QUESTIONS & ANSWERS

Kill your exam at first Attempt

KILL EXAMS

PW0-300 Dumps
PW0-300 Braindumps
PW0-300 Real Questions
PW0-300 Practice Test
PW0-300 dumps free

CWNP

PW0-300

Certified Wireless Network Expert

Answer: B, E

QUESTION: 130
Which parameters accurately describe the Beacon Interval field in the Beacon frame?

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

Answer: D, E

QUESTION: 131
Exhibit:

Packet	Source Physical	Dest. Physical	BSSID	Channel	Data Rate	Size	Protocol
59	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
60	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
61	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
62	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
63	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	11.0	260	PING Req
64	00:0D:ED:A5:4F:70	00:09:5B:66:E6:80		6	11.0	14	802.11 Ack
65	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	11.0	260	802.11 Frag
66	00:0D:ED:A5:4F:70	00:09:5B:66:E6:80		6	11.0	14	802.11 Ack
67	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	11.0	260	802.11 Frag
68	00:0D:ED:A5:4F:70	00:09:5B:66:E6:80		6	11.0	14	802.11 Ack
69	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	11.0	260	802.11 Frag
70	00:0D:ED:A5:4F:70	00:09:5B:66:E6:80		6	11.0	14	802.11 Ack
71	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	11.0	136	802.11 Frag
72	00:0D:ED:A5:4F:70	00:09:5B:66:E6:80		6	11.0	14	802.11 Ack
73	00:0D:ED:A5:4F:70	00:09:5B:66:E6:08		6	11.0	20	802.11 RTS
74	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70		6	11.0	14	802.11 CTS
75	00:09:5B:66:E6:80	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70	6	54.0	1064	PING Req
76	00:09:5B:66:E6:08	00:0D:ED:A5:4F:70		6	24.0	14	802.11 Ack
77		00:09:5B:66:E6:08		6	11.0	14	802.11 CTS
78	00:09:5B:66:E6:90	23:BD:1D:66:E6:80	00:0D:ED:A5:4F:70	6	54.0	1064	PING Reply
79		00:09:5B:66:E6:08		6	24.0	14	802.11 Ack
80	00:09:5B:66:E6:08	00:09:5B:66:E6:80	00:0D:ED:A5:4F:70	6	11.0	1064	PING Reply
81	00:09:5B:66:E6:80	00:0D:ED:A5:4F:70		6	11.0	14	802.11 Ack
82	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
83	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
84	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon
85	00:0D:ED:A5:4F:70	FF:FF:FF:FF:FF:FF	00:0D:ED:A5:4F:70	6	1.0	137	802.11 Beacon

ABC Company's WLAN administrator is getting complaints from one user that his WLAN throughput is sluggish compared to other users in his area. The administrator takes his diagnostics laptop, which has a wireless protocol analyzer installed, to the area where the complaining user works. The administrator uses the PING utility to test connectivity from the complaining user's wireless client station to another wireless client station across the closest access point, while capturing the wireless frames. The administrator sees what is displayed in this screenshot. From this screenshot, which statements can you conclude to be TRUE that are related to the complaining user's throughput problem?

A. The complaining user's WLAN client utilities are configured for a small fragmentation threshold.
B. The complaining user's station is retransmitting fragments many times likely due to nearby RF interference.
C. The access point and other stations are using ERP-OFDM modulation, and the complaining user's wireless client station is using HR-DSSS modulation.
D. The complaining user's wireless client station should be using RTS/CTS as a protection mechanism, but it is not.
E. The access point is not signaling for protection (Protection = no) in the Beacons, but it should be.

