Exam : PW0-100

Title : Wireless LAN Administration Certified Wireless Network Administrator (CWNA)

Ver : 05.08.08

QUESTION 1:

Which of these are NOT valid Service Set types as defined by the IEEE 802.11 standard?

A. BSS
B. IBSS
C. ESS
D. DSS

Answer: D

Explanation:
There are three types of Service Set: Basic Service Set (BSS), Extended Service Set (ESS), and Independent Basic Service Set (IBSS). (Reference: CWNA Study Guide, p. 218.)

QUESTION 2:

Which of the following is true of RF propagation communication?

A. The range of RF transmissions increases with frequency.
B. Low RF signal strength does not mean poor communications.
C. Low signal quality does not necessarily mean poor communications.
D. Due to the distances involved, sunspots do not affect RF communications.

Answer: B

Explanation:
1. The range of RF transmissions increases with greater transmitting power, not frequency. (CWNA Study Guide, p. 261)
2. Low RF signal strength will propagating in short range. (CWNA Study Guide, p. 261)
3. Low signal quality might occur when the RF waves scatter on uneven surface. (CWNA Study Guide, p. 52)
4. CWNA Study Guide did not mention anything about the sunspots and its effects.

QUESTION 3:

A point-to-point link between two buildings requires at least two of which device?

A. Workgroup Bridge
B. Access Point
C. Wireless Bridge
D. Ethernet Converter

Answer: A, B, C

Explanation:
Workgroup Bridge, Access Point, and Wireless Bridge with high-powered antennas can be used to establish a point-to-point link between two buildings. (CWNA Study Guide, Chapter 4: Infrastructure Devices)

QUESTION 4:

Which type of the following are directional antennas? Select all that apply,

A. Yagi
B. Parabolic Dish
C. Patch
D. Omni
E. Dipole
F. Bipolar

Answer: A, B, C, E

Explanation:
Yagi and Patch Antennas are the samples of semi-directional antennas. Dipole antenna is an omni-directional antenna. Parabolic Dish is one type of highly directional antenna. (CWNA Study Guide, p. 136-142)

QUESTION 5:

Which of the following can cause Multipath? (Choose three)

A. Body of water
B. Flat stretch of earth
C. Metal roof
D. Mountains
E. Trees
F. Concrete walls

Answer: A, B, C

Explanation:
Body of water, flat stretch of earth, and metal roof are considered to be smooth surface that can cause Multipath.
Reference should be Pages 394 & 400 CWNA Study Guide 3rd Edition
or Pages 328 & 334 CWNA Study Guide 2nd Edition

QUESTION 6:

Which of the following wireless LAN devices represent "legacy devices"? (Choose all that apply.

A. PCI Card
B. PC Card
C. ISA Card
D. USB adapter
E. Serial converter

Answer: C

Explanation:
PCI Card, PC Card, USB adapter and serial converter are not considered to be legacy devices. Don't get tricked by serial converter. Serial device is considered to be legacy device, not the converter itself.

QUESTION 7:

Which of these is required as part of a WLAN site survey? (Choose two)

A. Lightning arrestor.
B. Network manager interview.
C. Mobile access point.
D. VPN server.

Answer: B, C

Explanation:
Network manager interview and mobile access point are the requirements in order to have a successful WLAN site survey. (CWNA Study Guide, p. 349)

QUESTION 8:

Which of these items should be included in a RF Site Survey Report? (Choose two)

A. Cost estimated of equipment for a wireless LAN.
B. RF coverage drawings.
C. A list of potential interference sources.
D. Interviews with company executives on the requirements for a WLAN.
E. Security solution suggestions.

Answer: B, C

Explanation: RF coverage measurements and drawings & a list of potential interference

sources should be included in a RF Site Survey Report. Interviews with company executives on the requirements for a WLAN should be taken place BEFORE taking a site survey. Cost estimated of equipment for a wireless LAN should be calculated AFTER taking a site survey. (CWNA Study Guide, Chapter 11: Site Survey Fundamentals)

QUESTION 9:

The "hidden node" problem can be caused by?

A. Interfering obstacles between clients.
B. Clients broadcasting with too much power.
C. Access points broadcasting with too little power.
D. Clients being too close together.

Answer: A

Explanation:
Hidden node is a problem where two nodes can connect to an access point but they cannot connect to each other due to some obstacles or a large amount of distance between them. (CWNA Study Guide, p. 272)

QUESTION 10:

Antenna Diversity compensates for which of these common wireless LAN problems?

A. Near/Far
B. Hidden Node
C. Multipath
D. Adjacent Channel Interference

Answer: C

Explanation: In order to troubleshooting multipath successfully, antenna diversity is needed to compensate the certain conditions. (CWNA Study Guide, p. 270)

QUESTION 11:

Which authentication, authorization, and accounting (AAA) support options does the 802.11 standard specify?

A. RADIUS
B. LDAP
C. TACACS+
D. None of the above

Answer: D
Explanation. 802.11i (not 802.11) standard supports AAA.

QUESTION 12:

To achieve 54 Mbps, 802.11a uses which type of data modulation?

A. QFSK
B. BPSK
C. 64QAM
D. CCK

Answer: C

Explanation: On page 221 of the CWNA study Guide (2nd edition) it is mentioned that the 802.11a standard specifies the use of the ODFM technology. ODFM is the secret behind how 802.11a gets up to 54 Mbps data rates. In the answers given ODFM is not mentioned so this is something to think about.

QUESTION 13:

The IEEE 802.11 standard contains specifications on which of the following technologies?

A. 2.4 GHz FHSS, 2.4 GHz DSSS, Infrared
B. 2.4 GHz DSSS, 2.4 GHz FHSS
C. 2.4 GHz DSSS, Bluetooth
D. 2.4 GHz FHSS, Infrared

Answer: A

QUESTION 14:

Installing an extension cable to an antenna in a wireless LAN will have what effect? (Choose two)

A. The coverage distance of the antenna will be decreased.
B. The equivalent isotropically radiated power will be decreased.
C. There will be no effect
D. The RF signal power at the antenna input will be increased.

Answer: A, B

QUESTION 15:

Multipath can cause which of these effects at the receiving antenna? (Choose all that apply)

A. Increased signal amplitude.
B. Decreased signal amplitude.
C. Null signal.
D. Signal distortion.

Answer: A, B, C, D

QUESTION 16:

Which two of the following security issues exist with 802.11?

A. No support for encryption.
B. No support for roaming.
C. Vulnerable to disassociation attacks.
D. No central authentication, authorization, or accounting support.

Answer: C, D

Explanation: disassociation service - An IEEE 802.11 term that defines the process a station or
access point uses to notify that it is terminating an existing association.
Ref D:
opensystem authentication - The IEEE 802.11 default authentication method, which is a very simple, two-step process. First the station wanting to authenticate with another station sends an authentication management frame containing the sending station's identify. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.
the PPP authenticator merely passes through the
authentication exchange.

QUESTION 17:

Identify which of the following are appropriate uses of an IEEE 802.11 wireless LAN. (Choose all that apply)

A. Mobile access into the company network from a PDA.
B. "Core" role in an enterprise network.
C. Building-to-building bridging as a MAN solution.
D. Delivering data from applications that require full-duplex communications between nodes.

Answer: A, C

Explanation:
A: The most common component on any wireless network is the PCMCIA card. More

commonly known as "PC cards", these devices are used in notebook (laptop) computers and PDAs.
C: In addition to wireless LANs (WLANs), wireless personal area networks (WPANs), wireless metropolitan area networks (WMANs), and wireless wide area networks (WWANs) are also taking advantage of spread spectrum technologies. WPANs use Bluetooth technology to take advantage of very low power requirements to allow wireless networking within a very short range. WWANs and WMANs can use highly directional, high gain antennas to establish long-distance, high-speed RF links with relatively low power.

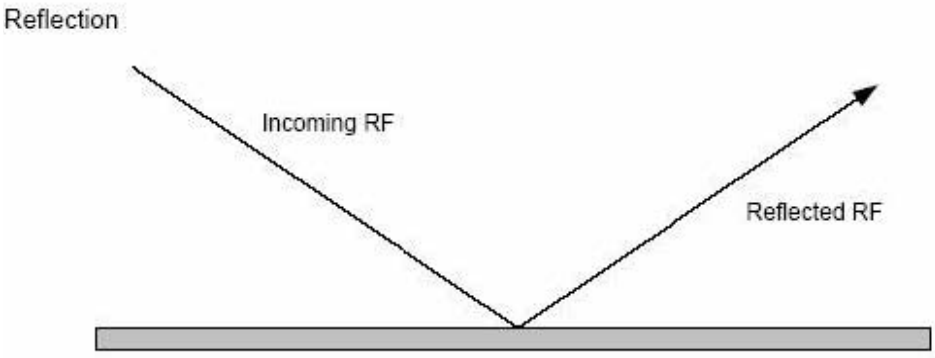
QUESTION 18:

The anomaly that occurs when RF signals propagate from a transmitter bounce off objects and then cause problems at the receiver is known as:

A. Fresnel Zoning
B. Multipath
C. Microwave interference
D. Diffraction

Answer: B

Explanation:



RF signal reflection can cause sericus problems for wireless LANs. This reflecting of the main signal from many objects in the area of the transmission is referred to as *multipath*. Multipath can have severe adverse affects on a wireless LAN, such as degrading or canceling the main signal and causing holes or gaps in the RF coverage area. Surfaces such as lakes, metal roofs, metal blinds, metal doors, and others can cause severe reflection, and hence, multipath.

QUESTION 19:

Which two functions can be configured on a WLAN client computer as part of the WLAN client utility software? (Choose two)

A. RADIUS username and password.

B. Connection speed.
C. Continuous Aware Mode.
D. Spanning Tree Protocol.
E. Bit ordering

Answer: B, C

Explanation:
B: Link status monitor utilities allow the user to view packet errors, successful transmissions, connection speed, link viability, and many other valuable parameters. There is usually a utility for doing real-time link connectivity tests so that, for example, an administrator would be able to see how stable a wireless link is while in the presence of heavy RF interference or signal blockage.
C: Wireless clients operate in one of two power management modes specified by the IEEE 802.11 standard. These power management modes are active mode, which is commonly called continuous aware mode (CAM) and power save, which is commonly called power save polling (PSP) mode

---

QUESTION 20:

Part of the roaming process involves? (Choose all that apply)

A. Implementing Mobile IP
B. Active Beacons.
C. Active Scanning.
D. Passive Scanning.

Answer: A, C, D

Explanation:
A: The layer 2 connection is still maintained by the access points, but since the IP subnet has changed while roaming, the connection to servers, for example, will be broken. Without subnet-roaming capability (such as with using a Mobile IP solution or using DHCP), wireless LAN access points must all be connected to a single subnet (a.k.a. "a flat network"). This work-around can be done at a loss of network management flexibility, but customers may be willing to incur this cost if they perceive that the value of the end system is high enough.
C D: The 802.11 standard does not define how roaming should be performed, but does define the basic building blocks. These building blocks include active & passive scanning and a reassociation process. The reassociation process occurs when a wireless station roams from one access point to another, becoming associated with the new access point.
The 802.11 standard allows a client to roam among multiple access points operating on the same or separate channels. For example, every 100 ms, an access point might transmit a beacon signal that includes a time stamp for client synchronization, a traffic indication map, an indication of supported data rates, and other parameters. Roaming clients use the beacon to gauge the strength of their existing connection to the access

point. If the connection is weak, the roaming station can attempt to associate itself with a new access point.

QUESTION 21:

The maximum aggregate capacity for an 802.11 DSSS system in a co-located environment is?

A. 2 Mbps
B. 6 Mbps
C. 22 Mbps
D. 24 Mbps

Answer: B

Explanation:
This question is slightly confusing.However, if read closely, it states that the system is in a "co-located" environment. From our previous discussion, since DSSS systems support a maximum of 3 APs in a co-located environment and given that the 802.11 standard allows speeds upto 2 Mbps, therefore, that would make the answer 2(x3) = 6Mpbs. Therefore, the answer should be B.

QUESTION 22:

After August 31, 2000, the FCC mandated that FHSS systems using fewer than 75 hops must have a maximum power output of?

A. 100mW
B. 125mW
C. 500MW
D. 1W

Answer: B

Explanation:
- a part of the 802.15 standard for WPANs (Wireless Personal Area Networks). Bluetooth is a close-range networking protocol primarily used for mobile devices, utilizing FHSS in the 2.4 GHz ISM band at around 1600 hops/second. Because of the high hop rate, Bluetooth devices will greatly interfere with other devices operating in the 2.4 GHz band.

QUESTION 23:

Which of the following us TRUE when using Bluetooth in an 802.11b environment?

A. Interference can be avoided by selecting different DSSS sub-channels

B. Interference can be avoided by allowing Bluetooth to use a proprietary hopping pattern.
C. Interference increases as distance between the two systems decreases.
D. Bluetooth does not interfere with DSSS.

Answer: C

Explanation:
Less than 75 hops enforces the Post August 31, 2000 rule for FHSS systems in which max. power is 125 mW and max. carrier frequency is 5 Mhz (See page 73 of the CWNA study Guide (2nd edition))

QUESTION 24:

Before going into a low-power state (sleep), what function must a wireless station operating in a BSS perform?

A. Notify the access point of its intention to sleep.
B. Notify other wireless stations of its intention to sleep.
C. Broadcast an ATIM on the network.
D. Send an RTS to the access point.

Answer: A

Explanation:
Traffic Indication Map (TIM) - transmitted by the access point to indicate to sleeping stations the presence of buffered transmissions for a particular station
Traffic Indication Map (TIM)
The TIM is used an as indicator of which sleeping stations have packets queued at the access point. This information is passed in each beacon to all associated stations. While sleeping, synchronized stations power up their receivers, listen for the beacon, check the TIM to see if they are listed, then, if they are not listed, they power down their receivers and continue sleeping.

QUESTION 25:

Which of the following are features included in the 802.11 standard? (Choose all that apply)

A. Support of asynchronous and time-bounded delivery service.
B. Use of the CSMA/CD and RTS/CTS protocols.
C. 802.1x with EAP support.
D. Wireless VPN tunnels with RADIUS authentication methods.

Answer: A

Explanation:

Point-to-Point Protocol (PPP) - A protocol that provides router-to-router and host-tonetwork connections over both synchronous and asynchronous circuits. PPP is the successor to SLIP.An IEEE 802.11 mode that enables contention-free frame transfer based on a priority mechanism; stations are polled for the need for frame transmission. Enables time-bounded services that support the transmission of voice and video

---

QUESTION 26:

Which of the following is a secure method of client device authentication onto a WLAN?

A. PLCP Login Layer
B. Open System Authentication
C. PMD Zones
D. CSMA/CA

Answer: B

Explanation:
The IEEE 802.11 standard specifies two methods of authentication: Open System authenticationand Shared Key authentication. The simpler and also the more secure of the two methods is Open System authentication
Open System Authentication
Open System authentication is a method of null authentication and is specified by the IEEE 802.11 as the default setting in wireless LAN equipment.Using this method of authentication, a station can associate with any access point that uses Open System authenticationbased only on having the right service set identifier (SSID). The SSIDs must match on both the access point and client before a client is allowed to complete the authentication process. Uses of the SSID relating to security will be discussed in Chapter 10 (Security).The Open System authentication process is used effectively in both secure and non-secure environments.
Open System Authentication Process
The Open System authentication process occurs as follows:
1. The wireless client makes a request to associate to the access point
2. The access point authenticates the client and sends a positive response and the client becomes associated (connected)

QUESTION 27:

A change in the direction and intensity of a group of waves after passing by an obstacle or the bending waves around an object is referred to as?

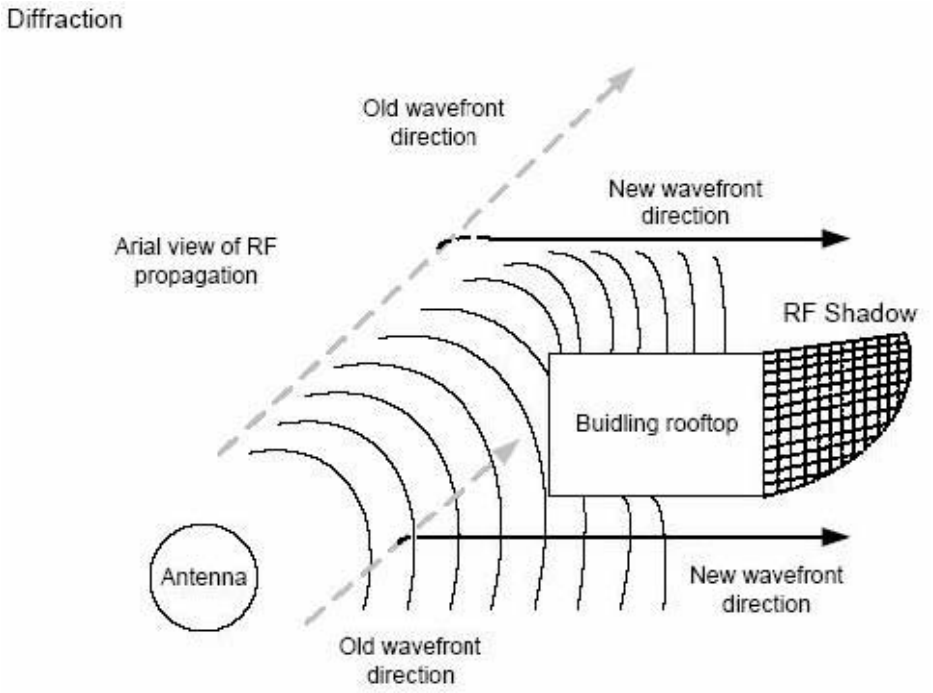
A. Diffraction
B. Refraction
C. Diffusion
D. Scattering

E. Reflection

Answer: A

Explanation:
Diffraction occurs when the radio path between the transmitter and receiver is obstructed by a surface that has sharp irregularities or an otherwise rough surface. At high frequencies, diffraction, like reflection, depends on the geometry of the obstructing object and the amplitude, phase, and polarization of the incident wave at the point of diffraction. Diffraction is commonly confused with and improperly used interchangeably with refraction.

Diffraction



QUESTION 28:

Attenuation is the term used to describe?

A. A decrease in RF signal strength.
B. A lengthening of the antenna cable.
C. The ratio of front-to-back antenna beam strength.
D. The apparent increase in an antenna's receives signal power.

Answer: A

Explanation:
Attenuation is simply a reduction of signal strength during transmission. You represent attenuation in decibels (dB), which is ten times the
logarithm of the signal power at a particular input divided by the signal power at an output of a specified medium. For example, an office wall (i.e., medium) that changes the propagation of an

RF signal from a power level of 200 milliwatts (the input) to 100 milliwatts (the output) represents 3 dB of attenuation. Consequently, positive attenuation causes signals to become weaker when traveling through the medium.
When signal power decreases to relatively low values, the receiving 802.11 radio will likely encounter bit errors when decoding the signal. This problem worsens when significant RF interference is present
Excessive attenuation causes the network's throughput to decrease because of operation at a lower data rate and the additional overhead necessary to retransmit the frames. Generally, this means that the user is operating within the outer bounds of an access point's range. There's enough attenuation present to decrease signal power below acceptable values. At worst case, signal power loss due to attenuation becomes so low that affected users will lose connectivity to the network

---

QUESTION 29:

Which spread spectrum technologies exhibit resistance to narrowband RF interference by design?

A. FHSS
B. DSSS
C. Point-to-point Infrared
D. Broadcast Infrared

Answer: A

Explanation:
Frequency hopping spread spectrum is a spread spectrum technique that uses frequency agility to spread the data over more than 83 MHz. Frequency agility refers to the radio's ability to change transmission frequency abruptly within the usable RF frequency band. In the case of frequency hopping wireless LANs, the usable portion of the 2.4 GHz ISM band is 83.5 MHz, per FCC regulation and the IEEE 802.11 standard.
Both FHSS and DSSS technologies have their advantages and disadvantages, and it is incumbenton the wireless LAN administrator to give each its due weight when deciding howto implement a wireless LAN. This section will cover some of the factors that shouldbe discussed when determining which technology is appropriate for your organization, including:
? Narrowband interference
? Co-location
? Cost
? Equipment compatibility & availability
The advantages of FHSS include a greater resistance to narrow band interference. DSSS systemsmay be affected by narrow band interference more than FHSS because of the use of22 MHz wide contiguous bands instead of the 79 MHz used by FHSS. This fact may be a serious consideration if the proposed wireless LAN site is in an environment that has such interference present.

QUESTION 30:

A 2.4 GHz Spread Spectrum phone located near an 802.11b compliant Access Point will not cause interference.

A. This is always true.
B. This is always false.
C. It depends on configuration of the Access Point and phone.

Answer: C

Explanation:
communications tower or other legitimate system, the wireless LAN administrator might have to consider using a wireless LAN system that utilizes a different set of frequencies. For example, if an administrator were responsible for the design and installation of an RF network at a large apartment complex, special considerations might be in order. If an RF interference source were a large number of 2.4 GHz spread spectrum phones, baby monitors, and microwave ovens in this apartment complex, then the administrator might choose to implement 802.11a equipment that uses the 5 GHz UNII bands instead of 802.11b equipment that shares the 2.4 GHz ISM band with these other devices. Unintentional jamming occurs regularly due to many different devices across many different industries sharing the 2.4 GHz ISM band with wireless LANs. Malicious jamming is not a common threat. The reason RF jamming is not very popular among hackers is that it is fairly expensive to mount an attack, considering the cost of the required equipment,

---

QUESTION 31:

Bluetooth uses which type of data modulation?

A. CCK
B. 64QAM
C. GFSK
D. BPSK

Answer: C

Explanation:
option. Bluetooth and HomeRF are both FHSS technologies that use GFSK modulation technology in the 2.4 GHz ISM band.

QUESTION 32:

When doing wireless LAN mathematical calculations, it is necessary to be able to convert which of the following?

A. dBm to milliwatts.
B. dBi to milliwatts
C. dB to watts
D. dBm to dBi

Answer: A

Explanation:
Milliwatt
When implementing wireless LANs, power levels as low as 1 milliwatt (1/1000 watt, abbreviated as "mW") can be used for a small area, and power levels on a single wireless LAN segment are rarely above 100 mW - enough to communicate up to a half mile in optimum conditions. Access points generally have the ability to radiate 30-100 mW of power, depending on the manufacturer. It is only in the case of point-to-point outdoor connections between buildings that power levels above 100 mW would be used. Most of thepower levels referred to by administrators will be in mW or dBm. These two units of measurement both represent an absolute amount of power and are both industry standard measurements.

QUESTION 33:

WEP keys are also known by what more generic name?

A. Certificates
B. Secure Tokens
C. Shared Secrets
D. SecureIDs

Answer: C

Explanation:
Shared secrets are strings of numbers or text that are commonly referred to as the WEP key. Certificates are another method of user identification used with wireless networks.
Just as with WEP keys, certificates (which are authentication documents) are placed on

---

QUESTION 34:

When considering erecting an outside antenna for use with a 2.4 GHz wireless LAN, which things are considered as you perform the site survey? (Choose two)

A. Is the weather in this area volatile?
B. Are there any FM radio stations nearby?
C. Are telephone lines located in this area?
D. Is there a possibility of future obstructions?

Answer: A, D

QUESTION 35:

Insertion loss on wireless LAN splitters is measured in?

A. db
B. dBi
C. dBm
D. milliwatts

Answer: A

Explanation:
The insertion loss should be significantly low (perhaps around 0.1 dB) so as not to cause high RF signal amplitude loss as the signal passes through the arrestor.
Low insertion loss (loss incurred by just introducing the item into the circuit) is necessary because simply putting the splitter in the RF circuit can cause a significant RF signal amplitude decrease. Insertion loss of 0.5 dB or less is considered good for an RF splitter.

QUESTION 36:

The FCC determines which of the following in the United States? (Choose all that apply)

A. RF Output power limits.
B. Appropriate RF Frequency band use.
C. IEEE standards.
D. Licensing of frequency bands.
E. Interoperability of license-free RF products
F. Licensing fee for end-user use of ISM bands

Answer: A, B, D

QUESTION 37:

Which weather conditions can cause damage to an outdoor spread spectrum wireless LAN? (Choose all that apply)

A. Lightning
B. Wind
C. Rain
D. Snow

Answer: A, B

Explanation:
Severely adverse weather conditions can affect the performance of a wireless LAN. In

general, common weather occurrences like rain, hail, snow, or fog do not have an adverse affect on wireless LANs. However, extreme occurrences of wind, fog, and perhaps smog can cause degradation or even downtime of your wireless LAN. A radomecan be used to protect an antenna from the elements.
Wind
Wind does not affect radio waves or an RF signal, but it can affect the positioning of outdoor antennas. For example, consider a wireless point-to-point link that connects two buildings that are 12 miles apart. Taking into account the curvature of the Earth (Earth bulge), and having only a five-degree vertical and horizontal beam width on each antenna, the positioning of each antenna would have to be exact. A strong wind could
Lightning can affect wireless LANs in two ways. First, lightning can strike either a wireless LAN component such as an antenna or it may strike a nearby object. Lightning strikes of nearby objects can damage your wireless LAN components as if these components are not protected by a lightning arrestor. A second way that lightning affects wireless LANs is by charging the air through which the RF waves must travel after striking an object lying between the transmitter and receiver.
twoantennas. This effect is called "antenna wind loading",

QUESTION 38:

Which of these are known methods of attacking a wireless LAN? (Choose two)

A. Broadcast Monitoring.
B. Rouge Access Points.
C. Passive Probes.
D. Excessive use of RTS/CTS protocol.

Answer: B, C

Explanation:
- method by which stations broadcast a probe frame, and all access points within range respond with a probe response frame; Similar to passive scanning, the station will keep track of the probe responses and make a decision on which access point to authenticate and associate with based on the probe responses having the strongest signal level

---

QUESTION 39:

If two DSS access points are placed on the same channel in the same physical space, which of the following will take place?

A. The available bandwidth to users will increase.
B. The available bandwidth to users will decrease.
C. The access points will interfere with each other.
D. Users will be able to roam between the two access points.

Answer: C

Explanation:
One option, which is the easiest, is to use channels 1 and 11 with only 2 access points, as illustrated in Figure 9.11. Using only these two channels will ensure that you have no overlap between channels regardless of proximity between systems, and therefore, no detrimental effect on the throughput of each access point. By way of comparison, two access points operating at the maximum capacity of 5.5 Mbps (about the best that you can expect by any access point), give you a total capacity of 11 Mbps of aggregate throughput, whereas three access points operating at approximately 4 Mbps each (degraded from the maximum due to actual channel overlap) on average yields only 12 Mbps of aggregate throughput. For an additional 1 Mbps of throughput, an administrator would have to spend the extra money to buy another access point, the time and labor to install it, and the continued burden of managing it.

QUESTION 40:

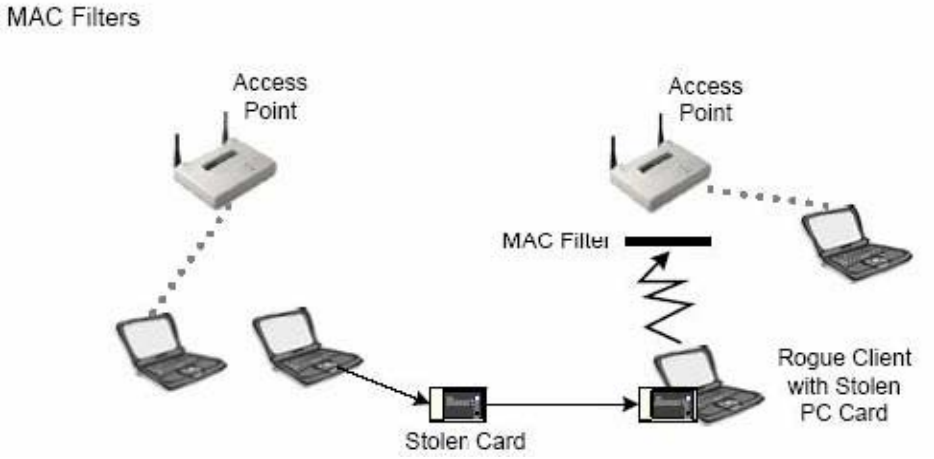
Where can MAC filters be implemented on a wireless LAN? (Choose all that apply)

A. Access Points
B. WLAN USB client
C. RADIUS servers
D. WLAN SNMP agent
E. Personal firewall software

Answer: A, C

Explanation:
A//
Wireless LANs can filter based on the MAC addresses of client stations. Almost all access points (even very inexpensive ones) have MAC filter functionality. The network administratorcan compile, distribute, and maintain a list of allowable MAC addresses andprogram them into each access point.If a PC card or other client with a MAC address that is not in the access point's MAC filter list tries to gain access to the wireless LAN, the MAC address filter functionality will not allow that client to associate with that access point.
Ref for C//Of course, programming every wireless client's MAC address into every access point across a large enterprise network would be impractical. MAC filters can be implemented onsome RADIUS servers instead of in each access point. This configuration makes MAC filters a much more scalable security solution. Simply entering each MAC address into RADIUS along with user identity information, which would have to be input anyway, is a good solution. RADIUS servers often point to another authentication

source, so that other authentication source would need to support MAC filters.



QUESTION 41:

Which of the following steps should be taken in the process creating a security solution for a wireless LAN network? (Choose all that apply)

A. Making backups of WEP keys in the event of a system failure.
B. Implementing VPN tunneling protocols such as IPSec or PPTP where possible.
C. Using four WEP keys in every access point.
D. Implementing wireless LAN connectivity in a DMZ area.
E. Place all wireless LAN users directly on the Internet segment of the network.

Answer: B, C, D

Explanation:
From the study guide, there are a number of measures that may be taken to secure a WLAN. Specifically, using multiple WEP keys (in-case of a compromise) and implementing VPN tunneling are both helpful in effectively securing a wireless LAN. Additionally, implementing the Wireless network in a DMZ area is much more worthwhile in a corporate environment for example. This effectively separates the un-trusted portion of the network from the core of the network with the help of a firewall. Therefore, the answer should be B,C,D.

QUESTION 42:

A sequence of hops in a Frequency Hopping Spread Spectrum system is referred to as?

A. Pattern
B. List
C. Channel
D. Array

Answer: A

Explanation:
A frequency hopping system will operate using a specified hop pattern.
See CWNA Official Study Guide, 3rd Edition, Page 181 (FHSS Hop Sequences and Channels)

QUESTION 43:

A LOSS of -10dB yields a power ratio of?

A. 1:3
B. 1:10
C. 2:1
D. 10:1

Answer: B

Explanation:
Power gain and loss are measured in decibels, not in watts, because gain and loss are relative concepts and a decibel is a relative measurement. Gain or loss in an RF system may be referred to by absolute power measurement (e.g. ten watts of power) or by a relative power measurement (e.g. half of its power). Losing half of the power in a system corresponds to losing 3 decibels. If a system loses half of its power (-3 dB), then loses half again (another -3 dB), then the total system loss is 3/4 of the original power - 1/2 first, then 1/4 (1/2 of 1/2). Clearly, no absolute measurement of watts can quantify this asymmetrical loss in a meaningful way, but decibels do just that.
As a quick and easy reference, there are some numbers related to gain and loss that an administrator should be familiar with. These numbers are:
-3 dB = half the power in mW
+3 dB = double the power in mW
-10 dB = one tenth the power in mW
We refer to these quick references as the 10's and 3's of RF math. When calculating power gain and loss, one can almost always divide an amount of gain or loss by 10 or 3 or both. These values give the administrator the ability to quickly and easily calculate RF loss and gain with a fair amount of accuracy without the use of a calculator.
If an access point were
connectedto a cable whose loss was -2 dB and then a connector whose loss was -1 dB, thenthese loss measurements would be additive and yield a total of -3 dB of loss. We willwalk through some RF calculations in the coming sections to give you a better idea ofhow to relate these numbers to actual scenarios.

QUESTION 44:

All access points transmit what at a fixed interval?

A. Association request management frame.

B. Probe request management frame.
C. Infrastructure beacon packet.
D. Beacon management frame.

Answer: D

Explanation:
Beacons (short for beacon management frame) are short frames that are sent from the accesspoint to stations (infrastructure mode) or station-to-station (ad hoc mode) in order toorganize and synchronize wireless communication on the wireless LAN. Beacons serve several functions, including the following.
Beacons synchronize clients by way of a time-stamp at the exact moment of transmission. When the client receives the beacon, it changes its own clock to reflect the clock of the access point. Once this change is made, the two clocks are synchronized.

QUESTION 45:

Seamless roaming is specified in what IEEE standard?

A. 802.11
B. 802.11b
C. 802.11a
D. All of the above.
E. None of the above.

Answer: E

Explanation:
Seamless roaming is specified in the 802.11F standard.
In situations where seamless roaming is required, a technique called channel reuse is used inorderto alleviate adjacent and co-channel interference while allowing users to roam throughadjacent cells. Channel reuse is the side-by-side locating of non-overlapping cells to form a mesh of coverage where no cell on a given channel touches another cell on that channel
After a wireless LAN is installed, it might not work exactly as planned, although it may be close. Spot-checking by a site surveyor after installation is complete is most helpful in avoiding troubleshooting situations during production use of the network. Items that should be checked are:
? Coverage in perimeter areas
? Overlapping coverage for seamless roaming
? Co-channel and adjacent channel interference in all areas

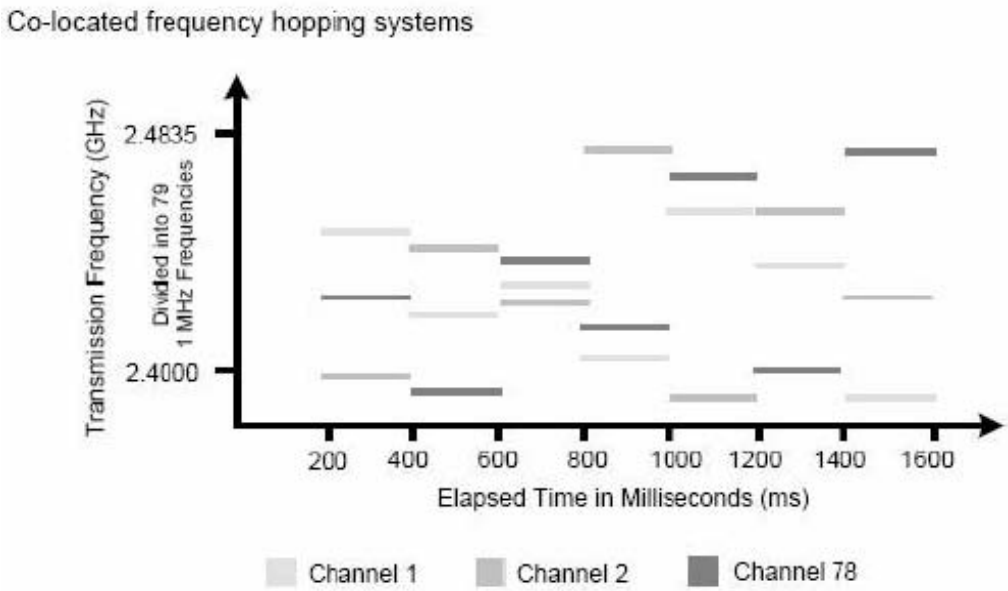
QUESTION 46:

Identify all true statements below.

A. FHSS is inherently more secure than DSSS.
B. FHSS uses frequently agility to enhance security.
C. The FHSS hopset can be determined by listening to traffic on each of the hopping channels.
D. Both FHSS and DSSS rely on user authentication and data encryption for security.

Answer: C

Explanation:
A frequency hopping system will operate using a specified hop pattern called a channel. Frequency hopping systems typically use the FCC's 26 standard hop patterns or a subset thereof. Some frequency hopping systems will allow custom hop patterns to be created, and others even allow synchronization between systems to completely eliminate collisions in a co-located environment.



Though it is possible to have as many as 79 synchronized, co-located access points, with this many systems, each frequency hopping radio would require precise synchronization with all of the others in order not to interfere with (transmit on the same frequency as) another frequency hopping radio in the area. The cost of such a set of systems is prohibitive and is generally not considered an option. If synchronized radios are used, the expense tends to dictate 12 co-located systems as the maximum.
In frequency hopping systems, the carrier changes frequency, or hops, according to a pseudorandomsequence. The pseudorandom sequence is a list of several frequencies to whichthe carrier will hop at specified time intervals before repeating the pattern. The transmitteruses this hop sequence to select its transmission frequencies. The carrier will remainat a certain frequency for a specified time (known as the dwell time), and then use asmall amount of time to hop to the next frequency (hop time). When the list of frequencieshas been exhausted, the transmitter will repeat the sequence.
In order for a frequency hopping system to be 802.11 or
OpenAir compliant, it must operate in the 2.4 GHz ISM band (which is defined by the FCC as being from 2.4000 GHz to 2.5000 GHz). Both standards allow operation in the range of 2.4000 GHz to 2.4835 GHz.

QUESTION 47:

What is a disadvantage of having a short dwell time when using a FHSS system?

A. Decreased range.
B. Decreased data throughput.
C. Decreased security.
D. Decreased resistance to narrowband interference.

Answer: B

Explanation:
When a frequency hopping radio jumps from frequency A to frequency B, it must change the transmit frequency in one of two ways. It either must switch to a different circuit tuned to the new frequency, or it must change some element of the current circuit in order to tune to the new frequency. In either case, the process of changing to the new frequency must be complete before transmission can resume, and this change takes time due to electrical latencies inherent in the circuitry. There is a small amount of time during this frequency change in which the radio is not transmitting called the hop time. The hop time is measured in microseconds (µs) and with relatively long dwell times of around 100-200 ms, the hop time is not significant. A typical 802.11 FHSS system hops between channels in 200-300 µs.
With very short dwell times of 500 - 600µs, like those being used in some frequency hoppingsystems such as Bluetooth, hop time can become very significant. If we look at theeffect of hop time in terms of data throughput, we discover that the longer the hop timein relation to the dwell time, the slower the data rate of bits being transmitted.
This translates roughly to longer dwell time = greater throughput.

QUESTION 48:

What does the PRNG acronym stand for in regards to the WEP protocol?

A. Passive Request Next Generation.
B. Pseudorandom Number Generator.
C. Protected Result Null Group.
D. Persistent Routing Network Gateway.

Answer: B

Explanation:
The IEEE 802.11 standard specifies the use of WEP.
WEP is a simple algorithm that utilizes a pseudo-random number generator (PRNG) and theRC4 stream ciphe r

QUESTION 49:

Which of the following is true of a 2.4 GHz RF link at a distance of 5 miles (8 kilometers). (Choose all that apply)

A. RF Line of Sight is required.
B. Visual Line of Sight is required.
C. Earth bulge must be factored into calculations.
D. The Fresnel Zone must be at least 60% clear of obstructions.
E. High gain omni-directional antenna.

Answer: A, D

Explanation:
From the study guide, Visual LOS is not required for a successful point-to-point connection. However RF LOS is required. Additionally, the Fresnel zone must be at least 60% clear of obstructions. Earth bulge is only factored in for greater then 7 mile links.

QUESTION 50:

Which two RF spread spectrum technologies does IEEE specify in the 802.11 standard? (Choose two)

A. Infrared
B. Frequency Hopping
C. Direct Sequencing
D. Wide Band

Answer: B, C

Explanation:
REF FOR B: a typical 802.11 frequency hopping WLAN might be implemented as an enterprise wireless networking solution while HomeRF is only implemented in home environments due to lower output power restrictions by the FCC
OR
Frequency agility refers to the radio's ability to change transmission frequency abruptly within the usable RF frequency band. In the case of frequency hopping wireless LANs, the usable portion of the 2.4 GHz ISM band is 83.5 MHz, per FCC regulation and the IEEE 802.11 standard.
REF FOR C//
In the 2.4 GHz ISM band, the IEEE specifies the use of DSSS at a data rate of 1 or 2 Mbps under the 802.11 standard.Under the 802.11b standard-sometimes called highrate wireless-data rates of 5.5 and 11 Mbps are specified.

QUESTION 51:

What are the two types of scanning used with wireless LANs? (Choose all that apply)

A. Passive
B. Beacon
C. Probe
D. Active

Answer: A, D

Explanation:
When you install, configure, and finally start up a wireless LAN client device such as a USB client or PCMCIA card, the client will automatically "listen" to see if there is a wireless LAN within range. The client is also discovering if it can associate with that wireless LAN. This process of listening is called scanning. Scanning occurs before any other process, since scanning is how the client finds the network.
There are two kinds of scanning: passive scanning and active scanning. In finding an access point, client stations follow a trail of breadcrumbs left by the access point. These breadcrumbs are called service set identifiers (SSID) and beacons. These tools serve as a means for a client station to find any and all access points.

QUESTION 52:

A wireless portal interconnects LANs conforming to what IEEE standards? (Choose two)

A. 802.11 and 802.3
B. 802.3 and 802.5
C. 802.5 and 802.11
D. 802.10 and 802.11
E. 802.5 and 802.10

Answer: A, C

Explanation:
An access point is considered a portal because it allows client connectivity from an 802.11 network to 802.3 or 802.5 networks. Access points are available with many different hardware and software options. The most common of these options are:
? Fixed or Detachable Antennas
? Advanced Filtering Capabilities
? Removable (Modular) Radio Cards
? Variable Output Power
? Varied Types of Wired Connectivity

QUESTION 53:

Choose the organization that creates wireless LAN standards.

A. IEEE
B. WLANA
C. WECA
D. Wi-Fi

Answer: A

QUESTION 54:

Under 802.11 standard, what modulation types are used when transmitting data using DSSS? (Choose all that apply)

A. CCK
B. GFSK
C. BPSK
D. QPSK
E. 64QAM

Answer: C, D

Explanation:
The high data rate of 802.11b-compliant devices is the result of using a different coding technique. Though the system is still a direct sequencing system, the way the chips are coded (CCK rather than Barker Code) along with the way the information is modulated (QPSK at 2, 5.5, & 11 Mbps and BPSK at 1 Mbps) allows for a greater amount of data to be transferred in the same time frame. 802.11b compliant products operate only in the 2.4 GHz ISM band between 2.4000 and 2.4835 GHz.

