PassQueen
a.k.a dumpsqueen.com

Implementing Cisco Enterprise Wireless Networks (300-430 ENWLSI)

Cisco 300-430

Version Demo

Total Demo Questions: 30

Total Premium Questions: 301

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Wireless Site Survey	20
Topic 2, Wired and Wireless Infrastructure	82
Topic 3, Mobility	30
Topic 4, WLAN High Availability	9
Topic 5, Security	99
Topic 6, Wireless Client Connectivity	18
Topic 7, Monitoring and Device Hardening	43
Total	301

QUESTION NO: 1

An engineer set up identity-based networking with ISE and configured AAA override on the WLAN. Which two attributes must be used to change the client behavior from the default settings? (Choose two.)

A. DHCP timeout

B. DNS server

C. IPv6 ACL

D. DSCP value

E. multicast address

ANSWER: C D

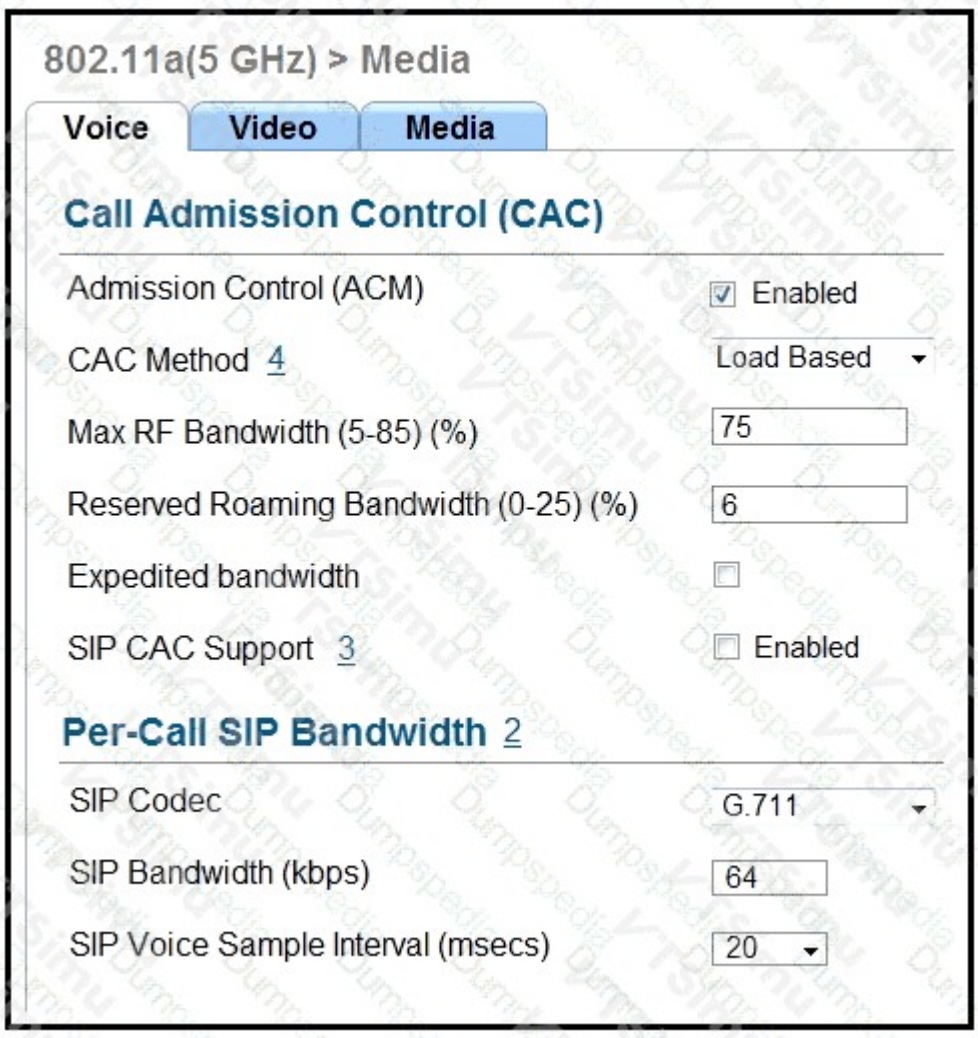
Explanation:

With AAA override enabled on the WLAN, Cisco ISE can return RADIUS authorization attributes that the wireless controller applies to an individual client session, replacing applicable WLAN-default behavior for that user. **IPv6 ACL** is an appropriate per-session authorization attribute because ISE can return an IPv6 access-control list name to the controller, which then enforces the named IPv6 policy for the authenticated wireless client. This enables identity-based IPv6 traffic permissions independent of the broadly configured WLAN policy.

DSCP value is also a supported controller-specific authorization setting. A RADIUS response can supply the Airespace DSCP value so the controller applies the specified Differentiated Services Code Point marking/handling to traffic for that client session. This lets authorization policy influence traffic treatment dynamically according to the user or endpoint identity established by ISE. Both settings are delivered as Cisco/Airespace vendor-specific RADIUS attributes and require AAA override to be enabled on the target WLAN so that session-specific RADIUS attributes can supersede the corresponding default settings. Cisco documents the controller's supported RADIUS attributes, including Airespace IPv6 ACL and DSCP attributes, at Cisco Wireless Controller RADIUS Attributes. See also Cisco ISE Authorization Policies.

QUESTION NO: 2

Refer to the exhibit.



Which two items must be supported on the VoWLAN phones to take full advantage of this WLAN configuration? (Choose two.)

A. TSPEC

B. SIFS

C. 802.11e

D. WMM

E. APSD

ANSWER: C D

Explanation:

802.11e and **WMM** enable a VoWLAN handset to participate in the wireless QoS mechanisms configured for voice. IEEE 802.11e defines MAC-layer quality-of-service enhancements, including enhanced distributed channel access, which differentiates traffic through access categories. This lets latency-sensitive voice frames contend for RF airtime with the priority characteristics appropriate for voice rather than using the same best-effort treatment as ordinary data.

Wi-Fi Multimedia is the Wi-Fi Alliance interoperability certification based on the relevant 802.11e QoS functions. A WMM-capable handset marks and queues its voice traffic in the voice access category and interoperates with the access point's WMM scheduling and prioritization behavior. Consequently, support for both 802.11e QoS operation and WMM allows the phone to use the WLAN's configured voice prioritization end to end over the wireless medium, helping reduce delay, jitter, and contention effects that directly affect call quality. Cisco's wireless QoS guidance identifies WMM as the standards-based mechanism used to classify and prioritize traffic over the WLAN, while the Wi-Fi Alliance describes WMM as QoS support for latency-sensitive multimedia applications such as voice. See Cisco Wireless QoS Configuration Guide and Wi-Fi Alliance: Wi-Fi CERTIFIED WMM.

QUESTION NO: 3

When using a Cisco Catalyst 9800 Series Wireless Controller, which statement about AutoQoS is true?

