireless adapters. Thus, the wireless LAN's MAC protocol typically should not require mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station. Typical wireless LAN implementations have features to reduce power consumption when the network is not being used, such as sleep mode.
- **Transmission robustness and security.** If not properly designed, a wireless LAN may be prone to interference, making it easy for intruders to eavesdrop. A properly designed wireless LAN permits reliable transmission, even in a noisy environment, and provides some level of security from eavesdropping.
- **Collocated network operation.** As wireless LANs become more popular, multiple wireless LANs are

likely to operate in close proximity. Consequently, a device assigned to one LAN may be able to transmit or receive without authorization on a nearby LAN. To prevent this, the wireless LAN scheme must use addressing and access control techniques.

- **License-free operation.** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band the LAN uses.
- **Handoff/roaming.** The MAC protocol the wireless LAN uses should let mobile stations move from one cell to another.
- **Dynamic configuration.** The MAC protocol's provision for addressing and network management should let organizations dynamically and automatically add, delete, or relocate end systems without disrupting other network users.

BALANCING STANDARDIZATION AND FLEXIBILITY

With so many possible applications and wireless configurations and the need to meet the specific requirements of wireless environments, some standardized approach to product creation is imperative. Without it, equipment from various vendors would not work together. But flexi-

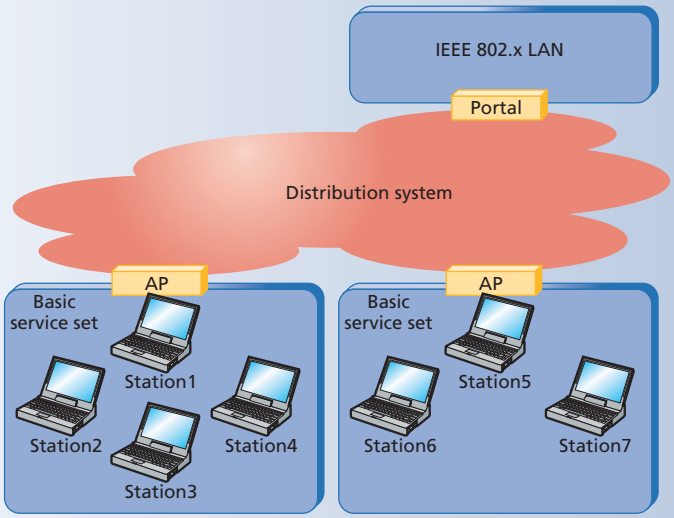
What Is the MAC Protocol?

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 fashion. This responsibility falls to the *medium access control* protocol, which ensures that all the end systems on a LAN cooperate. The MAC protocol requires that only one station 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.

Every LAN architecture includes a MAC layer, which is responsible for detecting errors and discarding any erroneous frames. Each end system monitors the shared medium for frames whose destination address is a match with its address and copies those frames.

The MAC layer for IEEE 802.11 is rather complex (see Figure 3 in the main text). Unlike MAC in Ethernet, for example, it includes a distributed coordination function with a rudimentary priority scheme, in which all stations cooperate for medium access. It also includes a point coordination function, implemented in a central controller, to accommodate urgent

Figure 2. IEEE's 802.11's extended service set architecture.



The smallest building block of a wireless LAN is a basic service set, which consists of stations that execute the same MAC protocol and compete for access to the same shared wireless medium. A basic service set may be isolated or, as is the case here, connected to a backbone distribution system through an access point (AP), which functions as a bridge and is implemented as part of a station. A central coordination function housed in the access point controls the MAC protocol or the protocol may be fully distributed. The basic service set generally corresponds to a cell. The distribution system can be a switch, wired network, or wireless network. The portal integrates the IEEE 802.11 architecture with a traditional wired LAN. The portal logic is implemented in a device, such as a bridge or router, that is part of the wired LAN and attached to the distribution system.

bility is also an imperative because applications evolve and requirements change.

Recognizing the need to balance these two imperatives, the IEEE tasked a separate working group to develop a complete set of specifications for a wireless LAN, including the details of the frequency used, transmission method, means of controlling access by various devices to the LAN, and security issues. The proposed specifications, IEEE 802.11, had to be flexible enough to satisfy a range of requirements and intended applications.

Work began on the original 802.11 in 1990. In 1999, at roughly the same time, the IEEE issued 802.11a and 802.11b. These three standards differ only in the physical layer of their architecture.

802.11 architecture

In the architecture's simplest form, each station *belongs* to a single basic service set—meaning that it is typically within wireless range of only the stations that also belong to that set. The exception is when two basic service sets overlap geographically, making the range narrow enough for a single station to participate in both sets. The association between a station and its basic service set is dynamic. Stations can turn off, come within range, and go out of range.

