CWNP

Exam PW0-205

certified wireless analusis professional(cwap)

Version: 5.0

[Total Questions: 120]

Topic break down

Topic	No. of Questions
Topic 0: A	60
Topic 1: B	60

Topic 0, A

A

Question No : 1 - (Topic 0)

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

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

Answer: B

Question No : 2 - (Topic 0)

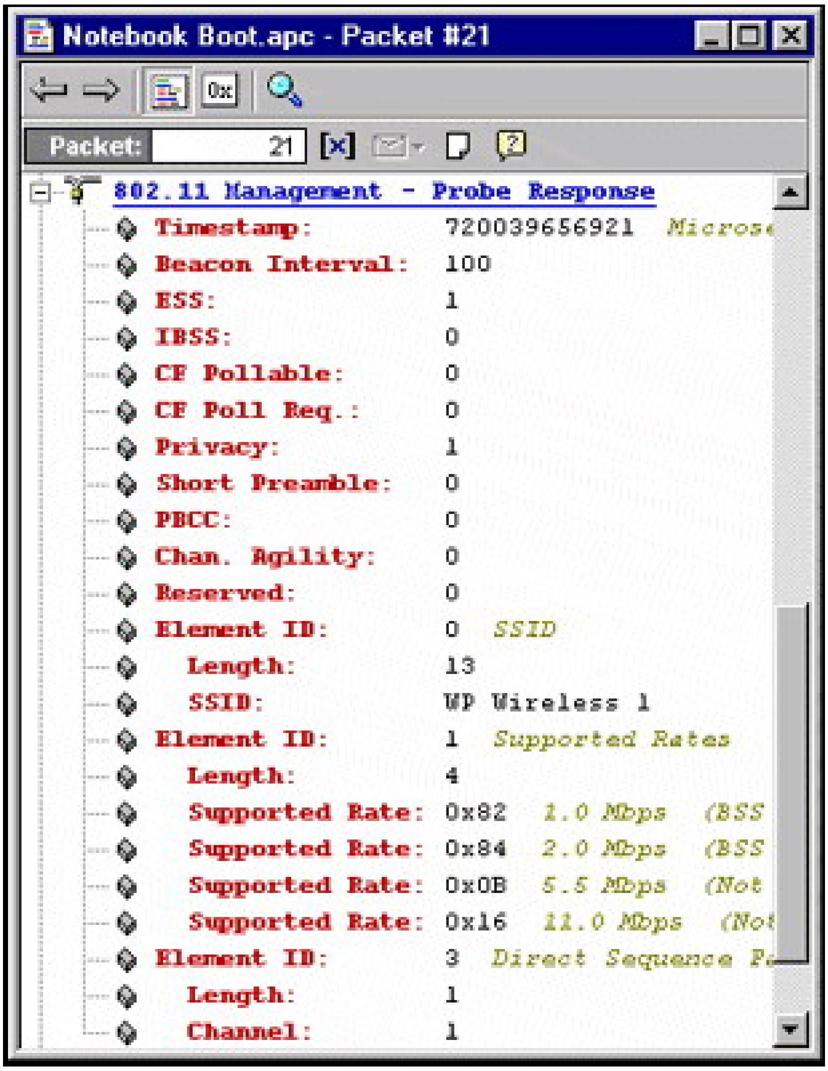
When using a wireless protocol analyzer, it is common to see Beacon Management frames (Beacons) being sent several times per second. Which of the following statements is true regarding Beacons?

A. Beacons can be disabled for security purposes.
B. The BSSID and Source Address are always the same.
C. The Destination address is always FF:FF:FF:FF:FF:FF.
D. The Receiver address and the BSSID are always the same.
E. The reason Beacons are transmitted so often is that they are unicast frames destined to each associated station.
F. The 802.11 standard specifies that all Beacons must contain a DTIM information element.

Answer: B,C

Question No : 3 - (Topic 0)

According to the information found in this screenshot of an 802.11b Probe Response frame, how many bits should stations use in their PPDU preambles when they begin transmitting data in the BSS?