A. It has a set of predefined profiles that you cannot modify further

B. It matches traffic and assigns each matched packet to QoS groups

C. It automates deployment of wired QoS and makes wireless QoS implementation easier

D. It allows the output policy map to put specific QoS queues into specific subgroups

ANSWER: B

Explanation:

It matches traffic and assigns each matched packet to QoS groups. On Cisco Catalyst 9800 Series Wireless Controllers, AutoQoS provides a streamlined QoS classification mechanism: it recognizes traffic according to the AutoQoS classification rules and associates the traffic with an internal QoS group. That QoS-group value is then used by the controller's QoS policy framework to apply the appropriate treatment, such as marking, policing, or queueing behavior, at the relevant point in packet processing. This approach makes policy handling consistent because classification is separated from the later actions that a QoS policy may apply. Cisco documents AutoQoS on Catalyst 9800 controllers as matching traffic and assigning matched packets to QoS groups, which is the key behavior described in the correct statement. The feature is particularly useful when standard enterprise application classes need predictable wireless QoS handling without manually constructing every classification rule from scratch. For additional Cisco configuration and architecture details, see the Cisco Catalyst 9800 QoS Configuration Guide and Cisco's Catalyst 9800 Series Wireless Controllers overview.

QUESTION NO: 4

A wireless engineer must configure access control on a WLC using a TACACS+ server for a company that is implementing centralized authentication on network devices. Which role value must be configured under the shell profile on the TACACS+ server for a user with read-only permissions?

A. ADMIN

B. MANAGEMENT

C. MONITOR

D. READ

ANSWER: C

Explanation:

MONITOR is the TACACS+ shell-profile role value used to grant read-only administrative access to a Cisco wireless LAN controller. When the controller authenticates an administrative user through TACACS+, it obtains authorization attributes from the server in addition to validating the user's identity. The shell profile supplies the role information that the controller uses to assign the administrator's privilege level. Configuring the role as **MONITOR** maps the authenticated account to the controller's monitoring privilege, allowing the user to view controller status, clients, access points, logs, and configuration information without granting configuration-changing permissions. This supports centralized administrative authentication while enforcing least-privilege access for operational staff who need visibility but must not alter the wireless environment. The TACACS+ server must return the role in the shell authorization profile associated with that user or user group, and the WLC must be configured to use TACACS+ for management-user authorization. Cisco's wireless-controller documentation describes the use of TACACS+ administrative roles and role-based management access; Cisco's TACACS+ overview also explains that authorization attributes can be returned after authentication. See Cisco Wireless Controller Configuration Guide: Managing User Accounts and Cisco TACACS+ technology overview.

QUESTION NO: 5

An engineer is performing a Cisco Hyperlocation accuracy test and executes the cmxloc start command on Cisco CMX. Which two parameters are relevant? (Choose two.)

A. X, Y real location

B. client description

C. AP name

D. client MAC address

E. WLC IP address

ANSWER: A D

Explanation:

For a Cisco Hyperlocation accuracy test, **X, Y real location** and **client MAC address** are the relevant inputs to `cmxloc start`. The test compares CMX's calculated client position with a known physical reference point. The X and Y values provide that ground-truth location in the map's coordinate system, allowing the tool to calculate location error and assess the accuracy of the Hyperlocation deployment at the selected test point.

The client MAC address identifies the wireless endpoint whose location CMX must retrieve and evaluate. CMX uses this identifier to associate the measurement with the client's observed wireless data and its computed position. Together, the known real-world coordinates and the unique client identifier supply the essential information for a repeatable accuracy measurement: where the client actually is and which client CMX should locate. Cisco's CMX documentation describes CMX location processing and map-coordinate-based client location information, while Cisco Hyperlocation documentation provides the deployment context for high-accuracy location services. See the Cisco CMX Configuration Guide and Cisco Hyperlocation overview.

QUESTION NO: 6

A corporation has employees working from their homes. A wireless engineer must connect 1810 OEAP at remote teleworker locations. All configuration has been completed on the controller side, but the network readiness is pending. Which two configurations must be performed on the firewall to allow the AP to join the controller? (Choose two.)

A. Block UDP ports 1812 and 1813 on the firewall.

B. Enable NAT Address on the 5520 with an Internet-routable IP address.

C. Configure a static IP on the OEAP 1810.

D. Allow UDP ports 5246 and UDP port 5247 on the firewall.

E. Allow UDP ports 12222 and 12223 on the firewall.

ANSWER: B D

Explanation:

OfficeExtend APs deployed at teleworker sites establish a CAPWAP control and data connection across the Internet to the enterprise wireless controller. Therefore, the Internet-edge firewall must permit UDP port 5246 for CAPWAP control traffic and UDP port 5247 for CAPWAP data traffic. Where the controller is located behind a firewall or NAT device, these permitted inbound flows must be translated or forwarded to the controller's management interface.

Configuring a NAT address on the 5520 with an Internet-routable IP address provides the externally reachable controller address that remote OfficeExtend APs use. The NAT address must correspond to the public address presented by the firewall and must be reachable through the CAPWAP UDP port-forwarding policy. Together, the public NAT address and UDP 5246/5247 firewall allowance let an OEAP 1810 discover and establish its secure CAPWAP session with the controller from a home Internet connection. Cisco's OfficeExtend deployment guidance documents the requirement for CAPWAP UDP ports 5246 and 5247 and the use of a controller NAT address when the controller is behind NAT. See Cisco OfficeExtend Access Point Deployment Guide and Cisco Wireless Controller Configuration Guide.

QUESTION NO: 7

An engineer is configuring a BYOD deploymernt strategy and prefers a single SSID model.

Which technology is required to accomplish this configuration?

A. mobility service engine

B. wireless control system

C. Identity Services Engine

D. Prime Infrastructure

ANSWER: C

Explanation:

Identity Services Engine is required because it supplies the identity-based policy and onboarding functions that make a single-SSID BYOD design practical. Rather than separating employee-owned, guest, and personally owned devices through multiple WLAN names, the wireless network can send authentication and authorization requests to Cisco ISE using RADIUS. ISE evaluates the authenticated user and endpoint context, including device type and ownership, and returns the appropriate authorization result. This enables differentiated access control, such as assigning a suitable VLAN, downloadable access control list, or security group tag, while clients join the same SSID.

For BYOD specifically, ISE provides device-registration and certificate-provisioning workflows. A user can onboard a personal device through the BYOD portal, after which the device can use certificate-based authentication for secure subsequent access. The wireless controller enforces the access decision received from ISE, while ISE remains the central policy decision point and endpoint onboarding service. Cisco documents BYOD as an ISE capability that uses client provisioning, registration, and certificate-based access to securely onboard personal devices. See Cisco's ISE Bring Your Own Device documentation and the Cisco Identity Services Engine product overview.

QUESTION NO: 8

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

Refer to the exhibit. 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?