Figure 2 shows a more complex form of the 802.11 architecture—an extended service set—in which a distribution system connects two or more basic service sets. Typically, the distribution system is a wired backbone LAN, but it can be any communications network. The extended service set appears as a single logical LAN to the logical link control level (described later). The access point is the logic within a station that provides access to the distribution system by providing services in addition to acting as a station.

802.11 services

IEEE 802.11 defines several services that the wireless LAN must provide if its usefulness is to match the functionality inherent in wired LANs.

Association. Before a station can transmit or receive frames on a wireless LAN, it must make its identity and address known. To do so, it establishes an association with an access point. The access point can then communicate this information to other access points, which makes it easier to route and deliver addressed frames. The reassociation service makes it possible for an established association to transfer from one access point to another, which is what lets a mobile station move. The disassociation service makes it possible for either a station or an access point to notify other access points that an existing association is terminated. A station should give this notification before leaving an area or shutting down.

Authentication Security. In wired LANs, stations establish their identity with other stations through a physical connection. The assumption is that access to that connection conveys the authority to connect to the LAN. With wireless LANs, however, users can establish a connection merely by having an attached antenna that is properly tuned. Stations must use an authentication service to establish their identity with other stations. IEEE 802.11 does not mandate any particular authentication scheme, which could be anything from relatively unsecure handshaking to public-key encryption. It does, however, specify two authentication algorithms, which vendors can decide to include in their products. It is then up to the buyer to pay for the extra capability.

The first is *open-system* authentication, in which two parties simply agree to exchange identities before sending data. One party sends a MAC control frame (see the "What Is the MAC Protocol?" sidebar), which indicates that this is an open system authentication exchange. The other party responds with its own authentication frame, and the process is complete.

In the second algorithm, *shared-key* authentication, the two parties share a secret key that no other party has, and the key is the basis for authentication. A handshaking protocol enables the two sides to verify that each has that key.

Privacy. With a wireless LAN, eavesdropping is a major concern because of the ease of capturing a transmission. To assure privacy, IEEE 802.11 provides for the optional use of encryption by specifying a scheme based on the Wired Equivalent Privacy (WEP) algorithm. To provide both privacy and data integrity, the WEP algorithm uses an encryption scheme based on the RC4 encryption algorithm. The idea in RC4 is that two communicating parties must share a 40-bit key, which encrypts and decrypts all frames. Although the 40-bit key provides only a modest level of security, it is enough to protect against casual eavesdroppers. For much stronger protections, some 802.11 vendors offer optional 128-bit encryption.

802.11 protocol layers

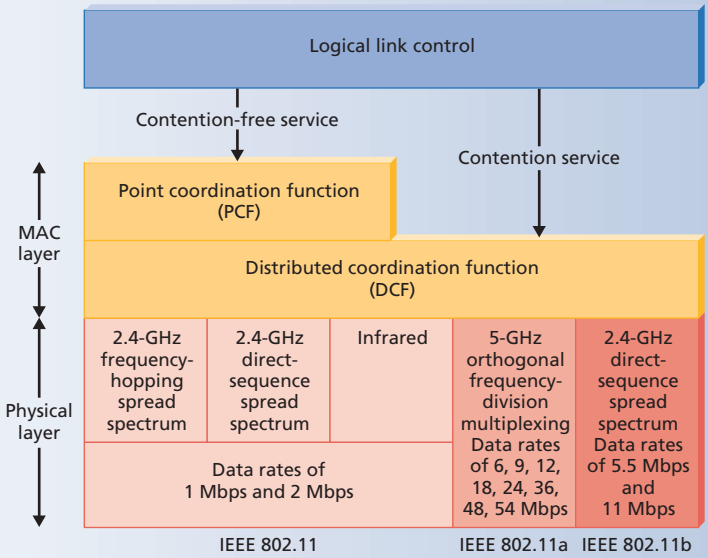
Figure 3 shows the standard's layered protocol architecture.

The top and middle layers define a rather complex set of mechanisms for regulating access to the LAN and for providing security. The physical layer specifies the actual transmission details and has been the focus of much work in the past three years.

The IEEE issued the physical layer for 802.11 in three stages. The first part, issued in 1997, is called simply IEEE 802.11. As Figure 3 shows, it includes the MAC layer and three physical layer specifications—all operating at data rates of 1 and 2 Mbps:

- direct-sequence spread spectrum (DS-SS), operating in the 2.4-GHz ISM (Industrial, Scientific, and Medical) band;
- frequency-hopping spread spectrum (FHSS), operating in the 2.4-GHz ISM band; and
- infrared, operating at a wavelength between 850 and 950 nm.

