

**Actualtests.com**

The Power of Knowing



Exam : PW0-300

Title : Wireless Security Professional

Ver : 03-03-2009

**QUESTION 1:**

A QoS STA is permitted to send which frame types of a Hybrid Coordinator?

- A. QoS Data + CF-ACK + CF-Poll
- B. Data + CF - Poll
- C. QoS Null
- D. PS-Poll
- E. CF-End + CF -Ack

Answer: C,D

---

**QUESTION 2:**

WMM-PS trigger frames can be what type of IEEE 802.11 frames?

- A. Reassociation
- B. PS-Poll
- C. QoS Data
- D. QoS + CF-Poll
- E. QoS Null
- F. CTS

Answer: C,E

---

**QUESTION 3:**

Given: Certkiller .com has an IEEE 802.11 WLAN secured by strong authentication (PEAP-EAP-MSCHAPv2) and encryption (CCMP/AES). They wish to implement wVoIP phones but have notices that the phones they have selected only supports WPA-Personal using TKIP/RC4.

How can Certkiller .com maintain their current level of data security while allowing the wVoIP phones network access?

- A. Enable application layer encryption for the voice protocol and implement a wireless intrusion prevention system (WIPS) on the wVoIP network segment
- B. Use a secure DHCP server that can restrict access to layer 3 addresses based on user authentication
- C. Use MAC filtering to the network segment where the wVoIP phones will be used
- D. Use a separate SSID for the wVoIP phones and map this new SSID to a separate VLAN on the wired infrastructure
- E. Using RBAC, allow only the appropriate voice protocol (SIP, H.323 etc) to a specific destination address on the network segment where the wVoIP phones will be used

Answer: D,E

**QUESTION 4:**

On an Enterprise IEEE 802.11 WLAN supporting both voice and data, why is WPA2-Personal security often preferred over WPA2-Enterprise Security for voice-enabled devices?

- A. WPA2-Personal imposes less encryption overhead than WPA2-Enterprise, resulting in better performance
- B. WPA2-Personal is more easily configured on the voice-enabled client devices than WPA2-Enterprise
- C. WPA2-Personal supports IEEE 802.11 fast/secure roaming between access points, whereas WPA2-Enterprise deployments may not
- D. Voice-enabled devices use application layer (L7) security mechanism, minimizing the need for scalable data link (L2) security
- E. WPA2-Enterprise voice-enabled devices consume battery life at a rate of almost double that of WPA2-Personal

Answer: C

---

**QUESTION 5:**

Given: An ingress frame arrives on the Ethernet port of an autonomous AP marked with an IEEE 802.1D user priority value:

Which IEEE 802.1D user priority values (by name) will assure the data payload carried by the Ethernet frame gets assigned to the highest priority WMM queue?

- A. Voice
- B. Network Control
- C. Best Effort
- D. Controlled Load
- E. Video

Answer: A,B

---

**QUESTION 6:**

A QoS STA obtains a TXOP for an access category (AC) after what two parameters are met?

- A. After a Block ACK Response
- B. After a scheduled service period ends
- C. The medium is idle at the AIFS[AC] slot boundary
- D. After a Target Beacon Transmission Time (TBTT)
- E. The backoff time for that AC has expired

Answer: C,E

---

**QUESTION 7:**

Given: An EDCA QoS BSS is operating as a Robust Security Network (RSN). Two QoS STAs in the QoS BSS are using a Direct Link to communicate.

When the RTS/CTS threshold is exceeded for a frame to be transmitted between the two QoS STAs, what is the frame exchange sequence, including interframe spaces?

- A. AIFS-RTS-SIFS-CTS-SIFS-DATA-SIFS-ACK
- B. AIFS-RTS-SIFS-CTS-DIFS-DATA-SIFS-ACK
- C. DIFS-RTS-CTS-SIFS-DATA-SIFS-ACK
- D. RIFS-RTS-SIFS-CTS-SIFS-DATA-SIFS-ACK
- E. DIFS-RTS-SIFS-ACK-SIFS-CTS-SIFS-ACK-SIFS-DATA-SIFS-ACK

Answer: A

---

**QUESTION 8:**

All successful frame transmissions within an EDCA TXOP are separated by what IEEE 802.11 entity?

- A. TBTT
- B. ACK
- C. SIFS
- D. AIFS
- E. PIFS
- F. CAP

Answer: C

---

**QUESTION 9:**

Given: Certkiller .com has recently installed its first access point. The access point is an ERP unit and both ERP and HR-DSSS client stations will be used on the wireless network simultaneously. The network administrator has appropriately configured the access point and all of the company's HR-DSSS wireless client stations to use short preambles for CCK transmissions. A visitor begins using a Personal Data Assistant (PDA) with an integrated HR-DSSS radio configured for use of long preambles on ABC's wireless network

Which statement describes what the network administrator will see with a wireless protocol analyzer?

- A. Once the visitor's PDA is associated to the access point, all HR-DSSS stations associated to the access point will begin using long preambles

- B. The visitor's PDA will communicate with the access point using long preambles and the access point will communicate with all other client stations using short preambles
- C. The visitor's PDA will not be able to associate to the wireless network and it will cause significant interference for other wireless stations
- D. The visitor's PDA will associate to the access point using MMPDUs with long preambles but then begin sending Data frames using short preambles since data frames can't use long preambles

Answer: A

### QUESTION 10:

Given: Shown are frames captured from an IEEE 80.1X/LEAP authentication. This WLAN is a Robust Security network (RSN) using the CCMP cipher suite.

Exhibit:

Packet	Dest. Physic	Source Physic	BSSID	Absolute Time	Delta Time	Relative Time	Protocol
1	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.727946		0.000000	002.11
2	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.728260	0.000314	0.000314	002.11
3	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.730018	0.001758	0.002072	002.11
4	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.730330	0.000312	0.002384	002.11
5	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.730830	0.000500	0.002884	002.11
6	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.731138	0.000308	0.003192	002.11
7	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.731390	0.000252	0.003444	002.11
8	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.731590	0.000200	0.003644	002.11
9	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.733010	0.001412	0.005056	002.11
10	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.733224	0.000214	0.005270	002.11
11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.733808	0.000584	0.005854	002.11
12	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.733848	0.000040	0.005894	002.11
13	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.734450	0.000602	0.006496	EAP Req
14	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.734555	-0.000095	0.006401	002.11
15	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.939073	0.204718	0.211277	EAP Req
16	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.939385	0.000312	0.211589	002.11
17	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.942649	0.003264	0.214853	EAP Req
18	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.942695	0.000046	0.214900	002.11
19	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.944581	0.001886	0.216786	EAP Req
20	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.944933	-0.000352	0.216434	002.11
21	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.939073	0.204718	0.229337	EAP Req
22	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.939385	0.000312	0.229649	002.11
23	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.942649	0.003264	0.233000	EAP Req
24	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.942695	0.000046	0.233046	002.11
25	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.972157	0.012884	0.245930	EAP Req
26	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.972203	0.000046	0.245976	002.11
27	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.972373	0.000170	0.246146	002.11
28	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.972413	0.000040	0.246186	002.11
29	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.974511	0.002098	0.248284	EAPOL-E
30	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.974831	0.000320	0.248604	002.11
31	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.976199	0.001368	0.249972	002.11
32	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.976243	0.000044	0.249996	002.11
33	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.977877	0.001634	0.251630	EAPOL-E
34	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	00:0D:11:11:11:11:11:11	12:10:20.978193	0.000316	0.251946	002.11

Using the information given in the screenshot, calculate how long it takes for only the frames that are part of the 4-Way handshake to complete.

- A. 210.443 ms
- B. 243.743 ms
- C. 3.018 ms
- D. 5.820 ms
- E. 237.753 ms

Answer: D

### QUESTION 11:

An HR-DSSS STA does not receive an ACK for a first-attempt data frame that is transmitted. In this case, what happens to the STA's DCF contention window?

- A. The contention window is not affected by failed Data Frame Deliveries
- B. The contention window is immediately closed and the frame is retransmitted
- C. The contention window approximately doubles in size
- D. The slot time within the contention window decreases by 50%
- E. It varies because the backoff algorithm is random

Answer: C

---

**QUESTION 12:**

Which statement are true regarding frame acknowledgement in an IEEE 802.11 WLAN?

- A. A client station's Reassociation Request frames are only acknowledged with a Reassociation Response from the access point when roaming in a WLAN secured with IEEE 802.1X/EAP
- B. ACK frames following Data frames with the more fragments bit set to 1 set the NAV of competing stations for a duration value equal to two SIFS plus the next Data fragment and its ACK
- C. Probe Request acknowledgement (sending of a Probe Response frame) is configurable in the access point and is always linked to SSID broadcast configuration in Beacons
- D. Data Frame fragments are acknowledged individually ( with an ACK frame)
- E. In a EDCA BSS, encrypted Data frames are only acknowledged by client stations, never by access points

Answer: B,D

---

**QUESTION 13:**

An HR-DSSS client station, sends a single 600 octet MSDU to another HR-DSSS 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 octets in length invoke the RTS/CTS protocol. How many CTS frames are transmitted on the wireless medium as part of the process of moving the 600 octet MSDU between the two client stations?

