

DUMPSBOSS.

CCIE Wireless (v3.1)

Cisco 400-351

Version Demo

Total Demo Questions: 13

Total Premium Questions: 272

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Planning & Designing WLAN Technologies	17
Topic 2, Configure and Troubleshoot the Network Infrastructure	25
Topic 3, Configure and Troubleshoot an Autonomous Deployment Model	12
Topic 4, Configure and Troubleshoot a Unified Deployment Model (Centralized)	4
Topic 5, Configure and Troubleshoot a Unified Deployment Model (Converged)	3
Topic 6, Configure and Troubleshoot Security & Identity Management	11
Topic 7, Configure and Troubleshoot Prime Infrastructure and MSE	7
Topic 8, Configure and Troubleshoot WLAN media and application services	15
Topic 9, Evolving Technologies	178
Total	272

QUESTION NO: 1

Which two statements about client management frame protection are true? (Choose two.)

- A. CCXv5 client and access points must discard broadcast Class 3 management frames.
- B. Client MFP can replace infrastructure MFP in case only CCXv5 clients are used.
- C. To use client MFP, the client must support CCXv4 and negotiate WPA with TKIP or higher.
- D. Client MFP encrypts Class 3 Unicast management frames using the security mechanisms defined by 802.11i.
- E. The only supported method to obtain the preuser MFP encryption keys is EAP authentication.

ANSWER: B D

QUESTION NO: 2

A wireless engineer has completed the configuration of the QoS profiles on the WLC and has assigned them to the WLANs. The engineer applies the profiles, tests them, and notices that traffic is blocked for some of the WLANs. Which problem is true?

- A. AVC must be enabled for the QoS profiles to work properly.
- B. The QoS profiles and the traffic restrictions of the WLANs are different.
- C. The QoS profiles have 802.1p tagging configured, and the WLANs that are assigned use untagged interfaces on the controller.
- D. The QoS profiles have 802.1p tagging disabled, and the WLANs that are assigned use tagged interfaces on the controller.

ANSWER: D

QUESTION NO: 3

A wireless engineer is configuring an autonomous access point and wants to make sure that client at the edge of the cell has the best possible reception of multicast frames. How must multicast frames be transmitted to achieve this goal?

- A. at the highest configured basic rate
- B. at the lowest configured basic rate
- C. at a highest configured mandatory rate
- D. from a dedicated radio interface

ANSWER: B

QUESTION NO: 4

When deploying Local Web Authentication on a Cisco WLC, you can authenticate users externally via RADIUS. Which three authentication methods are supported by the

Cisco WLC to authenticate guest users to a RADIUS server? (Choose three.)

- A. LEAP
- B. EAP-GTC
- C. EAP-TLS
- D. PAP
- E. EAP
- F. CHAP
- G. EAP-MD5
- H. EAP-FAST
- I. PEAP MS-CHAPv2

ANSWER: D F G

QUESTION NO: 5

Your WLC is running code 8.7 and you have deployed COS APs on your network. Which two 802.1X authentication methods are supported when the AP acts as a supplicant? (Choose two.)

- A. LEAP
- B. EAP-PSK
- C. EAP-TLS
- D. EAP-MD5
- E. EAP-FAST

ANSWER: C E

QUESTION NO: 6

Which protocol allows for IP mobility in-between Data Centers?

- A. OTV
- B. LISP
- C. FABRIC PATH
- D. VXLAN

ANSWER: B

QUESTION NO: 7

While configuring the root access point for WGB connectivity, the IT admin issues the no infrastructure client command. Which impact of this command is true?

- A. This command enables multi-VLAN support for the clients behind WGB.
- B. This command allows more than 20 WGBs to associate with the same access point.
- C. This command adds reliability to the multicast packet delivery from the access point to WGB.
- D. The SSID must be marked as infrastructure SSID when this command is in use or the WGB cannot connect.

ANSWER: B

QUESTION NO: 8

While troubleshooting a failed central web authentication configuration on Cisco WLC, you discover that the Cisco WLC Policy Manager State is showing RUN for new clients and not CENTRAL_WEB_AUTH. Which of the below is most likely causing this issue?

