Chapter 7

1: What types of user devices are most common with wireless WANs?

A1: Answer: Laptops, PDAs, and mobile phones.

2: Why do wireless WAN operators always charge for services?

A2: Answer: Wireless WANs are expensive to install.

3: Why must you be careful when selecting a wireless WAN radio NIC for your user device?

A3: Answer: There are many different types of wireless WANs that are not compatible with each other.

4: What is an advantage of a satellite system?

A4: Answer: It can cover vast areas. A single satellite can cover roughly one-third of the Earth's surface.

5: Which generation of cellular systems offers data rates up to 2 Mbps?

A5: Answer: Third generation (3G).

6: Which type of wireless WAN system is most common?

Exhibit 1010
Page 275 of 292

A6: Answer: Cellular systems.

7: Which of the two following cellular systems offers the highest data rates: GPRS or UMTS?

A7: Answer: UMTS.

8: What is the primary issue with meteor burst communications?

A8: Answer: Low data rates.

9: True or false: FDMA requires users to take turns transmitting signals.

A9: Answer: False.

10: How does CDMA keep users from interfering with each other?

A10: Answer: Each user transmits using a different code.

Exhibit 1010
Page 276 of 292

Chapter 8

1: What are the three major security threats of a wireless network?

A1: Answer: Traffic monitoring, unauthorized access, and DoS.

2: What is the primary means for guarding against traffic monitoring?

A2: Answer: Utilize encryption.

3: How do you keep hackers from gaining access to company resources through the wireless network?

A3: Answer: Incorporate the use of effective authentication.

4: What method will help alleviate the implications of a successful DoS attack?

A4: Answer: Have an alternative plan to carry on business in a manner that doesn't require the use of the wireless network.

5: Why is WEP not acceptable for protecting sensitive information?

A5: Answer: Hackers are able to crack the WEP encryption algorithm through the use of publicly available tools.

Exhibit 1010
Page 277 of 292

6: How is TKIP different than WEP?

A6: Answer: TKIP make use of a dynamic key distribution mechanism that updates keys periodically, whereas WEP makes use of static keys that don't change.

7: WPA uses TKIP and is a subset of the 802.11i standard. True or false?

A7: Answer: True.

8: Why is the use of MAC address filters not effective?

A8: Answer: It's difficult to manage and easy to spoof.

9: What is a rogue access point, and why does it pose a problem?

A9: Answer: A rogue access point does not have any security features set and is put in by a hacker or employee. The rogue access point offers an open port to the network for hackers to exploit.

10: What should you install on a laptop that a user will utilize on a public wireless LAN to avoid unauthorized people from accessing files on the laptop?

A10: Answer: Personal firewall.

Exhibit 1010
Page 278 of 292

Glossary

1G cellular
The initial (first-generation) cellular phone system that used analog signaling. This system did not effectively support the transmission computer data.

2G cellular
The first cellular phone system (second-generation) that used digital signaling that supports data rates of under 20 kbps.

3G cellular
A modified (third-generation) version of 2G cellular that offers better support for data communications, such as higher data rates.

802.11
A standard published by the IEEE that defines the radio characteristics and operation of a medium-range radio frequency LAN. Specifies the use of CSMA as the primary method for sharing access to a common air medium.

802.15
A standard published by the IEEE that defines the radio characteristics and operation of wireless PANs. 802.15 is based on the Bluetooth specification.

802.16
A standard published by the IEEE that defines the radio characteristics and operation of wireless MANs.

802.3

A standard published by the IEEE that defines the signal characteristics and operation of a wired local-area network. Defines the use of CSMA, which is similar to 802.11 wireless LANs.

access point
A type of base station that wireless LANs use to interface wireless users to a wired network and provide roaming throughout a facility.

ad hoc mode
A configuration of a wireless network that allows communications directly from one user device to another, without the need to travel through a base station. Ad hoc mode applies to both wireless PANs and wireless LANs.

analog signal
A signal whose amplitude varies continuously as time progresses. A radio wave is an example of an analog signal.