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:

Configure the shared-secret keys on the controller and the RADIUS server. A RADIUS shared secret is a value configured independently at both ends of the controller-to-server relationship. It is used to protect RADIUS attributes and to validate the authenticity of RADIUS messages. The wireless controller uses the configured secret when creating an Access-Request, and the RADIUS server uses the secret associated with that controller's source address to validate and process the request. The server likewise uses that shared secret when constructing its response.

If the secrets do not match, the RADIUS server cannot validate the request authenticator. In normal RADIUS operation, an invalid authenticator is commonly discarded rather than answered with a detailed failure response. That behavior appears in troubleshooting as authentication requests being dropped, while wireless users experience connection failures. Configuring an identical shared secret for the controller's RADIUS-server entry and the corresponding RADIUS-client definition on the server restores trusted RADIUS communication. The secret must also be associated with the correct controller source IP address, particularly where a management or dedicated interface is used as the RADIUS source. Cisco's RADIUS configuration guidance describes configuring a server key, and RFC 2865 defines the shared secret and request-authenticator validation behavior. See Cisco Wireless Controller RADIUS configuration documentation and RFC 2865.

QUESTION NO: 9

Which two events are outcomes of a successful RF jamming attack? (Choose two.)

A. disruption of WLAN services

B. unauthentication association

C. deauthentication broadcast

D. deauthentication multicast

E. physical damage to AP hardware

F. denial of wireless client connectivity

ANSWER: A F

Explanation:

A successful RF jamming attack creates radio-frequency interference that prevents legitimate Wi-Fi devices from using the affected channel reliably. Therefore, *disruption of WLAN services* is an expected outcome: clients can experience severe packet loss, retransmissions, poor throughput, and failure of time-sensitive applications while the interference is present. *Denial of wireless client connectivity* is also an outcome because the interference can prevent clients from successfully exchanging the 802.11 management and data frames required to discover, join, maintain, and use the WLAN. Depending on the jammer's strength, proximity, and the channel width in use, the impact can range from intermittent connectivity to a complete local wireless denial of service. Cisco wireless intrusion-prevention capabilities identify persistent RF interference and other sources that affect the RF environment; mitigation generally involves locating and removing or containing the interference source, rather than treating it as a normal client authentication event. Cisco also describes RF jamming as a wireless denial-of-service condition that affects communications over the radio medium. See Cisco's Wireless Controller Configuration Guide and Cisco's wireless security guidance.

QUESTION NO: 10

A network engineer must segregate all IPads on the guest WLAN to a separate VLAN. How does the engineer accomplish this task without using Cisco

ISE?

A. Create a local policy on the WLC.

B. Use 802.1x authentication to profile the devices.

C. Use an mDNS profile for the iPad device.

D. Enable RADIUS DHCP profiling on the WLAN.

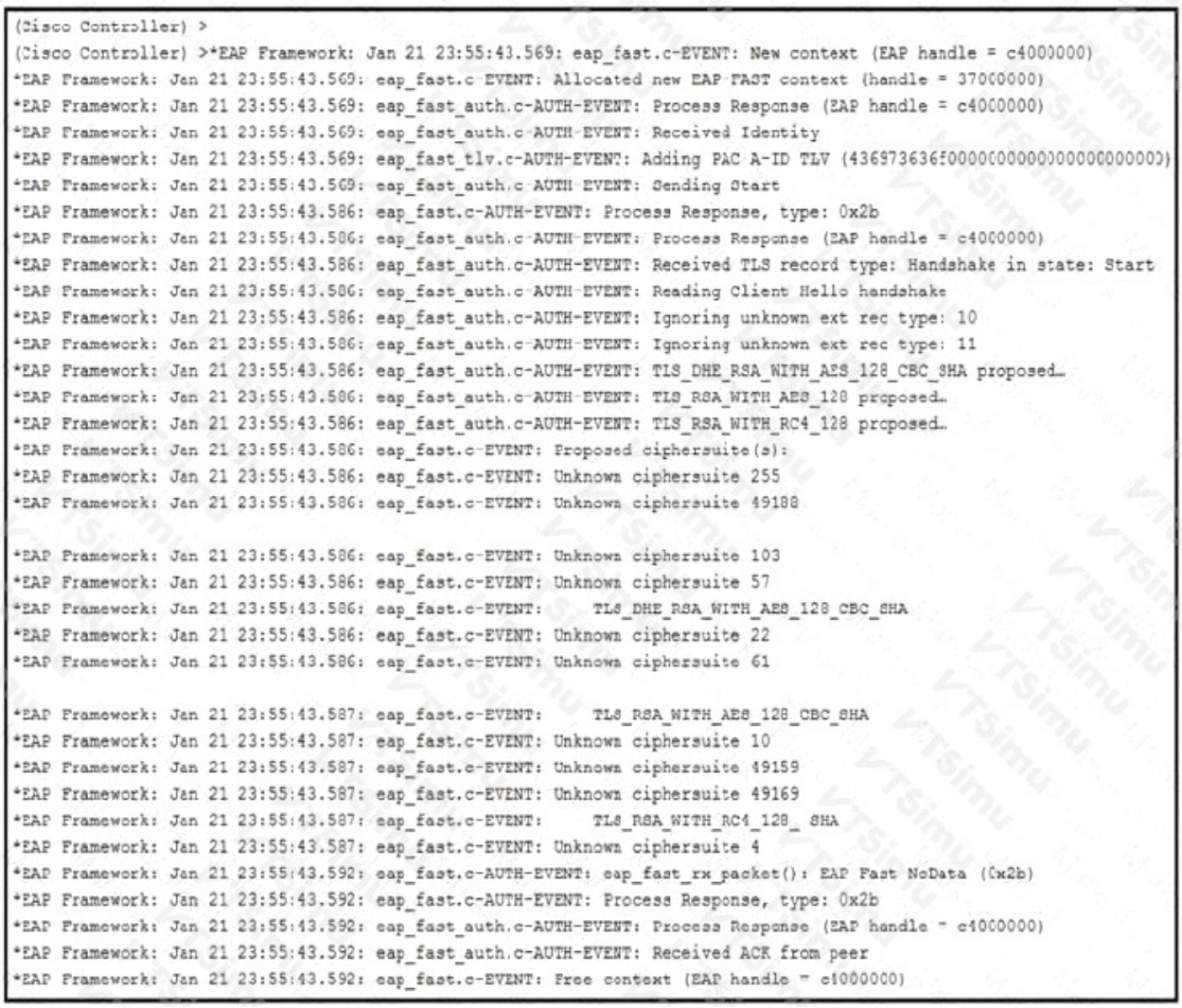
ANSWER: A

Explanation:

Create a local policy on the WLC. Cisco wireless controllers can perform client/device profiling locally and use the resulting profile as a condition in a locally configured policy. The controller identifies client characteristics from information available during association and onboarding, such as DHCP and HTTP attributes, and applies a policy action when the client matches the configured device classification. For this requirement, the local policy is built to match the iPad profile and assign the corresponding clients to the dedicated guest VLAN. This keeps iPad traffic logically separated at the controller while allowing the guest WLAN to remain available to other client types. The decision and VLAN assignment occur on the WLC, so an external Cisco ISE policy node is not required for the classification-to-VLAN workflow. The VLAN must also be present and reachable in the controller's wired infrastructure, and the applicable WLAN/policy configuration must permit the VLAN override or assignment. Cisco documents Catalyst 9800 client profiling and policy configuration in its Catalyst 9800 configuration guides. Cisco's Catalyst 9800 Wireless Controller documentation provides the related controller configuration references.