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

Answer: A

---

**QUESTION 14:**



Which statement accurately describes IEEE 802.11 Power Save Mode Operation in a Basic Service Set that does not support the QoS facility?

- A. After waking at a schedule TBTT, client stations automatically send Null Function frames to the access point with the power management bit cleared
- B. 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
- C. 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
- D. When the access point's buffer is full, the access point wakes all client stations using a PS-Poll frames so that they can receive the data
- E. 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

Answer: C

---

**QUESTION 15:**

Given: In an RSNA, non-AP STAs in an ESS set the Privacy subfield ( in the frame control field in the MAC header) to 0 within transmitted Association and Reassociation Request management frames.

How do APs process the privacy subfield in received association and reassociation request management frames?

- A. APs seeing a 0 immediately change the RSN IE field to 1 in Beacons
- B. APs interpret a 0 to mean subsequent frames are encrypted
- C. APs seeing a 0 enable management frame encryption
- D. APs ignore the Privacy subfield

Answer: D

---

**QUESTION 16:**

The IEEE 802.11 (as amended) Dynamic Frequency Selection (DFS) service is capable of performing what functions?

- A. Using modulation switching techniques to avoid interfering with radar systems
- B. Establishing a interference baseline on all 2.4 GHz channels
- C. Requesting and reporting of measurements in the current and other channels
- D. Testing channels for radar before using a channel and while operating in a channel
- E. Suspending operations on a channel with high IEEE 802.11 co-channel interference

Answer: C,D

---

**QUESTION 17:**

Which statement accurately describes why the Traffic indication map (TIM) information element is not shown in this Beacon frame?

Exhibit:



- A. Beacons only contain TIMs when the Power Management bit in the Frame Control Field of the MAC header is set to 1
- B. This model of access point does not support IEEE 802.11 compliant power save mode
- C. Beacons transmitted by IEEE 802.11 IBSS networks do not include TIMs
- D. This beacon frame is using a DTIM instead of a TIM
- E. This Beacon was captured on channel 2 but was transmitted on channel 1. This caused a loss of information elements within the Beacon

Answer: C

## QUESTION 18:

As a WLAN consultant, you have been contacted by one of your customers to go their premises to troubleshoot a problem with a single wireless client station (Station-Z). Your customer informs you that other wireless client stations are not having problems with wireless connectivity and that station-Z is configured in the same manner as all other wireless client stations on the network. Station-Z is showing an unusually high retransmission count in its client utilities. Using a wireless protocol analyzer, where and how would you begin troubleshooting this problem?

- A. Position the analyzer near Station-Z. Analyze Station-Z's transmissions and acknowledgements. Look for RF and obstacle-induced interference



- B. Position the analyzer half way between Station-Z and the access point. Analyze the distance between Station-Z and the access point
- C. Position the analyzer near the access point. See if Station-Z's frames are reaching the access point and if so, analyze their signal strength
- D. Position the analyzer near Station-Z. Analyze the frames Station-Z is receiving, looking for corrupted data frames

Answer: A,C

---

**QUESTION 19:**

Given: When using a wireless protocol analyzer, it is common to see Beacons transmitted several times per second.

Which statements are true regarding Beacons in an infrastructure BSS?

- A. The Destination address is always FF:FF:FF:FF:FF:FF
- B. The Receiver address and the BSSID are always the same
- C. The BSSID and Source Address are always the same
- D. Beacons can be disabled for security purposes

Answer: A,C

---

**QUESTION 20:**

When the To DS bit is set to 1 and the From DS bit is set to 0 in the frame control field of an IEEE 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 directly to the access point for the purpose of managing the access point
- C. A wireless client station could be sending data to a wireless client station across an access point
- D. A wireless client station could be sending data directly to another wireless client station as part of a QoS BSS direct link
- E. A wireless client station must be sending data to a wireless station where the frame has to transverse a Wireless Distribution System (WDS)

Answer: A,C

---

**QUESTION 21:**

Given: Certkiller .com is interested in deploying an IEEE 802.11 network that supports wVoIP devices. During a proof-of-concept test, they deployed a WLAN controller, one lightweight AP and QoS features in support their voice and data client devices in the 2.4

GHZ band. The network administrator has configured the access point to perform client connectivity and rogue wireless device scanning. As a test, John places a rogue AP on his network and configures it to use channel 11. The WLAN controller never reports the rogue AP.

Why does the WLAN controller never report the rogue AP?

- A. The rogue AP is operating in APSD mode and therefore does not transmit identifying management frames
- B. The rogue AP is using the encrypted management frame feature which masks its presence.
- C. Lightweight APs can only scan for rogue devices on the channel they are using. The authorized AP is on channel 1.
- D. Admission Control is enabled on the WLAN controller and the voice client is actively communicating through the AP during the entire test.

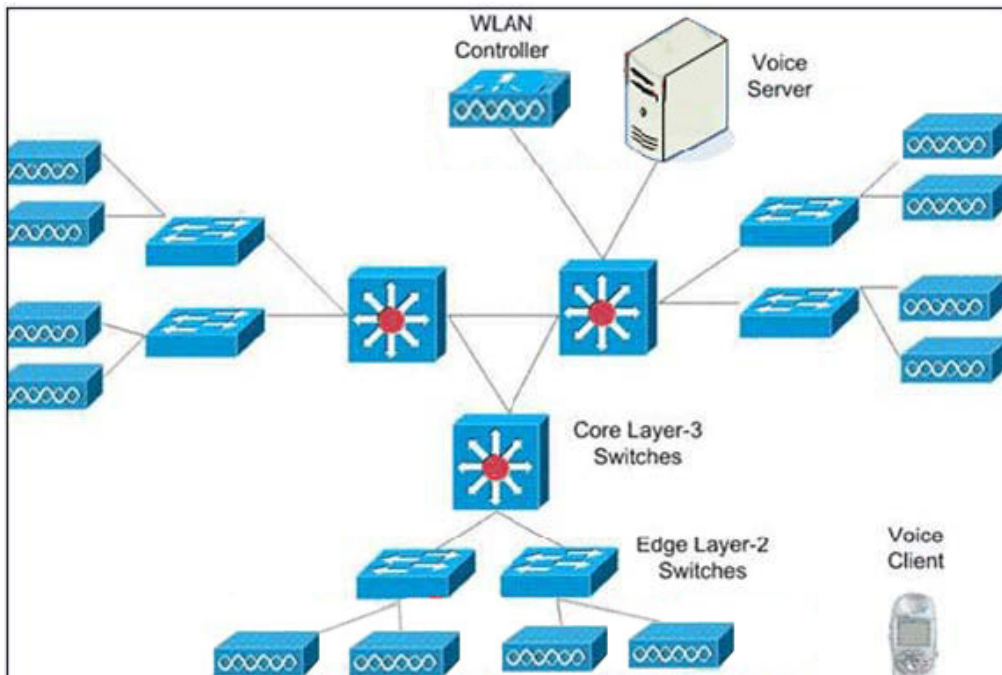
Answer: D

---

**QUESTION 22:**

Given: Certkiller .com is implementing a QoS enabled infrastructure that will support both voice and data. Their WLAN controller is connected to one of three core layer-3 Ethernet switches. Each core layer-3 Ethernet switch has multiple edge layer-2 Ethernet switches attached. Lightweight APs are connected to all edge layer-2 Ethernet switches. The WLAN controller is on subnet 10.1.1.0/24 and the APs are on numerous other subnets. The APs are connected to the WLAN controller via GRE tunnels.

Exhibit:



When a data packet is sourced at the voice client destined to the voice server, which devices along the path transmit frames with IEEE 802.1Q priority tags?

- A. Edge switch, core switches
- B. Voice Client, AP, WLAN controller
- C. Edge switches, core switches, WLAN controller
- D. AP, Core Switches, WLAN controller
- E. Voice Client

Answer: C

---

**QUESTION 23:**

What frame subtypes are specified in the IEEE 802.11 standard (as amended)?

- A. DTIM
- B. Data + ACK
- C. QoS Null
- D. EAPoL Key
- E. Block Ack Request
- F. Data + CF-End

Answer: C,E

---

**QUESTION 24:**

Certkiller .com is a small company that has hired you to troubleshoot an intermittent performance problem with their ERP WLAN. They have noticed that intermittently throughout a typical day, their WLANs latency increases enough to interrupt some mission critical applications. Considering that Certkiller .com has no baseline analysis, what possible first step do you take toward troubleshooting Certkiller .com's wireless network problem?