antenna
A physical device that converts electrical signals to radio or light waves—and vice versa—for propagation through the air medium. Antennae may be omnidirectional, which distributes radio waves in all directions, or directional, which focus the radio waves more in one direction than others.

association
A process whereby an 802.11 station (computer device) becomes a part of the wireless LAN. After association, the user can utilize network services.

authentication
The process of proving the identity of a user or base station. The use of usernames and passwords is a common authentication method, but many other, more-sophisticated authentication mecha-

Exhibit 1010
Page 280 of 292

nisms exist. For example, digital certificates can offer a means of authentication without user intervention.

base station
Hardware that interfaces wireless computing devices together and to a wired network. Access points and wireless routers are types of wireless LAN base stations.

Bluetooth
A specification published by the Bluetooth Special Interest Group that defines the radio characteristics and operation of a short-range, low-power radio frequency network. Many devices today support Bluetooth, but 802.15 is developing applicable standards.

bridge
A device that interconnects two networks at Layer 2. A bridge forwards data packets to another network based on the MAC address found in the packet header. Bridges play a key role in the deployment of wireless MANs.

carrier sense access
A process of sharing a common medium by first determining whether the medium is idle before transmitting data. This is part of the CSMA protocol.

carrier signal
The primary RF signal that carries data through the air medium. Various modulation types vary the carrier signal frequency, phase, or amplitude to represent information.

CDMA (code division multiple access)
A process where each user modulates their signals with a different, noninterfering code.

CDPD (Cellular Digital Packet Data)

Exhibit 1010
Page 281 of 292

A technology that enables the transmission of data over analog cell phone systems with data rates of 19.2 kbps. CDPD is becoming obsolete as newer 3G systems are becoming available.

CF (CompactFlash)
A small NIC for PDAs, cameras, and other small computer devices. Bluetooth and 802.11 CF NICs are readily available.

client device
Hardware having a user interface that enables the use of wireless network applications. Client device is another name for computer device.

computer device
Any end point of a wireless network, such as a laptop, PDA, or robot. The computer device is often referred to as a client device.

CSMA (carrier sense multiple access)
A process that allows multiple 802.11 stations to share a common air medium. Stations attempt to only transmit data when no other station is transmitting. Otherwise, collisions will occur and the station must retransmit the data.

data
Information, such as electronic files, that is stored and sent over a wireless network. Often data are sent in multiple packets, which are sent separately through the network.

data rate
The number of bits per second (bps) that data is sent. For example, 802.11b wireless LANs operate at up to 11 Mbps.

DCF (distributed coordination function)
A part of the 802.11 standard that defines how stations will contend for access to the air medium. DCF makes use of CSMA to regulate traffic on the network.

Exhibit 1010
Page 282 of 292

DHCP (Dynamic Host Configuration Protocol)
A protocol that automatically assigns unique IP addresses within an assigned range to network devices. Most home and public wireless LANs implement DHCP, making it easy for users to gain access to the network. DHCP automatically assigns a valid IP address to these users.

digital certificate
An electronic message that contains the credentials of a particular user. Digital certificates are used as a means for authenticating users or their computer devices.

digital signal
A signal that varies in amplitude steps as time advances. The digital signal represents data within a computer device. The digital signal must be converted to an analog form—known as modulation—before the data can be sent through the air medium.

DSSS (direct sequence spread spectrum)
A type of spread spectrum where a spreading code increases the signal rate of the data stream to diffuse the signal over a wider portion of the frequency band. 802.11b wireless LANs make use of direct sequence.

directional antenna
A type of antenna that focuses radio waves and range more in one direction than others. Directional antennae are commonly found in wireless MANs and wireless WAN systems. The directivity of the antenna increases range in one direction and decreases range in other directions.

distribution system
A wired system that physically interconnects access points in a wireless LAN. A common distribution system for wireless LANs, for example, is Ethernet.

Exhibit 1010
Page 283 of 292

encryption
The scrambling of data bits according to a key prior to sending the data over a network. WEP and WPA are examples of encryption that wireless LAN utilize.

Ethernet
A name that depicts 802.3 wired LANs. Ethernet is a common type of network that companies use to interconnect PCs and servers. Ethernet provides the distribution system of most wireless LANs.