QUESTION NO: 11

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 (436973636f0000000000000000000000)
*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?

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: A

Explanation:

The client is failing to accept certificate. PEAP begins by establishing a TLS tunnel between the wireless client and the EAP server before protected user authentication occurs. The controller's local EAP debug shows that the TLS exchange is terminated with a certificate-related alert from the client. This indicates that the client does not trust, cannot validate, or otherwise declines the certificate presented by the WLC's local EAP service. Because the outer TLS tunnel is not established, PEAP cannot proceed to the inner user-authentication phase, so the wireless connection fails before credentials can be validated.

For PEAP clients, the server certificate must be valid for its intended use and chain to a certification authority trusted by the client. The certificate identity should also match the server name configured or expected by the client. Deploying a certificate issued by an enterprise CA and ensuring that the corresponding root and any intermediate CA certificates are installed in the client trust store allows the client to validate the WLC local EAP certificate and complete the PEAP TLS negotiation. Cisco's wireless controller configuration documentation is available at Cisco Wireless LAN Controller Configuration Guides; PEAP's protected TLS-tunnel model is described in RFC 5216.

QUESTION NO: 12

What is the difference between PIM sparse mode and PIM dense mode?

A. Sparse mode supports only one switch. Dense mode supports multiswitch networks.

B. Sparse mode floods. Dense mode uses distribution trees.

C. Sparse mode uses distribution trees. Dense mode floods.

D. Sparse mode supports multiswitch networks. Dense mode supports only one switch.

ANSWER: C

Explanation:

Sparse mode uses distribution trees. Dense mode floods. is the best answer because PIM sparse mode (PIM-SM) is designed for networks in which multicast receivers are relatively sparsely distributed. Routers do not forward multicast traffic onto every PIM-enabled interface by default. Instead, routers with interested downstream receivers explicitly send PIM Join messages, creating multicast distribution-tree state only along the required path. PIM-SM can initially use a shared tree rooted at a Rendezvous Point and can transition to a source-specific shortest-path tree when appropriate.

PIM dense mode (PIM-DM) follows a flood-and-prune model. When a multicast source begins transmitting, the traffic is initially flooded through the PIM domain. Routers that have no interested downstream receivers subsequently send Prune messages, removing unnecessary branches from forwarding. This behavior makes the concise distinction in the answer accurate: sparse mode relies on joined distribution-tree branches, while dense mode begins by flooding multicast traffic and then prunes it. Cisco documents PIM-SM join behavior and shared/source-tree operation in its PIM Sparse Mode configuration guide, and describes PIM-DM flood-and-prune operation in its PIM Dense Mode configuration guide.

QUESTION NO: 13

Branch wireless users report that they can no longer access services from head office but can access services locally at the site. New wireless users can associate to the wireless while the WAN is down.

Which three elements (Cisco FlexConnect state, operation mode, and authentication method) are seen in this scenario? (Choose three.)

A. authentication-local/switch-local

B. WPA2 personal

C. authentication-central/switch-central

D. lightweight mode

E. standalone mode

F. WEB authentication

ANSWER: A B E

Explanation:

The FlexConnect access point is operating in **standalone mode**, which is the state entered when its WAN connection to the wireless LAN controller is unavailable. In this state, a FlexConnect AP can continue providing service for WLANs designed for branch survivability. The ability for existing wireless users to reach resources at the branch, while resources at head office are unreachable, indicates traffic is being handled locally rather than tunneled across the failed WAN.

authentication-local/switch-local is the appropriate FlexConnect WLAN behavior for this condition. Local switching keeps client data at the branch, allowing access to local network services independently of controller reachability. Local authentication supports client access during controller disconnection when the WLAN and AP are configured for locally survivable authentication behavior.

WPA2 personal uses a pre-shared key, so a newly connecting client can authenticate without requiring a reachable centralized AAA service across the WAN. This fits the observation that new users can associate while the WAN is down. Cisco documents that FlexConnect provides local switching and supports continued branch WLAN operation when an AP is disconnected from its controller. See Cisco Catalyst 9800 Series FlexConnect configuration documentation and Cisco FlexConnect deployment guidance.

QUESTION NO: 14

An enterprise has two WLANs configured on WLC. It is reported that when converting APs to FlexConnect mode, WLAN A works but WLAN B does not. When converting APs to local mode, WLAN B

works, but WLAN A does not. Which action is needed to complete this configuration?

A. Create a Cisco FlexConnect group with WLAN-VLAN mapping.

B. Disable local switching on the WLANs.

C. Map the AP group to the WLAN interface.

D. Join the APs to a Cisco FlexConnect group.

ANSWER: A

Explanation:

Create a Cisco FlexConnect group with WLAN-VLAN mapping. FlexConnect APs can use local switching, in which client traffic is bridged directly onto a VLAN at the branch site instead of being tunneled to the controller. To support this behavior consistently for the applicable WLAN, the controller must provide a WLAN-to-VLAN association that the FlexConnect AP can use. A FlexConnect group centralizes this configuration for multiple APs and enables VLAN mappings to be applied consistently across the group.

This mapping is especially important when a WLAN must work in FlexConnect local-switching operation while another WLAN uses controller-based handling in local AP mode. The group mapping identifies the local wired VLAN to which traffic for the locally switched WLAN is assigned, allowing the AP to bridge client frames correctly when operating as FlexConnect. Cisco documents that FlexConnect groups support WLAN VLAN mappings and that these mappings are downloaded to member APs for local switching. See Cisco's FlexConnect deployment guidance and the Cisco Wireless Controller FlexConnect configuration guide.

QUESTION NO: 15

Which two events are outcomes of a successful RF jamming attack? (Choose two.)

A. disruption of WLAN services

B. failure of client authentication and association

C. deauthentication broadcast

D. deauthentication multicast

E. physical damage to AP hardware

ANSWER: A B

Explanation:

A successful RF jamming attack creates radio-frequency interference that raises the noise floor or occupies the wireless channel. This prevents legitimate WLAN transmissions from being reliably received and decoded, resulting in disruption of WLAN services. Clients may experience severe packet loss, excessive retransmissions, loss of connectivity, and an inability to pass normal user traffic while the jammer is active. RF jamming can also cause failure of client authentication and association because those processes depend on successful bidirectional 802.11 frame exchanges between the client and access point. When interference prevents management and control frames from being exchanged consistently, a new client may be unable to join the WLAN, and a reconnecting client may fail to complete the authentication or association workflow. Cisco describes interference as a condition that degrades wireless performance and can prevent client connectivity; identifying the affected RF spectrum and channel utilization is therefore central to troubleshooting and wireless intrusion detection. See Cisco's wireless interference guidance and the Cisco RF Interference Deployment Guide.