- A. Using a protocol analyzer, you search for wireless clients that are transmitting too many Probe Request Frames and temporarily replace them as troubleshooting measure
- B. You perform a protocol analysis of Certkiller .com's premises looking for ERP Basic Service Sets that have both HR-DSSS and ERP stations associated. You then compare this information to where the latency is being experienced
- C. You install protocol analyzer probes near each access point in order to see if a large percentage of data frames are carrying their maximum payload over the next two days
- D. Using a protocol Analyzer, you search for rogue access points that might be causing interference in the 2.4 GHz ISM band by emitting Beacons

Answer: B

---

**QUESTION 25:**

In the frame decode shown, 1,2,5.5 and 11 mbps are all shown as supported data rates. 1

and 2 mbps are shown with ( basic) beside them. What does (basic) mean in this context?  
Exhibit:

No	Ch	Len	St	Pr	Source	Dest	Summary
116		101	0	1	SumbatA2:16:8C	FF:FF:FF:FF:FF:FF	802.11 beacon
+ network media info							
+ 802.11 MAC header							
- 802.11 Frame body							
timestamp : 25A39BB0:40000000							
beacon interval : 100 TU(s)							
+ capability info							
+ info : SSID							
- info : supported rates							
length : 4							
rate : 1.0 mbps (basic)							
rate : 2.0 mbps (basic)							
rate : 5.5 mbps							
rate : 11.0 mbps							
+ info : DS param set							
+ info : TIM							
+ info : unknown (7)							
+ info : unknown (173)							
+ info : unknown (221)							

- A. Basic Rates are optional data rates, often used for assuring connectivity for those stations that are at a significant distance from the access point
- B. The highest data rate set to Basic is automatically used to send broadcast traffic such as Beacon frames
- C. The access point requires the station to support Basic rates in order to associate to it Basic Service Set
- D. Base rates are only used for multicast traffic and do not affect unicast traffic

Answer: C

---

### QUESTION 26:

Given: An IEEE 802.11 data frame is encrypted with CCMP/AES and is carrying the maximum frame payload. This data frame is being transmitted from a QoS STA to a QoS AP.

What is the size of this IEEE 802.11 MPDU?

- A. 2356 octets
- B. 2350 octets
- C. 2346 octets
- D. 2304 octets
- E. 2312 octets
- F. 1500 octets

Answer: B

**QUESTION 27:**

Given: Certkiller .com is implementing a QoS enabled infrastructure that will support both voice and data. The WLAN controller is connected to one of three core layer-3 Ethernet Switches. Each core layer-3 Ethernet switch has multiple edge layer-2 Ethernet Switches attached. Lightweight APs are connected to all edge layer-2 Ethernet switches. The WLAN controller is on subnet 10.1.1.0/24 and the APs are on numerous other subnets. The APs are connected to the WLAN controller via LWAPP tunnels. When IEEE 802.11 frames arrive at a lightweight AP from a QoS STA that need to be sent to the WLAN controller, which bits can the AP mark to signal the layer-2 and layer-3 Ethernet switches to use higher priority processing?

- A. The IEEE 802.11 frame's QoS control bits
- B. The IP Header's TOS bits
- C. The Ethernet Frame's 802.1Q priority tag bits
- D. The LWAPP header's C bit

Answer: B,C

---

**QUESTION 28:**

This screenshot displays a frame capture of a single PING Request and PING Reply communication between two wireless client stations across a Wireless Distribution Systems (WDS). Which packet numbers have both the From DS and to DS bits sets to 1? Exhibit:

Packet	Address 1	Address 2	Address 3	Address 4	Data Rate	Size	Protocol
1	00:0D:65:C9:32:76	00:0A:8A:47:BF:4A	00:0A:8A:47:BC:1A		11.0	96	PING Req
2	00:0A:8A:47:BF:4A				11.0	14	802.11 Ack
3	00:0D:ED:A5:4F:70	00:0D:65:C9:32:76	00:0A:8A:47:BC:1A	00:0A:8A:47:BF:4A	11.0	102	PING Req
4	00:0D:65:C9:32:76				11.0	14	802.11 Ack
5	00:0A:8A:47:BC:1A	00:0D:ED:A5:4F:70	00:0A:8A:47:BF:4A		11.0	96	PING Req
6	00:0D:ED:A5:4F:70				11.0	14	802.11 Ack
7	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70	00:0A:8A:47:BF:4A		11.0	96	PING Reply
8	00:0A:8A:47:BC:1A				11.0	14	802.11 Ack
9	00:0D:65:C9:32:76	00:0D:ED:A5:4F:70	00:0A:8A:47:BF:4A	00:0A:8A:47:BC:1A	11.0	102	PING Reply
10	00:0D:ED:A5:4F:70				11.0	14	802.11 Ack
11	00:0A:8A:47:BF:4A	00:0D:65:C9:32:76	00:0A:8A:47:BC:1A		11.0	96	PING Reply
12	00:0D:65:C9:32:76				11.0	14	802.11 Ack

- A. 7
- B. 5
- C. 11
- D. 9
- E. 1
- F. 3

Answer: D,F

---

**QUESTION 29:**

What does a TXOP Limit value of 0 in the EDCA parameter set included in a QoS AP's or Probe Response frames indicates?

- A. It indicates that no MSDUs or MMPDUs may be transmitted by a non-pollable QoS STA
- B. It indicates that a single MSDU or MMPDU may be transmitted at any rate for each TXOP
- C. It indicates that QoS STAs may transmit voice MPDUs (Access Category 7,8) during TXOPs
- D. It indicates that QoS STAs must wait for the HC to transmit a Polled TXOP before they can transmit MSDUs or MMPDUs
- E. It indicates that one or more MSDUs or MMPDUs must be transmitted at the lowest rate during each TXOP

Answer: B

---

**QUESTION 30:**

When capturing traffic using an IEEE 802.11 protocol analyzer that has a single 2.4 GHz radio card, which statement is true?

- A. All transmissions on only one 2.4 GHz channel will be captured at any given time
- B. Transmissions on one 2.4 GHz channel and some of the traffic on overlapping channels can be captured simultaneously
- C. All transmissions on all 2.4 GHz channels can be captured simultaneously
- D. The number of channels that an analyzer can capture simultaneously is dependent on the vendor's implementation

Answer: B

---

**QUESTION 31:**

Given: While using the EDCA access mechanism, QoS STAs and QoS APs must use a backoff algorithm in order to arbitrate for medium access. The backoff procedure includes randomly choosing an integer from the contention window.

When may QoS STAs and QoS APs decrement their randomly chosen Backoff Time?

- A. Immediately preceding a TBTT
- B. During every PCF interframe space (PIFS)
- C. Only when the medium is considered idle
- D. Only during the contention Free Repetition Interval
- E. Immediately following a DTIM Beacon

Answer: C

---

**QUESTION 32:**

Given: An IEEE 802.11 Authentication frame includes information used to initiate a multi-frame exchange between a client station and an access point that ultimately results



in the verification of the identity of the client station.

Which of the following are information fields in the authentication frame?

- A. Contention-Free parameter set
- B. Algorithm number
- C. Challenge text
- D. Supported rates
- E. Transaction sequence number

Answer: B,E

---

**QUESTION 33:**

The More Fragments subfield is found in which IEEE 802.11 frame field?

- A. Protocol Order Field
- B. QoS Control Field
- C. Frame Control Field
- D. Sequence Control Field
- E. MAC Service Data Unit field
- F. Fragmentation Control Field

Answer: C

---

**QUESTION 34:**

Which statement is FALSE regarding use of admission control in a QoS BSS?

- A. If a QoS STA desire to send data without admission control using an access category (AC) that mandates admission control, the QoS STA will use a lower priority AC that does not use admission control
- B. A QoS AP uses ACM subfields in the EDCA parameter set element to indicate admission control requirements for each access category (AC)
- C. The ACM bit is static for the duration of the lifetime of a BSS
- D. The IEEE 802.11 QoS facility implements a single admission control mechanism for use in contention-free periods (CFPs) and contention periods (CPs)
- E. A hybrid coordinator may enforce admission control policies during both contention-free periods (CFPs) and contention periods (CPs)

Answer: D

---

**QUESTION 35:**

What are two techniques used for real-time tracking for wVoIP devices within a facility?

- A. RF calibration

- B. Triangulation
- C. Client positioning
- D. SNR provisioning
- E. RF fingerprinting

Answer: B,E

---

**QUESTION 36:**

Given: While using the EDCA access mechanism, QoS STAs and QoS APs must use a backoff algorithm in order to arbitrate for medium access. The backoff procedure includes randomly choosing an integer from the contention window.  
When may QoS STAs and QoS APs decrement their randomly chosen Backoff Time?

- A. Only when the medium is considered idle
- B. During every PCF interframe space (PIFS)
- C. Immediately following a DTIM Beacon
- D. Immediately preceding a TBTT
- E. Only during the contention Free Repetition Interval

Answer: A

---

**QUESTION 37:**

Given: Certkiller .com has a WLAN Controller with 5 WLANs configured, each with its own SSID, security parameters and the default Beacon interval value of 100 time units (TUs)  
How often and in what manner are Beacons transmitted from a lightweight AP that is broadcasting Beacons for all 5 WLANs?