FDMA (frequency division multiple access)
A process that divides a relatively wide frequency band into smaller subbands, where each user transmits voice and data over an assigned subband.

FHSS (frequency hopping spread spectrum)
A type of spread spectrum where the transceiver hops from one frequency to another, according to a known hopping pattern, to spread the signal over a wider portion of the frequency band. Older 802.11 wireless LANs utilize frequency hopping.

firewall
A device that keeps users connecting to a specific part of the network from accessing important resources. Because of their vulnerability, access points of wireless LANs are often placed outside the firewall.

frequency
The number of times per second that a signal repeats itself. Often measured in Hertz (Hz), which is the number of cycles occurring each second. Frequencies of wireless LANs, for example, are within the 2.4-GHz and 5-GHz bands.

FSK (frequency shift-keying)

Exhibit 1010
Page 284 of 292

A modulation process that makes slight changes to the frequency of the carrier signal to represent information in a way that's suitable for propagation through the air.

GPS (global positioning system)
A system that enables people having a GPS client device to easily determine their geographical position. GPS offers the basis of an excellent navigation system, as well as location-based services over wireless networks.

hacker
A person who has the desire and ability to steal information that resides on a network. Hackers often try breaking into corporate systems for fun and to exploit the vulnerabilities of wireless networks.

hotspot
The location of a public wireless LAN. Hotspots are found within areas where people congregate with computer devices including airports, hotels, convention centers, and coffee shops.

interference
Unwanted signals that disrupt the operation of a wireless network. The presence of interference decreases the performance of a wireless network.

interoperability
A condition where computer devices are able to successfully interface with a wireless network.

IP (Internet Protocol)
A protocol that routes packets between computer devices attached to a network. The IP places a header field in front of each packet that contains the source and destination IP address of the packet.

IP address

Exhibit 1010
Page 285 of 292

A numerical address corresponding to a connection of a network device to the network. For example, every wireless network NIC will have an IP address. Each NIC must have an IP address associated with it if the user will be making use of TCP/IP applications, such as sending and receiving e-mail, browsing the web, or interfacing with a corporate application server.

IPSec (IP Security)
A protocol that supports secure exchange of packets at the network layer of a network. IPSec is commonly implemented in VPNs and encrypts data packets across the entire network; often referred to as end-to-end encryption.

IrDA (Infrared Data Association)
A standard specifying an interoperable, low-cost, low-power, serial data communications standard for short-range applications. IrDA is found in many laptops and PDAs.

LDAP (Lightweight Directory Access Protocol)
A protocol that enables accessing information directories.

location-based services
The ability to track the location of users and deliver information to them that relates to position within a particular area.

medium access control (MAC) layer
A part of a network architecture that manages and maintains communications on a shared medium. The MAC layer is the brains of a NIC or base station and enforces the rules all devices must follow.

medium
The space in which communications signals, such as radio waves, propagate. With wireless networks, the medium is air.

medium access

Exhibit 1010
Page 286 of 292

A process whereby multiple computer devices share a common medium. The most common medium access method for wireless networks is CSMA.

modulation
Modulation creates a radio or light signal from the network data so that it is suitable for propagation through the air medium. Examples of modulation types are FSK, PSK, and QAM.

NAT (Network Address Translation)
A protocol that maps official IP addresses to private addresses that may be in use on their internal networks. For example, a broadband Internet service provider may offer only one official IP address to a home owner. NAT, along with DHCP, enables the homeowner to have multiple PCs and laptops sharing the single official IP address.

NIC (Network Interface Card)
A hardware device that interfaces a computer device to a network. Also known as radio card and client card.

noise floor
The amplitude of electromagnetic signals in a particular area while the wireless network is not operating.

OFDM (orthogonal frequency division multiplexing)
A process that divides a modulated signal into multiple subcarriers, prior to transmission, through the air medium to improve performance. 802.11a and 802.11g wireless LANs, and some proprietary wireless MANs, utilize OFDM.

optical fiber
A long piece of small-diameter glass with a covering that carries light signals. An optical fiber cable has a protective coating, making it difficult to distinguish from copper-based cables.

