TestHorse

Certified IT practice exam authority

Accurate study guides, High passing rate!
Testhorse provides update free of charge in one year!

http://www.testhorse.com

Exam : **PW0-205**

Title : Certified wireless analusis professional(cwap)

Version : DEMO

1. Which of the following descriptions accurately describes IEEE 802.11 compliant Power Save mode operation in a DCF Basic Service Set?

A. Following a period of time in a low power state, client stations wake themselves and automatically poll the access point for traffic using a PS-Poll frame.

B. When the access point's buffer is full, the access point wakes all client stations using a PS-Poll frame so that they can receive the data.

C. Upon receiving traffic for a dozing station, the access point wakes the client station using a PS-Poll frame so that the client station can receive the data.

D. After waking from a low power state, client stations listen for the next beacon to determine if sending a PS-Poll frame to the access point is necessary.

E. After waking at a schedule TBTT, client stations automatically send Null Function frames to the access point with the Power Management bit cleared.

Answer: D

2. The Timestamp field, found in 802.11 Beacon Management frames, is 8 bytes in length and serves which of the following purposes?

A. Keeps all client stations in a BSS synchronized to within approximately 4 microseconds of the access point.

B. Allows client stations in the IBSS to pick the best of multiple beacons.

C. Used to notify client stations using power management features of how long their queued frames have been held by the access point.

D. Informs associating client stations how often to expect Beacon Management frames to be sent by the access point.

E. Allows all client stations in a BSS to calculate how long it took for the Beacon Management frame to traverse the wireless medium.

Answer: AB

3. Choose the true statements regarding wireless network discovery processes for an 802.11b network.

A. Client stations may continually send Probe Request frames on all 802.11b channels in the 2.4 GHz ISM band in a consecutive manner, regardless of their association state.

B. Access points send Beacon Management frames on all 802.11b channels in the 2.4 GHz ISM band in a consecutive manner including the channel for which the access point is configured.

C. Client stations send Probe Request frames on all 802.11b channels in the 2.4 GHz ISM band in a consecutive manner until they associate with an access point. After associating to an access point, they are no longer allowed to transmit Probe Request frames.

D. Access points send Beacon Management frames only on the 802.11b channel in the 2.4 GHz ISM band for which the access point is configured.

E. Client stations send Probe Request frames on all 802.11b channels in the 2.4 GHz ISM band in a consecutive manner until they receive at least 3 Probe Response frames.

Answer: AD

4. Which is true of the Association Identifier (AID) used in 802.11 wireless LANs?

A. The AID has a maximum value of 2048, and is used to uniquely identify a wireless client station associated with an access point.

B. The AID has a maximum value of 2007, and resides in the duration/ID field of a PS-Poll frame only.

C. When bit 16 of the field is zero, the value in bits 15-0 represent the remaining duration of a frame exchange.

D. The least significant 8 bits of this field are used by the wireless client station to identify which bit in a TIM indicates that the access point has frames buffered for the wireless client station.

E. The AID is used by the access point in DCF mode to reduce duplicate transmissions when sending multicasts.

Answer: B

5. When an access point sends an RTS frame, the duration field will contain an amount of time, measured in microseconds, equal to which of the following?

A. 2 ACK, 1 RTS, 1 DATA, 4 SIFS

B. 1 ACK, 1 CTS, 1 DATA, 3 SIFS

C. 1 DATA, 1 RTS, 2 SIFS, 1 DIFS, 1 ACK

D. 1 RTS, 1 CTS, 1 DATA, 2 ACK, 4 SIFS

Answer: B

6. Which of the following is true regarding frame acknowledgement in an 802.11 wireless LAN?

A. ACK frames following Data fragments set the NAV of competing stations for a duration equal to two SIFS plus the next Data fragment and its ACK.

B. A client station reassociation request frames are only acknowledged with a reassociation response from the access point when roaming in a wireless LAN secured with 802.1X/EAP.

C. Probe request acknowledgement (sending of a probe response) is configurable in the access point and is always linked to SSID broadcast configuration in Beacons.

D. Beacon frames are acknowledged by all client stations configured for PCF mode.

E. Frame fragments are acknowledged individually (with an ACK frame)

F. In PCF mode, WEP-Data frames are only acknowledged by client stations, never by access points.

Answer: AE

7. An 802.11b client station, sends a single 600 byte MSDU to another 802.11b client station while operating as part of an unsecured infrastructure BSS. Due to thresholds set on all client stations and the access point, all MPDUs over 300 bytes in length invoke the RTS/CTS protocol. How many individual CTS frames are transmitted on the wireless medium as part of the entire process of moving the 600 byte MSDU between the two client stations?