- A. One Beacon will be transmitted onto the WM every 20 TUs and the Beacon for each SSID is transmitted every 100 TUs
- B. One Beacon will be transmitted onto the WM every 100 TUs and the Beacons for each WLAN will be rotated
- C. Five Beacons will be transmitted back-to-back as a "Beacon Burst" every 100 TUs and Beacons for each WLAN will be transmitted in the order they were created
- D. One Beacon will be transmitted for each WLAN every 500 TUs

Answer: A

---

**QUESTION 38:**

What is indicated to a QoS AP when a QoS STA sets U-APSD Flag bits to 1 in association and Reassociation frames?

- A. Which access categories are scheduled

- B. Which access categories are both trigger and delivery enabled
- C. The maximum number of data frames that should be queued by the QoS AP for that QoS STA
- D. Which user priorities are mapped to access categories
- E. The number of TXOPs that are requested by this QoS STA

Answer: B

---

**QUESTION 39:**

According to the IEEE 802.11 standard (as amended), transmit power information is carried in which frames?

- A. Beacon frame
- B. Channel switch announcement frame
- C. Measurement report frame
- D. TCP Report frame
- E. Probe Response frame
- F. ADDTS Repose frame

Answer: A,D,E

---

**QUESTION 40:**

What are two techniques used for real-time tracking for wVoIP devices within a facility?

- A. RF calibration
- B. SNR provisioning
- C. Client positioning
- D. Triangulation
- E. RF fingerprinting

Answer: D,E

---

**QUESTION 41:**

Given: Certkiller .com has a VoIP implementation in place over the Ethernet Network at their facility. To watch for anomalies and no monitor statistics of VoIP Phone calls, Certkiller .com's administrator has configured a set of VoIP filters on their distributed Ethernet Protocol Analyzer. Certkiller .com has recently installed a dual-band IEE 802.11 controller-based WLAN system (with lightweight APs) that is configured for WMM and WPA-2 Enterprise and a wireless intrusion prevention system (WIPS). Considering the CCMP/AES encryption used on the WLAN segment, Certkiller .com's administrator knows that no Layer 3-7 data will be available via their WIPS.

What is the best way for the network administrator to gather call setup and jitter VoIP statistics for the wireless segment?

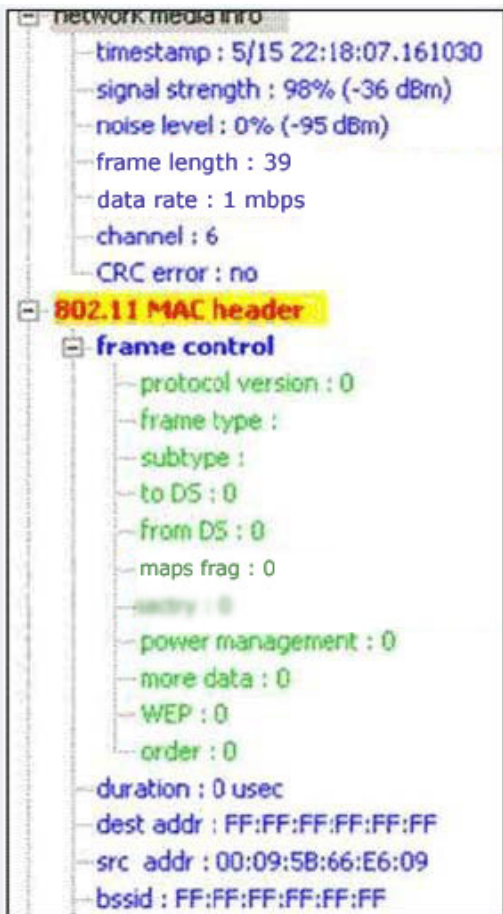
- A. Place an IEEE 802.11 voice analyzer in the middle of the STA-to-AP connection and gather statistics from management frames sent by each
- B. Configure the WIPS for frame slicing at 128 bits and measure statistics carried in the IEEE 802.11 frame header's QoS Control Field
- C. Have a Wireless network management system (WNMS) poll the access points for wVoIP statistics every second
- D. Connect an IEEE 802.11 voice analyzer to the wired network so that it can communicate with the VoIP server platform while it analyzes WLAN calls
- E. Since the data payload encryption is impossible to crack, the only useful statistics the administrator can gather is call duration

Answer: D

---

**QUESTION 42:**

Referencing this decode of an HR-DSSS frame, choose the statement that could be true:  
Exhibit:



- A. This frame was sent from one access point to another access point along a wireless distribution system
- B. This frame was sent to a wireless client station from a node on the wired segment and

WEP was not used

- C. This frame was sent from a wireless client station to request information about BSSs within range
- D. This frame was the first fragment in a series of 3 fragments (as part of a fragment burst) sent from a wireless client station to a station on the wired network
- E. This frame was sent from a wireless client station to an access point for the purpose of managing the access point's configuration

Answer: C

---

**QUESTION 43:**

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. 1 ACK, 1 CTS, 1 DATA, 3 SIFS
- B. 2 ACK, 1 RTS, 1 Data, 4 SIFS
- C. 1 DATA, 1 RTS, 2 SIFS, 1 DIFS, 1 ACK
- D. 1 RTS, 1 ACK, 1 CTS, 1 DATA, 3 SIFS
- E. 1 RTS, 1 CTS, 1 DATA, 2 ACK, 4 SIFS

Answer: A

---

**QUESTION 44:**

How long, in microseconds, is the required slot time announced by an AP in an ERP BSS when both HR-DSSS and ERP-OFDM client stations are associated to the AP?

- A. 2
- B. 20
- C. 9
- D. 10
- E. 4

Answer: B

---

**QUESTION 45:**

An IEEE 802.11 protocol analyzer using a single radio, dual-band 2.4 GHz (ERP)/ 5 GHz (OFDM) PC card is able to perform which tasks?

- A. Capture and decode all protection mechanism frames
- B. Capture and decode transmissions from 900 MHz a DSSS system
- C. Capture, decrypt and decode WPA2/CCMP compliant IEEE 802.1X/PEAP unicast data frames
- D. Capture and decode OFDM, HR-DSSS and ERP-OFDM transmissions simultaneously

E. Capture and decode IEEE 802.11-compliant FHSS access point transmissions in the 2.4 GHz ISM band

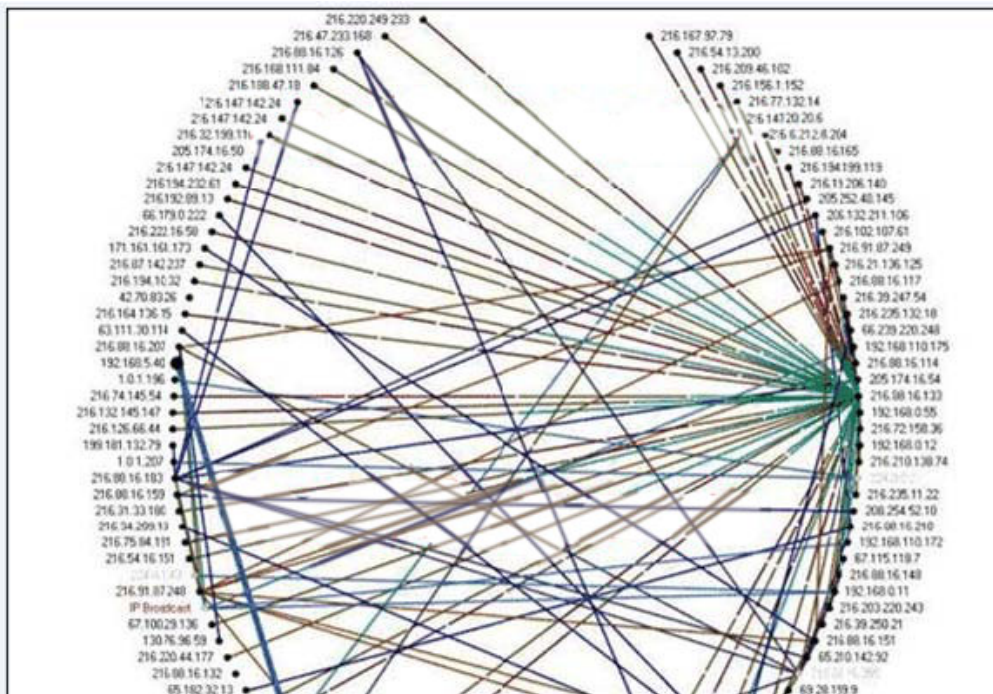
Answer: A

---

**QUESTION 46:**

In order to get a visual representation of conversations happening on the WLAN, a peer map like the one shown can be used. Which statements are true based on the peer map shown in the graphic?

Exhibit:



- A. This peer map displays MAC layer addressing information
- B. This peer map quickly identifies all access points in the WLAN
- C. This peer map illustrates the modulation in use for each peer connection
- D. This peer map distinguishes between the different security mechanisms used between each pair of network nodes
- E. This peer map shows how much data is traversing each peer connection relative to the other connections

Answer: E

---

**QUESTION 47:**

When an originator QoS STA wishes to initiate a Block ACK agreement with a recipient QoS STA, what is the first frame sent by the originator?

