Vendor: Cisco

Exam Code: 350-101

Exam Name: Implementing and Operating Cisco Wireless Core Technologies (WLCOR)

Version: DEMO

QUESTION 1
What does a high SNR value result in?

A. presence of multipath signal distortion
B. use of directional array patterns in wireless signaling
C. increased data integrity with fewer errors
D. modification of output frequency ranges

Answer: C
Explanation:
A high SNR means the received signal is much stronger than the noise floor, allowing the receiver to decode frames more accurately and maintain better data integrity with fewer transmission errors.

QUESTION 2
In an RF environment, what does high interference result in?

A. unreliable frame aggregation
B. inconsistent channel performance
C. scheduled contention access
D. extended coverage patterns

Answer: B
Explanation:
High interference disrupts RF communication and causes unstable channel behavior, leading to inconsistent wireless performance, retransmissions, and reduced reliability.

QUESTION 3
What is the time taken for an RF signal to travel from the transmitter to the receiver known as?

A. reflection
B. propagation delay
C. scattering
D. link speed

Answer: B
Explanation:
Propagation delay is the time an RF signal takes to travel through the medium from the transmitter to the receiver.

QUESTION 4
To double the range of a transmitter, which value must the transmitter be changed to if it is currently at 17 dBm?

A. 14 dBm
B. 20 dBm
C. 27 dBm
D. 100 dBm

Answer: C

Explanation:
Doubling transmitter range requires a significant transmit power increase, and in this simplified RF planning context the required change is a 10 dB increase. Starting from 17 dBm, increasing by 10 dB gives 27 dBm.

QUESTION 5
Which result is produced using a power ratio of 10:1 in standard decibel calculations?

A. -20 dB
B. 5 dB
C. 10 dB
D. 15 dB

Answer: C
Explanation:
A 10:1 power ratio equals 10 dB because standard decibel power calculations use 10 × log10(power ratio), and 10 × log10(10) equals 10 dB.

QUESTION 6
Refer to the exhibit.

```
%DOT1X-5-FAIL: Chassis 1 R0/1: wncd: Authentication failed for client (9C:4E:36:8A:2B:F1) with reason (Cred Fail)
```

The Catalyst 9800 WLC logs show when a client with MAC address 9C:4E:36:8A:2B:F1 fails to connect to a WLAN configured for Wi-Fi Protected Access 3-Enterprise with 802.1X. Which action must the engineer take to resolve the issue?

A. Ensure that the AP is using the appropriate credentials.
B. Change the WLAN to Wi-Fi Protected Access 2-Personal and configure a preshared key.
C. Verify the client's Active Directory credentials and ensure that the RADIUS server is reachable.
D. Disable RADIUS NAC on the policy profile assigned to the WLAN.

Answer: C
Explanation:
WPA3-Enterprise with 802.1X depends on valid client credentials and successful communication with the RADIUS authentication server, so credential validation and RADIUS reachability are the key areas to verify when the log shows a credential failure.

QUESTION 7
Refer to the exhibit.

```
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to validate eapol mic. MIC mismatch.
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to validate eapol key m2. 11r MIC validation failed
[client-keymgmt] [17419]: (ERR): MAC: 1111.2222.3333  Keymgmt: Failed to eapol key m1 retransmit failure. Max retries for M1 over
[client-orch-sm] [17419]: (note): MAC: 1111.2222.3333  Send delete mobile. Sending DELETE MOBILE succesfully for BSSID: 6871.1111.2222 AP slot: 1
```

A network engineer must create a PSK WLAN that will be anchored to the DMZ. After this WLAN is created, users cannot connect to it. Based on the output from the RA trace, which action must the engineer take to resolve the issue?

A. Disable fast transition 802.11r on the WLAN.

B. Configure matching passwords on the client and the WLAN.
C. Remove the anchor WLC from the mobility group.
D. Configure matching WLANs on the foreign and the anchor.

Answer: B
Explanation:
A MIC validation failure during the WPA key exchange on a PSK WLAN indicates that the client and WLAN are using different preshared keys, so the passphrase must match on both sides for authentication to complete successfully.

QUESTION 8
Refer to the exhibit.

```
[client-orch-sm] [17419]: (note): MAC: 1111.2222.3333  Association received. BSSID 1234.5678.abcd, WLAN Corp-WLAN,
[client-orch-sm] [17419]: (debug): MAC: 1111.2222.3333  Received Dot11 association request.
[client-auth] [17419]: (note): MAC: 1111.2222.3333  L2 Authentication initiated. method DOT1X, Policy VLAN 50, AAA override = 0 , NAC = 0
[auth-mgr] [17419]: (info): [1111.2222.3333:capwap_90000005] auth mgr attr add/change notification is received for attr audit-session-id(819)
[radius] [17419]: (info): RADIUS: Received from id 1812/115 192.168.1.11:0, Access-Accept, len 309
[radius] [17419]: (info): RADIUS:  Tunnel-Type          [64]     6  VLAN                  [13]
[radius] [17419]: (info): RADIUS:  Tunnel-Medium-Type   [65]     6  ALL_802               [6]
[radius] [17419]: (info): RADIUS:  Tunnel-Private-Group-Id[81]     6  "100"
[radius] [17419]: (info): Valid Response Packet, Free the identifier
[client-auth] [17419]: (note): MAC: 1111.2222.3333  L2 Authentication Key Exchange Start. Resolved VLAN: 50
```

A client authenticates via 802.1X against an ISE server that is configured to return a specific VLAN ID (VLAN 100) via an attribute value pair. However, the administrator reviews the RA trace and notices that the client is placed in the wrong VLAN (VLAN 50).