QUESTION NO: 16

An engineer needs read/write access to rename access points and add them to the correct AP groups on a wireless controller. Using Cisco ISE TACACS, which custom attributes is the minimum required?

A. role1=WLAN

B. role1=WLAN role2=SECURITY

C. role1=WLAN role2=WIRELESS

D. role1=WIRELESS

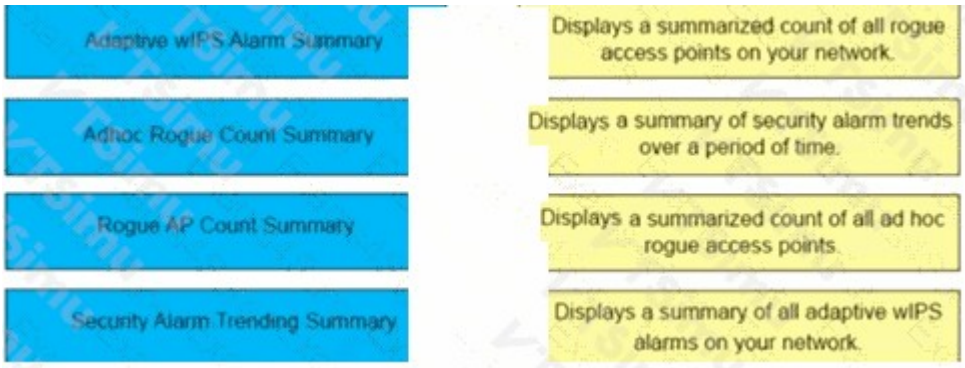
ANSWER: D

Explanation:

`role1=WIRELESS` is the minimum required TACACS+ authorization attribute because it assigns the Wireless role on the Cisco wireless controller. This role is intended for administrators who need read/write access to wireless configuration functions, including access point administration. An engineer assigned this role can perform AP-focused operational tasks such as changing an access point's name and assigning the access point to an AP group, without requiring the broader privileges associated with a full controller administrator role. In Cisco ISE, this value is typically returned to the controller as a TACACS+ shell profile custom attribute, commonly using the Cisco AV-pair format `Airespace-AVPair=role1=WIRELESS`. The controller consumes the returned role value during administrative authorization and applies the corresponding wireless-management permissions to the authenticated user session. Because the requested work is limited to wireless and AP-group administration, the single Wireless role is sufficient and represents the least-privilege assignment for the stated requirement. Cisco documents the controller's role-based TACACS+ administrative authorization model and the use of role attributes for management users in its Cisco Wireless Controller Configuration Guide; Cisco ISE TACACS+ shell-profile configuration is described in the Cisco ISE Administrator Guide.

QUESTION NO: 17 - (DRAG DROP)

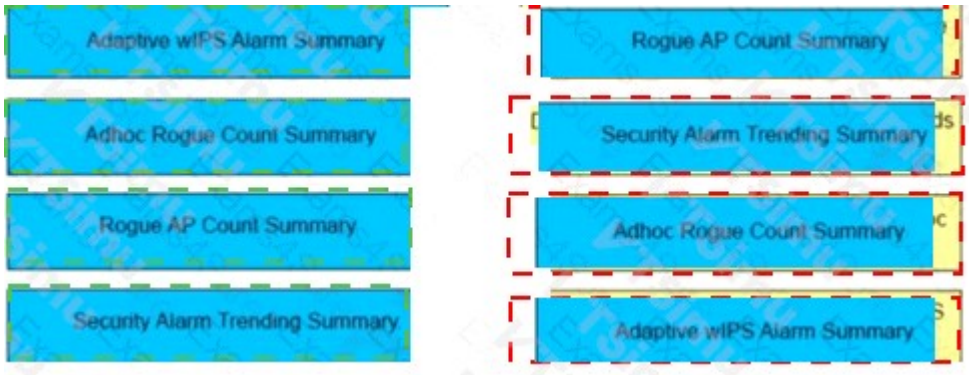
A wireless engineer wants to schedule monthly security reports in Cisco Prime infrastructure. Drag and drop the report the from the left onto the expected results when the report is generated on the right.



ANSWER:

Answer:

Answer:



Explanation:

Cisco Prime Infrastructure security reporting uses report names that identify both the monitored security feature and the type of aggregation produced when the scheduled report runs. **Rogue AP Count Summary** is the report used to produce a summarized count of rogue access points detected in the network. **Security Alarm Trending Summary** provides the historical, time-oriented view of security alarms, making it the report that summarizes security alarm trends over a selected period. **Adhoc Rogue Count Summary** specifically focuses on ad hoc rogue access points and returns their summarized count. **Adaptive wIPS Alarm Summary** is associated with adaptive wireless intrusion prevention system alarms and produces a summary of those alarms for the network.

These mappings follow the normal Cisco report-naming convention: the feature named in the report title—rogue access points, security alarms, ad hoc rogues, or adaptive wIPS alarms—is the data domain included in the output, while terms such as *Count Summary*, *Trending Summary*, and *Alarm Summary* identify whether the result is an aggregate count, a trend over time, or an alarm-focused summary. This lets an engineer schedule monthly reports with the expected content rather than relying on a report title alone. Cisco Prime Infrastructure documentation describes the platform's reporting capabilities and the use of reports to collect and present managed-network information in its Cisco Prime Infrastructure User Guide.

QUESTION NO: 18

A customer uses a Cisco Catalyst 9800 Series Wireless Controller and Cisco 802.11axAPs. The management has requested the ability to see what type of devices are on the wireless network. Which two types of local device profiling must be used? (Choose two)

A. Ip address

B. wireless supplicant

C. RADIOUS

D. DHCP

E. MAC Address OUI

ANSWER: D E

Explanation:

DHCP and **MAC Address OUI** provide the Catalyst 9800 controller with locally available device-identification attributes. DHCP profiling uses information supplied during a client's DHCP exchange, particularly the DHCP option parameters and their ordering, to build a fingerprint that can indicate the operating system or device category. This is valuable because many wireless endpoint types expose distinctive DHCP characteristics when obtaining an address.

MAC Address OUI profiling examines the organizationally unique identifier in the first portion of a client MAC address. The OUI identifies the organization to which the MAC block was assigned and can help classify clients by manufacturer. Used together, DHCP fingerprinting and OUI lookup give the controller complementary evidence: DHCP characteristics help identify the client platform or behavior, while OUI data supplies vendor context. This allows local profiling to classify wireless devices without requiring an external identity-services platform for those basic profiling inputs. Cisco documents device profiling as a Catalyst 9800 wireless-controller capability; see the Cisco Catalyst 9800 Series support documentation and Cisco's Catalyst 9800 configuration guides.

