ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

On a branch office deployment, it has been noted that if the FlexConnect AP is in standalone mode and loses connection to the WLC, all clients are disconnected, and the SSID is no longer advertised. Considering that FlexConnect local switching is enabled, which setting is causing this behavior?

A. ISE NAC is enabled

B. 802.11r Fast Transition is enabled

C. Client Exclusion is enabled

D. FlexConnect Local Auth is disabled

Answer: D

Explanation:
When FlexConnect APs are in standalone mode due to losing connection to the WLC, they should still be able to serve clients if local switching and authentication are enabled. The issue described occurs because FlexConnect Local Authentication is disabled. With local auth enabled, the AP can authenticate clients directly, without needing to communicate with the WLC, thus allowing the SSID to remain advertised and clients to stay connected even if the WLC is unreachable. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 2

An engineer must implement intrusion protection on the WLAN. The AP coverage is adequate and on-channel attacks are the primary concern. The building is historic, which makes adding APs difficult. Which AP mode and submode must be implemented?

A. AP mode: local, AP submode: none

B. AP mode: monitor, AP submode: WIPS

C. AP mode: monitor, AP submode: none

D. AP mode: local, AP submode: WIPS

Answer: B

Explanation:

In a historic building where adding APs is challenging, the best approach to implement intrusion protection with a focus on on-channel attacks is to use APs in monitor mode with the Wireless Intrusion Prevention System (WIPS) submode. This setup allows the APs to dedicate their time to scanning the environment for threats without serving clients, which is suitable given the adequate
coverage and the need to monitor for attacks. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 3

An engineer is implementing a FlexConnect group for access points at a remote location using local switching but central DHCP. Which client feature becomes available only if this configuration is changed?

A. multicast

B. static IP

C. fast roaming

D. mDNS

Answer: C

Explanation:

In a FlexConnect group with local switching but central DHCP, clients can use features like multicast and static IP without any issues. However, fast roaming, which allows clients to move seamlessly between access points with minimal delay, requires the access points to handle client information locally. If the configuration is changed to allow local DHCP, then the access points can cache client credentials, enabling fast roaming.

Reference :=

CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Cisco documentation on FlexConnect configurations

Question: 4

A FlexConnect remote office deployment is using five 2702i APs indoors and two 1532i APs outdoors. When a code upgrade is performed and FlexConnect Smart AP Image Upgrade is leveraged, but no FlexConnect Master AP has been configured, how many image transfers between the WLC and APs will occur?

A. 1

B. 2

C. 5

D. 7

Answer: B

Explanation:

When using FlexConnect Smart AP Image Upgrade without a configured FlexConnect Master AP, the WLC will transfer the image to one indoor AP and one outdoor AP separately. Each AP model needs a different firmware image due to hardware differences. Therefore, there will be two image transfers from the WLC: one for the 2702i APs and another for the 1532i APs.

Reference :=

CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Cisco documentation on FlexConnect Smart AP Image Upgrade

Question: 5

Where is a Cisco OEAP enabled on a Cisco Catalyst 9800 Series Wireless Controller?

A. RF Profile

B. Flex Profile

C. Policy Profile

D. AP Join Profile

Answer: B

Explanation:

The Cisco OfficeExtend Access Point (OEAP) feature is enabled on a Cisco Catalyst 9800 Series Wireless Controller through the Flex Profile. The Flex Profile allows for the configuration of various settings specific to FlexConnect deployments, including OEAP settings, which enable remote workers to connect to the corporate network securely.

Reference :=

Cisco documentation on Catalyst 9800 Series Wireless Controllers

Question: 6

When configuring a Cisco WLC, which CLI command adds a VLAN with VLAN ID of 30 to a FlexConnect group named BranchA-FCG?

A. config flexconnect BranchA-FCG vlan 30 add

B. config flexconnect BranchA-FCG vlan add 30

C. config flexconnect group BranchA-FCG vlan 30 add

D. config flexconnect group BranchA-FCG vlan add 30

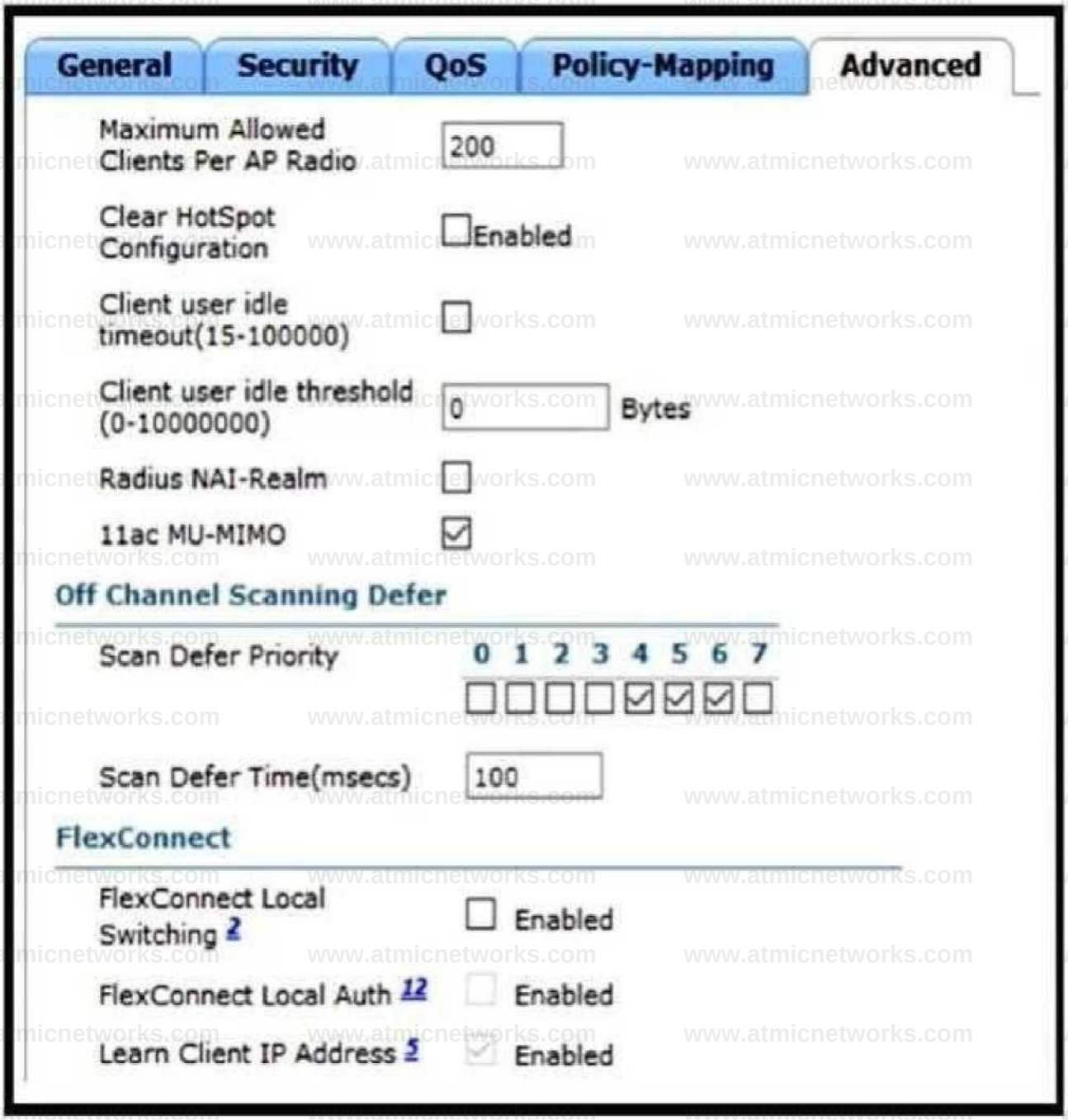
Answer: C

Explanation:

The correct command to add a VLAN with a specific ID to a FlexConnect group in a Cisco Wireless LAN Controller (WLC) is 'config flexconnect group BranchA-FCG vlan 30 add'. This command specifies the FlexConnect group name 'BranchA-FCG' and the VLAN ID '30', followed by the action 'add', which is consistent with Cisco's CLI syntax for WLC configuration. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 7

Refer to the exhibit.



A customer has implemented Cisco FlexConnect deployments with different WLANs around the globe and is opening a new branch in a different location. The engineer's task is to execute all the wireless configuration and to suggest how to configure the switch ports for new APs. Which configuration must the switching team use on the switch port?

A. trunk mode

B. access mode

C. single VLAN

D. multiple VLAN

Answer: A

Explanation:

: For new Access Points (APs) in a Cisco FlexConnect deployment, switch ports should be configured in trunk mode. This allows the APs to handle traffic for multiple WLANs or SSIDs, each associated with different VLANs. Trunk mode enables the AP to tag traffic with the correct VLAN IDs as per its configuration. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 8

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?

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: 9

An engineer configures a Cisco Aironet 600 Series OfficeExtend AP for a user who works remotely. What is configured on the Cisco WLC to allow the user to print a printer on his home network?

A. split tunneling

B. SE-connect

C. FlexConnect

D. AP failover priority

Answer: A

Explanation:

Split tunneling on a Cisco Aironet 600 Series OfficeExtend AP allows for traffic to be divided between two different networks. In this case, it enables the user to access the corporate network for work- related tasks while simultaneously allowing them to print to a printer on their home network. This is achieved by routing the traffic meant for the corporate network to the WLC, while local traffic such as the connection to a home printer is kept on the local network. Reference := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/aironet-602-officeextend-access- point/117540-configure-splittunneloeap-00.html

Question: 10

An engineer must configure a Cisco WLC to support Cisco Aironet 600 Series OfficeExtend APs. Which two Layer 2 security options are supported in this environment? (Choose two.)

A. Static WEP + 802.1X

B. WPA+WPA2

C. Static WEP

D. CKIP

E. 802.1X

Answer: B, E

Explanation:

The Cisco Aironet 600 Series OfficeExtend APs support various Layer 2 security options, including WPA+WPA2 and 802.1X. WPA and WPA2 provide secure encryption for wireless data, while 802.1X offers a robust authentication framework. These security options ensure that the wireless network is protected against unauthorized access and data breaches, which is crucial for remote workers connecting to the corporate network. Reference := CCNP Enterprise Wireless Design ENWLSD 300425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 11

An organization is supporting remote workers in different locations. In order to provide wireless network connectivity and services, OfficeExtend has been implemented. The wireless connectivity is working, but users report losing connectivity to their local network printers. Which solution must be used to address this issue?

A. OEAP gateway override

B. OEAP split tunnel

C. WLAN static IP tunneling

D. FlexConnect local switching

Answer: B

Explanation:

The OfficeExtend Access Point (OEAP) split tunnel feature allows the separation of corporate and local traffic. By implementing a split tunnel, remote workers can maintain wireless connectivity to the corporate network while simultaneously accessing local network resources such as printers. This solution ensures that local traffic does not have to traverse the corporate network, which can cause connectivity issues like the ones reported by the users. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 12

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:

The remote LAN (RLAN) feature on the OfficeExtend Access Point (OEAP) is used to extend the wired network through more than one port. This allows the creation of a wired interface on the OEAP that can be associated with a specific VLAN, providing connectivity for wired devices at remote locations. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 13

An engineer must implement Cisco Identity-Based Networking Services at a remote site using ISE to dynamically assign groups of users to specific IP subnets. If the subnet assigned to a client is available at the remote site, then traffic must be ofloaded locally, and subnets are unavailable at the remote site must be tunneled back to the WLC. Which feature meets these requirements?

A. learn client IP address

B. FlexConnect local authentication

C. VLAN-based central switching

D. central DHCP processing

Answer: C

Explanation:

VLAN-based central switching is the feature that meets the requirements stated. With this feature, when a subnet assigned to a client is available at the remote site, the traffic is ofloaded locally. If the subnet is not available, the traffic is tunneled back to the Wireless LAN Controller (WLC). This setup allows for dynamic assignment of clients to specific IP subnets using Cisco Identity-Based Networking Services with ISE. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 14

An engineer must configure Cisco OEAPs for three executives. As soon as the NAT address is configured on the management interface, it is noticed that the WLC is not responding for APs that are trying to associate to the internal IP management address. Which command should be used to reconcile this?

A. config flexconnect office-extend nat-ip-only disable

B. config network ap-discovery nap-ip-only enable

C. config flexconnect office-extend nat-ip-only enable

D. config network ap-discovery nat-ip-only disable

Answer: C

Explanation:

When configuring Cisco OfficeExtend Access Points (OEAPs), enabling NAT IP only for office-extend is necessary if the APs are behind a NAT device and need to communicate with the Wireless LAN Controller (WLC) using the internal IP management address. The command config flexconnect office- extend nat-ip-only enable allows the APs to discover and associate with the WLC when the management interface is configured with a NAT address.

Question: 15

An engineer is responsible for a wireless network for an enterprise. The enterprise has distributed offices around the globe, and all APs are configured in FlexConnect mode. The network must be configured to support 802.11r and CCKM. What needs to be implemented to accomplish this goal?

A. Enable VLAN-based central switching.

B. Enable FlexConnect local authentication.

C. Enable FlexConnect local switching.

D. Create FlexConnect groups.

Answer: B

Explanation:

For an enterprise wireless network with distributed offices globally and APs configured in FlexConnect mode, enabling FlexConnect local authentication is essential to support 802.11r and CCKM. This configuration allows for fast roaming and maintains a secure connection by locally authenticating the clients without having to go back to the central site, thus providing a seamless and efficient roaming experience for the users.