QUESTION 55:

The ETS1 standard being developed to compete against 802.11a is known as?

A. HomeRF
B. OpenAir
C. HiperLan/2
D. Bluetooth

Answer: C

Explanation:
The standards ETSI has established, HiPerLAN/2 for example, directly compete against standards created by the IEEE such as 802.11a. There has been much discussion about IEEE and ETSI unifying on certain wireless technologies, but nothing

has materialized as of this writing. This effort is referred to as the "5UP" initiative for "5 GHz Unified Protocol." The IEEE's attempt at interoperability with ETSI's HiperLAN/2 standard is the new forthcoming 802.11h standard.

QUESTION 56:

WECA requires which of the following WEP security settings for Wi-Fi certification?

A. Single 104-bit key.
B. Dial 40-bit keys.
C. Single 128-bit key.
D. Single 40-bit key.

Answer: D

Explanation:
The 802.11 standard leaves WEP implementation up to wireless LAN manufacturers, so each vendor's implementation of WEP keys may or may not be the same, adding another weakness to WEP. Even WECA's Wi-Fi interoperability standard tests include only 40-bit WEP keys.
Among WECA's list of interoperability checks is the use of 40-bit WEP keys. Note that 40- and 64-bit keys are the same thing. A 40-bit "secret" key is concatenated with a 24-bit Initialization Vector (IV) to reach the 64-bits. In the same manner, 104- and 128-bit keys are the same. WECA does not specify interoperability of 128-bit keys; hence, no compatibility is to be expected between vendors displaying the Wi-Fi seal when using 128-bit WEP keys.

QUESTION 57:

Under the 802.11 standard, what modulation is used when transmitting data using FHSS?

A. CCK
B. GFSK
C. BPSK
D. QPSK

Answer: B

Explanation:
(DQPSK), and Gaussian Frequency Shift Keying (GFSK) are the types of modulation used by 802.11 and 802.11b products on the market today.Bluetooth and HomeRF are both FHSS technologies that use GFSK modulation technology in the 2.4 GHz ISM band.
Differential Quadrature Phase Shift Keying

QUESTION 58:

Which of the following features are found in wireless Residential Gateways? (Choose all that apply)

A. DHCP client
B. 802.1q
C. Spanning Tree Protocol (STP)
D. Network Address Translation (NAT)
E. PPPoE
F. 802.1x
G. 802.11c

Answer: A, D, E

Explanation:
Residential wireless gateways are now available with VPN technology, as well as NAT, DHCP, PPPoE, WEP, MAC filters, and perhaps even a built-in firewall.These devices are sufficient for small office or home office environments with few workstations and a shared connection to the Internet. Costs of these units vary greatly depending on their range of offered services. Some of the high-end units even boast static routing and RIPv2.

QUESTION 59:

Which of these WLAN devices cause loss in the RF signal path? (Choose all that apply)

A. Cable
B. Connector
C. Amplifier
D. Attenuator
E. Inducer
F. Inductor

Answer:
A. B, D

Explanation: An RF attenuator is a device that causes precisely measured loss (in -dB) in an RF signal.
While an amplifier will increase the RF signal, an attenuator will decrease it.

QUESTION 60:

Beacon frames are used for? (Choose two)

A. Time synchronization.

B. Passing channel selection information.
C. Limiting data requests.
D. Reserving the medium for QoS implementations.

Answer: A, B

Explanation: According to the book, the beacon frames are used for time synchroniztion and channel information (for DSSS and FHSS).

QUESTION 61:

Which one of the following is necessary as part of an RF Site Survey Report?

A. Detailed RF coverage area map.
B. Time sheet itemizing length of time to accomplish survey.
C. Recommended implementation solution including at least two manufacturer's gear.
D. Recommended wireless security solutions.

Answer: A

Explanation: An RF site survey is a map to successfully implementing a wireless network. Site surveying involves analyzing a site from an RF perspective and discovering what kind of RF coverage a site needs in order to meet the business goals of the customer. During the site survey process, the surveyor will ask many questions about a variety of topics, which are covered in this chapter. These questions allow the surveyor to gather as much information as possible to make an informed recommendation about what the best options are for hardware, installation, and configuration of a wireless LAN.
A site survey is an attempt to define the contours of RF coverage from an RF source (an access point or bridge) in a particular facility. Many issues can arise that prevent the RF signal from reaching certain parts of the facility. For example, if an access point were placed in the center of a medium-sized room, it would be assumed that there would be RF coverage throughout the room. This is not necessarily true due to phenomena such as multipath, near/far, and hidden node. There may be "holes" in the RF coverage pattern due to multipath or stations that cannot talk to the network due to near/far.

QUESTION 62:

Which units of measure below are measurements of relative power (a change in power)? (Choose all that apply)

A. dBm
B. dBi
C. dB

D. mW

Answer: B, C

Explanation: The units of relative power are db and dbi.

QUESTION 63:

What does the acronym "Wi-Fi" stand for?

A. Wireless Fiber.
B. Wireless Interoperability Forum Institution.
C. Wireless Frequency Industry.
D. Wireless Fidelity.

Answer: D

Explanation:
The Wireless Ethernet Compatibility Alliance (WECA) provides testing of 802.11b compliant DSSS wireless LAN equipment to ensure that such equipment will operate in the presence of and interoperate with other 802.11b DSSS devices. The interoperability standard that WECA created and now uses is called Wireless Fidelity, or Wi-Fi, and those devices that pass the tests for interoperability are "Wi-Fi compliant" devices

---

QUESTION 64:

By default, IEEE 802.11 devices are set to which type of WEP authentication?

A. Shared Key Authentication.
B. Open System Authentication.
C. No Authentication.
D. IEEE 802.11 does not specify use of WEP.

Answer: B

Explanation: The IEEE 802.11 standard specifies two methods of authentication: Open System
authenticationand Shared Key authentication. The simpler and also the more secure of the two methods is Open System authentication.

QUESTION 65:

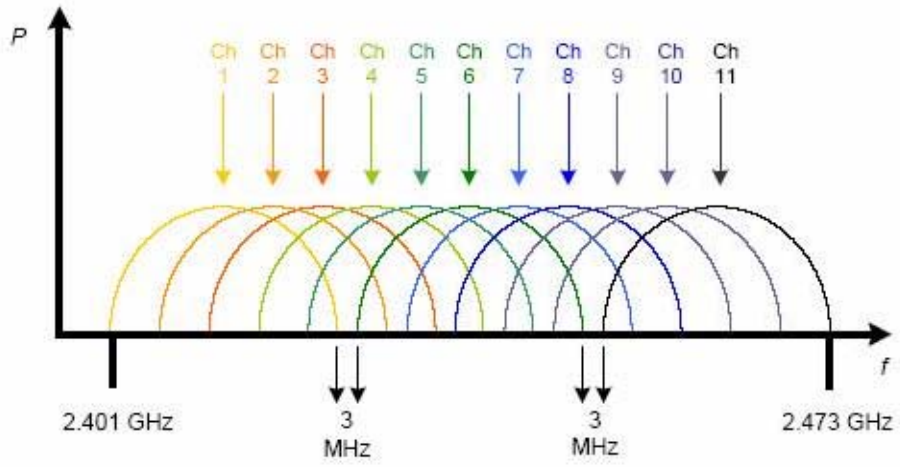
Direct Sequence Spread Spectrum (DSSS) technology uses channels that are _____ Mhz wide to transmit data in the 2.4 GHz ISM band.

A. 11
B. 20
C. 22
D. 30

Answer: C

Explanation: The portion of the 2.4 GHz ISM band that is useable for wireless LANs consists of 83.5
MHz. DSSS channels are 22 MHz wide, and there are 11 channels specified for use in the United States.

DSSS channel allocation and spectral relationship



QUESTION 66:

A GAIN of +3dB yields a power ratio of?

A. 2:1
B. 3:1
C. 10:1
D. 1:10

Answer: A

Explanation:
The reference point that relates the logarithmic dB scale to the linear watt scale is:
1 mW = 0 dBm
The m in dBm refers simply to the fact that the reference is 1 milliwatt (1 mW) and therefore a dBm measurement is a measurement of absolute power.
The relationship between the decibels scale and the watt scale can be estimated using the following rules of thumb:
+3 dB will double the watt value:
(10 mW + 3dB ?___ 20 mW)

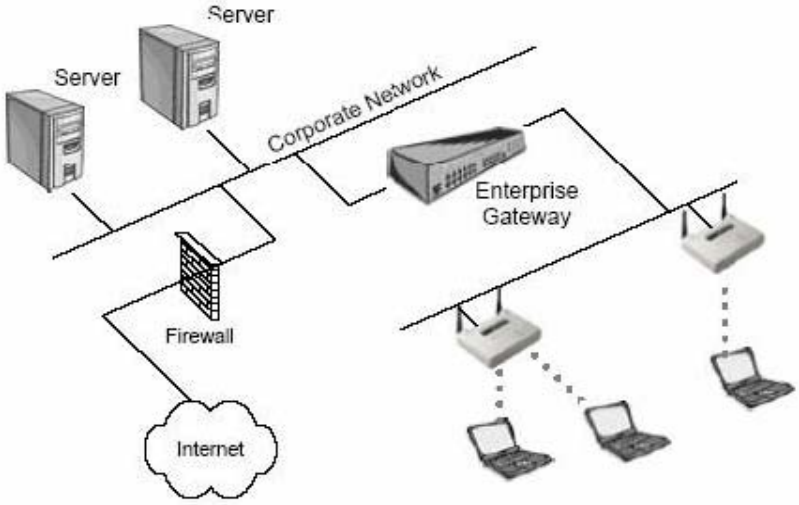
QUESTION 67:

Available WLAN security solutions include?

A. Mobile IP.
B. 802.1x with EAP.
C. LDAP with PAP.
D. OSPF

Answer: B

Explanation: the more features
the access point has, the more the access point will cost. For example, some SOHO access points will have WEP, MAC filters, and even a built-in web server. If features such as viewing the association table, 802.1x/EAP support, VPN support, routing functionality, Inter-access point protocol, and RADIUS support are required, expect to pay several times as much for an enterprise-level access point.



Authentication technologies incorporated into enterprise wireless gateways are often built into the more advanced levels of access points. For example, VPN and 802.1x/EAP connectivity are supported in many brands of enterprise level access points.

QUESTION 68:

WLAN client-side devices may use which of the following
security features?

A. Wireless NetBIOS support.
B. IPX/SPX support.
C. Encrypted file sharing.
D. EAP/LEAP support.

Answer: D

Explanation: EAP-Cisco Wireless. Also called LEAP (Lightweight Extensible Authentication
Protocol), this EAP authentication type is used primarily in Cisco wireless LAN access points. LEAP provides security during credential exchange, encrypts data transmission using dynamically generated WEP keys, and supports mutual authentication.

QUESTION 69:

Which of the following protocols is a common option in Wireless Residential Gateway devices?

A. OSPF
B. NAT
C. BGP
D. IGMP

Answer: B

Explanation: Wireless Gateways
Residential wireless gateways are now available with VPN technology, as well as NAT, DHCP, PPPoE, WEP, MAC filters, and perhaps even a built-in firewall.These devices are sufficient for small office or home office environments with few workstations and a shared connection to the Internet. Costs of these units vary greatly depending on their range of offered services. Some of the high-end units even boast static routing and RIPv2.

QUESTION 70:

When planning RF links, earth bulge should be considered when planning paths over?

A. 2 miles / 3.2 kilometers.
B. 4 miles / 6.4 kilometers.
C. 7 miles / 11.2 kilometers.
D. 10 miles / 16 kilometers.

Answer: C

Explanation: Earth bulge - the amount of rise of the earth's surface between long-distance radio links;
must be calculated into tower height for radio links greater than 7 miles

---

QUESTION 71:

RTS/CTS is an extension to the implementation of which of the

following?

A. CSMA/CD
B. CSMA/CA
C. PCF
D. SIFS

Answer: B

Explanation: Request-to-Send/Clear-to-Send (RTS/CTS) - an extension to CSMA/CA, in which
clients enter into a 4-way handshake with an access point to send data. (1) Client sends RTS packet to request use of the medium, (2) if the medium is free, access point sends the CTS packet to the client, (3) client sends the DATA to the receiving client, (4) receiving client sends the ACK packet to acknowledge receipt of the DAT
A. 4-way
handshake = RTS-CTS-DATA-ACK

QUESTION 72:

The WEP protocol is intended to support which of these security goals? (Choose all that apply)

A. Confidentiality
B. Controlled Access
C. Longevity
D. Data Integrity
E. Impenetrable security
F. Authentication by certificate
G. Encryption tunneling

Answer: A, B, D

QUESTION 73:

Ad Hoc mode cannot be used for which of the following? (Choose all that apply)

A. In an Extended Service Set.
B. In an airport.
C. In a Basic Service Set.
D. In a hotel room.

Answer: A, C

QUESTION 74:

How should the site survey engineer document the "dead spots" in the area to be covered by a

WLAN?

A. Showing the network administrator the spots in person.
B. Marking the spots with markers or flags.
C. Dead spots are not recorded in a site survey.
D. Marking the locations of dead spots on a site blueprint or floor plan.

Answer: D

QUESTION 75:

What are two methods specified by IEEE 802.11 to authenticate a user in a wireless LAN? (Choose two)

A. Shared secrets
B. Certificates
C. Usernames
D. Passwords

Answer: A, B

Explanation: Use of PPTP with shared secrets is very simple to implement and provides a reasonable
level of security, especially when added to WEP encryption. Use of IPsec with shared secretsor certificates is generally the solution of choice among security professionals in this arena. When the VPN server is implemented in an enterprise gateway, the same process takes place except that, after the client associates to the access point, the VPN tunnel is established with the upstream gateway device instead of with the access point itself.

QUESTION 76:

Choose the term that means "an amplitude reduction in the signal"

A. Offset
B. Amplification
C. Attenuation
D. Limiting

Answer: C

Explanation: attenuation - a term used to describe decreasing the amplitude of an RF signal due to
resistance of cables, connectors, splitters, or obstacles encountering the signal path

---

QUESTION 77:

Which of the following are mechanisms defines by 802.11b for providing access control and privacy on a wireless LAN? (Choose two)

A. RADIUS
B. WEP
C. AES
D. SSID

Answer: B, D

Explanation:
REF FOR B //
Open System authentication is a very simple process. As the wireless LAN administrator, you have the option of using WEP (wired equivalent privacy) encryption with Open System authentication. If WEP is used with the Open System authentication process, there is still no verification of the WEP key on each side of the connection during authentication. Rather, the WEP key is used only for encrypting data once the client is authenticated and associated.
REF FOR D//: The service set identifier (SSID) is a unique, case sensitive, alphanumeric value from 2-
32 characters long used by wireless LANs as a network name. This naming handle is used for segmenting networks, as a rudimentary security measure, and in the process of joining a network. The SSID value is sent in beacons, probe requests, probe responses, and other types of frames. A client station must be configured for the correct SSID in order to join a network. The administrator configures the SSID (sometimes called the ESSID) in each access point.Some stations have the ability to use any SSID value instead of only one manually specified by the administrator. If clients are to roam seamlessly among a group of access points, the clients and all access points must be configured with matching SSIDs. The most important point about an SSID is that it must match EXACTLY between access points and clients.

QUESTION 78:

Which item(s) would NOT be beneficial for a network manager to provide to an engineer doing an indoor site survey?

A. Blueprints of the facility.
B. Available lifts for mounting access points.
C. Access to network backbone routers.
D. A list of RF systems already in use in the facility.
E. Diagram of available AC power.
F. Previous site survey reports.

Answer: B

QUESTION 79:

Prior to August 31, 2000, the FCC required the use of how many channels with a 2.4 GHz FHSS system before repeating the pattern?

A. 70
B. 75
C. 79
D. 83

Answer: B

Explanation: No overlapping frequencies are allowed under either rule. If the minimum 75 MHz of
used bandwidth within the frequency spectrum were cut into pieces as wide as the carrier frequency bandwidth in use, they would have to sit side-by-side throughout the spectrum with no overlap. This regulation translates into 75 non-overlapping carrier frequencies under the pre- 8/31/00 rules and 15-74 non-overlapping carrier frequencies under the post- 8/31/00 rules.
The IEEE states in the 802.11 standard that FHSS systems will have at least 6 MHz of carrier frequency separation between hops. Therefore, a FHSS system transmitting on 2.410 GHz must hop to at least 2.404 if decreasing in frequency or 2.416 if increasing in frequency. This requirement was left unchanged by the IEEE after the FCC change on 8/31/00.

QUESTION 80:

After August 31, 2000, the FCC allowed a maximum channel
bandwidth for FHSS of?

A. 1 MHz
B. 2 MHz
C. 5 MHz
D. 11 MHz

Answer: C

Explanation: Certified Wireless Network Administrator Study Guide, page 54

QUESTION 81:

What type of modulation does 1Mbps DSSS use?

A. GFSK
B. BPSK

C. QPSK
D. CCK

Answer: B

Explanation: Certified Wireless Network Administrator Study Guide, page 225

QUESTION 82:

The process of moving from one BSS to another without losing connection is known as?

A. Switching
B. Passing
C. Roaming
D. Scanning

Answer: C

Explanation: Certified Wireless Network Administrator Study Guide, page 370

QUESTION 83:

Which of the following are advantages of a wireless LAN over a
wired LAN?

A. Greater flexibility.
B. Greater adaptability.
C. Higher speeds available.
D. More simplified installation.

Answer: A, B, D,

Explanation: Certified Wireless Network Administrator Study Guide, pages 2, 5, 6

QUESTION 84:

What type pf spreading code does 1Mbps DSSS use?

A. Barker
B. Chip
C. QPSK
D. CCK

Answer: A

Explanation: Certified Wireless Network Administrator Study Guide, page 225

QUESTION 85:

Which of the following are security risks in a wireless LAN? (Choose all that apply)

A. Physical security
B. Cellular phones
C. Radio frequency jamming
D. Packet sniffing
E. Casual eavesdropping

Answer: A, C, D, E

Explanation: Certified Wireless Network Administrator Study Guide, Pages 282, 283, 291

QUESTION 86:

While an access point is operating in Distributed Coordination Function (DCF) mode, which of the following is true? (Choose two)

A. CSMA/CA is used to avoid collisions.
B. Wireless clients are polled for data transmission.
C. Time-bounded data such as voice and video are supported.
D. DCF supports large enterprise environments due to scalability.

Answer: A, D

Explanation: According to the study guide, when the access point is in DCF mode, it contends for the medium along with other stations. Thus no QoS is guaranteed and Voice and Video are not supported.

QUESTION 87:

Which two functions can be configured on a WLAN client computer as part of the WLAN client utility software?

A. snmp management utility
B. Infrastructure mode
C. tftp server
D. firmware loader utility

Answer: B, D

Explanation: Certified Wireless Network Administrator Study Guide, Page 91

QUESTION 88:

Which of the following household appliances are likely sources of interference in the 2.4 GHz band?

A. Microwave ovens
B. Satellite TV
C. Unterminated CATV
D. Fluorescent lights

Answer: A

Explanation: Certified Wireless Network Administrator Study Guide, page 335

QUESTION 89:

The 802.11a standard specifies what number of non-overlapping channels across all 5 GHz UNII bands combined?

A. 15
B. 12
C. 4
D. 20

Answer: B

Explanation: According to the study guide, each of the 3 bands in the 5 GHz UNII band (lower, middle, upper) contain 4 non-overlapping channels. The question ask the number of such channels "combined". That would be B (12)

QUESTION 90:

HomeRF is more secure than 802.11b because?

A. HomeRF uses a 32-bit IV.
B. HomeRF uses the SWAP protocol.
C. HomeRF uses an SSID.
D. HomeRF uses a non-ISM band.

Answer: A

Explanation: Certified Wireless Network Administrator Study Guide, page 164

QUESTION 91:

Which of the following questions is important to ask BEFORE performing an RF site survey?

A. What is the expected user density per access point?
B. What is the budget for the wireless LAN installation?
C. Is there an existing WLAN infrastructure in place?
D. What manufacturer's equipment is preferred for this installation?

Answer: A, C

Explanation: Certified Wireless Network Administrator Study Guide, page 311

QUESTION 92:

In relation to the 802.11 series of standards, which of the following best describes Direct Sequence Spread Spectrum (DSSS)? Select two.

A. DSSS is more sensitive to fixed-frequency RF noise in the 2.4GHz ISM band than FHSS.
B. DSSS is more significantly affected by multipath from narrowband sources than FHSS.
C. A DSSS access point can handle a larger number of simultaneous connections than a FHSS access point.
D. DSSS has higher throughput in Point-to-Point links than FHSS.

Answer: A, B

Explanation: service set identifier (SSID) is a unique, case sensitive, alphanumeric value from 2-
32 characters long used by wireless LANs as a network name. This naming handle is used for segmenting networks, as a rudimentary security measure, and in the process of joining a network. The SSID value is sent in beacons, probe requests, probe responses, and other types of frames. A client station must be configured for the correct SSID in order to join a network. The administrator configures the SSID (sometimes called the ESSID) in each access point.Some stations have the ability to use any SSID value instead of only one manually specified by the administrator. If clients are to roam seamlessly among a group of access points, the clients and all access points must be configured with matching SSIDs. The most important point about an SSID is that it must match EXACTLY between access points and clients.
There are two kinds of scanning: passive scanning and active scanning. In finding an access point, client stations follow a trail of breadcrumbs left by the access point. These breadcrumbs are called service set identifiers (SSID) and beacons. These tools serve as a means for a client station to find any and all access points.

QUESTION 93:

Which if these will be the most susceptible to multipath interference?

A. 1 Mbps DSSS

B. 5 Mbps FHSS
C. 11 Mbps DSSS
D. 1 Mbps FHSS

Answer: C
DSSS is the most susceptible to multipath interference, also as transmission rates frames are less resistant to corruption.
See http://www.wi-fiplanet.com/tutorials/article.php/1121691
For Explanation as to why DSSS is most susceptible.
See CWNA Official Study Guide, 3rd Edition, Page 389
For Explanation as to Dynamic Rate Selection

QUESTION 94:

Which of the following are true of FHSS?

A. FHSS is affected by RF interference to a lesser degree than DSSS.
B. FHSS used the entire 2.4 GHz ISM band.
C. FHSS uses frequency diversity to retransmit lost packets on different frequencies.
D. FHSS is very susceptible to interference from Bluetooth systems.

Answer: A, B

QUESTION 95:

After 8/31/00, which of the following are true of FHSS?

A. Avoids multipath interference.
B. Hops to different frequencies to avoid attenuation.
C. Must use a minimum of 15 hops.
D. Cannot use a hop pattern of more than 40 hops.

Answer: C

QUESTION 96:

What is the maximum transmitter output allowed by the FCC for radio transmitters utilizing FHSS technology (>50 hopping channels) in any of the ISM bands?

A. 4 Watts
B. 30 dBm
C. 100 mW
D. 27 dBm
E. 125 mW

Answer: E

Explanation: According to the study guide, in pre-08/31/00 rules, the maximum tranmitter output was 1 watt. However, in post-08/31/00 rules, the transmitter output was reduced to 125 mW, for all systems utilizing fewer than 75 hops in a sequence. Since the question asks for output for >50 hops, then I presume the answer should be 125 mW.

QUESTION 97:

The number of simultaneously active co-located systems is more scalable with which spread spectrum technology?

A. FHSS
B. DSSS
C. IrDA
D. 802.11b

Answer: A

Explanation:
It is clearly stated in the study guide that FHSS systems are more co-locatable than DSSS systems. Specifically you can co-locate upto 26 FHSS systems (non-synchronised), where as only 3 are allowed with DSSS systems. Thus, in this question, the answer is A (FHSS).

QUESTION 98:

An advantage of DSSS over FHSS is:

A. Range
B. Multipath immunity
C. Co-location scalability
D. Speed

Answer: D

Explanation: An understood advantage and also one of the biggest advantages of DSSS systems over FHSS systems is greater system throughput (speed). In DSSS, speeds of upto 11 mbps can be acheived whereas FHSS only allows a max. of 2 Mbps (while simultanously operating in 802.11 compliant mode).

QUESTION 99:

DSSS systems use what type of modulation when transmitting at 2 Mbps?

A. BPSK
B. QPSK
C. CCK

D. GFSK

Answer: B

Explanation:
The high data rate of 802.11b-compliant devices is the result of using a different coding technique. Though the system is still a direct sequencing system, the way the chips are coded (CCK rather than Barker Code) along with the way the information is modulated (QPSK at 2, 5.5, & 11 Mbps and BPSK at 1 Mbps) allows for a greater amount of data to be transferred in the same time frame. 802.11b compliant products operate only in the 2.4 GHz ISM band between 2.4000 and 2.4835 GHz. Modulation and coding are further discussed in Chapter 8 (MAC & Physical Layers).

QUESTION 100:

Narrowband RF interference will cause significant problems for implementing of which of the following technologies?

A. FHSS
B. DSSS
C. IrDA
D. HomeRF

Answer: B

Explanation: According to the study guide, FHSS systems are more resistent to Narrowband interference then DSSS systems. This is due to the agility of FHSS systems and their utilization of the entire 2.4 Ghz band (83.5 Mhz). Since HomeRF is an FHSS implementation and IrDA does not utilize RF technology, the answer should be B (DSSS).

QUESTION 101:

Direct Sequence Spread Spectrum (DSSS) technology uses _____ Mhz carriers on which to transmit data.

A. 1
B. 2
C. 5
D. 11

Answer: A

Explanation: DSSS utilizes 1 Mhz carriers (Chapter 3, page 76).

QUESTION 102:

Which of these has an effect on Wireless LAN throughput? (Choose two)

A. Distance between transmitter and receiver.
B. Use of fragmentation.
C. Temperature of environment.
D. Channel being used.

Answer: A, B

Explanation: Wireless LAN throughput is affected by the distance between the transmitter and receiver (lesser distance, lesser error-rate, thus greater throughput) and the amount of fragmentation being utilized. The lesser the fragmentation, the fewer packets need to be sent and the greater the throughput. Therefore, the answer should be A,B.

QUESTION 103:

Wireless LAN throughput is based, in part, on which two of these?

A. Standard or Proprietary protocols.
B. Whether a hub or switch is connected to the Ethernet port of the access point.
C. Use of RTS/CTS.
D. Air density in surrounding area.

Answer: A, C

Explanation: Wireless LAN throughput is also affected by usage of Proprietary data-link layer protocols and RTS/CTS. Using RTS/CTS increases overhead over the network due to the continous handshaking process for each packet sent on the network. This reduces WLAN throughput. Thus the answer should be A,C.

QUESTION 104:

Which spread spectrum technology is recommended for environments that have narrowband interference?

A. Infrared
B. Direct Sequencing
C. Frequency Hopping
D. Wide Band

Answer: C

Explanation: According to the study guide, FHSS systems are more resistent to Narrowband interference then DSSS systems. This is due to the agility of FHSS systems and their utilization of the entire 2.4 Ghz band (83.5 Mhz). Since HomeRF is an FHSS implementation and IrDA does not utilize RF technology.

QUESTION 105:

Wireless LAN throughput is partially based on which of the following variables?

A. Use of acknowledgements on the network.
B. Whether Infrared or Spread Spectrum is used.
C. Packet size is use.
D. Manufacturer's hardware limitations.

Answer: B, C

Explanation: Infrared (IR) is a light-based transmission technology and is not spread spectrum-spread
spectrum technologies all use RF radiation. IR devices can achieve a maximum data rate of 4 Mbps at close range, but as a light-based technology, other sources of IR light can interfere with IR transmissions. The typical data rate of an IR device is about 115 kbps, which is good for exchanging data between handheld devices. An important advantage of IR networks is that they do not interfere with spread spectrum RF networks. For this reason, the two are complementary and can easily be used together.

QUESTION 106:

What is the minimum hop rate for FHSS as specified by the FCC?

A. 1 hop every 1.0 seconds.
B. 1 hop every 0.4 seconds.
C. 1 hop every 0.8 seconds.
D. None of the above.

Answer: B

Explanation: As mentioned in the study guide, according to the rules specified by the FCC, the maximum dwell time that can be set for FHSS systems is 400 ms. Thus after, the frequency must be changed. Thus, the answer should be B (0.4).

QUESTION 107:

Wireless LAN throughput can change based on: (Choose two)

A. Use of polling on the access point.
B. Use of Token Ring or Ethernet on the network backbone.
C. Type of antenna(s) in use.
D. Type of spread spectrum technology in use.

Answer: A, D

Explanation: Wireless LAN throughput can change based on use of PCF mode for the access point and also on the type of spread spectrum technology used (using explanation for question 98). Antenna type only effects system coverage/range. Thus the answer should be A,D.

QUESTION 108:

Using DSSS technology with two access points in the same physical area, the first access point is configured to use channel 6.
Which channel on the second access point should be selected to result in the greatest network throughput?

A. channel 1
B. channel 4
C. channel 8
D. channel 9

Answer: A

QUESTION 109:

Because of the limited number of non-overlapping channels available in the 2.4 GHz 802.11b standard, what is the maximum number of access points that can be co-located without causing contention in the wireless network?

A. 1
B. 2
C. 3
D. 15

Answer: C

Explanation: This question is slightly ambiguous. Since it does not use the word "theoretical max." or "practical max.", there really can be 2 answers to this. However, since the study guide mentions that for most purposes (including channel re-use), 3 co-locatable systems can be setup, thus the answer should be C (3)
Note: It is clearly stated in the study guide that FHSS systems are more co-locatable than DSSS systems. Specifically you can co-locate upto 26 FHSS systems (non-synchronised), where as only 3 are allowed with DSSS systems.

QUESTION 110:

1mW of power is the equivalent to which of the following?

A. 0dB
B. +10dB
C. +10dBi
D. 0 dBm

Answer: D

Explanation:
For absolute measurements, the reference power P2 is defined at 1 milliwatt, hence dBm, and 0 dBm = 1 mW:

dBmPower unit	mWpower unit	dBmPower unit	mWpower unt
+20	100 mW	-30	1 µW
+10	10 mW	-40	100 nW
0	**1 mW**	**-50**	**10 nW**
-10	100 µW	-60	1 nW
-20	10 µW	-70	100 pW

QUESTION 111:

Which of these will be needed to perform a site survey? (Choose two)

A. Access to the customer's computer systems
B. Physical access to the facility
C. Ladders and/or lifts
D. RF signal generator

Answer: B, D

QUESTION 112:

What happens to packets destined to sleeping wireless stations when using a BSS?

A. They are dropped by the access point
B. They are buffered by the access point
C. They are sent to the sleeping station
D. They are buffered to the source station

Answer: B

QUESTION 113:

The 802.11 standard defines which of the following data rates for DSSS?

A. 1Mb
B. 2Mb
C. 1 & 2Mb
D. 1, 2, 5.5, AND 11Mb

Answer: C

Explanation:
IEEE 802.11. This standard specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps using either direct sequence (DSSS) or frequency hopping spread spectrum (FHSS). IEEE 802.11b data is encoded using DSSS (Direct Sequence Spread Spectrum) technology. DSSS works by taking a data stream of zeros and ones and modulating it with a second pattern, the chipping sequence.

QUESTION 114:

What is the final step in conducting a proper site survey?

A. Interviewing network users for necessary requirements of the WLAN.
B. Measuring RF coverage in the area to be serviced by the WLAN.
C. Providing an RF Site Survey Report.
D. Identifying possible sources of RF signal and interference.

Answer: C

QUESTION 115:

-Which of the following has been designated by NIST as a backup algorithm to AES?

A. MARS
B. RC6
C. Twofish
D. Serpent
E. DES
F. None of the above.

Answer: F

QUESTION 116:

Which of these is the default authentication method as specified in the IEEE 802.11 standard?

A. Open System
B. Shared Key
C. Dynamic Key
D. No default authentication setting is specified in 802.11

Answer: A

Explanation:
Authentication.IEEE802.11 supports two subtypes of authentication services: Open System and Shared Key. The type of authentication invoked is controlled by the AuthenticationType parameter while the type of authentication that may be accepted by a STA is controlled by the security-related Management Information Base (MIB) attribute dot11AuthenticationType. Open System is a default null authentication algorithm that involves a two-step process consisting of an identity assertion and request for authentication followed by authentication result.

QUESTION 117:

Which of the following tasks must be included in a long-distance RF Path Survey?

A. Determine the antenna location coordinates.
B. Documenting seasonal changes in the environment.
C. Determine all current and future path obstructions.
D. Whether the link is over water or land.

Answer: C

QUESTION 118:

The following statement: "When using high quality cables and connectors in a wireless LAN, the signal strength will not degrade", is:

A. Always true
B. Always false
C. Depends on the lengths of cable.
D. Depends on the type of adapter.

Answer: B
No matter how high the quality of the connectors and cable you are using there will always be some degradation or attenuation.

Connectors drop about .25dB
See CWNA Official Study Guide, 3rd Edition, Page 160

QUESTION 119:

What type of modulation does 2Mbps DSSS use?

A. GFSK
B. BPSK
C. QPSK
D. CCK

Answer: C

Explanation:
Table 1 summarizes the IEEE WLAN standards:

	802.11	802.11a	802.11b	802.11g
Standard Approved	July 1997	September 1999	September 1999	Draft stage. Completion expected in 2002.
Available Bandwidth	83.5 MHz	300 MHz	83.5 MHz	83.5 MHz
Unlicensed Frequencies of Operation	2.4-2.4835 GHz DSSS, FHSS	5.15-5.35 GHz OFDM 5.725-5.825Ghz OFDM	2.4-2.4835GHz DSSS	2.4-2.4835GHz DSSS, OFDM
Number of Non-Overlapping Channels	3 (Indoor/Outdoor)	4 Indoor (UNII1) 4 Indoor/Outdoor (UNII2) 4 Outdoor (UNII3)	3 (Indoor/Outdoor)	3 (Indoor/Outdoor)
Data Rate per Channel	2, 1 Mbps	54, 48, 36, 24, 18, 12, 9, 6 Mbps	11, 5.5, 2, 1 Mbps	54, 36, 33, 24, 22, 12, 11, 9, 6, 5.5, 2, 1 Mbps
Modulation Type	DQPSK (2 Mbps DSSS) DBPSK (1 Mbps DSSS) 4GFSK (2Mbps FHSS) 2GFSK (1Mbps FHSS)	BPSK (6, 9 Mbps) QPSK (12, 18 Mbps) 16-QAM (24, 36 Mbps) 64-QAM (48, 54 Mbps)	DQPSK/CCK (11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)	OFDM/CCK (6,9, 12,18,24,36,48,54) OFDM (6,9,12,18, 24,36,48,54) DQPSK/CCK (22, 33, 11, 5.5 Mbps) DQPSK (2 Mbps) DBPSK (1 Mbps)
Compatibility	802.11	Wi-Fi5	Wi-Fi	Wi-Fi at 11Mpbs and below

Modulation Type: DQPSK uses 2 Mbps DSSS.

QUESTION 120:

Wireless stations communicating without the use of an access point are known collectively as:

A. Client mode
B. Client Peer mode
C. Infrastructure mode
D. Basic Service Set
E. Independent Basic Service Set

Answer: E

Explanation:
Independent Basic Service Set Identifier (IBSSID) - A special case of SSID used to identify a network of wireless computers configured to communicate directly with one another without using an access point.

QUESTION 121:

When packets are queued at the access point for a sleeping station, which of the following takes place for stations to receive their queued packets? (Choose three)

A. The AP transmits information about which stations have queued packets.
B. The AP retransmits the packets at an interval until the station receives it and sends acknowledgement.
C. Stations request their queued packets from the access point.
D. Stations awake at a pre-known time.
E. The AP transmits an ATM to the clients to wake them up.

Answer: A, C, E

QUESTION 122:

As a signal propagates through space, it tends to degrade as its wave becomes wider with distance.
This phenomenon is called:

A. Expansion Loss
B. Free-Space Path Loss
C. Transmission Obfuscation
D. Connection-point Attenuation

Answer: B

Explanation:
As the transmitted signal traverses the atmosphere its power level decreases at a rate inversely proportional to the distance traveled and proportional to the wavelength of the signal. The formula used by RF Workbench accounts for only the diminishing voltage without accounting for absorption or dispersion by the atmosphere. Click here for a 1-way calculator and here for a 2-way (radar) calculator.

$$\text{Path Loss} = 20 * \log_{10}\left[\frac{4 * \Pi * d}{\lambda}\right] \{dB\}, \text{ where } \begin{vmatrix} d = \text{distance } \{\text{same units as } \lambda\} \\ \lambda = \text{wavelength } \{\text{same units as } d\} \end{vmatrix}$$

QUESTION 123:

Which of the following statements are true of a peer-to-peer connection using a wireless LAN?

A. It requires an Access Point to connect two or more wireless clients together.
B. It requires a Bridge to connect two or more wireless clients together.
C. It requires both an Access Point and a Bridge to connect the wireless clients.
D. It does not require an Access Point or a Bridge for the clients to connect to each other.

Answer: D

QUESTION 124:

WLAN solutions may include use of _____ as part of the security solution.

A. 802.1b
B. CGMP
C. HSRP
D. RADIUS

Answer: D

QUESTION 125:

Voltage Standing Wave Ratio can be caused by:

A. Mismatched impedance between devices in series with the main signal.
B. Reflected DC voltage on the main signal line.
C. RF signal diffusion or scattering.
D. Inductance (crosstalk) between adjacent conductors.

Answer: A

QUESTION 126:

After August 31, 2000, the FCC allows a minimum of how many channels with a 2.4 GHz FHSS system before repeating the pattern?

A. 6
B. 15
C. 22
D. 30

Answer: B

QUESTION 127:

What link speeds does the IEEE 802.11 standard support?

(Select all that apply.)

A. 1 Mbps
B. 2 Mbps
C. 5.5 Mbps
D. 11 Mbps

Answer: A, B

Explanation: According to the study guide, the IEEE 802.11 standard supports 1 & 2 Mbps link speeds. Thus the answer should A,B

QUESTION 128:

Which of these are true regarding the IEEE 802.11a standard?
Select all that apply.

A. Supports speeds up to 54 Mbps.
B. Supports speeds up to 22 Mbps.
C. Operates in the 5 GHz UNI bands.
D. Operates in the 2.4 GHz ISM band.
E. Used OFDM modulation technology.
F. Uses CCK modulation technology.

Answer: A, C, E

QUESTION 129:

Whole in AD HOC mode, a wireless LAN network operates using which function?

A. PCP
B. DCF
C. CD-Poll
D. DF-Poll

Answer: B

Explanation: The answer is definitely B which is DCF. In PCF an AP is required for polling and in ad-hoc mode there is no AP.
DCF (Distributed Coordination Function).
PCF (Point Coordination Function)

QUESTION 130:

When implementing dynamic rate shifting with a DSSS system, as the range increases, what

happens to the speed of the transmission?

A. The range will have no effect on the speed.
B. As the range increases the speed decreases.
C. As the range increases the speed increases.
D. Dynamic rate selection can only be used with FHSS.

Answer: B

QUESTION 131:

When a station drops its speed due to Automatic Rate Selection it:

A. Decreases its power output level to transmit at a slower speed.
B. Changes the data modulation type or the code keying sequence.
C. Increases its power output level to attempts to maintain connection speed.
D. Increases the fragmentation threshold to maintain greater throughput.

Answer: B

Explanation: Since each link speed has a different modulation technique associated with it, the modulation type and the code spreading technique is changed when the speed drops. However, there is no change in power output level and power output does not affect throughput/speed. Thus the answer should be B.

QUESTION 132:

Which of these spread spectrum technologies requires Line of Sight to operate properly? (Select all that apply.)

A. Frequency Hopping
B. Infrared
C. Direct Sequencing
D. Laser

Answer:
A. C

Explanation: According to the study guide, all spread spectrum technologies require line-of-sight (RF LOS) to operate properly. Therefore, the answer should be A,C.

QUESTION 133:

Which of these is NOT part of the RF coverage map that will be included with the RF Site Survey Report?

A. Maximum number of users for each cell.
B. Coverage area of each cell.
C. Channel of each cell.
D. Power settings of each access point.
E. Antenna type used with each access point.

Answer: A

QUESTION 134:

In terms of RF power, 1 Watt (1000 mW) = _____ dBm.

A. 3
B. 10
C. 20
D. 30
E. None of the above.

Answer: D

QUESTION 135:

Where is the SSID stored in a client computer?

A. PC Card firmware
B. Windows registry
C. On the Master Boot Record of the hard drive.
D. On the hard drive as an encrypted file.
E. SSIDs are not stored on client computers.

Answer: E

QUESTION 136:

A network administrator wishing to give access to a group of wired users in a remote building on a campus would deploy which WLAN devices to accomplish this task? (Choose two)

A. Wireless Gateway at the central building.
B. Workgroup Bridge at the remote building.
C. Wireless Bridge at the remote building.
D. Access Point at the central building.
E. USB client at the remote building

Answer: C, D

QUESTION 137:

Which organization is responsible for determining acceptable output power limitations for the UNII bands in the United States?

A. FCC
B. IEEE
C. ETSI
D. IrDA

Answer: A

QUESTION 138:

Which of the following frequency ranges is NOT an ISM band?

A. 902 - 928 MHz
B. 2.400 - 2.500 GHz
C. 5.500 - 5.700 GHz
D. 5.725 - 5.875 GHz

Answer: C

QUESTION 139:

Where can MAC filters be implemented on a wireless LAN?
(Select all that apply.)

