Vendor: CWNP

Exam Code: PW0-205

Exam Name: Certified wireless analusis professional(cwap)

Version: Demo

QUESTION NO: 1

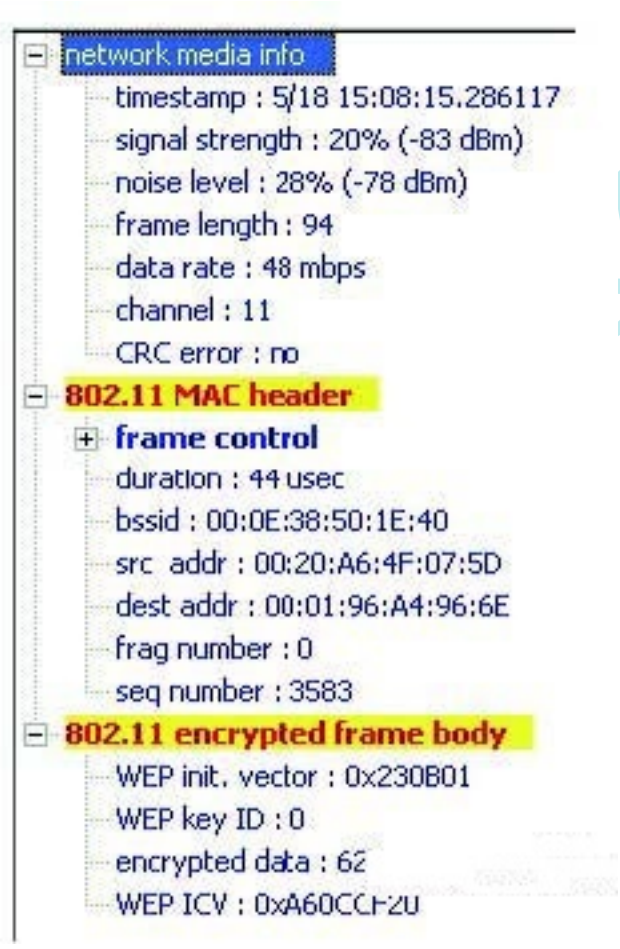
Before accurate statistical troubleshooting with a wireless protocol analyzer can be performed on a wireless LAN, which of the following must be completed?

A. Directional traffic filtering
B. Operational traffic policy
C. Traffic injection analysis
D. Baseline traffic analysis
E. Quality of Service (QoS) design

Answer: D

QUESTION NO: 2

Given the 802.11 frame decode shown, which of the following statements are true.



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

Answer: C,E

QUESTION NO: 3

According to the IEEE 802.11 standard, 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 2312 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. The MPDU frame FCS field is 4 bytes, while the MMPDU frame FCS field is 8 bytes.
D. An MMPDU header may only contain three address fields, but an MPDU may have four address fields.

Answer: D

QUESTION NO: 4

An administrator for ABC Company has noticed an intermittently high number of retransmissions on their purely 802.11g wireless LAN coming from some of the access points near the break room, especially when wireless stations are using the FTP protocol to pull down large sales report data files from the company's FTP server. The administrator decides to hire a consultant to test some configuration changes hoping to improve performance of the wireless LAN. As the consultant, what test do you recommend performing?

A. Change the fragmentation threshold value on all access points near the break room to a smaller value.
B. Change the DTIM interval in all access points near the break room to a shorter interval.
C. Set all supported data rates on the access points near the break room to Basic
D. Enable support of short preambles on all access points near the break room.
E. Decrease the output power on all access points and stations throughout the ESS to form smaller cells in case there is a hidden node.

Answer: A

QUESTION NO: 5

In the 802.11 series of wireless LAN standards, there is a medium access rule regarding formatting of preambles in response to MMPDUs. What does this rule state?