Notebook Boot.apc - Packet #21

Packet: 21

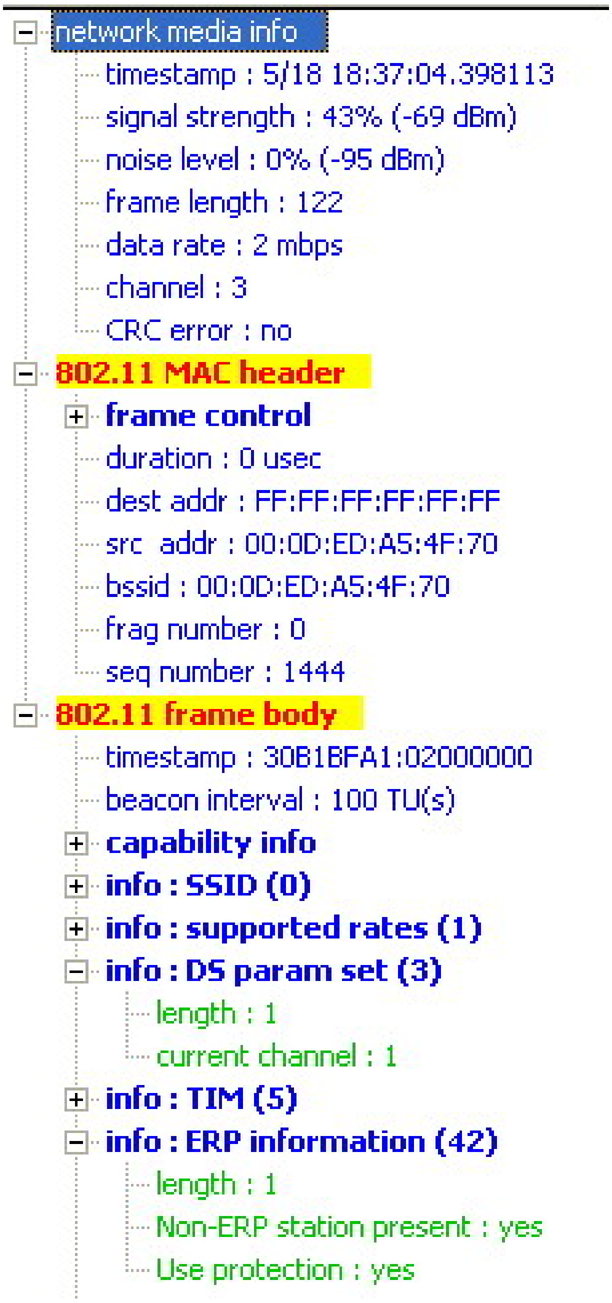
```
802.11 Management - Probe Response
    Timestamp:               720039656921   Microso
    Beacon Interval:         100
    ESS:                     1
    IBSS:                    0
    CF Pollable:             0
    CF Poll Req.:            0
    Privacy:                 1
    Short Preamble:          0
    PBCC:                    0
    Chan. Agility:           0
    Reserved:                0
    Element ID:              0   SSID
      Length:                13
      SSID:                  WP Wireless 1
    Element ID:              1   Supported Rates
      Length:                4
      Supported Rate:        0x82   1.0 Mbps    (BSS
      Supported Rate:        0x84   2.0 Mbps    (BSS
      Supported Rate:        0x0B   5.5 Mbps    (Not
      Supported Rate:        0x16   11.0 Mbps   (Not
    Element ID:              3   Direct Sequence Pa
      Length:                1
      Channel:               1
```

A. 192 bits
B. 144 bits
C. 128 bits
D. 72 bits
E. 56 bits

Answer: B

Question No : 4 - (Topic 0)

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



```
⊟ network media info
    timestamp : 5/18 18:37:04.398113
    signal strength : 43% (-69 dBm)
    noise level : 0% (-95 dBm)
    frame length : 122
    data rate : 2 mbps
    channel : 3
    CRC error : no
⊟ 802.11 MAC header
  ⊞ frame control
    duration : 0 usec
    dest addr : FF:FF:FF:FF:FF:FF
    src  addr : 00:0D:ED:A5:4F:70
    bssid : 00:0D:ED:A5:4F:70
    frag number : 0
    seq number : 1444
⊟ 802.11 frame body
    timestamp : 30B1BFA1:02000000
    beacon interval : 100 TU(s)
  ⊞ capability info
  ⊞ info : SSID (0)
  ⊞ info : supported rates (1)
  ⊟ info : DS param set (3)
        length : 1
        current channel : 1
  ⊞ info : TIM (5)
  ⊟ info : ERP information (42)
        length : 1
        Non-ERP station present : yes
        Use protection : yes
```