QUESTION NO: 19

An engineer is following the proper upgrade path to upgrade a Cisco AireOS WLC from version 7.3 to 8.9. Which two ACLs for Cisco CWA must be configured when upgrading from the specified codes?

(Choose two.)

A. Permit 0.0.0.0 0.0.0.0 any DNS any

B. Permit 0.0.0.0 0.0.0.0 UDP DNS any

C. Permit 0.0.0.0 0.0.0.0 UDP any DNS

D. Permit any any any

E. Permit 0.0.0.0 0.0.0.0 UDP any any

ANSWER: B C

Explanation:

Central Web Authentication requires clients to resolve names before they can reach the authentication portal and complete redirection. Therefore, the redirect ACL must explicitly permit DNS request traffic from a client's ephemeral UDP source port to the DNS service port, represented by *Permit 0.0.0.0 0.0.0.0 UDP any DNS*. It must also permit the corresponding DNS response traffic, which originates from the DNS service port and returns to the client's ephemeral UDP port, represented by *Permit 0.0.0.0 0.0.0.0 UDP DNS any*.

These two entries provide the bidirectional UDP flow needed for ordinary DNS resolution while preserving the intended preauthentication access-control behavior of the CWA redirect ACL. DNS access is important in this workflow because a wireless client commonly uses a hostname for the guest portal, identity service, or other resources required during authentication; without successful resolution and return traffic, the client cannot reliably continue the web-authentication exchange. Cisco's CWA guidance documents DNS as traffic that must be allowed by the redirect ACL, and Cisco wireless configuration documentation describes ACL rules as protocol- and port-specific traffic permits. See Cisco's Central Web Authentication configuration guidance and the Cisco AireOS client-access control documentation.

QUESTION NO: 20

A hospital wants to offer indoor directions to patient rooms utilizing its existing wireless infrastructure. The wireless network has been using location services specifications. Which two components must be installed to support this requirement? (Choose two.)

A. WIPS

B. Cisco MSE

C. Cisco CMX Visitor Connect

D. Cisco CMX AppEngage

E. Cisco CMX Analytics

ANSWER: B D

Explanation:

Cisco MSE and **Cisco CMX AppEngage** provide the two necessary functional layers for this indoor wayfinding deployment. Cisco Mobility Services Engine supplies the location-services platform that collects wireless location information and calculates the position of wireless devices within the mapped hospital environment. Accurate client location is the foundational input needed to determine where a visitor is relative to a patient room, hallway, or other destination.

Cisco CMX AppEngage uses that location context to support location-aware experiences in a mobile application. It enables organizations to integrate CMX location capabilities with an app and present contextual content and services to visitors. For a hospital navigation use case, the app can use the client location supplied by the location-services platform together with the facility map and destination information to guide a visitor through the building. This combines the backend positioning capability of Cisco MSE with the application-facing engagement and location integration capabilities of Cisco CMX AppEngage. Cisco describes the Mobility Services Engine location role in its MSE data sheet and identifies AppEngage as a CMX capability for location-aware mobile engagement in the Cisco CMX data sheet.

QUESTION NO: 21

An engineer configures the wireless LAN controller to perform 802.1x user authentication. Which configuration must be enabled to ensure that client devices can connect to the wireless, even when WLC cannot communicate with the RADIUS?

A. pre-authentication

B. local EAP

C. authentication caching

D. Cisco Centralized Key Management

ANSWER: B

Explanation:

local EAP is the required configuration because it lets the wireless LAN controller authenticate applicable 802.1X clients against credentials maintained locally on the controller, rather than requiring every authentication request to be processed by an external RADIUS server. When it is configured as the fallback authentication mechanism and the configured RADIUS servers are unreachable, the controller can use its local EAP user database to continue authenticating clients. This provides authentication-service resilience during a RADIUS connectivity or availability outage.

To use this capability, the administrator must enable local EAP on the controller and create the necessary local user entries and credentials. The WLAN security configuration must also use a compatible 802.1X/EAP setup and be associated with the appropriate authentication-server configuration. Local EAP is therefore not merely a record of an earlier authentication; it is an authentication service hosted directly by the controller that can be used when external AAA communication cannot be completed. Cisco documents local EAP as controller-based authentication and describes its use with external RADIUS availability considerations in the Cisco Wireless Controller Configuration Guide. The underlying 802.1X framework is defined by the Extensible Authentication Protocol (EAP), RFC 3748.

QUESTION NO: 22

For security purposes, an engineer enables CPU ACL and chooses an ACL on the Security > Access Control Lists > CPU Access Control Lists menu. Which kind of traffic does this change apply to as soon as the change is made?

A. wireless traffic only

B. wired traffic only

C. VPN traffic

D. wireless and wired traffic

ANSWER: D

Explanation:

wireless and wired traffic is correct because a CPU access control list protects the controller's control plane by filtering packets that are destined for the wireless LAN controller CPU. This is distinct from a WLAN or interface ACL, which is associated with a particular client data path or interface. Once CPU ACL processing is enabled and an ACL is selected, the controller evaluates qualifying CPU-bound traffic received from both the wired side and the wireless side against that ACL. The policy therefore takes effect immediately for packets attempting to reach controller services and the controller's management/control plane, such as management and control protocols addressed to the controller itself. It does not wait for a WLAN-specific ACL assignment, because the CPU ACL is a global controller CPU protection mechanism. Cisco describes CPU ACLs as a means of controlling traffic directed to the controller CPU and notes their applicability to wired and wireless traffic. This behavior helps reduce the controller control plane's exposure to unauthorized or unnecessary traffic while preserving normal forwarding of traffic that is not directed to the CPU. See Cisco's Cisco Wireless Controller Security Configuration Guide and the Cisco Wireless Controller Command Reference.

QUESTION NO: 23

CMX Facebook Wi-Fi allows access to the network before authentication. Which two elements are available? (Choose two.)

A. Allow HTTP traffic only before authentication and block all the traffic.

B. Allow all the traffic before authentication and intercept HTTPS only.

C. Allow HTTPs traffic only before authentication and block all other traffic.

D. Allow all the traffic before authentication and intercept HTTP only.

E. Allow SNMP traffic only before authentication and block all the traffic.

ANSWER: C D

Explanation:

CMX Facebook Wi-Fi provides configurable preauthentication access behavior so that a client can reach the resources needed to complete the Facebook Wi-Fi flow while the network still controls what is reachable before authorization. The available behavior represented by *Allow HTTPs traffic only before authentication and block all other traffic.* permits secure web traffic during the unauthenticated stage and restricts other traffic until the user completes authentication. This is useful when the required interaction is expected to use HTTPS.