- A. ActionBAReq



- B. BlockAckSetupReq
- C. ADDBA Request
- D. BlockAckPolicyReq
- E. BlockAckReq

Answer: C

---

**QUESTION 48:**

To effect Preauthentication, a STA's supplicant sends an IEEE 802.1X/EAPoL Start Message. How is the EAPoL Start Message Addressed?

- A. DA = MAC of the default gateway; RA = Ethernet MAC of the targeted AP
- B. DA = BSSID of the targeted AP; RA = BSSID of the AP to which the STA is associated
- C. DA = MAC of the default gateway; RA= BSSID of the AP to which the STA is associated
- D. DA = BSSID of the targeted AP; RA = Ethernet MAC of the targeted AP

Answer: B

---

**QUESTION 49:**

Which parameters accurately describe the Beacon Interval field in the Beacon frame?

- A. 4-Octet length
- B. Measured in time units of 1024
- C. Value can range from 0 to 2007
- D. Indicates the exact time interval between Beacon transmission
- E. Indicates the desired time interval between TBTTs

Answer: B,E

---

**QUESTION 50:**

Choose the true statements regarding wireless network discovery processes for an HR-DSSS network.

- A. Access points send Beacon frames only on the HR-DSSS channel in the 2.4 GHz ISM band for which the access point is configured
- B. Client stations may continually send probe request frames on all HR-DSSS channels in the 2.4 GHz ISM band in a consecutive manner, regardless of their association state
- C. Client stations send Probe Request frames on all HR-DSSS channels in the 2.4 GHz ISM band in a consecutive manner until they receive at least 3 Probe Response frames
- D. Access points send Beacon frames on all HR-DSSS channels in the 2.4 GHz ISM band in a consecutive manner including the channel for which access point is configured

E. Client stations send Probe Request frames on all HR-DSSS 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

Answer: A,B

---

**QUESTION 51:**

ERP access points may provide which service to increase overall network performance in a BSS when only ERP stations are associated to the access point?

- A. Fast BSS Transition
- B. Short Slot Time
- C. 4-Way Handshake
- D. Arbitrary Beacon Spacing
- E. Short PLCP Preamble Support

Answer: B

---

**QUESTION 52:**

Which sets of IEEE 802.11 control frames have the same frame format and address positions?

- A. CTS and ACK
- B. RTS and ACK
- C. RTS and CTS
- D. RTS and CF-Poll
- E. PS-Poll and CF-End

Answer: A

---

**QUESTION 53:**

In which IEEE 802.11 frames is the SSID carried, provided the SSID is not specifically removed through software configuration by an Administrator?

- A. Association Request
- B. Reassociation Response
- C. Probe Response
- D. Disassociation
- E. Authentication
- F. Reassociation Request

Answer: A,C,F

---

**QUESTION 54:**

Which information elements are contained in an IEEE 802.11 Probe Request Frame?

- A. SSID
- B. Capability information
- C. Association ID
- D. Supported rates
- E. Status Code

Answer: A,D

---

**QUESTION 55:**

Which statements regarding an IEEE 802.11 Channel Switch Announcement frame are true?

- A. Channel switch announcement frames are the only place where the channel switch announcement element is found
- B. Channel switch announcement frames carry information elements from an AP to a STA in a BSS
- C. Channel Switch Announcement frames use the Action frame body format
- D. Channel switch announcement frames must be transmitted immediately following a DTIM Beacon so that dozing stations will receive the channel switch information
- E. Channel Switch Announcement frames are transmitted after the wireless medium has been idle for a PIFS

Answer: B,C

---

**QUESTION 56:**

In a Clause 18 (HR-DSSS) frame's PLCP header, what does the 16-bit length field indicate?

- A. The length of time in microseconds it will take to transmit the MPDU
- B. The size in octets of the MPDU being transferred in the PPDU
- C. The size in bits of the entire PPDU frame
- D. The length of time in kilo microseconds it will take to transmit the PSDU

Answer: A

---

**QUESTION 57:**

When site surveying for an IEEE 802.11 network that will carry both voice and data traffic, what makes co-channel IEEE 802.11 transmissions more determined than random

RF noise in some cases?

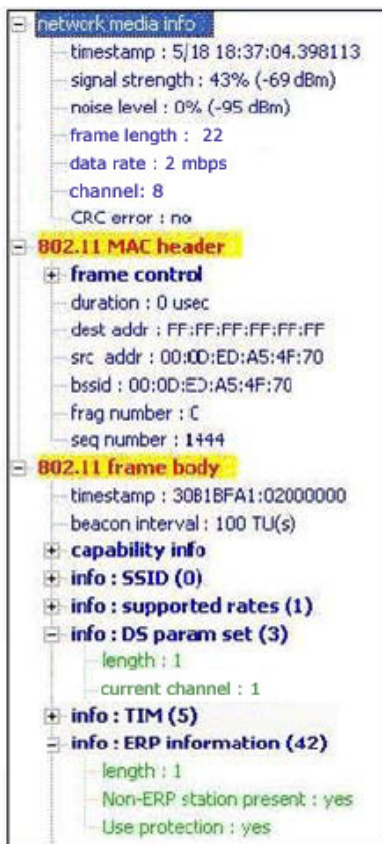
- A. Co-channel IEEE 802.11 transmissions increase channel utilization thus limiting the number of voice calls that can be handled by the WLAN
- B. Co-channel interfaces will cause self-configuring access points to constantly remap channel settings, which may disrupt or terminate voice calls
- C. Co-channel IEEE 802.11 transmissions cause excessive collisions, which can cause frame retransmissions to overflow jitter buffers
- D. Co-channel interface raises the RF noise floor higher than random RF noise, resulting in poor signal quality and high jitter

Answer: A

---

### QUESTION 58:

Given the IEEE 802.11 Beacon frame decode shown, determine which statement is true.



- A. The duration value of 0 usec means that this access point is operating in HEMM mode
- B. ERP mobile stations must use the RTS/CTS protocol before data transmissions
- C. The access point has both 1 Mbps and 2 Mbps configured as basic rates
- D. The access point is operating on channel 3
- E. This Beacon frame came from an ERP access point

Answer: E

---

**QUESTION 59:**

Laptop-1 transmits an MPDU using three addresses in the MAC header. Choose the correct statement.

- A. The BSS must be an infrastructure BSS because the third address is present and used for the MAC address of the access points radio
- B. The BSS must be Ad Hoc (IBSS) network because access points do not allow wireless stations to exchange MPDUs
- C. There is no enough information given to determine whether this is an infrastructure BSS or an Ad Hoc (IBSS) network
- D. The BSS must be infrastructure BSS because an Ad Hoc (IBSS) network uses only two addresses in the MAC header.

Answer: C

---

**QUESTION 60:**

When an IEEE 802.11 standard (as amended) compliant WLAN security solution is being used with IPSec/ESP for layered security, what will a WLAN protocol analyzer see as the security mechanism is use?

- A. Protocol 88:95
- B. CCMP, TKIP or WEP
- C. IPSec/ESP
- D. Both WEP and IPSec/ESP

Answer: B

---

**QUESTION 61:**

What events will cause an established TSPEC to be deleted by a AP?

- A. Traffic Stream inactivity timeout
- B. Reassociation of the non-AP QoS STA with another QoS AP
- C. Receipt of a DELBA frame from a non-AP QoS STA
- D. Receipt of an update TSPEC frame from a non-AP QoS STA
- E. Disassociation of the non-AP QoS STA using the TSPEC from the QoS BSS
- F. A controlled Access Phase (CAP) burst

Answer: A,B,E

---

**QUESTION 62:**

Determine which statement is true using the information in the analyzer trace shown.

Exhibit:

Packet	Source Physical	Dest. Physical	Protocol
227	00:90:96:5C:D7:D3	00:90:96:5C:D7:D5	PING Req
228	00:A0:F8:A2:16:8C	00:90:96:5C:D7:D3	802.11 Ack
229	00:90:96:5C:D7:D3	00:90:96:5C:D7:D5	PING Req
230	00:90:96:5C:D7:D5	00:A0:F8:A2:16:8C	802.11 Ack
231	00:90:96:5C:D7:D5	00:90:96:5C:D7:D3	PING Reply
232	00:A0:F8:A2:16:8C	00:90:96:5C:D7:D5	802.11 Ack
233	00:90:96:5C:D7:D5	00:90:96:5C:D7:D3	PING Reply
234	00:90:96:5C:D7:D3	00:A0:F8:A2:16:8C	802.11 Ack