Question: 16

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: D, E

Explanation:

To ensure the 1810 OEAP can join the controller from remote teleworker locations, the firewall must allow specific UDP ports that are used for AP communication with the controller. UDP ports 5246 and 5247 are used for Control and Provisioning of Wireless Access Points (CAPWAP) control and data messages, while UDP ports 12222 and 12223 are used for OfficeExtend APs' data traffic. Blocking these ports would prevent the APs from joining the controller, hence they must be allowed on the firewall.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_Cisco_OfficeExtend_Access_Point_.pdf

Question: 17

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:

FlexConnect is a wireless solution for branch office and remote office deployments. It allows APs to switch client data traffic locally and perform client authentication locally when they are disconnected from the WLC. For WLAN A to work in FlexConnect mode and WLAN B to work in local mode, the APs need to be part of a FlexConnect group with proper WLAN-VLAN mappings. This ensures that the correct VLAN is used for each WLAN, which is essential when the APs are operating in FlexConnect mode. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 18

An engineer wants the wireless voice traffic class of service to be used to determine the queue order for packets received, and then have the differentiated services code point set to match when it is resent to another port on the switch. Which configuration is required in the network?

A. Platinum QoS configured on the WLAN

B. WMM set to required on the WLAN

C. msl qos trust dscp configured on the controller switch port

D. msl qos trust cos configured on the controller switch port

Answer: C

Explanation:

The configuration required is to trust the DSCP (Differentiated Services Code Point) on the controller switch port. This

ensures that the voice traffic's class of service is maintained throughout the network. By trusting DSCP, the switch will preserve the DSCP value set by the wireless LAN controller, which is responsible for marking the voice packets.
Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 19

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: C

Explanation:

AutoQoS simplifies the deployment of QoS by automating the process. On the Cisco Catalyst 9800 Series Wireless Controller, AutoQoS takes into account the characteristics of wireless traffic and helps in implementing a consistent QoS policy across both wired and wireless parts of the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 20

A network engineer is deploying 8865 IP phones with wireless clients connected to them. In order to apply the appropriate QoS, the IP voice traffic needs to be distinguished from client data traffic.
Which switch configuration feature must be enabled?

A. Voice VLAN

B. QBSS

C. WME

D. QoS routing

Answer: A

Explanation:

The Voice VLAN feature on switches allows the network to distinguish between voice traffic and data traffic from wireless clients connected to IP phones. This is crucial for applying the appropriate QoS to ensure that voice traffic is prioritized over client data traffic. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 21

A network engineer wants to implement QoS across the network that supports multiple VLANs. All the APs are connected to switch ports and are configured in local mode. Which trust model must be configured on the switch ports to which the APs are connected?

A. CoS

B. WMM UP

C. DSCP

D. IPP

Answer: C

Explanation:

Differentiated Services Code Point (DSCP) is the trust model that must be configured on the switch ports to which the APs are connected in local mode. This is because DSCP provides a way to classify and manage network traffic and to provide QoS. DSCP can be trusted on the switch port, and the AP can then mark the packets with the appropriate DSCP value, which will be retained across the network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 22

An enterprise started using WebEx as a virtual meeting solution. There is a concern that the existing wireless network will not be able to support the increased amount of traffic as a result of using WebEx. An engineer needs to remark the

QoS value for this application to ensure high quality in meetings. What must be implemented to accomplish this task?

A. QoS preferred call index

B. UP to DSCP map

C. AVC profiles

D. WLAN quality of service profile

Answer: C

Explanation:

Application Visibility and Control (AVC) profiles must be implemented to remark the QoS value for WebEx traffic. AVC profiles allow the network to identify different applications and provide the appropriate QoS treatment, ensuring high-quality meetings. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference: https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2018/pdf/BRKEWN-3003.pdf

Question: 23

A corporation has a wireless network where all access points are configured in FlexConnect. The WLC has a Data WLAN and a VoWiFi WLAN implemented where centrally-switched SSID is configured for the APs. Which QoS configuration must be implemented for the wireless packets to maintain the marking across the wired and wireless network?

A. Set QoS to Platinum.

B. Enable CAC.

C. Allow WMM.

D. Trust DSCP.

Answer: D

Explanation:

Trusting DSCP is essential for maintaining the QoS markings across the wired and wireless network in a FlexConnect deployment. By trusting DSCP, the WLC and APs will preserve the QoS markings set by applications and devices, ensuring consistent QoS treatment throughout the network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 24

A company is collecting the requirements for an on-premises event. During the event, a wireless client connected to a dedicated WLAN will run a video application that will need on average 391595179 bits per second to function properly. What is the QoS marking that needs to be applied to that WLAN?

A. Platinum
B. Gold
C. Silver
D. Bronze

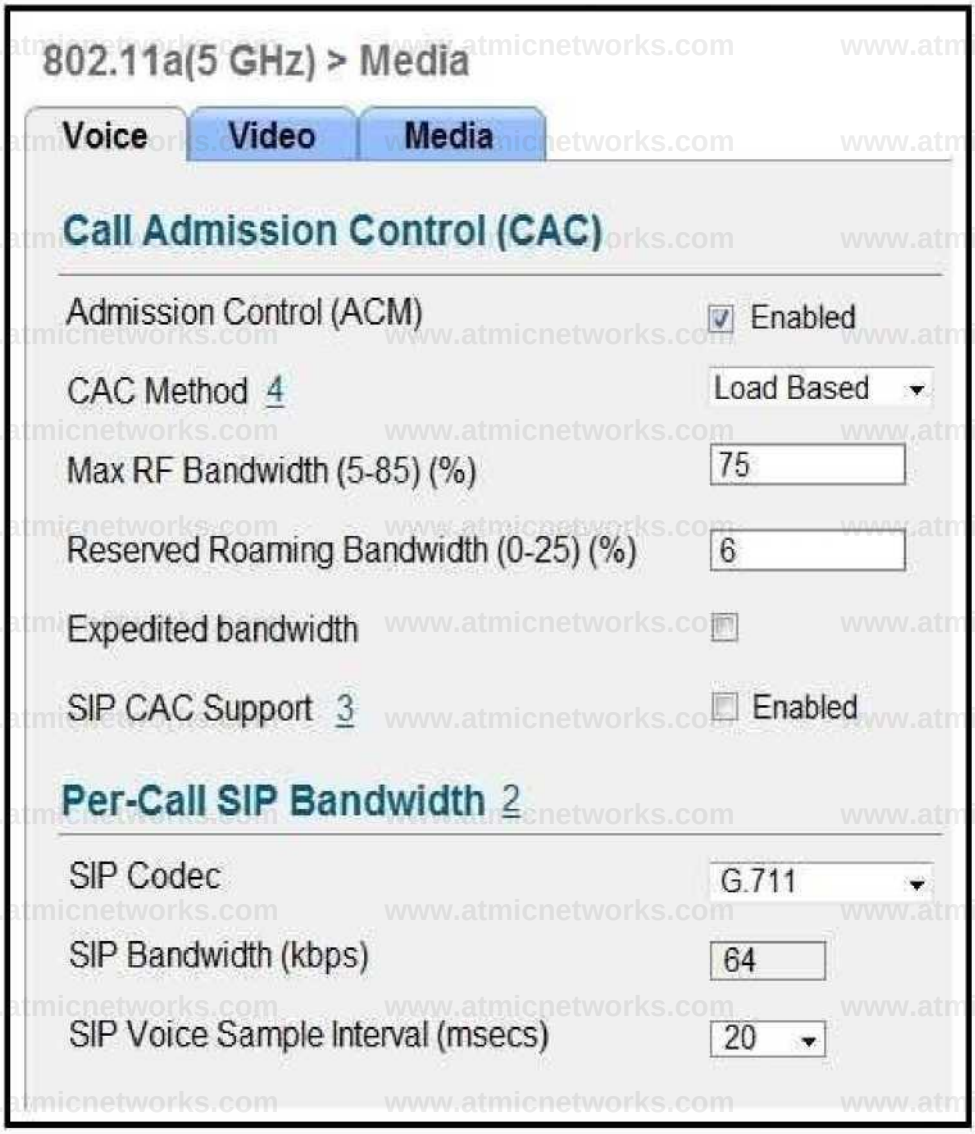
Answer: A

Explanation:

The Platinum QoS marking is typically used for the highest-priority traffic, such as voice and video. Given the requirement for a high average bitrate for the video application, Platinum would be the appropriate QoS marking to ensure the necessary bandwidth and priority on the WLAN. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 25

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:

To take full advantage of the WLAN configuration, VoWLAN phones must support 802.11e, which is a standard for wireless QoS, and Wi-Fi Multimedia (WMM), which is a subset of 802.11e that provides prioritized media delivery. These standards ensure that voice traffic is prioritized appropriately in the wireless network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 26

An engineer must use Cisco AVC on a Cisco WLC to prioritize Cisco IP cameras that use the wireless network. Which element do you configure in a rule?

A. permit-ACL

B. WMM required

C. mark

D. rate-limit

Answer: C

Explanation:

Cisco AVC (Application Visibility and Control) on a Cisco Wireless LAN Controller (WLC) is used to prioritize traffic by marking the packets. For Cisco IP cameras that use the wireless network, the AVC rule would be configured to mark the

packets with a specific QoS value, ensuring that the video traffic is treated with higher priority as it traverses the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 27

An IT administrator is managing a wireless network in which most devices are Apple iOS. A QoS issue must be addressed on the WLANs. Which configuration must be performed?

A. Enable Fastlane globally under Wireless > Access Points > Global Configuration.

B. Create a new AVC Profile named AUTOQOS-AVC-PROFILE and apply to all WLANs.

C. Enable Fastlane under each WLAN setting.

D. Enable WMM TSPEC/TCLAS negotiation under Wireless > Advanced.

Answer: C

Explanation:

Apple's Fastlane technology is used to prioritize traffic from iOS devices on the network. By enabling Fastlane under each WLAN setting, the network can recognize and prioritize traffic from Apple iOS devices, addressing the QoS issues for these devices on the WLANs. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference: https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/technotes/8-3/Optimizing_WiFi_Connectivity_and_Prioritizing_Business_Apps.pdf

Question: 28

What is the Cisco recommended configuration for a Cisco switch port connected to an AP in local mode for optimal voice over WLAN performance with an 8821 wireless phone?

A. switchport encapsulation dot1q

switchport mode trunk

mls qos trust device cisco-phone

B. switchport mode access

mls qos trust device cisco-phone

C. switchport mode access mls qos trust cos

D. switchport mode access mls qos trust dscp

Answer: D

Explanation:

For optimal voice over WLAN performance with a Cisco 8821 wireless phone, the Cisco recommended configuration is to set the switch port to access mode and trust the DSCP markings. This ensures that voice traffic is appropriately prioritized in the network, providing better quality of service for voice communications. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/8821/english/Deployment/8 821_wlandg.pdf

Question: 29

An engineer has configured Media Stream on the WLC and must guarantee at least 2 Mbps stream per user. Which RRC template should the engineer use?

A. coarse

B. medium

C. low

D. ordinary

Answer: A

Explanation:

The Media Stream feature on a Cisco WLC allows for the prioritization of streaming media. To guarantee at least 2 Mbps stream per user, the 'coarse' Resource Reservation Control (RRC) template should be used, as it provides the necessary bandwidth allocation for each user's media stream. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0101010.html

Question: 30

Refer to the exhibit.

```
AL-CORE#show mls qos map cos-dscp
   Cos-dscp map:
         cos: 1 2  3  4  5  6  7
        ------------------------
        dscp: 8 16 24 32 45 48 56
```

Which COS to DSCP map must be modified to ensure that voice traffic is tagged correctly as it traverses the network?

A. COS of 6 to DSCP 46

B. COS of 3 to DSCP 26

C. COS of 7 to DSCP 48

D. COS of 5 to DSCP 46

Answer: D

Explanation:

In Quality of Service (QoS) for networking, Class of Service (COS) and Differentiated Services Code Point (DSCP) are used for traffic classification and prioritization. Voice traffic is generally given high priority due to its sensitivity to delay and requires proper tagging to maintain quality over the network.

The correct mapping for voice traffic, according to best practices, is a COS value of 5 mapped to a DSCP value of 46. This is because DSCP 46 corresponds to Expedited Forwarding (EF), which is typically used for voice traffic prioritization in IP networks.

The exhibit shows the output from a command on a network device that displays the current mappings between COS values and DSCP values. The mapping that needs modification for correct voice traffic tagging can be identified by looking at the standard practice for voice QoS, which uses a COS value of 5 mapped to a DSCP value of 46.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 31

Which QoS level is recommended for guest services?

A. gold

B. bronze

C. platinum

D. silver

Answer: B

Explanation:

The bronze QoS level is typically recommended for guest services in a wireless network environment. This level prioritizes basic internet access, which is suitable for guest services that do not require high bandwidth or low latency. It ensures that more critical services are not impacted by guest traffic, which is often less sensitive to performance fluctuations. Reference := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 32

An engineer wants to configure WebEx to adjust the precedence and override the QoS profile on the WLAN. Which configuration is needed to complete this task?

A. Change the WLAN reserved bandwidth for WebEx
B. Create an AVC profile for WebEx
C. Create an ACL for WebEx
D. Change the AVC application WebEx-app-sharing to mark

Answer: B

Explanation:

To adjust the precedence and override the QoS profile on the WLAN for WebEx, an Application Visibility and Control (AVC) profile needs to be created for WebEx. AVC profiles allow for the identification and prioritization of specific applications over the wireless network, ensuring that critical applications like WebEx receive the necessary bandwidth and QoS treatment. Reference := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 33

All APs are receiving multicast traffic, instead of only the APs that need it. What is the cause of this problem?

A. The multicast group includes all APs

B. The wrong multicast address was used

C. The multicast group is assigned the wrong VLAN

D. Multicast IGMP snooping is not enabled

Answer: D

Explanation:
If all APs are receiving multicast traffic instead of only those that need it, it indicates that Multicast Internet Group Management Protocol (IGMP) snooping is not enabled. IGMP snooping is a feature that allows a network switch to listen to IGMP network traffic and ensure that multicast packets are only sent to the ports associated with interested receivers, thus preventing unnecessary traffic on the network. Reference := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 34

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:

Protocol Independent Multicast (PIM) sparse mode and dense mode are two different multicast routing mechanisms. Sparse mode uses distribution trees and is designed for networks where multicast groups are sparsely distributed across the network, minimizing unnecessary traffic. In contrast, dense mode floods the network with multicast traffic and then prunes back the branches where there are no interested receivers, which can lead to inefficient use of bandwidth. Reference := CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 35

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?