A. 1

B. 2

C. 3

D. 4

Answer: B

8. A wireless network administrator has examined the frame retry counts on several client stations in a WLAN that is not using encryption, and has determined that they are extraordinarily high. For this reason, he has decided to configure station fragmentation thresholds to 400 bytes. With this configuration change, when a data frame with a 1500 byte MSDU is transmitted by one of the wireless client stations to a wired station through an access point, what will be the order and size (in bytes) of the fragments as they're transmitted?

A. Frame1 = 400, Frame2 = 400, Frame3 = 400, Frame4 = 300

B. Frame1 = 300, Frame2 = 300, Frame3 = 300, Frame4 = 300, Frame5 = 300

C. Frame1 = 300, Frame2 = 400, Frame3 = 400, Frame4 = 400

D. Frame1 = 400, Frame2 = 400, Frame3 = 400, Frame4 = 400, Frame5 = 40

E. The fragmentation threshold setting on client stations only affects received frames, not transmitted frames

F. The fragmentation threshold setting on client stations is not a manual adjustment, and can only be auto-configured by access points

Answer: D

9. The 802.11 series of standards calls for use of a Traffic Indication Map (TIM) and a Delivery Traffic Indication Message (DTIM). Which of the following is true regarding the TIM and DTIM in an infrastructure BSS?

A. The TIM is a field in the Beacon Management frame that holds a map of every client station associated to an access point. It is used for broadcast traffic delivery.

B. The TIM and DTIM are both part of the Beacon management frame and are both sent in every Beacon for the purpose of announcing the modulation type and supported rate set of the access point.

C. The DTIM parameters are part of each Beacon's TIM Information Element, and they are used to indicate queued broadcast/multicast data to client stations using power management features in the BSS.

D. The DTIM is used in 802.11a and 802.11g Beacons whereas the TIM is used only in 802.11b Beacons. The DTIM purpose is to allow for higher rates of Beacon broadcasting and thus raise overall data rates in OFDM based systems.

E. A DTIM period of 0 means that every TIM is a DTIM.

F. The first Beacon sent during a CFP must contain a DTIM

Answer: CF

10. When the ToDS bit is set to 1 and the FromDS bit is set to 0 in the Frame Control field of an 802.11 Data frame, what might this indicate about the infrastructure and the wireless conversation?

A. A wireless client station could be sending data to a wired station through an access point.

B. A wireless client station must be sending data to a wireless station where the frame has to traverse a

Wireless Distribution System (WDS).

C. A wireless client station must be sending data directly to the access point for the purpose of managing the access point.

D. A wireless client station could be sending data to a wireless client station across an access point.

E. A wireless client station could be sending data directly to another wireless client station as part of an IBSS.

Answer: AD

11. When using a wireless protocol analyzer, it is common to see Beacon Management frames (Beacons) being sent several times per second. Which of the following statements is true regarding Beacons?

A. Beacons can be disabled for security purposes.

B. The BSSID and Source Address are always the same.

C. The Destination address is always FF:FF:FF:FF:FF:FF.

D. The Receiver address and the BSSID are always the same.

E. The reason Beacons are transmitted so often is that they are unicast frames destined to each associated station.

F. The 802.11 standard specifies that all Beacons must contain a DTIM information element.

Answer: BC

12. When RTS/CTS is used in DCF mode, what is the frame exchange sequence between two wireless stations including interframe spaces?

A. DIFS-RTS-SIFS-CTS-SIFS-DATA-SIFS-ACK

B. DIFS-RTS-ACK-CTS-ACK-DATA-SIFS-ACK

C. DIFS-RTS-CTS-SIFS-ACK-DATA-SIFS-ACK

D. EIFS-RTS-CTS-SIFS-DATA-SIFS-ACK

E. PIFS-RTS-SIFS-CTS-SIFS-DATA-SIFS-ACK

Answer: A

13. The 802.11 standard allows for frame fragmentation due to an unreliable medium. Which two fields in the 802.11 frame are involved in numbering data frame fragments and notifying the receiving station

when all of the fragments of a data frame have been received?

A. Capability Information field

B. Frame Control field

C. ERP Information field

D. Sequence Control field

E. DS Parameter field

F. Ordered Service field

Answer: BD

14. In a DCF 802.11g network, when is the Power Management subfield of the Frame Control field set to a value of 1?

A. Only in management frames sent by a client station immediately prior to entering a low power state (dozing) that are part of a frame exchange sequence.