A. WLAN Ethernet Converter
B. Wireless Bridges
C. In WLAN clients software that supports EAP
D. Wireless Workgroup Bridges

Answer: B, D

Explanation: Both, Wireless bridges and Wireless Workgroup bridge support MAC filtering. Thus both can implement MAC filters. Therefore, the answer should be B,D.

QUESTION 140:

"Earth Bulge" is a factor when planning wireless data transmission paths longer than:

A. 3 miles / 4.8 kilometers
B. 7 miles / 11.2 kilometers
C. 15 miles / 24 kilometers
D. 22 miles / 35.2 kilometers

Answer: B

QUESTION 141:

TO form a WEP key, the WEP secret keys is concatenated with the:

A. Plain text
B. IV
C. PRNG
D. ICV
E. Keystream

Answer: B

QUESTION 142:

What is an advantage of having a long dwell time when using a FHSS system?

A. Increased resistance to narrowband interference
B. Increased range
C. Increased data throughput
D. Increased security

Answer: C

QUESTION 143:

Which is true of the Service Set Identifier (SSID)? (Select all that apply.)

A. It has a maximum length of 32 bytes
B. It is case se sensitive
C. It is alphanumeric
D. At least 8 characters must be uppercase
E. It must be uppercase

Answer: A, B, C

Explanation: According to the study guide, the SSID is from 2-32 characters long, is case-sensitive and is composed of alphanumeric characters. Thus the answer should be A,B,C.

QUESTION 144:

What is the effective range of HomeRF?

A. 150 feet / 45.7 meters
B. 300 feet / 90.4 meters
C. 500 feet / 152.4 meters
D. 1000 feet / 304.8 meters

Answer: A

QUESTION 145:

What is the VERTICAL beam width of an omni-directional antenna?

A. 45 degrees
B. 75 degrees
C. 360 degrees
D. It varies

Answer: D

Explanation: The vertical beam-width of an omni-directional antenna is from 7 to 80 degrees while the horizontal beam-width is 360 degrees.

QUESTION 146:

What is the effective range of broadcast infrared?

A. 60 feet / 18.3 meters
B. 150 feet / 45.7 meters
C. 300 feet / 91.4 meters
D. 1000 feet / 304.8 meters

Answer: B

QUESTION 147:

Which of the following are NOT considered WLAN security solutions (Select all that apply.)

A. Use of VLANs on switches
B. Passive Scanning Probes
C. Wi-Fi hardware certification
D. Shared Key Authentication

Answer: B, C

Explanation: According to the Study Guide, Wi-Fi hardware certification specifies

inter-operatibility b/w 802.11b devices. It is not considered a WLAN security solution and neither is passive scanning. Therefore, the answer should be B,C.

QUESTION 148:

Common network management protocols supported in access points include: (Choose two)

A. http
B. snmp
C. smtp
D. rsvp
E. ftp

Answer: A, B

Explanation: Answer is A and B not B and C as given. See Pages 231 CWNA Study Guide 3rd edition. Access is via HTTP or HTTPS when a built-in web server exist in the AP.

QUESTION 149:

An access point is emitting a 100 mW signal that is connected to a length of cable with a 3 dB loss. If the cable is then connected to a +9 dBi antenna, what is the EIRP from the antenna in dBm?

A. 20 dBm
B. 23 dBm
C. 29 dBm
D. 26 dBm

Answer: D

QUESTION 150:

When performing a site survey for a hospital application, potential sources of RF interference include which of the following?

A. High population of patients
B. Long hallways
C. Fire doors
D. Metal blinds

Answer: D

QUESTION 151:

Which one of the following is NOT important to have access to in order to perform an RF site

survey on a warehouse facility?

A. Facility blueprints
B. Forklift for moving stored materials when necessary
C. Lifts for mounting access points
D. Termination closet locations

Answer: B

QUESTION 152:

The term "Wireless LAN Gateway" can describe which of the following?

A. A wireless client performing routing functions for other clients in an Ad Hoc network.
B. A VPN device sitting between an access point and a distribution switch on a network.
C. A specialized access point with VPN and Layer 3 services.
D. All of the above.

Answer: C

QUESTION 153:

Which two functions are configurable on a WLAN client computer as part of the WLAN client utility software? Select two.

A. SSIDs
B. WEP keys
C. Access Control Lists
D. Beacon management frames
E. FTP Client

Answer: A, B

QUESTION 154:

What is the purpose of a wireless Ethernet Converter? (Choose two)

A. To bridge between Ethernet segments on a wireless LAN.
B. To connect a client with a wired network interface card to a wireless network.
C. To connect an access point to a wireless bridge.
D. To eliminate computer disassembly while adding wireless LAN functionality.

Answer: B, D

Explanation: According to the study guide, a wireless Ethernet converter may be used to

connect a wired NIC to a wireless network. Additionally, it prevents disassembly of a PC desktop for installation of a wireless NIC card into a PCI slot for example. In this case, the already installed wired NIC may be connected to the wireless network by means of a wireless
ethernet converter. A Wireless LAN does NOT have any ethernet segments. Therefore, the answer should be B,D

QUESTION 155:

Antenna GAIN is denoted by use of which of the following?

A. +dBi
B. -dBi
C. +dB
D. +dBm

Answer: A

Explanation:
When quantifying the gain of an antenna, the decibel units are represented by dBi. The unit of measurement dBi refers only to the gain of an antenna. The "i" stands for "isotropic", which means that the change in power is referenced against an isotropic radiator.
Reference:
CWNA Official Study Guide, Page 34

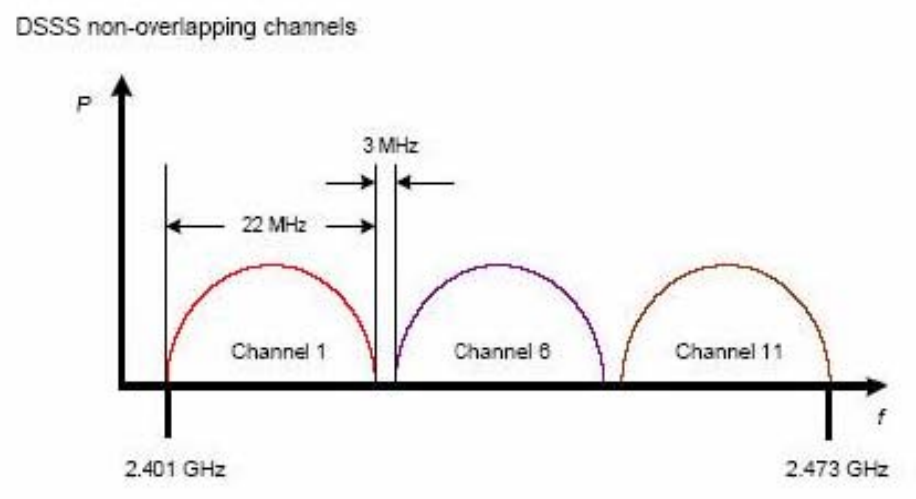
QUESTION 156:

What is the maximum number of non-overlapping DSSS channels in the 2.4 GHz ISM band?

A. 3
B. 5
C. 6
D. 11

Answer: A

Explanation:
There is a maximum of three co-located direct sequence systems possible because channels 1, 6 and 11 are the only theoretically non-overlapping channels. The 3 non-overlapping channels are illustrated in the Figure.



Reference:
CWNA Official Study Guide, Page 57

QUESTION 157:

Using the Wi-Fi Interoperability Test Plan, which of the following are goals of the Wireless Ethernet Compatibility Alliance (WECA):

A. To finalize the IEEE 802.11b standard.
B. To ensure interoperability among 802.11b devices.
C. To finalize the Wi-Fi standard.
D. To promote the use of 802.11b technology.

Answer: B

Explanation:
The Wireless Ethernet Compatibility Alliance (WECA) provides testing of 802.11b compliant DSSS wireless LAN equipment to ensure that such equipment will operate in the presence of and interoperate with other 802.11b DSSS devices. The interoperability standard that WECA created and now uses is called Wireless Fidelity, or Wi-Fi , and those devices that pass the tests for interoperability are "Wi-Fi compliant" devices.
Reference:
CWNA Official Study Guide, Page 60

QUESTION 158:

Prior to August 31, 2001, the FCC mandated a maximum channel bandwidth for FSSS technology of:

A. 1 MHz
B. 2 MHz
C. 5 MHz
D. 11 MHz

Answer: A

Explanation: The Pre August 31, 2000 rule states that the bandwidth is 1 Mhz. See page 74 of the CWNA Study Guide 2nd edition

---

QUESTION 159:

WLAN security solutions may include using: (Select all that apply.)

A. IPSec with shared keys
B. IP unnumbered
C. NLSP with SPX support
D. TKIP
E. Static session keys

Answer: A, D

Explanation: WLAN security solutions mentioned in the study guide include IPSec with shared keys (for Wireless VPN) and the Temporal Key Integrity Protocol (TKIP).

QUESTION 160:

Wireless LANs are designed to play what role(s) in a network?

A. Access
B. Distribution
C. Core
D. All of the above

Answer: A

Explanation:
Wireless LANs are deployed in an access layer role, meaning that they are used as an entry point into a wired network. In the past, access has been defined as dial-up, ADSL, cable, cellular, Ethernet, Token Ring, Frame Relay, ATM, etc. Wireless is simply another method for users to access the network.
Reference:
CWNA Official Study Guide, Page 4

QUESTION 161:

Which of the following are disadvantages of a wireless LAN in comparison to a wired LAN?

A. Offers less throughput
B. Initially more expensive

C. Not easily scalable
D. Difficult to modify the network

Answer: A

Explanation:
As with any relatively new technology, there are many issues that affect implementation and utilization of wireless
networks. There are both common and specific issues depending on the type of wireless network. Some of the common factors include electromagnetic interference and physical obstacles that limit coverage of wireless networks, while others are more specific, such as standards, data security, throughput, ease of use, etc.

QUESTION 162:

What type of modulation is used for 2Mbps FHSS?

A. GFSK
B. BPSK
C. QPSK
D. CCK

Answer: A

Explanation:
Modulation and Spreading Code Types for 802.11 & 802.11b

	Spreading Code	Modulation Technology	Data Rate
2.4 GHz DSSS	Barker Code	DBPSK	1 Mbps
	Barker Code	DQPSK	2 Mbps
	CCK	DQPSK	5.5 Mbps
	CCK	DQPSK	11 Mbps
2.4 GHz FHSS	Barker Code	2GFSK	1 Mbps
	Barker Code	4GFSK	2 Mbps

It can be seen from the table that 2 Mbps FHSS uses the GFSK Modulation Technology.
Reference:
CWNA Official Study Guide, Page 214

QUESTION 163:

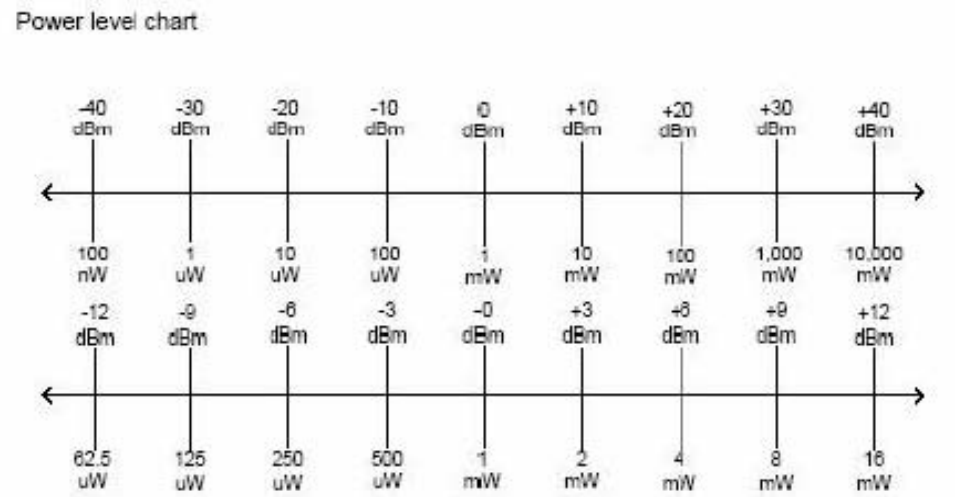
The measure of 100 mW of power is equivalent to which of the following units of measure?

A. +20 dBm
B. -20 dBm
C. +20 dB

D. -20 dB

Answer: A

Explanation:
It can be seen from the graph that +20dBm means 100mW of Power



Reference:
CWNA Official Study Guide, Page 33

QUESTION 164:

Which of the following link speeds are supported by the IEEE 802.11b standard?

A. 1 Mbps
B. 2 Mbps
C. 5.5 Mbps
D. 11 Mbps

Answer: A, B, C, D

Explanation:
IEEE 802.11b devices operating at 5.5 or 11 Mbps are able to communicate with 802.11 devices operating at 1 or 2 Mbps because the 802.11b standard provides for backward compatibility. Users employing 802.11 devices do not need to upgrade their entire wireless LAN in orderto use 802.11b devices on their network.
Reference:
CWNA Official Study Guide, Page 55

QUESTION 165:

Which of the following items are needed to perform a site survey?

A. An encryption key server.

B. Knowledge of nearby RF sources.
C. Wireless workgroup bridge.
D. A mobile equipment cart.
E. TFTP server software.

Answer: D

Explanation:
During most surveys scratch paper, grid paper, and copies of blueprints or floor plans are necessary. When added to the amount of equipment that will be carried around, this amount of paper and documentation tends to become a burden. For this reason, a sufficiently large mobile equipment cart that can contain all the necessary gear is quite useful while moving through a facility.
Reference:
CWNA Official Study Guide, Page 312

QUESTION 166:

What option allows a wireless PC Card to adjust its transmission speed to compensate for the changing nature of the frequency channel?

A. Dynamic Rate shifting
B. Rate Lock Agility
C. Automatic Speed Select
D. Hi-Lo Automatic Adjustment

Answer: A

Explanation:
Adaptive (or Automatic) Rate Selection (ARS) and Dynamic Rate Shifting (DRS) are both terms used to describe the method of dynamic speed adjustment on wireless LAN clients. This speed adjustment occurs as distance increases between the client and the access point or as interference increases. It is imperative that a network administrator understands how this function works in orderto plan for network throughput, cell sizes, power outputs of access points and stations, and security.
Reference:
CWNA Official Study Guide, Page 205

QUESTION 167:

In order to obtain Wi-Fi certification, a manufacturer's OFDM system must adhere to which of the following?

A. Predetermined frequency hopping patterns designated by the IEEE 802.11 standard.
B. Designated power consumption settings as determined by the FCC.
C. AES encryption and support VPN protocols such as PPTP and L2TP.
D. OFDM systems are not included in Wi-Fi certification.

E. A maximum speed of 54 Mbps.

Answer: E

Explanation:
802.11g and 802.11a compliant wireless LAN equipment specify use of orthogonal frequency division multiplexing (OFDM), allowing speeds of up to 54 Mbps, which is a significant improvement over the 11 Mbps specified by 802.11b.
Reference:
CWNA Official Study Guide, Page 215

QUESTION 168:

How is the fragmentation setting configured on a wireless LAN?

A. On the wireless station.
B. On the access point by the network administrator.
C. The network layer protocol being used.
D. Automatically on the access point.

Answer: B

Explanation:
One way to use fragmentation to improve network throughput in times of heavy packet errors is to monitor the packet error rate on the network and adjust the fragmentation level manually.
Reference:
CWNA Official Study Guide, Page 205

QUESTION 169:

Which of the following options is a possible wireless LAN security solution?

A. PPTP
B. 802.11f
C. IRDP
D. 802.11e
E. IrDA

Answer: A

Explanation:
Use of PPTP with shared secrets is very simple to implement and provides a reasonable level of security, especially when added to WEP encryption. Use of IPsec with shared secrets or certificates is generally the solution of choice among security professionals in this arena.

Reference:
CWNA Official Study Guide, Page 276

QUESTION 170:

For which of the following technologies will narrowband RF interference cause significant problems during implementation?

A. FHSS
B. DSSS
C. IrDA
D. HomeRF

Answer: B

Explanation: According to the study guide, FHSS systems are more resistent to Narrowband interference then DSSS systems. This is due to the agility of FHSS systems and their utilization of the entire 2.4 Ghz band (83.5 Mhz). Since HomeRF is an FHSS implementation and IrDA does not utilize RF technology

---

QUESTION 171:

Which of the following statements are TRUE regarding antenna diversity? (Select all that apply.)

A. Both antennas may be used for data transmission simultaneously.
B. Only one antenna may be used for data transmission at any given time.
C. Both antennas may be used for receiving data simultaneously.
D. Only one antenna may be used for receiving data at any given time.

Answer: B, D

Explanation: According to the study guide, antenna diversity is achieved with multiple antennas and multiple inputs to a single receiver. Due to this configuration, only one antenna may be used to receive data at any given time by the receiver (based on the signal strength). Additionally, only one antenna may be used to transmit data at any given time (based on the previous antenna used for signal reception). Therefore, the answer should be B,C.

QUESTION 172:

In a wireless LAN which of the following can cause RF signal gain? (Select all that apply.)

A. Antenna extension cable
B. Attenuator
C. Antenna
D. Connectors

E. Amplifier

Answer: C. E

Explanation: This is a tricky question. Ideally, the candidate would select just the amplifier as the RF signal gain element. However, the study guide mentions time and again that antennas may also be used to increase the gain of the RF signal. Therefore, the answer should be C,E.

QUESTION 173:

Which of the following results should be included in an RF site survey report? Select two.

A. Digital photographs of access point locations.
B. A thorough analysis of the client's existing network infrastructure problems.
C. A spectral analysis of any RF interference.
D. Log files of file transfer throughput tests of the wireless LAN.
E. Screen captures of any network security weakness noted during the site survey.

Answer: A, C

Explanation: According to the study guide, the RF site survey report should include a spectral analysis of any sources of RF interference. Additionally, once the RF coverage areas have been determined and the hardware locations marked out, digital photos of access point locations should also be included as part of the RF site survey report. Therefore,the answer should A,C.

QUESTION 174:

Which of the following statements describe the 802.11 implementation of WEP?

A. WEP use is optional.
B. WEP use is mandatory.
C. WEP using 64-bit (also called 40-bit) encryption is a requirement for Wi-FiTM certification by the Wi-Fi Alliance.
D. WEP using 128-bit (also called 104-bit) encryption is a requirement for Wi-FiTM certification by the Wi-Fi Alliance.
E. WEP must use DES for encryption.

Answer: A, C

Explanation: The 802.11 implenentation of WEP, by the requirements set-forth by the IEEE, should be optional and not mandatory for use with 802.11 complient hardware. Additionally, WEP using 40-bit single keys is also a test and a requirement for Wi-Fi certification.

QUESTION 175:

What weather condition is has NO measurable impact on outdoor spread spectrum WLANs?

A. Lightning
B. Bright sunlight
C. Fog
D. Rain

Answer: B

QUESTION 176:

Which of the following are devices into which a wireless LAN PC Card client device can be inserted? (Select all that apply.)

A. 16-bit ISA slot
B. PCI host adapter
C. SCSI host adapter
D. USB host adapter
E. EIDE controller

Answer: B, D

Explanation: From the information provided for Wireless LAN client devices in the study guide for the CWNA, PCI and USB adapters are used with wireless LAN PC cards for certain implementations. Therefore, the answer should B,D.

QUESTION 177:

What answer below gives the complete text for the acronym EIRP?

A. Equivalent Isotropically Radiated Power
B. Efficient Isolated Radio Power
C. Effective Isotropic Radio Propagation
D. Effective Isolation Radio Prepending

Answer: A

Explanation:
The term used for the power radiated by the antenna is Equivalent IsotropicallyRadiated Power (EIRP).
Reference:
CWNA Official Study Guide, Page 149

QUESTION 178:

Which of the following items are security risks in a wireless LAN? (Select all that apply.)

A. Causal eavesdropping with cellular phones.
B. Spectral analysis
C. RF jamming
D. Packet analysis
E. SNMP support on access points
F. Open access to wireless infrastructure devices

Answer: C, F

Explanation: It is well known that RF jamming is one of the key security risks associated with Wireless LANs. Also, open access (without any type of security) is clearly a security hazard for wireless LANs and a treat for hackers and the like :) Therefore, the answer should C,F.

QUESTION 179:

What is the name of the method by which a mobile client moves beyond the range of one AP and regains access to the wireless network by roaming to a different AP?

A. Reacquiring
B. Reconnecting
C. Reassociation
D. Reapplication

Answer: C

Explanation:
Reassociationusually occurs because the wireless station has physically moved away from the original access point, causing the signal to weaken. In other cases, reassociation occurs due to a change in radio characteristics in the building, or due simply to high network traffic on the original access point. In the latter case, this function is known as loadbalancing, since its primary function is to distribute the total wireless LAN load most efficiently across the available wireless infrastructure.
Reference:
CWNA Official Study Guide, Page 185

QUESTION 180:

Which of the following are possible locations that the MAC address of a wireless LAN access point can be found? (Select all that apply.)

A. Printed on the PC Card that is inserted into the radio set.

B. In the routing table of the access point.
C. Printed on the bottom of the access point.
D. In the access point's setup manual.
E. Broadcasted in beacon management frames.
F. In the manufacturer's OUI file.

Answer: C, E

Explanation: Since this is not specifically mentioned in the study guide for the CWNA, we are not entirely sure about the answer. However, the study guide does clearly indicate that the MAC is always sent in the clear (without any encryption) with any and all types of wireless frames broadcasted. This includes beacons. Therefore the answer should include E

QUESTION 181:

What statement identifies the purpose of an RP site survey seport?

A. To record throughput results according to documented requirements.
B. To detail security options.
C. To offer possible vendor-specific solutions.
D. To record measurements of RF coverage and interference in a given area.
E. To test the environment for possible RP leakage.

Answer: D

QUESTION 182:

Which of the following may result from using RTS/CTS in a wireless LAN?

A. Interframe spacing is increased resulting in additional network overhead.
B. Increased network security due to frame authentication.
C. Decreases latency due to frame fragmentation.
D. Decreases network overhead due to the hidden node problem.

Answer: D

Explanation: According to the study guide, in a situation where a hidden node problem has occurred in the wireless network, RTS/CTS may be used to eliminate the overhead of the continous collision of packets that is severely decreasing the overall throughput of the Wireless LAN. RTS/CTS is not associated with frame fragmentation. Therefore, the answer should be D.

QUESTION 183:

What is a method of client authentication onto a wireless LAN?

A. PLCP login layer
B. Open System authentication
C. PMD zones
D. CSMA/CA

Answer: B

Explanation:
The open system authentication is the default method of authentication between your card and the access point. Anybody that wants to be authenticated with the base station can be. Even when this information is sent using the
wired equivalent privacy protocol (WEP), which is designed to provide for confidentiality when using a wireless
network, the authentication management frames are still sent in clear text, thus helping to defeat the use of this particular security protocol.

QUESTION 184:

What option describes a device that supports VPN connectivity and authentication for wireless access users?

A. Enterprise Wireless Gateway
B. Residential Wireless Gateway
C. Wireless Workgroup Bridge
D. Network Layer Bridge

Answer: A

Explanation:
Authentication technologies incorporated into enterprise wireless gateways are often built into the more advanced levels of access points. For example, VPN and 802.1x/EAP connectivity are supported in many brands of enterprise level access points.
Reference:
CWNA Official Study Guide, Page 93

QUESTION 185:

According to the IEEE 802.11 standard, what is the largest frame size that can traverse a wireless LAN without mandatory fragmentation?

A. 1492 bytes
B. 1500 bytes
C. 2346 bytes
D. 9000 bytes

Answer: C

Explanation:
Data frame is variable in length (29-2346 bytes). Duration ID field contains a value, measured in microseconds from the end of the frame, sufficient to protect the transmission of a subsequent acknowledgement frame. If the data frame is multicast address, the duration/ID value is zero.

QUESTION 186:

What is the maximum number of nodes that a HomeRF wireless LAN can accommodate?

A. 64
B. 127
C. 512
D. 1024

Answer: B

Explanation:
Note: The book specifies the max. as 25 nodes.

QUESTION 187:

Which of the following are appropriate uses of an IEEE 802.11b wireless LAN?

A. Mobile access into the company network form a PDA.
B. 'Core' role in a large network.
C. Building-to-building campus bridging.
D. Delivering data from applications that require full-duplex communications between nodes.

Answer: A, C

QUESTION 188:

What is the minimum rate for Frequency Hopping with HomeRF's SWAP protocol?

A. 4 hops/second
B. 30 hops/second
C. 50 hops/second
D. 400 hops/second

Answer: C

Explanation: We not sure what the minimum hopping rate for a HomeRF system is. However, the standard hopping rate for HomeRF is 50 hops/second. Therefore, we presume that the answer is 50 hops/second (C).

QUESTION 189:

What method of identity verification is used by Open System Authentication?

A. VPN
B. EAP
C. ACL
D. Null

Answer: D

Explanation:
Open authentication is a null authentication algorithm. The access point will grant any request for authentication. It might sound pointless to use such an algorithm, but open authentication has its place in 802.11 network authentication. Authentication in the 1997 802.11 specification is connectivity-oriented.

QUESTION 190:

Which of the following indicates a decrease in the amplitude of an RF signal caused by an external interference source?

A. Inductance
B. Reactance
C. Loss
D. Amplification

Answer: C

QUESTION 191:

What is the expended text form for the wireless LAN security acronym WEP?

A. Wireless Equivalent Protocol
B. Wired Equivalent Privacy
C. Wireless Enhances Privacy
D. Wires Enhanced Protocol

Answer: B

Explanation:
Open System authentication is a very simple process. As the wireless LAN administrator, you have the option of using WEP (wired equivalent privacy) encryption with Open System authentication.
Reference:
CWNA Official Study Guide, Page 174

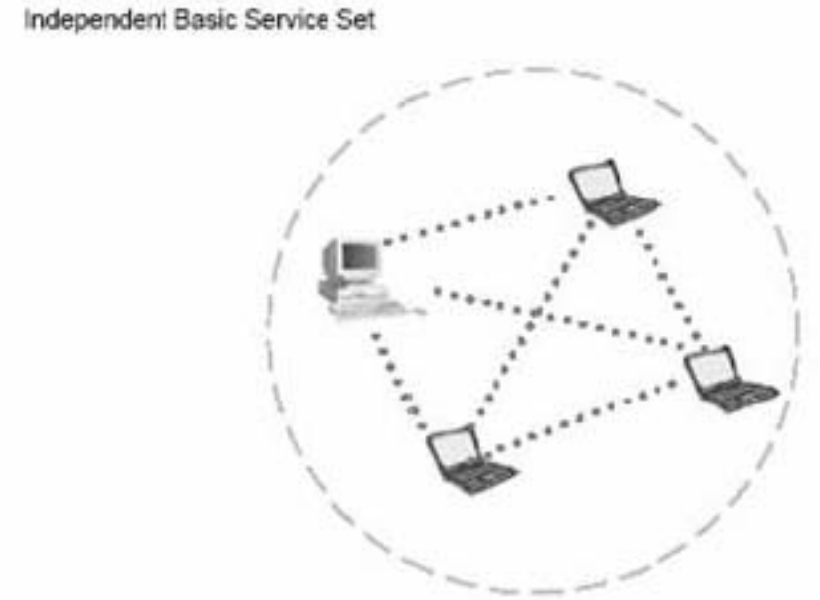
QUESTION 192:

What Wireless LAN configuration implements power management by having stations transmit beacons after they awake from sleep mode?

A. Integrated Service Set (IIS)
B. Basic Service Set (BSS)
C. Independent Basic Service Set (IBSS)
D. Extended Service Set (ESS)

Answer: C

Explanation:
An independent basic service set is also known as an ad hoc network. An IBSS has no access point or any other access to a distribution system, but covers one single cell and has one SSID, as shown in Figure 7.11. The clients in an IBSS alternate the responsibility of sending beacons since there is no access point to perform this task.



Reference:
CWNA Official Study Guide, Page 182

QUESTION 193:

By default, what type of authentication is used by IEEE 802.11 devices?

A. Shared Key authentication
B. Open System authentication
C. No authentication
D. IEEE 802.11 does not specify any authentication types.

Answer: B

Explanation:
Open System authentication is a method of null authentication and is specified by the IEEE 802.11 as the default setting in wireless LAN equipment. Using this method of authentication, a station can associate with any access point that uses Open System authentication based only on having the right service set identifier (SSID).
Reference:
CWNA Official Study Guide, Page 174

QUESTION 194:

Which of the following factors must be considered whenever encryption and authentication are to be implemented in any system?

A. The customer's need for privacy
B. Ease of use & implementation
C. Government regulations
D. Manufacturer liability

Answer: A

QUESTION 195:

Which of the following types of antennas can be used for Antenna Diversity?

A. Dipole
B. Omni-directional
C. Patch
D. Parabolic Dish
E. Yagi
F. Parabolic Grid

Answer: A, B

Explanation: Omni-directional/Dipole antennas are the most appropriate for use in antenna diversity situations.

QUESTION 196:

802.11b DSSS performance is negatively affected by which of the following factors? (Select three.)

A. Co-located DSSS on non-overlapping channels
B. Multipath
C. Co-located Bluetooth

D. Near/Far problem
E. Co-located high power infrared
F. Low power narrowband outside the DSSS channel

Answer: B, C, D

Explanation: From the study guide, 802.11b DSSS is affected by the negative effects of Multipath and all-band intereference (in this case, a co-located Bluetooth device). Although Near/far is a performance problem for a remote client station, it does not necessarily have a negative impact on the Wireless LAN as a whole.

QUESTION 197:

According to the IrDA, what is the maximum speed for an Infrared LAN system?

A. 1Mbps
B. 2Mbps
C. 4Mbps
D. 10Mbps

Answer: C

Explanation: According to the study guide and the information present on the IrDA web-site, the max. speed for a Infra-red LAN system is 4mpbs. Therefore the answer should be C.

QUESTION 198:

Manufactures of 802.11 compliant wireless LAN client devices allow for configuration of which of the following?

A. 802.1q tagging
B. Shared Key authentication
C. TKIP accounting
D. Private security authorization
E. Open System authentication

Answer: B, E

Explanation:
The IEEE 802.11 standard specifies two methods of authentication: Open System authentication and Shared Key authentication. The simpler and also the more secure of the two methods is Open System authentication. For a client to become authenticated, the client must walk through a series of steps with the access point.
Reference:
CWNA Official Study Guide, Page 174

QUESTION 199:

What term best describes a device designed to increase the power of the RF signal in a wireless LAN?

A. Attenuator
B. RF Injector
C. Amplifier
D. Active Ethernet

Answer: C

QUESTION 200:

What spread spectrum technology is more scalable for increasing the number of simultaneously active, co-located systems?

A. FHSS
B. DSSS
C. IrDA
D. 802.11b

Answer: A

Explanation: An understood advantage and also one of the biggest advantages of DSSS systems over FHSS systems is greater system throughput (speed). In DSSS, speeds of upto 11 mbps can be acheived whereas FHSS only allows a max. of 2 Mbps (while simultanously operating in 802.11 compliant mode).

QUESTION 201:

What unit of measurement is used to determine the insertion loss on wireless LAN splitters?

A. dB
B. dBi
C. dBm
D. milliwatts

Answer: A

Explanation:
Power gain and loss are measured in decibels, not in watts, because gain and loss are relative concepts and a decibel is a relative measurement. Gain or loss in an RF system may be referred to by absolute power measurement (e.g. ten watts of power) or by a relative power measurement (e.g. half of its power).

Reference:
CWNA Official Study Guide, Page 31

QUESTION 202:

Which of the following are security issues within the 802.11 standard? (Select all that apply.(Select all that apply.)

A. No support for encryption.
B. No support for roaming.
C. Vulnerable to disassociation attacks.
D. No central authentication, authorization, or accounting support.
E. Specifies use of the SSID as a dynamic security mechanism.

Answer: C, D

QUESTION 203:

What statement defines the term POLARIZATION?

A. The power supply's positive/negative orientation.
B. The signal's modulation type (Amplitude-, Frequency-, or Pulse Width-Modulated).
C. The antenna's latitudinal position, with respect to the North and South Poles.
D. The vertical or horizontal orientation of the electrical field around the antenna.

Answer: D

Explanation:
Polarization is the physical orientation of the antenna in a horizontal or vertical position. The electric field is parallel to the radiating elements (the antenna element is the metal part of the antenna that is doing the radiating) so, if the antenna is vertical, then the polarization is vertical.
Horizontal polarization - the electric field is parallel to the ground
Vertical polarization - the electric field is perpendicular to the ground
Reference:
CWNA Official Study Guide, Page 112

QUESTION 204:

An access point that emits a 1000 milliwatt signal is connected to a cable and its connectors with 10 dB loss. The cable is then connected to a 3 dB gain antenna.
What is the resulting EIRP in milliwatts from the antenna?

A. 100 mW
B. 200 mW
C. 300 mW

D. 500 mW

Answer: B

QUESTION 205:

What may result when a 2.4 GHz DSSS phone is located near an 802.11b compliant access point?

A. The phone will always interfere with the access point.
B. The access point will always interfere with the phone.
C. The phone will interfere with the access point when they are on the same channel.
D. The access point will always avoid use of the same frequencies that the phone is using.
E. The phone will always choose a channel different from the access point.

Answer: C

Explanation:
Microwave ovens, 2.4 GHz cordless phones, radiology equipment, and baby monitors are common sources of RF interference in the 2.4 GHz band. These potential interference sources need to be documented in the survey as potential problems with the installation. Microwave ovens can easily be replaced, though radiology equipment in a hospital installationmay not be. 2.4 GHz phones running on the same channel as the wireless LAN can render a wireless LAN useless.
Reference:
CWNA Official Study Guide, Page 323

QUESTION 206:

Which of the following utilities might be included in the utility software for a wireless LAN client device? (Select all that apply.)

A. Wireless LAN client radio diagnostics
B. IP diagnostics
C. FRP client
D. Site monitor
E. Link test utility
F. Beacon modification utility

Answer: D, E

Explanation: Utilities that are provided in the software for a Wireless LAN client device would include the Site Monitor software as well the Link test utility.

QUESTION 207:

What term indicates an RF signal that bounces off a smooth or coated surface and changes signal direction?

A. Diffraction
B. Reflection
C. Refraction
D. Diffusion
E. Scattering

Answer: B

Explanation:
Reflection occurs when a propagating electromagnetic wave impinges upon an object that has very large dimensions when compared to the wavelength of the propagating wave. Reflections occur from the surface of the earth, buildings, walls, and many other obstacles. If the surface is smooth, the reflected signal may remain intact, though there is some loss due to absorption and scattering of the signal.
Reference:
CWNA Official Study Guide, Page 20

QUESTION 208:

Which of the following is a type of highly directional antenna?

A. Yagi
B. Parabolic Dish
C. Patch
D. Dipole

Answer: B

Explanation:
As their name would suggest, highly-directional antennas emit the most narrow signal beam of any antenna type and have the greatest gain of these three groups of antennas. Highly-directional antennas are typically concave, dish-shaped devices, as can be seen in Figures 5.10 and 5.11. These antennas are ideal for long distance, point-to-point wireless links. Some models are referred to as parabolic dishes because they resemble small satellite dishes.
Reference:
CWNA Official Study Guide, Page 110

QUESTION 209:

What organization created the 802.11 standard?

A. Wi-Fi Alliance
B. WLIF

C. IEEE
D. ISO

Answer: C

QUESTION 210:

Wireless LAN client utility software may include which of the following components?

A. VPN client software
B. Personal firewall software
C. Intrusion detection software
D. A load balancing feature
E. EAP authentication

Answer: D

Explanation:
With replicated servers, authentication requests are routed to the fastest performing server, resulting in more efficient performance. RSA ACE/Agent(r) software provides this load balancing by detecting server response times and routing the requests accordingly. Administrators can also define manual load balancing sequences.

QUESTION 211:

The 802.11b standard specifies which of the following power modes of operation?

A. Awake Signal Standby Mode
B. Beacon Poll Mode
C. Continuous Aware Mode
D. Power Save Polling Mode

Answer: C, D

Explanation: The 802.11b standard specifies two power modes: Continous Aware Mode (CAM) and Power Save Polling mode (PSP). Therefore, the answer should be C,D.

QUESTION 212:

Which of the following pieces of equipment are needed to perform a wireless LAN site survey? (Select all that apply.)

A. A laptop or handled computer
B. A desktop PC
C. An Ethernet hub
D. A wireless LAN PC Card

E. A wireless workgroup bridge

Answer: A, D

Explanation: Some of the essential equipment needed for a site survey include a labtop/PDA and a wireless LAN PC card. Therefore, the answer should be A,D.

QUESTION 213:

Antenna dissipative LOSS is denoted by use of which of the following measurement units?

A. +dB
B. -dBi
C. +dBi
D. +dBm

Answer: B

QUESTION 214:

The IEEE 802.11 standard defines which of the following modes of operation for an 802.11 compliant wireless LAN? (Select all that apply.)

A. Client/Server
B. Ad Hoc
C. End-to-end
D. Infrastructure

Answer: B, D

Explanation: The IEEE 802.11 standard defines the following modes of operation: Infra-structure mode and Adhoc mode. Therefore, the answer should be B,D.

QUESTION 215:

What is the minimum number of access points required for performing an RF site survey?

A. 4
B. 3
C. 2
D. 1

Answer: D

QUESTION 216:

The propagation distance of an RF signal depends in part on which of the following factors? Select two.

A. Antenna gain
B. Receiving station sensitivity
C. Fresnel Zone blockage
D. Use of Power over Ethernet

Answer: A, C

Explanation: Pg 88 CWNA Study Guide 3rd edition

QUESTION 217:

Which of the following are known methods for attacking the security of a wireless LAN? (Select all that apply.)

A. Broadcast monitoring
B. Rouge access points
C. Passive probing
D. Excessive use of RTS/CTS protocol
E. Network segmentation

Answer: B, C

QUESTION 218:

Which of the following are considered types of Line-of-Sight?

A. Radio Frequency
B. Sustained
C. Reflective
D. Visual

Answer: A, D

Explanation: According to the study guide, there are 2 types of line of sight: Radio Frequency line-of-sight and Visual line-of-sight. Therefore, the answer is A,D.

QUESTION 219:

What does NOT cause RF signal degradation for spread spectrum wireless LANs?

A. Multipath
B. The Fresnel Zone
C. Bad RF line-of-sight

D. Severely bad weather
E. Narrowband interference

Answer: B

QUESTION 220:

There are two types of "Line-of-sight". When a point-to-point transmission's quality and strength are decreased by Fresnel Zone blockage, which of the two is affected?

A. Radio Frequency
B. Direct
C. Horizontal
D. Reflected

Answer: A

Explanation: When the Fresnel Zone is blocked, the RF Line of sight is impaired (according to chapter 2 of the study guide). Therefore the answer should be A (Radio Frequency).

QUESTION 221:

During Point Coordination Function what Interframe Space does the access point use?

A. PIFS
B. SIFS
C. DIFS
D. EIFS

Answer: A

QUESTION 222:

With reference to multipath interference, what phase identifies the time between when the first signal is received and the last echoed signal is received?

A. Fade Length
B. Time Delay
C. Delay Spread
D. Echo Spread

Answer: C

QUESTION 223:

As specified by the FCC, what is the minimum hop rate for FHSS systems in the 2.4 GHz ISM band?

A. 1 hop every 0.2 seconds
B. 1 hop every 0.4 seconds
C. 1 hop every 0.8 seconds
D. 1 hop every 1.0 seconds

Answer: B

Explanation: As mentioned in the study guide, according to the rules specified by the FCC, the maximum dwell time that can be set for FHSS systems is 400 ms. Thus after, the frequency must be changed. Thus, the answer should be B (0.4).

QUESTION 224:

What organization sponsors certification for wireless LAN hardware interoperability?

A. WLANA
B. OpenAir
C. Wi-Fi Alliance
D. IEEE

Answer: C

QUESTION 225:

In a 2.4 GHz FHSS system, how wide is "all-band" interference?

A. 1.0 MHz
B. 2.0 MHz
C. 22.0 MHz
D. 83.5 MHz

Answer: D

Explanation: All band interference is interference in the entire usable band which is 83.5 Mhz in this case. DSSS uses a 22 Mhz bandwidth

---

QUESTION 226:

Which of the following practical components of a written corporate would assist in securing a wireless LAN? (Select all that apply.)

A. Physical security
B. Use of routing protocols that support wireless LANs.

C. Jamming devices at the perimeter of the network.
D. Limit cell size to only what is needed.
E. Meshed wire must always be used in the lining of the building structure.

Answer: A, D

Explanation: From the options provided and from the references of the study guide, Physical Security and Limiting cell size to only what is needed are the 2 components of a written corporate. Therefore, the answer should be A,D.

QUESTION 227:

Which of the following affect Wireless LAN throughput? (Select all that apply.)

A. Type of data being transmitted.
B. Use of RTS/CTS
C. Number of users accessing the Wireless LAN simultaneously.
D. RF interference
E. Delay spread

Answer: B, C, D

Explanation: According to the study guide, system throughput is effected by use of RTS/CTS, number of users on the WLAN, and RF interference. In this case, the amount of data, not the type, is what effects throughput. Therefore, the answer should be B,C,D.

QUESTION 228:

As part of the WEP algorithm, what is the expanded text form of the PRNG acronym?

A. Passive Request Next Generation
B. Pseudorandom Number Generator
C. Protected Result Null Group
D. Persisting Routing Network Gateway

Answer: B

QUESTION 229:

In a FHSS system, what mechanism is used to maintain hopping synchronization in a Basic Service Set?

A. RTS/CTS
B. Beacon frames
C. PCF
D. Clocking signal

Answer: B

QUESTION 230:

An RF signal of 2 Watts is applied to a 100-foot antenna cable, however, only 1 Watt of transmit power is actually developed at the input of the transmitting antenna.
What is the resulting cable loss, measured in decibels (dB)?