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: 36

A network engineer observes a spike in controller CPU overhead and overall network utilization after multicast is enabled on a controller with 500 APs. Which feature corrects the issue?

A. controller IGMP snooping

B. multicast AP multicast mode

C. broadcast forwarding

D. unicast AP multicast mode

Answer: D

Explanation:

Enabling unicast AP multicast mode can correct the issue of increased controller CPU overhead and overall network utilization after multicast is enabled. This mode allows the controller to send multicast traffic to the APs as unicast, which is more efficient for the wireless medium and reduces the load on the controller's CPU.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 37

An engineer is configuring multicast for wireless for an all-company video meeting on a network using EIGRP and BGP within a single domain from a single source. Which type of multicast routing should be implemented?

A. Protocol Independent Multicast Dense Mode

B. Source Specific Multicast

C. Multicast Source Discovery Protocol

D. Protocol Independent Multicast Sparse Mode

Answer: D

Explanation:

For a network using EIGRP and BGP within a single domain from a single source, Protocol Independent Multicast Sparse Mode (PIM-SM) is the most suitable multicast routing to be implemented. PIM-SM is efficient for networks with a large number of networks and few receivers, which seems to be the case for an all-company video meeting.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300 430 Official Cert Guide)

Question: 38

Which statement about the VideoStream/Multicast Direct feature is true?

A. IP multicast traffic is reliable over WLAN by default as defined by the IEEE 802.11 wireless multicast delivery mechanism.

B. Each VideoStream client acknowledges receiving a video IP multicast stream.

C. It converts the unicast frame to a multicast frame over the air.

D. It makes the delivery of the IP multicast stream less reliable over the air, but reliable over Ethernet.

Answer: B

Explanation:

The true statement about the VideoStream/Multicast Direct feature is that each VideoStream client acknowledges receiving a video IP multicast stream. This feature enhances the reliability of IP multicast traffic over WLAN by using client acknowledgments to ensure delivery.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-

guide/b_cg81/multicast_broadcast_setup.html

Question: 39

Which configuration is applied to prevent the network from a Layer 2 flooding of multicast frames with a seamless transfer of multicast data to the client when roaming from one controller to another?

A. Enable IGMPv3 on the central Layer 3 switch.

B. Enable IGMP snooping on the WLC.

C. Enable multicast mode on the WLC.

D. Create multicast groups on the central Layer 3 switch.

Answer: B

Explanation:

To prevent the network from a Layer 2 flooding of multicast frames and ensure a seamless transfer of multicast data to the client when roaming, IGMP snooping should be enabled on the WLC. This feature allows the WLC to monitor and control multicast traffic at Layer 2, preventing unnecessary multicast forwarding.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 40

An engineer is configuring multicast for two WLCs. The controllers are in different physical locations and each handles around 500 wireless clients. How should the CAPWAP multicast group address be assigned during configuration?

A. Each WLC must be assigned a unique multicast group address.

B. Each WLC management address must be in the same multicast group.

C. Both WLCs must be assigned the same multicast group address.

D. Each WLC management address must be in a different multicast group.

Answer: A

Explanation:

When configuring multicast for two WLCs in different physical locations, each handling around 500 wireless clients, it is important to assign a unique multicast group address to each WLC. This ensures that multicast traffic is properly segregated and managed within each controller's network.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 41

A wireless network has been implemented to enable multicast video to be streamed reliably over the wireless link to the wireless users. After a client reports that the video is unable to stream, the administrator determines that the client is connecting at a data rate of 12 Mbps and is trying to stream to a valid multicast address on the network. Which two actions must be applied? (Choose two.)

A. Turn off IGMP snooping for all the configured WLANs on the controller.

B. Implement video-stream for the multicast video on the controller.

C. Allow multicast-direct to work correctly and multicast-direct to be enabled globally.

D. Change the WLAN QoS value to Bronze for the WLAN that multicast will be enabled.

E. Allow RTSP to stream the video due to wireless multicast not using acknowledgements.

Answer: B, C

Explanation:

To ensure reliable streaming of multicast video over a wireless link, it's essential to optimize the multicast settings on the controller. Option B, implementing video-stream for the multicast video on the controller, is a feature that optimizes the delivery of multicast streams by converting them into unicast streams for specific clients, thus improving reliability. Option C, allowing multicast-direct to work correctly, involves enabling multicast-direct globally, which allows multicast packets to be sent directly to clients without the need for them to subscribe to a specific multicast group, enhancing efficiency and reliability. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 42

Which two restrictions are in place with regards to configuring mDNS? (Choose two.)

A. mDNS uses only UDP port 5436 as a destination port.

B. mDNS cannot use UDP port 5353 as the destination port.

C. mDNS is not supported on FlexConnect APs with a locally switched WLAN.

D. Controller software must be newer than 7.0.6+.

E. mDNS is not supported over IPv6.

Answer: C, D

Explanation:

mDNS has specific restrictions regarding its configuration. Option C is correct because mDNS is not supported on FlexConnect APs with a locally switched WLAN, which limits its deployment in certain network designs. Option D is also correct; the controller software must be newer than version 7.0.6 to support mDNS features, which means that older controller software versions do not have the necessary capabilities to handle mDNS. Reference: CCNP Enterprise Wireless Design ENWLSD 300425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 43

A network engineer needs to configure multicast in the network. The implementation will use multiple multicast groups and PIM routers. Which address provides automatic discovery of the best RP for each multicast group?

A. 224.0.0.13

B. 224.0.0.14

C. 224.0.1.39

D. 224.0.1.40

Answer: C

Explanation:

In a multicast implementation using multiple multicast groups and PIM routers, the address that provides automatic discovery of the best RP (Rendezvous Point) for each multicast group is 224.0.1.39. This address is used by the Auto-RP feature, which allows for dynamic RP discovery and simplifies the management of multicast groups across the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 44

A shopping center uses AireOS controllers with Cisco Wave 2 APs. A separate WLAN named Guest-012345678-WLAN is used for guest wireless clients. Management needs location analytics to determine popular areas. CMX must track only associated clients. What must be selected on the CMX server settings?

A. Exclude probing clients

B. Duty Cycle Cutoff

C. Enable Locally Administered MAC Filtering

D. Enable Location MAC Filtering

Answer: A

Explanation:

For location analytics in a shopping center using AireOS controllers with Cisco Wave 2 APs, the CMX server settings must exclude probing clients to track only associated clients. This setting ensures that the location analytics data reflects the movements of clients that are actively connected to the WLAN, providing accurate insights into popular areas within the shopping center. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/the_cisco_cmx_detect_and_locate_service.html#id_123333

Question: 45

A wireless engineer needs to implement client tracking. Which method does the angle of arrival use to determine the location of a wireless device?

A. received signal strength

B. triangulation

C. time distance of arrival

D. angle of incidence

Answer: B

Explanation:

The angle of arrival (AoA) method for client tracking determines the location of a wireless device using triangulation. This technique involves measuring the angle at which the signal arrives at different receivers (access points) and using this information to pinpoint the device's location within the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Reference: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/WiFiLBS-DG/wifich2.html

Question: 46

Which two steps are needed to complete integration of the MSE to Cisco Prime Infrastructure to track the location of clients/rogues on maps? (Choose two.)

A. Synchronize access points with the MSE.

B. Add the MSE to Cisco Prime Infrastructure using the CLI credentials.

C. Add the MSE to Cisco Prime Infrastructure using the Cisco Prime Infrastructure communication credentials.

D. Apply a valid license for Wireless Intrusion Prevention System.

E. Apply a valid license for location tracking.

Answer: C, E

Explanation:

To integrate the Mobility Services Engine (MSE) with Cisco Prime Infrastructure for tracking the location of clients and rogues on maps, it is essential to add the MSE to Cisco Prime Infrastructure using the communication credentials specific to Cisco Prime Infrastructure. This ensures that both
systems can communicate effectively. Additionally, a valid license for location tracking must be applied to enable the MSE's location services capabilities. Without this license, the MSE would not be able to provide client and rogue location tracking functionalities. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 47

An IT department receives a report of a stolen laptop and has information on the MAC address of the laptop. Which two settings must be set on the wireless infrastructure to determine its location?
(Choose two.)

A. Location History for Clients must be enabled on the MSE.

B. Client location tracking must be enabled on the MSE.

C. Location History for Visitors must be enabled on the MSE.

D. Location History for Rogue APs & Rogue Clients must be enabled on the MSE.

E. Tracking optimization must be enabled on the WLC.

Answer: A, B

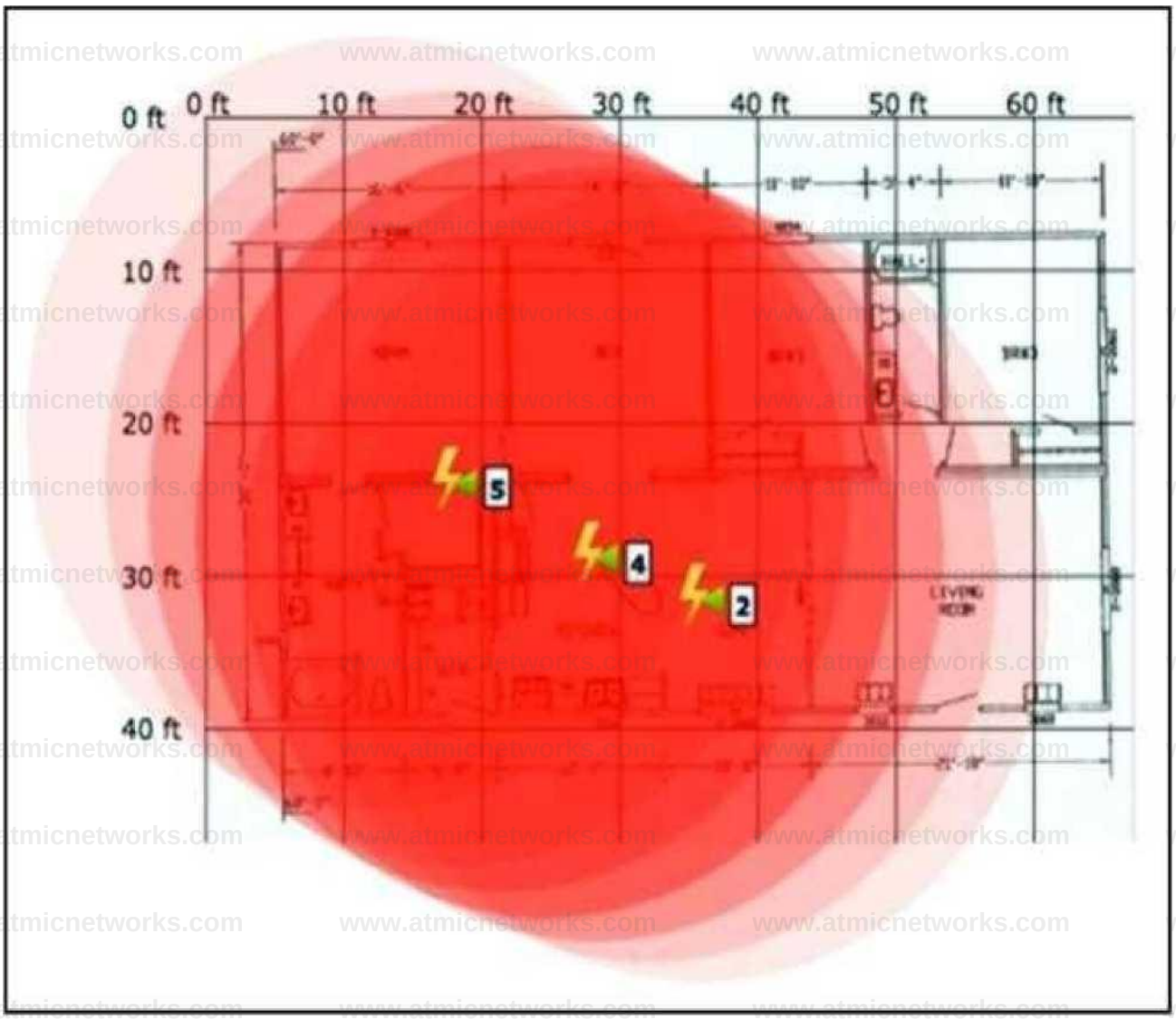
Explanation:

When an IT department needs to locate a stolen laptop using its MAC address, enabling Location History for Clients on

the Mobility Services Engine (MSE) is crucial as it allows for historical tracking of client devices' locations. Furthermore, Client location tracking must also be enabled on the MSE; this feature actively tracks and updates the current position of all client devices in real-time. Both settings are necessary to provide a comprehensive view of where the laptop has been over time and its current location within the wireless network's coverage area. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 48

Refer to the exhibit.



An engineer needs to manage non-802.11 interference. What is observed in the output on PI?

A. At least one strong interferer is impacting connectivity at this site.

B. Several light interferers are collectively impacting connectivity at this site.

C. The three individual clusters shown indicate poor AP placement.

D. RF at this site is unable to provide adequate wireless performance.

Answer: A

Explanation:

The output observed in Prime Infrastructure suggests that there is at least one strong interferer impacting connectivity at this site. This conclusion is drawn from observing areas marked with intense red coloring indicating high levels of RF interference which could degrade wireless performance significantly if not addressed.

Question: 49

After looking in the logs, an engineer notices that RRM keeps changing the channels for non-IEEE 802.11 interferers. After surveying the area, it has been decided that RRM should not change the channel. Which feature must be enabled to ignore non-802.11 interference?