A. The rule states that if a mixed set of stations (long/short preamble settings) are associated to the access point, only long preambles may be used for response-MMPDUs.
B. The rule states that only long preambles may be used in response-MMPDUs regardless of any other factor.
C. The rule states that short preambles should be used in response-MMPDUs until a single station associates to the BSS using the long-preamble format, after which, only long preambles are used.
D. The rule states that a response-MMPDU must be sent with the same type of preamble as the request-MMPDU that triggered the response-MMPDU.
E. The rule states that only short preambles may be used in response-MMPDUs regardless of any other factor.

Answer: D

QUESTION NO: 6

Determine which of the following statements is true using the information in the analyzer trace shown.

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

Answer: C

QUESTION NO: 7

ABC Company is having throughput problems on their 802.11b wireless LAN. A wireless administrator has noticed in the wireless client station utilities that the MAC CRC Error count is higher on stations with problems than those client stations without problems. A high MAC CRC

Error count is NOT attributable to which of the following?

A. Co-located PCF and DCF mode access points that are using non-overlapping 2.4 GHz channels
B. High multipath conditions due to bounced signals
C. 2.4 GHz ISM band interference from sources such as wireless phones
D. Collisions due to dense population of client station adapters
E. Overlapping access point coverage on a single channel

Answer: A

QUESTION NO: 8

Which three of the following are true regarding the duration/ID field in unfragmented Data frames?

A. The duration/ID field is always set to zero unless Data is sent to the broadcast address of FF:FF:FF:FF:FF:FF.
B. When a Data frame is sent to a multicast address, the duration/ID field is always set to 32,768.
C. The duration/ID field is measured in microseconds and always rounded up to the next highest integer.
D. 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
E. Valid frames with a duration/ID field valueof ?32,767 are used by receiving stations to update their NAV.
F. The duration/ID field is set to include the SIFS and ACK frame that follow the data frame.

Answer: C,E,F

QUESTION NO: 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 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.
B. A DTIM period of 0 means that every TIM is a DTIM.
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 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.
E. The first Beacon sent during a CFP must contain a DTIM
F. 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.

Answer: C,E

QUESTION NO: 10

ABC Company has two access points (AP-1 and AP-2) connected to an Ethernet hub. Which of the following describes how the access points will handle a frame sent from a wired node to a wireless station associated to AP-1?

A. AP-1 will check its association table and broadcast the frame onto the wireless medium. AP-2 will check its association table and drop the frame.
B. AP-1 and AP-2 will both issue ARP frames onto the wireless medium, and if they receive a reply, they will broadcast the data frame onto the wireless medium.
C. AP-1 will automatically forward the frame onto the wireless medium. AP-2 will notify the wired node that it does not have an association ID for the station.
D. AP-1 and AP-2 will automatically forward the frame onto the wireless medium regardless of any other criteria.
E. AP-1 will check its association table and broadcast the frame onto the wireless medium. AP-2 will check its switching table and forward the frame to AP-1.

Answer: A

QUESTION NO: 11

An 802.11b PPDU's preamble consists of two fields and can collectively be considered "long" or "short" by the 802.11b standard. Which of the following is true regarding the PLCP preamble?

A. An 802.11b access point that supports both long and short preambles may allow stations that are using different preamble lengths to communicate through it simultaneously.
B. A short preamble uses a Sync field of 40 bits, and stations and access points must have matching preamble lengths in order to communicate.
C. Long and short preamble lengths are both variable depending on the modulation in use on the network, and access points always inform stations of the preamble length in use on the network.
D. When short preambles are being used, the Sync and SFD fields both consist of 16 bits. Only access points have configurable preamble lengths.

E. A long preamble uses a Sync field of 128 bits, and both stations and access points may have configurable preamble lengths.
F. 802.11g stations associating to 802.11b access points must use the DSSS preamble length specified by the access point.

Answer: E,F

QUESTION NO: 12

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

Answer: B

QUESTION NO: 13

Which of the following information will a wireless LAN protocol analyzer capture if it can only capture Data Link information?

A. Source IP Address
B. Null Function Data frames
C. TCP SYN datagram
D. ShortInterframe Spaces
E. Sequence Control fields

Answer: B,E

QUESTION NO: 14

In an 802.11b PLCP header, what does the 16-bit length field indicate?