A. 0.5 dB
B. 1 dB
C. 3 dB
D. 5 dB

Answer: C

QUESTION 231:

Which of the following describe differences in the encryption techniques of HomeRF and 802.11b?

A. HomeRF uses DSSS and 802.11b uses FHSS technology.
B. HomeRF uses wideband FHSS whereas 802.11b uses narrowband FHSS.
C. The Initialization Vector (IV) of 802.11b is 24-bit, whereas the IV of HomeRF is 32-bit.
D. HomeRF specifies how IVs are chosen, how IVs are chosen in the 802.11b is not specified.

Answer: C, D

Explanation: According to the study guide (chapter 6, page 227), HomeRF uses a 32-bit IV and also specifies how IVs should be chosen. Conversely, 802.11 uses a 24 bit IV and does not specify how the IV is selected. Therefore, the answer should be C,D.

QUESTION 232:

In a FHSS system, how much of the 2.4 GHz ISM band spectrum is used?

A. 20 MHz
B. 22 MHz
C. 83.5 MHz
D. 100 MHZ

Answer: C

QUESTION 233:

In the wireless LAN client utility software, which of the following functions may be configured?

Select all that apply.

A. Modulation type
B. Connection speed
C. Continuous Aware Mode
D. Spanning Tree Protocol
E. Bit ordering

Answer: B, C

QUESTION 234:

Which option may be used as a wireless LAN security feature?

A. Probe request frames
B. Protocol filters
C. Active scanning keys
D. ATIM windows

Answer: B

Explanation:
Protocol filters (IP protocol, IP port, and Ether type) prevent or allow the use of specific protocols through the bridge's Ethernet and radio ports. You can set up individual protocol filters or sets of filters. You can filter protocols for wireless client devices, users on the wired LAN, or both. For example, an SNMP filter on the bridge's radio port prevents SNMP access through the radio but does not block SNMP access from the wired LAN.
IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific IP or MAC addresses. You can create a filter that passes traffic to all addresses except those you specify, or you can create a filter that blocks traffic to all addresses except those you specify.
Reference:
http://www.cisco.com/univercd/cc/td/doc/product/wireless/aero1400/br1410/pscg15/p15filt.htm

---

QUESTION 235:

Power over Ethernet (PoE) may be delivered to a wireless bridge by which of the following mechanisms? Select two.

A. DC Voltage injector
B. AC Line voltage injector
C. Active Ethernet switch
D. RF Injector module
E. Over 2.4 GHz frequencies

Answer: A, C

QUESTION 236:

What node is effectively cut off from communicating with the wireless network during Near/Far?

A. Access point
B. Far node
C. Near node
D. All nodes

Answer: B

QUESTION 237:

If no obstacles are intruding more than 20% into the Fresnel Zone what type of Line of Sight exists?

A. Radio Frequency
B. Radiological
C. Designated
D. Absolute

Answer: A

Explanation:
In radio communications, a Fresnel zone (pronounced as FRA-nel Zone) is one of a (theoretically infinite) number of a concentric ellipsoids of revolution which define volumes in the radiation pattern of a (usually) circular aperture. Fresnel zones result from diffraction by the circular aperture.
The cross section of the first Fresnel zone is circular. Subsequent Fresnel zones are annular in cross section, and concentric with the first.
The concept of Fresnel zones may also be used to analyze interference by obstacles near the path of a radio beam.
This Zone must be determined first, so as to keep it free from obstructions.
Maximum Obstruction allowable is: 40%
Recommended Obstruction is: 20%
For establishing Fresnel Zone first we must determine the RF Line of Sight (RF LoS), which in simple terms is a straigt line between the transmitting and receiving Antenna.
Now the zone surrounding the RF LoS is said to be the Fresnel Zone.
Reference:
http://en.wikipedia.org/wiki/Fresnel_zone

QUESTION 238:

What wireless LAN device management method is NOT used by wireless LAN manufacturers?

A. Telnet
B. Console
C. SNMP
D. HTTP
E. Custom applications
F. IPSec Tunnel
G. SSH

Answer: F

Explanation: Page 231 in CWNA Study Guide 3rd edition

QUESTION 239:

When there is an increase in the gain of an antenna, there is also a corresponding increase in which of the following?

A. Beam width
B. Range
C. Dissipated heat
D. Polarization radius

Answer: B

Explanation:
Although an increase in gain of an omni-directional antenna would correspond to an increase in "'polarization radius" or horizontal range, we believe the answer that is more correct would be range. A high gain, highly-directional parabolic dish antenna would have a long distance range, however the "polarization radius" is really non-existent due to the directionality of the parabolic dish antenna.
See CWNA Offical Study Guide, 3rd Edition, page 86 (Highly, directional antenna (Usage))

QUESTION 240:

What 802.11 technology must be used to co-locate five (5) non-interfering access points?

A. OFDM
B. FHSS
C. Infrared
D. DSSS

Answer: B

Explanation:

Reference: CWNA Official Study Guide, 3rd Edition, Page 208 (Co-Location)
Note:

IEEE 802.11 Radio Link Interfaces

Standard	Maximum Bit Rate	Fallback Rates	Channels Provided	Band	Radio Technique
802.11	2 Mbps	1 Mbps	3	2.4 GHz ISM	FHSS or DSSS
802.11b	11 Mbps	5.5 Mbps 2 Mbps 1 Mbps	3	2.4 GHz ISM	DSSS
802.11a	54 Mbps	48 Mbps 36 Mbps 24 Mbps 18 Mbps 12 Mbps 9 Mbps 6 Mbps	12*	5 GHz U-NII	OFDM
802.11g	54 Mbps	Same as 802.11a Plus 2 Mbps and 1 Mbps	3	2.4 GHz ISM	OFDM

- In November 2003 the FCC increased the frequency allocation in the U-NII band from 300 MHz to 555 MHz. Initially, there were twelve 802.11a WLAN channels defined in the original 300 MHz, and the IEEE has yet to determine how many additional channels will be assigned in the new allocation.

FHSS – Frequency Hopping Spread Spectrum
DSSS – Direct Sequence Spread Spectrum
OFDM – Orthogonal Frequency Division Multiplexing

The two major problems with 2.4 GHz systems are the limited amount of radio spectrum available and the potential for interference from other users. The FCC has allocated 83.5 MHz of radio spectrum to the ISM band, and as each 802.11b WLAN channel requires roughly 25 MHz, only three non-interfering channels can be accommodated. To provide interoperability with 802.11b systems, 802.11g uses the same three channels.
The answer is 802.11a that operates in the less congested 5 GHz band, and it will quickly become the preferred option for commercial users. In the US, the 5 GHz Unlicensed National Information Infrastructure (U-NII) band was initially allocated 300 MHz of non-contiguous bandwidth between 5.150 and 5.585 GHz supporting 12 non-interfering channels.
Reference:
http://www.wsta.org/publications/articles/0804_article02.html

---

QUESTION 241:

Which of the following problems can be caused by VSWR? Select two.

A. Transmitter burnout
B. Decrease RF signal amplitude at the receiver
C. RF antenna failure
D. RF connector deterioration

Answer: A, B
CWNA Offical Study Guide, 3rd Edition, page 41 (Effects of VSWR)

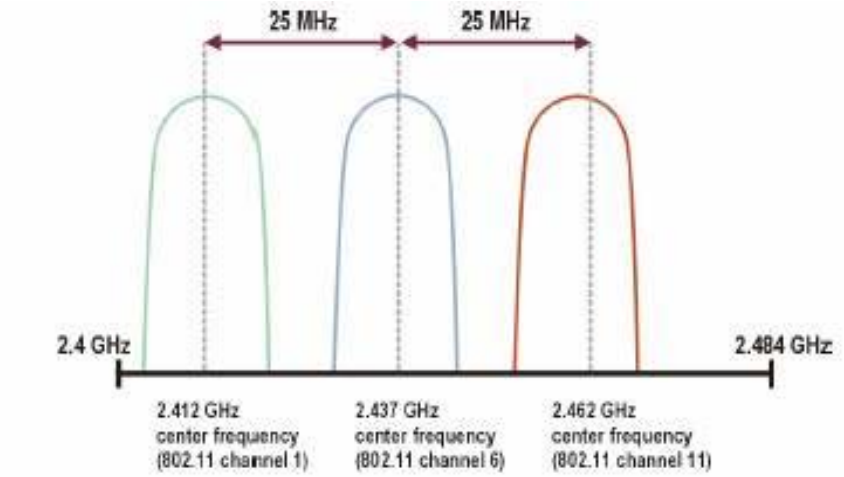
QUESTION 242:

In a DSSS system, which of the following channel pairs DO NOT overlap? Select two.

A. channel 10 - channel 11
B. channel 5 - channel 10
C. channel 3 - channel 7
D. channel 1 - channel 11

Answer: B, D

Explanation:
DSSS (ISM band) channels are indeed 22 MHz wide ? for example, the FCC-specified channel 1 occupies 2.412 GHz +/- 11 MHz. But only one radio can transmit on this channel at any point in time -- using the 802.11b standard, a chipping code spreads signal across the entire 22 MHz channel. All other radios MUST listen when another radio is transmitting to avoid interference. Consider adjacent two radios, one listening to channel 1 (2.412 GHz) and another sending on channel 3 (2.422 GHz). These channels overlap from 2.412-2.422 GHz, so outgoing signal on channel 3 will collide with simultaneous incoming signal on channel 1. The result would be a high bit error rate and excessive retransmission, yielding low or even no effective throughput. For best results, adjacent radios should use non-overlapping channels? For example, the minimum 3 MHz gap between channels 1 and 6 (2.437 GHz). Wider inter-channel gaps further reduce the probability of interference.



Source: *The IEEE 802.11 Handbook: A Designer's Companion*

Reference:
http://expertanswercenter.techtarget.com/eac/knowledgebaseAnswer/0,295199,sid63_gci976361,00.html

---

QUESTION 243:

What type of scanning requires listening to each channel for a specified period of time awaiting transmission of beacons that contain proper SSIDs for association?

A. Passive
B. Active
C. Distributed
D. Coordinated

Answer: A

Explanation: This can be easily verified in page 246 in CWNA Study Guide 2nd edition

---

QUESTION 244:

What RF communications technique is categorized by low peak power and wide bandwidth?

A. Complementary Code Keying
B. Narrowband
C. Spread Spectrum
D. Fragmentation

Answer: C

Explanation: Spread Spectrum - A radio transmission technology
that "spreads" the user information over a
much wider bandwidth than otherwise required in

order to gain benefits such as improved interference tolerance and unlicensed operation.

QUESTION 245:

What information types are passed from the access point to wireless clients using the beacon management frame? Select two.

A. Time synchronization
B. Encrypted data
C. Association responses
D. Channel selection information

Answer: A, D

Explanation:
Page 244 in CWNA Study Guide 2nd edition
Page 334 in CWNA Study Guide 3rd edition

QUESTION 246:

What frame type does a wireless station transmit to find an access point?

A. Superframe
B. Probe frame
C. ICMP frame
D. Location frame

Answer: B

Explanation: To find an access point a client may send a probe request management frame.

QUESTION 247:

What is the terminology used by the 802.11 standard for two or more Basic Service Sets connected by a common distribution system?

A. Enhanced Service Set
B. Distributed Service Set
C. Independent Service Set
D. Extended Service Set

Answer: D

Explanation: An extended service set is two or more basis service sets connected by a common distribution system.

QUESTION 248:

While an access point is operating in Distributed Coordination Function (DCF) mode, which of the following is TRUE?

A. CSMA/CS is used to avoid collisions.
B. Wireless clients are polled for data transmissions.
C. Time-bounded data such as voice and video are better supported.
D. Network overhead is increased due to polling.

Answer: A

Explanation: The asynchronous type of service is provided by the distributed coordination function (DCF), which implements the basic access method of the IEEE 802.11 MAC protocol and is also known as the carrier sense multiple access with collision avoidance (CSMA/CA) protocol.

QUESTION 249:

Which of the following are likely causes of propagated RF signal degradation? Select three.

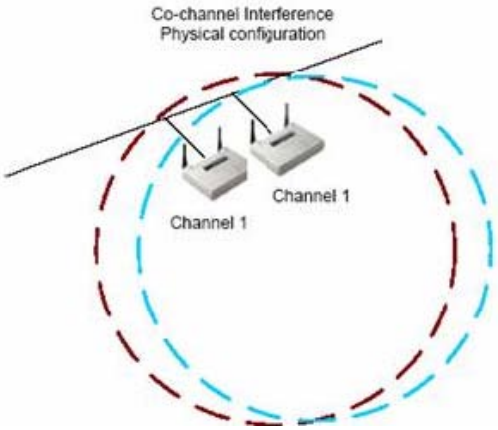
A. An amplifier in the RF signal path
B. Trees in the Line-of-Sight
C. Weak receiver sensitivity
D. Co-channel interference
E. Adjacent channel interference
F. Flocks of birds in the signal path

Answer: B, D, E

Explanation: While it is true that absorption of RF by various materials (buildings, trees, water vapor, etc.) tends to increase with frequency, remember we are talking about "free space" here. The frequency dependence in this case is solely due to the decreasing effective aperture of the receiving antenna as the frequency increases. This is intuitively reasonable, since the physical size of a given antenna type is inversely proportional to frequency. If we double the frequency, the linear dimensions of the antenna decrease by a factor of one-half, and the capture area by a factor of one-quarter. The antenna therefore captures only one-quarter of the power flux density at the higher frequency versus the lower one, and delivers 6 dB less signal to the receiver. However, in most cases we can easily get this 6 dB back by increasing the effective aperture, and hence the gain, of the receiving antenna. For example, suppose we are using a parabolic dish antenna at the lower frequency
A consideration when planning or troubleshooting an RF link is the Fresnel Zone. The Fresnel Zone occupies a series of concentric ellipsoid-shaped areas around the LOS path, as can be seen in Figure 2.10. The Fresnel Zone is important to the integrity of the RF link because it defines an area around the LOS that can introduce RF signal interference

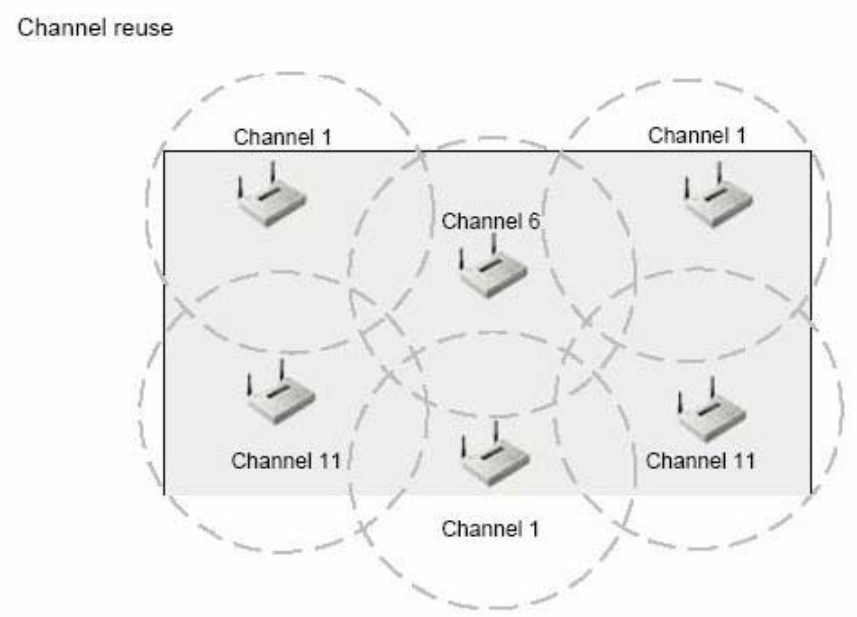
if blocked. Objects in the Fresnel Zone such as trees, hilltops, and buildings can diffract or reflect the main signal away from the receiver, changing the RF LOS. These same objects can absorb or scatter the main RF signal, causing degradation or complete signal loss.
///
A consideration when planning or troubleshooting an RF link is the Fresnel Zone. The Fresnel Zone occupies a series of concentric ellipsoid-shaped areas around the LOS path, as can be seen in Figure 2.10. The Fresnel Zone is important to the integrity of the RF link because it defines an area around the LOS that can introduce RF signal interference if blocked. Objects in the Fresnel Zone such as trees, hilltops, and buildings can diffract or reflect the main signal away from the receiver, changing the RF LOS. These same objects can absorb or scatter the main RF signal, causing degradation or complete signal loss.
// To illustrate co-channel interference, assume a 3-story building, with a wireless LAN on each floor, with the wireless LANs each using channel 1. The access points' signal ranges, or cells, would likely overlap in this situation. Because each access point is on the same channel, they will interfere with one another. This type of interference is known as co-channel interference.
In order to troubleshoot co-channel interference, a wireless network sniffer will be needed. The sniffer will be able to show packets coming from each of the wireless LANs using any particular channel. Additionally, it will show the signal strength of each wireless LAN's packets, giving you an idea of just how much one wireless LAN is interfering with the others.
The two solutions for co-channel interference are, first, the use of a different, nonoverlapping channel for each of the wireless LANs, and second, moving the wireless LANs far enough apart that the access points' cells do not overlap. These solutions are the same remedy as for adjacent channel interference.
D, E:
Co-channel Interference
Co-channel interference can have the same effects as adjacent channel interference, but is an altogether different set of circumstances. Co-channel interference as seen by a spectrum analyzer is illustrated in Figure 9.17 while how a network configuration would produce this problem is shown in Figure

FIGURE 9.18 Co-channel Interference in a network



To illustrate co-channel interference, assume a 3-story building, with a wireless LAN on each floor, with the wireless LANs each using channel 1. The access points' signal ranges, or cells, would likely overlap in this situation. Because each access point is on the same channel, they will interfere with one another. This type of interference is known as co-channel interference.
In order to troubleshoot co-channel interference, a wireless network sniffer will be needed. The sniffer will be able to show packets coming from each of the wireless LANs using any particular channel. Additionally, it will show the signal strength of each wireless LAN's packets, giving you an idea of just how much one wireless LAN is interfering with the others.
The two solutions for co-channel interference are, first, the use of a different, nonoverlapping channel for each of the wireless LANs, and second, moving the wireless LANs far enough apart that the access points' cells do not overlap. These solutions are the same remedy as for adjacent channel interference

Channel reuse



wireless clients are polled for data transmission
WHEN AN ACCESS POINT is operating in distributed coordination function mode,

---

QUESTION 250:

Which types of spread spectrum technologies are allowed by the FCC for use in the ISM bands? Select three.

A. FHSS
B. DSSS
C. Infrared
D. Narrowband
E. OFDM

Answer: A, B, E

Explanation:
The license-free ISM bands have been set aside internationally for use in Industrial, Scientific and Medical applications.In each of these bands, the radio devices are required to use spread spectrum modulation techniques. The two types of allowed spread spectrum modulation are direct sequence (DSSS) and frequency hopping (FHSS). In the US, Canada, South and Central America, much of Asia, and most of Europe, the ISMbands fall in the900 MHz (L-band), 2.4 GHz (S-band) and 5.8 GHz (C-band) frequency spectrum.The largest ISM band, the 5.8 GHz band (C-band)is the least-used worldwide and offers a contiguous 125 MHz block of spectrum for high-speed network applications.
Reference:
http://www.airlinx.com/products.cfm/product/1-0-0.htm

QUESTION 251:

The Wi-Fi Alliance added interoperability testing to the Wi-Fi certification process for 802.11a devices to ensure that they are interoperable with which device?

A. 802.11 devices
B. 802.11b devices
C. 802.11a devices
D. 802.11g devices
E. HiperLAN/2 devices

Answer: C

Explanation: The lower 5 GHz UNII band and the 2.4 GHz ISM band are the same width - 100 MHz. 802.11a equipmentis new and significantly more expensive than 802.11b equipmentand is not compatible with 802.11b or 802.11g equipment in any capacity. The UNII bands (all three of them) allow for a larger useable portion than does the 2.4 GHz ISM band, yielding a maximum of 4 non-overlapping DSSS channels.
Wi-Fi is the hardware compatibility standard created and maintained by WECA for 802.11b devices. IEEE 802.11g devices use the 2.4 GHz ISM band are backwards compatible with 802.11b. 802.11a devices use a different set of frequencies and a different modulation type from 802.11b, and are thus incompatible.
A recent addition to the list of devices using direct sequence technology is the IEEE 802.11a standard, which specifies units that can operate at up to 54 Mbps. Unfortunately for 802.11 and 802.11b device users, 802.11a is wholly incompatible with 802.11b because it does not use the 2.4 GHz band, but instead uses the 5 GHz UNII bands.
The 5 GHz UNII bands are made up of three separate 100 MHz-wide bands, which are used by 802.11a-compliant devices. The three bands are known as the lower, middle, and
//
The standards ETSI has established, HiPerLAN/2 for example, directly compete against standards created by the IEEE such as 802.11a. There has been much discussion about IEEE and ETSI unifying on certain wireless technologies, but nothing

has materialized as of this writing. This effort is referred to as the "5UP" initiative for "5 GHz Unified Protocol." The IEEE's attempt at interoperability with ETSI's HiperLAN/2 standard is the new forthcoming 802.11h standard.
ETSI's original HiPerLAN standard for wireless, dubbed HiperLAN/1, supported rates of up to 24 Mbps using DSSS technology with a range of approximately 150 feet.
HiperLAN/1 used the lower and middle UNII bands, as do HiperLAN/2, 802.11a, and the new 802.11h standard. The new HiperLAN/2 standard supports rates of up to 54 Mbps and uses all three of the UNII bands.
ETSI's HiperLAN/2 standard has interchangeable convergence layers, support for QoS, and supports DES and 3DES encryption. The supported convergence layers are ATM, Ethernet, PPP, FireWire, and 3G.
HiperLAN/2 - An extension to the HiperLAN protocol developed by ETSI (European Telecommunications Standards Institute) that provides a 54 Mbps data rate in the 5GHz band.

QUESTION 252:

Before a client can participate in a Wireless LAN, which of the following must occur? Select two.

A. The client must be associated.
B. The client must be issued an IP address by a DHCP server.
C. The client must negotiate an encryption algorithm with the Access Point.
D. The client must be authenticated.

Answer: A, D

QUESTION 253:

When the frame size on a wireless LAN is reduced, what is the corresponding result?

A. The amount of data that needs to be transmitted is decreased.
B. RTS/CTS is automatically invoked.
C. The possibility of collisions is decreased.
D. The CSMA/CD protocol is used instead of the CSMA/CA protocol.
E. Fragmenting the frames can add more collisions

Answer: E

Explanation: The answer given per CWNA Official Study Guide, 2nd Edition, Page 298 (Figure 8.1)would correspond to the correct answer being C.
However, if you look at the CWNA Official Study Guide, 3rd Edition, Page 409.
This states that fragmenting the frames can add more collisions.

QUESTION 254:

Which of the following are types of highly directional antennas? Select two.

A. Grid
B. Parabolic Dish
C. Patch
D. Dipole
E. Circular Scope

Answer: A, B

QUESTION 255:

Which list should be included in an RF Site Survey Report for a long distance outdoor bridge link?

A. A list of RF interference sources near the middle of the wireless link
B. A list of tree types in the immediate area around each antenna
C. A list of above ground power lines in the immediate area around each antenna
D. A list of potential physical security hazards for each bridge location
E. A list of RF interference sources near either antenna

Answer: D

Explanation:
The following is a list of the most basic questions that must be answered before the actual physical work of the site survey begins. These questions are purposely open-ended because each one results in more information being passed from the client to the surveyor, thus making the surveyor better prepared to go on-site and do the site survey. Most, if not all, of these questions can be answered via phone, fax, or email, assuming the people with the answers to the questions are available. Again, the more prepared one is before arriving at the site (with a site survey toolkit), the more valuable the time on-site will be. Some of the topics you may want to question the network management about before performing your site survey:
1. Facilities Analysis
2. Existing Networks
Facility Analysis
Aside from the obvious size
differences, you must take into account the number of users, security requirements, bandwidth requirements, budget, and what kind of impact jet engines have on 802.11 RF signals, if any, etc.
The second facility type is a real estate office with approximately 25 agents. In this environment, security is important, but not mandated by law, so rudimentary security measures might suffice. Coverage will likely be adequate with only 1 or 2 centrallylocated access points, and bandwidth requirements would be nominal since most of the access is Internet-based or transferring small files back and forth to the file server.
Outdoor wireless connections are vulnerable to security attacks, since the intruder would

not have to be inside the building to get into the network. Once it is determined that the survey is for indoors, outdoors, or both, obtain any and all property survey documents and diagrams that are available. Indoors, these documents will show you the floor layout, firewalls, building structure information, wiring closets, and other valuable information. Outdoors, these documents will show how far the outdoor wireless LAN can safely extend without significant chance of intrusion.
Outdoor Surveys
For outdoor surveys, record the following items on a copy or sketch of the property:
1. Trees, buildings, lakes, or other obstructions between link sites
2. If in winter, locate trees that will grow leaves during other seasons and may interfere with the RF link
3. Visual and RF line of sight between transmitter and receiver
4. Link distance (note: if greater than 7 miles, calculate compensation for Earth bulge)
5. Weather hazards (wind, rain, snow, lightning) common to the area
6. Tower accessibility, height, or need for a new tower
7. Roof accessibility, height

QUESTION 256:

What method of identity verification is used by Open System Authentication?

A. VPN
B. EAP
C. ACL
D. Null
E. MAC Filter

Answer: D

QUESTION 257:

Which of the following authentication options support digital certificates as client identification?

A. CHAP
B. EAP-TLS
C. PAP
D. MS-CHAPv2

Answer: B

Explanation:
What is the TLS (Transport Layer Security) Authentication Method?
EAP-TLS is an IETF-standardized authentication method based on the same protocol used for secure Web traffic via the SSL (Secure Sockets Layer) protocol.
TLS authentication within EAP is very simple. You take the TLS session establishment dialog between the supplicant and the authentication server and pack each TLS message inside of an EAP-TLS packet. When the TLS authentication dialog succeeds, the authenticator is informed

and access to the network is granted.
Although TLS has actually set up an encrypted channel between the authentication server and the supplicant, this channel is not used---the supplicant wants to talk to the authenticator, not the authentication server. Instead, a piece of the keying material created during the TLS session establishment for that channel is sent to the authenticator. Then, the supplicant (which already knows the TLS-established secret key) and authenticator use that key for WEP encryption.
In EAP-TLS, certificates are used to authenticate the authentication server to the supplicant, and, optionally, to authenticate the supplicant to the authentication server. The authentication server starts by sending its digital certificate to the supplicant. The most common authentication used today on the Web with SSL is one-way authentication - a server sends its certificate to your browser to prove its identity.
Reference:
http://www.ilabs.interop.net/WLAN_Sec_2002_Spring/ni_2002_las_eap_types.pdf

---

QUESTION 258:

An RF signal of 2 Watts is applied to a 100-foot antenna cable, however, only 1 Watt of transmit power is actually developed at the input of the transmitting antenna. What is the resulting cable loss, measured in decibels (dB)?

A. 0.5 dB
B. 1 dB
C. 3 dB
D. 5 dB

Answer: C

Explanation:
The decibel (dB) is one of the most useful parameters in radio communications. It allows one to simply add all of the losses and gains together in order to calculate how much power is actually leaving the antenna and to calculate the effective radiated power.
The decibel itself is a ratio, it has no unit and is meaningless unless you state the value or unit that it is related to.
Transmitter output power can be quoted in decibel watts (dBW). This value is calculated from the equation 10 log10 P, where P is the power in watts.
A decibel (as applied to system gain or loss) is defined by the equation:

$$dB = 10 * Log_{10} \left(\frac{Pout}{Pin}\right)$$

db = 10 log (2 / 1) = 10 log 2 = 3 db
http://website.lineone.net/~colin_mccord/Radio/decibel.htm

QUESTION 259:

Which of the following are purposes of a wireless Ethernet Converter? Select two.

A. To wireless bridge between two or more wired Ethernet segments

B. To connect a client with a wired network interface card to a wireless network
C. To convert an Ethernet switch into an access point
D. To eliminate computer disassembly while adding wireless LAN functionality
E. To connect a serial printer to the wireless network

Answer: B, D

QUESTION 260:

What does the IEEE 802.11b standard define?

A. How Mobile IP is implemented on a wireless LAN
B. How a station associates with Access Points
C. How users are tracked between two Access Points on the same subnet
D. How users are tracked across subnet boundaries

Answer: B

Explanation: While 802.11b defines how a station associates with APs, it does not define how APs track users as they roam about, either at Layer 2 between two APs on the same subnet, or at Layer 3 when the user crosses a router boundary between subnets.
The first issue is handled by vendor-specific inter-AP protocols, which vary in performance

---

QUESTION 261:

Which of the following features assist in the reduction of lost data due to wireless LAN PC Cards (Clients) entering sleep mode while operating in AD HOC mode? Select two.

A. Access point queue buffers
B. The access point transmits the TIM to notify stations of queued packets
C. PC Cards have an established wake up period
D. Use of ATIM window

Answer: C, D

Explanation: Announcement Traffic Information Message (ATIM) - used in Ad Hoc mode to
indicate to stations the presence of transmissions bound for a particular station; tells stations not to enter sleep mode before receiving their transmitted frames
An ATIM is used for the purpose of notifying stations that are using power save poll (PSP) mode that there is data queued for them by other stations, awaiting delivery. After stations send the ATIMs to other stations, the ATIM window (the time during which ATIMs are sent) closes and the data is then delivered according to CSMA/CA medium access rules.
Incorrect answers:

In ad-hoc mode there is no AP and this fact eliminates A and B as answers
See page 358 CWNA Study Guide 3rd edition

QUESTION 262:

Which of the following is the shortest Interframe Space?

A. PIFS
B. SIFS
C. DIFS
D. All Interframe Spaces are the same length

Answer: B

Explanation: Refer to the diagram:

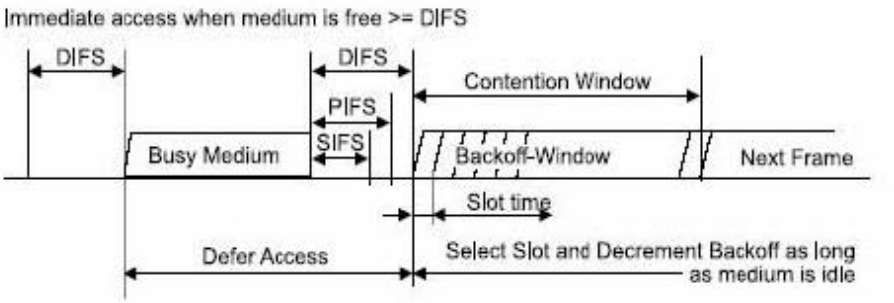


Figure 1.1: IFS relationships in IEEE802.11 (source: [3])

QUESTION 263:

What action occurs when a wireless station drops its speed due to Automatic Rate Selection?

A. Decreases its power output level to transmit at a slower speed
B. Changes the data modulation type or the code keying sequence
C. Increases its power output level to attempt to maintain connection speed
D. Increases the fragmentation threshold to maintain greater throughput

Answer: B

QUESTION 264:

What term identifies the bending of an RF signal when it passes through a medium with different density?

A. Reflection
B. Refraction
C. Scattering

D. Diffraction

Answer: B

QUESTION 265:

Which of the following items is NOT necessary to document as part of a long-distance RF path survey?

A. Antenna location at end of the link
B. Seasonal changes in the environment
C. All current and future path obstructions
D. Whether the link is over water or land
E. Air traffic landing zones

Answer: E

Explanation: There are many outdoor interference sources, and some can change just by their nature.
Seek out and record the effects of the following:
1. Trees, buildings, lakes, or other obstructions or reflective objects
2. Trees without leaves that will later have leaves or that will grow to interfere with the Fresnel zone.
3. Automobile traffic - if linking two buildings at first-story height across a road, a large truck or bus could disable the link.
Record the interference source, its location, and its effect and potential effect on wireless LAN coverage, range, and throughput. This data should be recorded both on your copy of the blueprint as well as in a separate list for easy future reference. Taking pictures of interference sources that are permanent (e.g., lakes and buildings) will serve as a visual reference to the client.

QUESTION 266:

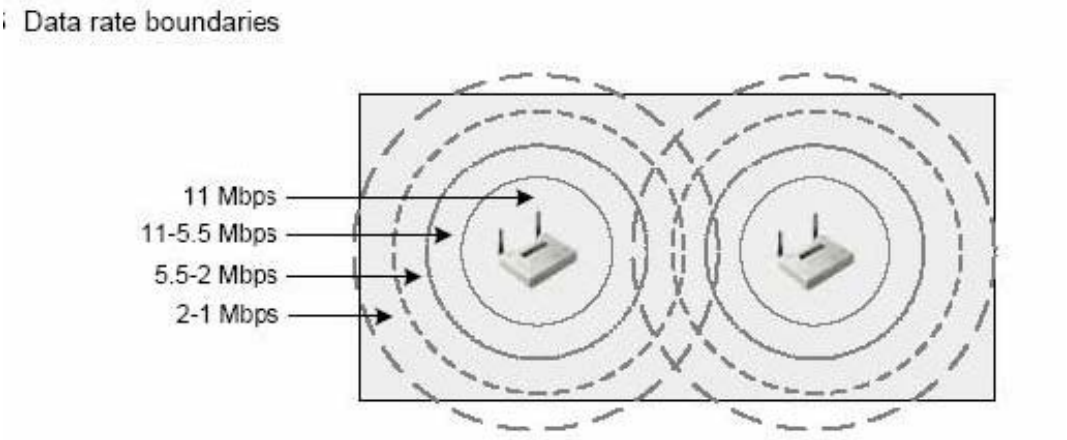
While performing an RF site survey for an 802.11b Wireless LAN, what minimum bandwidth setting should you use?

A. It will be based on throughput requirements
B. Always use 1 Mbps
C. No minimum bandwidth settings are required.
D. Always use 11 Mbps

Answer: D

Explanation: If you are using an 802.11b wireless LAN, for example, record where the data rate decreases from 11Mbps to 5.5Mbps to 2Mbps to 1Mbps, as shown in Figure 11.16. These boundaries should somewhat resemble concentric circles, with the slower data rate areas further from the access point than the

higher data rates. The client organization must be told that when a user roams out past the coffee machine to the mailroom, that user will not get the highest possible throughput due to the data rate decrease, which, in turn, is due to the distance increase.



QUESTION 267:

What is the name for a group of wireless stations communicating without the use of an access point?

A. Client mode
B. Client Peer mode
C. Infrastructure mode
D. Basic Service Set
E. Independent Basic Service Set

Answer: E

QUESTION 268:

When comparing omni-directional antennas with antennas that focus the signal into a narrow beam, which of the following attributes is higher for narrow beam antennas?

A. Noise reception
B. kfactor
C. Gain
D. Down tilt angle
E. Wind loading

Answer: C

QUESTION 269:

You are administering a network with wireless LAN components for Certkiller .com. The wireless portion of the network is configured using statically assigned WEP keys stored on each

station's wireless PC Card. It has been reported to you that one of the wireless client computers containing a wireless PC Card has been stolen. What reasonable actions could be taken to restore the wireless LAN to the former level of security? Select two.

A. All WEP keys could be reprogrammed on all wireless LAN devices
B. Only those clients that use the same keys as the stolen client could be reprogrammed and that particular WEP key could be removed from all access points
C. Nothing could be done; this situation would not pose a security risk
D. Invoke a corporate policy that would call for periodic inventory of wireless LAN devices
E. Turn down the power on all access points so that an intruder could not connect to the network

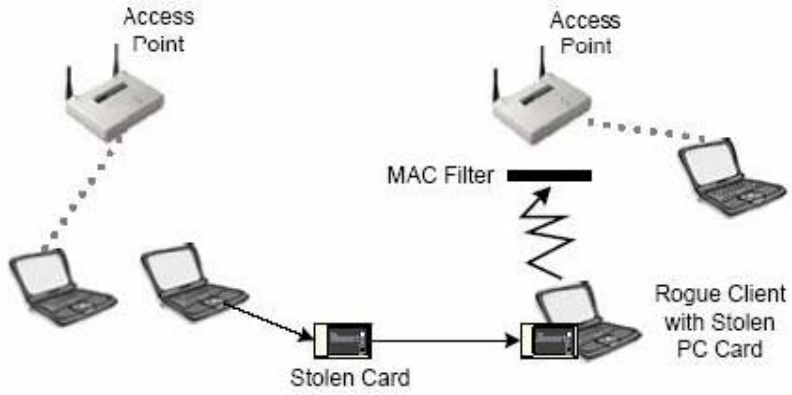
Answer: B, D

Explanation:

Wireless LANs can filter based on the MAC addresses of client stations. Almost all access points (even very inexpensive ones) have MAC filter functionality. The network administrator can compile, distribute, and maintain a list of allowable MAC addresses and program them into each access point. If a PC card or other client with a MAC address that is not in the access point's MAC filter list tries to gain access to the wireless LAN, the MAC address filter functionality will not allow that client to associate with that access point. Figure 10.4 illustrates this point.

Of course, programming every wireless client's MAC address into every access point across a large enterprise network would be impractical. MAC filters can be implemented on some RADIUS servers instead of in each access point. This configuration makes MAC filters a much more scalable security solution. Simply entering each MAC address into RADIUS along with user identity information, which would have to be input anyway, is a good solution. RADIUS servers often point to another authentication source, so that other authentication source would need to support MAC filters.

MAC Filters



MAC filters can work in reverse as well. For example, consider an employee who left a company and took their wireless LAN card with them. This wireless LAN card holds the WEP key and MAC filters, which, for the sake of this example, are not used. The administrator could then create a filter on all access points to disallow the MAC address of the client device that was taken by the employee. If MAC filters were already being used on this network when the wireless LAN card was stolen, removing the particular client's MAC address from the *allow* list would work as well.

Although MAC filters may seem to be a good method of securing a wireless LAN in some instances, they are still susceptible to the following intrusions:

- Theft of a PC card that is in the MAC filter of an access point
- Sniffing the wireless LAN and then spoofing with the MAC address after business hours

---

QUESTION 270:

Before going into a low-power state (sleep), what function must a wireless station operating in a BSS perform?

A. Notify the access point of its intention to sleep
B. Notify other wireless stations of its intention to sleep
C. Broadcast an AITM on the network
D. Send an RTS to the access point

Answer: A

Explanation:
When using PSP mode in a BSS, stations first send a frame to the access point to inform theaccess point that they are going to sleep, (temporarily powering down). The access pointthen records the sleeping stations as asleep. The access point buffers any frames that are intended for the sleeping stations. Traffic for those clients who are asleep

continues arriving at the access point, but the access point cannot send traffic to a sleeping client. Therefore, packets get queued in a buffer marked for the sleeping client.

QUESTION 271:

If two DSSS access points are placed on the same channel in the same physical space, which of the following results will occur? Select three.

A. The available bandwidth to users will increase
B. The available bandwidth to users will decrease
C. The access points will interfere with each other
D. One access point will automatically adjust its channel
E. All client computers will alternate connectivity between access points
F. Users will be able to roam between the two access points

Answer: B, C, E

Explanation:
Co-channel interference results from two APs transmitting on the same channel in the same area. In a typical 802.11 wireless network, APs continually broadcast a signal, and any wireless client within range can lock onto that signal to make a connection. But when APs are placed close enough together to provide continuous coverage over a large area, it's possible (or even likely) that some APs will generate signals that interfere with other APs. When this happens, two or more APs transmit packets at the same time on the same channel, corrupting packets and causing clients to experience transmission delays and lower performance. In addition, clients located equidistant between two APs on the same channel may flip-flop, not knowing whether to access one or the other.
Reference: http://wirelessreview.com/infrastructure/technology/wlan_power_architecture_041105/

QUESTION 272:

Speeds of up to _____ Mbps are allowed within the IEEE 802.11a standard.

A. 36
B. 54
C. 72
D. 100

Answer: B

QUESTION 273:

You are administering a network with wireless LAN components for Certkiller .com. The wireless portion of the network is configured using statically assigned WEP keys stored on each station's wireless PC Card. It has been reported to you that one of the wireless client computers containing a wireless PC Card has been stolen. What reasonable actions could be taken to restore

the wireless LAN to the former level of security? Select two.

A. Install a wireless VPN that would base authentication on usernames and password
B. Disable the wired port on each access point until the stolen PC Card could be recovered
C. Install a wireless LAN encryption and authentication system that would implement 802.1x/EAP and RADIUS
D. Connect each access point into a switch instead of into a hub
E. Switch all wireless client PC Cards to a different manufacturer to prevent future security breaches

Answer: A, C

QUESTION 274:

Before performing a site survey for a hospital, the network manager notifies you that there are connection-oriented medical applications used across the hospital network. Because the application is connection-oriented, it will be sensitive to service disruptions. For this reason, it is particularly important to locate sources of RF interference and RF dead spots. Which of the following items put the application at risk of time-outs? Select three.

A. High population of patients
B. Long hallways
C. Fire doors
D. Metal blinds
E. Radiology departments
F. Mobile food carts

Answer: C, D, E

QUESTION 275:

Which of the following technologies are components used as part of security solution in a wireless LAN? Select three.

A. MAC filters
B. WLIF
C. RADIUS server
D. WINS Servers
E. VPN server
F. Authenticated DNS

Answer: A, C, E

QUESTION 276:

In the IEEE 802.11 standard, which Radio Frequency spread spectrum technologies are

specified? Select two.

A. Infrared
B. Frequency Hopping
C. Direct Sequencing
D. Wide Band

Answer: B, C

QUESTION 277:

By design, what 802.11 spread spectrum technology exhibits resistance to narrowband RF interference?

A. FHSS
B. DSSS
C. Point-to-point Infrared
D. Broadcast Infrared

Answer: A

QUESTION 278:

Which items are benefits of a wireless LAN? Select two.