A. Avoid Cisco AP Load

B. Avoid Non-802.11 Noise

C. Avoid Persistent Non-WiFi Interference

D. Avoid Foreign AP Interference

Answer: C

Explanation:

The feature that must be enabled to ignore non-802.11 interference is “Avoid Persistent Non-WiFi Interference.” This setting allows the Radio Resource Management (RRM) to not react to non-802.11 noise and interference, which can be crucial in environments where such interference is common but does not significantly impact wireless performance. By enabling this feature, RRM will not change the channel in response to non-IEEE 802.11 interferers, thus maintaining a stable channel
plan. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI
300-430 Official Cert Guide)

Question: 50

Which two protocols are used to communicate between the Cisco MSE and the Cisco Prime Infrastructure network management software? (Choose two.)

A. HTTPS

B. Telnet

C. SOAP

D. SSH

E. NMSP

Answer: A, E

Explanation:

The two protocols used to communicate between the Cisco Mobility Services Engine (MSE) and the Cisco Prime Infrastructure network management software are HTTPS and NMSP (Network Mobility Services Protocol). HTTPS is used for secure web-based communications, while NMSP is a Cisco proprietary protocol used specifically for efficient, real-time communication between MSE and network management software like Cisco Prime Infrastructure. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 51

An engineer must configure MSE to provide guests access using social media authentication. Which service does the engineer configure so that guests use Facebook credentials to authenticate?

A. Social Connect

B. Client Connect

C. Visitor Connect

D. Guest Connect

Answer: A

Explanation:

To provide guests access using social media authentication, the engineer must configure the "Social Connect" service. This service allows guests to use their Facebook credentials, among other social media platforms, to authenticate and gain network access. It simplifies the guest access process by leveraging existing social media accounts for authentication. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 52

A network engineer has been hired to perform a new MSE implementation on an existing network. The MSE must be installed in a different network than the Cisco WLC. Which configuration allows the devices to communicate over NMSP?

A. Allow UDP/16113 port on the central switch.

B. Allow TCP/16113 port on the firewall.

C. Allow UDP/16666 port on the VPN router.

D. Allow TCP/16666 port on the router.

Answer: B

Explanation:
For the MSE to communicate with the Cisco Wireless LAN Controller (WLC) over NMSP when installed on a different network, the necessary configuration is to allow TCP/16113 port on the firewall. NMSP uses TCP port 16113 for its communications, and opening this port on the firewall will enable the MSE and WLC to establish a connection and communicate effectively. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 53

What is the default NMSP echo interval between Cisco MSE and a Wireless LAN Controller?

A. 10 seconds

B. 15 seconds

C. 30 seconds

D. 60 seconds

Answer: B

Explanation:

The default NMSP echo interval between Cisco MSE and a Wireless LAN Controller is 15 seconds. This interval determines how frequently the MSE sends echo messages to the WLC to maintain the NMSP connection and ensure that the link is active and operational. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference:

https://www.cisco.com/en/US/docs/wireless/mse/3350/6.0/CAS/configuration/guide/msecg_ch4_CAS.html

Question: 54

An engineer just added a new MSE to Cisco Prime Infrastructure and wants to synchronize the MSE with the Cisco 5520 WLC, located behind a firewall in a DMZ. It is noticed that NMSP messages are failing between the two devices. Which traffic must be allowed on the firewall to ensure that the MSE and WLC are able to communicate using NMSP?

A. TCP 1613

B. UDP 16113

C. UDP 1613

D. TCP 16113

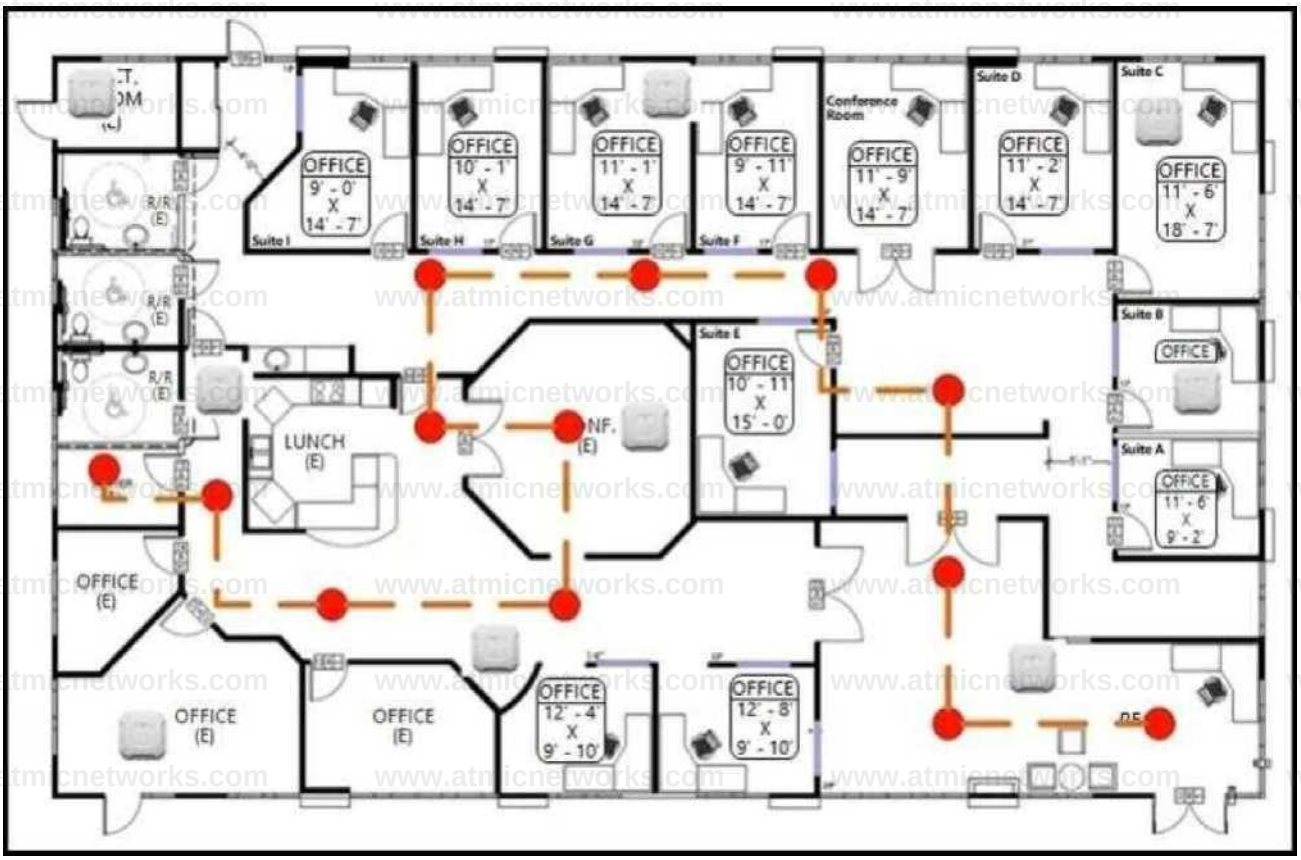
Answer: D

Explanation:

The Network Mobility Services Protocol (NMSP) is the protocol used by Cisco Mobility Services Engine (MSE) to communicate with Cisco Wireless LAN Controllers (WLCs). For NMSP messages to successfully pass through a firewall, the correct port must be allowed. The default port for NMSP traffic is TCP 16113. Therefore, to ensure communication between MSE and WLC using NMSP, TCP port 16113 must be allowed on the firewall. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 55

Refer to the exhibit.



An engineer needs to configure location services in an office. The requirement is to use FastLocate and achieve higher locations refresh rates. Which location-based technique should be implemented?

A. probe-based

B. location patterning

C. data packet-based

D. angulation

Answer: A

Explanation:

FastLocate technology enhances location updates' frequency by utilizing probe requests from clients for real-time location tracking. This method increases the refresh rate of client locations significantly compared to other methods that rely on data packets or RSSI measurements of associated clients
only. By implementing a probe-based technique, an engineer can achieve higher location refresh rates as required for

location services in an office environment. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 56

An engineer is managing a wireless network for a shopping center. The network includes a Cisco WLC, a Cisco MSE, and a Cisco Prime Infrastructure. What is required to use Cisco CMX Location Analytics?

A. Enable tracking parameters in Cisco MSE.

B. Enable Context Aware and CMX Browser Engage.

C. Install Cisco Prime Infrastructure with floor maps.

D. Set history parameters in Cisco MSE.

Answer: A

Explanation:

Cisco Connected Mobile Experiences (CMX) Location Analytics requires accurate tracking of devices within the wireless network's coverage area. To utilize CMX Location Analytics effectively, it is essential to enable tracking parameters in Cisco Mobility Services Engine (MSE). This allows MSE to collect data on device locations and movements within the environment, which can then be analyzed by CMX for insights into customer behavior, asset tracking, or other analytical purposes. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 57

An engineer configures a deployment to support:

Cisco CMX

licenses for at least 3000 APs
6000 wIPS licenses

The Cisco vMSE appliance must be sized for this deployment. Which Cisco vMSE Release 8 option must the engineer deploy?

A. Large vMSE

B. Low-End vMSE

C. Standard vMSE

D. High-End vMSE

Answer: D

Explanation:

For a deployment that supports Cisco Connected Mobile Experiences (CMX), licenses for at least 3000 Access Points (APs), and wIPS licenses for 6000 sensors, a High-End vMSE is required. This version of MSE is designed to handle large-scale deployments with high license and sensor requirements, ensuring that the system can manage the data and analytics for such a substantial wireless environment. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 58

A new MSE with wIPS service has been installed and no alarm information appears to be reaching the MSE from controllers. Which protocol must be allowed to reach the MSE from the controllers?

A. SOAP/XML

B. NMSP

C. CAPWAP

D. SNMP

Answer: B

Explanation:

When an MSE with wIPS service is installed, it is crucial for alarm information to reach the MSE from the controllers. The Network Mobility Services Protocol (NMSP) is the protocol that facilitates this communication. Ensuring that NMSP is allowed through any firewalls or network security devices is essential for the proper functioning of the wIPS service. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 59

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:

The Cisco Hyperlocation feature requires enabling on both the wireless LAN controller and Cisco CMX to function correctly. This allows for precise location tracking by integrating data from both components. Additionally, if the Cisco CMX server is a virtual machine (VM), it is recommended to use a high-end VM to handle the processing demands of Cisco Hyperlocation deployments, ensuring optimal performance and accuracy.

Question: 60

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:

When performing a Cisco Hyperlocation accuracy test, the relevant parameters include the X, Y real location and the client MAC address. The X, Y coordinates provide the actual location data needed for the test, while the client MAC address identifies the specific device being located.

Question: 61

Where is Cisco Hyperlocation enabled on a Cisco Catalyst 9800 Series Wireless Controller web interface?

A. Policy Profile

B. AP Join Profile

C. Flex Profile

D. RF Profile

Answer: D

Explanation:

Cisco Hyperlocation is enabled in the RF Profile on a Cisco Catalyst 9800 Series Wireless Controller web interface. The RF Profile contains settings that pertain to radio frequency management, which includes the configuration for Hyperlocation.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/b_wl_16_10_cg/cisco-hyperlocation.html

Question: 62

The Cisco Hyperlocation detection threshold is currently set to -50 dBm. After reviewing the wireless user location, discrepancies have been noticed. To improve the Cisco Hyperlocation accuracy, an engineer attempts to change the detection threshold to -100 dBm. However, the Cisco Catalyst 9800 Series Wireless Controller does not allow this change to be applied. What actions should be taken to resolve this issue?

A. Disable Cisco Hyperlocation, change the Cisco Hyperlocation detection threshold, and then enable it.

B. Create a new profile on Cisco CMX with the new Cisco Hyperlocation detection range, and apply it on the WLAN.

C. Place the APs to monitor mode, shutdown the radios, and then change the Cisco Hyperlocation detection threshold.

D. Shutdown all radios on the controller, change the Cisco Hyperlocation detection range, and enable the radios again.

Answer: D

Explanation:

To resolve the issue of changing the Cisco Hyperlocation detection threshold, the engineer should shut down all radios on the controller, change the Cisco Hyperlocation detection range, and then enable the radios again. This process

ensures that the new threshold settings are applied correctly across the network.

Question: 63

An engineer must track guest traffic flow using the WLAN infrastructure. Which Cisco CMX feature must be configured and used to accomplish this tracking?

A. analytics

B. connect and engage

C. presence

D. detect and locate

Answer: D

Explanation:

To track guest traffic flow using the WLAN infrastructure, the 'detect and locate' feature of Cisco CMX must be configured and used. This feature allows the engineer to monitor the location and movement of guests within the WLAN coverage area.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 64

An engineer has successfully implemented 10 active RFID tags in an office environment. The tags are not visible when the location accuracy is tested on the Cisco CMX Detect and Locate window. Which setting on Cisco CMX allows the engineer to view the tags?

A. Enable RFID tags in tracking options.

B. Enable probing clients for active tags.

C. Define an RFID group globally and add the tags.

D. Enable hyperlocation services for RFID.

Answer: A

Explanation:

In Cisco CMX, to view active RFID tags, the engineer needs to enable the tracking of these tags within the system settings. This is typically done by selecting an option that allows for RFID tag tracking, which makes them visible on location-based services like the Detect and Locate window of Cisco CMX. By enabling this feature, the system starts to interpret signals from RFID tags and displays their location accordingly. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 65

An engineer completed the basic installation for two Cisco CMX servers and is in the process of configuring high availability, but it fails. Which two statements about the root of the issue are true?

(Choose two.)