Exhibit 1010
Page 287 of 292

PC Card

A credit-card–sized device that provides extended memory, modems, connectivity to external devices, and wireless network capabilities to small computer devices, such as laptops and PDAs. Many PC Cards implement Bluetooth and 802.11 technologies.

PDA (personal digital assistant)

A small device that people use to store contact information, schedules, and to-do lists. Some PDAs run software programs, such as e-mail clients and web browsers.

point-to-multipoint system

A system where communications is directly from one user to several others.

point-to-point system

A system where communications is directly from one user to another.

PSK (phase shift keying)

A modulation process that makes slight changes to the phase of the carrier signal in order to represent information in a way that's suitable for propagation through the air.

public wireless LAN

A type of wireless LAN, often referred to as a hotspot, that anyone having a properly configured computer device can access.

QAM (quadrature amplitude modulation)

A modulation process that makes slight changes to the amplitude and phase of the carrier signal to represent information in a way that's suitable for propagation through the air.

radio NIC

A type of NIC that transmits and receives RF signals.

Exhibit 1010
Page 288 of 292

RADIUS (Remote Authentication Dial-In User Service)
An authentication and accounting system that many WISPs use to handle access control and billing on wireless networks.

repeater
A device that receives and retransmits signals for the sole purpose of extending range.

RF signal
A radio frequency signal that is designed to propagate through the air medium.

rogue access point
An access point that is unauthorized and has configuration settings that might enable someone to gain access to network resources.

router
A type of base station that implements special networking protocols, such as DHCP and NAT, which enable users to use TCP/IP applications.

satellite
A signal repeater located in orbit around the Earth. Satellites offer wireless WAN coverage using radio signals.

snooper
Someone who casually—and usually inadvertently—disrupts a wireless network.

spread spectrum
The spreading of the carrier signal over a wider part of the frequency spectrum. Direct sequence and frequency hopping are two types of spread spectrum.

TCP (Transmission Control Protocol)

Exhibit 1010
Page 289 of 292

A protocol that establishes and maintains connections between computer devices attached to a network. TCP is used in conjunction with IP, which is commonly referred to as TCP/IP.

TDMA (time division multiple access)
A process that allows only one user to transmit in any given time slot. Each user has use of the entire bandwidth during its assigned time slot.

terminal emulation
A mechanism for users to interface over a network to applications running on a centralized computer. VT-220, 3270, and 5250 are types of terminal emulation.

transceiver
A device that both transmits and receives information. The transceiver resides in a radio NIC.

VPN (virtual private network)
The use of special software on the client device that controls access to remote applications and secures the connection from end to end using encryption.

WEP (Wired Equivalent Privacy)
A part of the 802.11 standard that defines encryption between devices connected to a wireless LAN.

Wi-Fi
A brand name given to wireless LANs that comply with standards as defined and published by the Wi-Fi Alliance. Wi-Fi standards are based on the 802.11 standard.

Wi-Fi Protected Access (WPA)
A security protocol, defined by the Wi-Fi Alliance, that enables computer devices to periodically obtain a new encryption key. WPA version 1 implements Temporal Key Integrity Protocol (TKIP) and

Exhibit 1010
Page 290 of 292

WEP; whereas, WPA version 2 implements the full 802.11i standard (which includes AES).

wireless LAN
A network that satisfies wireless networking needs within the area of a building or college campus. 802.11 and Wi-Fi are popular standards defining wireless LANs.

wireless MAN
A network that satisfies wireless networking needs within the area of a city. Wireless MANs make use of 802.16 and proprietary standards.

wireless PAN
A network that satisfies wireless networking needs within a small room or reach of a person. Bluetooth and 802.15 are popular technologies for wireless PANs.

wireless WAN
A network that satisfies wireless networking needs over a large geographical area, such as a country or continent. Satellites offer a means for extending radio signals over a wireless WAN.

WISP (wireless Internet service provider)
A company that offers wireless connection services to the Internet for homes and offices. WISPs often provide wireless access in public wireless LAN hotspots.

Exhibit 1010
Page 291 of 292

Index

Exhibit 1010
Page 292 of 292