Answer: A, C

QUESTION: 132
Exhibit:

Packet	Dest. Physical	Source Physical	BSSID	Absolute Time	Delta Time	Relative Time	Protocol
1	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.727946		0.000000	802.11 Probe Req
2	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.728260	0.000314	0.000314	802.11 Ack
3	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.730018	0.001758	0.002072	802.11 Probe Rsp
4	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.730330	0.000312	0.002384	802.11 Ack
5	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.730830	0.000500	0.002884	802.11 Auth
6	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.731138	0.000308	0.003192	802.11 Ack
7	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.731390	0.000252	0.003444	802.11 Auth
8	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.731598	0.000208	0.003652	802.11 Ack
9	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.733010	0.001412	0.005064	802.11 Assoc Req
10	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.733324	0.000314	0.005378	802.11 Ack
11	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.733808	0.000484	0.005862	802.11 Assoc Rsp
12	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.733848	0.000040	0.005902	802.11 Ack
13	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.734450	0.000602	0.006504	EAP Request
14	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.734355	-0.000095	0.006409	802.11 Ack
15	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.939073	0.204718	0.211127	EAP Response
16	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.939385	0.000312	0.211439	802.11 Ack
17	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.942649	0.003264	0.214703	EAP Request
18	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.942695	0.000046	0.214749	802.11 Ack
19	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.944581	0.001886	0.216635	EAP Response
20	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.944893	0.000312	0.216947	802.11 Ack
21	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.957283	0.012390	0.229337	EAP Success
22	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.957329	0.000046	0.229383	802.11 Ack
23	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.958951	0.001622	0.231005	EAP Request
24	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.959273	0.000322	0.231327	802.11 Ack
25	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.972157	0.012884	0.244211	EAP Response
26	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.972203	0.000046	0.244257	802.11 Ack
27	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.972373	0.000170	0.244427	802.1x
28	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.972413	0.000040	0.244467	802.11 Ack
29	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.974511	0.002098	0.246565	EAPOL-Key
30	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.974831	0.000320	0.246885	802.11 Ack
31	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70	Cisco:A5:4F:70	12:10:20.976199	0.001368	0.248253	802.1x
32	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9		12:10:20.976243	0.000044	0.248297	802.11 Ack
33	00:0D:ED:A5:4F:70	00:40:96:A1:9A:F9	Cisco:A5:4F:70	12:10:20.977877	0.001634	0.249931	EAPOL-Key
34	00:40:96:A1:9A:F9	00:0D:ED:A5:4F:70		12:10:20.978193	0.000316	0.250247	802.11 Ack

Given: Shown are frames captured from an IEEE 802.1X/LEAP authentication. This WLAN is a Robust Security Network (RSN) using the CCMP cipher suite. 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. 3.018 ms
B. 5.820 ms
C. 210.443 ms
D. 237.753 ms
E. 243.743 ms

Answer: B

QUESTION: 133
ABC Company is having throughput problems on their ERP WLAN. 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. Collisions due to dense population of client stations
B. Overlapping access point coverage on a single channel
C. High multipath conditions due to reflected signals
D. 2.4 GHz ISM band interference from sources such as wireless phones
E. Co-located DCF and EDCA access points that are using non-overlapping 2.4 GHz channels