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

Answer: D

QUESTION NO: 15

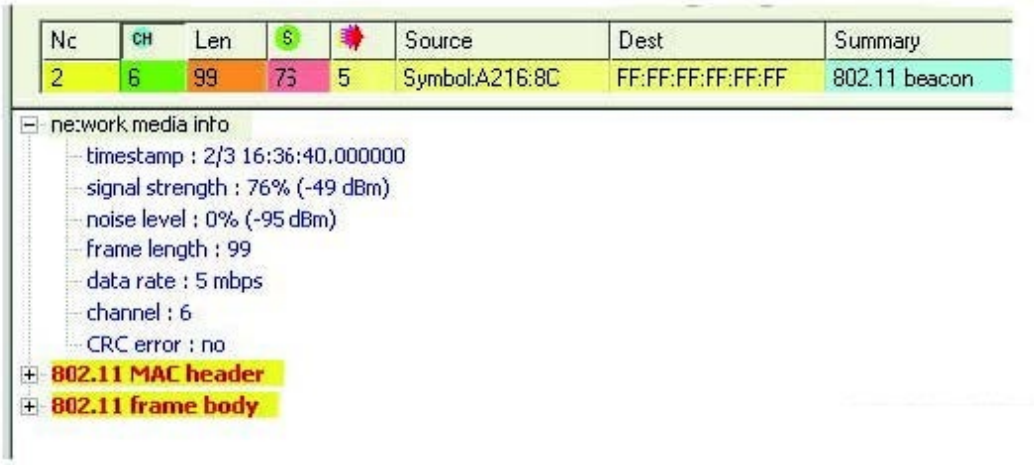
In the frame decode shown, 1, 2, 5.5, and 11 Mbps are all shown as supported data rates. 1 and 2 Mbps are shown with (basic) beside them. What does (basic) mean in this context?

A. Basic rates are only used for multicast traffic, and do not affectunicast traffic.
B. Basic rates are those rates required by the access point to participate in a Basic Service Set.
C. The highest data rate set to basic is automatically used to send broadcast traffic such as Beacon Management frames.
D. Basic rates are optional data rates, often used for assuring connectivity for those stations that are at a significant distance from the access point.

Answer: B

QUESTION NO: 16

Using the wireless LAN protocol analyzer's frame decode shown as a reference, which of the following access point data rate configuration settings must be correct?



A. Basic: 11, 5.5, 2 Mbps - Supported 1 Mbps
B. Basic: 2, 1 Mbps - Supported: 11, 5.5 Mbps
C. Basic: 11 Mbps - Supported: 5.5, 2, 1 Mbps
D. Basic: None - Supported: 11, 5.5, 2, 1 Mbps
E. Basic: 11, 5.5 Mbps - Disabled: 2, 1 Mbps

Answer: E

QUESTION NO: 17

Given one screenshot of a fragment burst and another screenshot of one of the data frames decoded, determine which statements are true.

A. The sequence number of 169 shown inthe decode is unique to the communication between the transmitting station and the access point.
B. The transmitter of this frame is allowed to change its power management mode toActive.D.The transmitter of this frame is allowed to change its power management mode to Active.
C. The frame decode shown is of the second fragment in the sequence.

D. The duration value of 508usec is exactly enough to reserve the medium on behalf of the SIFS and ACK to follow this fragment
E. This fragment is aretransmission.E.This fragment is a retransmission.E.This fragment is a retransmission.
F. The RTS/CTS threshold value on the transmitter is set to 500 bytes.

