Cisco 300-430 Mock Exam

Shared by Carpenter on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
(Cisco Controller) >
(Cisco Controller) >*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: New context (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast.c-EVENT: Allocated new EAP-FAST context (handle = 37000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Received Identity
*EAP Framework: Jan 21 23:55:43.569: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f000000000000000000000000)
*EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Sending Start
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 10
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: Ignoring unknown ext rec type: 11
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA proposed…
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_AES_128 proposed…
*EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.c-AUTH-EVENT: TLS_RSA_WITH_RC4_128 proposed…
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Proposed ciphersuite(s):
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 255
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 49188

*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 103
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 57
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT:     TLS_DHE_RSA_WITH_AES_128_CBC_SHA
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 22
*EAP Framework: Jan 21 23:55:43.586: eap_fast.c-EVENT: Unknown ciphersuite 61

*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT:     TLS_RSA_WITH_AES_128_CBC_SHA
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 10
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49159
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 49169
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT:     TLS_RSA_WITH_RC4_128_ SHA
*EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown ciphersuite 4
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b)
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = c4000000)
*EAP Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EVENT: Received ACK from peer
*EAP Framework: Jan 21 23:55:43.592: eap_fast.c-EVENT: Free context (EAP handle = c4000000)
```

An engineer deployed a Cisco WLC using local EAP. Users who are configured for EAP-PEAP cannot connect to the network. Based on the local EAP debug on the controller provided, why is the client unable to connect?

Options:

A- The client is failing to accept certificate.

B- The Cisco WLC is configured for the incorrect date.

C- The Cisco WLC local EAP profile is misconfigured.

D- The user is using invalid credentials.

Answer:

C

Explanation:

The issue with users configured for EAP-PEAP not being able to connect to the network, when a Cisco Wireless LAN Controller (WLC) is deployed using local EAP, typically points to a misconfiguration in the local EAP profile on the WLC. EAP-PEAP relies on a server-side certificate to create a secure TLS tunnel for the authentication process. If the local EAP profile is not correctly configured with the proper certificate or other necessary settings, the authentication process will fail, preventing users from connecting.Reference:= (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question 2

Question Type: MultipleChoice

Refer to the exhibit.

```
(Cisco Controller) >show nmsp notification interval

NMSP Notification Interval Summary

RSSI Interval:
 Client.............................................. 20 sec
 RFID................................................ 20 sec
 Rogue AP............................................ 20 sec
 Rogue Client........................................ 20 sec