A. Native and flexible QoS features
B. Mobility in the enterprise
C. Strong security by design
D. Reduced cost of ownership for portable networks
E. Moderate cost of licensing

Answer: B, D

QUESTION 279:

Multipath can cause which of the following effects at the receiving antenna? Select two.

A. Increased signal amplitude
B. Decreased signal amplitude
C. Signal regeneration
D. Signal splitting
E. Signal purification

Answer: A, B

QUESTION 280:

Where can the frame fragmentation threshold setting be manually configured on a wireless LAN? Select two.

A. On the wireless station by the end user
B. On the access point by the network administrator
C. The network layer protocol programming interface
D. On the enterprise wireless gateway

Answer: A, B

Explanation:
Pg 299 in CWNA User Guide 2nd edition

QUESTION 281:

A transmitter that emits an 80 mW signal is connected to a cable with 6 dB loss. If the cable is connected to an antenna with a 16dBi gain, what is the resultant power output in mW (EIRP) from the antenna?

A. 160mW
B. 320mW
C. 800mW
D. 1600mW

Answer: C

Explanation:
Net Gain= -6 dB + 16 dBi = + 10 dBi which represents a tenfold increase in power.
Resultant output Power = 10 times input power= 10 X 80 mW = 800 mW

QUESTION 282:

How many antennas are required to implement Antenna Diversity on a wireless LAN device?

A. 1
B. 2
C. 3
D. 4

Answer: B

QUESTION 283:

Which of the following solutions can be applied to the "hidden node" problem with wireless LAN? Select three.

A. Increase output power on clients
B. Remove interfering obstacles between clients
C. Move clients closer together
D. Increase output power on access points
E. Remove the access point from network

Answer: A, B, C

QUESTION 284:

What options best describes a Network Layer device designed to provide Internet or network connectivity to a small number of wireless nodes?

A. Residential Wireless Gateway
B. Wireless Workgroup Bridge
C. Wireless Bridge
D. Universal Access Point

Answer: A

QUESTION 285:

To what device can a wireless bridge (acting as a wireless bridge) connect wirelessly?

A. A wireless bridge
B. An access point
C. An Ethernet wireless Gateway
D. An Ethernet converter

Answer: A

QUESTION 286:

What component is concatenated with the WEP secret key to form a WEP key?

A. Plain text
B. IV
C. PRNG
D. ICV
E. Key stream

Answer: B

QUESTION 287:

What is an appropriate use of an IEEE 802.11b wireless LAN?

A. Large peer-to-peer network that requires high throughput
B. Use with high-demand application servers
C. Last Mile connectivity to compete with Telco & Cable providers
D. Streaming video applications to the desktop

Answer: C

Explanation:
See CWNA Official Study Guide, 3rd Edition, Page 11 (Last Mile Data Delivery - Wireless ISP)

QUESTION 288:

How many 3.4 GHz ISM band DSSS channels are available for use in the United States according to the FCC?

A. 1
B. 11
C. 12
D. 14

Answer: B

QUESTION 289:

A LOSS of 3 dB will yield what power ratio?

A. 1:3
B. 1:10
C. 2:1
D. 1:2

Answer: D

Explanation:
Loss of 3 dB results in the halving of output power.

QUESTION 290:

Assume that you are performing a site survey. The plan is to erect an outside tower on the ground for a 2.4 GHz wireless LAN antenna. Which of the following questions should you consider asking? Select two.

A. Are nearby buildings in my line-of-sight?
B. Are there cordless phones in use in nearby buildings?
C. Is grounding available?
D. How heavy is the antenna?
E. Are there any nearby radio stations using 2.4 GHz frequencies?

Answer: A, E

Explanation:
For A see CWNA Official Study Guide, 3rd Edition, page 515. For E see CWNA Official Study Guide, 3rd Edition, page 488.

QUESTION 291:

Lightning arrestors protect wireless LANs from what type of power fluctuation?

A. Direct lightning strikes
B. High transient current
C. Severe voltage sag
D. RF Noise due to jamming

Answer: B

QUESTION 292:

Which of the following factors determine the diameter of a wireless LAN link Fresnel Zone? Select two.

A. Height of the antennas
B. Size of the antennas dishes
C. Distance between the antennas
D. Frequency of the transmission
E. Transmission power

Answer: C, D

Explanation:
Pg 38 in CWNA User Guide 2nd edition

QUESTION 293:

What is the bandwidth of a single DSSS channel in the 2.4 GHz ISM band?

A. 20 MHz
B. 22 MHz

C. 24 MHz
D. 30 MHz

Answer: B

Explanation:
Pg 76 in CWNA User Guide 2nd edition

QUESTION 294:

Which of the following criteria is used by wireless client devices to associate with an access point? Select two.

A. Signal strength
B. Physical distance to the closest access point
C. Signal quality
D. Round trip time of a PING packet

Answer: A, C

Explanation:
Page 337 CWNA Study Guide 3rd edition

QUESTION 295:

Enterprise Wireless Gateways often use RADIUS to authenticate users. The RADIUS server may query which of the following database types for authentication? Select three.

A. CAM table
B. Novell Directory Service
C. ODBC-compliant databases
D. LDAP-compliant databases
E. WINS

Answer: B, C, D

QUESTION 296:

Which of the following are goals of the Wi-Fi Interoperability Test Plan?

A. To finalize the IEEE 802.11b standard
B. To ensure interoperability among 802.11b, 802.11a, 802.11g and future IEEE standards devices
C. To finalize Wi-Fi standard
D. To promote the use of 802.11a technology
E. To ensure interoperability between HomeRF and 802.11 FHSS devices

Answer: B
See CWNA Official Study Guide, 2nd Edition, Page 60
Not A, C: Old goals that have been met already.

QUESTION 297:

Which layers of the OSI model are specified as part of the 802.11 standard? Select two.

A. Physical
B. Data-Link
C. Network
D. Transport

Answer: A, B

QUESTION 298:

Wireless LAN antennas have radiation fields called lobes. Which of the following are different types of lobes on Wireless LAN antennas? Select two.

A. Side lobes
B. Directional lobes
C. Cylindrical lobes
D. Main lobes
E. Top lobes

Answer: A, D

QUESTION 299:

Which of the following factors influence Wireless LAN throughput? Select two.

A. Number of simultaneous users using the Wireless LAN
B. Antenna height
C. Use of VPN tunnels across the wireless LAN
D. Roaming handoff speed

Answer:

QUESTION 300:

What IEEE standard or draft specifies seamless roaming between access points?

A. 802.11
B. 802.11i

C. 802.11a
D. 802.11e
E. 802.11f

Answer: E

Explanation:
Page 316 CWNA Study Guide 3rd edition

QUESTION 301:

What stream cipher is used for encryption as part of WEP?

A. DES
B. RC4
C. SSL
D. 3DES

Answer: B

Explanation:
Wired Equivalent Privacy (WEP) was intended to provide the same level of privacy over wireless networks that one would expect from wired networks. WEP is part of the IEEE 802.11 standard document, and defines how encryption must support the authentication, integrity, and confidentiality of packets transmitted using wireless equipment. The IEEE standards committee chose to use RC4, a proven encryption algorithm, for wireless security. All wireless vendors support 802.11.

QUESTION 302:

The measure of 1 mW of power is equivalent to which of the following logarithmic units of measure?

A. 0 dB
B. +10 dB
C. +10 dBi
D. 0 dBm

Answer: D

Explanation:
For absolute measurements, the reference power P2 is defined at 1 milliwatt, hence dBm, and 0 dBm = 1 mW:

dBmPower unit	mWpower unit	dBmPower unit	mWpower unt

+20	100 mW	-30	1 µW
+10	10 mW	-40	100 nW
0	**1 mW**	**-50**	**10 nW**
-10	100 µW	-60	1 nW
-20	10 µW	-70	100 pW

QUESTION 303:

Which of the following statement indicates a key principle of RF propagation and communication?

A. The range of RF transmissions increases as the frequency in use increases.
B. Even if low RF signal strength is indicated, signal quality may be high enough for good communication.
C. Low signal quality, when coupled with high signal strength, always yield good communication.
D. Due to the distance involved, sun spots do not affect RF communication.

Answer: B

QUESTION 304:

Earth Bulge is a factor when planning wireless data transmission paths longer than what length?

A. 3 miles / 4.8 kilometers
B. 7 miles / 11.2 kilometers
C. 15 miles / 24 kilometers
D. 22 miles / 35.2 kilometers

Answer: B

Explanation:
The ESTeem Model 192E is a IEEE 802.11b compatible wireless LAN transceiver that can used to build a Wireless Local Area Network (WLAN) for line-of-sight distances to 7 miles for fixed base and mobile applications.
Earth bulge
must be calculated into tower height for radio links greater than 7 miles.
Reference: CWNA official Study Guide, Pg. 352

QUESTION 305:

What is the maximum transmit power of a 2.4 GHz ISM band radio in point-to-multipoint configuration as specified by FCC regulations?

A. +10 dBm
B. +20 dBm
C. +30 dBm
D. +40 dBm

Answer: C

Explanation:
At Intentional Radiator Power limit = 1 watt= + 30 dBm
At EORP Power limit = 4 Watts = + 36 dBm
From the answers given if power is at the Intentional Radiator then the answer is C.
Pg 215 in CWNA User Guide 2nd edition

QUESTION 306:

Which of the following elements are part of performing a site survey? Select two.

A. Disabling fire alarms throughout the facility
B. Interviewing the network manager
C. Obtaining blueprints of floor plans of the facility
D. Making a list of all wireless network cards MAC addresses
E. Unlocking all wiring closets doors

Answer: B, C

Explanation:
C: Among the first items to request from a network manager are blueprints or some kind of map showing the layout of the facility, as shown in Figure 11.5. Without the official building or facility schematics, a diagram must be created that shows the dimensions of the areas, the offices, where the walls are located, network closets, power outlets, etc.

FIGURE 11.5 Blueprints or floor plans

Reference: CWNA Official Study Guide, Page 334

QUESTION 307:

Which modulation and spreading code types are used for 1 Mbps DSSS transmission in an IEEE 802.11 wireless LAN system?

A. DBPSK/Barker Code
B. DBSPK/CCK
C. DQPSK/CCK
D. 4GFSK/Barker Code

Answer: A

Explanation:

FIGURE 8.9 Modulation and Spreading Code Types for 802.11 & 802.11b

	Spreading Code	Modulation Technology	Data Rate
2.4 GHz DSSS	Barker Code	DBPSK	1 Mbps
	Barker Code	DQPSK	2 Mbps
	CCK	DQPSK	5.5 Mbps
	CCK	DQPSK	11 Mbps
2.4 GHz FHSS	Barker Code	2GFSK	1 Mbps
	Barker Code	4GFSK	2 Mbps

Reference:
CWNA Official Study Guide, Page 243
Note: you cannot get 11 Mbps in an 802.11 system You can only get 1 & 2 Mbps.

QUESTION 308:

AES specifies which of the following encryption key sizes? Select three.

A. 104-bit
B. 128-bit
C. 192-bit
D. 256-bit
E. 512-bit
F. 1024-bit

Answer: B, C, D

Explanation:
The Advanced Encryption Standard (AES) is gaining acceptance as an appropriate replacement for the RC4 algorithm used in WEP. AES uses the Rijndale (pronounced 'RINE-dale') algorithm in the following specified key lengths:

128-bit
192-bit
256-bit
AES is considered to be un-crackable by most cryptographers, and the National Institute of Standards and Technology (NIST) has chosen AES for the Federal Information Processing Standard, or FIPS. As part of the effort to improve the 802.11 standard, the 802.11i working committee is considering the use of AES in WEPv2.
Reference: CWNA Official Study Guide, Page 295

QUESTION 309:

Which of the following are units of measure for a relative change in power level? Select two.

A. dBm
B. dBi
C. dB
D. mW

Answer: B, C

Explanation:
B and C represents a relative change in power level while A and D represents an absolute change in power level. See page 44 in CWNA Study Guide 2nd edition

---

QUESTION 310:

Using IEEE compliant 802.11b wireless LAN systems, what is the maximumdata transmission rate that can be achieved in any given area without network contention?

A. 11 Mbps
B. 22Mbps
C. 33Mbps
D. 54 Mbps

Answer: A

Explanation:
This is the theoretical amount.

QUESTION 311:

Which of the following frequencies are considered by the FCC to be ISM frequencies? Select three.

A. 840 MHz
B. 905 MHz

C. 1.95 GHz
D. 2.45 GHz
E. 5.80 GHz
F. 3.1 GHz

Answer: B, D, E

QUESTION 312:

What term is used to describe the amount of time spent by a wireless LAN radio transmitting data on a channel in an FHSS system?

A. Convergence
B. Dwell
C. Coding
D. Broadcast

Answer: B

Explanation:
The frequency of the carrier is periodically modified (hopped) following a specific sequence of frequencies.
In FHSS systems, the spreading code is this list of frequencies to be used for the carrier signal, a.k.a. the "hopping sequence"
The amount of time spent on each hop is known as dwell time and is typically in the range of 100 ms.

QUESTION 313:

Which of the following statements describe the 802.11 implementation and interoperability of WEP? Select two.

A. WEP use is optional
B. WEP use is mandatory
C. WEP using 64-bit (also called 40-bit) encryption is a requirement for Wi-Fi certification by the Wi-Fi Alliance
D. WEP using 128-bit (also called 104-bit) encryption is a requirement for Wi-Fi certification by the Wi-Fi Alliance
E. WEP must use DES for encryption

Answer: A, C

Explanation:
Pg 381, 382 in CWNA User Guide 2nd edition

QUESTION 314:

Which of the following hardware components may contribute to wireless LAN security?

A. Enterprise Wireless Gateways
B. Secured grid antennas
C. N-type connectors
D. WEP attenuators

Answer: A

Explanation:
An enterprise wireless gateway is a device that can provide specialized authentication and connectivity for wireless clients. Enterprise wireless gateways are appropriate for large- scale wireless LAN environments providing a multitude of manageable wireless LAN services such as rate limiting, Quality of Service (QoS), and profile management.
It is important that an enterprise wireless gateway device needs to have a powerful CPU and fast Ethernet interfaces because it may be supporting many access points, all of which send traffic to and through the enterprise wireless gateway.
Reference: CWNA Official Study Guide, Page 122

QUESTION 315:

Which of the following types of antennas are used in wireless LANs? Select two.

A. Panel
B. Parabolic dish
C. Extended Backlobe
D. Category 7
E. Polar plane

Answer: A, B

Explanation:
The type of antenna used affects the range either by focusing the RF energy into a tighter beam transmitting it farther (as a parabolic dish antenna does); or by transmitting it in all directions (as an omni-directional antenna does), reducing the range of communication.
Semi-directional antennas come in many different styles and shapes. Some semidirectional
antennas types frequently used with wireless LANs are Patch, Panel, and Yagi (pronounced "YAH-gee") antennas. All of these antennas are generally flat and designed for wall mounting. Each type has differentcoverage characteristics. Figure 5.7 shows some examples of semi-directional antennas.
Reference: CWNA Official Study Guide, Page 137

QUESTION 316:

Under the 802.11 standard what spread spectrum technology allows for the highest number of co-located access points with the least interference?

A. Frequency Hopping
B. Infrared
C. Direct Sequence
D. OFDM

Answer: A

QUESTION 317:

According to the IEEE 802.11 standard, what is the RF spectrum bandwidth used by FHSS and DSSS?

A. 2.4000 - 2.4835 MHz
B. 2.4000 - 2.4830 GHz
C. 2.4000 - 2.5000 GHz
D. 2.4000 - 2.4835 GHz

Answer: D

Explanation:
The IEEE 802.11 standard specifies data rates of 1 Mbps and 2 Mbps and OpenAir (a standardcreated by the now defunct Wireless LAN Interoperability Forum) specifies data ratesof 800 kbps and 1.6 Mbps. In orderfor a frequency hopping system to be 802.11 or OpenAircompliant, it must operate in the 2.4 GHz ISM band (which is defined by the FCC as being from 2.4000 GHz to 2.5000 GHz). Both standards allow operation in the rangeof 2.4000 GHz to 2.4835 GHz.
Reference: CWNA Official Study Guide, Page 80

QUESTION 318:

Which of the following is an omni-directional antenna?

A. Patch antenna
B. Dipole
C. Yagi antenna
D. Panel antenna

Answer: B

Explanation:
The most common wireless LAN antenna is the Dipole antenna. Simple to design, the

dipoleantenna is standard equipment on most access points. The dipole is an omnidirectional antenna, because it radiates its energy equally in all directions around its axis. Directional antennas concentrate their energy into a cone, known as a "beam."
Reference: CWNA Official Study Guide, Page 134

QUESTION 319:

Wireless LAN client utility software includes what monitoring function?

A. Radio airtime ratio monitor
B. Sleep time monitor
C. Real-time throughput monitor
D. Link statistics monitor

Answer: D

Explanation:
Link status monitor utilities allow the user to view packet errors, successful transmissions, connection speed, link viability, and many other valuable parameters. There is usually a utility for doing real-time link connectivity tests so that, for example, anadministrator would be able to see how stable a wireless link is while in the presence ofheavy RF interference or signal blockage.
Reference: CWNA Official Study Guide, Page 119

QUESTION 320:

The Wi-Fi Alliance certifies products compatible with which standards?

A. 802.11a
B. 802.11b
C. 802.15
D. 802.16
E. 802.11f

Answer: B

Explanation:
The Wireless Fidelity (a.k.a. Wi-Fi) seal indicates that a vendor's hardware has undergoneextensive testing to assure interoperability with other devices manufacturedto meet the 802.11b standard. In orderto be interoperable with other 802.11b equipment, the equipment under test would most likely have to meet the same802.11b standards.
Reference: CWNA Official Study Guide, Page 193

QUESTION 321:

According to the FCC, what is the frequency range of the 2.4 GHz ISM band?

A. 2.4000 - 2.5000 GHz
B. 2.4000 - 2.4750 GHz
C. 2.4000 - 2.4725 GHz
D. 2.4000 - 2.4835 GHz

Answer: D

Explanation:
The 802.11 radio WLANs operate in the 2.4GHz (2.4 to 2.483 GHz) unlicensed Radio Frequency (RF) band. The maximum isotropic transmission power in this band allowed by FCC in US is 1Wt, but 802.11 devices are usually limited to the 100mWt value.

QUESTION 322:

What symptom cannot be caused by Multipath?

A. Loss of signal at receiving end.
B. Reduces signal strength at receiving end.
C. Increased signal strength at receiving end.
D. Appearance of ghost access points.
E. Corrupted data at the receiving end.

Answer: D

QUESTION 323:

The distance an RF signal will be propagated depends in part on which two of the following factors?

A. Output power of the Intentional Radiator
B. Spread Spectrum technology in use
C. Transmission frequency
D. Aperture size of receiving antenna

Answer: A, C

Explanation:
Pg 418 & 419 in CWNA User Guide 3rd edition

QUESTION 324:

What is a characteristic of Ad Hoc wireless LANs?

A. Support for client polling.

B. The lack of an access point.
C. Support for time-bounded services.
D. Functionality to support seamless roaming between networks.
E. VPN functionality.

Answer: B

Explanation:
The terms ad hoc and IBSS are interchangeable. Both indicate a lack of an access point in a wireless LAN where stations are communicating directly with each other.
Reference: CWNA Official Study Guide, Page 228

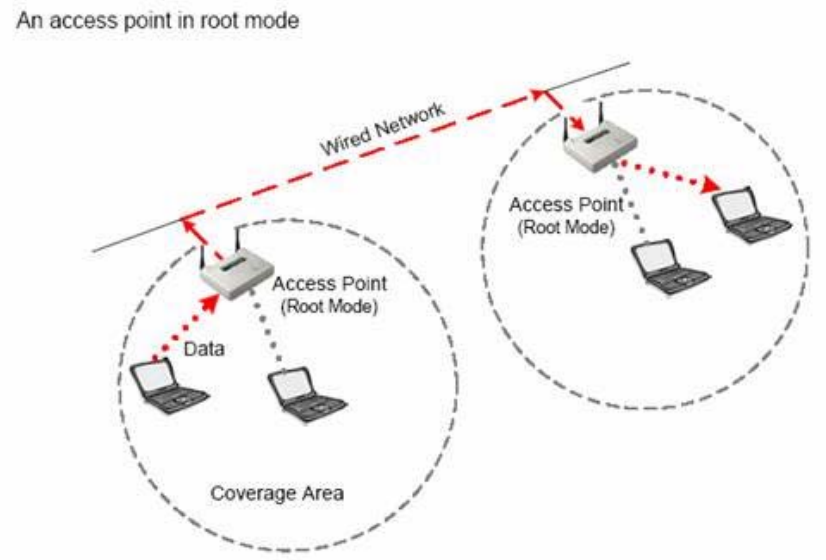
QUESTION 325:

Which communication methods may be used between access points? Select all that apply.

A. Communicating over the wired segment in repeater mode.
B. Communicating over the wired segment in root mode.
C. Communicating over the wireless segment in repeater mode.
D. Access points never communicate with each other.
E. Communicating over the wired segment in bridge mode.

Answer: A, B

Explanation:
Root Mode is used when the access point is connected to a wired backbone through its wired (usually Ethernet) interface. Most access points that support modes other than root mode come configured in root mode by default.



Reference: CWNA Official Study Guide, Page 103
A is correct as well. See CWNA Official Study Guide, 2nd Edition, Page 299

QUESTION 326:

Which of the following items are sometimes used in an indoor site survey?

A. An encryption key server.
B. Spectrum analyzer
C. Wireless workgroup bridge
D. A mobile equipment cart
E. SSH Server

Answer: B

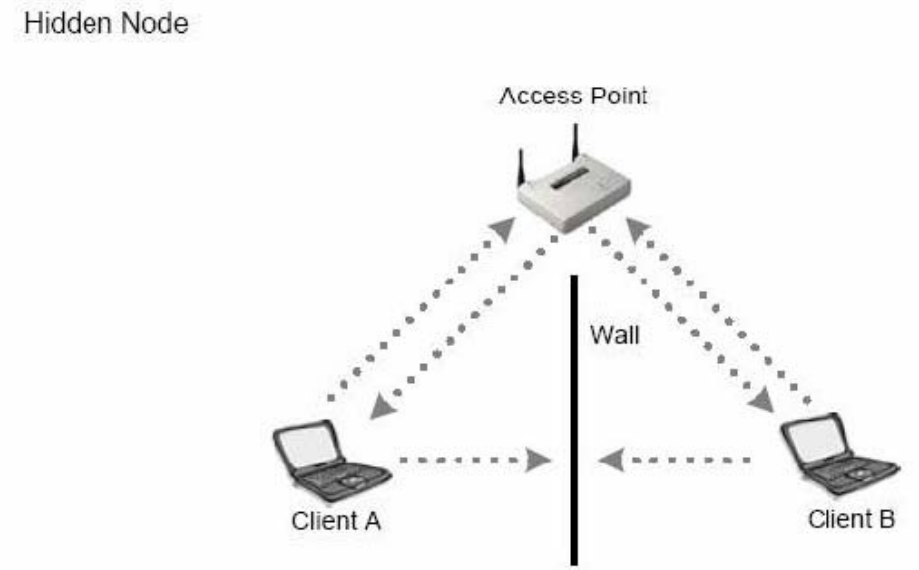
QUESTION 327:

What is a cause of the "hidden node" problem?

A. Interfering obstacles between clients.
B. Clients broadcasting with too much power.
C. Access points broadcasting with too little power.
D. Clients being too close together.

Answer: A

Explanation:
Hidden node is a situation encountered with wireless LANs in which at least one node is unableto hear (detect) one or more of the other nodes connected to the wireless LAN. In thissituation, a node can see the access point, but cannot see that there are other clients alsoconnected to the same access point due to some obstacle or a large amount of distancebetween the nodes. This situation causes a problem in medium access sharing, causingcollisions between node transmissions.



Reference: CWNA Official Study Guide, Page 103

QUESTION 328:

Which of the following items are often used as part of an indoor wireless LAN site survey? Select all that apply.

A. Lightning arrestor
B. Network manager interview
C. Mobile access point
D. VPN server
E. GPS device

Answer: B, C

QUESTION 329:

Which of the following results should be included in an RF Site Survey Report for an indoor wireless LAN?

A. Measurements for current sources of RF interference.
B. An analysis of the clients existing network infrastructure.
C. Screenshots of the site survey software at particular coverage points.
D. Analysis detailing how well the clients particular application works over wireless.
E. What type of antennas should be used for building-to-building bridge links.
F. A list of what layer 3 protocols should be used over the wireless LAN for maximum throughput.

Answer: A

QUESTION 330:

Which of the following conditions will prevent seamless roaming?

A. No MAC filters on the Access Points.
B. WEP key mismatch between clients and Access Points.
C. Use of different vendor's IEEE 802.11b compliant DSSS hardware.
D. Mismatched SSID between clients and Access Points.
E. Roaming between FHSS and DSSS systems.

Answer: B, D, E

QUESTION 331:

For which of the following options can the Ad Hoc mode be used?

A. In an Extended Service Set
B. In a Basic Extended Service Set
C. Ina a Basic Service Set
D. In an Independent Basic Service Set

Answer: D

Explanation:
An independent basic service set is also known as an ad hoc network. An IBSS has no access point or any other access to a distribution system, but covers one single cell and has one SSID, as shown in Figure 7.11. The clients in an IBSS alternate the responsibility of sending beacons since there is no access point to perform this task.
Reference: CWNA Official Study Guide, Page 211

QUESTION 332:

Which of the following are involved in maintaining synchronization in a FHSS wireless LAN?

A. Client stations use probe response frames for verifying their internal clock's time.
B. Receiver checks and corrects its clock at time of receiving beacon frame.
C. Access point gets time information from an external time-source using NTP.
D. Access points transmit beacon frames. Stations receive beacon frames.
E. A clocking frame is sent from access points to clients.
F. Beacon frames contain the transmitters clock information at the moment of transmission.

Answer: B, F

Explanation:
Page 334 CWNA Study Guide 3rd edition

QUESTION 333:

What specific antenna methodology is used to help eliminate null areas of RF coverage (sometimes caused by Multipath)?

A. Diversity
B. Amplification
C. Polarization
D. Linearization
E. Dual Alignment

Answer: A

Explanation:
Antenna diversity was devised for the purpose of compensating for multipath. Antenna diversity means using multiple antennas, inputs, and receivers in order to compensate for the conditions that cause multipath. There are four types of receiving antenna diversity, one of which is predominantly used in wireless LANs.
Reference: CWNA Official Study Guide, Page 258

QUESTION 334:

Which of the following can be wireless LAN client devices? Select all that apply.

A. PC Card
B. Workgroup Bridge
C. Ethernet Converter
D. Root Access Point
E. Root Wireless Bridge
F. Yagi Antenna

Answer: A, C

Explanation:
The term "client devices" will, for purposes of this discussion, cover several wireless LAN devices that an access point recognizes as a client on a network. These devices include:
1. PCMCIA & Compact Flash Cards
2. Ethernet & Serial Converters (C)
3. USB Adapters
4. PCI & Adanters (A)
Wireless LAN clients are end-user nodes such as desktop, laptop, or PDA computers that need wireless connectivity into the wireless network infrastructure. The wireless LAN client devices listed above provide connectivity for wireless LAN clients. It is important to understand that manufacturers only make radio cards in two physical formats, and those are PCMCIA and Compact Flash (CF). All radio cards are built (by the

manufacturers) into these card formats and then connected to adapters such as PCI, ISA, USB, etc.
Reference: Page 257 of CWNA Study Guide 3rd edition

QUESTION 335:

In an IBSS, what happens to packets destined for sleeping wireless stations?

A. They are dropped by the access point.
B. They are buffered by the access point.
C. They are sent to the sleeping station.
D. They are buffered at the source station.

Answer: D

Explanation:
The power saving communication process in an IBSS is very different than when power savingmode is used in a BSS. An IBSS does not contain an access point, so there is no deviceto buffer packets. Therefore, every station must buffer packets destined from itselfto every other station in the Ad Hoc network. Stations alternate the sending of beaconson an IBSS network using varied methods, each dependent on the manufactu
Reference: CWNA Official Study Guide, Page 221

QUESTION 336:

Which of the following factors should be considered when determining the link budget for a long-distance point-to-point wireless LAN link?

A. Antenna gain
B. Typical wind direction and strength
C. Transmitter power
D. Object type to be penetrated
E. Free Space Path Loss
F. Weather during given times of year

Answer: A, C, E

Explanation:
Pg 98 in CWNA User Guide 3rd edition

QUESTION 337:

Which of the following statements describe an Enterprise Wireless Gateway?

A. A wireless client performing bridging functions for other clients in an Ad Hoc network.
B. A VPN enabled device positioned between a group of access points and the network

backbone.
C. A specialized access point device with VPN and Network Layer services.
D. An authentication server running on the network backbone.

Answer: C

QUESTION 338:

Which of the following statements are TRUE for 802.11 FHSS?

A. FHSS is affected by narrowband RF interference to a leaser degree than DSSS.
B. FHSS uses all 100 MHz of the 2.4 GHz ISM band.
C. FHSS uses frequency diversity to retransmit lost packets on different frequencies.
D. FHSS is highly susceptible to interference from class 2 Bluetooth systems at a distance of up to 1 mile (1.6 km).

Answer: A

QUESTION 339:

Which of the following are advantages of an 802.11-based wireless LAN when compared to a wired LAN?

A. Greater mobility
B. Greater environment adaptability
C. Higher speeds available
D. Less costly installation
E. More flexible infrastructure power cabling options

Answer: A, D

QUESTION 340:

Assume that you are performing a site survey. The plan is to erect an outside tower on top of a building for a 2.4 GHz wireless LAN antenna. Which questions should you consider asking?

A. Is the roof adequate to support the tower?
B. It a permit required?
C. What is the average and peak wind velocity on top of the roof?
D. Are there any cellular towers near?
E. Is this location north or south of the Equator?

Answer: A, B

Explanation:
pg 488 in CWNA User Guide 3rd edition

QUESTION 341:

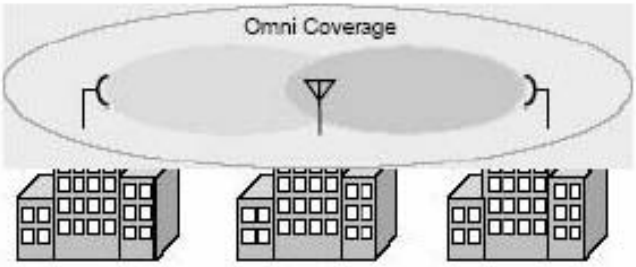
What is the most effective antenna to use for communicating from a central point, out to four remote points (one North, one South, one East, and one West of the central point)?

A. Yagi
B. Patch
C. Parabolic Dish
D. Omni-directional

Answer: D

Explanation:
Omni-directional antennas are used when coverage in all directions around the horizontal axis of the antenna is required. Omni-directional antennas are most effective where large coverage areas are needed around a central point. For example, placing an omnidirectional antenna in the middle of a large, open room would provide good coverage.
Omni-directional antennas are commonly used for point-to-multipoint designs with a hub-n-spoke topology (See Figure 5.6). Used outdoors, an omni-directional antenna should be placed on top of a structure (such as a building) in the middle of the coverage area. For example, on a college campus the antenna might be placed in the center of the campus for the greatest coverage area.

FIGURE 5.6 Point-to-multipoint link



Reference: CWNA Official Study Guide, Page 136

QUESTION 342:

Which common network protocols are supported in access points for configuration? Select all that apply.

A. HTTP
B. SNMP
C. SMTP
D. RSVP
E. LSA

Answer: A, B

Explanation:
HTTP if there is a built-in web server in the AP pg 231 in CWNA User Guide
3rd edition

QUESTION 343:

Power over Ethernet (PoE) provides which of the following effects to a wireless LAN?

A. Injects DC power onto the Category 5 Ethernet cable.
B. Reduces the need for additional AC power outlets.
C. Allows the network designer to use access points instead of bridges.
D. Allows Access Points and Bridges to be installed in areas up to 200 meters from the wiring closet.
E. Eliminates the need for external antennas on access points and bridges.
F. Allows the data cable to be extended beyond the typical 100 meter limit.

Answer: A, B

Explanation:
Power over Ethernet (PoE) is a method of delivering DC voltage to an access point, wirelessbridge, or wireless workgroup bridge over the Cat5 Ethernet cable for the purposeof powering the unit. PoE is used when AC power receptacles are not available wherewireless LAN infrastructure devices are to be installed. The Ethernet cable is used tocarry both the power and the data to the units.
Reference: CWNA Official Study Guide, Page 147

QUESTION 344:

Which of the following are mandatory characteristics of WEP according to the IEEE 802-11 standard?

A. Exportable
B. Extremely difficult to break
C. Computationally efficient
D. Self-synchronizing
E. Use of RC5 encryption
F. Scalable to 256 bits of encryption

Answer: A, C, D

Explanation:
pg 381 in CWNA User Guide 2nd edition

QUESTION 345:

When an RF wave propagates through space, its amplitude at any given point degrades as it becomes wider with distance. This natural expansion causes what negative effect in a wireless LAN system?

A. Linear Circumference Loss
B. Free-Space Path Loss
C. Transmission Obfuscation
D. Connection-point Attenuation

Answer: B

QUESTION 346:

What can MAC filters be implemented on a wireless LAN?

A. Access points
B. Wireless LAN USB client
C. RADIUS servers
D. Wireless LAN SNMP agent
E. Personal firewall software

Answer: A, C

Explanation:
pgs 391 & 392 in CWNA User Guide 2nd edition

QUESTION 347:

Focusing the antenna lobe in a desired direction caused an increase in the distance a propagated RF wave will travel. What term defines this effect?

A. Extension
B. Active Amplification
C. Beam Narrowing
D. Passive Gain

Answer: D

Explanation:
Antennas have passive gain, which means they do not increase the power that is input into them, but rather shape the radiation field to lengthen or shorten the distance the propagated wave will travel. The higher the antenna gain, the farther the wave will travel, concentrating its output wave more tightly so that more of the power is delivered to the destination (the receiving antenna) at long distances.
Reference: CWNA Official Study Guide, Page 142

QUESTION 348:

What is the VSWR value that indicates a perfect impedance match between an antenna and the attached cable?

A. 0:0
B. 1:1
C. 10:1
D. 0:1

Answer: B

Explanation:
VSWR is a ratio, so it is expressed as a relationship between two numbers. A typical VSWR value would be 1.5:1. The two numbers relate the ratio of impedance mismatch against a perfect impedance match. The second number is always 1, representing the perfect match, where as the first number varies. The lower the first number (closer to 1), the better impedance matching your system has. For example, a VSWR of 1.1:1 is better than 1.4:1. A VSWR measurement of 1:1 would denote a perfect impedance match and no voltage standing wave would be present in the signal path.
Reference: CWNA Official Study Guide, Page 53

QUESTION 349:

What organization currently creates wireless LAN operational standards?

A. IEEE
B. WLANA
C. Wi-Fi Alliance
D. WLIF

Answer: A

Explanation:
It is the job of the IEEE to create standards of operation within the confines of the regulations created by the FCC. The IEEE and OpenAir standards regarding FHSS systems describe:
1. what frequency bands may be used
2. hop sequences
3. dwell times
4. data rates
Reference: CWNA Official Study Guide, Page 80

QUESTION 350:

Which of the following conversions may be necessary when performing wireless LAN

mathematical calculations?

A. dBm to milliwatts
B. dBi to milliwatts
C. dB to watts
D. dBm to dBi

Answer: A

Explanation:
This equation can be manipulated to reverse the conversion, now converting dBm to mW:

$$Pmw = \log^{-1}\left(\frac{P_{dbm}}{10}\right)$$

*Note: $\log^{-1}$ denotes the inverse logarithm (inverse log)

Most of the power levels referred to by administrators will be in mW or dBm. These two units of measurement both represent an absolute amount of power and are both industry standard measurements.
Reference: CWNA Official Study Guide, Page 61

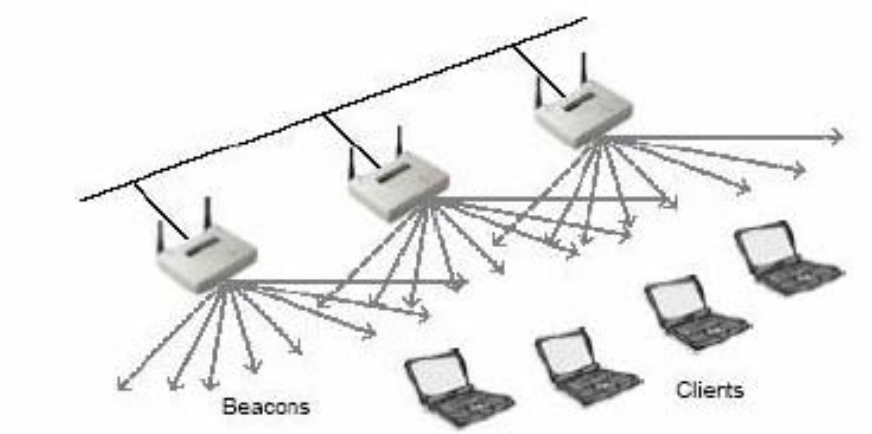
QUESTION 351:

What statement is TRUE regarding the Service Set Identifier (SSID)?

A. It is used when forming a MAC filter on an access point.
B. It is prepended to the MAC address when doing protocol filtering.
C. It is broadcast by the access point in its beacons by default.
D. It is the unit's serial number.

Answer: C

Explanation:
In configurations where there are multiple access points, the SSID of the network the station wishes to join may be broadcast by more than one of these access points. In this situation, the station will attempt to join the network through the access point with the strongest signal strength and the lowest bit error rate.



Reference: CWNA Official Study Guide, Page 199

QUESTION 352:

What method should the site surveyor use to document the dead spots in the are to be covered by a Wireless LAN?

A. Showing the network administrator the spots in person.
B. Marking the spots with markers or flags and roping off the area.
C. Dead spots should not be recorded in a site survey.
D. Marking the locations of dead spots on a site blueprint or floor plan.

Answer: D

QUESTION 353:

In the manufacturer wireless LAN client utility software, which of the following functions may be configured?

A. DSSS or FHSS channel
B. Power Save Poll mode
C. Half-duplex or Full-duplex modes
D. VPN tunneling protocol
E. Beacon modification utility

Answer: B

QUESTION 354:

What IEEE standard specifies 11 Mbps as its top speed and backwards speed compatibility with the IEEE 802.11 standard?

A. 802.11b
B. 802.11g
C. 802.11a

D. 802.11i

Answer: A

Explanation: Wi-Fi is the hardware compatibility standard created and maintained by WECA
for 802.11b devices. IEEE 802.11g devices use the 2.4 GHz ISM band are backwardscompatible with 802.11b. 802.11a devices use a different set of frequencies and a different modulation type from 802.11b, and are thus incompatible.
Reference: CWNA official Study Guide, Pg. 45

QUESTION 355:

When a wireless LAN is operating in AD HOC mode, what must occur for traffic to be transmitted outside of the peer-to-peer environment?

A. One of the cell-members must perform routing.
B. It is not possible for traffic to leave an AD HOC wireless LAN.
C. One of the cell-members must perform bridging.
D. An access point must be introduced into the environment.

Answer: A

Explanation:
Page 265 CWNA Study Guide 2nd edition

QUESTION 356:

In an 802.11 wireless network, how is the WEP initialization vector (IV) transmitted?

A. In the clear and poses a security threat.
B. In encrypted form and is secure.
C. In encrypted form and can be compromised with enough computing power.
D. The initialization vector is not transmitted.
E. In the clear and is compressed but not encrypted?

Answer: A

Explanation:
When WEP is referred to as being simple, it means that it is weak. The RC4 algorithm was inappropriately implemented in WEP, yielding a less-than-adequate security solution for 802.11 networks. Both 64-bit and 128-bit WEP (the two available types) have the same weak implementation of a 24-bit Initialization Vector (IV) and use the same flawed process of encryption. The flawed process is that most implementations of WEP initializehardware using an IV of 0 - thereafter incrementing the IV by 1 for each packet

sent. For a busy network, statistical analysis shows that all possible IVs (224) would be exhausted in half a day, meaning the IV would be reinitialized starting at zero at least once a day. This scenario creates an open door for determined hackers. When WEP is used, the IV is transmitted in the clear with each encrypted packet.
Reference: CWNA official Study Guide, Pg. 288

QUESTION 357:

Outdoor spread spectrum wireless LANs are NOT affected by what weather condition?

A. Smog
B. Wind loading
C. Temperature
D. Snow

Answer: C

Explanation:
Choice B is wrong because A strong wind could easily move one or both antennas enough to completely degrade the signal between the two antennas. This effect is called "antenna wind loading"
Choice A and D are wrong because Severely adverse weather conditions can affect the performance of a wireless LAN. In general, common weather occurrences like rain, hail, snow, or fog do not have an adverse affect on wireless LANs. However, extreme occurrences of wind, fog, and perhaps smog can cause degradation or even downtime of your wireless LAN.
Reference: CWNA official Study Guide, Pg. 244

QUESTION 358:

Which of the following could be considered as part of a wireless LAN security solution?

A. Physical security policy
B. Passive scanning probes
C. Wi-Fi hardware certification
D. Shared Key authentication
E. Use of only directional antennas

Answer: D

Explanation:
Wired Equivalent Privacy (WEP) is an encryption algorithm used by the Shared Key authentication process for authenticating users and for encrypting data payloads over only the wireless segment of the LAN. The IEEE 802.11 standard specifies the use of WEP.
Reference: CWNA official Study Guide, Pg. 260

QUESTION 359:

Which of the following effects will result from installing an extension cable to an antenna in a wireless LAN? Select all that apply.

A. The area covered by the antenna will decrease.
B. The Equivalent Isotropically Radiated Power (EIRP) will decrease.
C. The data throughput rate will increase.
D. The RF signal power at the antenna input will increase.
E. 802.11 frames must be fragmented further resulting in lost throughput.