Answer: A,B

QUESTION NO: 18

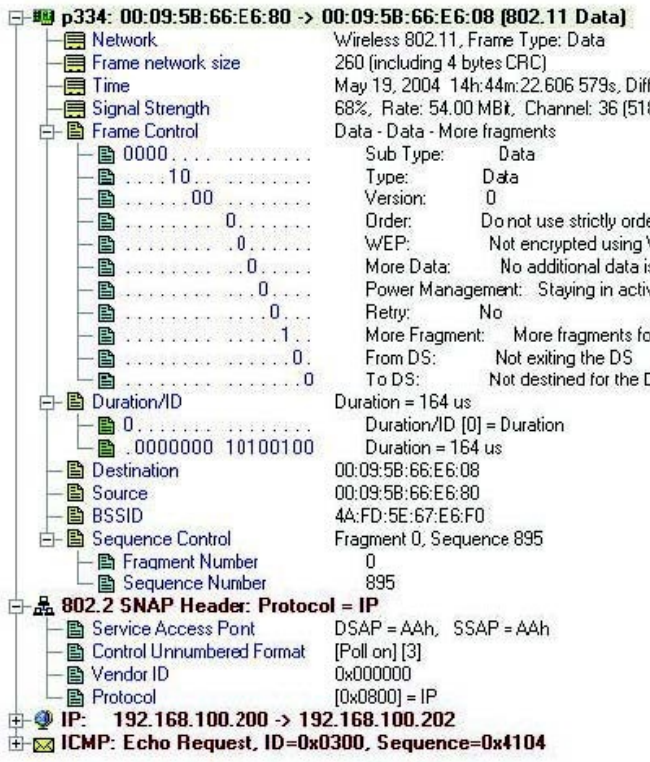
When an 802.11 station operating in Power Save mode with a ReceiveDTIMs parameter of TRUE receives a beacon containing a DTIM indicating queued broadcast traffic, what task does the 802.11 standard require the client station to perform?

A. The client station must send an ATIM frame to the access point if the station is the first AID in the DTIM list.
B. The client station must arbitrate for the medium and immediately issue an RTS directed to the access point with the NAV set to a value of 32,768.
C. To remain awake to receive the broadcast frame(s) to follow the beacon that contains the DTIM.
D. The client station must broadcast a CTS-to-Self frame indicating the station need to control the medium long enough to receive all of the broadcast frames.
E. The client station must send a CF-Poll Response frame to the access point with the Reason Code set to 0x00.
F. The client station must send a PS-Poll frame to the access point for every broadcast frame it receives with the More Data bit set to one.

Answer: C

QUESTION NO: 19

Given the screenshot shown, choose the statement that accurately describes what is being seen by this protocol analyzer.



A. One wireless station sent an Echo Request (PING) to another wireless station through an access point.

B. The BSSID has been randomly generated.

C. The Duration field value's 164 microseconds is sufficient to reserve the RF medium for only the following frames: SIFS, ACK.

D. Bits (0-14) of the Duration/ID field in this frame indicates the AID of the source station

Answer: B

QUESTION NO: 20

Given the displayed wireless protocol analyzer trace, which of the following is true?

Source Physical	Dest. Physical	BSSID	Flags	Channel	Signal	Data Rate	Size	Protocol
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	*	1	99%	1.0	146	802.11 Probe Rsp
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	91%	1.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70	*	1	91%	1.0	34	802.11 Auth
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	99%	1.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	*	1	99%	11.0	34	802.11 Auth
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	91%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70	*	1	90%	1.0	118	802.11 Assoc Req
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	99%	1.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	*	1	97%	11.0	91	802.11 Assoc Rsp
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	90%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	97%	11.0	82	EAP Request
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	90%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70		1	90%	11.0	82	EAP Response
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	96%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	96%	11.0	82	EAP Request
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	80%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70		1	90%	11.0	77	EAP Response
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	94%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	96%	11.0	82	EAP Success
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	80%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70		1	90%	11.0	82	EAP Request
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	94%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	94%	11.0	82	EAP Response
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	83%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	94%	11.0	135	EAPOL-Key
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	80%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70		1	90%	11.0	159	EAPOL-Key
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	96%	11.0	14	802.11 Ack
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		1	96%	11.0	161	EAPOL-Key
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		#	1	80%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	00:0D:ED:A5:4F:70		1	90%	11.0	135	EAPOL-Key
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	94%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	W	1	91%	11.0	384	802.11 WEP Data
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	100%	11.0	14	802.11 Ack
00:40:96:A1:9A:F9	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	W	1	91%	11.0	84	802.11 WEP Data
00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		#	1	100%	11.0	14	802.11 Ack