Spectrum Interval:
 Interferer device................................... 20 sec

(Cisco Controller) >
```

An administrator notices slower location updates from the controller to Cisco CMX. Which command must be configured to get an update every 5 seconds for rogues?

Options:

A- config location notification interval rssi rogues 5
B- config nmsp notification interval rssi rogues 5
C- config subscription notification interval rssi rogues 5

D- config cmx notification interval rssi rogues 5

Answer:

B

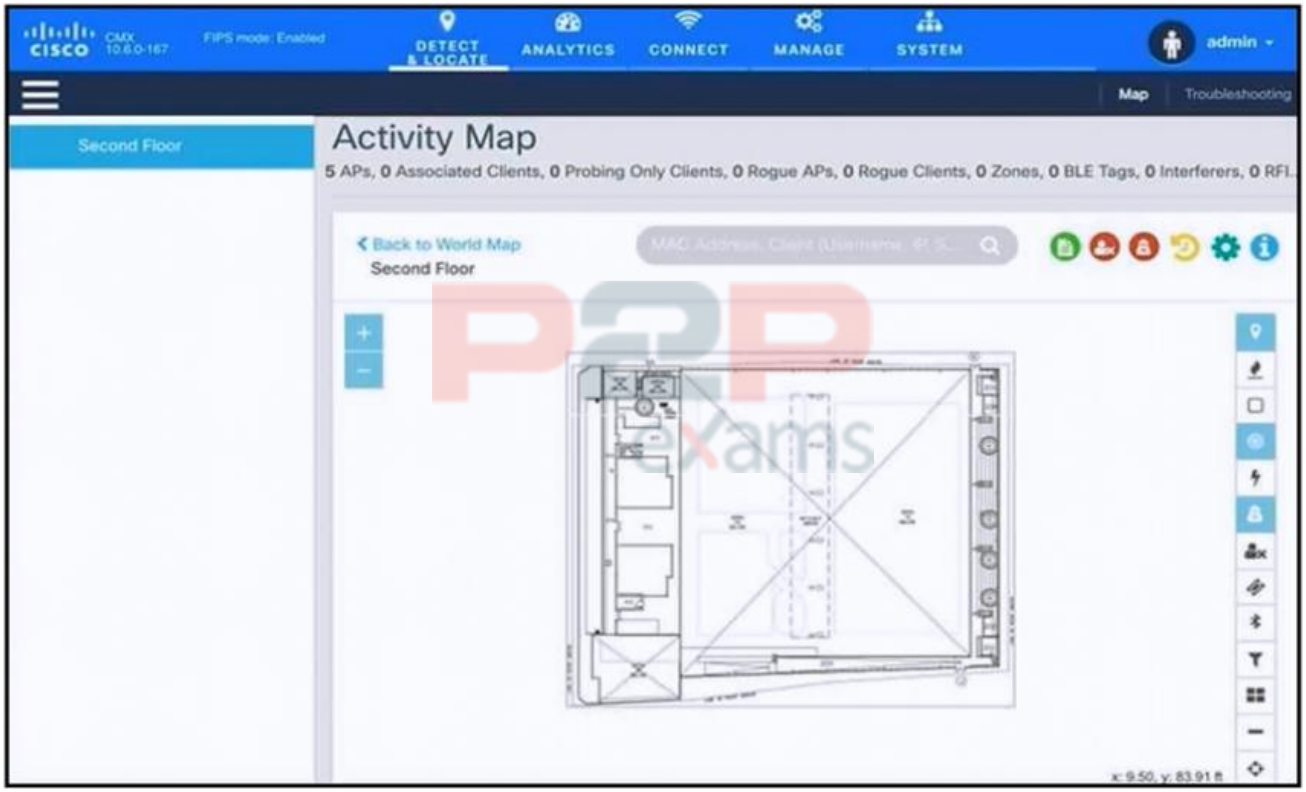
Explanation:

The correct command to configure the controller to update Cisco CMX every 5 seconds for rogue devices is ''config nmsp notification interval rssi rogues 5''. NMSP (Network Mobility Services Protocol) is used by Cisco wireless controllers to manage and communicate with connected services such as Cisco CMX. The command structure ''config nmsp notification interval'' followed by the specific type of device or metric, in this case, 'rssi rogues', and the desired interval time '5' seconds, sets the frequency of NMSP notifications for RSSI updates related to rogue devices.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



An engineer has deployed the Cisco CMX solution to track and detect the number of users who visit the office each day. The CMX dashboard is not showing any dat

a. Which action resolves this issue?

Options:

A- Configure Single Sign-On authentication.
B- Add the WLCs to CMX.
C- Copy the exported Maps from CMX server to PI using SCP.
D- Install an evaluation license to CMX server.

Answer:

B

Explanation:

The issue with the Cisco CMX dashboard not showing any data can be resolved by integrating the Wireless LAN Controllers (WLCs) with the CMX system. The CMX solution relies on data from the WLCs to track and detect users' presence in the office area. Without the WLCs being added to CMX, the system cannot collect the necessary analytics and location data for its operations.

Question 4

Question Type: MultipleChoice

A wireless administrator must assess the different client types connected to Cisco Catalyst 9800 Series Wireless Controller without using any external servers. Which configuration must be added to the controller to achieve this assessment?

Options:

A- native profile
B- MAC classification
C- local profile
D- device classification

Answer:

D

Explanation:

To assess different client types connected to a Cisco Catalyst 9800 Series Wireless Controller without using external servers, the device classification feature (D) can be used. This feature allows the controller to classify devices based on their MAC addresses and other characteristics.Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question 5

Question Type: MultipleChoice

An employee with administrative rights has a Cisco OEAP at home. The employee must add an SSID to connect personal devices. Which two actions enable the employee to access the AP configuration? (Select two.)

Options:

A- Enter the IP address of the OEAP in a web browser.
B- Obtain the IP address of the OEAP from a sticker on the device.
C- Obtain the IP address of the OEAP from the home router of the employee.
D- Connect to the preconfigured SSID and obtain the IP address of the AP from the welcome page.
E- Connect to the IP address of the OEAP via SSH.

Answer:

A, E

Question 6

Question Type: MultipleChoice

Refer to the exhibit.