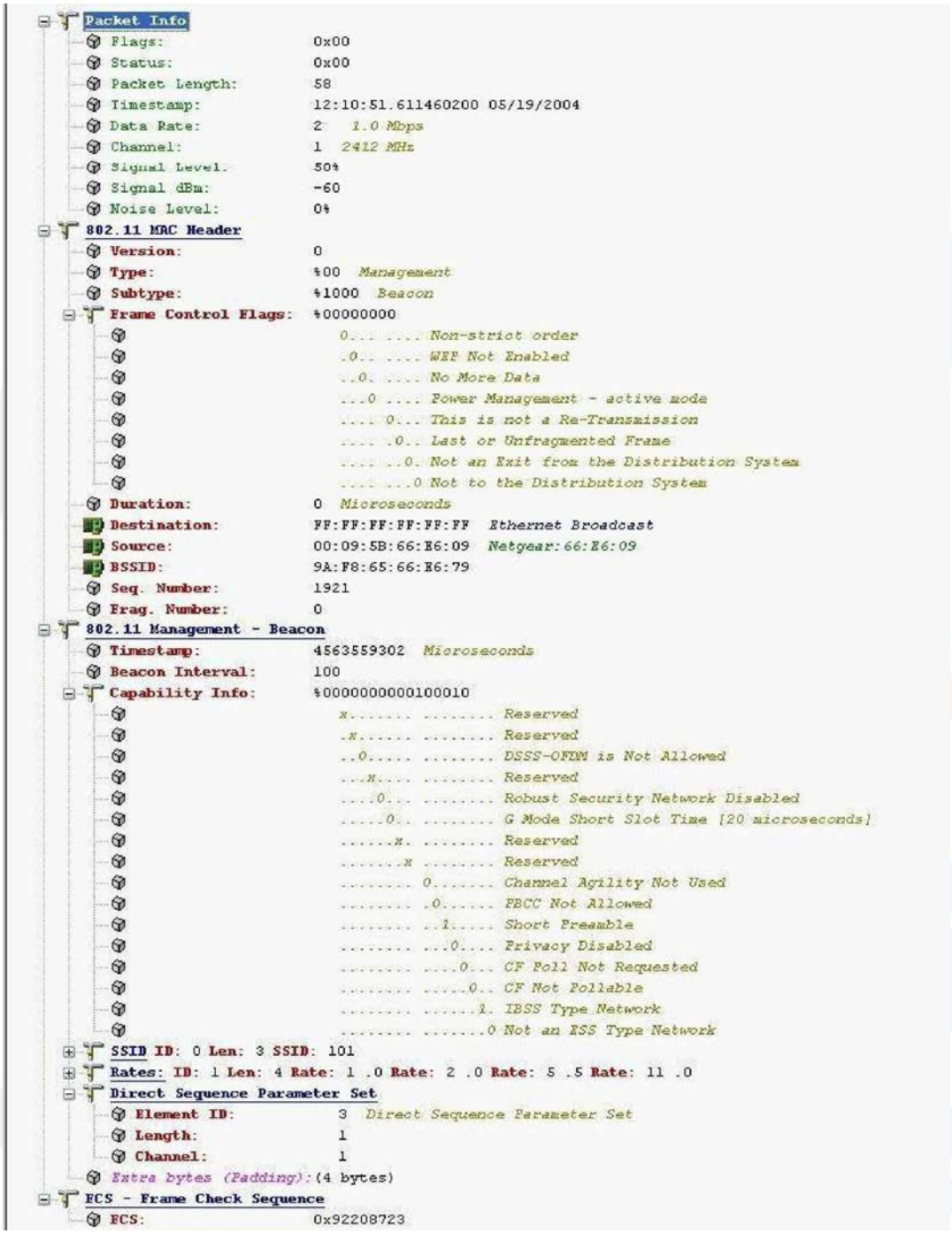
Answer: E

QUESTION: 134
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 MPDU frame's FCS field is 4 bytes, while the MMPDU frame's FCS field is 8 bytes.
B. The MMPDU frame body is limited to 200 bytes, whereas the MPDU frame body can carry up to 2304 bytes.
C. 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.
D. An MMPDU header may only contain three address fields, but an MPDU may have four address fields.
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: D

QUESTION: 135
Exhibit:


Packet Info
Flags: 0x00
Status: 0x00
Packet Length: 58
Timestamp: 12:10:51.611460200 05/19/2004
Data Rate: 2 1.0 Mbps
Channel: 1 2412 MHz
Signal Level: 50%
Signal dBm: -60
Noise Level: 0%
802.11 MAC Header
Version: 0
Type: %00 Management
Subtype: %1000 Beacon
Frame Control Flags: %00000000
0... .... Non-strict order
.0.. .... WEP Not Enabled
..0. .... No More Data
...0 .... Power Management - active mode
.... 0... This is not a Re-Transmission
.... .0.. Last or Unfragmented Frame
.... ..0. Not an Exit from the Distribution System
....0 Not to the Distribution System
Duration: 0 Microseconds
Destination: FF:FF:FF:FF:FF:FF Ethernet Broadcast
Source: 00:09:5B:66:E6:09 Netgear:66:E6:09
BSSID: 9A:F8:65:66:E6:79
Seq. Number: 1921
Frag. Number: 0
802.11 Management - Beacon
Timestamp: 4563559302 Microseconds
Beacon Interval: 100
Capability Info: %0000000000100010
x..... ..... Reserved
.x..... ..... Reserved
..0..... ..... DSSS-OFDM is Not Allowed
...x.... ..... Reserved
....0... ..... Robust Security Network Disabled
.....0.. ..... G Mode Short Slot Time [20 microseconds]
......x. ..... Reserved
.......x ..... Reserved
..... 0..... Channel Agility Not Used
..... .0..... PBCC Not Allowed
....1..... Short Preamble
....0.... Privacy Disabled
....0... CF Poll Not Requested
....0.. CF Not Pollable
....1. IBSS Type Network
....0 Not an ESS Type Network
SSID ID: 0 Len: 3 SSID: 101
Rates: ID: 1 Len: 4 Rate: 1 .0 Rate: 2 .0 Rate: 5 .5 Rate: 11 .0
Direct Sequence Parameter Set
Element ID: 3 Direct Sequence Parameter Set
Length: 1
Channel: 1
Extra bytes (Padding): (4 bytes)
FCS - Frame Check Sequence
FCS: 0x92208723

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

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

Answer: C

QUESTION: 136
Which statement accurately describes IEEE 802.11 Power Save mode operation in a Basic Service Set that does not support the QoS facility?

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

QUESTION: 137
Which statements are true regarding the duration/ID field in unfragmented Data frames?

A. The duration/ID field specifies the amount of time required for the SIFS and ACK that follow the data frame.
B. The duration/ID field is measured in microseconds and always rounded up to the next highest integer.
C. When a Data frame is sent to a multicast address, the duration/ID field is always set to 32,768.
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. 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. Valid frames with a duration/ID field value of less than 32,768 are used by unintended recipients to update their NAV.

Answer: A, B, F

QUESTION: 138
Given: ABC Company 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 100 TUs, and the Beacons for each WLAN will be rotated round-robin.
B. One Beacon will be transmitted onto the WM every 20 TUs, and the Beacon for each SSID is transmitted every 100 TUs.
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: B

QUESTION: 139
Bill works at ABC Company's help desk. Around lunch time, Bill gets a call asking for the password of network user S0NDRA. Bill gives the caller some erroneous information about user S0NDRA, and immediately contacts ABC Company's security department about a social engineering attack. Bill is trained to recognize S0NDRA as a red alert, but how does Bill know that a social engineering attack is in progress?

A. ABC Company uses IEEE 802.1X/EAP-TTLS as their wireless security protocol for user authentication, and EAP-TTLS uses an "anonymous" user name outside the TLS tunnel. In this case, the anonymous user is named S0NDRA, and it can be seen in clear text on a wireless protocol analyzer.
B. ABC Company uses FakeAP as a protection mechanism against hackers. FakeAP is a utility that transmits thousands of fake management frames that can confuse hackers. S0NDRA has been configured as a fake user name in these management frames and can be seen on a wireless protocol analyzer.
C. ABC Company uses IEEE 802.1X/PEAP-EAP-TLS as their wireless security protocol for user authentication, and PEAP has a programmable integrated intrusion detection mechanism currently named S0NDRA. This intrusion mechanism is picked up, in clear text, on wireless protocol analyzers as a user name.
D. ABC Company uses IPSec VPNs to secure their wireless LAN. IPSec VPNs use an "anonymous" name field during the authentication process when using digital certificates. The network administrator has configured all wireless client stations to use S0NDRA in the anonymous name field so that wireless protocol analyzers will mistakenly think it is a real user name.

Answer: A

QUESTION: 140
The More Fragments subfield is found in which IEEE 802.11 frame field?

A. Sequence Control field
B. Protocol Order field
C. Fragmentation Control field
D. Frame Control field

E. MAC Service Data Unit field
F. QoS Control field

Answer: D