A. Both 00:40:96:A1:9A:F9 and 00:0D:ED:A5:4F:70 are operating in Ad Hoc mode using WPA-compliant 802.1X/EAP authentication.
B. 00:0D:ED:A5:4F:70 is a client station sending unicast data frames to a network node on the wired LAN.
C. 00:40:96:A1:9A:F9 is a client station performing a successful 802.1X/EAPreauthentication.
D. 00:40:96:A1:9A:F9 is a station sending encrypted broadcast data using an encryption key generated by the authenticator.
E. FF:FF:FF:FF:FF:FF is the access point, and data encrypted with static WEP is being sent from a wired station to the wireless station 00:40:96:A1:9A:F9.

Answer: D

QUESTION NO: 21

In the 802.11b standard, the PLCP header Service field has a Modulation Selection bit. Which of the following are true regarding use of the Modulation Selection bit?

A. The Modulation Selection bit is used by the access point in CF-End frames to note which modulation will be used for Data frames in the contention period to follow.
B. Based on the setting of the Modulation Selection bit and the value in the Signal field, the modulation to be used can be uniquely determined.
C. Based on the Modulation Selection bit in received Data frames, the receiving station can determine which modulation to use when sending acknowledgements.
D. The Modulation Selection bit is used to determine whether CCK or PBCC is in use for any speed where either could be used.
E. The Modulation Selection bit is used to determine which modulation will be used to send the entire PPDU.

Answer: B,D

QUESTION NO: 22

What is an advantage of being able to fragment MSDUs and MMPDUs on a wireless network?

A. Increased throughput due to interference from other 802.11 stations.
B. Decreased translation time between 802.3 and 802.11 networks at the access point.
C. Increased throughput in an 802.11b/g mixed mode environment.
D. Decreased number of 802.11 control and management frames required for transmission.
E. Increased throughput in a clean RF environment
F. Decreased retransmission overhead in a noisy RF environment.

Answer: F

QUESTION NO: 23

In compliance with the 802.11g standard, access points may provide which services to increase overall network performance in an OFDM-only environment?

A. Arbitrary Beacon Spacing
B. DownstreamQoS
C. Short Slot Time
D. Short PLCP Preamble support
E. Fast Sleep Recovery

Answer: C

QUESTION NO: 24

Which features of a wireless LAN protocol analyzer allow troubleshooters to monitor network events that are happening while the troubleshooters are not watching the analyzer user interface?

A. Event Triggers
B. Node Statistics
C. Notifications
D. Peer Map
E. Trending Analysis
F. Alarms

Answer: A,C,F

QUESTION NO: 25

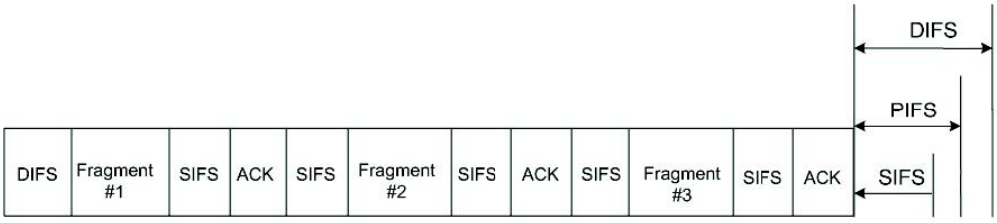
The 802.11 standard allows for frame fragmentation due to an unreliable medium. Which two fields in the 802.11 frame are involved in numbering data frame fragments and notifying the receiving station when all of the fragments of a data frame have been received?

A. Ordered Service field
B. Sequence Control field
C. Frame Control field
D. ERP Information field
E. Capability Information field
F. DS Parameter field

Answer: B,C

QUESTION NO: 26

What 802.11 MAC layer function is illustrated by the following diagram?