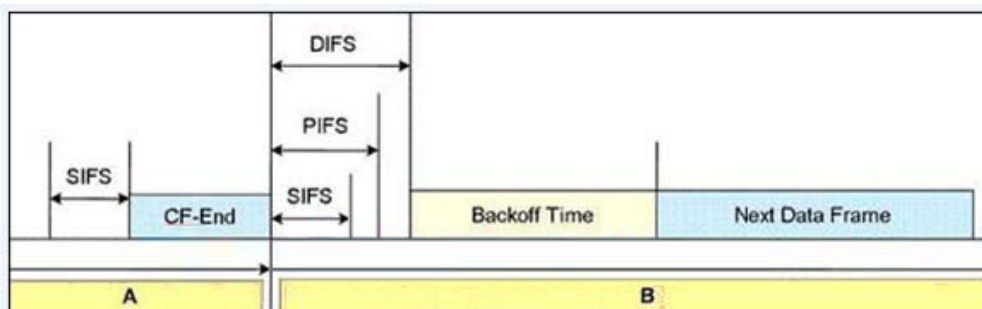
- A. This analyzer trace displays one PING Request/PING Reply packet exchange between two wireless client stations through an access point
- B. This analyzer trace displays two PING Request/PING Reply packet exchanges between two wireless client stations that are part of an IBSS
- C. This analyzer trace displays one PING Request/ PING Reply packet exchange between a wireless client station and a wired station through an access point
- D. This analyzer trace displays two PING Request/PING Reply packet exchanges between two wireless client stations through an access point

Answer: A

---

### QUESTION 63:

Referring to the diagram, match label boxes A and B with their appropriate name:  
Exhibit:



- A. A = Data Period, B = Interframe Space Period
- B. A = Contention-Free Period, B = Contention Window
- C. A = Contention-Free Period, B = Contention Period
- D. A = ATIM Window, B = Data Window
- E. A = Congestion Control Period, B = Arbitration Window

Answer: C

---

### QUESTION 64:

Many autonomous access points support IEEE 802.1Q VLAN tagging. When analyzing a WLAN system using IEEE 802.1Q tags, where can the VLAN tag number be seen?



- A. In the Frame Control Field of the MPDU header
- B. In the Beacon Management frame's Capabilities fixed field
- C. In the Sequence Control field of the MSDU
- D. In the PLCP header's Service Field
- E. In the Ethernet header on the wired port of the access point

Answer: E

---

**QUESTION 65:**

Given: The traffic Identifies (TID) is assigned to an MSDU in the layers above the MAC.

There are 16 possible TID values:

What statements is true about TID values?

- A. 12 values are assigned to traffic categories (TC) and 4 values are assigned to traffic streams (TS)
- B. All 16 values can be used for traffic categories (TC) or traffic streams (TS)
- C. 4 Values are assigned to traffic categories (TC) and 12 values are assigned to traffic streams (TS)
- D. 8 values are assigned to traffic categories (TC) and 8 values are assigned to traffic streams (TS)

Answer: D

---

**QUESTION 66:**

Given: Certkiller .com has an IEEE 802.11 WLAN secured by strong authentication (PEAP-EAP-MSCHAPv2) and encryption (CCMP/AES). They wish to implement wVoIP phones but have notices that the phones they have selected only supports WPA-Personal using TKIP/RC4.

How can Certkiller .com maintain their current level of data security while allowing the wVoIP phones network access?

- A. Enable application layer encryption for the voice protocol and implement a wireless intrusion prevention system (WIPS) on the wVoIP network segment
- B. Use a separate SSID for the wVoIP phones and map this new SSID to a separate VLAN on the wired infrastructure
- C. Use a secure DHCP server that can restrict access to layer 3 addresses based on user authentication
- D. Use MAC filtering to the network segment where the wVoIP phones will be used
- E. Using RBAC, allow only the appropriate voice protocol (SIP, H.323 etc) to a specific destination address on the network segment where the wVoIP phones will be used

Answer: B,E

---

**QUESTION 67:**

An administrator decides to optimize WLAN performance by adjusting the fragmentation threshold on each access point to a value must lower than the default of 2346 bytes. She notices that when wireless client stations are doing prolonged data transfers from a wired server, that downstream performance is better than it was before her adjustments. One problem she has not yet solved is why performance in the upstream direction has not been improved due to these adjustments. As a wireless protocol analyst, which of the following explanations would you give to the administrator?

- A. Fragmentation thresholds settings are only effective in the downstream direction (toward the wireless client stations) as specified by the IEEE 802.11 standard
- B. When configure fragmentation threshold values, it is important to enable RTS/CTS also in order to get effective bi-directional results
- C. Fragmentation thresholds are uniquely set on each wireless client station and access point and effect only transmissions from that node in particular
- D. Fragmentation is only supported bi-directionally when Antenna Diversity is enabled on both wireless client stations and the access points

Answer: C

---

**QUESTION 68:**

The IEEE 802.11 TSPEC element contains which parameters?

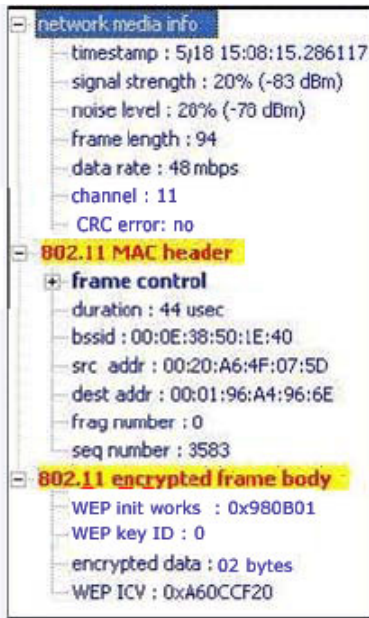
- A. Inactivity Interval
- B. Length
- C. Service Start Time
- D. Traffic Stream info
- E. Traffic Category info

Answer: A,B,C,D

---

**QUESTION 69:**

Given the IEEE 802.11 frame decode shown, which statements are true?  
Exhibit:



- A. The frame in the decode is an MMPDU
- B. The MSDU was successfully encrypted with WEP
- C. The frame is a layer 2 broadcast
- D. The 44 ec duration value is sufficient to cover the SIFS and ACK to follow
- E. The frame is the last fragment in a sequence of 3 fragments

Answer: B,D

---

### QUESTION 70:

Given: Certkiller .com is an auto parts manufacturer, and they have contracted you to perform a WLAN site survey t relieve their wVoIP quality problems. Your initial site survey shows a minimum signal strength of 75 dBm around the facility. This is less than the - 70 dBm recommended by the wVoIP manufacturer. Your recommend increasing each APs output power and after a follow-up site survey, the new minimum signal strength is 069 dBm. Unfortunately, the wVoIP problems are now worse than before. How can you remedy this problem?

- A. Change the polarity of each AP's antennas
- B. Move the APs closer together
- C. Increase each wVoIP phone's output power to overcome the RF interface sources
- D. Install directional antennas that focus the RF signal away from obstacles causing multipath
- E. Increase each APs output power even further to overcome the RF noise problems

Answer: D

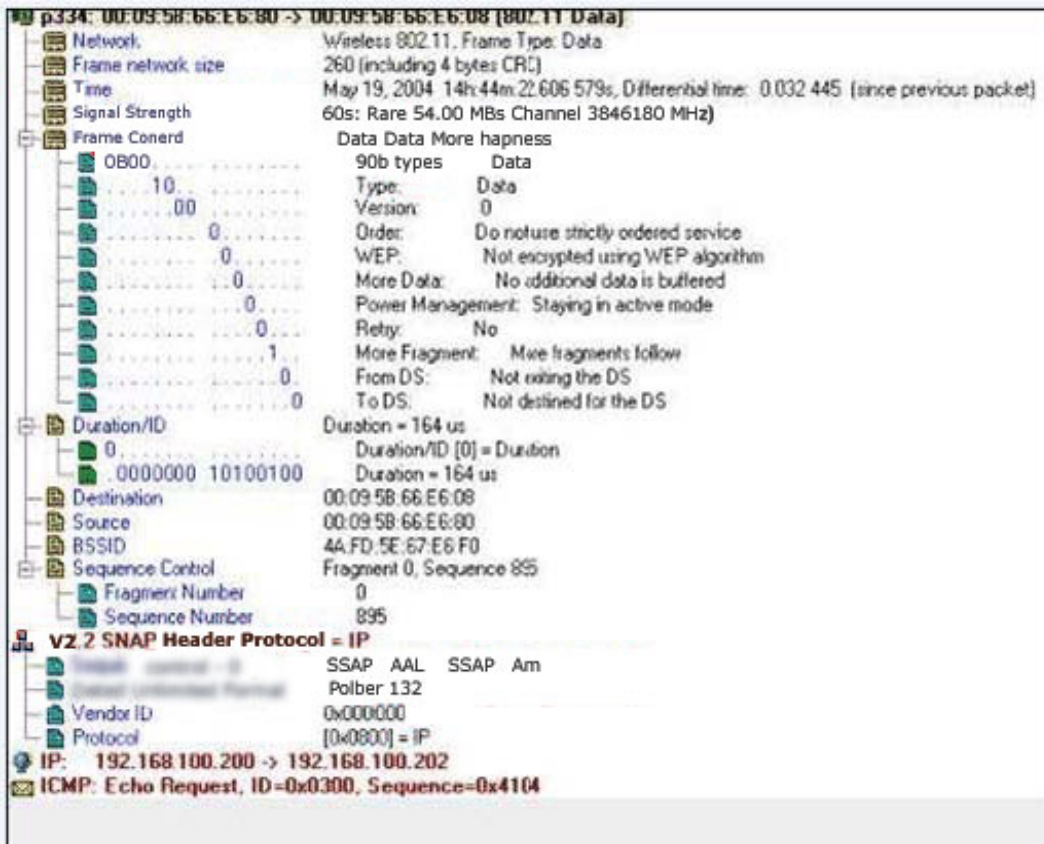
---

### QUESTION 71:

Given the screenshot shown, choose the statement that accurately describes what is being

seen by this protocol analyzer.