Answer: A, B
CWNA Offcial Study Guide, 3rd Edition, Pages 141-142 (RF Attenuators)

QUESTION 360:

Which of the following functions require scanning functions in a wireless LAN? Select all that apply.

A. Finding and joining a new infrastructure network.
B. Finding a new access point while roaming.
C. Finding and joining a new ad hoc network.
D. Wireless multicasting
E. Authentication to an access point.
F. Use of the 802.1x/EAP authentication process.

Answer: A, B, C

Explanation:
Scanning functions involves three types of frames: beacons, probe requests, and probe responses. See CWNA Official Study Guide, 3rd Edition, Page 333 (Locating a Wireless LAN)
Stations send a probe request when they are actively seeking a new network to join. See CWNA Official Study Guide, 3rd Edition, Page 336 (Active Scanning)

QUESTION 361:

Direct Sequence Spread Spectrum (DSSS) systems use _____ MHz wide carrier frequencies to transmit data.

A. 1
B. 2
C. 5
D. 11

Answer: A

Explanation:
The frequency hopping physical layer has 22 hop patterns to chose from. The frequency hopping physical layer is required to hop across the 2.4GHz ISM band covering 79 channels. Each channel occupies 1Mhz of bandwidth and must hop at the minimum rate specified by the regulatory bodies of the intended country. A minimum hop rate of 2.5 hops per second is specified for the United States.
The DSSS physical layer uses an 11-bit Barker Sequence to spread the data before it is transmitted.
See pg 76 in CWNA User Guide 2nd edition.

QUESTION 362:

Which of the following are types of frames specified by the 802.11 for wireless LAN transmissions?

A. Data frames
B. Control frames
C. Management frames
D. Coordination frames
E. Media frames

Answer: A, B, C

Explanation:
There are three main types of frames:

- Data Frames: which are used for data transmission
- Control Frames: which are used to control access to the medium (e.g. RTS, CTS, and ACK), and
- Management Frames: which are frames that are transmitted the same way as data frames to exchange management information, but are not forwarded to upper layers.

Each of these types is as well subdivided into different Subtypes, according to their specific function.

QUESTION 363:

A transmitter that emits a 50 mW signal is connected to a cable with 3 dB loss. If the cable is connected to an antenna with a 13 dBi gain, what is the resultant power output in mW at the antenna?

A. 250 mW
B. 300 mW
C. 400 mW
D. 500 mW

Answer: D
Explanation
Net Gain= -3 dB + 13 dBi = + 10 dBi which represents a tenfold increase

in power.
Resultant output Power = 10 times input power= 10 X 50 mW = 500 mW

QUESTION 364:

What is the maximum frequency hop separation of a 2.4 GHz FHSS system (in MHz)?

A. 8 MHz
B. 5 MHz
C. 6 MHz
D. 15 MHz

Answer: C

Explanation:
For FHSS systems, IEEE 802.11 defines 79 different hops for the carrier frequency. Using these 79 frequencies, IEEE 802.11 defines 78 hopping sequences (each with 79 hops) grouped in three sets of 26 sequences each. Sequences from same set encounter minimum collisions and therefore may be allocated to collocated systems. Theoretically, 26 FHSS systems may be collocated, but collisions will still occur in significant amounts. To lower the amount of collisions to acceptable levels, the actual number of FHSS collocated systems should be around 15.
All the above is correct for the case in which the FHSS collocated systems are allowed to operate independently, without any synchronization among their hopping sequences.
If synchronization is allowed, 79 systems could be collocated (theoretically), each one of them using at any moment in time, one of the 79 available frequencies. However, this would require expensive filters in the radio circuitry. Actual products require about 6 MHz separation allowing the collocation of about 12 systems, without any collision! While such synchronization is not always allowed in the unlicensed band of 2.4 GHz, it is common practice in the licensed bands.
The possibility of having collocated systems without collisions, has a tremendous impact on the aggregate capacity / throughput of the installation as well as its efficiency in terms of bps per Hz.

QUESTION 365:

Which of the following descriptions characterizes the IEEE 802.11 shared-key authentication scheme handshakes?

A. One-step process
B. Two-step process
C. Three-step process
D. Four-step process

Answer: D

Explanation:
The 802.11 standard also includes an optional, more advanced form of authentication referred to as shared key authentication. This is a four step process. The client sends an authentication

request frame, and the access point responds with a frame containing a string of characters called challenge text.

QUESTION 366:

Which of the following integrated devices do Access Points typically provide?

A. Lighting arrestor for power circuit protection.
B. Hard drives for configuration backup and operating system storage.
C. Flash RAM for firmware storage.
D. Link and indicator LEDs for status monitoring.
E. Video output port.

Answer: C, D

QUESTION 367:

What is the FCC explanation of the output power of the intentional Radiator?

A. Transmitter output power plus attached cable and connector loss.
B. Transmitter output power only.
C. Output power radiated from antenna.
D. Transmitter output plus gain of the first amplifier only.

Answer: A

QUESTION 368:

Which two of the following elements should be documented in the RF Site Survey Report?

A. Roaming requirements
B. Security requirements
C. Equipment manufacturer recommendations
D. Throughput requirements
E. Wired LAN integration requirements

Answer: A, D

Explanation:
Some of the topics you may want to question the network management about before performing your site survey:
1. Facilities Analysis
2. Existing Networks
3. Area Usage & Towers
4. Purpose & Business Requirements
5. Bandwidth & Roaming Requirements

6. Available Resources
Reference: CWNA official Study Guide, Pg. 297

QUESTION 369:

Which of the following items can cause SIGNIFICANT multipath effects?

A. Trees
B. Body of water
C. Clear glass
D. Metal blinds
E. Long hallway

Answer: D

Explanation:
Common wireless local area network (WLAN) environments with a high probability of multipath interference, include
these:
* airport hangars
* steel mills
* manufacturing areas
* distribution centers
* other locations where the antenna of an RF device is exposed to metal structures, such as:
o walls
o ceilings
o racks
o shelving
o other metallic items

QUESTION 370:

What handshake method is used by RTS/CTS?

A. Two-way handshake
B. Three-way handshake
C. Four-way handshake
D. Five-way handshake

Answer: C

Explanation:
The 802.11 Distributed Coordination Function (DCF) uses a 4-way distributed handshake mechanism (RTS/CTS/DATA/ACK) to resolve contentions between peers. We need to make a distinction between the sender and recipient of a particular packet, and the transmitter and receiver associated with a specific transmission activity: the terms sender and recipient refer to

the RTS/CTS/DATA/ACK transaction as a whole, while transmitter and receiver refer to a specific transmission activity within such a transaction.

QUESTION 371:

Which of the following items are used in performing long-distance outdoor path surveys? Select all that apply.

A. Topographical map
B. Building blueprints
C. 2-way radios
D. Desktop PC
E. Black Electrical tape

Answer: A, C

Explanation:
If a survey to create an outdoor wireless link is being done, obtain the appropriate antennas, amplifiers, connectors, cabling, and other appropriate equipment before arriving. Generally, the more experienced site surveying professionals do the outside site surveys because of the more complex and involved calculations and configuration scenarios that are necessary for outdoor wireless LANs.
Knowing characteristics of the wireless link (distance, link speed required, power output required, etc.) beforehand will aid in determining whether just an omni antenna or an entire outdoor testing lab will be required. Remember that it takes two or more antennas to create a wireless link depending on the number of locations involved in the link.
Binoculars, comfortable walking shoes, rain gear, different lengths of cables, different types of connectors, and some method of communicating with someone at the other end of the link (i.e., a cell phone or walkie-talkie) will also make outdoor site surveys more efficient.
Reference: CWNA official Study Guide, Pg. 312, Page 507 of CWNA Study Guide 3rd edition

---

QUESTION 372:

For which of the following reasons should enterprise organizations use centralized encryption key servers?

A. Distributed key generation
B. Key storage and archiving
C. On-going key rotation
D. MobileIP VPNs
E. Key distribution

Answer: E

Explanation:

For enterprise wireless LANs using WEP as a basic security mechanism, centralized encryption key servers should be used if possible for the following reasons:
Centralized key generation
Centralized key distribution
Ongoing key rotation
Reduced key management overhead
Reference: CWNA official Study Guide, Pg. 264

QUESTION 373:

What type of modulation is used for FHSS transmission in an IEEE 802.11 wireless LAN system?

A. GFSK
B. DBPSK
C. DQPSK
D. CCK
E. OFDM
F. 16QAM

Answer: A

Explanation:
Bluetooth and HomeRF are both FHSS technologies that use GFSK modulation technology in the 2.4 GHz ISM band.
Differential Binary Phase Shift Keying (DBPSK), Differential Quadrature Phase Shift Keying (DQPSK), and Gaussian Frequency Shift Keying (GFSK) are the types of modulation used by 802.11 and 802.11b products on the market today.
Reference: CWNA official Study Guide, Pg. 214

QUESTION 374:

What technology may be implemented to improve upon the original 802.11 standard security?

A. Dynamic WEP key management
B. 802.1x with CHAP support
C. Wireless Equivalent Protocol
D. IGMP

Answer: A

Explanation:
The core functionality of WEP lies in what are known as keys, which are the basis for the encryption algorithm discussed in the previous section of this chapter. WEP keys are implemented on client and infrastructure devices on a wireless LAN. A WEP key is an alphanumeric character string used in two manners in a wireless LAN. First, a WEP key

can be used to verify the identity of an authenticating station. Second, WEP keys can be used for data encryption.
Reference: CWNA official Study Guide, Pg. 262

QUESTION 375:

What term identifies a change in the direction and intensity of radio waves striking a fixed obstacle and the bending of the waves around that obstacle?

A. Diffraction
B. Refraction
C. Diffusion
D. Scattering
E. Reflection

Answer: A

Explanation:
Diffraction occurs when the radio path between the transmitter and receiver is obstructed bya surface that has sharp irregularities or an otherwise rough surface. At high frequencies, diffraction, like reflection, depends on the geometry of the obstructing object and the amplitude, phase, and polarization of the incident wave at the point of diffraction.
Reference: CWNA official Study Guide, Pg. 22

QUESTION 376:

What is an advantage of having a short dwell time when using a FHSS system?

A. Increased resistance to narrowband interference
B. Increased security
C. Increased data throughput
D. Increased range

Answer: A

Explanation:
DSSS products spread their transmission power thinly across the spectrum. Transmitted power in any specific segment of the band is low. As a result, low levels of interference can easily overpower the DSSS transmission. FHSS products, in contrast, use relatively high power in a narrow segment of the band for a short time. This allows the FHSS signal to overpower the interference in their segment of the band.

QUESTION 377:

A GAIN of 10 dB will yield what power ratio?

A. 1:2
B. 2:1
C. 10:1
D. 5:1

Answer: C

Explanation:
Gain of 10 dB results in a tenfold increase.
Therefore Power Ratio will be 10 to 1.

QUESTION 378:

In a DSSS system, which of the following channel pairs DO NOT overlap?

A. channel 1- channel 6
B. channel 2 - channel 4
C. channel 8 - channel 10
D. channel 3 - channel 6

Answer: A

Explanation:
IEEE 802.11 standard for wireless LAN [1] provides multiple channels available for use. The IEEE 802.11b physical layer (PHY) has 14 channels, 5MHz apart in frequency [1]. However, to be totally non-overlapping, the frequency spacing must be at least 30MHz. So channels 1, 6 and 11 are typically used for communication in current implementations, and thus we have 3 channels for use. IEEE 802.11a provides 12 channels, 8 in the lower part of the band for indoor use and 4 in the upper part for outdoor use [2].

QUESTION 379:

What cryptographic algorithm does the FIPS-197 publication propose for U.S. Government use in protecting sensitive (unclassified) information?

A. 3DES
B. Rijndael
C. WEPv2
D. SSID
E. Two-fish

Answer: B

Explanation:
The Advanced Encryption Standard (AES) is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197, that specifies a cryptographic algorithm for use by U.S.

Government organizations to protect sensitive, unclassified information. NIST anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States - in some cases.
This standard specifies the Rijndael algorithm ([3] and [4]), a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard.

QUESTION 380:

The 802.11b standard specifies which of the following power modes?

A. Awake Signal Standby Mode
B. Beacon Poll Mode
C. Continuous Aware Mode
D. Power Save Polling Mode

Answer: C, D

Explanation:
In addition to controlling media access, the 802.11 HR MAC supports power conservation to extend the battery life of portable devices. The standard supports two power-utilization modes, called Continuous Aware Mode and Power Save Polling Mode.

QUESTION 381:

Antenna GAIN is denoted by which of the following measurement units?

A. +dBi
B. +Bi
C. +dB
D. +dBm

Answer: A

Explanation:
Antenna gain and loss are measured in decibels. When quantifying the gain of an antenna, the decibel units are represented by dBi. The unit of measurement dBi refers only to the gain of an antenna. The "i" stands for "isotropic", which means that the change in power is referenced against an isotropic radiator.
Reference: CWNA official Study Guide, Pg. 34

QUESTION 382:

Which of the following affects the amount of effective wireless LAN bandwidth available to the user?

A. Which layer 3 protocol is used
B. Wireless LAN vendor hardware
C. Temperature
D. Fragmentation threshold settings

Answer: D

Explanation:
RTS Threshold feature increases available bandwidth by eliminating RTS/CTS traffic from the air, thus reducing the cost. By setting RTS length threshold to a maximum value, the transmitter will effectively never use RTS and the option is virtually switched off.

QUESTION 383:

What are two reasons why a collision avoidance protocol is used in wireless LAN technology?

A. Collision detection protocols are susceptible to man-in-the-middle attacks.
B. Collision avoidance protocols allow use of antenna diversity.
C. Implementing a collision detection mechanism requires a full-duplex radio.
D. It cannot be assumed that all radios hear each other.

Answer: C, D

QUESTION 384:

What is the minimum number of frequencies that a FHSS system can use in a sequence if it using a carrier bandwidth of 1 MHz?

A. 54
B. 100
C. 79
D. 75

Answer: D

Explanation:
FHSS is also forced to hop within 400 msec. It has to use no less than 75 channels. This means that it is very difficult to get a FHSS system to do 2Mbps and there will be some extra overhead that will affect data throughput.
Note:
Frequency Hopping (FHSS): derived from military radio technology where it was designed to be inherently secure and reliable under adverse battle conditions. Divides the available 83.5 MHz spectrum (in most countries) into 79 (or 75) discrete 1 MHz channels (the 4.5 MHz left over provides a 'guard bands' at either end of the spectrum), the Radio then hops around these 1 MHz channels in a 'pseudo-random' sequence, using a minimum of 75 frequencies every 30 seconds

and using any single frequency for a max. of 400 milliseconds.
pg 181 in CWNA User Guide 3rd edition

QUESTION 385:

What organization creates regulations for radio frequency use in the United States?

A. IEEE
B. IETF
C. FCC
D. ETSI

Answer: C

Explanation:
In the Big LEO service, systems must be capable of providing both continuous service to users in the United States and global coverage. The FCC recognizes, however, that private industry is best positioned to determine what type of technology and systems make best business sense and are most responsive to customer needs. Thus, the FCC requires only that the minimum technical requirements needed to prevent interference are met, and seeks to provide licensees maximum flexibility.

QUESTION 386:

Which of the following are locations where the WEP key is often stored on a client computer?

A. In an encrypted .key file.
B. In the Windows registry.
C. In the computer's BIOS.
D. On the hard drive in a text file.
E. In the PC Card firmware.
F. WEP keys are not stored on client computers.

Answer: B

Explanation:
When communicating over the wire, wireless network equipment uses WEP keys to encrypt the data stream. The keys themselves are not sent over the network but rather are generally stored on the wireless adapter or in the Windows Registry.
Static WEP keys are write-only and temporary; therefore, they cannot be read back from the client adapter, and they are lost when power to the adapter is removed or the Windows device is rebooted. Although the keys are temporary, you do not need to re-enter them each time the client adapter is inserted or the Windows device is rebooted. This is because the keys are stored (in an encrypted format for security reasons) in the registry of the Windows device. When the driver loads and reads the client adapter's

registry parameters, it also finds the static WEP keys, unencrypts them, and stores them in volatile memory on the adapter.
Note: Possibly E as well.

QUESTION 387:

Which of the following items are essential when performing an RF site survey on a warehouse facility?

A. Facility blueprints showing wiring closet locations.
B. Forklift for moving stored materials when necessary.
C. Lifts or ladders for mounting temporary access points.
D. Long category 5 cables for connecting access points to wiring closets.
E. Binoculars and a rain suite.

Answer: A, C

QUESTION 388:

As specified in the IEEE 802.11 standard, what is the default authentication method for a wireless client device to authenticate to an access point?

A. Open System
B. Shared Key
C. Dynamic Key
D. 802.1x/EAP

Answer: A

Explanation:
When your network card identifies the hotspot, your card and the hotspot undertake a process of mutual authentication by exchanging data in management frames. There are two standard mechanisms that can be used, the Open System Authentication and the Shared Key Authentication. The open system authentication is the default method of authentication between your card and the access point. Anybody that wants to be authenticated with the base station can be. Even when this information is sent using the wired equivalent privacy protocol (WEP), which is designed to provide for confidentiality when using a wireless network, the authentication management frames are still sent in clear text, thus helping to defeat the use of this particular security protocol.

QUESTION 389:

What option is considered a possible wireless LAN security solution?

A. 802.11g
B. RIPv2 tunneling

C. VRRP
D. IPsec with certificates

Answer: D

Explanation:
If the objective of deploying IPSec is to protect against vulnerabilities in the wireless LAN security protocols, you must deploy certificate-based authentication, or use an authentication method which tightly binds the inner and outer authentications. IPSec tunnels can be secure against compound binding problems, although this is difficult to do using tunneled legacy authentication based on XAUTH---the most common implementation.

QUESTION 390:

Which of the following are used by wireless LANs to overcome the problem associated with the inability to detect collisions?

A. Collision avoidance
B. Positive acknowledgments
C. Frame fragmentation
D. Station polling

Answer: A

Explanation:
Collision detection is difficult to implement in wireless networks because it requires simultaneous transmission and reception on the same band. Access is controlled by collision avoidance (CA) instead. Any access delay is typically small delay due to the higher speeds involved.
Creating a mechanism to prevent the potential conflicts in the shared medium has always been a challenge for Network Designers. A set of different proposals and drafts are available, initially for the wired and lately for wireless environments, based on so-called collision avoidance techniques. The basic idea is to negotiate the data exchange before the collision happens, or to force the non-active users to defer their translation for a period of time.

QUESTION 391:

What is the total bandwidth of the 2.4 GHz ISM band?

A. 70 MHz
B. 83.5 MHz
C. 90.5 MHz
D. 100 MHz

Answer: B

Explanation:
Current FCC regulations expressly authorize adaptive hopping as a means to minimize interference, but its implementation is blocked for Bluetooth and IEEE 802.11b communications by other constraints. The FCC requires narrowband hoppers (those with bandwidths up to1 MHz) to use at least 75 hopping frequencies and the band itself is only 83.5 MHz.
pg 304 in CWNA User Guide 3rd edition

QUESTION 392:

Which of the following problems can be caused by VSWR? Select two.

A. Transmitter burnout
B. Decreased RF signal amplitude at the receiver
C. RF antenna failure
D. RF connector deterioration

Answer: A, B

QUESTION 393:

What is the FCC definition of Equivalent Isotrophically Radiated Power (EIRP)?

A. Transmitter output power plus attached cable and connector loss
B. Transmitter output power only
C. Power supplied to the antenna plus antenna gain
D. Power radiated by an amplifier due to an improper seal

Answer: C

QUESTION 394:

What statement is TRUE regarding the Service Set Identifier (SSID)?

A. It is an identifier used in SSH sessions to an access point or wireless bridge
B. It is a common network name for the devices in a Wireless LAN system
C. It is a number used in identifying the unit's manufacturer
D. It is a number used by wireless clients only for identification of access points.

Answer: B

QUESTION 395:

On a wireless LAN, which of the following MUST be true regarding all wireless client devices accessing the same access port?

A. All users are in a single collision domain

B. All users are in a single layer 3 broadcast domain
C. All users have full duplex communication with that access point
D. All users incorporate the Spanning Tree protocol to avoid loops in the layer 2 topology

Answer: A

QUESTION 396:

Wireless LAN client software may include which of the following components?
Select three.

A. Spectrum analyzer
B. Table of known APs
C. RF noise generator
D. Table of associated Ad Hoc clients
E. FCC license certificate for the manufacturer

Answer:

QUESTION 397:

How many 2.4 GHz ISM band DSSS channels are available for use in the United States according to the FCC?

A. 1
B. 11
C. 12
D. 14

Answer: B

QUESTION 398:

What is the HORIZONTAL beam width of an omni-directional antenna?

A. 45 degrees
B. 90 degrees
C. 180 degrees
D. 360 degrees
E. It varies

Answer: D

QUESTION 399:

Which of the following pieces of equipment might be part of a site survey equipment

kit for outdoor site surveys? Select two.

A. Two-way radios if working in teams
B. Certificate server for authentication testing
C. A mobile equipment cart
D. A clinometer
E. An RF attenuator

Answer: A, B, D

Explanation:
For A follow this link.
http://www.wi-fiplanet.com/tutorials/article.php/953661
For B and D.
See CWNA Official Study Guide, 3rd Edition, Pages 265-267
Outdoor Site Surveys
Point-to-Point (PTP) and Point-to-Multi-Point (PTMP) outdoor surveys typically are more complex than indoor surveys and require more skill to perform quality surveys. An outdoor survey should include the following areas of review:
1. Site Description
2. Site access information
3. Determination of optimal RF coverage
4. Power requirements/location
5. Interference Analysis
6. Microwave interferers
7. Obstruction evaluation
8. Visual building inspection
9. Topographical map study
10. Free space loss
11. Installation equipment
12. Special circumstances
13. Site location characteristics
14. Success Prediction
15. Determination of Radio placement/mounting
16. Environmental considerations
17. Antenna placement
18. Drive Data
19. Visual tower inspection
20. Cable routing
21. Equipment list
22. Link budget
23. Area weather analysis
Outdoor surveys typically require a combination of software analysis and onsite visits. From a software point a typographical map overview is reviewed which is then combined with the onsite visit and drive data. Free space loss is calculated and the fresnel zone is determined.

QUESTION 400:

Which of the following is an authentication service used in wireless 802.1x implementations?

A. WEP
B. AES
C. RADIUS
D. SSL
E. DRAS

Answer: C

Explanation:
Page 432 of CWNA Study Guide 3rd edition

QUESTION 401:

Which of the following should be included in a wireless security solution to address common security concerns? Select two.

A. One WEP key for the entire organization
B. Use of only Shared Key authentication with static WEP keys
C. WEP keys that are generated dynamically upon user authentication
D. Rotated broadcast WEP keys

Answer: C, D

QUESTION 402:

Which of the following are mechanisms defines by 802.11 for providing access control and privacy on a wireless LAN? (Choose two)

A. RADIUS
B. WEP
C. AES
D. SSID
E. 802.1x/EAP

Answer: B, D

Explanation:
SSID Network access control can be implemented using an SSID associated with an AP or a group of Aps. The SSID provides a mechanism to "segment" a wireless network into multiple networks service by one or more Aps. Each AP is programmed with a SSID corresponding to a specific

wireless network. To access this network, client computers must be configured with the correct SSID.
WEP
WEP provides encrypted communication using an encryption key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network.
The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, used to protect link layer communication from eavesdropping and other attacks.
This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security we find in a wired medium.

QUESTION 403:

Enterprise Wireless Gateways may support which of the following network security (VPN) protocols? Select three.

A. OSPF
B. L2TP
C. IPSec
D. ICMP
E. IRDP
F. PPTP

Answer: B, C, F

Explanation:
The following VPN tunnels can be used: PPTP, L2TP, SSH & IPSec
Page 277 of CWNA Study Guide 3rd edition

QUESTION 404:

What is an attribute of a lightning arrestor?

A. Cannot handle a direct lightning strike and will discharge energy to an Earth ground connection.
B. Can handle a direct lightning strike and will discharge energy to a chassis ground connection
C. Cannot handle a direct lightning strike and will discharge energy into the network to which it is connected
D. Can handle a direct lightning strike and will discharge energy directly into lightning rod

Answer: A

Explanation:
Page 146 of CWNA Study Guide 3rd edition

QUESTION 405:

In a DSSS system, which of the following channel pairs DO NOT overlap? Select two.

A. channel 5 - channel 9
B. channel 6 - channel 12
C. channel 2 - channel 10
D. channel 4- channel 7

Answer: B, C

QUESTION 406:

What is the minimum number of frequencies that a FHSS system can use in a sequence if the system is using a carrier bandwidth of 5 MHz?

A. 15
B. 25
C. 55
D. 75

Answer: A

QUESTION 407:

Which of the following items means that measurable ability to resist radio frequency interference?

A. EMF stability
B. Signal Strength Ratio
C. Jamming Margin
D. Signal Squelch

Answer: B

QUESTION 408:

Which type of scanning uses Probe Requests and Response frames?

A. Passive
B. Active
C. Associative
D. Sequence

Answer: B

QUESTION 409:

Which of the following are measurement units for a calculable amount of power?

A. dB
B. dBm
C. dBi
D. mW

Answer: D
The answer to this question could really be B or D with D being the choice if looking for the one best answer.

QUESTION 410:

What topic would be included in an RF Site Survey Report?

A. Internet connectivity placement and speed
B. Wireless LAN troubleshooting techniques
C. Appropriate equipment types to implement
D. Wireless LAN Security analysis

Answer: C

QUESTION 411:

What features assist in the reduction of lost data due to wireless LAN PC cards (clients) going to sleep while operating in INFRASTRUCTURE mode? Select two.

A. Access point queue buffers
B. Establishes wake-up intervals on the PC card
C. PC cards randomly alternative beacon transmissions
D. Use of ATIM window

Answer: A, B

Explanation:
D is wrong since this only works in an ad-hoc mode

QUESTION 412:

Which two of the following characteristics of MAC filters make it simple for hackers to bypass MAC filters in access points? Select all that apply.

A. MAC addresses are broadcast in the clear
B. MAC addresses are only 12 bytes long and are easy to guess
C. MAC filters can be easily altered on access points by via SNMP
D. Client MAC addresses may be easily changed in the Windows registry

E. The IEEE published the Organizationally Unique Identifier (OUI) list publicly

Answer: A, C
Reference: See CWNA Official Study Guide, 3rd Edition, Pages 408-409 (Throughput)

QUESTION 413:

What is the maximum dwell time allowed by the FCC for Frequency Hopping systems?

A. 100 ms per 30 second period
B. 400 ms per 30 second period
C. 800 ms per 30 second period
D. 1000 ms per 30 second period

Answer: B

QUESTION 414:

Which of the following are advantages of Power over Ethernet (PoE)? Select all that apply.

A. Reduced number of Ethernet switches necessary to build a LAN
B. Flexibility of placement of access points where no power is available
C. Reduced number of Ethernet drops necessary for cabling a LAN
D. Cost savings of installing AC power receptacles
E. Allows data cables to exceed the 100 meter limit

Answer: B, D

QUESTION 415:

What term best describes a device designed to decrease the power of the RF signal in a wireless LAN?

A. Amplifier
B. Capacitance coupler
C. Resistance Injector
D. Attenuator

Answer: D

QUESTION 416:

You are performing an outdoor site survey for Certkiller .com. Certkiller, the network manager approaches. She informs you that Certkiller .com has just decided to erect a tower to place a 2.4 GHz wireless LAN antenna.

Which of the following questions should you ask prior to completion of the site survey?

A. Is the weather in this area volatile?
B. Are there many squirrels or birds in this particular area?
C. Are power lines located near where the tower will be placed?
D. Is there a possibility of future obstructions around the tower location?
E. Are there any underground water pipes in the area?
F. Has the area been zoned for commercial use?

Answer: A, D

QUESTION 417:

Which of the following factors influence wireless LAN throughout?

A. Nearby satellite TV dishes in use
B. Fresnel zone circumference
C. Use of RTS/CTS
D. Air density and barometric pressure in surrounding area

Answer: C

QUESTION 418:

You are administering a network with wireless LAN components for Certkiller .com. The wireless portion of the network is configured using statically assigned WEP keys stored on each station's wireless PC Card. It has been reported to you that one of the wireless client computers containing a wireless PC Card has been stolen. What reasonable actions could be taken to restore the wireless LAN to the former level of security? Select one.

A. Polling could be configured on each access point
B. The wireless LAN could be disabled until the stolen PC card is recovered
C. The stolen PC card's MAC address could be filtered on all access points
D. The wireless network authentication scheme could be changed to assign WEP keys dynamically, both remedying this situation and reducing future security threats.
E. A policy could be implemented that called for all static WEP keys to be changed daily

Answer: C

QUESTION 419:

Which of the following types of secret key implementations are part of WEP (not including the Initialization Vector? Select all that apply.

A. 40-bit
B. 56-bit

C. 80-bit
D. 96-bit
E. 104-bit

Answer: A, E

Explanation:
WEP provides encrypted communication using an encryption key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network.
WEP specifies the use of a 40 bit encryption key and there are also implementations of 104 bit keys.The encryption key is concentrated with a 24 bit "initialisation vector", resulting in a 64 or 128 bit key. This key is input into a pseudorandom number generator. The resulting sequence is used to encrypt the data to be transmitted.
WEP uses the RC4 PRNG algorithm from RSA Data Security.
The 802.11 standard does not specify a management protocol, so all WEP keys on a network must be managed manually. WEP security is not available in ad hoc (or peer-to-peer) 802.11 networks that do not use Aps.

QUESTION 420:

What spread spectrum technology specified in the IEEE 802.11 series of standards is most resilient in the presence of narrowband RF interference?

A. Frequency Hopping
B. Direct Sequencing
C. infrared
D. Laser

Answer: A

QUESTION 421:

Which of the following refer to the electrical fields emitted from antennas? Select all that apply.

A. Beams
B. Lobes
C. Fans
D. Bands
E. Legs

Answer: A, B

QUESTION 422:

Which of the following characteristics describe narrowband RF interference?

A. It has higher peak amplitude than spread spectrum RF
B. May cause degradation of a spread spectrum RF signal
C. May appear as a multiple of the carrier frequency
D. May appear as a sideband of the resonant frequency

Answer: A

QUESTION 423:

What Wireless LAN configuration implements power management by having stations transmit beacons after they awake from sleep mode?

A. Integrated Service Set (ISS)
B. Basic Service Set (BSS)
C. Independent Basic Service Set (IBSS)
D. Extended Service Set (ESS)

Answer: C

QUESTION 424:

For seamless roaming to be successful, which of the following items must match between Access Point and the wireless client device when WEP is being used? Select all that apply.

A. Matched Service Set Identifiers
B. Matched MAC filters on both units
C. Matched WEP keys
D. Matched scanning types
E. Matched spread spectrum technology in use on both units

Answer: A, B, C, E

QUESTION 425:

Manufactures of 802.11 compliant wireless LAN client devices allow for administrator configuration of which of the following on the client? Select one.

A. 802.1q tagging
B. Shared Key authentication
C. TKIP
D. Private security authorization

Answer: B

QUESTION 426:

Which two of the following items assist in performing an indoor site survey? Select two

A. Facility blueprint
B. RF Line-of-Sight
C. Wireless LAN client utilities
D. Rubber gloves
E. Site survey report

Answer: A, C

QUESTION 427:

Which reasons indicate why throughput on a FHSS system is less than throughput on a DSSS system at the same rated bandwidth? Select all that apply.

A. FHSS has the overhead of hop time
B. FHSS systems have larger interframe gape times
C. FHSS uses CSMA/CD instead of CSMA/CA

Answer: A

QUESTION 428:

Which of the following are mechanisms defined by the 802.11 standard providing a secure operating environment? Select all that apply.

A. VPNs
B. Shared Key Authentication
C. WEP
D. Access Control Lists
E. 802.1x/EAP
F. Intrusion Detection

Answer: B, C

Explanation:
Question pertains to 802.11 standard hence the answer is B & C

QUESTION 429:

Which of the following are appropriate uses of a wireless LAN using IEEE 802.11b technology? Select two.

A. Network Extensions to reach remote parts of a building

B. "Access" role in an enterprise network
C. Streaming audio & video applications to the desktop
D. High speed network backbone in a hosting facility

Answer: A, B
For answer A.
See CWNA Official Study Guide, 3rd Edition, Page 8 (Network Extension to Remote Areas)
For answer B.
See CWNA Official Study Guide, 3rd Edition, Page 5 (Three Main Roles for Wireless LANs)

QUESTION 430:

Which of the following options is a possible wireless LAN security solution?

A. L2TP with RADIUS
B. PEAP with TACACS
C. Universal Data Protocol
D. EAP-MD5 with PAP support

Answer: A

QUESTION 431:

Which of the following protocols is NOT supported on an 802.11b wireless LAN?

A. IPX/SPX
B. TCP/IP
C. DECnet
D. Netbeui
E. ISDN

Answer: E

Explanation:
ISDN is not a network protocol.

QUESTION 432:

What agency governs the allocation of building permits for eracting towers for mounting wireless LAN equipment?

A. Federal law
B. FCC
C. Local municipalities

D. FAA

Answer: D

Explanation:
We think the answer is D since the FCC requires that the FAA be notified for towers that are greater than 200 feet above ground. For towers that are less than 20 feet high, FAA notification is not required. See pages 488 and 489 in CWNA Study Guide 3rd edition

---

QUESTION 433:

What information types are passed from the access point to the wireless clients using the Beacon Management Frame? Select two.

A. Traffic Indication Map
B. Announcement Traffic Indication Message
C. Service Set Identifier
D. MAC filter sequence numbers

Answer: A, C
Fragmentation. An 802.11 station can use the optional fragmentation protocol to divide 802.11 data frames into smaller pieces (fragments) that are sent separately to the destination. Each fragment consists of a MAC Layer header, FCS (frame check sequence), and a fragment number indicating its ordered position within the frame. With thresholds properly set, fragmentation can reduce the amount of data that needs retransmission. RF interference often causes only a small number of bit errors to occur. Instead of resending the entire data frame, the station implementing fragmentation only needs to retransmit the fragment containing the bit errors. The key to making fragmentation improve throughput is to set the thresholds properly. A threshold too low will result in smaller fragments (making retransmissions efficient), but the greater number of fragments requires substantial overhead because of the additional headers and checksums. As with RTS / CTS, use a trial and error process to set the threshold while keeping an eye on consequential throughput. If there is no appreciable RF interference, then it's best to deactivate fragmentation.

QUESTION 434:

If devices each using one of the following frequency spectrums has identical power output and an identical antenna, the device using which of the following spectrums would have the longest range?

A. 900 MHz
B. 2.4 GHz
C. 5.7 GHz
D. 1800 MHz

Answer: A

Explanation: The range is inversely proportional to the frequency therefore the smallest frequency will result in the highest range, power output being equal.

QUESTION 435:

In a wireless LAN, which of the following can cause power degradation in the RF signal?

A. Antenna extension cable
B. Open air space between transmitter and receiver
C. The transmitter
D. Connectors
E. Amplifier
F. Bright sunlight

Answer: A, B, D

Explanation:
A and D introduces impedance which would cause degradation. B will also contribute by free space path loss and by multi-path

---

QUESTION 436:

What term refers to the RF signal amplitude degradation as the propagated wave moves through space?

A. Distance Attenuation
B. Free-Space Path loss
C. Path-Signal loss
D. Signal Path Attenuation

Answer: B

QUESTION 437:

Which of the following statements describe characteristics of an RF Site Survey Report?

A. It restates the client's requirement and business justification for the wireless LAN
B. It is a one-page inspection summary certificate
C. It contains the results from the RF interference and coverage analysis
D. It is an internal document to the site surveying form and never shared with the client
E. It contains a report on the cooperative behaviour of the union

Answer: A, C

QUESTION 438:

Which technology experiences difficulties due to the "Near/Far" problem?

A. Laser
B. IrDA
C. DSSS
D. FSO

Answer: C

QUESTION 439:

According to FCC regulations, when an RF amplifier is used in a wireless LAN configuration what statement is correct?

A. The RF amplifier must be sold and used as part of a certified system.
B. The RF amplifier can be sold and used as a stand-alone unit for use with any other software
C. The RF amplifier must provide a fixed output that does not exceed FCC regulations for EIRP
D. The amplifier itself must have a FCC certification number

Answer: A
See CWNA Official Study Guide, 3rd Edition, Page 137 (Special Stipulations on Amplifiers)

QUESTION 440:

What wireless LAN client device attaches multiple computers on a wired LAN into a wireless LAN access point as a single client?

A. USB client
B. Wireless Bridge
C. Workgroup Bridge
D. PC Card

Answer: C
See CWNA Official Study Guide, 3rd Edition, Page 253 (Wireless Workgroup Bridges)

QUESTION 441:

As a wireless LAN administrator at Certkiller .com, which of the following security attacks must you protect your network against? Select all that apply.

A. Reassocation
B. MAC spoofing
C. Active Probing

D. Casual eavesdropping
E. Fragmentation

Answer: B, C

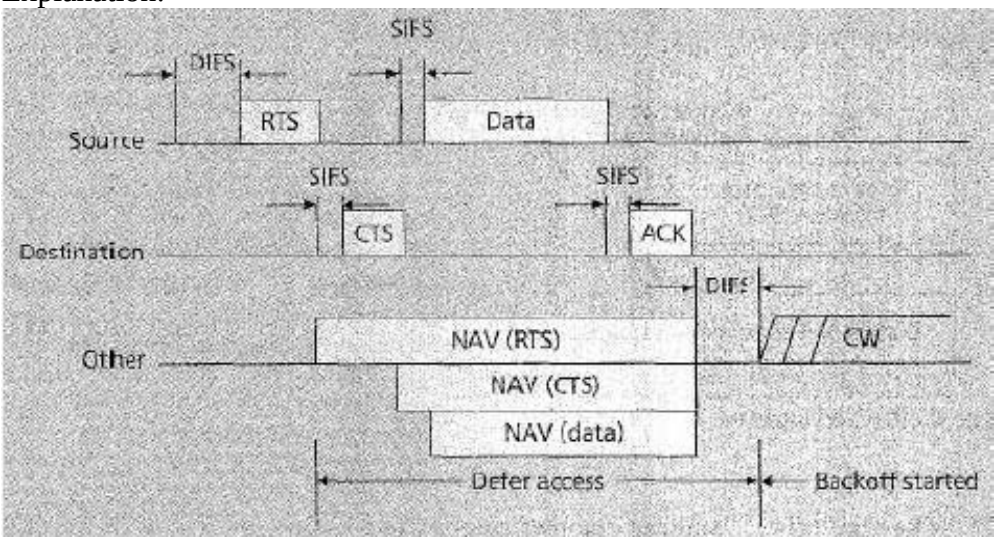
QUESTION 442:

What option lists the correct order for the RTS/CTS protocol's 4-way handshake?

A. RTS, CTS, ACK, DATA
B. RTS, ACK, CTS, DATA
C. RTS, CTS, DATA, ACK
D. RTS, ACK, DATA CTS

Answer: C

Explanation:



Sequence is RTS, CTS, Data and ACK.

QUESTION 443:

What term refers to a reduction in signal amplitude at the receiving antenna due to multipath effects?

A. Upfade
B. Absorption
C. Nullfade
D. Downfade
E. Reflection

Answer: D

Explanation:
pg 329 in CWNA User Guide 2nd edition

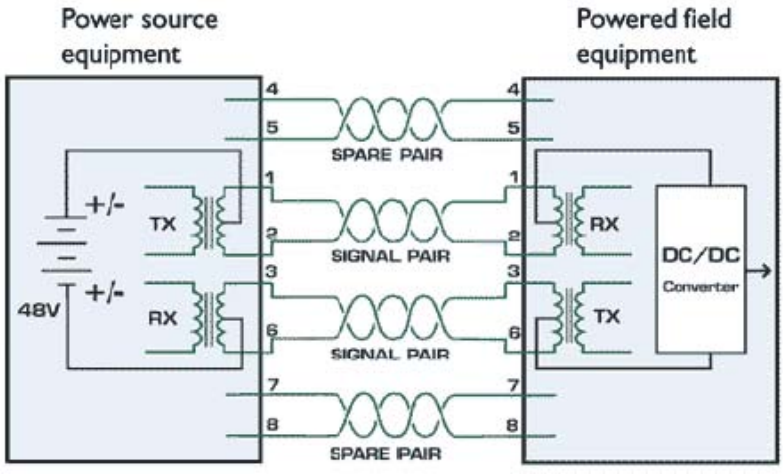
QUESTION 444:

The IEEE 802.3af standard specifies what type of voltage and which set of wires for in-line powering devices such as access points and wireless bridges?

A. 48 VDC over pins 1, 2, 3, & 6 in Category 5 cable
B. 44-57 VDC over pins 1, 2, 3, & 6 in Category 5 cable
C. 24 VAC over pins 4, 5, 7, & 8 in Category 5 cable
D. 48 VDC over pins 4, 5, 7, & 8 in Category 5 cable
E. At least 40 VDC over pins 1, 2, 3, & 6 or 4, 5, 7, & 8 in Category 5 cable
F. At least 24 VDC over pins 4, 5, 7, & 8 in Category 5 cable

Answer: B

Explanation:
Basic properties of the standard IEEE 802.3af
1. voltage between 44V and 57V
2. maximal current 550mA
3. maximal trigger current 500mA
4. typical current 10mA - 350mA
5. overload detection 350mA - 500mA
6. maximal demand of 5mA in idle condition
Two problems are connected with the Power over Ethernet (PoE). The first one is the need to keep the possibility to use older networks elements and the second one is the compliance of the 802.3af standard if all 8 cable cores (4 pairs) in contemporary cabling (CAT5)are used. Therefore the 802.3af standard specifies the application of the PoE on contemporary cabling for 10Mbit, 100Mbit and 1000Mbit Ethernet.