- A. The Web Login Page under the Cisco WLC security settings should be set to External (Redirect to external server).
- B. The WLAN NAC State should be set to RADIUS NAC.
- C. The WLAN Layer 2 security should be set to WPA+WPA2.
- D. The WLAN Layer 3 security should be set to Web Policy with Conditional Web Redirect.

ANSWER: C

QUESTION NO: 9

You have been called onsite to troubleshoot a voice over wireless issue. Roaming within the indoor premises is working fine. However, when the customer roaming to the outdoor area, the call drops and the phone has to reauthenticate to the network. All indoor APs are model 3700, and the outdoor APs are 1500 series.

Which two options are possible causes of this problem? (Choose two.)

- A. The phone gets the initial roaming channel list based on 802.11ax from the first connection, which includes only indoor channels 36 to 64. The outdoor channels are from 100 to 140.
- B. Deployment is in ETSI domain.
- C. The phone gets the initial roaming channel list based on 802.11d from the first connection, which includes only indoor channels 36 to 64. The outdoor channels are from 100 to 140.
- D. The SSID is operating on 2.4 Ghz.
- E. The phone gets the initial roaming channel list based on 802.11c from the first connection, which includes only indoor channels 36 to 64. The outdoor channels are from 100 to 140.

ANSWER: A D

QUESTION NO: 10

Refer to the exhibit. You are configuring an autonomous AP in WGB mode. You configure d1 radio as shown in the exhibit. Which command must you use on the root bridge to ensure the successful negotiation of a link?

WBG(config-if) # interface d1

WBG(config-if) # mobile station scan 5180 5200 5220 5240

A. RB(config-if)# interface d0

RB(config-if)# channel 5180 5200 5220 5240

B. RB(config-if)# interface d1

RB(config-if)# mobile station 5180 5200 5220 5240

C. RB(config-if)# interface d1

RB(config-if)# mobile station 5180

D. RB(config-if)# interface d1

RB(config-if)# channel 5180

ANSWER: D

QUESTION NO: 11

You are deploying a Cisco OfficeExtend Access Point 1810 for home office needs. Which two statements for OEAP 1810 deployment are true? (Choose two.)

A. Personal SSID configuration is not supported for local home networking on OfficeExtend mode

B. A total of eight (WLAN + RLAN) is supported on AIR-OEAP1810. Once can have more than eight (WLAN + RLAN) associated on the AP group, but only the first eight (WLAN + RLAN) are usable

C. Ethernet Ports-AIR-OEAP1810 supports Cisco Discovery Protocol or LLDP on Ethernet ports

D. MAC filtering is not a supported authentication/security method

E. PoE Uplink-AIR-OEAP1810 does not support Cisco Discovery Protocol it supports LLDP on the uplink PoE port for power negotiation.

ANSWER: A C

QUESTION NO: 12

Channel group 1 neighbors									
Partner's information:									
Port	Flags	LACP port	Priority	Dev ID	Age	Admin Key	Oper Key	Port Number	Port State
Gi0/19	SA	32768		0008.2feb.1100	12s	0x0	0x1	0x102	0x3D
Gi0/20	SA	32768		0008.2feb.1100	22s	0x0	0x1	0x103	0x3D
switch-1#									

Refer to the exhibit. A network administrator is installing a new converged access Cisco WLC. The uplink connection is to be a Gigabit port channel. Which characteristic is true?

A. The port channel is currently down.

B. The port channel mode is set to active and sends PDUs at 1 sec intervals.

C. The port channels uses a Cisco proprietary protocol.

- D. The port-channel member interfaces must be set to trunk mode.
- E. The port channel mode is set to active and sends PDUs at 30 sec intervals.

ANSWER: C E

QUESTION NO: 13

On a Cisco autonomous AP, the maximum number of attempts to send a packet (packet retries) is set to 32 by default. Which statement about the result when the AP has tried to send a packet for that number of attempts and no response is received from the client is true?

- A. The access point drops the packet.
- B. The access point resets the radio interface.
- C. The access point disassociates the client.
- D. The client MAC address is excluded for 60 seconds.

ANSWER: A

Explanation:

The maximum data retries setting determines the number of attempts the wireless device makes to send a packet before giving up and dropping the packet.

The default setting is 32.

Reference:

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15_2_4_JB/configuration/guide/scg15-2-4-Book/scg15-2-4-chap6-radio.html#pgfId-1039239