A. Sequential Fragmentation
B. PCF mode polling
C. Fragment Bursting
D. Sequential Acknowledgements
E. CP Regulated Spacing

Answer: C

QUESTION NO: 27

When operating in an 802.11b/g mixed mode environment in which both 802.11b and 802.11g client stations are present and transmitting data on the network, which of the statements below are accurate concerning the 802.11g access point responsibilities in the Basic Service Set?

A. The access point will alternate transmitting beacons using long and short preambles so that client stations using either preamble length can associate.

B. The access point may transmit beacons using a short preamble only if all of the client stations in the BSS have indicated support for short preambles.
C. If beacons are transmitted using short preambles, all associated client stations are required to transmit all data frames using short preambles.
D. The access must transmit beacons using a short preamble in a mixed mode environment. Client stations not supporting short preambles will not be able to associate.

Answer: B

QUESTION NO: 28

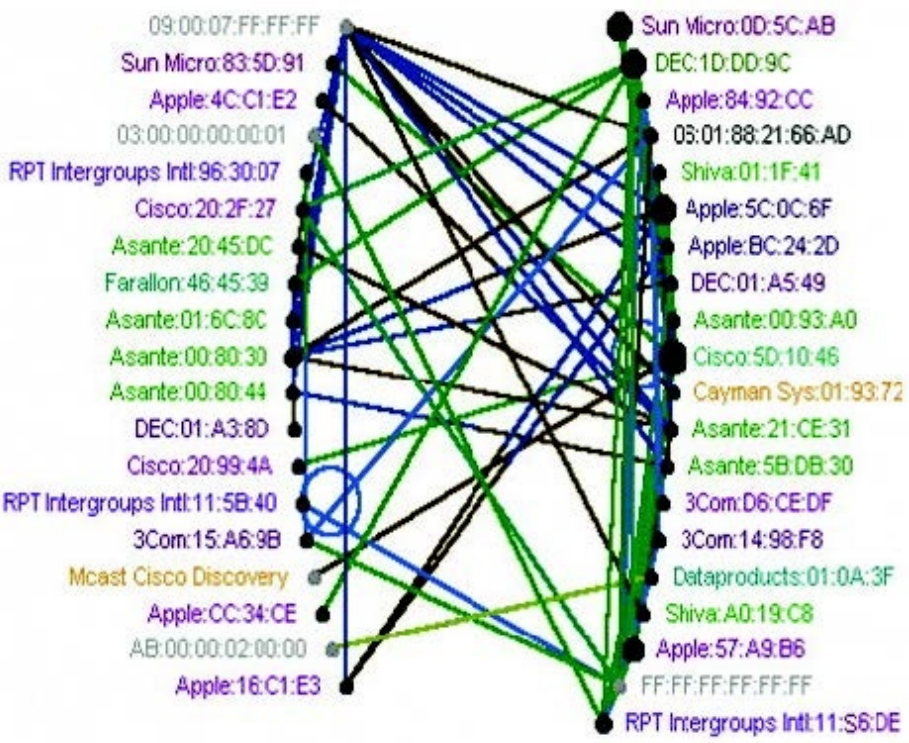
The More Fragments subfield is found in which 802.11 frame field?

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

Answer: B

QUESTION NO: 29

In order to get a visual representation of conversations happening across a wireless LAN, a Peer Map like the one shown can be used. Which of the following is true of most peer maps?



Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

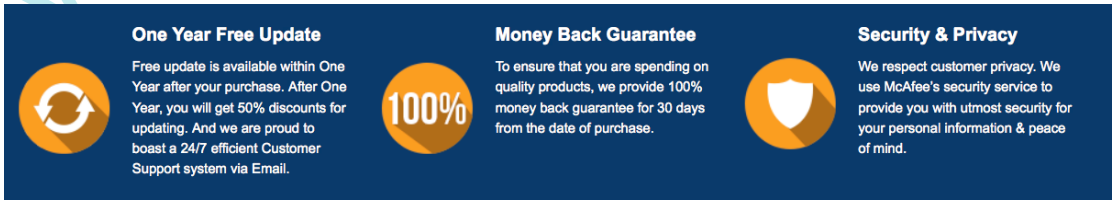
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.