A. The Cisco CMX instances are installed in the same subnet.

B. The types of the primary and secondary Cisco CMX installations differ.

C. The delay between the primary and secondary instance is 200 ms.

D. The sizes of the primary and secondary Cisco CMX installations differ.

E. Both Cisco CMX installations are virtual.

Answer: B, D

Explanation:

For high availability configuration in Cisco CMX servers to work correctly, both primary and secondary servers must be identical in terms of installation type (physical or virtual) and size (resources allocated like CPU, RAM). If there is a mismatch in these aspects, it can lead to failure in setting up high availability as they need to synchronize data between them seamlessly. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 66

Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
2	0.003747	10.48.39.251	10.48.71.21	UDP	146	9999 4 2003 Lai=l04
3	1.087479	10.48.39.214	10.48.71.21	UDP	130	9999 4 2003 Len=88
4	2.733577	10.48.39.214	10.48.71.21	UDP	130	9999 4 2003 Lee=8S
5	2 999859	10.48.39.251	10.48.71.21	UDP	178	9999 4 2003 Loi-136
6	3.001227	10.48.39.251	10.48.71.21	LDP	162	9999 4 2003 Larl'O
7	4.355249	10.48.39.214	10.48.71.21	UDP	146	9999 4 2003 Lai=IO4
8	5.999538	10.48.39.251	10.48.71.21	UDP	178	9999 4 2003 Lai=136
9	6.000959	10.48.39251	10.48.71.21	UDP	146	9999 4 2003 Leu=104
10	8.9994 IS	10.48.39.251	10.48.71.21	LDP	146	9999 4 2003 Leu=l04
11	9.000791	10.48.39251	10.48.71.21	UDP	178	9999 4 2003 Leu 136
12	9.262904	10.48.39214	10.48.71.21	LDP	146	9999 4 2003 Lai 104
13	10,894785	10.48,39.214	10.48.71,21	UDP	130	9999 4 2003 Lee-88
14	11.995126	10.48.39.251	10.48.71.21	UDP	194	9999 4 2003 LcnM<2
15	11.999193	10.48.39.251	10.48.71.21	UDP	162	9999 4 2003 Lap 120
16	14.994902	10.48.39.251	10.48.71.21	UDP	178	9999 4 2003 Leu-136
17	14,996368	10.48.39.251	10.48.71.21	I DP	162	9999 4 2003 Lai-120
18	17,994857	10.48.39.251	10.48.71.21	UDP	146	9999 4 2003 Lai 104
19	17.996231	10.48.39.251	10.48.71.21	UDP	162	9999 4 2003 Lee-120
20	18.102843	10.48.39.251	10.48.71.21	UDP	130	9999 4 2003 Lai-88
21	21.098408	10.48.39.251	10.48.71.21	UDP	146	9999 4 2003 Lai=104
22	21.099952	10.48.39.251	10.48.71.21	UDP	162	9999 4 2003 Lai=120
23	24.0985 74	10.48.39.251	10.48.71.21	UDP	146	9999 4 2003 Lai-104
24	24.099804	10.48.39.251	10.48.71.21	UDP	162	9999 4 2003 Len=120
25	27.098099	10.48.39.251	10.48.71.21	UDP	162	9999 4 2003 Lai-120
26	27.099839	10.48.39.251	10.48.71.21	UDP	130	9999 4 2003 Lai-88
27	28.880307	10.48.39.164	10.48.71.21	UDP	146	9999 4 2003 Lee-104
28	28.881569	10.48.39.214	10.48.71.21	CAPP	146	CAPP MD5 Encrypted
29	30.094237	10.48.39.251	10.48.71.21	LDP	178	9999 4 2003 Lai 136
30	30.097812	10.48.39.251	1048.71.21	UDP	146	9999 4 2003 Lar ID
31	30.513451	10.48.39.214	10.48.71.21	UDP	130	9999 4 2003 Lav-88
32	30.515926	10.48.39.164	10.48.71.21	UDP	130	9999 4 2003 Lai -SS

> Frame 1 162 bytes on wire (1296 bits) 162 bytes captured (1296 bits)
> Ethernet I. Src. Ciscotnc_2a c4 a3 (00 06:8 2a c4 a3). Dst Vmware_99 4e 19 (00 50 56 994e 19)
> Internet Protocol Verson 4. Src: 10 48 39 251, Dst 10 48 71 21
> User Datagram Protocol, Src Port 9999 (9999) Dst Port 2003 (2003)
v Data (120 bytes)
Data ae 2144 to 00 00 b4 51 ef 06 fdcbb? 6c 03 c7
(Length 120|

The image shows a packet capture that was taken at the CLI of the Cisco CMX server. It shows UDP traffic from the WLC coming into the server. What does the capture prove?

A. The Cisco CMX server receives NetFlow data from the WLC.

B. The Cisco CMX server receives NMSP traffic from the WLC.

C. The Cisco CMX server receives SNMP traffic from the WLC.

D. The Cisco CMX server receives Angle-of-Arrival data from the WLC.

Answer: B

Explanation:

The image provided shows a packet capture with multiple entries displaying UDP traffic between two IP addresses using different ports (notably port number '16666' which is commonly used for NMSP). Network Mobility Services Protocol (NMSP) is used by wireless controllers like WLCs to communicate with management software such as Cisco's Mobility Services Engine or CMX. This protocol helps in managing various mobility services across wireless networks. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 67

A Cisco CMX 3375 appliance on the 10.6.1 version code counts duplicate client entries, which creates wrong location analytics. The issue is primarily from iOS clients with the private MAC address feature enabled. Enabling this feature requires an upgrade of the Cisco CMX 3375 appliance in a high availability pair to version 10.6.3. SCP transfers the Cisco CMX image, but the upgrade script run fails. Which configuration change resolves this issue?

A. Upgrade the high availability pair to version 10.6.2 image first and then upgrade to version 10.6.3.

B. Save configuration and use the upgrade script to upgrade the high availability pair without breaking the high availability.

C. Break the high availability using the cmxha config disable command and upgrade the primary and secondary individuality.

D. Run root patch to first upgrade to version 10.6.2 and then migrate to version 10.6.3.

Answer: C

Explanation:

The issue with duplicate client entries from iOS clients with the private MAC address feature enabled can be resolved by breaking the high availability using the cmxha config disable command and upgrading the primary and secondary individually. This approach allows for each appliance to be upgraded without affecting the high availability pair's synchronization and operation. Reference: The solution is supported by best practices for upgrading Cisco appliances in

a high availability configuration, as outlined in the CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 68

An engineer has implemented advanced location services for a retail wireless deployment. The marketing department wants to collect user demographic information in exchange for guest WLAN access and to have a customized portal per location hosted by the provider. Which social connector must be tied into Cisco CMX to provide this service?

A. Gmail

B. Google+

C. Facebook

D. MySpace

Answer: C

Explanation:

To collect user demographic information in exchange for guest WLAN access and to have a customized portal per location, the marketing department should tie the Facebook social connector into Cisco CMX. Facebook is widely used for social login features and provides access to demographic data when users consent, making it the ideal choice for this requirement. Reference: The use of social connectors for demographic data collection is discussed in the context of advanced location services in the official certification guide.

Question: 69

What are two considerations when deploying a Cisco Hyperlocation? (Choose two.)

A. NTP configuration is available, but not recommended.

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

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

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

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

Answer: D, E

Explanation:

When deploying Cisco Hyperlocation, it is important to enable the feature on both the wireless LAN controller and Cisco CMX to ensure proper functionality and data accuracy. Additionally, if the Cisco CMX server is a VM, a high-end VM is required to handle the processing demands of Cisco Hyperlocation deployments. Reference: The considerations for deploying Cisco Hyperlocation are covered in the certification guide, which emphasizes the importance of enabling the feature on both the controller and CMX, as well as the hardware requirements for the CMX server.

Question: 70

After installing and configuring Cisco CMX, an administrator must change the NTP server on the Cisco CMX server. Which action accomplishes this task?

A. Manually edit /etc/ntp.conf using an XML editor before restarting the server by using service restart all services.

B. Log in to the Cisco CMX CLI and issue set ntp server NTP_IP where NTP_IP is the IP of the NTP server.

C. Manually edit /etc/ntp.conf as the admin user before restarting ntpd by using service ntpd restart.

D. Log in to the Cisco CMX GUI as the administrator and type the IP address of the NTP server in System tab > Settings> TimeZone/NTP.

Answer: B

Explanation:

To change the NTP server on the Cisco CMX server, the administrator should log in to the Cisco CMX CLI and issue the command set ntp server NTP_IP, where NTP_IP is the IP address of the new NTP server. This method is straightforward and does not require manual editing of configuration files or restarting the entire server. Reference: The process for changing the NTP server on a Cisco CMX server is detailed in the official certification guide, which provides step-by-step instructions for using the CLI.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200906-Troubleshooting-CMX-connectivity-with- WL.pdf

Question: 71

A customer managing a large network has implemented location services. Due to heavy load, it is needed to load balance the data coming through NMSP from the WLCs. Load must be spread between multiple CMX servers to help optimize the data flow for APs. Which configuration in CMX meets this requirement?

A. cmxctl config feature flags nmsplb.cmx-ap-grouping true

B. cmxctl config feature flags nmsplb.cmxgrouping true

C. cmxctl config feature flags nmsplb.cmx-loadbalance true

D. cmxctl config feature flags nmsplb.cmx-rssi-distribute true

Answer: A

Explanation:

To load balance the data coming through NMSP from the WLCs and spread the load between multiple CMX servers, the configuration cmxctl config feature flags nmsplb.cmx-ap-grouping true should be used. This enables the load balancing feature and helps optimize the data flow for APs in a large network environment. Reference: The configuration for load balancing in CMX is explained in the certification guide, which outlines the commands and flags necessary to manage data flow efficiently.

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_command/cmxcli106/cmxcli1051_chapter_010.html#wp7273815000https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/214894- optimize-cmx-performance.html

Question: 72

An engineer needs to provision certificates on a Cisco Catalyst 9800 Series Wireless Controller. The customer uses a third-party CA server. Which protocol must be used between the controller and CA server to request and install certificates?

A. SCEP

B. TLS

C. LDAP

D. SSL

Answer: A

Explanation:

The Simple Certificate Enrollment Protocol (SCEP) is used to securely issue certificates to network devices in a scalable manner. When provisioning certificates on a Cisco Catalyst 9800 Series Wireless Controller using a third-party CA server, SCEP is the protocol that facilitates this process. It allows the controller to request and install certificates automatically, which is essential for establishing secure
communications within the network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300 425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/trustpoints/b-configuring-trustpoints-on-cisco-catalyst-9800- series-controllers/c-workflow-to-configure-a-trustpoint-for-a-third-party-certificate-on-catalyst-9800.html

Question: 73

A corporation has recently implemented a BYOD policy at their HQ. Which two risks should the security director be concerned about? (Choose two.)

A. network analyzers

B. malware

C. lost and stolen devices

D. keyloggers

E. unauthorized users

Answer: B, C

Explanation:

With the implementation of a BYOD policy, the security director should be concerned about malware and lost and stolen devices. Malware can compromise the corporate network if infected devices connect to it. Lost and stolen devices pose a risk of unauthorized access to corporate data and resources, potentially leading to data breaches.
Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 74

When implementing self-registration for guest/BYOD devices, what happens when an employee tries to connect four devices to the network at the same time?

A. The last device is removed and the newly added device is updated as active device.

B. The registration is allowed, but only one device is connected at any given time.

C. All devices are allowed on the network simultaneously.

D. Purge time dictates how long a device is registered to the portal.

Answer: B

Explanation:

In a self-registration setup for guest/BYOD devices, when an employee tries to connect multiple devices simultaneously, the system allows the registration of all devices. However, it restricts the active connection to only one device at a time. This ensures that network resources are not overburdened by a single user connecting multiple devices. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 75

What is an important consideration when implementing a dual SSID design for BYOD?

A. After using the provisioning SSID, an ACL that used to make the client switch SSIDs forces the user to associate and traverse the network by MAC filtering.

B. If multiple WLCs are used, the WLAN IDs must be exact for the clients to be provisioned and traverse the network correctly.

C. SSIDs for this setup must be configured with NAC State-RADIUS NAC for the clients to authenticate with Cisco ISE, or with NAC State-ISE NAC for Cisco ISE to associate the client.

D. One SSID is for provisioning and the other SSID is for gaining access to the network. The use of an ACL should not be enforced to make the client connect to the REAL SSID after provisioning.

Answer: D

Explanation:

In a dual SSID design for BYOD, one SSID is used for provisioning devices, and the other is for network access. It's important not to enforce an ACL to switch SSIDs after provisioning because this could disrupt the user experience. Instead, the process should be seamless, with the device automatically connecting to the access SSID after provisioning is complete. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 76

Refer to the exhibit.

```
(Cisco WLC) >show dhcp proxy

DHCP Proxy Behaviour enabled
```

```
interface Vlan63
 ip address 1010 63 252/22
 description Dot1x_BYOD no shutdown
```

A network administrator deploys the DHCP profiler service in two ISE servers: 10.3.10.101 and 10.3.10.102. All BYOD devices connecting to WLAN on VLAN63 have been incorrectly profiled and are assigned as unknown profiled endpoints. Which action efficiently rectifies the issue according to Cisco recommendations?

A. Nothing needed to be added on the Cisco WLC or VLAN interface. The ISE configuration must be fixed.

B. Disable DHCP proxy on the Cisco WLC.

C. Disable DHCP proxy on the Cisco WLC and run the ip helper-address command under the VLAN interface to point to DHCP and the two ISE servers.

D. Keep DHCP proxy enabled on the Cisco WLC and define helper-address under the VLAN interface to point to the two ISE servers.

Answer: C

Explanation:

Disabling DHCP proxy on the Cisco WLC and running the ip helper-address command under the VLAN interface to point to DHCP and the two ISE servers is the recommended action. This allows direct communication between clients and DHCP/ISE servers, which is necessary for accurate device profiling.

Question: 77

An engineer must implement a BYOD policy with these requirements:

Onboarding unknown machines

Easily scalable

Low overhead on the wireless network

Which method satisfies these requirements?

A. triple SSID

B. single SSID

C. open SSID

D. dual SSID

Answer: B

Explanation:

A single SSID method satisfies the requirements for a BYOD policy that includes onboarding unknown machines, scalability, and low overhead on the wireless network. It simplifies network access for users and reduces overhead by minimizing broadcast traffic associated with multiple SSIDs.