B. On any Data frame sent by the access point subsequent to a PS-Poll frame.

C. On any frame transmitted by a client station operating in Power Save mode.

D. Only in the PS-Poll frame sent from a client station operating in Power Save mode to an access point after the client station awakens from a low power state (dozing).

Answer: C

15. An 802.11e compliant Data frame, also called an MPDU, may have a maximum header size of how many octets?

A. 28

B. 30

C. 34

D. 36

E. 40

Answer: C

16. An 802.11 data frame has multiple address fields. How many address fields are there and how are they used?

A. Two address fields, used for SA, DA

B. Three address fields, used for SA/TA, DA/RA, BSSID

C. Four address fields, used for SA, DA, BSSID/TA, RA

D. Five address fields, used for SA, DA, TA, RA, BSSID/HA

E. Six address fields, used for SA, DA, TA, RA, BSSID, HA

Answer: C

17. How does an access point operating in DCF mode notify a client station operating in Power Save mode of multiple multicast frames queued at the access point?

A. The access point sets the Beacon DTIM to indicate that it has queued multicast traffic for the client station.

B. The access point sends the client station a CF-Poll frame with the AID subfield set to the station MAC address.

C. The access point responds to the client station PS-Poll frame with the AID subfield set to a value equal to the number of queued multicast frames.

D. The access point sets the More Data subfield in the Frame Control field of each Data frame to 1 until the last multicast frame is delivered.

E. The access point sets the Duration field of each Beacon to a value equal to the amount of time it will take to send all of the queued multicast frames to the client station.

Answer: AD

18. ABC Company has recently installed its first access point. The access point is an 802.11g unit, and both 802.11g and 802.11b client stations will be used on the wireless network simultaneously. The network administrator has appropriately configured the access point and all of the company 802.11b wireless client stations to use short preambles for CCK transmissions. A visitor begins using a Personal Data Assistant (PDA) with integrated 802.11b configured for use of long preambles on ABC wireless network. Which of the following describes what the network administrator will see with a wireless protocol analyzer?

A. Once the visitor PDA is associated to the access point, all 802.11b stations associated to the access point will begin using long preambles.

B. The visitor PDA will not be able to associate to the wireless network, and it will cause significant interference for other wireless stations.

C. The visitor PDA will communicate with the access point using long preambles, and the access point will communicate with all other client stations using short preambles.

D. The visitor PDA associates to the access point using MMPDUs with long preambles, then begins sending Data frames using short preambles.

E. Only after the visitor's PDA associates to the access point, will the 802.11g client stations begin using protection mechanisms.

Answer: A

19. In which of the following IEEE 802.11a frames can the SSID be found providing the SSID is not specifically removed through firmware configuration by an administrator?

A. Association Request

B. Reassociation Request

C. Probe Response

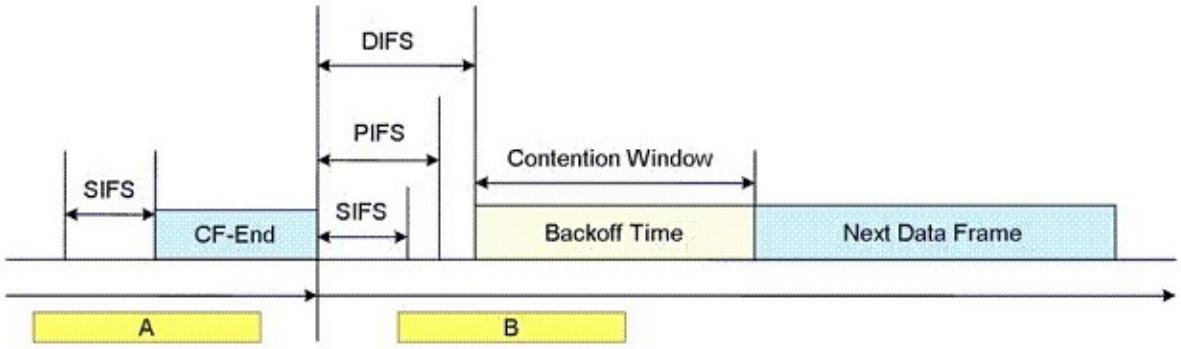
D. Disassociation

E. Authentication

F. Reassociation Response

Answer: ABC

20. Referring to the diagram, match label boxes A and B with their appropriate name.



A. A = Contention-Free Period, B = Contention Period

B. A = ATIM Window, B = Data Window

C. A = Congestion Control Period, B = Arbitration Window

D. A = Frame Control Period, B = Backoff Window

E. A = Data Period, B = Interframe Space Period

Answer: A