Because of the Ethernets configuration of the physical layer is the supply voltage transported by wires that are assigned for data transmission. The signals in Ethernet are transported by twisted pairs, which are connected to signal transformers included in

devices on both sides of the wire.The middle-pointsof coil windingare on theinner side of these transformersconnected (according the original specification of Ethernet)to the ground over the isolating transformer. In case that these middle-points of coil winding are connected to another direct level, the data signal on the output of device will have different direct value against the ground, because the same transformer is placed on the other end of the wire.

QUESTION 445:

Which of the following are essential for establishing a high quality 2.4 GHz point-to-point RF link at a distance of 5 miles (8 kilometers)?

A. 2-way power splitters at each end of the link
B. Proper link budget calculations
C. Proper Earth bulge calculations
D. Fresnel Zone that is at least 60% clear of obstructions
E. Low gain omni-directional antenna

Answer: B, D

QUESTION 446:

What frequency range does the 802.11a standard operate in?

A. 900 MHz range
B. 2.4 GHz range
C. 5 GHz range
D. 8 GHz range

Answer: C

Explanation:
802.11a transmits radio signals in the frequency range above 5 GHz. This range is "regulated," meaning that 802.11a gear utilizes frequencies not used by other commercial wireless products like cordless phones

---

QUESTION 447:

What RF communications technique is categorized by high peak power and narrow bandwidth?

A. Spread Spectrum
B. Narrowband
C. Wideband
D. Laserband

Answer: B

QUESTION 448:

What is an important benefit of RC4?

A. Has a fast encryption speed
B. PRNG is concatenated with the secret key
C. Key stream is incorporated with plain text
D. Uses up to 4096-bit keys

Answer: A

Explanation:
Page 378 of CWNA Study Guide 2nd edition

QUESTION 449:

A transmitter that emits a 50 mW signal is connected to a cable with 3 dB loss. If the cable is connected to an antenna with a 13 dBi gain, what is the resultant power output in mW at the antenna?

A. 50 mW
B. 250 mW
C. 500 mW
D. 1000 mW

Answer: C
Explanation
Net Gain= -3 dB + 13 dBi = + 10 dBi which represents a tenfold increase
in
power
Resultant output Power = 10 times input power= 10 X 50 mW = 500 mW

QUESTION 450:

Choose the term that specifies an RF ware's orientation as it leaves the antenna element.

A. Propagation attack edge
B. E plane polarization
C. Directrional frequency pattern
D. Signal distribution design

Answer: B

QUESTION 451:

Which of the following are types of wireless LAN antennas?

A. Dipole
B. Bi-directional
C. Patch
D. Elongated
E. Isotropic

Answer: A, C

Explanation:
A dipole antenna is a straight electrical conductor measuring 1/2 wavelength from end to end and connected at the center to a radio-frequency (RF) feed line. This antenna, also called a doublet, is one of the simplest types of antenna, and constitutes the main RF radiating and receiving element in various sophisticated types of antennas. The dipole is inherently a balanced antenna, because it is bilaterally symmetrical.
Dipole antennas can be oriented horizontally, vertically, or at a slant. The polarization of the electromagnetic field (EM) radiated by a dipole transmitting antenna corresponds to the orientation of the element. When the antenna is used to receive RF signals, it is most sensitive to EM fields whose polarization is parallel to the orientation of the element. The RF current in a dipole is maximum at the center (the point where the feed line joins the element), and is minimum at the ends of the element. The RF voltage is maximum at the ends and is minimum at the center.

QUESTION 452:

Which of the following statements is TRUE regarding RF cables and connectors?

A. Connector quality does not affect RF signal quality
B. Cable quality affects only VSWR measurements
C. Two like connector types may vary in their manufacturer specifications
D. High quality cables are expensive, but cause no loss

Answer: C

Explanation:
Pages 189 & 190 in CWNA Study Guide 2nd edition

QUESTION 453:

While an access point is operating in Distributed Coordination Function (PCF) mode, which of the following is TRUE?

A. CSMA/CS is used to avoid collisions.
B. Polled stations contend for the medium in order to send broadcasts and multicast traffic
C. Time-bounded data such as voice and video can be given an improved quality of service.

D. Network overhead is increased due to polling.

Answer: A

Explanation:
Page 301 of CWNA Study Guide 2nd edition

QUESTION 454:

In order to obtain Wi-Fi certification, a manufacturer's OFDM system must adhere to which of the following?

A. Predetermined frequency hopping patterns designated by the IEEE 802.11 standard.
B. Designated power consumption settings as determined by the FCC.
C. AES encryption and support VPN protocols such as PPTP and L2TP.
D. OFDM systems are not included in Wi-Fi certification.
E. Inclusion of 12, 18, & 24 Mbps link rates.

Answer: E

Explanation:
IEEE 802.11 standard specifies a 2.4 GHz operating frequency with data rates of 1 and 2 Mbps using either Direct Sequence Spread Spectrum (DSSS) or Frequency Hopping Spread Spectrum (FHSS). The IEEE 802.11a standard specifies an OFDM physical layer (PHY) that splits an information signal across 52 separate subcarriers to provide transmission of data at a rate of 6, 9, 12, 18, 24, 36, 48, or 54 Mbps. In the 802.11a IEEE standard the 6, 12, and 24 Mbps data rates are mandatory. Four of the subcarriers are pilot subcarriers that the system uses as a reference to disregard frequency or phase shifts of the signal during transmission.

QUESTION 455:

Which IEEE standards specify a data rate up to 54 Mbps? Select all that apply.

A. 802.11
B. 802.11b
C. 802.11g
D. 802.11a
E. 802.11i
F. 802.1x

Answer: C, D

Explanation:
Wireless developers wanted speed, performance faster than the promised 11Mbps of 802.11b, and we wanted plenty of it. We were grasping at straws like a monster-clown in search of adrenochrome. Atheros and Radiata were working against each other on the chips required,

getting power demands and cost down, and signal range up.

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; when wiring is inconvenient
Devices currently using the standard	Consumer products by Linksys, Intel, lucent, proxim,cisco; chipsets made by Radiata

802.11g is an easy choice for corporate sites and home users to adopt because it doesn't require an upgrade to client equipment. 802.11g is backward-compatible with 802.11b, and it offers speeds similar to those of 802.11a.

Standard	IEEE 802.11g, Wi-Fi
Frequency wavelength	2.4GHz
Data bandwidth	54Mbps, 48Mbps, 36Mbps, 24Mbps, 12Mbps, 6Mbps
Security measures	WEP, OFDM, AES (in Broadcom 54g) and possibly WPA/Wi-Fi protected access
Optimum operating range	1000 ft. under ideal conditions; expect 150 ft. indoors, 300 ft. outdoors, under normal conditions
Best suited for a specific purpose or device type	Roaming laptops in home or business; when wiring is inconvenient
Devices currently using the standard	Consumer products by Apple, Linksys, Lucent, lucent, cisco, buffalo, belkin; chipsets Broadcom, Atheros, Intersil

QUESTION 456:

Enterprise Wireless Gateways often use RADIUS to authenticate users. Which of the following database types might the RADIUS server query to authenticate the user for the Enterprise Wireless Gateway? Select all that apply.

A. Windows NT Domain
B. Microsoft Access
C. A text file
D. UNIX NIS
E. LMHOSTS

Answer:

QUESTION 457:

Wireless LAN client software may include which of the following components? Select all that apply.

A. Site survey utility
B. Signal strength monitor
C. Wireless packet analyzer
D. IP subnet calculator
E. Layer 3 diagnostic utilities

Answer: A, B

QUESTION 458:

Which two of the following weather conditions have a measurable impact on outdoor spectrum WLANs in the 5 GHz frequency range?

A. Bright sunlight
B. Heavy mist or rain
C. Hot temperatures
D. Dense fog
E. Ambient audible noise floor

Answer: B, D

QUESTION 459:

Which of the following indicates an increase in the amplitude of an RF signal caused by an external source?

A. Attenuation

B. Diffraction
C. Gain
D. VSWR

Answer: C

QUESTION 460:

What feature allows a wireless PC Card to adjust its transmission speed to compensate for the changing nature of the immediate RF environment?

A. Enhanced Speed Lock
B. Rate Lock Agility
C. Automatic Speed Select
D. Automatic Rate Selection

Answer: D

QUESTION 461:

The 802.11a standard specifies what number of non-overlapping channels in each UNII band?

A. 3
B. 4
C. 6
D. 8

Answer: B

Explanation:
According to the study guide, each of the 3 bands in the 5 GHz UNII band (lower, middle, upper) contain 4 non-overlapping channels. The question ask the number of such channels "combined".

QUESTION 462:

For radio transmitters utilizing FHSS technology with >75 hopping frequencies in the 2.4 GHz ISM band, what is the maximum EIRP allowed by the FCC in a point-to-multipoint environment?

A. 4 Watts
B. 30 dBm
C. 100 mW
D. 27 dBm

Answer: B

Explanation:
Pre 8/31/00 used here which specifies the power of 1 Watt = 30 dBm
pg 73 in CWNA User Guide 2nd edition

QUESTION 463:

What term refers to a block in communication between a wireless client and an access point due to high power transmitter operating closer to the access point?

A. Hidden Node
B. Near/Far
C. RTS/CTS
D. CSMA/CA
E. Multipath

Answer: B

QUESTION 464:

What is the reason that using the SSID is NOT recommended as a secure method to permit or deny access to a wireless LAN?

A. The SSID is not accessible until the user is associated
B. The SSID is encrypted, and only authorized users have access to the decryption key
C. The SSID cannot be used to authorize users in this way
D. The SSID is broadcast in the clear by default in multiple WLAN frame types

Answer: D

QUESTION 465:

Which option may be used as a wireless LAN security solution?

A. Wireless router with integrated firewall features
B. Wireless bridge with integrated access point
C. Circularly-polarized antennas
D. Secure amplifiers
E. Layer3 switch running RIPv2

Answer: A

QUESTION 466:

The IEEE 802.11, 802.11b, and 802.11g standards specifies use of the 2.4 GHz ISM band.

What frequencies are actually used for data transmission?

A. 2.4000 - 2.5000 GHz
B. 2.4000 - 2.4750 GHz
C. 2.4000 - 2.4725 GHz
D. 2.4000 - 2.4835 GHz

Answer: D

Explanation:
The 802.11 radio WLANs operate in the 2.4GHz (2.4 to 2.483 GHz) unlicensed Radio Frequency (RF) band. The maximum isotropic transmission power in this band allowed by FCC in US is 1Wt, but 802.11 devices are usually limited to the 100mWt value.

QUESTION 467:

Which of the following statements are TRUE regarding wireless LAN performance?

A. Smaller frame sizes result in greater throughput in a high interference environment
B. Use of the maximum wireless frame size on the access point will increase throughput between the wired and wireless networks
C. Segmentation and reassembly have no effect on latency
D. Frames are a fixed size on a wireless LAN

Answer: A

Explanation:
Fragmentation. An 802.11 station can use the optional fragmentation protocol to divide 802.11 data frames into smaller pieces (fragments) that are sent separately to the destination. Each fragment consists of a MAC Layer header, FCS (frame check sequence), and a fragment number indicating its ordered position within the frame. With thresholds properly set, fragmentation can reduce the amount of data that needs retransmission. RF interference often causes only a small number of bit errors to occur. Instead of resending the entire data frame, the station implementing fragmentation only needs to retransmit the fragment containing the bit errors. The key to making fragmentation improve throughput is to set the thresholds properly. A threshold too low will result in smaller fragments (making retransmissions efficient), but the greater number of fragments requires substantial overhead because of the additional headers and checksums. As with RTS / CTS, use a trial and error process to set the threshold while keeping an eye on consequential throughput. If there is no appreciable RF interference, then it's best to deactivate fragmentation.

QUESTION 468:

What is the name of the area surrounding a transmitted RF beam after it leaves an antenna?

A. Inductance Zone
B. Fresnel Zone
C. Interference Zone
D. Diffraction Zone

Answer: B

Explanation:
In elevated ranges sometimes diffraction fences are used to further minimize the reflections from the ground. There are two cautions that should be emphasized. First, the diffraction fence should not intercept the main beam of the source antenna. Secondly, the top edge of the fence should not be straight knife edge, but rather serrated to reduce the edge diffraction.
Beyond the immediate neighborhood of the reactive field the radiating field begins to dominate. The extent of this region is $l/2^1 < r < 2D2/l$, where D is the largest dimension of the antenna. This region can be divided into two subregions. For $l/2^1 < r < D2/4l$ the fields decay more rapidly than 1/r and the radiation pattern (relative angular distribution of the field) is dependent on r.
For $D2/4l < r < 2D2/l$ the fields decay as 1/r, but the radiation pattern is dependent on r. The radiation pattern is equal to the Fourier transform of the aperture distribution with a phase error of more than 22.5º. The phase error is dependent on r (for r the phase error is equal to zero). This region is often referred to as the Fresnel zone, a terminology borrowed from optics

---

QUESTION 469:

Which of the following are disadvantages of a wireless LAN in comparison to a wired LAN? Select two.

A. Facility must be surveyed for radio frequency behavior
B. Packet analyzer cannot be used for troubleshooting
C. Corrupted frames cannot be retransmitted
D. Offers less throughput
E. Interoperability with other similar devices is not possible

Answer: B, D

QUESTION 470:

The measure of 0 dBm refers to what quality of power?

A. 1 mW
B. 10 mW
C. 100 mW
D. 1W

Answer: A

Explanation:

For example, dBm refers to a reference power of one milliwatt. The following table lists some commonly used dB units and their reference levels and abbreviations.
Unit Reference
dBw 1 watt
dBm 1 milliwatt
dBu 0.775 volts*
dBV 1 volt
dBmV 1 millivolt
dBuV 1 microvolt
dBuV/m 1 microvolt/meter
dBSPL 2x10^-6 Newtons/meter squared

QUESTION 471:

Which link speeds are mandatory to meet IEEE 802.11a specifications?

A. 6, 12, 18 Mbps
B. 12, 18, 24 Mbps
C. 18, 24, 26 Mbps
D. 6, 12, 24 Mbps

Answer: D

Explanation:
Data Rates
802.11b supports data rates of 1, 2, 5.5, and 11 Mbps. 802.11a supports mandatory data rates of 6, 12, and 24 Mbps and optional data rates of 9, 18, 36, and 54 Mbps.

QUESTION 472:

The IEEE 802.11f draft specifies use of what protocol?

A. Point-to-point Security Protocol
B. Inter-Access Point Protocol
C. Transmit Power Control
D. Intermediate Frequency Protocol

Answer: B

Explanation:
The inter access point protocol (IAAP) and other proprietary methods are used to support roaming between different APs. Various studies have shown that handoff delays between different APs can be as high as 400 ms. The 802.1x additions to pre-authentication, as part of the 802.11i draft, and the AP roaming protocols, as part of the 802.11f draft, address methods to decrease handoff delays. Silicon vendors must provide support for these features as part of their MAC implementations in order to support VoIP mobility.

QUESTION 473:

Which of the following statements describe WEP? Select all that apply.

A. Use the DES encryption algorithm
B. Encrypts the Layer3 through Layer7 information
C. Encrypts the Layer 2 head & trailer of each frame
D. Uses the RC4 encryption algorithm
E. Encrypts frames between wireless and wired network computers

Answer: D

Explanation:
WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext.

QUESTION 474:

Which of the following is the longest Interframe Space?

A. PIFS
B. SIFS
C. DIFS
D. All Interframe Spaces are the same length

Answer: C

Explanation:
The DIFS is used in the CP and describes the duration of time in which the medium has to be idle before a station is allowed to send or decrement its backoff. DIFS is the longest interframe space and consequently has the lowest priority.

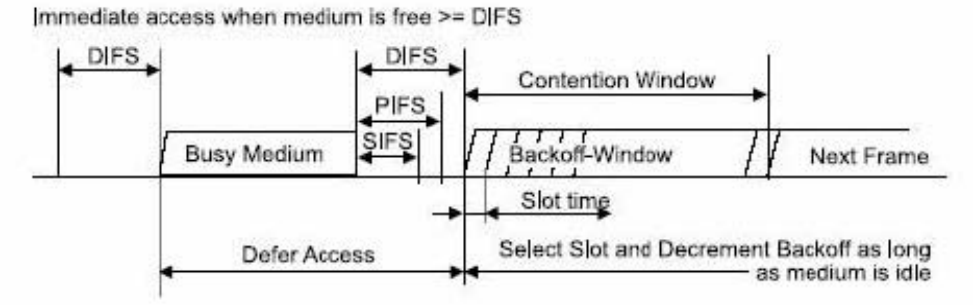


Figure 1.1: IFS relationships in IEEE802.11 (source: [3])

QUESTION 475:

Which of the following tasks are part of conducting a long-distance RF path survey? Select three.

A. Obtaining terrain elevation maps and aerial photos
B. Determining antenna heights
C. Documenting aircraft patterns in the area
D. Identifying possible reflections points
E. Listing the types of trees found between each end of the link

Answer: A, B, D

QUESTION 476:

What medium arbitration algorithm is used by wireless LANs?

A. CSMA/CD
B. Full-duplex
C. Spanning Tree
D. CSAM/CA

Answer: D
The MAC layer is a set of protocols which is responsible for maintaining order in the use of a shared medium. The 802.11 standard specifies a carrier sense multiple access with collision avoidance (CSMA/CA) protocol. In this protocol, when a node receives a packet to be transmitted, it first listens to ensure no other node is transmitting. If the channel is clear, it then transmits the packet.

QUESTION 477:

Which of the following security methods are NOT addressed within the 802.11 standard? Select three.

A. Per-packet authentication
B. User identification
C. Device identification
D. Device authentication
E. User authentication
F. Segmentation controls

Answer: B, E, F

QUESTION 478:

What characteristics determine the diameter of the first Fresnel Zone for a wireless LAN link?

A. Height of the antennas
B. Size of the antenna elements
C. Distance between the antennas
D. Frequency of the transmission
E. Transmission power
F. Antenna gain

Answer: CD

QUESTION 479:

In an environment with no RF interference, what factors influence the throughput of an IEEE 802.11a wireless LAN using a single access point?

A. Distance between the client and access point
B. Fresnel Zone circumference at the center of the wireless link
C. Air density and temperature of the immediate environment
D. The channel being used by the access point
E. Nearby satellite TV dishes in use
F. VLAN tags that are returned as a RADIUS attribute instead of statically tied to SSIDs
G. Use of frame fragmentation on the wireless medium

Answer: AG

QUESTION 480:

What conditions can prevent an 802.11g client device from roaming seamlessly between two access points that are part of the same wireless LAN system?

A. The new access point fails to receive the client's PMK as part of the reassociation process.
B. The role-based profile on the WLAN switch is preventing the client from using certain access points on the network.
C. One access point is 802.11b-compliant, and the other access point is 802.11g-compliant.
D. The client device and the access points have mismatched service set identifiers.
E. The client device and the enterprise wireless gateway have different IPSec preshared keys.
F. One access point has 802.11H frame translation enabled, and the other has RFC 1042 frame translation enabled.

Answer: ABD

QUESTION 481:

An 802.11b access point may control use of the RF medium for a specified period of time using which of the listed items?

A. Short Slot Times
B. Bacon Frames
C. RTS/CTS Protocol
D. CSMAIVD Protocol
E. CTS-to-Self Frames
F. DTIM Interval

Answer: BCE
For answer B.
See CWNA Official Study Guide, 3rd Edition, Page 333 (Beacons)
For answer C.
See CWNA Official Study Guide, 3rd Edition, Page 383 (RTS/CTS)
For answer E.
See CWNA Official Study Guide, 3rd Edition, Page 387 (CTS-to-Self)

QUESTION 482:

What weather conditions have a measurable impact on outdoor spread spectrum WLANs operating in the 2.4 GHz frequency range?

A. Bright Sunlight
B. Snow
C. Gamma Radiation
D. Air Stratification
E. Barometric Pressure

Answer: BD

QUESTION 483:

Given: Certkiller .com performs top-secret government contract work and has recently purchased an 802.11 Wireless Intrusion
Prevention System (WIPS) to enforce their "NO WIRELESS" network security policy.
What attacks are not recognized by 802.11 WIPS?

A. Deauthentication
B. MAC Spoofing
C. Protocol Jamming
D. Protocol Analysis
E. RF Jamming
F. FHSS Rogue APs

Answer: DF

QUESTION 484:

What word describes an RF signal that bounces off a smooth or coated surface and changes direction?

A. Diffraction
B. Reflection
C. Refraction
D. Diffusion
E. Scattering

Answer: B

QUESTION 485:

What causes an excessive Voltage Standing Wave Ratio (VSWR) in an 802.11a WLAN?

A. Mismatched impedance between devices in series with the main RF signal
B. Reflected DC current on the main RF signal line
C. Scattered RF signal along the main signal path
D. Inductance (crosstalk) between adjacent conductors

Answer: A

QUESTION 486:

What factors affect the propagation distance of an RF signal?

A. Antenna gain
B. Receiving station sensitivity
C. Fresnel zone blockage
D. Power over Ethernet (PoE) usage
E. Antenna polarization
F. Link budget calculations

Answer: AC

QUESTION 487:

As an RF wave propagates through space, the wave front experiences natural expansion. What is the negative effect of this expansion in a wireless LAN system?

A. Linear Diffusion Loss

B. RF signal Attenuation
C. Transmission Obfuscation
D. Fresnel Zone Thinning
E. Azimuth Inflation

Answer: B

QUESTION 488:

For multipath interference, what defines the time between the first signal received and when the last echoed signal is received?

A. Fade Margin
B. Reflection Deviation
C. Delay Spread
D. Echo Reference
E. Event Horizon

Answer: C

QUESTION 489:

Given: Return Loss is the decrease of forward energy ma system because some of the power is being reflected back toward the transmitter.
What can cause a high return loss in an RF transmission system?

A. A Voltage Standing Wave Ratio (VSWR) of 1.5:1
B. An impedance mismatch between devices in the CK system
C. Cross-polarization of the RF signal as it passes through the RF system
D. The use of multiple connector types in the RF system (e.g. N-type and SMA-type)
E. High output power at the transmitter and use of a low-gain antenna

Answer: B

QUESTION 490:

What phrase defines Equivalent Isotropically Radiated Power (EIRP)?

A. Transmitter output power plus attached cable and connector loss
B. Transmitter output power only
C. Power supplied to the antenna plus antenna gain
D. Power radiated by an amplifier due to an improper connection or seal
E. Power supplied to an RF antenna

Answer: C

QUESTION 491:

What scales can measure a calculable power quantity?

A. dB
B. dBm
C. dBi
D. mW
E. RSSI
F. dBd

Answer: BD

QUESTION 492:

What scales are used to measure relative changes in power levels?

A. dBm
B. dBi
C. dB
D. mW
E. dBW
F. RSSI

Answer: BC

QUESTION 493:

Given: A wireless LAN transmitter that emits a 100mW signal is connected to a cable with a 3 dB loss.
If the cable is connected to an antenna with a 10 dBi gain, what is the resultant EIRP at the antenna element?

A. 50mW
B. 250mW
C. 500mW
D. 750mW
E. 1000mW

Answer: C

QUESTION 494:

Given: A wireless LAN transmitter that emits an 80mW signal is connected to a cable with 6 dB loss. The cable is connected to an antenna with a 16 dBi gain.
What is the resultant antenna power output (EIRP)?

A. 160mW
B. 320mW
C. 800mW
D. 1200mW
E. 1600mW

Answer: C

QUESTION 495:

In a long-distance RF link, what statement about Fade Margin is true?

A. Fade Margin is the amount of signal strength in addition to the Link Budget.
B. The Fade Margin of a long-distance RF link does not account for antenna gain.
C. The Fade Margin is rarely taken into account on a long-distance RF link.
D. Fade Margin and System Operating Margin are synonymous, interchangeable terms.

Answer: A

QUESTION 496:

What factors are required to establish a high quality 2.4 GHz point-to-point RF link at a distance of 5 miles (8 kilometers)?

A. Accurate Link Budget calculations
B. Accurate Earth Bulge calculations
C. System Operating Margin (SOM) of at least 30 dB
D. A minimum antenna gain of 12 dBi
F. A Fresnel Zone that is at least 60% clear of obstructions
F. Use of a parabolic dish or grid antenna

Answer: AE

QUESTION 497:

What phrase describes the effect from a propagated RF wave that increases the distance the wave travels when the RF antenna lobe is focused in a desired direction?

A. Polar Extension
B. Active Amplification
C. B cam Compression
D. Passive Gain
E. Phased Array Propagation

Answer: D

QUESTION 498:

What characteristic increases as the gain of an antenna is increased?

A. Beamwidth
B. Range
C. Dissipated heat
D. Polarization radius
E. Fresnel Zone

Answer: B

QUESTION 499:

What determines the orientation of an RF wave as it leaves the antenna element?

A. Propagation Pitch
B. Polarization
C. Wave Front Trajectory
D. Signal Focus Angle
E. Acclimatization

Answer: B

QUESTION 500:

What statements are true concerning the wavelength of an RF signal?

A. Reflected RF signals that are greater than 1800 out of phase with the main RF signal have different wavelengths.
B. The wavelength can only be calculated if the amplitude and phase of the RF signal are l2own.
C. The antenna element must have an exact length of one wavelength to transmit or receive an RF signal of a given frequency.
D. The wavelength is 300 meters per sec / frequency in MHz.
E. The wavelength of an RF signal can be measured from crest to crest between waves.

Answer: DE

QUESTION 501:

What statements about the beamwidth of an RF antenna are true?

A. The higher the gain of an antenna, the more narrow the beamwidth is, both horizontally and vertically.

B. The RF signal stops propagating at the beamwidth borders.
C. Beamwidth is calculated by the -3 dB points from the center axis, both horizontally and vertically.
D. Horizontal beamwidth is displayed (in degrees) on the antenna Elevation Chart.
E. Beamwidth is calculated by the wavelength points from the center axis, both horizontally and vertically.
F. Vertical beamwidth is displayed (in degrees) on the antenna Azimuth Chart.

Answer: AC

QUESTION 502:

Given: Certkiller .com is a Wireless Internet Service Provider that provides wireless access to neighborhoods around their hometown.
They have installed towers with sectorized omnidirectional antenna arrays using 90° of horizontal beamwidth per sector.
What is the next step in configuring the antenna array?

A. Calculating the System Operating Margin (SOM).
B. Configuring the down tilt of each antenna in the array.
C. Providing DC power to each antenna in the array.
D. Calculating the Fresnel Zone clearance.

Answer: B

QUESTION 503:

What are some common specifications for 802.11 WLAN antennas'?

A. Spectral Purity Rating
B. Frequency Range in MHz
C. Impedance in Ohms
D. VSWR Rating
E. Output Power in EIRP
F. Return Loss Rating
G. Polarization

Answer: BCDG

QUESTION 504:

Compared to an omni-directional antenna, what attribute is higher for an antenna with narrow beamwidths?

A. Down Tilt Angle
B. Linearization Factor

C. Noise Reception
D. Gain
E. Diffraction

Answer: D

QUESTION 505:

What antenna technologies are used to help eliminate null areas of RF coverage within a facility?

A. Antenna Diversity
B. Phase Dispersion
C. Circular Polarization
D. Beam Linearization
E. Multiple Input/Multiple Output
F. Spectral Clarification

Answer: AE

QUESTION 506:

What is the most common mount type for installing a wireless LAN antenna to an outdoor mast (pole)?

A. Suction cups with threaded posts
B. Perforated radome enclosure
C. Magnetic mount with bulkhead adapter
D. U-bolt with base clamp
E. Tilt-n-swivel universal mount with ratchet adjustment

Answer: D

QUESTION 507:

What are the valid types of lightning arrestors used with 802.11 wireless LAN?

A. Coaxial arrestor with a metal oxide varistor (MOV) input circuit
B. Tuned quarter-wave stub arrestor
C. Coaxial arrestor with a gas discharge tube
D. Inductor-based bond-sensing arrestor
E. Parallel tuned tank-circuit arrestor

Answer: BC

QUESTION 508:

Lightning arrestors protect wireless LANs from what type of power fluctuation?

A. Severe Voltage Sag (Brownout)
B. In-line DC Voltage Spikes
C. Induced High-Frequency AC Current
D. Direct Lightning Strikes

Answer: C

QUESTION 509:

Given: Certkiller .com is experiencing connectivity problems with their existing building-to-building bridge link. A brick wall on the roof of one building is partially blocking the Fresnel Zone, and the connection is dropping many frames. The administrator moves the antenna to an area not obstructed by the brick wall, and then realizes the RF cable cannot reach the new location.
If an RF extension cables used, what are the likely results?

A. The data throughput rate will increase because VSWR will decrease.
B. The Equivalent Isotropically Radiated Power (EIFP) will decrease.
C. The antenna coverage area will decrease.
D. The return loss will increase unless the impedance of the RF extension cable is equal to 50% of the antenna impedance.
E. The likelihood of a direct lightning strike will increase, placing the entire WLAN system at risk.

Answer: B,C

QUESTION 510:

What statements describe the RF cables and connectors that are used with 802.11 WLAN equipment?

A. The connector type (e.g. N-type, SMA, or RP-TNC) determines the amount of insertion loss caused by the connector
B. Cable quality affects the amount of VSWR and return loss in the signal path.
C. Two similar connectors, manufactured by different companies, may vary in their specifications.
D. The highest quality RF cables cause no loss.
E. Increasing the frequency rating of an RF cable creates less spurious RF emissions and enhances network security.

Answer: BC

QUESTION 511:

According to the IEEE 802.11-1999 (R2003) standard, what are the lowest and highest frequency centers used by FHSS in North
Americaand Europe(excluding Spainand France)?

A. 2.4000 - 2.4835 MHz
B. 2.402-2.480 GHz
C. 2.4000 - 2.5000 GHz
D. 2.401-2.483 GHz
E. 2.401 - 2.478 GHz

Answer: B

QUESTION 512:

In 802.11a WLANs, what statements are true concerning the use of Orthogonal Frequency Division Multiplexing (OFDM)?

A. Six (6) "pilot" sub-carriers are used as a reference to disregard frequency and phase shifts of the signal during transmission.
B. OFDM transmissions in the lower U-NII band are limited to 40 mW.
C. 16QAM modulation is used at the 54 Mbps data rate.
D. The OFDM PHY is divided into two sub-layers, the LLC and PLCP.
E. Forty-eight (48) sub-carriers are used as parallel symbol transmission paths.

Answer: BE

QUESTION 513:

I an IEEE 802.11b wireless LAN system, what modulation type is used for 11 Mbps DSSS transmission?

A. Barker Code
B. DBSPK
C. DQPSK
D. 4GFSK
E. CCK
F. 16QAM

Answer: C

Explanation: See CWNA Official Study Guide, 3rd Edition, Page 195 for DQPSK and Page 196 for Encoding vs. Modulation discussion.
Not CCK: CCK is a spreading code not the modulation. CCK is a method of encoding.

QUESTION 514:

According to the IEEE 802.11b amendment, what modulation types are used when transmitting data frames using DSSS technology? Select all that apply.

A. OFDM
B. 4GFSK
C. BPSK
D. 16QAM
E. QPSK
F. 64QAM
G. CCK

Answer: CE
Not CCK: CCK is a Spreading code not a modulation Technology

QUESTION 515:

What factors influence the application layer throughput of an 802.11g client on an IEEE 802.11g wireless LAN?

A. Number of simultaneous 802.11g clients using the same access point
B. Antenna height of the access point
C. Use of VPN tunnels across the wireless LAN by the 802.11g client.
D. Roaming handoff speed between access points
E. Use of integrated antennas (versus detachable antennas) on the 802.11g client
F. Association of an 802.11b client to the same 802.11g access point as the 802.11g client

Answer: ACF

QUESTION 516:

How many DSSS channels are specified by the 802.11 standard, without reference to a specific regulatory domain?

A. 1
B. 11
C. 12
D. 14

Answer: D

QUESTION 517:

The 802.11-1999 (R2003) standard, excluding amendments, requires how much separation

between the center frequencies of non-overlapping DSSS channels?

A. 20 MHz
B. 25 MHz
C. 28 MHz
D. 30 MHz

Answer: D

QUESTION 518:

In an 802.11g ERP-OFDM system, what channel pairs are considered non-overlapping?

A. Channels 4 and 10
B. Channels 2 and 6
C. Channels 3 and 7
D. Channels 1 and 9
E. Channels 9 and 11
F. Channels 4 and 8

Answer: AD

QUESTION 519:

Given: A company has several stations connected to a single radio access point, and all stations are actively transmitting and receiving in the BSS.
What factors affect the amount of wireless bandwidth available to each station?

A. Number of actively transmitting stations associated to the access point
B. Beacon interval value configured in the access point
C. Co4ocated access points on non-overlapping channels
D. Fragmentation threshold settings on each station
E. Distance from the access point to the most distant station
F. The layer 3 protocol used by each station to transmit data over the wireless link

Answer: ADE

QUESTION 520:

How far apart are the center frequencies of the channels of an 802.11a wireless LAN system operating on the middle U-NII band (5.25 -5.35 GHz)?

A. 10 MHz
B. 15 MHz
C. 20 MHz
D. 22 MHz

E. 30 MHz

Answer: C

QUESTION 521:

In the 802.11g amendment, how much separation is required between the center frequencies of non-overlapping ERP channels?

A. 10 MHz
B. 11 MHz
C. 20 MHz
D. 22 MHz
E. 25 MHz
F. 30 MHZ

Answer: E

QUESTION 522:

The IEEE 802.11-1999 (R2003) standard and the 802.11b and 802.11g amendments specify the use of DSSS and OFDM spread spectrum technology for data transmission within the 2.4 GHz ISM band in accordance with regulatory agency requirements of the FCC (US), IC (Canada), and ETSI (Europe). What is the specified frequency range for data transmission within the 24 GHz ISM hand?

A. 2.4000 - 2.5000 GHz
B. 2.4010 - 2.4750 GHz
C. 2.4000 - 2.4725 GHz
D. 2.4000 - 2.4835 GHz
E. 2.4020 - 2.4950 GHz

Answer: D

QUESTION 523:

What IEEE document specifies a methodology for seamless roaming between access points?

A. 802.11j
B. 802.11d
C. 802.11f
D. 802.11s
E. 802 11n

Answer: C

QUESTION 524:

What frame types for wireless LAN transmissions are specified in the IEEE 802.11-1999 (R2003) standard and its amendments?

A. Null Data
B. Data + ACK
C. DTIM
D. QoS Data
E. Authentication
F. Data + CF-End

Answer: ADE
Note: We are not to sure how valid this question is. There are 3 main frame types: control, management, and data with several sub-types.
See CWNA Official Study Guide, 3rd Edition, Page 365 (Wireless Frame Types)

QUESTION 525:

What device feature is user configurable for 802.11i-compliant wireless LAN client devices?

A. 802.11Q Tagging
B. SNMP Community Strings
C. TKIP Configuration Parameters
D. RADIUS Server P Port
E. EAP Authentication Type

Answer: E

QUESTION 526:

What Physical Layer (PHY) specifications are addressed by the IEEE 802.11-1999 (R2003) standard?

A. FHSS
B. OFDM
C. ERP-PBCC
D. DSSS-OFDM
E. EFP-OFDM
F. DSSS

Answer: AF

QUESTION 527:

What phrases are defined by the IEEE 802.11h amendment?

A. Mobile IP Implementation
B. Inter-Access Point Protocol
C. Client Station Tracking
D. Transmit Power Control
E. Mesh Network Connectivity
F. Dynamic Frequency Selection

Answer: DF

QUESTION 528:

What OSI model layers are specifically addressed by the IEEE 802.11-1999 (R2003) standard?

A. Physical
B. MAC
C. Network
D. Transport
E. LLC
F. Application

Answer: AB

QUESTION 529:

What feature is specifically addressed in the IEEE 802.11g amendment?

A. Asynchronous and Time-Bounded Delivery Service Support
B. CSMA/CD and RTS/CTS Protocol Support
C. ERP-PBCC Modulation Support
D. VPN Tunnel and RADIUS Authentication Support
E. 802.1X/EAP Support

Answer: C

QUESTION 530:

What statements about deauthentication in 802.11 wireless LANs are true?

A. The deauthentication service may be invoked by a station or access point.
B. An access point may refuse deauthentication flames sent by a station.
C. Deauthentication is a notification, not a request.

D. Deauthentication flumes have an encrypted payload.
E. Only access points may issue deauthentication frames.

Answer: AC

QUESTION 531:

What steps are part of the 802.11 reassociation process?

A. A client station transmits a Reassociation Request frame to its current access point
B. The access point informs the Integration Service of the reassociation.
C. The access point invokes the Reassociation Service to initiate reassociation with the client station.
D. An access point transmits a Reassociation Response frame to a client station with a status value
E. The Reassociation Service informs the Distribution System that an association is moving

Answer: DE

QUESTION 532:

Given: An 802.11i-compliant wireless client station wants to seamlessly roam between 802.11i-compliantaccess points. The client station and all access points are part of a Robust Security Network (RSN). The client station is running a VoIP application that is latency sensitive.
In orderfor the client station to seamlessly and quickly roam between access points, what values must be passed from the client station to the new access point in a Reassociation Request frame?

A. The IP subnet information
B. The MSDU fragmentation threshold values
C. The client station's configuration profile name
D. The Pair wise Master Key Identifier
E. The wireless VLAN tag parameters
F. The old access point MAC address

Answer: DF

QUESTION 533:

What statements about the Service Set Identifier (SSID) are true?

A. The SSID is a special security identifier used only in 802.11i-compliant sessions.
B. The SSID is a common network name for the devices in a wireless LAN system.
C. The SSID is a number used for identifying the device's manufacturer.

D. The SSID is an arbitrary number assigned to each AP by each wireless client for roaming purposes only.
E. The SSID is an alphanumeric information field having a value of 0 - 32 octets.

Answer: BE

QUESTION 534:

According to the IEEE 802.11-l999 (R2003) standard, what features are required for an Independent Basic Service Set (IBSS)?

A. A self-contained network architecture
B. An access point as the focal point of communication
C. Wired connectivity to a Basic Service Set (BSS)
D. No Distribution System access available
E. Logical integration service function
F. The presence of one or more portal entities

Answer: AD

QUESTION 535:

What wireless LAN type implements power management using stations to participate in transmitting beacons after they awake from dozing?

A. Integrated Service Set (ISS)
B. Basic Service Set (BSS)
C. Ad Hoc PSP Mode Set (APMS)
D. Extended Service Set (ESS)
E. Dynamic Power Save Set (DPSS)
F. Independent Basic Service Set (IBSS)

Answer: F

QUESTION 536:

What is the BSSID for an infrastructure mode 802.11 wireless LAN?

A. A randomly generated MAC address used for uniquely identifying a BSS
B. The MAC address of the 802.11 radio in the access point
C. The network name
D. The identifier used to allow client stations to roam between multiple access points

Answer: B

QUESTION 537:

Given: A station has been operating in IEEE 802.11 -compliant Power-Save mode, and awakens from a low-power state (ding) just before a beacon is transmitted.The station detects the bit corresponding to its AD is set in the TIM.
This station must remain awake until one of two processes is completed. What are the two processes?

A. The station completes a flame exchange, and the access point sends a beacon containing a DTIM.
B. The access point clears all AID bits and transmits all buffered broadcast frames.
C. The station receives a response back from the AP to its PS-Poll frame.
D. The station receives a beacon with a TIM that indicates the AP does not have any buffered frames for this station.
E. The access point receives a CF-Poll Response frame from the station.

Answer: CD

QUESTION 538:

Given: Unicast data frames are queued at the access point for a dozing station that is operating in IEEE 802.11-compliant Power-Save mode.
What actions are required for the station to receive the queued frames?

A. The AP transmits information about stations that have queued frames in its beacons.
B. The AP retransmits the first queued data frame at a pre-determined interval until the station receives it and sends an acknowledgement.
C. Stations request their queued frames from the access point using a PS-Poll frame.
D. Stations awake at a predetermined time.
E. The AP transmits a multicast ATIM to all stations with queued unicast data to wake them up.
F. Stations send a PS-Poll frame to the AP with the DTIM bit set to 1.

Answer: ACD

QUESTION 539:

As specified in the IEEE 802.11-1999 (R2003) standard, what is the largest payload (MSDU) that maybe carried by the MAC frame?

A. 1492 bytes
B. 1500 bytes
C. 1508 bytes
D. 2304 bytes
E. 2346 bytes
F. 2358 bytes

Answer: D

QUESTION 540:

How many MAC address fields can be supported by the 802.11 MAC data frame?

A. 2
B. 3
C. 4
D. 5

Answer: C

QUESTION 541:

Given: An 802.11-compliant wireless client may use certain criteria to select the best access point.
What are the criteria?

A. Received Signal Strength Indicator value
B. Physical distance to the closest access point
C. Prioritized RF positioning information from each access point
D. Round trip time of a link test packet
E. Signal-to-Noise Ratio value
F. Relative position of narrow band RF interference sources

Answer: AE

QUESTION 542:

What information is passed in the beacon management frames of an 802.11g access point to nearby 802.11b wireless stations?

A. Time Synchronization information
B. Encrypted Data
C. Capability Information of the access point
D. Spread Spectrum Parameter Set information
E. Announcement Traffic Indication Messages
F. Doze state of all associated stations
G. VLAN Identifiers

Answer: ACD

QUESTION 543:

What is required for maintaining time synchronization in a FHSS wireless LAN?

A. Stations use authentication frames for verifying the internal clock time.
B. When receiving beacon frames, stations check and correct their clocks using the timestamp included in the frames.
C. Access points synchronize time information from an external time-source using NTP.
D. A continuous heartbeat frame (used specifically for time synchronization) is sent from access points to associated stations.