Question: 78

A company has a single WLAN configured for 802.1x authentication with the QoS set to Silver. This WLAN supports all corporate and BYOD access. A decision has been made to allow users to install Cisco Jabber on their personal mobile devices. Users report poor voice quality when using Jabber. QoS is being applied only as best effort. What must be configured to ensure that the WLAN remains on the Silver class and to ensure Platinum class for Jabber?

A. Configure QoS on the mobile devices that have Jabber installed.

B. Enable Cisco Centralized Key Management on the WLAN so that the Jabber-enabled devices will connect.

C. Configure the WLAN to broadcast on 5 GHz radios only and allow Jabber users to connect.

D. Configure an AVC profile for the Jabber traffic and apply it to the WLAN.

Answer: D

Explanation:

Configuring an AVC profile for the Jabber traffic and applying it to the WLAN ensures that voice traffic from Cisco Jabber receives Platinum QoS while keeping other WLAN traffic at Silver class. AVC allows for deep packet inspection which can identify Jabber application packets so they can be given priority over other types of traffic.

Question: 79

An engineer is implementing profiling for BYOD devices using Cisco ISE. When using a distributed model, which persona must the engineer configure with the profiling service?

A. Device Admin Node

B. Primary Admin Node

C. Monitor Node

D. Policy Services Node

Answer: D

Explanation:

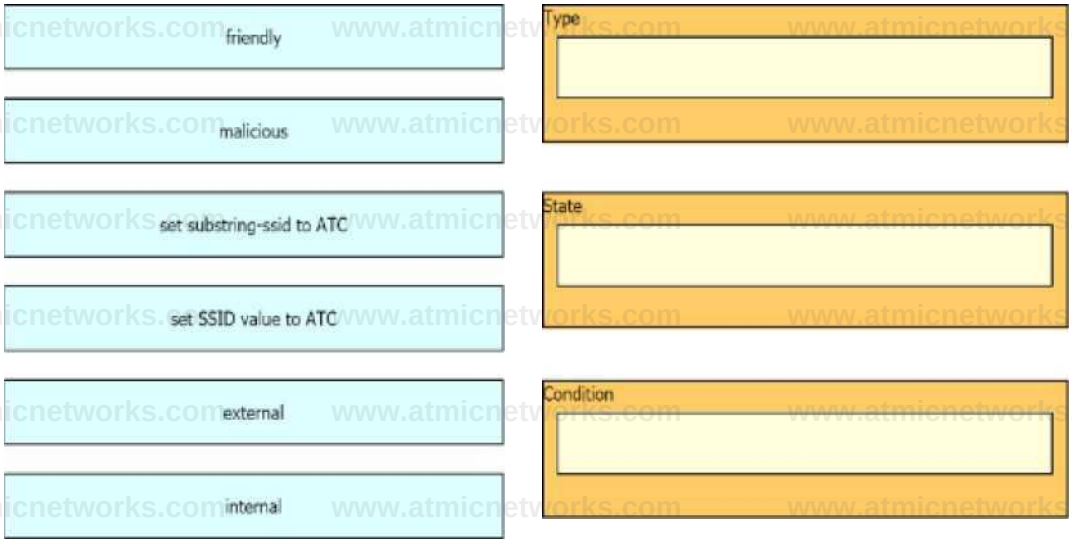
In a distributed deployment of Cisco ISE, profiling services are configured on Policy Services Nodes (PSNs). These nodes handle all context-based access control, including profiling services.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 80

DRAG DROP

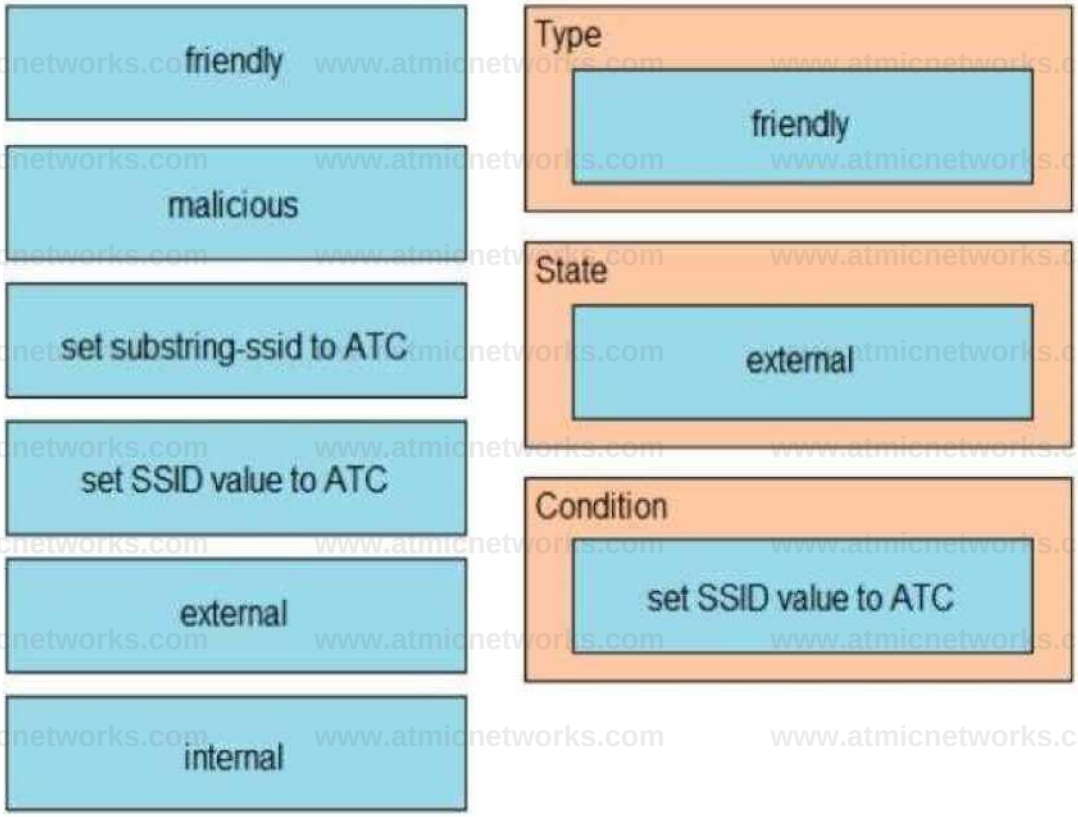
The network management team in a large shopping center has detected numerous rogue APs from local coffee shops that are broadcasting SSIDs. All of these SSIDs have names starting with ATC (for example, ATC302, ATC011, and ATC566). A wireless network engineer must appropriately classify these SSIDs using the Rogue Rules feature. Drag and drop the options from the left onto the categories in which they must be used on the right. Not all options are used.



Answer:

Explanation:

Answer Area



Question: 81

What must be configured on ISE version 2.1 BYOD when using Single SSID?

A. open authentication

B. 802.1x

C. no authentication

D. WPA2

Answer: B

Explanation:

In Cisco ISE version 2.1 for BYOD with a Single SSID setup, 802.1x must be configured to provide the necessary layer of security and to facilitate the device registration process. 802.1x authentication allows for the use of EAP (Extensible Authentication Protocol) to authenticate users before they can access the network. This ensures that only authorized devices can join the BYOD network, providing a secure method for device onboarding and access control. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 82

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:

For a large company requiring support for 32 VLANs for different departments, the most efficient solution is to configure one single SSID and use Cisco ISE for dynamic VLAN assignment based on user roles. Cisco ISE can classify users into different groups and assign them to the appropriate VLANs. This approach reduces the complexity of managing multiple SSIDs and simplifies the user experience while maintaining a high level of security and network segmentation. Reference: CCNP
Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 83

Which feature on the Cisco Wireless LAN Controller must be present to support dynamic VLAN mapping?

A. FlexConnect ACL

B. VLAN name override

C. CCKM/OKC

D. AAA override

Answer: D

Explanation:

The feature required on the Cisco Wireless LAN Controller to support dynamic VLAN mapping is AAA override. This feature allows for the assignment of VLANs on a per-user basis as determined by the authentication, authorization, and accounting server. When AAA override is enabled, attributes such as VLAN ID can be dynamically applied to a user's session after successful authentication and authorization. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 84

Which three properties are used for client profiling of wireless clients? (Choose three.)

A. HTTP user agent

B. DHCP

C. MAC OUI

D. hostname

E. OS version

F. IP address

Answer: A, B, C

Explanation:

Client profiling involves using various properties to identify and classify wireless clients. The HTTP user agent can provide information about the client's device type and browser, DHCP can reveal details about the client's network configuration and requests, and the MAC OUI (Organizationally Unique Identifier) can be used to determine the manufacturer of the device. These properties are crucial for profiling because they offer insights into the device's capabilities and identity. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 85

Which command set configures a Cisco Catalyst 9800 Series Wireless Controller so that the client traffic enters the network at the AP switch port?

A **config terminal**
wireless profile policy [policy name] local switching
end

B **config terminal**
wireless flexconnect policy [policy name] local switching
end

C **config terminal**
wireless flexconnect policy [policy name] no central switching
end

D **config terminal**
wireless profile policy [policy name]
no central switching end

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The correct command set for configuring a Cisco Catalyst 9800 Series Wireless Controller so that the client traffic enters the network at the AP switch port is Option C:

config terminal

wireless profile policy [policy name]

no central switching

end

This configuration disables central switching, which means that client traffic will be locally switched at the access point level rather than being sent through the controller. This is useful in scenarios where local switching is preferred due to reasons such as reducing latency or conserving bandwidth on WAN links. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 86

What is the default IEEE 802.1x AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller?

A. EAP-PEAP with 802.1x port authentication

B. EAP-TLS with 802.1x port authentication

C. EAP-FAST with CAPWAP DTLS + port authentication

D. EAP-FAST with CAPWAP DTLS

Answer: D

Explanation:

The default IEEE 802.1x AP authentication configuration on a Cisco Catalyst 9800 Series Wireless Controller is EAP-FAST with CAPWAP DTLS (Option D). This method uses EAP-FAST for authentication within a secure tunnel established by Datagram Transport Layer Security (DTLS) over CAPWAP, which provides both security for authentication credentials and encryption for wireless management frames. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 87

An engineer must implement rogue containment for an SSID. What is the maximum number of APs that should be used for containment?

A. 1

B. 2

C. 3

D. 4

Answer: B

Explanation:

For rogue containment on an SSID, it's recommended to use two access points for containment (Option B). Using more than two can lead to unnecessary interference and potential disruption of service for legitimate users, while using just one may not be effective enough in containing the rogue SSID. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference:
https://www.cisco.com/c/en/us/td/docs/wireless/technology/roguedetection_deploy/Rogue_Detec tion.html

Question: 88

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, E

Explanation:

When upgrading a Cisco AireOS WLC from version 7.3 to 8.9, it's crucial to configure ACLs that allow necessary traffic for Cisco Central Web Authentication (CWA). The correct ACLs to configure are:

B . Permit 0.0.0.0 0.0.0.0 UDP DNS any: This ACL allows DNS queries from any source to any destination, which is essential for resolving domain names during the upgrade process.

E . Permit 0.0.0.0 0.0.0.0 UDP any any: This ACL permits all UDP traffic from any source to any destination, ensuring that services relying on UDP can continue to function during the upgrade.

These ACLs ensure that critical services like DNS resolution are not interrupted during the upgrade process, which could otherwise lead to system instability or failure to access network resources. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732- central-web-auth-00.html

Question: 89

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: A, D

Explanation:

CMX Facebook Wi-Fi is designed to provide limited access to the network before a user completes authentication. This feature allows HTTP traffic only before authentication while blocking all other traffic, which corresponds with option A. Additionally, it intercepts HTTP traffic to redirect the user to the authentication page, which aligns with option D. The purpose of these restrictions is to ensure that users can be directed to log in via Facebook for Wi-Fi access without

compromising network security by allowing unchecked access. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/td/docs/wireless/mse/8-0/CMX_Connect_Engage_Visitor_Connect/Guide/Cisco_CMX_Connect_Engage_Config_Guide_VC/C MX_Facebook_Wi-Fi.html

Question: 90

An engineer is implementing Cisco Identity-Based Networking on a Cisco AireOS controller. The engineer has two ACLs on the controller. The first ACL, named BASE_ACL, is applied to the corporate_clients interface on the WLC, which is used for all corporate clients. The second ACL, named HR_ACL, is referenced by ISE in the Human Resources group policy. What is the resulting ACL when a Human Resources user connects?