```
from ncclient import manager

wlc = manager.connect(
    host="192.168.1.10",
    port=830,
    username="admin",
    password="C1sco123",
    hostkey_verify=False
)

<config>
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
    <tacacs>
      <server>
        <name>TACACS-Server</name>
        <address>
          <ipv4>192.168.1.100</ipv4>
        </address>
        <key>Cisco123</key>
        [                                        ]
      </server>
    </tacacs>
  </native>
</config>
```

Refer to the exhibit. A network administrator must implement device access controls on a Cisco Catalyst C9800-80 WLC to secure administrative access for the GUI and CLI using TACACS+. The administrator is configuring the WLC directly using NETCONF with a Python script to define a TACACS+ server. This server will handle authentication for GUI and CLI access. The TACACS+ server at 192.168.1.100 requires a specific setting to ensure it is the primary server for authentication requests from the WLC. The administrator confirmed that the shared secret Cisco123 matches the server configuration, and the timeout is set to 10 seconds. Which XML code snippet must be placed onto the box in the code to complete the script?

```
<timeout>10</timeout>
<single-connection>true</single-connection>
```

```
<timeout>10</timeout>
<port49>true</port49>
```

```
<timeout>10</timeout>
<priority1>true</priority1>
```

```
<timeout>priority1</timeout>
<single-connection>port49</single-connection>
```

Options:

A- Option A
B- Option B
C- Option C
D- Option D

Answer:

A

Question 7

Question Type: MultipleChoice

Which AP model of the Cisco Aironet Active Sensor is used with Cisco DNA Center?

Options:

A- 1800s
B- 3600e
C- 3800s
D- 4800i

Answer:

A

Explanation:

The Cisco Aironet 1800s Active Sensor is designed to work with Cisco DNA Center. It is a compact, flexible sensor that provides insights into the wireless network's health and is used for proactive monitoring and troubleshooting.Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, which includes information on Cisco DNA Center and compatible AP models.

Question 8

Question Type: MultipleChoice

An engineer has been hired to implement a way for users to stream video content without having issues on the wireless network. To accomplish this goal, the engineer must set up a reliable way for a Media Stream to work between Cisco FlexConnect APs. Which feature must be enabled to guarantee delivery?

Options:

A- Unicast Direct
B- IGMP Direct
C- Multicast Direct
D- Multicast-to-Unicast Direct

Answer:

C

Explanation:

To ensure reliable streaming of video content on the wireless network between Cisco FlexConnect APs, Multicast Direct must be enabled. This feature allows for efficient multicast traffic delivery by converting multicast streams into unicast streams for each client, which guarantees delivery even in environments where reliable multicast is not feasible.Reference:= CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question 9

Question Type: MultipleChoice

A user is trying to connect to a wireless network that is configured for WPA2-Enterprise security using a corporate laptop. The CA certificate for the authentication server has been installed on the Trusted Root Certification Authorities store on the laptop. The user has been prompted to enter the credentials multiple times, but the authentication has not succeeded. What is causing the issue?

Options:

A- There is an IEEE invalid 802.1X authentication policy on the authentication server.
B- The user Active Directory account is locked out after several failed attempts.
C- There is an invalid 802.1X authentication policy on the authenticator.
D- The laptop has not received a valid IP address from the wireless controller.

Answer:

C

Explanation:

The issue described indicates a problem with the 802.1X authentication policy on the authenticator, which is typically the wireless controller or access point. Even though the CA certificate is correctly installed on the laptop, if the authenticator's policy is incorrectly configured or does not match the required settings for the corporate network, the user's authentication attempts will fail. It is essential to review and correct the 802.1X policy settings on the authenticator to resolve this issue.Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question 10

Question Type: MultipleChoice

A corporation is spread across different countries and uses MPLS to connect the offices. The senior management wants to utilize the wireless network for all the employees. To ensure strong connectivity and minimize delays, an engineer needs to control the amount of traffic that is traversing between the APs and the central WLC. Which configuration should be used to accomplish this goal?

Options:

A- FlexConnect mode with central switching enabled
B- FlexConnect mode with central authentication
C- FlexConnect mode with OfficeExtend enabled
D- FlexConnect mode with local authentication

Answer:

A

Explanation:

FlexConnect is a wireless solution for branch office and remote office deployments. It allows APs to switch data traffic locally and perform client authentication locally when their connection to the controller is interrupted. For the scenario described, where a corporation is spread across different countries and wants to minimize delays while ensuring strong connectivity, FlexConnect with central switching enabled is appropriate. This configuration allows traffic to be switched locally at the AP, reducing the amount of traffic traversing the MPLS network to the central WLC, thus minimizing delays.Reference:= CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question 11

Question Type: MultipleChoice

Refer to the exhibit.

Event	5405 RADIUS Request dropped
Failure Reason	11036 The Message-Authenticator RADIUS attribute is invalid

A wireless engineer has integrated the wireless network with a RADIUS server. Although the configuration on the RADIUS is correct, users are reporting that they are unable to connect. During troubleshooting, the engineer notices that the authentication requests are being dropped. Which action will resolve the issue?

Options:

A- Allow connectivity from the wireless controller to the IP of the RADIUS server.
B- Provide a valid client username that has been configured on the RADIUS server.
C- Configure the shared-secret keys on the controller and the RADIUS server.
D- Authenticate the client using the same EAP type that has been set up on the RADIUS server.

Answer:

C

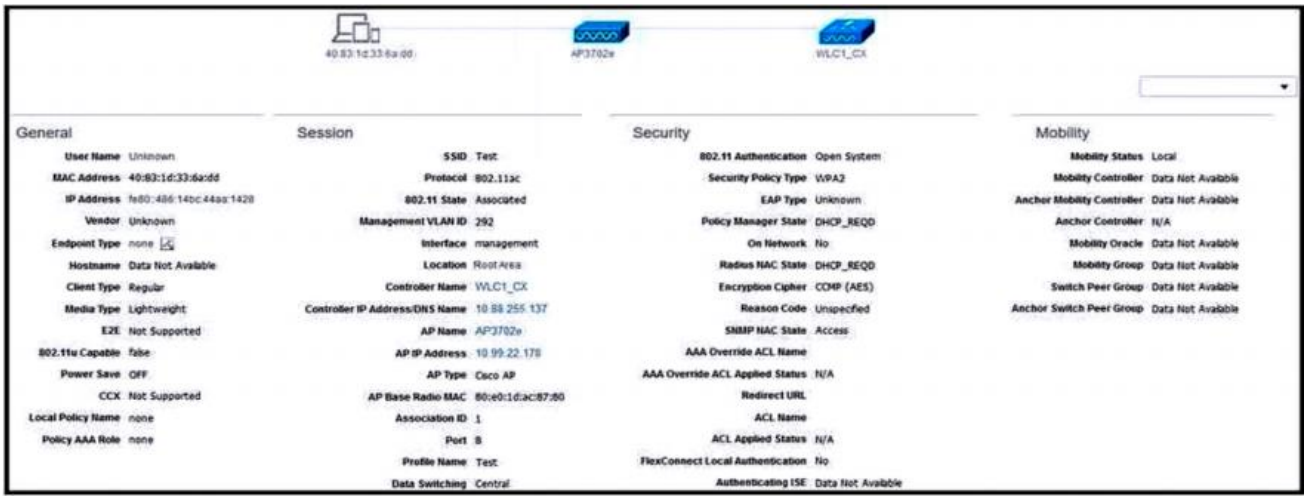
Explanation:

The issue described indicates that authentication requests from the wireless network to the RADIUS server are being dropped. This problem is often due to a mismatch in shared-secret keys between the wireless controller and the RADIUS server. The shared secret is a password-like value that must be configured on both sides to ensure secure communication. By configuring both sides with matching shared-secret keys, it ensures that authentication messages are properly encrypted and decrypted by each party, allowing for successful user connection.Reference: (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question 12

Question Type: MultipleChoice

Refer to the exhibit.



What is the reason that the wireless client cannot get the RUN state?

Options:

A- It has no communication with Cisco ISE.
B- An authentication error has occurred.
C- It is not getting the IP address.
D- Because of central switching, the AP must reach the Cisco ISE directly.

Answer:

C

Explanation:

The wireless client cannot reach the RUN state because it is not receiving an IP address. This is a crucial step in the connection process, as a valid IP address is necessary for the client to communicate on the network. Without it, the client cannot achieve the RUN state, which indicates full authentication and association.