Exhibit:



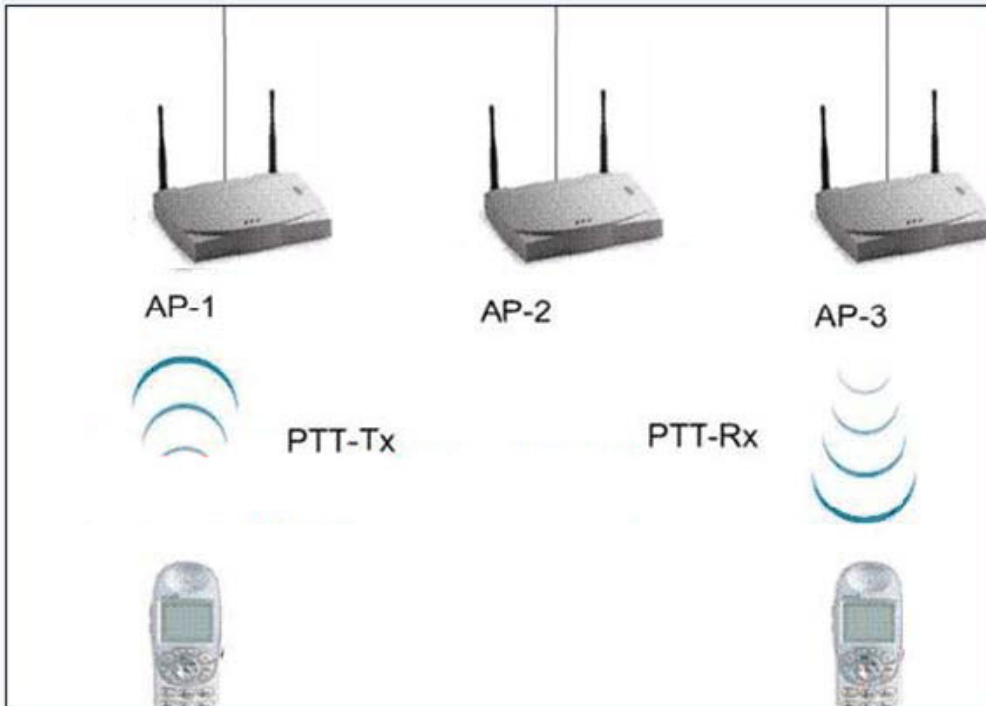
- A. The Duration field value's 164 microseconds is sufficient to protect only the SIFS and ACK that follow this frame
- B. A QoS STA sent an MPDU to another QoS STA via a Direct Link
- C. A QoS STA sent an MPDU to a non-QoS STA through an access point
- D. Bits (0-14) of the Duration/ID field in this frame indicates the AID of a source station
- E. The BSSID has been randomly generated

Answer: E

## QUESTION 72:

Given: Certkiller .com has implemented a HR-DSSS wVoIP network (as illustrated) and the HR-DSSS phones in use support Push-to-Talk (PTT). PTT adds 4% bandwidth utilization to the AP with the transmitting phone. PTT adds 1% bandwidth utilization to all other HR-DSSS APs in the system. Not all APs in the system are used to support wVoIP phones.

Exhibit:



In order to stop a PTT transmission from causing unnecessary utilization of APs participating in wVoIP (like AP-2 in the illustration), what can the network administrator do?

- A. Disable multicast routing on the wired infrastructure
- B. Create a separate SSID and VLAN for wVoIP phones and configure APs to support the wVoIP VLAN
- C. Enable Internet Group Management Protocol (IGMP) on the wired infrastructure network
- D. Create separate VLANs for unicast and multicast frames across the entire network infrastructure
- E. Disable the 1 Mbps data rate on all non-wVoIP APs so that multicast will not be transmitted onto the wireless network
- F. Disable QoS support on non-wVoIP APs

Answer: B,C

---

**QUESTION 73:**

The IEEE 802.11 standard ( as amended ) specifies two protection mechanism: RTS/CTS and CTS-to-self. Which statement is true regarding use of these two protection mechanism?

- A. Use of RTS/CTS introduces more latency than CTS-to-self due to a higher number of frames transmitted onto the wireless medium
- B. A CTS-to-self frame sent by a client station may reach fewer nodes than the RTS/CTS frame exchange

- C. RTS and CTS frames use short interframe spaces (SIFS) and CTS-to-self frames use PCF interframe spaces (PIFS)
- D. RTS and CTS frames get relayed through the access point, whereas the CTS-to-self frames do not
- E. All client stations in a basic service area (BSA) hear RTS, CTS and CTS-to-self frames, so either the RTS/CTS mechanism or CTS-to-self mechanism can be used with equal effectiveness

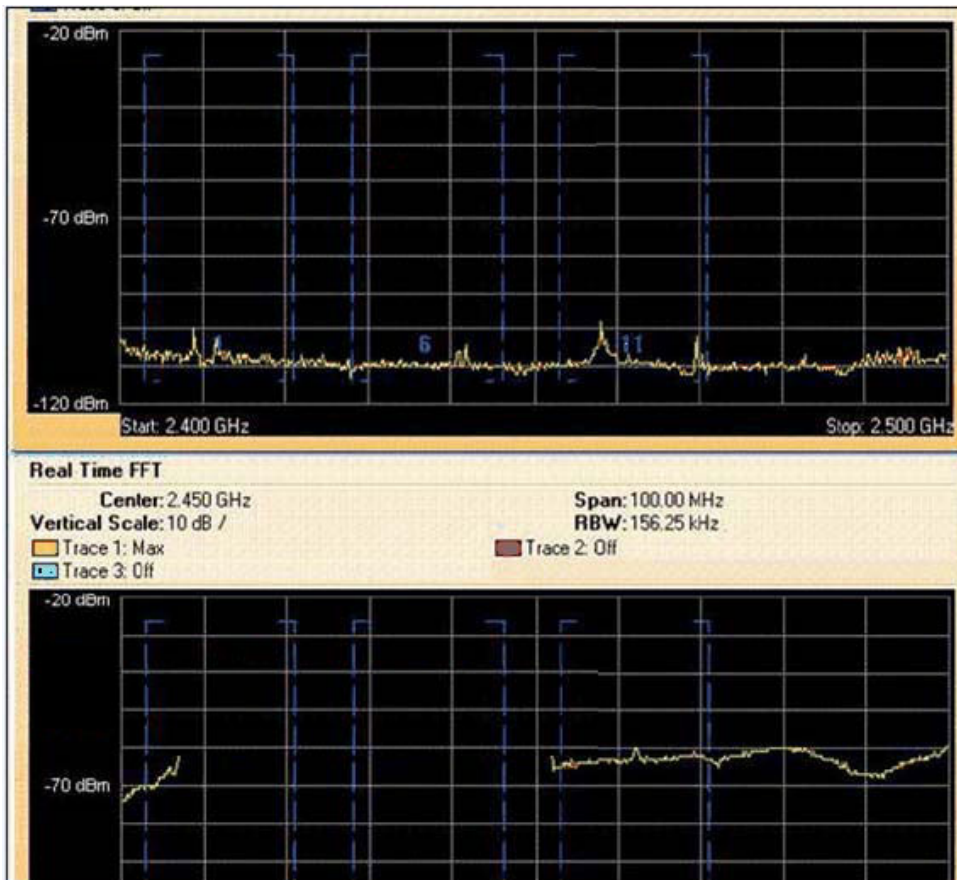
Answer: A,B

---

**QUESTION 74:**

Given: Certkiller .com recorded the 2.4 GHz band with a spectrum analyzer prior to installing their ERP WLAN. Image-A is how the band appeared prior to the WLAN installation. Image-B is how the band appears now and all channels on their WLAN have ceased to function.

Exhibit:



What is the best explanation as to why their WLAN is no longer functioning properly?

- A. A malfunctioning IEEE 802.11 OFDM radio card is transmitting continuously
- B. A wideband RF power source is corrupting all IEEE 802.11 transmissions
- C. A manual site survey tool is actively testing the throughput of their WLAN



D. A new microwave oven was installed in the cafeteria

Answer: B

---

**QUESTION 75:**

Which information elements are contained in an IEEE 802.11 Probe Request Frame?

- A. SSID
- B. Capability information
- C. Association ID
- D. Status Code
- E. Supported rates

Answer: A,E

---

**QUESTION 76:**

Which statements are true regarding the duration/Id field in unfragmented Data frames?

