CWNA

Exam PW0-100

certified wireless network administrator(cwna)

Version: 5.0

[Total Questions: 120]

Topic 1, A

A

Question No : 1 - (Topic 1)

What criteria can an 802.11 wireless client use to select the best access point with which to associate?

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 narrowband RF interference sources

Answer: A,E

Question No : 2 - (Topic 1)

The IEEE 802.11 standard (as amended) specifies which features for strong security?

A. SSID Hiding
B. EAP-TTLS
C. 4-Way Handshake
D. CCMP Cipher Suite
E. IPSec VPN Support

Answer: C,D

Question No : 3 - (Topic 1)

Given: Co-located ERP-OFDM access points can experience adjacent channel interference and resulting throughput degradation when operating on non-overlapping channels.

What causes this condition to occur?

A. The access points are too close to one another.
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: A,D,F

Question No : 4 - (Topic 1)

What are possible causes of the "hidden node" problem with 802.11 WLANs?

A. Data frames 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 too close in proximity to each other
E. Interfering obstacles between client stations
F. Large 802.11 cells with physically distributed stations
G. 802.11 radios with distributed antenna systems

Answer: E,F,G

Question No : 5 - (Topic 1)

Using only a software access point, a narrowband RF jamming device, and a DHCP server application, what common WLAN attack can be successfully performed on inadequately secured wireless client stations?

A. Hijacking Attack
B. Management Interface Exploit Attack
C. Eavesdropping Attack
D. Encryption Cracking Attack

Answer: A

Question No : 6 - (Topic 1)

According to the IEEE 802.11 standard (as amended), how much separation is required between the center frequencies of non-overlapping ERP (clause 19) channels?

A. 10 MHz
B. 11 MHz
C. 20 MHz
D. 22 MHz
E. 25 MHz
F. 30 MHz

Answer: E

Question No : 7 - (Topic 1)

Given: A WLAN transmitter that emits a 100 mW 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 EIRP at the antenna element?

A. 50 mW
B. 250 mW
C. 500 mW
D. 750 mW
E. 1000 mW

Answer: C

Question No : 8 - (Topic 1)

What statements about the 802.11 standard's QoS facility enhancements are true?

A. Two new channel access methods are introduced.
B. A new 2-byte QoS Control field has been added to the MAC frame.
C. QoS-capable stations (QSTAs) 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: A,B

Question No : 9 - (Topic 1)

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. t type of building construction material introduces the least amount of RF signal loss?

A. Chain-link fence
B. Wood-studded drywall
C. Concrete or brick wall
D. Aluminum siding

Answer: B

Question No : 10 - (Topic 1)

What three cipher suites are specified by the IEEE 802.11 standard (as amended)?

A. CCMP
B. WPA2
C. IPSec
D. 802.1X
E. SSH2
F. WEP
G. TKIP

Answer: A,F,G

Question No : 11 - (Topic 1)

The WPA/WPA2-Enterprise certifications 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 No : 12 - (Topic 1)

Given: ABC Company has hired you to perform a site survey on their facility. ng an interview, the network manager informs you that the new wireless network must use U-NII bands and OFDM, and a VoIP application will be used extensively over the wireless network.

What items do you need to include in the site survey report?

A. End-user coverage requirements
B. 802.1X/EAP type support requirements for each AP
C. Real-time application troubleshooting techniques
D. User-specific throughput requirements and AP capacity information
E. Best practice documents concerning health hazards for 802.11 VoIP phone use

Answer: A,D

Question No : 13 - (Topic 1)

In an Infrastructure Basic Service Set (BSS), what 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. Stations broadcast Probe Request frames on all channels within the governmental regulatory domain. Nearby access points respond with Probe Response frames. Stations record information found in the Probe Response frames for use in the association process.
C. 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.
D. Stations broadcast Beacons on a single channel. Nearby stations record information found in the Beacons for use in the association process.

Answer: B

Question No : 14 - (Topic 1)

What statements about deauthentication in 802.11 WLANs are true?

A. A station or access point may transmit a deauthentication frame.
B. An access point may refuse deauthentication frames sent by a station.
C. Deauthentication is a notification, not a request.
D. Deauthentication frames have an encrypted payload.
E. Only access points may issue deauthentication frames.

Answer: A,C

Question No : 15 - (Topic 1)

Given: You are the network administrator for ABC Company. manager has recently attended a wireless security seminar. 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 the 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 frames. 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 WLAN, provided they have the correct security credentials.
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: A,C

Question No : 16 - (Topic 1)

Your organization has multiple client devices, some that support WEP, some that support WPA, and some that support WPA2. e client devices that support only WEP are capable of being firmware upgraded to support the TKIP cipher suite. he wireless administrator, you are required to provide the strongest industry standard layer-2 security possible while implementing a consistent solution for all devices. 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 No : 17 - (Topic 1)

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 locations, updating an access point's 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 No : 18 - (Topic 1)

What term describes the effect of increasing the intensity of an RF wave when the RF antenna lobe is focused in a desired direction?

A. Polar Extension
B. Active Amplification
C. Beam Compression
D. Passive Gain
E. Phased Array Propagation

Answer: D

Question No : 19 - (Topic 1)

What items are essential for performing an RF site survey for 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: A,E

Question No : 20 - (Topic 1)

As part of a manual site survey report, what is the best method for documenting "dead spots" in an area covered by an indoor 802.11 WLAN?

A. Showing the dead spots to the network administrator in 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 giving them to end users.

Answer: D

Question No : 21 - (Topic 1)

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 No : 22 - (Topic 1)

Given: ABC Company 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 attack will not be recognized by the WIPS?

A. Deauthentication
B. MAC Spoofing
C. Protocol Jamming
D. Eavesdropping
E. RF Jamming

Answer: D

Question No : 23 - (Topic 1)