A. HR_ACL appended with BASE_ACL
B. HR_ACL only
C. BASE_ACL appended with HR_ACL
D. BASE_ACL only

Answer: C

Explanation:

When implementing Cisco Identity-Based Networking on a Cisco AireOS controller with two ACLs where one is applied directly on the WLC interface and another referenced by ISE for a specific group policy, the resulting ACL for a user in that group would be a combination of both ACLs. The BASE_ACL applied on the corporate_clients interface acts as the default ACL for all corporate clients, while HR_ACL is specific for Human Resources users. When a Human Resources user connects, HR_ACL takes precedence but does not replace BASE_ACL; instead, it appends its rules to those of BASE_ACL resulting in an aggregated set of rules from both ACLs. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 91

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, E, F

Explanation:

In this scenario where branch wireless users can still associate locally but cannot access head office services due to WAN downtime indicates that Cisco FlexConnect is likely in use. The correct elements are: A - authentication-local/switch-local: This means that client authentication and data switching are happening locally at the branch. E - standalone mode: With WAN down, FlexConnect APs operate in standalone mode allowing clients to associate even without connectivity back to WLC. F - WEB authentication: This could be used as an authentication method regardless of WAN state since it's processed locally at AP level. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 92

Refer to the exhibit.

```
(Cisco Controller) >
(Cisco Controller) >'!AJ Framework: Jan 21 23:35:43.569: eatrast.c-EVENT: New context (EAP handle [1] c4000000)
•EXP Framework: Jan 21 23:55:43.569: eap_fast.e-EVENT: Allocated new EAR-FAST context (handle = 37000000)
•EAP Framework: Jan 21 23:55:43.569: eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle [3] C40000O0)
'EAR Framework: Jan 21 23:55:43.569: eapfastauth.c-AUTH-r^NT: Received Identity
'EAR Framework: Jan 21 23:55:43.569: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f00000000000000000000)
•EAP Framework: Jan 21 23:55:43.569: eap_£ast_auth.c-AUTH-EVENT: Sending Start
•EAP Framework: Jan 21 23:55:43.586: eap_£ast.c-AUTH-EVENT: Precess Response, type: 0x2c
•EAR Framework: Jan 21 23:55:43.586: eap_£ast_auth.c-AUTH-EVENT: Process Response (EAP handle - c4000000)
•EAP Framework: Jan 21 23:55:43.536: eap_fast_auth.c-AUTH-EVENT: Received ILS record type: Handshake in state: Start
•EAR 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 23:55:43.526: 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-
•EAR Framework; Jan 21 23:55:43.586: eap_£ast_auth.c-AUTH-EVENT: n>S_RSA_WITH_AE3_128 proposed-
•EAP Framework: Jan 21 23:55:43.586: eap_fast_auth.e-AUTH-EVENT: TL3_R3A_HITH_RC4_128 proposed-.
•EAP Framework: Jan 21 23:55:43.586: eap_£ast.c-EVENT: Proposed ciphersuite(s):
•EAP Framework: Jan 21 23:55:43.586: eap_£ast.c-EVENT: Unknown ciphersuite 255
•EAP Framework: Jan 21 23:55:43.586: eap fast.c-EVENT: Unknown eiphersuite 49188

•EAR 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
•EAR Framework: Jan 21 23:55:43.586: eap_:ast.e-EVENT:                TL3_DHE_R3A_»ITH_AES_128_*BC_3HA
•EAR Framework: Jan 21 23:55:43.586: eap_£ast.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; eapjast. c-EVENT:                TLS_RSA_WITH_A£3_128_CBC_3HA
•EAR Framework: Jan 21 23:55:43.587: eap_£ast.c-EVENT: Unknown ciphersuite 10
•EAP Framework: Jan 21 23:55:43.587: eap_fast.c-EVENT: Unknown eiphersuite 49159
•EAR 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:                TL3_RSA_WITH_RC4_128_ SHA
•EAR Framework: Jan 21 23:55:43.587; sap fast.c-EVENT: Unknown ciphersuite 4
•EAP Framework: Jan 21 23:55:43.592: eap_fast.c-AUTH-EV£NT: eap_£ast_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 (EA? handle = c4000000)
•EAR Framework: Jan 21 23:55:43.592: eap_fast_auth.c-AUTH-EV»NT: Received ACK from peer
•EAP Framework: Jan 21 23:55:43.592: eap_fast.e-£T£NT: Free context (EAR 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: 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: 93

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: B, D

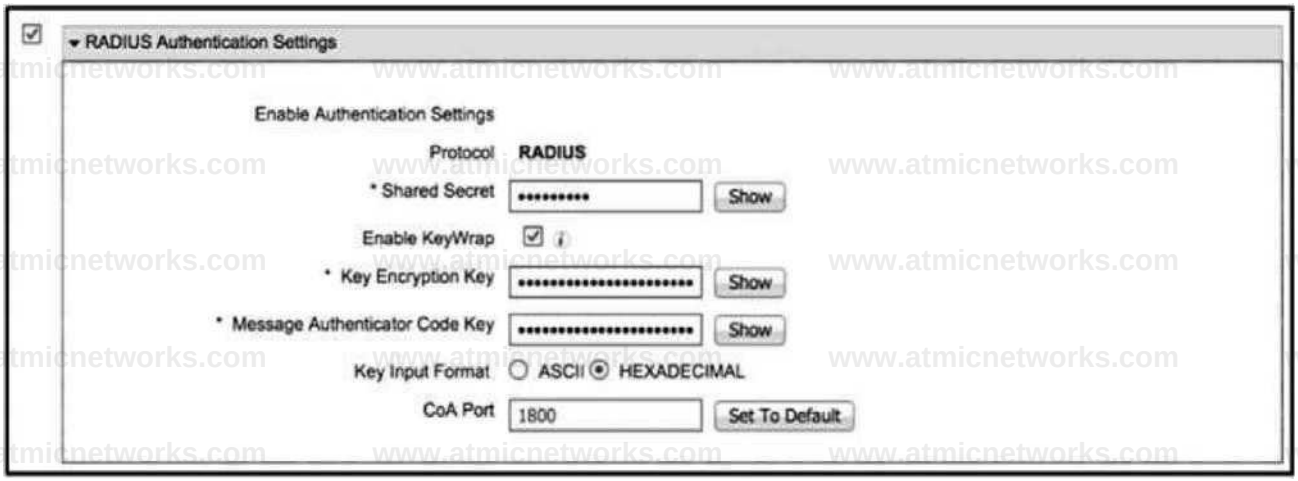
Explanation:

When setting up identity-based networking with ISE and configuring AAA override on the WLAN, the attributes that can be used to change the client behavior from the default settings include the DNS server and DSCP value. The DNS server attribute allows for the specification of a DNS server per
client, which can be essential for directing traffic through specific network paths or applying policies based on domain name resolutions. The DSCP value attribute is used to mark the packets with a specific Quality of Service (QoS) level, which can prioritize or deprioritize traffic as

needed. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 94

Refer to the exhibit.



The security team has implemented ISE as an AAA solution for the wireless network. The wireless engineer notices that though clients are able to authenticate successfully, the ISE policies that are designed to place them on different interfaces are not working. Which configuration must be applied in the RADIUS Authentication Settings section from the ISE Network Device page?

A. Disable KeyWrap.

B. Use ASCII for the key input format.

C. Change the CoA Port.

D. Correct the shared secret.

Answer: C

Explanation:

The configuration that must be applied in the RADIUS Authentication Settings section from the ISE Network Device page

when clients are able to authenticate successfully but the ISE policies designed to place them on different interfaces are not working is to change the CoA Port. The CoA (Change of Authorization) port is used by ISE to send messages to the network device to apply different policies post-authentication. If the CoA port is not correctly configured, the network device will not receive or act upon these messages, resulting in clients not being placed on the correct interfaces as per ISE policies. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 95

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: B

Explanation:

The AAA override feature on a WLAN allows for individualized security policies to be applied to users after they are authenticated by the AAA server, which in this case is Cisco ISE (Identity Services Engine). The company policy requires that all users be denied access to any resources until they pass validation. By using AAA override, the network can enforce access control policies based on user credentials and group membership, ensuring that users cannot access network resources until they have been validated by Cisco ISE. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 96

A Cisco WLC has been added to the network and Cisco ISE as a network device, but authentication is failing. Which configuration within the network device configuration should be verified?

A. SNMP RO community

B. device interface credentials

C. device ID

D. shared secret

Answer: D

Explanation:

When a Cisco Wireless LAN Controller (WLC) is added to Cisco ISE as a network device for authentication purposes, it is crucial to verify the shared secret configured within the network device settings. The shared secret is used to secure communication between the WLC and ISE, ensuring that the authentication messages are encrypted and authenticated. If the shared secret does not match on both the WLC and ISE, the authentication will fail.
Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 97

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?

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: 98

A wireless engineer is configuring LWA using ISE. The customer is a startup company and requested the wireless users to authenticate against a directory, but LDAP is unavailable. Which solution should be proposed in order to have the same security and user experience?

A. Use SAML.

B. Use the internal database of the RADIUS server.

C. Use a preshared key on the corporate WLAN.

D. Use Novell eDirectory.

Answer: B

Explanation:

For a startup company without LDAP, using the internal database of the RADIUS server is a viable solution to authenticate wireless users. This approach allows the company to maintain a directory of users within the RADIUS server itself, providing similar security and user experience as LDAP would. Users can be authenticated against this internal database, ensuring secure access to the wireless network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 99

An engineer has implemented 802.1x authentication on the wireless network utilizing the internal database of a RADIUS server. Some clients reported that they are unable to connect. After troubleshooting, it is found that PEAP authentication is failing. A debug showed the server is sending an Access- Reject message. Which action must be taken to resolve authentication?

A. Use the user password that is configured on the server.

B. Disable the server certificate to be validated on the client.

C. Update the client certificate to match the user account.

D. Replace the client certificates from the CA with the server certificate.

Answer: B

Explanation:

If PEAP authentication is failing and the server is sending an Access-Reject message, one possible action to resolve the issue is to disable the server certificate validation on the client. This means that the client device will not check the authenticity of the RADIUS server's certificate, which can
sometimes resolve connection issues, especially if there is a problem with the certificate chain or trust settings. However, this should be done with caution as it reduces the security of the authentication process. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 100

A customer wants to allow employees to easily onboard their personal devices to the wireless network. The visitors also must be able to connect to the same network without the need to engage with anyone from the reception desk. Which process must be configured on Cisco ISE to support this requirement?

A. MAC authentication bypass

B. native supplicant provisioning

C. local web auth

D. self-registration guest portal

Answer: D

Explanation:

To meet the requirement of allowing employees to easily onboard their personal devices and visitors to connect without reception desk intervention, configuring a self-registration guest portal on Cisco ISE is the appropriate solution. This feature enables guests to create their own accounts and gain network access, streamlining the process for both employees' personal devices and

visitors. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 101

A customer has a distributed wireless deployment model where the WLCs are located in the data centers. Because the file servers are located in the data center, the traffic from the corporate WLAN "Corp-401266017" must go through the controllers, where the guest WLAN "Guest-19283746" traffic must use the local Internet line installed in each office. Which configuration will accomplish this task?

A. Disable Local Switching for the corporate and guest WLAN.

B. Disable Local Switching for the corporate WLAN and enable it for the guest WLAN.

C. Enable Local Switching for the corporate and guest WLAN.

D. Enable Local Switching for the corporate WLAN and disable it for the guest WLAN.

Answer: B

Explanation:

In a distributed wireless deployment model, the traffic can either be switched locally or sent back to the controller. For the corporate WLAN "Corp-401266017", it is essential that the traffic goes through the controllers in the data center to access the file servers securely. Therefore, local switching should be disabled for this WLAN. Conversely, for the guest

WLAN “Guest-19283746”, the requirement is to use the local Internet line. Enabling local switching for this WLAN allows the traffic to bypass the controller and use the local internet, reducing latency and potentially providing a better user experience for guests. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, specifically the sections discussing WLAN traffic forwarding and local switching options.

Question: 102