A. The access point is operating on channel 3.
B. The access point has both 1 Mbps and 2 Mbps configured as basic rates.
C. This Beacon Management frame came from an 802.11g access point.
D. The duration value of 0 usec means that this access point is operating in PCF mode.
E. ERP-OFDM mobile stations must use the RTS/CTS protocol before Data transmissions

Answer: C

Question No : 5 - (Topic 0)

XYZ Corporation has an 802.11b/g mixed mode deployment, and they are currently experiencing random throughput problems around the entire network. When the network was originally installed, there were both 802.11b and 802.11g stations on the network, but throughput levels were acceptable at any given time. To troubleshoot this issue, you have deployed a distributed wireless protocol analyzer, and it has noted a significantly greater percentage of 1 Mbps Data traffic being sent in random places across the network as compared with the initial baseline testing. When the network was installed, you considered only a minimal amount of 1 Mbps Data traffic acceptable. What could be causing this problem, and how would the analyzer know about the 1 Mbps traffic?

A. Due to changes in the office environment, some client stations are moving further away from the access points than when the baseline tests were performed. The analyzer views the SIGNAL field in the PLCP header to see the frames transmission rates.
B. A wireless network management system has updated all access points to allow only use of the long slot time. The analyzer views the SERVICE field in the PLCP header to see the frames?transmission rates.
C. A new 802.11g station has a minimum transmission rate set at 1 Mbps. The analyzer views the Start Frame Delimiter (SFD) field in the PLCP header to see the frames?transmission rates.
D. An access point configured for 802.11b/g mixed mode has been reconfigured to send downstream traffic in a round-robin fashion when protection is enabled. The analyzer views the length of the preamble to determine the transmission rate of associated stations.

Answer: A

Question No : 6 - (Topic 0)

A wireless LAN protocol analyzer utilizing a radio card compliant with IEEE 802.11a, 802.11b, and 802.11g standards will be able to perform which of the following tasks?

A. Recognize and decode 802.11-compliant FHSS access point transmissions in the 2.4 GHz ISM band.
B. Recognize and decode all 802.11g frames regardless of the modulation used at the physical layer.
C. Recognize and decode 802.11a, 802.11b, and 802.11g transmissions simultaneously.
D. Recognize and decode transmissions from 900 MHz Pre-DSSS system in order to report an intrusion to a centralized security console.
E. Recognize, decrypt, and decode unicast data frames encrypted with WPA-compliant 802.1X/EAP between stations and access points when an appropriate username and password combination is entered into the analyzer software.
F. Recognize and decode all protection mechanisms sent by a transmitter using CCK.

Answer: F

Question No : 7 - (Topic 0)

An 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 fixed fields in the Authentication frame?

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

Answer: B,D

Question No : 8 - (Topic 0)

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

A. Following a period of time in a low power state, client stations wake themselves and automatically poll the access point for traffic using a PS-Poll frame.
B. When the access point's buffer is full, the access point wakes all client stations using a PS-Poll frame so that they can receive the data.
C. Upon receiving traffic for a dozing station, the access point wakes the client station using a PS-Poll frame so that the client station can receive the data.
D. After waking from a low power state, client stations listen for the next beacon to determine if sending a PS-Poll frame to the access point is necessary.
E. After waking at a schedule TBTT, client stations automatically send Null Function frames to the access point with the Power Management bit cleared.

Answer: D

Question No : 9 - (Topic 0)

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

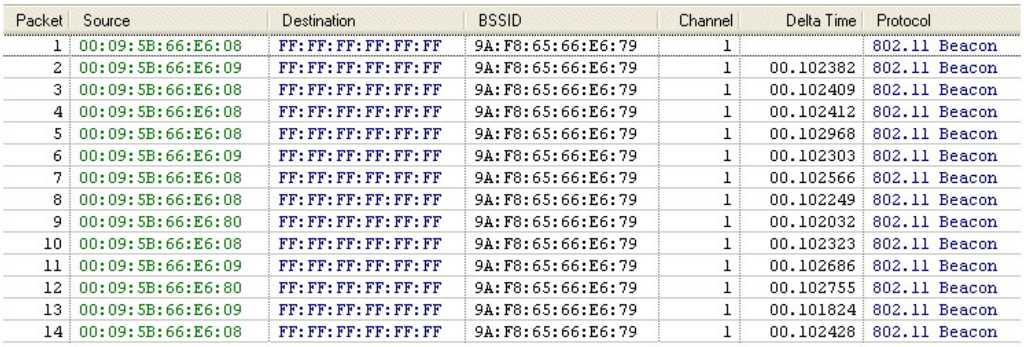
A. The AID has a maximum value of 2048, and is used to uniquely identify a wireless client station associated with an access point.
B. The AID has a maximum value of 2007, and resides in the duration/ID field of a PS-Poll frame only.