What must the administrator implement to resolve the issue?

A. Configure the policy profile to allow ISE to override the VLAN.
B. Configure VLAN 100 as an SVI on the WLC.
C. Configure VLAN 100 on the trunk ports of the WLC.
D. Configure AAA VLAN enable on the WLAN.

Answer: A
Explanation:
The RA trace shows that AAA override is disabled, so the VLAN returned by ISE is not applied. Enabling AAA override on the policy profile allows the WLC to honor the VLAN assignment returned by the authentication server.

QUESTION 9
A retail store has a Cisco 9176 FlexConnect AP at a branch location and must ensure that wireless clients continue to access the network even if the WAN link to the central controller is down. The AP must authenticate users locally during outages and still sync with the controller when connectivity is restored. The IT administrator wants centralized management for all APs but requires high availability for branch users. Which set of CLI commands on the 9800 WLC configures the AP to meet these requirements?

A. config wlan branch1 flexconnect local-switching
B. config wireless local ap vlan 6 wlan branch1
C. wireless profile policy outage
flexconnect local authentication
D. wireless profile policy outage
no central authentication

Answer: D
Explanation:
Disabling central authentication in the wireless policy profile allows the FlexConnect AP to perform local authentication during WAN or controller outages, while the AP remains centrally managed by the Catalyst 9800 WLC when connectivity is restored.

QUESTION 10
Refer to the exhibit.

```
AP-1# show interfaces wired 0

wired0    Link encap:Ethernet  HWaddr C8:8B:5E:BA:D0 eMac Status: UP
          inet addr:172.16.100.104  Bcast:172.16.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:2400  Metric:1
          full Duplex, 1000 Mb/s

Wired0 Port Statistics:
ID          :              2            TYPE        :             0
RX PKTS     :          35109/431        TX PKTS     :          1307/11
RX OCTETS   :       2899435/34925       TX OCTETS   :       377424/1575
RX ERR      :          287/0            TX ERR      :          0/0
```

An engineer configured a static IP address on a LWAPP, but it is not reachable for management. The engineer configured the wrong gateway and must now change the default gateway to 172.16.100.1.

Which CLI command must the engineer use?

A. capwap ap ip default-gateway 172.16.100.1
B. capwap ap controller ip address 172.16.100.1
C. capwap ap ip 172.16.100.104 255.255.255.192 172.16.100.1
D. capwap ap ip 172.16.100.104 255.255.255.0 172.16.100.1

Answer: D
Explanation:
The AP static IP configuration must include the AP IP address, subnet mask, and default gateway together. The displayed AP address uses a /24 mask, so the command with 172.16.100.104 255.255.255.0 172.16.100.1 correctly updates the default gateway while preserving the proper IP settings.

QUESTION 11
An engineer must troubleshoot complex wireless performance issues in a large office which is using a Cisco 9176 AP. The engineer must analyze traffic patterns and identify potential sources of interference. The AP must capture all wireless frames in the air and send them to a remote protocol analyzer for detailed inspection. Client connectivity is not required from the AP during the troubleshooting window. Which CLI command must the engineer use on the WLC to enable the required AP mode for this purpose?

A. ap name office1st mode monitor
B. ap name office1st mode sniffer
C. ap name office1st mode local
D. ap name office1st mode rogue-detector

Answer: B
Explanation:
Sniffer mode configures the AP to capture wireless frames over the air and forward them to a remote protocol analyzer for detailed packet inspection during troubleshooting.

QUESTION 12
Refer to the exhibit.

```
2025/08/14 08:44:47.540451753 {wncmgrd_R0-0}{1}: [errmsg] [15350]: (note): %CLIENT_EXCLUSION_SERVER-5-
ADD_TO_EXCLUSIONLIST_REASON_DYNAMIC: R0/0: wncmgrd: Client MAC: 02c7.c85d.fbfc was added to exclusion list associated
with AP Name:BLD4-L03-02, BSSID:MAC: ac14.0cb2.df6f, reason:Redirect ACL failure
2025/08/14 08:44:47.541509605 {wncd_x_R0-0}{1}: [client-orch-sm] [15754]: (note): MAC: 02c7.c85d.fbfc  Client delete
initiated. Reason: CO_CLIENT_DELETE_REASON_EXCLUDE_PUNT_ACL_FAIL, details: , fsm-state transition 00|00|00|00|00|00|00|
00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|00|01|
```

A retail business is deploying guest wireless across its remote branch locations. Each branch uses FlexConnect APs in local switching mode, and the central wireless LAN controller is configured with an ACL named CWA_REDIRECT. Cisco ISE is configured to return this ACL during the authentication process for central web authentication (CWA). However, when clients attempt to connect to the guest wireless LAN, they are added to the exclusion list.

Which configuration step resolves the connectivity issue?

A. Include the ACL CWA_REDIRECT in the AP-Join profile.
B. Change the ACL to include the ISE IP address.
C. Map the ACL CWA_REDIRECT to the flex profile as a policy ACL.
D. Add the ACL CWA_REDIRECT to the policy profile.

Answer: C
Explanation:
For FlexConnect APs using local switching, the redirect ACL returned during CWA must be available in the Flex profile as a policy ACL so the AP can apply it locally during guest authentication.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

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

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**