Figure 3. IEEE's 802.11's layered protocol architecture.



The lowest (physical) layer, defines the frequency band, data rate, and other details of the actual radio transmission. Above the physical layer is the medium access control (MAC) layer, which regulates access to the shared radio frequency band so that station transmissions do not interfere with one another. 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 stations in turn. Higher-priority traffic—traffic with greater timing requirements—uses this coordination function. Finally, the logical link control layer provides an interface to higher layers and performs basic link-layer functions such as error control.

The infrared option never gained market support because it requires unobstructed line-of-sight and because the available data rates are limited. The other two schemes use spread-spectrum approaches, which require a much wider bandwidth than is actually necessary to support a given data rate. The idea behind using the wider bandwidth is to minimize interference and drastically reduce the error rate. The FHSS scheme achieves spread spectrum by frequently jumping from one carrier frequency to another; thus, any interference or performance degradation at a given frequency affects only a small fraction of the transmission.

The DS-SS scheme increases a signal's data rate by mapping each data bit into a string of bits, with one string used for binary 1 and another for binary 0. The higher data rate uses a greater bandwidth. The idea is to spread each bit

Table 1. WECA-certified interoperable 802.11b products (as of April 2001).

Company	Product
3Com	AirConnect 11Mbps Wireless LAN PCI Card AirConnect 11Mbps Wireless LAN Access Point AirConnect 11Mbps Wireless LAN Access Point 2.0 AirConnect 11Mbps Wireless LAN PC Card AirConnect 11Mbps Wireless LAN PC Card 2.0 Home Wireless Gateway
Acer	Access Point Warplink 2412 IEEE 802.11b WLAN PC Card Model Warplink 2411
Acrowave	AWL-1100C PCMCIA Card Station Card PCI Model AWL-1100P
Actiontec	802.11 Wireless LAN PC Card
Ambit	Station Card LAN-Express Model T60L198
Apple Computer	AirPort Base Station AirPort Client Card
Askey	11Mbps Wireless LAN PC Card Model WLC010
Atmel	PCMCIA Station Card Model AT76C502
Buffalo	AirStation Access Point WLA-L11 AirStation Access Point WLAR-128 AirStation Access Point WLAR-L11 AirStation Access Point WLAR-L11-L AirStation Access Point WLAR-L11-M AirStation Access Point WLAR-L11-S AirStation Wireless LAN Card WLI-PCM-L11
Cisco	Aironet 340 Series Access Point Aironet 340 Series PCI Card Aironet 340 Series Wireless PC Card
Compaq	WL100 11Mbps Wireless LAN PC Card WL200 11Mbps Wireless LAN PCI Card WL300 11Mbps Wireless LAN Software Access Point WL400 11Mbps Wireless LAN Hardware Access Point
ELSA	AirLancer MC-11 Station Card LANCom Wireless IL-11 Access Point
EMTAC	11Mbps WLAN PC Card A2424
Enterasys	RoamAbout 802.11b DS High Rate PC Card RoamAbout Access Point 2000
Eumitcom	PC Card WL-11000-1 PC Card WL-11000-P
Fujitsu	Wireless Access Point Model No. FMWT-501 (in Japanese only) Wireless LAN Card, Model No. FMV-JW181 (in Japanese only)
IBM	Access Point Model 9085 High Rate Wireless LAN PC Card Model 09N9863 High Rate Wireless LAN PC Card- 12D4
Intel	PRO/Wireless 2011 LAN Access Point PRO/Wireless 2011 LAN PC Card
Intermec	2101 Universal Office Access Point Access Point Model 2100 Access Point Model 2102 Station Card Radio Model 2126 PC Card Type II Integrated
Intersil	PRISM II Station Card Model HWB3163-04-Ref-Rev B5
Lucent	Access Point Model AP-1000 Access Point Model AP-500 Orinoco PC Card – Gold Orinoco PC Card – Silver Orinoco WavePoint-II Access Point
NEC	Access Point Model 336-0106697 Wireless LAN Card Model 136-277158
NextComm	Wireless PC Card – Mirror Model 700-0002
Nokia	A032 WLAN Access Point A040 Ethernet WLAN Adapter C110 Wireless LAN Card C111 Wireless LAN Card
NTT-ME	MN 128 SS-LAN Card 11
Proxim	Harmony 802.11 PC Card Model 8432
Samsung	SWL-2000N 11Mbps Wireless LAN PC Card SWL-2000P 11Mbps Wireless LAN PCI Card
Siemens	PC Card Model I-Gate 11M PC Card / V4411-Z9-X1 PC Card Model I-Gate 11M PCI / V4411-Z11-X1
Sony	Wireless LAN PC Card PCWA-C100
Symbol	Spectrum24 Access Point Model AP4121 Spectrum24 High Rate 11Mbps Access Point Spectrum24 High Rate 11Mbps Wireless LAN Adaptor Model LA4121 Spectrum24 High Rate 11Mbps Wireless LAN PC Card
Toshiba	Wireless LAN Mini-PCI Card / PA3070U-1MPC Wireless LAN PC Card / PA3064U-1PCC
Z-COM	LANEscape Wireless Station Card Model XI-300
ZoomAir	Wireless PC Card Wireless Software Access Point

out over time, which minimizes effects from interference and degradation.