C. When bit 16 of the field is zero, the value in bits 15-0 represent the remaining duration of a frame exchange.
D. The least significant 8 bits of this field are used by the wireless client station to identify which bit in a TIM indicates that the access point has frames buffered for the wireless client station.
E. The AID is used by the access point in DCF mode to reduce duplicate transmissions when sending multicasts.

Answer: B

Question No : 10 - (Topic 0)

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



Packet	Source	Destination	BSSID	Channel	Delta Time	Protocol
1	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1		802.11 Beacon
2	00:09:5B:66:E6:09	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102382	802.11 Beacon
3	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102409	802.11 Beacon
4	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102412	802.11 Beacon
5	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102968	802.11 Beacon
6	00:09:5B:66:E6:09	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102303	802.11 Beacon
7	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102566	802.11 Beacon
8	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102249	802.11 Beacon
9	00:09:5B:66:E6:80	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102032	802.11 Beacon
10	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102323	802.11 Beacon
11	00:09:5B:66:E6:09	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102686	802.11 Beacon
12	00:09:5B:66:E6:80	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102755	802.11 Beacon
13	00:09:5B:66:E6:09	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.101824	802.11 Beacon
14	00:09:5B:66:E6:08	FF:FF:FF:FF:FF:FF	9A:F8:65:66:E6:79	1	00.102428	802.11 Beacon

A. Four access points are on the same channel in the same physical area.
B. Four wireless stations are operating as two separate Ad Hoc networks.
C. One access point is operating in PCF mode. The screenshot is not displaying CF-Poll frames that have been filtered out.
D. Three wireless stations are participating in an Ad Hoc wireless LAN.

Answer: D

Question No : 11 - (Topic 0)

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

A. Traffic injection analysis
B. Operational traffic policy
C. Directional traffic filtering
D. Baseline traffic analysis

E. Quality of Service (QoS) design

Answer: D

Question No : 12 - (Topic 0)

When an 802.11i-compliant wireless LAN security solution is being used with IPSec/ESP, what will a wireless LAN protocol analyzer see as the security mechanism in use?

A. TKIP or CCMP
B. IPSec/ESP
C. Unknown protocol
D. Both WEP and IPSec/ESP

Answer: A

Question No : 13 - (Topic 0)

There are many differences between analyzing wireless and wired networks. In a wireless network, there is no guarantee one wireless client station can hear another station's transmissions. With no corrective actions or corrective mechanisms implemented, this hidden node situation may cause which measurable statistics parameter to be incremented in a wireless protocol analyzer?

A. Duration length
B. Retransmission Count
C. Contention Window
D. Slot Time
E. Fragment Interval
F. DTIM Interval

Answer: B

Question No : 14 - (Topic 0)

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 to determine which modulation will be used to send the entire PPDU.

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. 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.

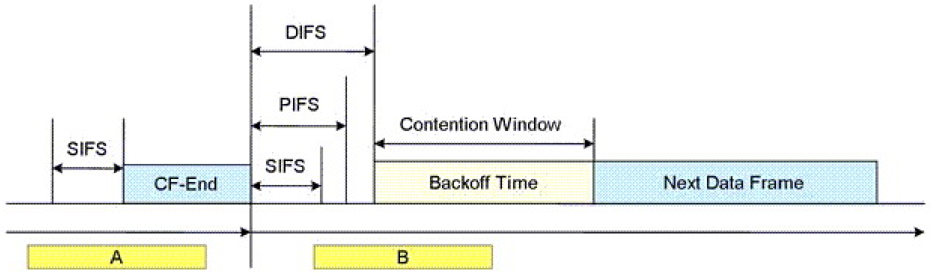
D. The Modulation Selection bit is used to determine whether CCK or PBCC is in use for any speed where either could be used.

E. Based on the Modulation Selection bit in received Data frames, the receiving station can determine which modulation to use when sending acknowledgements.

Answer: B,D

Question No : 15 - (Topic 0)

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



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

B. A = ATIM Window, B = Data Window

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

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

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

Answer: A

Question No : 16 - (Topic 0)

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?