- A. The duration/ID field is measured in microseconds and always rounded up to the next highest integer
- B. The duration/ID field specifies the amount of time required for the SIFS and ACK that follow the data frame
- C. If the More Fragments bit in the frame control field of the MAC header is set to 0, then the duration/ID field is also set to 0
- D. Valid frames with a duration/ID field value of less than 32.768 are used by unintended recipients to update their NAV
- E. The duration/ID field is always set to zero unless Data is sent to the broadcast address of FF:FF:FF:FF:FF:FF
- F. When a Data frame is sent to a multicast address, the duration/ID field is always set to 32.768

Answer: A,B,D

---

**QUESTION 77:**

What does a TXOP Limit value of 0 in the EDCA parameter set included in a QoS AP's or Probe Response frames indicates?

- A. It indicates that one or more MSDUs or MMPDUs must be transmitted at the lowest rate during each TXOP
- B. It indicates that QoS STAs must wait for the HC to transmit a Polled TXOP before they can transmit MSDUs or MMPDUs
- C. It indicates that no MSDUs or MMPDUs may be transmitted by a non-pollable QoS STA

- D. It indicates that a single MSDU or MMPDU may be transmitted at any rate for each TXOP
- E. It indicates that QoS STAs may transmit voice MPDUs (Access Category 7,8) during TXOPs

Answer: D

---

**QUESTION 78:**

When the To DS bit is set to 1 and the From DS bit is set to 0 in the frame control field of an IEEE 802.11 data frame, what might this indicate about the infrastructure and the wireless conversation?

- A. A wireless client station must be sending data directly to the access point for the purpose of managing the access point
- B. A wireless client station could be sending data to a wired station through an access point
- C. A wireless client station could be sending data to a wireless client station across an access point
- D. A wireless client station could be sending data directly to another wireless client station as part of a QoS BSS direct link
- E. A wireless client station must be sending data to a wireless station where the frame has to transverse a Wireless Distribution System (WDS)

Answer: B,C

---

**QUESTION 79:**

In the analyzer trace shown, the TBTT is nominally 102.5 milliseconds. Why does the Beacon transmission interval vary?

Exhibit:

Packet	Source	Destination	BSSID	Channel	Signal	Data Rate	Delta Time	Protocol
54	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	74%	2.0	00.102544	802.11 Beacon
55	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102451	802.11 Beacon
56	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102253	802.11 Beacon
57	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102357	802.11 Beacon
58	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102515	802.11 Beacon
59	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102342	802.11 Beacon
60	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102494	802.11 Beacon
61	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102280	802.11 Beacon
62	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102548	802.11 Beacon
63	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	74%	2.0	00.102541	802.11 Beacon
64	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102379	802.11 Beacon
65	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	74%	2.0	00.102312	802.11 Beacon
66	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	72%	2.0	00.102421	802.11 Beacon
67	00:A0:F8:A2:16:8C	FF:FF:FF:FF:FF:FF	00:A0:F8:A2:16:8C	6	75%	2.0	00.102408	802.11 Beacon

- A. The DCF interframe space (DIFS) is nominally 50, but typically varies by as much as 10 causing delays in Beacons
- B. Beacon frames vary in size and therefore some take slightly longer to send than others
- C. This is a trace of an ERP network where both HR-DSSS and ERP nodes are active on the network. The access point is changing slot times from short to long as needed
- D. The access point must compete to gain access to the RF medium in order to transmit a

Beacon

Answer: D

---

**QUESTION 80:**

As a consultant for Certkiller .com, you have been asked to go to a customer site to troubleshoot a problem with intermittently slow throughput on an indoor ERP WLAN. You take your dual-band 2.4 GHz (ERP) / 5 GHz (OFDM) IEEE 802.11 protocol analyzer along as a troubleshooting tool. Which event will the protocol analyzer allow you to see that you would like not see without it?

- A. Intermittent narrowband RF interference
- B. Individually stations repeatedly disconnecting from their access points
- C. An abnormally high amount of data rate changes on particular stations
- D. The 2.4 GHz medium is saturated due to too many bandwidth-intensive applications

Answer: B,C,D

---

**QUESTION 81:**

Given: The graphic is taken from a spectrum analyzer:

Exhibit: image028.jpg

What type (s) of wireless system (s) is/are illustrated?

- A. An IEEE 802.11 HR-DSSS system on channel 6 and a Bluetooth 2.0 EDR system
- B. An IEEE 802.11 ERP system on channel 6 and an IEEE 802.11 FHSS system
- C. An IEEE 802.11 ERP system using TPC and DFS features in the 2.4 GHz band
- D. An RFID system using HR-DSSS on channel 6

Answer: B

---

**QUESTION 82:**

According to the IEEE 802.11 standard (as amended), what is one structural difference between a MAC Protocol Data Unit (MPDU) and a MAC Management Protocol Data Unit (MMPDU)?

- A. The MMPDU frame body is limited to 200 bytes, whereas the MPDU frame body can carry up to 2304 bytes
- B. The MPDU header always places the BSSID in the first address field, but in the MMPDU the BSSID can be found in any of the address fields
- C. An MMPDU header may only contain three address fields, but an MPDU may have four address fields
- D. The MPDU frame's FCS field is 4 bytes, while the MMPDU frame's FCS field is 8 bytes

E. Both the MPDU and MMPDU have a QoS Control (QC) field, but all bits of the MMPDU's QC field are always 0

Answer: C

---

**QUESTION 83:**

What statements about ERP slot times are true?

- A. The optional 9 slot time may not be used if the BSS has one or more associated non-ERP stations
- B. When the ERP-OFDM modulation is in use, the SIFS and slot time are always equal
- C. When the ERP DSSS-OFDM modulation is in use all stations may use the 9 slot time
- D. All interframe spaces are calculated based on the slot time value
- E. When HR-DSSS is in use in an ERP BSS, a slot time consists of a RX-to-TX turnaround time and an energy detect time totaling 20

Answer: A,E

---

**QUESTION 84:**

What IEEE 802.11 MAC Layer function is illustrated by the following diagram?

Exhibit: image002.jpg

- A. Fragment Brusing
- B. HCCA Polling
- C. CP Regulated Spacing
- D. Unscheduled APSD
- E. Sequential Acknowledgements

Answer: A

---

**QUESTION 85:**

Before accurate statistical troubleshooting with a wireless protocol analyzer can be performed on a WLAN, which task must be completed?

- A. Security Policy Implementation validation
- B. QoS data queuing verification
- C. Baseline traffic analysis
- D. IEEE 802.11 protocol version identification

Answer: C

---

**QUESTION 86:**

What method is used in an IEEE 802.11 WLAN to configure a QoS AP to deliver queued frames to a QoS STA during an unscheduled service period?

- A. The WLAN controller's WMM access categories are manually configured by an administrator
- B. A QoS STA sends a (Re)Association frame to the QoS AP with the U-APSD Flag subfields set to 1
- C. The QoS STA's client utility WMM access categories are manually configured by an administrator
- D. A QoS STA sends a TSPEC Request Frame to the QoS AP specifying its traffic flow requirements before using power management features

Answer: B

---

**QUESTION 87:**

In the HR-DSSS Analyzer trace shown, what explains why the probe request frame and probe response frame are transmitted at different data rates.

Exhibit: image008.jpg

- A. The client station's output power is set at approximately half of the access point's output power. The higher output power of the access point allows it to successfully transmit at higher data rates than the client station
- B. The client station sends a probe request frame using any one of its supported rates, which in this case is 1 Mbps. The access point sends a Probe Response frame using any supported rate common to both client stations, which in this case is 2 mbps
- C. An RF interface source is located near the client station sending the probe request frame causing it to slow its transmission rate in order to successfully communicate with the access point
- D. HR-DSSS client stations always send probe request frames at 1 mbps regardless of configuration. The access point is required to send probe response frames at its highest basic rate, which in this case is 2 mbps

Answer: B

---

**QUESTION 88:**

In the HR-DSSS frame decode shown, why does the protocol analyzer not show "(basic)" beside 5.5 and 11 Mbps data rates?

Exhibit: image022.jpg

- A. 5.5 and 11 Mbps data rates are not supported on this access point
- B. 5.5 and 11 Mbps data rates may only be used when all client stations associated to the access point are connected at a data rate of at least 5.5 Mbps
- C. 5.5 and 11 Mbps data rates are not required by this BSS
- D. Only two data rates may be configured as "basic" rates and the administrator has

chosen to select 1 and 2 mbps as basic rates

Answer: C

---

**QUESTION 89:**

Shown is a screenshot of a wireless protocol analyzer displaying the decode information for a single 802.11 encrypted data + CF - Poll Frame. The infrastructure BSS on which this information was captured is using WEP and this particular frame was sent from a client station (STA) to an access point (AP).

Exhibit: image020.jpg

As a protocol analyst, how would you explain the existence of this frame on the wireless medium given the information in the decode?

- A. The access point is operating as a repeater and clients must poll repeater access points in order to transmit data frames through them
- B. The frame was sent by a client station that does not comply with IEEE HR-DSSS standard to an access point that is Wi-Fi certified
- C. The frame was misinterpreted based on insufficient information received by the analyzer due to frame corruption
- D. The IEEE 802.11 network is using both version 1 and version 2 protocols simultaneously. This unexpected frame is from the version 2 protocol set

Answer: C