Most of the early 802.11 networks used the FHSS scheme, which is simpler. Networks that used the DS-SS scheme were more effective, but all the original 802.11 products had data rates of at most 2 Mbps, which limited their usefulness.

In 1999,the IEEE issued the second and third physical layers, IEEE 802.11a and IEEE 802.11b, at roughly the same time. IEEE 802.11a operates in the 5-GHz band at data rates up to 54 Mbps. IEEE 802.11b operates in the 2.4-Ghz band at 5.5 and 11 Mbps. Because 802.11b is easier to implement, it has yielded products first.

802.11b

IEEE 802.11b extends the IEEE 802.11 DS-SS scheme, providing data rates of 5.5 and 11 Mbps through the use of a more complex modulation technique.

Resources

Web sites

- **IEEE 802.11 Wireless LAN Working Group (http://grouper.ieee.org/groups/802/11/index.html): This site contains working group documents plus discussion archives.**
- **Wireless Ethernet Compatibility Alliance (http://www.wirelessethernet.org): This industry group promotes the interoperability of 802.11 products with each other and with Ethernet.**
- **Wireless LAN Association (http://www.wlana.com): Besides an introduction to the technology, this site includes a discussion of implementation considerations and case studies from users.**

Books

- ***Wireless LANs*, J. Geier, Macmillan Tech. Pub., New York, 1999. This book contains detailed coverage of all the IEEE 802.11 standards with numerous case studies.**
- ***IEEE 802.11 Handbook: A Designer's Companion*, B. O'Hara and A. Petrick, IEEE Press, New York, 1999. Excellent technical treatment of IEEE 802.11.**
- ***Wireless Communications and Networks*, W. Stallings, Prentice Hall, Upper Saddle River, N.J., 2001. Detailed technical coverage of wireless LANs and all the IEEE 802.11 standards.**

The 802.11b specification quickly led to product offerings, including chip sets, PC cards, access points, and systems. Apple Computer was the first to field 802.11b products, offering the AirPort wireless network option to users of its iBook portable computer. Other companies, including Cisco, 3Com, and Dell, have followed.

Although all these products are based on the same standard, potential users still worry that products from different vendors may not interoperate successfully. Recognizing this concern, the Wireless Ethernet Compatibility Alliance (WECA) created a test suite to certify interoperability for 802.11b products. Interoperability tests have been going on since early 2000 and a number of products have achieved certification. Table 1 lists the WECA-certified products available as of April 2001.

802.11a

Although 802.11b is successful to some degree, the data rate is still too low for applications that need a truly high-speed LAN. IEEE 802.11a targets this specific need. Unlike the other 802.11 standards, it specifies the 5-GHz band, and it replaces the spread-spectrum scheme with the faster orthogonal frequency-division multiplexing. OFDM, also called multicarrier modulation, uses up to 52 carrier signals at different frequencies, sending some of the bits on each channel. Possible data rates are 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

First-generation 802.11a products should appear by the end of 2001, with WECA interoperability and compliance testing also beginning by that time.

OVERCOMING OBSTACLES

One concern for original 802.11 and 802.11b products is interference with other systems that operate in the 2.4-GHz band, such as Bluetooth, HomeRF, and with many other devices that use the same portion of the spectrum, including baby monitors and garage door openers. A coexistence study group, IEEE 802.15, is examining this issue and so far the prospects are encouraging. The idea is to provide mechanisms that let devices from the two types of LANs exchange information and cooperate to minimize mutual interference.

As more IEEE 802.11-compliant products become available, security has become another major issue. Wireless LANs are uniquely vulnerable to both eavesdropping and unauthorized transmission because transmission is wireless rather than confined to a cable. The IEEE 802.11 standard has provided for ways to address these concerns, and more vendors should routinely implement the security portion of the standard as part of their offerings.

With these security features in place, IEEE 802.11 is poised to have a significant impact on the LAN marketplace. As the demand for mobility and freedom from wiring requirements increases, the standard offers a comprehensive yet flexible approach to wireless LAN products. ■

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.* ¶