



PW0-270^{Q&As}

Certified Wireless Analysis Professional

Pass CWAP PW0-270 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/pw0-270.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CWAP
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

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.

Packet	Dest. Physical	Source Physical	SSID	Absolute Time	Delta Time	Relative Time	Protocol
1	00:0D:ED:A5:4F:70	00:41:96:A1:9A:F9	Cisco:A5:4F:73	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:73	12:10:20.730016	0.001756	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	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:73	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	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:73	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:73	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	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:73	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	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:73	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	12:10:20.950951	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:73	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:73	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	12:10:20.974511	0.002098	0.246565	EAP01-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:73	12:10:20.976109	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	00:41:96:A1:9A:F9	Cisco:A5:4F:73	12:10:20.977877	0.001634	0.249931	EAP01-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

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

Correct Answer: B

QUESTION 2

Which statement accurately describes IEEE 802.11 Power Save 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 scheduled TBTT, client stations send Null Function frames to the access point with the Power Management bit set back to zero.

Correct Answer: D

QUESTION 3

Which statements are true regarding wireless network discovery and scanning processes for an HT network? (Choose 2)

- A. Client stations may continually send Probe Request frames on all HT channels in the 2.4 GHz ISM band in a consecutive manner, regardless of their association state.
- B. Access points send Beacon frames on all HT channels in the 2.4 GHz ISM band in a consecutive manner including the channel for which the access point is configured.
- C. Client stations send Probe Request frames on all HT 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 no longer transmit Probe Request frames.
- D. Access points send Beacon frames only on the HT channel in the 2.4 GHz ISM band for which the access point is configured, and only after scanning that channel to discover existing BSSs.
- E. Client stations send Probe Request frames on all HT channels in the 2.4 GHz ISM band in a consecutive manner until they receive at least 3 Probe Response frames.

Correct Answer: AD

QUESTION 4

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).



No	Ch	Len	S	R	Source	Dest	Summary
162	6	64	75	11	Askey:5C:D7:D3	Symbol:42:16:8C	802.11 encrypted data + CF-Poll

network media info

- timestamp : 2/8 20:06:57.113562
- signal strength : 75% (-50 dBm)
- noise level : 0% (-95 dBm)
- frame length : 64
- data rate : 11 mbps
- channel : 6
- CRC error : yes

802.11 MAC header

frame control

- protocol version : 2
- frame type : data
- subtype : data + CF-Poll
- to DS : 0
- from DS : 0
- more frag : 0
- retry : 0
- power management : 0
- more data : 0
- WEP : 1
- order : 0

duration : 117 usec

dest addr : 00:A0:F8:A2:16:8C

src addr : 00:90:96:5C:D7:D3

bssid : FF:FF:55:DA:CF:FE

frag number : 0

seq number : 1018

802.11 encrypted frame body

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 IEEE 802.11 network is using both version 1 and version 2 protocols simultaneously. This unexpected frame is from the version 2 protocol set.
- 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 access point is operating as a repeater, and clients must poll repeater access points in order to transmit data frames through them.
- D. The frame was misinterpreted because of insufficient information received by the analyzer due to frame corruption.

Correct Answer: D

QUESTION 5

When an originator QoS STA initiates a BlockAck agreement with a recipient QoS STA, what is the first frame sent by the originator?



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

Correct Answer: C

[PW0-270 PDF Dumps](#)

[PW0-270 Exam Questions](#)

[PW0-270 Braindumps](#)