The alternative available behavior, *Allow all the traffic before authentication and intercept HTTP only.*, permits client traffic before authentication while redirecting unencrypted HTTP requests to the portal workflow. This approach uses HTTP interception as the trigger for captive-portal presentation, while retaining broader preauthentication access. These are the two CMX Facebook Wi-Fi preauthentication access models described for configuring the service; the administrator selects the model appropriate to the guest-access and portal-redirection design. Cisco's CMX Facebook Wi-Fi configuration documentation is available at Cisco CMX Facebook Wi-Fi documentation. For related captive portal and web authentication behavior, see Cisco Wireless Controller Web Authentication Configuration Guide.

QUESTION NO: 24

A company wants to switch to BYOD to reduce IT support costs for the company. Which option is an impact of BYOD should be considered?

A. increased VPN connections

B. restricted device enforcement

C. increased phishing attacks

D. decreased support calls

ANSWER: C

Explanation:

increased phishing attacks is an important BYOD impact to consider because personally owned endpoints can access corporate email, applications, and data while being outside the organization's full lifecycle control. A BYOD program commonly introduces varied operating-system versions, patch levels, endpoint-security products, browser configurations, and user security practices. That diversity can increase exposure to credential-harvesting messages and malicious links, particularly when personal devices are used for both private and business communications. A successful BYOD design should therefore pair device onboarding with identity-based access controls, multifactor authentication, email and web protections, endpoint compliance checks, user awareness training, and an incident-response process for compromised devices or credentials. Cisco describes BYOD as enabling personal-device access while requiring secure policy enforcement and network visibility; these controls are fundamental when protecting enterprise resources accessed from unmanaged or partially managed devices. NIST likewise emphasizes that organizations must address the security risks of personally owned mobile devices through defined policies and technical safeguards. Reducing support expense can be a business objective, but the security consequences of broadening the endpoint population must be assessed and mitigated before deployment. See Cisco's BYOD solution overview and NIST SP 800-124 Rev. 2.

QUESTION NO: 25

An engineer is setting up a WLAN to work with a Cisco ISE as the AAA server. The company policy requires that all users be denied access to any resources until they pass the validation. Which component must be configured to achieve this stipulation?

A. WPA2 passkey

B. AAA override

C. CPU ACL

D. preauthentication ACL

ANSWER: D

Explanation:

A preauthentication ACL must be configured because it defines the traffic that a wireless client is permitted to send before completing the required validation process, such as web authentication through Cisco ISE. The controller applies this ACL while the client is in the preauthentication state, allowing only the minimum connectivity needed to reach required infrastructure, commonly including DNS, DHCP, and the ISE portal. All other traffic is denied until validation succeeds. This implements the policy requirement that users cannot access internal or external resources before being validated, while still allowing the client to obtain an address and be redirected or connected to the authentication service. After successful validation, the client transitions to its authorized access state and receives the access controls defined by the WLAN and the applicable ISE authorization result. Cisco documents that a preauthentication ACL is used to control traffic before web authentication and should permit access to resources necessary for the authentication workflow. See Cisco's Wireless Controller Configuration Guide and the Cisco ISE configuration guides.

QUESTION NO: 26

A network engineer is implementing BYOD on a wireless network. Based on the customer requirements, a dual SSID approach must be taken. Which two advanced WLAN configurations must be performed? (Choose two.)

A. Set NAC State to Radius NAC.

B. Set Allow AAA Override to Enabled.

C. Set DHCP Addr. Assignment to Required.

D. Select DHCP Profiling.

E. Select Enable Session Timeout.

ANSWER: A B

Explanation:

For a Cisco ISE BYOD deployment using separate onboarding and secure-access SSIDs, **Set NAC State to Radius NAC.** is required so that the wireless controller uses RADIUS-based Network Admission Control interactions for the WLAN. This setting allows ISE to participate in controlling the client session after authentication, including applying authorization outcomes as the endpoint transitions through BYOD registration and certificate-based access.

Set Allow AAA Override to Enabled. is also required because ISE must be able to return per-user or per-session authorization attributes to the controller. AAA override enables the controller to honor RADIUS attributes supplied by ISE, such as the VLAN, ACL, QoS policy, or other authorization policy elements appropriate to the authenticated BYOD user and device. This is particularly important in a dual-SSID design, where the onboarding workflow and the post-provisioning secure-access workflow rely on ISE-driven policy decisions rather than a single static WLAN policy.

Cisco's BYOD prescriptive deployment guidance identifies RADIUS NAC and AAA Override as advanced WLAN settings for this workflow. See the Cisco ISE BYOD Prescriptive Deployment Guide and Cisco ISE BYOD administration documentation.

QUESTION NO: 27

What is configured to use more than one port on the OEAP to extend the wired network?

A. remote LAN ACL

B. AAA override

C. client load balancing

D. remote LAN

ANSWER: D

Explanation:

Remote LAN is configured on an OfficeExtend access point (OEAP) to extend a wired LAN from the central wireless controller to the remote location. A remote LAN is a controller-defined wired network service that is associated with an OEAP Ethernet port and a VLAN. When a wired endpoint connects to an assigned OEAP port, its traffic is carried through the OEAP's CAPWAP tunnel to the controller, where the remote-LAN configuration applies the appropriate VLAN and network policy. This makes the remote Ethernet connection an extension of the enterprise wired network rather than simply a locally bridged home-office connection.

Multiple physical Ethernet ports on supported OEAP models can be assigned for Remote LAN use, allowing more than one wired device or wired-network connection to use the centrally managed enterprise network. The controller configuration creates the Remote LAN, specifies its identifier and VLAN, and associates it with the relevant access point Ethernet interfaces. Cisco documents Remote LAN as the feature used to provide wired connectivity through OfficeExtend APs and to map Ethernet ports to centrally managed wired VLAN services. See Cisco's Remote LAN configuration documentation and its OfficeExtend AP deployment overview.

QUESTION NO: 28

Which two statements about the requirements for a Cisco Hyperlocation deployment are true? (Choose two.)

A. After enabling Cisco Hyperlocation on Cisco CMX, the APs and the wireless LAN controller must be restarted.

B. NTP can be configured, but that is not recommended.

C. The Cisco Hyperlocation feature must be enabled on the wireless LAN controller and Cisco CMX.

D. The Cisco Hyperlocation feature must be enabled only on the wireless LAN controller.

E. If the Cisco CMX server is a VM, a high-end VM is needed for Cisco Hyperlocation deployments.

ANSWER: C E

Explanation:

Cisco Hyperlocation must be enabled in both the wireless LAN controller and Cisco CMX because the two systems have complementary functions. The controller enables and collects the enhanced location telemetry from compatible access points, while Cisco CMX consumes and processes that telemetry to calculate the more precise client location information. Enabling the capability in only one component does not establish the complete Hyperlocation workflow.

A high-end virtual-machine deployment is also required when Cisco CMX is deployed as a VM for Hyperlocation. Hyperlocation produces substantially more location-related data and requires additional compute resources compared with standard location processing. Cisco documents its VM sizing profiles for CMX and identifies the high-end profile as the appropriate virtual deployment type for this feature, ensuring sufficient CPU, memory, and storage performance for the location calculations and telemetry load. Review Cisco's Cisco CMX installation and configuration guides for CMX deployment guidance and the Cisco Hyperlocation configuration documentation for controller and CMX enablement requirements.