Answer: B

QUESTION 544:

Given: An IEEE 802.11g-compliant access point is not specifically programmed to oppose the IEEE 802.11-1 999 (R2003) standard implementation.
When is the access point required by the standard to respond to Probe Request frames from nearby 802.11b stations?

A. When the Probe Request frames contain a matching 5511) value
B. When the access point is configured for Open System authentication
C. When the Probe Request frames contain a null 5511) value
D. When the Probe Request frames contain all basic data rates specified by the access point
E. When the access point is operating in 802.11b-only mode

Answer: AC

QUESTION 545:

In an Infrastructure Basic Service Set (BSS), what paragraph best describes the Active Scanning process?

A. Access points broadcast beacons on all channels on each radio within the regulatory domain.
Nearby stations record information found in the beacons for use in the association process.
B. Access points broadcast beacons on a single channel on each radio for which they are programmed.
Nearby stations record information found in the beacons for use in the association process.
C. Stations broadcast beacons on all channels with in the regulatory domain.
Nearby stations record information found in the beacons for use in the association process.
D. Stations broadcast beacons on a single channel.
Nearby stations record information found in the beacons for use in the association process.

E. Stations broadcast probe request frames on all channels with in the regulatory domain.
Nearby access points respond with probe response flames. Stations record information found in the probe response frames for use in the association process.
F. Stations broadcast probe request frames on the single channel for which they are programmed.
Nearby access points respond on that channel with probe response frames. Stations record information found in the probe response frames for use in the association process.

Answer: E

QUESTION 546:

What Interframe Space is used in 802.11 DCF mode when the acknowledgement frame is not received by the transmitter of the previous unicast data frame?

A. PIFS
B. SIFS
C. DIFS
D. EIFS

Answer: D

QUESTION 547:

Inan 802.11b BSS, what prevents each station from using the full network bandwidth (11 Mbps) when multiple stations are actively transmitting and receiving within the BSS?

A. The queuing buffer memory size of the access point
B. The station's default fragmentation threshold value (2346 bytes)
C. The authentication mechanism in use by each station
D. The WLAN devices operate in a shared medium.
E. WLANs use the CSMA/CA protocol

Answer: DE

QUESTION 548:

What statement about 802.11a wireless LAN performance is true?

A. Smaller flame sizes result in greater throughput in a high RF interference environment.
B. Use of the maximum wireless frame size on the access point will increase throughput between the wired and wireless networks.
C. Changing the security mechanism from WEP-104 to WPA-Personal will increase

throughput.
D. Compared to an Independent BSS, an Infrastructure BSS can provide almost twice the throughput between wireless nodes.

Answer: A

QUESTION 549:

Given: A station and an access point are operating in Point Coordination Function (PCF) mode.
While operating in a Contention-Free Period (CFP), what statement is true?

A. CSMA/CA is used by the access point during polling to avoid collisions with stations in the same BSS.
B. Pollable stations contend for the medium to transmit broadcast and multicast traffic.
C. Latency-sensitive data (e.g. voice and video) can be given a higher priority than during the Contention Period (CP).
D. MAC flame overhead is decreased because pollable stations use smaller MAC headers.
E. Frame fragmentation by stations is prohibited by the 802.11 standard.

Answer: C

QUESTION 550:

Within what IEEE 802.11 mode do Independent Basic Service Sets always operate?

A. CSMA/CD Mode
B. Open System Mode
C. Extended Service Set Mode
D. Distributed Coordination Function Mode
E. Power Save Mode

Answer: D

QUESTION 551:

What statements about Point Coordination Function (PCF) in a BSS are true?
Select all that apply.

A. When polled by the Point Coordinator, client stations may send multiple data frames across the RF medium.
B. Client stations must be CF-pollable to operate in a Point-Coordinated BSS.
C. The Point Coordinator may reside in the AP for an Infrastructure BSS or ma non-AP station for an Independent BSS.

D. When a client station transmits a data frame that goes unacknowledged, the client station may retransmit the data frame during the next CP.
E. The Point Coordinator may retransmit an unacknowledged data flame after a PIFS time.

Answer: B,D,E
See ANSI/IEEE Std 802.11, 1999 Edition (R2003)-----(9.3 PCF)

QUESTION 552:

Given: The EEE 802.11e amendment calls for Quality of Service (Q0S) enhancements to the IEEE 802.11 standard.
What statements about the QoS enhancements are true?

A. New QoS data frame types are introduced both for PCF and DCF operation.
B. A new2-byteQoS Control field has been added to the MAC frame.
C. QoS-capable stations (QSTA5) may optionally choose to use AIFS when non-QSTAs are present in the BSS.
D. New QoS control frame types are introduced for DCF operation.
E. Eight (8) user priorities map to eight (8) transmit queues

Answer: AB

QUESTION 553:

Given: The IEEE 802.11g amendment requires use of slot times as part of the contention backoff procedure.
What statements about 802.11g slot times are true?

A. When the ERP-OFDM modulation is in use, the SIFS and slot time are always equal.
B. When HR/DSSS is in use, a slot time consists of a 5 ms Rx-to-Tx turnaround time and a 15 ms energy detect time.
C. All interframe spaces are calculated based on the slot time value.
D. The optional 9 ms slot time may not be used if the network has one or more associated non-ERP stations.
E. When the ERP DSSS-OFDM modulation is in use, all stations may use the 9 ms slot time.

Answer: BD

QUESTION 554:

Given: Certkiller .com has decided to install an 802.lla/g wireless LAN to support 250 wireless users, but they are concerned about network security. They have decided to implement three mandatory security mechanisms: 1) Role-Based Policy Enforcement, 2) 802.1X/EAP-TTLS, and 3) Bandwidth Management.

What devices will meet the security goals?

A. Enterprise Encryption Gateway
B. Wireless Intrusion Prevention System
C. Wireless LAN Switch
D. Enterprise Wireless Gateway
E. Wireless Mesh Router System
F. Residential Wireless Gateway

Answer: C,D

QUESTION 555:

What is one advantage of using Enterprise Encryption Gateways (EEGs) in large enterprise environments?

A. The network design is simpler because EEGs do not present a routed (layer-3) boundary at the network's distribution layer.
B. An AAA server is not needed because EEGs do not require authentication of wireless client devices.
C. A centralized controller is not needed because EEG s coordinate client session handoffs among themselves.
D. EEGs remove the decision of roaming from the wireless client stations making the roaming process faster. This helps boost the performance of applications such as VoIP.
E. EEG client software is 802.1X-enabled allowing the EEG to act as the supplicant in forming an EAP connection with enterprise-class access points or WLAN switches.

Answer: A

QUESTION 556:

Given: Wireless LAN switches (also called WLAN controllers) use "thin" access points. Compared to "thick" (also called "fat") access points, what are the advantages of thin access points in an enterprise environment?

A. Thin APs require less power to operate and extend the maximum distance for using 802.3af to power the AP.
B. In case of theft, a thin AP contains no useable information.
C. Thin APs allow secure management of the wireless network infrastructure over the wireless medium.
D. Thin access points reduce costs by only containing a minimal hardware configuration.
E. Thin access points natively support layer-3 roaming by building a tunnel to the controller during boot up.

Answer: BD

QUESTION 557:

What network protocols are commonly supported by EnterpriseWireless Gateway devices? Select all that apply.

A. Virtual Router Redundancy Protocol (VRRP)
B. Network Address Port Translation (NAPT)
C. Gateway Load Balancing Protocol (GLBP)
D. Role Based Access Control (RBAC)
E. Hot Standby Router Protocol (HSRP)
F. Point-to-Point Tunneling Protocol (PPTP)
G. Light Weight Access Point Protocol (LWAPP)

Answer: BDF

QUESTION 558:

What statements about the 802.11af-2003 amendment to the IEEE 802.3-2002 standard are true? Choose all that apply.

A. If a dial-radio access point requires 11 W to operate, an 802.3af-compliant end-span switch allocates 15.4 W to the powered interface.
B. 802.3af-compliant end-span and mid-span PSE devices support l0/l00/l000Base-T data rates.
C. Class 4 powered devices may use a maximum of 15.4W of power.
D. End-span 802.3af-compliant Ethernet switches must simultaneously support class 3 powered devices on every powered interface.
E. 802.3af-compliant end-span PSE devices may source power of 44 -57 VDC on the active data wires or the spare copper pairs.

Answer: A,B,E
Reference: http://www.ieee802.org/3/af/PAR-802-3af.pdf

QUESTION 559:

Given: Certkiller .com is opening a new branch office that needs an 80211 WLAN to support a mission-critical application.
The IT manager has considered implementing a remote office WLAN switch with "thin" access points instead of several independent "fat" access points. He has asked you, the Senior Network Engineer, about the primary differences between the two solutions. What statements define characteristics of WLAN switches?

A. WLAN switches automatically eliminate problems with co-channel and adjacent channel interference because the intelligence is in a single device.

B. The Inter Access Point Protocol (IAPP) allows thin access points from one vendor to be used with WLAN switches from another vendor
C. Thin access points download their firmware and configuration from the WLAN switch upon initialization, thus reducing management overhead.
D. Thin and fat access points support 802.3af Power over Ethernet (PoE), and some thin access points support dual, redundant PoE ports.
E. WLAN switches and fat access points support a wide variety of authentication and encryption parameters. If a WLAN switch is used, all attached thin access points must use the same security parameters.
F. Fat access points can be plugged into edge switches of any kind, but thin access points must be plugged directly into the WLAN switch.

Answer: CD

QUESTION 560:

What are some common components of 802.11b wireless LAN client utilities?

A. Site Survey Utility
B. Signal Strength Meter
C. Protocol Analyzer Utility
D. Access Control List (ACL) Configuration
E. Power Management Mode State Monitor
F. Profile Configuration Tool
G. Real-time Throughput Monitor

Answer: ABF

QUESTION 561:

What components maybe included with 802.11a/g wireless LAN client utilities?

A. PHY Layer Selection Tool
B. Connection Speed Indicator
C. Spectrum Analyzer Tool
D. Link Statistics Monitor
E. QoS Access Category Selector
F. Frequency Band Support Selector
G. Authentication/Encryption Selection Tool

Answer: BDFG

QUESTION 562:

Given: Certkiller .com is a small educational establishment that is beginning to realize last growth. Until now, each department had its own snail building and

servers. Students connected to the departmental servers via Ethernet switches.
Certkiller has recently built a data center in building 100 and wants to connect six other buildings to building 100 using the fastest available 802.11 technology. The primary goal of the network design is to increase throughput between building 100 and the other buildings.
As a consultant, how would you design the wireless network?

A. Place one 802.11g bridge with an omni-directional antenna on building 100 and place one 802.11g bridge with a patch antenna pointing to building 100 on all other buildings.
B. Place three 802.11a bridges using sector antennas on building 100 and place one 802.11a bridge with a patch antenna pointing to building 100 on all other buildings.
C. Place an 802.11a/g dual-radio access point with omni-directional antennas on building 100 and let students directly connect to the AP from their laptops.
D. Place an 802.11g mesh router on each building.

Answer: B

QUESTION 563:

What are possible causes of the "hidden node" problem with 802.11 WLANS?

A. Data frames are too large for the physical environment
B. Client stations broadcasting with too much power
C. Access points broadcasting with too little power
D. Client stations are too dose in proximity
E. Interfering obstacles between client stations

Answer: E

QUESTION 564:

What describes the effects of narrowband RF interference on 802.11g WLANs?

A. Narrowband RF interference will often have a higher peak amplitude than the 802.11g channel, causing a throughput reduction.
B. If narrow band RF interference occupies the same frequency space as the 802.11g WLAN, the WLAN will become inoperative.
C. Narrow band RF interference may appear on a spectrum analyzer as a similar-shaped adjacent channel to an 802.11g WLAN.
D. The harmonics of the interfering narrow-band RF signal can decrease spectral distortion in the 802.11g WLAN.

Answer: A

QUESTION 565:

Given: An 802.11a RF signal reaches a receiving antenna by direct and indirect (reflected) paths.
What effect could the reflected 802.11a signal have on the RF signal that took the direct line-of-sight path?

A. The direct signal is amplified. The amplification results in a signal that is stronger at the receiving antenna than was originally transmitted.
B. The direct signal will not be received if the indirect signal is greater than 90° out-of-phase.
C. Adjacent channel interference occurs. The interference creates distortion of the signal, rendering it corrupt and unreadable.
D. The direct signal nay be attenuated and distorted if the indirect signal arrives at the receiver 90° out-of-phase.
E. Co-channel interference occurs. The interference causes attenuation and phase inversion of the direct signal.

Answer: D

QUESTION 566:

What phrase refers to the level of interference that an RF system is able to accept and still maintain a specified level of performance (e.g. maintaining a specified bit-error ratio when the signal-to-noise ratio is decreasing)?

A. EMF Stability
B. Distortion Pad
C. Jamming Margin
D. Squelch Buffer
E. Demarcation Ratio

Answer: C

QUESTION 567:

Given: Co-located 802.11b access points can experience adjacent channel interference and ensuing throughput degradation when operating on non-overlapping channels.
What can cause this condition to occur?

A. The access points are too close in proximity.
B. Reflective objects in the area are causing significant multipath.
C. A client station is using active scanning to probe for access points on multiple channels.
D. The output power on each access point is too high.
E. A client station pre-authenticates to multiple access points in the area.
F. The antenna gain on the access point is too high.

Answer: ADF

QUESTION 568:

Given: The enhanced confidentiality, data authentication, and replay protection mechanisms of the 802.11i-2004 amendment require fresh cryptographic keys.
What wireless protocols are compatible with the requirement of the 802.11i-2004 amendment to provide fresh cryptographic keys?

A. 4-Way Handshake
B. EAPoL Handshake
C. Group Handshake
D. 802. 1X/EAP Handshake
E. AES-CCMP Handshake
F. STAKey Handshake

Answer: AC

QUESTION 569:

What describes the AES-CCMP data protection mechanism implemented by the 802.11i-2004 amendment?

A. It uses the 256-bit Rijndael encryption algorithm to protect the MEDU Data field.
B. It protects the integrity of both the MPDU Data field and selected portions of the MPDU header.
C. Support for CCMP using a 128-bit key is mandatory for Robust Security Network (RSN) compliance.
D. It uses either the RC4 stream cipher or 3DES block cipher to encrypt the MPDU Data field.
E. It uses a 192-bit encryption algorithm to protect authentication between the supplicant and authentication server.

Answer: BC

QUESTION 570:

Given: The 802.11i-2004 amendment specifies the use of 802.1X port-based access control and EAP authentication. The 802.lX-2004 standard specifies two Port Access Entities (PAEs), the authenticator and the supplicant, and also specifies a system role called the authentication server.
What network authentication services are suitable for operating in the system role of authentication server in an 802.11 wireless network?

A. LDAP

B. SQL
C. RADIUS
D. Diameter
E. SOAP/HTTP
F. Kerberos

Answer: CDF

QUESTION 571:

What security related problems are inherent in the 802.11-1999 (R2003) standard?

A. Specifies use of the SSID as a dynamic security mechanism
B. Integrated support for only one EAP type: EAP-MD5
C. Deauthentication frames are not authenticated
D. No authentication, authorization, or accounting (AAA) support
E. Integrated support for only one data encryption cipher: DES

Answer: CD

QUESTION 572:

The 802.11i-2004 amendment specifies mandatory support of the _____ cipher suite for Robust Security Network
Associations, and optional use of the _____ cipher suite, designed for use with pre-RSNA hardware.

A. CCKM, WPA
B. 802.1X/EAP, WEP
C. TLS, SSL
D. CCMP, TKIP
E. PMK, GMK

Answer: D

QUESTION 573:

Given: The IEEE 802.11-1999 (R2003) standard specifies a 4 byte initialization vector (IV) and a 4 byte Integrity Check Value (ICV) as part of WEP frame body expansion.The 802.11i-2004 amendment specifies an additional 8 byte message integrity check (MIC) called "Michael" and an additional 4 bytes of IV, bringing the total frame body expansion overhead to 20 bytes for TKIP.
The 802.11i-2004 amendment introduced a CCMP header of __and a MIC of_____ to replace both TKIP and WEP.
Select the answer option needed to fill in both blanks.

A. 8 bytes, 8 bytes
B. 8 bytes, 12 bytes
C. 8 bytes, 20 bytes
D. 12 bytes, 8 bytes
E. 12 bytes, 20 bytes

Answer: A

QUESTION 574:

Given: Certkiller .com has recently decided to purchase and install an 802.11a/gwireless LAN. The network administrator decides to purchase a wireless LAN switch because of its wide range of EAP support. Certkiller .com has no Public Key Infrastructure (PKI), but likes the EAP-TLS model of wireless security.
As a hired consultant you mention an EAP type that closely resembles the functionality of EAP-TLS, but does not use certificates.
What EAP type did you mention?

A. EAP-TTLS
B. EAP-MD5
C. EAP-PEAP
D. EAP-FAST
E. EAP-SIM

Answer: D

QUESTION 575:

What EAP types require the 802.1X authentication server to have an X.509 certificate installed?

A. EAP-TTLS
B. EAP-TLS
C. PEAP-MS-CHAPv2
D. EAP-SIM
E. EAP-FAST
F. EAP-GTC

Answer: ABC

QUESTION 576:

Given: Wired Ethernet LANs have always been susceptible to generic types of attack, and the security administrator must guard against such attacks. What unique security vulnerabilities are introduced with IEEE 802.1 1 wireless LANS?

A. Protocol Analysis
B. Spectral Analysis
C. Management Frame Injection
D. D Default Password Access
E. MAC Layer Protocol Exploits

Answer: C, E

QUESTION 577:

Using only a software access point, a narrowband RF jamming device, and a DHCP server application, what common wireless
LAN attacks can be successfully performed on inadequately secured wireless client stations?

A. Hijacking Attack
B. Man-in-the-middle Attack
C. Eavesdropping Attack
D. Encryption Cracking Attack
E. Management Interface Exploit Attack

Answer: A

QUESTION 578:

What network security protocols are supported on EnterpriseWireless Gateways and WLAN Switches?

A. IGMP/CGMP
B. L2TP/IPSec
C. PAgP/LACP
D. 802.1X/EAP-TLS
E. IFDP/GLBP
F. LACILNS

Answer: BD

QUESTION 579:

Given: Certkiller .com has implemented a high-capacity wireless LAN switch to enable all employees to be more productive.
The network administrator is having difficulty providing employees of each department access only to network resources to which they are specifically authorized.
What wireless LAN switch feature would allow the network administrator to accomplish this task?

A. Captive Portal
B. Resource Access Protocol
C. Role-based Firewall
D. Access Control Lists
E. IDS Signatures

Answer: C

QUESTION 580:

Given: Similar to an access point, the coverage area of a Wireless Intrusion Prevention System (WIPS) is called its Field of View (FOV).WIPS sensor site surveys are performed to determine the locations where sensors are best placed, based on sensor sensitivity, antenna gain, environmental blockage, AP density, and many other factors.
What are three standard FOV configurations?

A. Unauthorized Device Detection
B. All Trusted Traffic Monitoring
C. All Channel Throughput Monitoring
D. Trusted AP Monitoring
E. Known/Untrusted AP Monitoring
F. Trusted Client Monitoring

Answer: ABD

QUESTION 581:

Given: Network users at a large clothing manufacturer have been asking the network administrator to implement a wireless LAN.
The network administrator and the Chief Technology Officer (CTO) have called a meeting of several senior management personnel to discuss it. The first orderof discussion is corporate policy concerning implementation and use of wireless LAN technology.
What specific topics are appropriate in this policy meeting?

A. Security risks and audits
B. Government regulations
C. User productivity impact
D. Gathering information for the site survey
E. Permits and zoning requirements
F. Hardware recommendations

Answer: ACD

QUESTION 582:

Given: You are the network administrator for Certkiller .com. Your manager has recently attended a wireless security seminar. The seminar speaker insisted that a wireless network could be hidden from potential intruders if you disabled the broadcasting of the SSID in beacons and configured access points not to respond to probe request frames that have a null SSID field
Your manager asks your opinion about these security practices. How would you respond?

A. Any 802.11 protocol analyzer can see the SSID in clear text in frames other than beacons and probe response flames. This negates any benefit of trying to hide the SSID by configuring beacons and probe response frames.
B. These security practices prevent manufacturers' client utilities from seeing the SSID. This means that the SSID cannot be obtained, except through social engineering, guessing, or use of WIPS.
C. Broadcasting the SSID in beacons and allowing access points to respond to probe request frames with null SSID fields allows authorized users to easily find and connect to the wireless LAN, provided they have the correct security credentials. This decreases help desk calls.
D. Any tenants in the same building using a wireless intrusion protection system (WIPS) will be able to obtain the SSID by exploiting probe delay timers. This poses a security risk.
E. An additional security practice is equally crucial to hiding the wireless network's SSID: deauthentication frames. The access point and client stations must both be configured to remove the SSID from deauthentication frames.

Answer: AC

QUESTION 583:

Given: The network administrator at XYZ Company recently attended a training class on wireless security and realized that he still needs to update the corporate security policy to address wireless LAN technology (even though WLAN technology is not yet permitted on the network). The network administrator is trying to remember some of the items that should be addressed in the security policy update, and has asked you to help.
What topics would you suggest for the security policy update?

A. Physical security of wireless LAN infrastructure devices
B. Intrusion monitoring and response procedures
C. Adding RF jamming devices at the perimeter of the building
D. Limit wireless LAN cell size to only what is needed
E. Social engineering attacks
F. End-user and technical staff training

Answer: BF

QUESTION 584:

What statements determine the viability of long-distance outdoor 802.11b bridge 1ink?

A. Determining whether there are any 24 GHz signals that cross the RF path near the center of the Fresnel Zone.
B. Determining the effects on the natural environment between the antenna locations.
C. Determining whether there are any bodies of water between the antenna locations.
D. Determining distance from any nearby airports.
E. Determining the minimum antenna heights.
F. Determining proximity to, and effects on, emergency warning systems.

Answer: DE

QUESTION 585:

Given: Before performing a site survey for a hospital, the network manager notifies you that there is a connection-oriented, real-time medical application used across the hospital network. Because the application is real-time, it is sensitive to service disruptions and latency. For this reason, it is particularly important to locate sources of RF interference, blockage, and dead spots.
What can put the application at risk of time-outs?

A. High concentration of patients in an area
B. Long hallways
C. Elevator shafts
D. Metal mesh glass
E. Radiology room
F. Intercom system

Answer: CDE

QUESTION 586:

What items are essential for performing an RF site survey on a warehouse facility?

A. Facility floor plans showing wiring closet locations
B. Forklift for moving stored materials when necessary
C. High-gain antennas for use in penetrating chain link fences
D. Long category 5 cables for connecting access points to wiring closets
E. Lifts and ladders for mounting temporary access points

Answer: AE

QUESTION 587:

Given: You are an independent contractor, hired to perform a site survey for ABCHospital. You are interviewing the network manager to gather business and security

requirements for the future 802.11g wireless LAN. You want to clarify business requirements and achieve the expected performance, application support, and return on investment (ROI)
What questions should you ask the network manager?

A. Are there any occasions when an abnormally high number of WLAN users will be present?
B. Are there any applications that require full-duplex communication over the WLAN?
C. Will the WLAN management platform be distributed or centralized?
D. Are there any time-sensitive applications that will operate over the WLAN?
E. Are there any walkie-talkie handsets in use at the hospital that would conflict with the WLAN?

Answer: AD

QUESTION 588:

When performing an 802.11b site survey in a multi-tenant building with ten (10) floors, what two aspects should a Site Surveyor keep in mind?

A. All doors in the entire building should be open during the site survey.
B. The omni-directional antennas of the access points should be oriented parallel to the floor to maximize the coverage pattern across as many floors as possible.
C. The channel reuse pattern should be three dimensional with the RF cell extending coverage of each access point to only one floor above and one floor below.
D. The Fresnel Zone is completely blocked between floors so each floor is considered a separate site survey.
E. Placing access points directly above and below each other from floor-to-floor typically causes co-channel and/or adjacent channel interference.

Answer: CE

QUESTION 589:

Given: Certkiller .com is constructing a building-to-building 802.11g bridge link using patch antennas. The buildings are 4 blocks apart in the middle of a large city. Certkiller .com is using the rooftop of each building for antenna placement. There are several buildings closely spaced between the two locations, but there is a narrow visual line-of-sight. The link does not work as Certkiller .com had hoped.
What would you do to rectify this problem in the most cost-effective manner?

A. Change the antennas to high gain parabolic dish or grid antennas with a narrow beamwidth. This will sufficiently shrink the Fresnel Zone to an area where other buildings are not impeding.
B. Decrease the output power to the minimum allowed by the link budget calculation. This will minimize the size of the Fresnel Zone and increase the quality of the

wireless link.
C. Use a vertically-polarized antenna on one building and a horizontally-polarized antenna on the other to decrease the size of the Fresnel Zone. Cross-polarization will shrink the Fresnel Zone size while allowing the output power to remain the same.
D. On top of each building, place a mast or tower that is tall enough to completely clear the Fresnel Zone of obstructions between the two antennas.

Answer: D

QUESTION 590:

Given: A municipality has contracted you to perform a site survey to enable an 802.11g WLAN for the City Planning Department (CPD) located on the second floor of a commercial, multi-tenant building. The first floor contains a coffee shop while the third and fourth floors are leased by a law firm. Both the coffee shop and the law firm are using 802.11b access points.
The CPD planning engineers must be able to access their Geographical Information System (GIS) using the 802.11g WLAN. After performing a traffic study on the GIS over the existing wired LAN, you determine that a minimum data rate of 5.5Mbps will be required from all of the CPD common areas and from the coffee shop on the first floor.
During the site survey, what steps should you take to determine if the minimum data rate can be met?

A. At each proposed 802.11g AP location, use an 802.11 protocol analyzer to look for beacons from 802.11b APs.
B. At each proposed 802.11g AP location, enable an 802.11g AP and 802.11g client station. Associate the client station to the 802.11g AP, and then check the 802.11g client station data rate in use with the manufacturer utilities.
C. Temporarily install a distributed wireless intrusion prevention system (WIPS) throughout the CPD facility. At each proposed 802.11g AP location, place a WIPS sensor and then associate an 802.11g client station with the AP. Monitor the WIPS console for sudden drops in throughput
D. At each proposed 802.11g AP location, associate an 802.11g AP and client station. Use an 802.11 protocol analyzer to look for CTS flames sent by either the 802.11g AP or the 802.11g client station.
E. At each proposed location, enable an 802.11g AP. Associate an 802.1 lb client station with an 802.11b AP at the coffee shop. Monitor the connection with an 802.11 protocol analyzer, and look for RTS frames sent by the 802.11b station.

Answer: A,D

QUESTION 591:

Given: Certkiller .com is planning to install a new 802.11a/g wireless LAN, but wants to upgrade its wired infrastructure first to provide the best user experience possible.

Certkiller .com has hired you to perform the site survey. During the interview with the network manager, you are told that the new Ethernet edge switches will support VoIP phones and 802.11a/g access points, both using 802.3af compliant PoE
After hearing this information, what immediate concerns do you note?

A. VoIP phones and 802.11 access points should never be powered by the same edge switch.
B. Use of a networking protocol that assists in appropriating only necessary power to each PoE capable port would be beneficial.
C. VoIP phones can only be powered using PoE up to 50 meters while 802.11 access points can be powered using PoE up to 100 meters.
D. The power budget in the edge switches must be carefully planned and monitored.
E. The 802.3af standard does not specify the use of VoIP phones, so their voltage and pin outs are proprietary and incompatible with 802.3af compliant 802.11 access points.

Answer: B,D

QUESTION 592:

Given: Certkiller .com has hired you to perform a site survey on their facility.During an interview, the network manager informs you that the new wireless network must be 802.11a, and a VoIP application will be used extensively over the wireless network.
What elements should you include in the site survey report?

A. End-user roaming requirements
B. 802.1X/EAP type support requirements for each AP
C. Real-time application troubleshooting techniques
D. Per-user throughput requirements and AP capacity information
E. Best practice documents concerning health hazards for 802.11a VoIP phone use

Answer: AD

QUESTION 593:

Given: You are being interviewed by Certkiller .com for a possible position as a wireless site survey engineer. The interviewing manager asks you what items should be included in a typical RF site survey report.
What is your response?

A. Cost estimate of the WLAN equipment
B. RF coverage map for each 802.11 PHY considered
C. Detailed documentation on physical security hazards in the RF coverage area
D. A list of RF interference sources and a diagram of dead spots
E. Documentation on how each WLAN user group will authenticate to the network

Answer: BD

QUESTION 594:

What is the best method for documenting" dead spot' in an area covered by an indoor 802.11g wireless LAN?

A. Showing the dead spots to the network administration person.
B. Marking the dead spots with markers, flags, or other visible indicators.
C. Dead spots should not be recorded in a site survey report.
D. Marking the dead spots on a blueprint or floor plan.
E. Taking digital photographs of dead spots and give them to end users.

Answer: D

QUESTION 595:

What statements define the contents of a typical RF site survey report?

A. It is a series of notes taken during the interview with the network manager and given only to the site survey project manager.
B. It is a one-page network inspection summary, used to create a certificate of compliance.
C. It contains the results from the RF interference and coverage analysis.
D. It is an internal document used by the site surveying firm. It is not shared with the client.
E. It states the customer requirements and business justification for the wireless LAN.

Answer: CE

QUESTION 596:

Given: Certkiller .com has hired you, a wireless network consultant, to perform an indoor site survey of their 7-story facility.
Certkiller .com rents out unused space in their building to other companies, and the other companies use 802.11 WLANs already.
Certkiller .com wants all of the offices they occupy to be surveyed as part of the project.
What actions should be recommended as part of the site survey project?

A. Disabling fire alarms throughout the facility.
B. Interviewing the network and facility managers.
C. Obtaining floor plans of the facility.
D. Making a list of MAC addresses for all wireless network cards.
E. Procuring a mobile equipment cart.
F. Unlocking all wiring closet doors prior to the site survey.

Answer: BCE

QUESTION 597:

Given Your consulting firm recently completed a virtual site survey for Certkiller .com
Certkiller .com insists on a manual verification of the virtual site survey report.
Using site survey software operating in both passive and active modes, what tasks can be performed as part of the virtual site survey verification?

A. Quantitatively analyze sources of RF interference and noise
B. Identify client roaming patterns within the facility
C. Emulate client experience to measure connection speed, retry rate, and frame loss
D. Verify the optimal AP location suggestions
E. Validate authentication and encryption mechanisms used by each client station
F. Simultaneously capture and analyze data on each 802.11 channel to measure true system-wide throughput
G. Validate each access point is identically configured to allow for seamless roaming

Answer: ACD

QUESTION 598:

Which data rate is specified in the 802.11g amendment that is not specified in the 802.11a amendment to the IEEE 802.11-1999 (R2003) standard?

A. 2Mbps
B. 6 Mbps
C. 12 Mbps
D. 54 Mbps
E. Both amendments support the same data rates

Answer: A

QUESTION 599:

Devices compliant with the 802.11-1999 (R2003) standard (including all amendments) use which radio bands?

A. 902 - 928 MHz ISM band
B. 2.4000 - 4.4835 GHz ISM band
C. 5.470 - 5.725 GHz U-NII band
D. 5.15 - 5.25 GHz U-NII band
E. 5.725 - 5.875 GHz ISM band

Answer: B, D

QUESTION 600:

While working on a presentation document in a conference room equipped with a wireless network, you notice that, as you turn your laptop in different directions, your wireless signal strength changes. What RF signal property is primarily responsible for this change in signal strength?

A. The RF signal's amplitude is changing due to a change in the visual line-of-sight.
B. The RF signal's wavelength is being affected by varying antenna gain.
C. The RF signal's multipath is changing the amount of RF absorbed by nearby objects.
D. The RF signal's phase is oscillating due to electromagnetic interference (EMI).
E. The RF signal's polarization is different than the receiving antenna.

Answer: E

QUESTION 601:

You have been hired by Certkiller to troubleshoot their 802.11abgh-compliant, Wi-Fi-certified access point and wireless client devices. After completing a site survey,you identify five neighboring 802.11b access points belonging to Certkiller; one on channel 1, three on channel 6, and one on channel 11. To best avoid co-channel and adjacent channel interference, what suggested change is most appropriate?

A. Configure Certkiller 's access point to use channel 1, 802.11g OFDM-only mode, and to operate in PCF mode.
B. Configure Certkiller 's access point to use channel 3, 802.11g-standard mode, and to use the RTS/CTS protection mechanism all the time.
C. Configure Certkiller 's access point to use 802.11a with dynamic frequency selection (DFS).
D. There is no available configuration that would avoid co-channel or adjacent-channel inteference in this situation.

Answer: C

QUESTION 602:

What facts should you consider when choosing a spread spectrum technology for your wireless LAN network?

A. An 802.11b Direct Sequence Spread Spectrum (DSSS) signal offers higher data rates and is less susceptible to narrowband interference than an 802.11 Frequency Hopping Spread Spectrum system.
B. While 802.11g devices can use either DSSS or OFDM technology, 802.11a devices only support OFDM. Therefore 802.11g devices always use OFDM to communicate with

802.11a devices.
C. When 802.11b devices are present in an 802.11g BSS, the use of DSSS will diminish network throughput significantly over a purely OFDM environment.
D. An 802.11g system supporting only the data rates required by the 802.11g amendment can interoperate with 802.11b devices.
E. 802.11g systems use OFDM technology to obtain speeds equal to 802.11a systems and to communicate with 802.11b devices.

Answer: C,D

QUESTION 603:

When using 802.3af-compliant Power-over-Ethernet switches at the network edge, what situation has the potential to adversely affect the proper operation of your 802.3af-compliant access points?

A. A large number of 802.3af-compliant VoIP phones are attached to the same Ethernet switch.
B. Access points that do not support the 802.3af standard are attached to the same Ethernet switch.
C. The Ethernet switch's uplink ports are not connected to an 802.3af-compliant core or distribution Ethernet switch.
D. PoE is provided on both 10/100 and 1000BaseTx ports on the same Ethernet switch.

Answer: A

QUESTION 604:

What are valid IEEE 802.11-1999 (R2003) specifications regarding Direct Sequence Spread Spectrum (DSSS) technology?

A. Minimum transmit power should be no less than 0 dBm.
B. Power control should be provided for transmitted power greater than 1 Watt.
C. DSSS systems must be able to interoperate with FHSS systems at the same data rate.
D. The impedance level of the transmit antenna port(s) shall be 75 Ohms if the port is exposed.
E. A basic data rate and an enhanced data rate are specified for the 802.11 DSSS physical layer.

Answer: A,E

QUESTION 605:

Which wireless LAN device type can be implemented as part of the core or access network layers in an enterprise installation?

A. Wireless mesh router
B. Wireless access point
C. Wireless bridge
D. Wireless workgroup bridge
E. Wireless LAN switch
F. Enterprise encryption gateway

Answer: A

QUESTION 606:

What advantages does using predictive site survey modeling software offer over performing a traditional "manual" site survey?

A. Predictive modeling software can predict the ideal access point location more than 99% of the time.
B. Predictive modeling software makes it simple to try various access point's locations, updating an access point coverage pattern in real-time.
C. Predictive modeling software provides more reliable data than manual surveys when fine-tuning access point placement.
D. Interference sources from external networks can be more accurately measured when using predictive modeling software.
E. It takes less time to create a reasonably accurate initial site survey using predictive modeling software than when performing a manual survey.

Answer: B,E

QUESTION 607:

Given: You have been hired by Certkiller to implement an outdoor WLAN connection between two buildings that are 2 kilometers (1.24 miles) from each other. Your first required objective is to create a point-to-point link between the two buildings within FCC regulations. Your second required objective is to provide an industry-standard security solution capable of supporting mutual authentication. As an optional objective, you must protect your wireless bridges from environmental elements such as windblown dust, rain, and splashing water.
You install an 802.11b wireless bridge at each building, configuring one in root mode and the other in non-root mode. You set each radio for 1 watt (+30 dBm) and attach 9 dBi omni-directional antennas to both. Each wireless bridge is placed in a NEMA-compliant enclosure intended for outdoor use. You configure each bridge for 802.11i-compliant security features.
Which statement is true about the solution you chose to deploy?

A. Your solution meets both required objectives and the optional objective.
B. Your solution meets the first required objective and the optional objective, but not the second objective.

C. Your solution meets the second required objective and the optional objective, but not the first required objective.
D. Your solution meets neither required objective but meets the optional objective.
E. Your solution meets both required objectives, but does not meet the optional objective.
F. Your solution does not meet either required objective, or the optional objective.

Answer: C

QUESTION 608:

Which items are specified by or derived from the IEEE 802.11i wireless LAN security amendment?

A. CCMP / AES
B. WPA2-Enterprise
C. IP Security (IPSec)
D. 802.1X/EAP framework
E. Secure Shell

Answer: A,B,D

QUESTION 609:

Your organization has many client devices, some that support WEP, some that support WPA, and some that support WPA2. Those client devices that support only WEP are capable of being firmware upgraded to support the TKIP wireless security protocol. As the wireless administrator, you are required to provide the strongest industry standard layer-2 security possible while implementing a consistent solution for all devices. What security measures should you implement to meet your organization's requirements?

A. 802.1X/EAP authentication
B. TKIP/RC4 encryption
C. Shared Key authentication
D. CCMP/AES encryption
E. WEP-128 encryption with a passphrase
F. Transport Layer Security (TLS)

Answer: A,B

QUESTION 610:

The WPA/WPA2-Enterprise certification programs from the Wi-Fi Alliance include use of which Extensible Authentication Protocol (EAP) types?

A. EAP-TTLS

B. PEAPv0 / EAP-MSCHAPv2
C. EAP-TLS
D. EAP-FAST
E. EAP-MD5
F. LEAP
G. PEAPv1 / EAP-GTC

Answer: A,B,C,G

QUESTION 611:

During the information gathering phase of a site survey, it is important to gather and record information about radio frequency related interference and blockage sources, which result in reduced signal coverage. What type of building construction material introduces the least amount of RF signal loss?

A. Insulation-doped glass window
B. Wood-studded drywall
C. Concrete or brick wall
D. Aluminum siding
E. Chain-link fence

Answer: B

QUESTION 612:

Given: You have been hired by a local school to wirelessly connect a mobile classroom to the school's network infrastructure. You are considering placing a wireless workgroup bridge at the mobile classroom to make the wireless connection back to the main building in which the school's data center is located.
What must you consider before implementing a wireless workgroup bridge in this scenario?

A. You will need to connect a wireless bridge to the main building's network infrastructure to make the connection to the wireless workgroup bridge at the mobile classroom.
B. You will only be able to connect wired devices to the wireless workgroup bridge and not any wireless client devices in the mobile classroom.
C. If you connect the wireless workgroup bridge to an access point at the main building, the access point will not be able to provide connections to other wireless client devices during communication with the wireless workgroup bridge.
D. If you need to use security options such as MAC filtering, WEP, or WPA-Personal, you will need to use a dedicated wireless bridge at the mobile classroom instead of the wireless workgroup bridge.

Answer: B

QUESTION 613:

Regarding association and re-association processes, which statements describe 802.11-1999 (R2003) network operation?

A. When actively scanning for a network to join, clients transmit Probe Request frames, which contain most of the same information found in beacons.
B. Access points can ignore stations using a null (blank) SSID field in their Probe Request frames, but must respond with a Probe Response frame if a station has a specific SSID matching their own.
C. In order to provide seamless roaming, some vendors allow a station to associate with a new access point while still associated with the old one as long as both access points are from the same vendor.
D. When a station is in the cell range of multiple access points, it will associate with an access point that uses active scanning before associating with an access point that uses passive scanning.
E. A station cannot attempt to associate with an access point until that access point authenticates the station.

Answer: A,E

QUESTION 614:

Given: Co-locating access points means that they physically reside in the same immediate area and typically operate at low power.
Which statements are true regarding 802.11-compliant systems and co-located access points?

A. The same number of 802.11b systems and 802.11g systems can be co-located in the 2.4 GHz ISM band without adjacent channel interference.
B. Up to four 802.11a access points in the 5.15 ?5.25 GHz U-NII band can be co-located without performance degradation.
C. 802.11 FHSS systems have a co-location throughput advantage over 802.11b DSSS systems because they are frequency agile and make use of more discrete channels.
D. 802.11g access points configured for 802.11g-compliant operation use protection mechanisms to prevent OFDM transmissions from colliding with the DSSS transmissions. This prevents performance degradation when 802.11g systems are co-located with 802.11b access points.
E. An 802.11-compliant FHSS system operating at its maximum data rate would require at least three co-located access points to achieve the same throughput as an 802.11b DSSS system operating at its lowest DSSS data rate.

Answer: A,B

QUESTION 615:

A client calls and tells you they are trying to connect a new laptop to their 802.11g network. The client utility shows that the access point has high signal strength, and there is an excellent connection to the access point. Their laptop is unable to get a valid IP address and thus cannot connect to servers on their wired network. What two wireless network problems can cause this situation?

A. The laptop's MAC address has not been added to the access point's filter list.
B. The wireless client device is using the wrong WEP key.
C. The wireless client device is using the wrong network name (ESSID)
D. The wireless client device is configured to use Shared Key authentication.
E. The access point is experiencing a significant amount of co-channel interference.

Answer: A,B

QUESTION 616:

What is an advantage of using WPA-Personal instead of WEP-128 as a security solution for 802.11a networks?

A. WPA-Personal uses 802.1X/EAP for authentication, and WEP-128 uses preshared keys.
B. WPA-Personal is based upon IEEE 802.11 industry standards, but WEP is not.
C. WPA-Personal uses CCMP for encryption, and WEP-128 uses TKIP for encryption.
D. Each station using WPA-Personal uses a unique encryption key to encrypt data, but WEP-128 stations all use the same encryption key.
E. Only users that know the preshared key can view other stations?encrypted data when WPA-Personal is in use. With WEP-128, this is not possible.

Answer: D