QUESTION NO: 29

A wireless engineer must implement a corporate wireless network for a large company in the most efficient way possible. The wireless network must support 32 VLANs for 300 employees in different departments. Which solution must the engineer choose?

A. Configure a second WLC to support half of the APs in the deployment.

B. Configure one single SSID and implement Cisco ISE for VLAN assignment according to different user roles.

C. Configure different AP groups to support different VLANs, so that all of the WLANs can be broadcast on both radios.

D. Configure 16 WLANs to be broadcast on the 2.4-GHz band and 16 WLANs to be broadcast on the 5.0-GHz band.

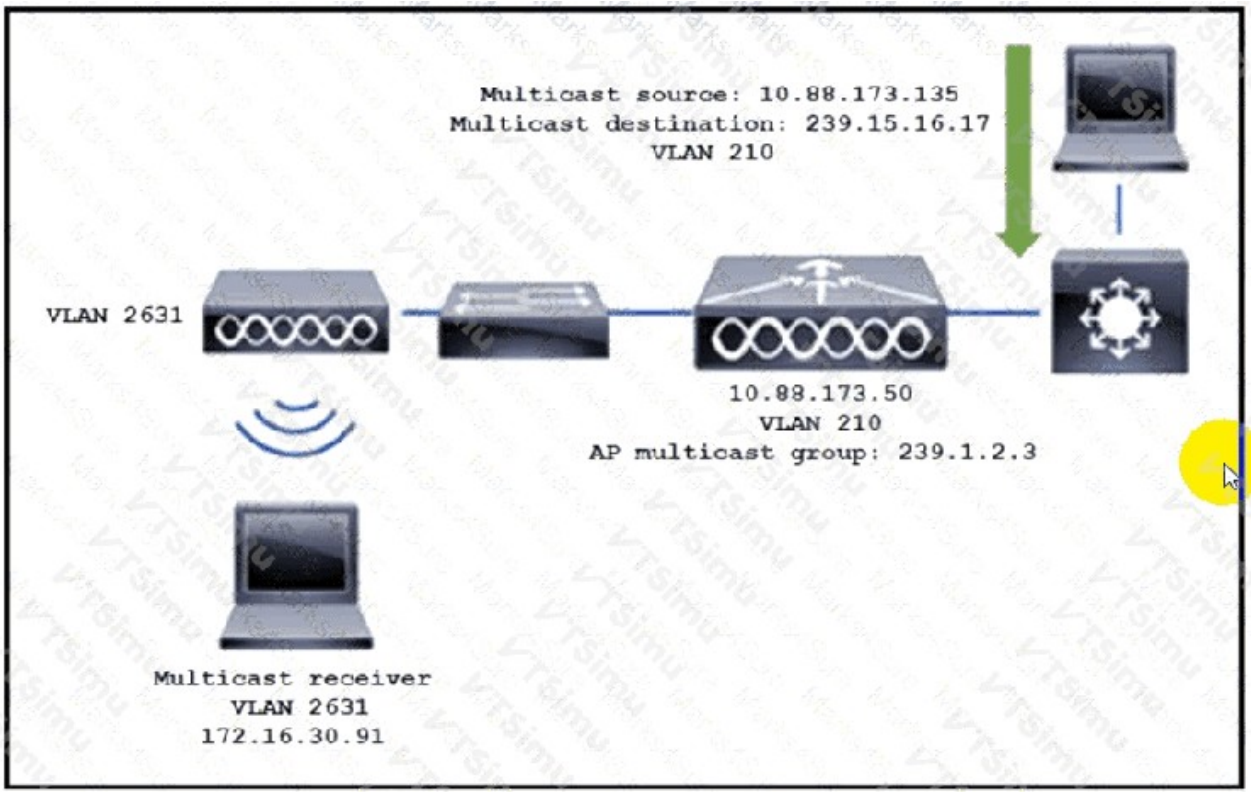
ANSWER: B

Explanation:

Configure one single SSID and implement Cisco ISE for VLAN assignment according to different user roles. is the most efficient design because it separates user access policy from the wireless network name. A single corporate SSID can use WPA2/WPA3-Enterprise with 802.1X authentication, forwarding authentication requests to Cisco ISE through RADIUS. ISE evaluates the authenticated user's identity, group membership, device context, and authorization policy, then returns the appropriate VLAN assignment as RADIUS authorization attributes. The wireless controller applies that result and places each user into the department-specific VLAN while all users join the same SSID.

This approach supports the required 32 departmental VLANs without creating an excessive number of SSIDs. It provides a scalable operational model for 300 employees: adding, moving, or changing a user's departmental access is handled in the identity and authorization policy rather than by modifying WLAN broadcasts or reconfiguring client SSID profiles. Cisco documents VLAN assignment through RADIUS authorization as part of identity-based network access, and Cisco ISE authorization policies can return the network access attributes required for differentiated access. See Cisco's Identity Services Engine Administrator Guide and the Cisco Wireless Controller Configuration Guide.

QUESTION NO: 30



Refer to the exhibit. A network administrator must implement a video stream using the multicast-direct feature on a Cisco Catalyst 9800 WLC. After the configuration, the clients should be able to stream video from a multicast source. The APs used are Cisco 9130-AXI. Which two implementations must the engineer perform? (Choose two.)

A. Enable multicast routing on VLAN 2631 for the wireless client VLAN.

B. Enable multicast routing on VLAN 210 for the wireless management VLAN.

C. Enable IGMP v3 support to support AP IOS-based access points.

D. Enable IGMP support across multicast hosts, routers, and multilayer switches.

E. Configure the CAPWAP multicast group address to enable multicast mode on the device.

ANSWER: A C

Explanation:

Multicast routing must be enabled for VLAN 2631, the wireless-client VLAN, so multicast traffic from the source can be routed to the client subnet associated with the WLAN. Multicast Direct does not use a controller-to-AP multicast CAPWAP group; instead, the Catalyst 9800 uses client group-membership information and sends the multicast stream to the applicable APs using unicast CAPWAP encapsulation. The client VLAN must therefore participate correctly in the routed multicast design so that the controller can receive and distribute the stream to interested wireless clients.

Enable IGMP v3 support to support AP IOS-based access points because Cisco 9130-AXI access points are Cisco IOS XE-based APs. For Multicast Direct, IGMPv3 is required for this AP platform family to communicate multicast group joins and leaves correctly, allowing the controller to identify APs with interested receivers and replicate the stream only where needed. This supports efficient video delivery while avoiding unnecessary multicast flooding over the wireless network. Cisco documents Multicast Direct behavior and its multicast/IGMP requirements in the Catalyst 9800 wireless controller configuration guide: Cisco Catalyst 9800 Series Multicast Configuration Guide. Platform details for the AP are available from Cisco Catalyst 9130AX Series Data Sheet.