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 BYOD setup using a dual SSID approach, the first SSID is typically used for device registration and the second for network access. Setting the NAC State to Radius NAC enables the network access control (NAC) to use RADIUS for authentication, authorization, and accounting. Allowing AAA Override enables the RADIUS server to dynamically change the VLAN and ACLs assigned to the endpoint, which is crucial for BYOD where devices need to be placed into the correct VLAN based on user role and device type. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, particularly the chapters on BYOD and advanced WLAN configuration.

Question: 103

Which three characteristics of a rogue AP pose a high security risk? (Choose three.)

A. open authentication

B. high RSSI

C. foreign SSID

D. accepts clients

E. low RSSI

F. distant location

Answer: A, C, D

Explanation:

A rogue AP with open authentication poses a high security risk as it does not require a password, making it easy for unauthorized users to connect. If the rogue AP accepts clients, it can potentially capture sensitive data from those clients. A foreign SSID indicates that the AP is not part of the managed network and could be maliciously installed to lure unsuspecting users. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, focusing on security risks associated with rogue APs.

Question: 104

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

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: 105

Which component must be integrated with Cisco DNA Center to display the location of a client that is experiencing connectivity issues?

A. Cisco Hyperlocation Module

B. Wireless Intrusion Prevention System

C. Cisco Connected Mobile Experiences

D. Cisco Mobility Services Engine

Answer: D

Explanation:

The Cisco Mobility Services Engine (MSE) integrates with Cisco DNA Center to provide advanced location services, including the tracking of clients experiencing connectivity issues. This integration allows network administrators to visualize and troubleshoot client locations effectively. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, which details the integration of location services within Cisco DNA Center.

Question: 106

The IT manager is asking the wireless team to get a report for all guest user associations during the past two weeks. In which two formats can Cisco Prime save this report? (Choose two.)

A. CSV

B. PDF

C. XLS

D. DOC

E. plain text

Answer: AB

Explanation:

Reference: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/user/guide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide_chapter_01010.html

Question: 107

A customer is experiencing performance issues with its wireless network and asks a wireless engineer to provide information about all sources of interference and their impacts to the wireless network over the past few days. Where can the requested information be accessed?

A. CleanAir reports on Cisco Prime Infrastructure

B. Performance reports on Cisco Prime Infrastructure

C. Interference Devices reports on Cisco Wireless LAN Controller

D. Air Quality reports on Cisco Wireless LAN Controller

Answer: A

Explanation:

Question: 108

An engineer must provide a graphical report with summary grouped data of the total number of wireless clients on the network. Which Cisco Prime Infrastructure report provides the required data?

A. Client Traffic Stream Metrics

B. Client Summary

C. Posture Status Count

D. Mobility Client Summary

Answer: D

Explanation:

Question: 109

An engineer is using Cisco Prime Infrastructure reporting to monitor the state of security on the WLAN. Which output is produced when the Adaptive wIPS Top 10 AP report is run?

A. last 10 wIPS events from monitor mode APs

B. last 10 wIPS events from sniffer mode APs

C. last of 10 sniffer mode APs with the most wIPS events

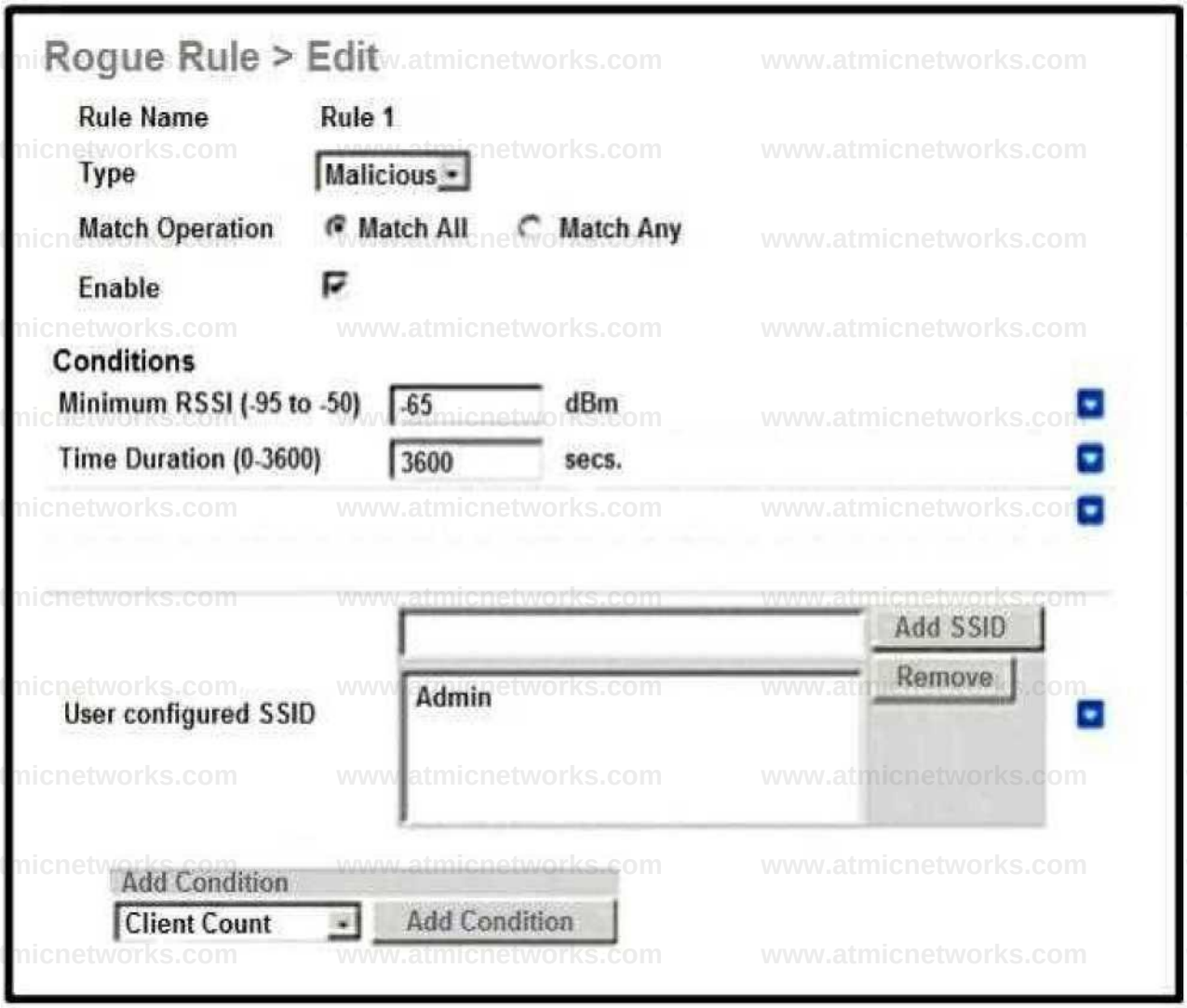
D. last of 10 monitor mode APs with the most wIPS events

Answer: A

Explanation:

Question: 110

Refer to the exhibit.



An engineer tries to manage the rogues on the Cisco WLC. Based on the configuration, which AP is marked as malicious by the controller?

A. rogue AP with SSID admin seen for 4000 seconds and heard at -70dBm

B. rogue AP with SSID admin seen for 3000 seconds and heard at -60dBm

C. rogue AP with SSID admin seen for 4000 seconds and heard at -60dBm

D. rogue AP with SSID admin seen for 3000 seconds and heard at -70dBm

Answer: C

Explanation:

The configuration for the Rogue Rule named “Rule 1” is set to classify an access point (AP) as malicious if it meets certain conditions. The rule specifies that the AP must have a Minimum RSSI (Received Signal Strength Indicator) of less than or equal to -65 dBm and must have been seen for a Time Duration greater than or equal to 3600 seconds. Among the options provided, both A and C have been seen for more than 3600 seconds, which satisfies the Time Duration condition. However, for the RSSI condition, only option C with an RSSI of -60 dBm meets the criteria of being less than or equal to -65 dBm. Therefore, option C is the correct answer, as it fulfills both conditions set by the Rogue Rule.

Question: 111

Which devices can be tracked with the Cisco Context Aware Services?

A. wired and wireless devices

B. wireless devices

C. wired devices

D. Cisco certified wireless devices

Answer: A

Explanation:

Cisco Context Aware Services provide real-time tracking of mobile assets and users by gathering contextual information from networked devices. This service is not limited to wireless devices; it can
track both wired and wireless devices within the network. The technology utilizes elements like Received Signal Strength Indicator (RSSI) and Time Difference of Arrival (TDoA) for location tracking and telemetry. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, and Cisco Context Aware Software FAQ.

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/context-aware-software/110836- cas-faq.html

Question: 112

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

Answer: A, E

Explanation:

A successful RF jamming attack primarily disrupts WLAN services by overwhelming the network with noise or unwanted signals, making it impossible for legitimate devices to communicate effectively. While physical damage to AP hardware is not a direct outcome of RF jamming, the persistent interference can lead to hardware malfunction due to overheating or overcompensation for the poor signal environment. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 113

An engineer must create an account to log in to the CLI of an access point for troubleshooting. Which configuration on the WLC will accomplish this?

A. Allow New Telnet Sessions

B. ReadWrite User Access Mode

C. SNMP V3 User

D. Global Configuration Enable Password

Answer: B

Explanation:

To create an account for CLI access to an access point for troubleshooting, the WLC must be configured to allow user access with the capability to make changes. The ReadWrite User Access Mode enables an engineer to have full read and write access to the AP's configuration via the CLI, which is necessary for performing troubleshooting tasks. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 114

A multitenant building contains known wireless networks in most of the suites. Rogues must be classified in the WLC. How are the competing wireless APs classified?

A. adhoc

B. friendly

C. malicious

D. unclassified

Answer: D

Explanation:

In a multitenant building, competing wireless APs are initially classified as 'unclassified' in the WLC. This classification means that the APs are not recognized as part of the network's infrastructure. Over time, administrators can classify these APs as 'friendly', 'malicious', or maintain them as 'unclassified' based on their potential impact on the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 115

An enterprise has recently deployed a voice and video solution available to all employees using AireOS controllers. The employees must use this service over their laptops, but users report poor service when connected to the wireless network. The programs that consume bandwidth must be identified and restricted. Which configuration on the WLAN aids in recognizing the traffic?

A. NetFlow Monitor

B. AVC Profile

C. QoS Profile

D. Application Visibility

Answer: B

Explanation:

Application Visibility and Control (AVC) profiles in AireOS controllers allow the identification and management of bandwidth consumption by different applications. By using AVC, administrators can set policies to prioritize or restrict bandwidth for specific applications, thus ensuring that critical services like voice and video are not adversely affected by bandwidth-heavy programs. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 116

Which customizable security report on Cisco Prime Infrastructure will show rogue APs detected since a point in time?

A. Network Summary

B. Rogue APs Events

C. New Rogue APs

D. Rogue APs Count Summary

Answer: C

Explanation:

The customizable security report in Cisco Prime Infrastructure that shows rogue access points (APs) detected since a point in time is the “New Rogue APs” report. This report is specifically designed to track and list all newly detected rogue APs within the network from a specified time, allowing network administrators to quickly identify unauthorized devices. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert

Guide)

Question: 117

After receiving an alert about a rogue AP, a network engineer logs into Cisco Prime Infrastructure and looks at the floor map where the AP that detected the rogue is located. The map is synchronized with a mobility services engine that determines that the rogue device is actually inside the campus. The engineer determines that the rogue is a security threat and decides to stop if from broadcasting inside the enterprise wireless network. What is the fastest way to disable the rogue?

A. Go to the location where the rogue device is indicated to be and disable the power.

B. Create an SSID similar to the rogue to disable clients from connecting to it.

C. Update the status of the rogue in Cisco Prime Infrastructure to contained.

D. Classify the rogue as malicious in Cisco Prime Infrastructure.

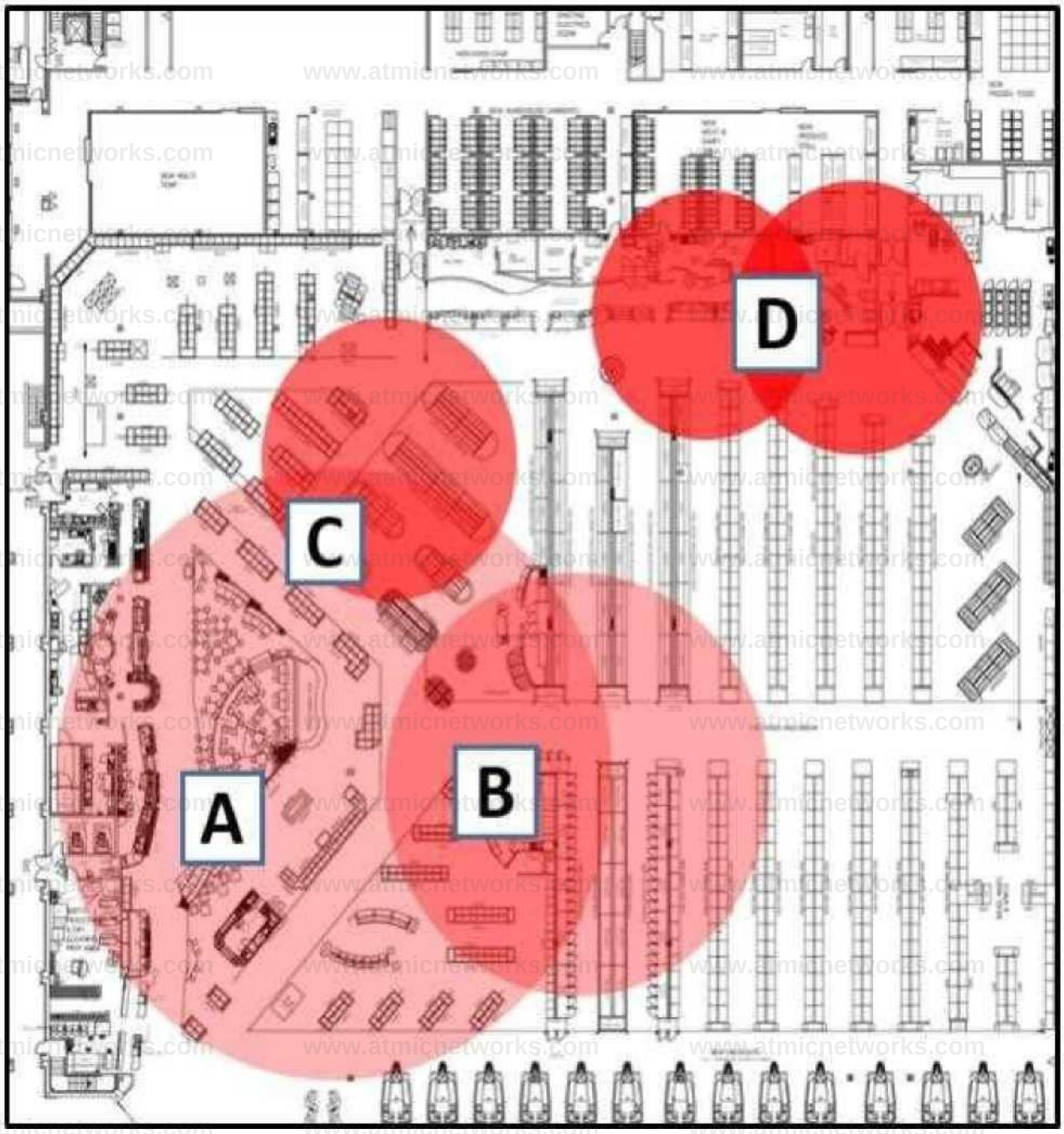
Answer: C

Explanation:

When a network engineer receives an alert about a rogue AP and determines it is a security threat inside the campus, the fastest way to disable it is by updating its status in Cisco Prime Infrastructure to 'contained'. This action instructs the system to prevent the rogue device from communicating with other devices on the network, effectively isolating it without having to physically locate or manually disable it. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 118

Refer to the exhibit.



Which area indicates the greatest impact on the wireless network when viewing the Cisco CleanAir Zone of Impact map of interferers?

A. A

B. B

C. C

D. D

Answer: A

Explanation:

The exhibit provided appears to be a floor map overlay with Cisco CleanAir Zone of Impact for interferers, which shows different areas affected by interference on a wireless network. The area labeled 'A' indicates the greatest impact on the wireless network due to its larger size compared with other zones, suggesting more significant interference or a stronger source of interference within this zone. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Reference: https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless- controllers/112139-cleanair-uwn-guide-00.html

Question: 119

A wireless network engineer must present a list of all rogue APs with a high severity score to senior management. Which report must be created in Cisco Prime Infrastructure to provide this information?

A. Rogue AP Count Summary

B. New Rogue APs

C. Rogue AP Events

D. Rogue APs

Answer: D

Explanation:

: In Cisco Prime Infrastructure, the report that must be created to present a list of all rogue APs with a high severity score to senior management is the "Rogue APs" report. This report provides detailed information about rogue access points detected in the network, including their severity score, which helps in assessing the potential risk they pose to the network security. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 120

An engineer must run a Client Traffic Stream Metrics report in Cisco Prime Infrastructure. Which task must be run before the report?

A. scheduled report

B. radio performance

C. client status

D. software

Answer: C

Explanation:

Before running a Client Traffic Stream Metrics report in Cisco Prime Infrastructure, the task that must be run is “client status”. This task collects the necessary data regarding the clients’ traffic streams, which is then used to generate the report. Reference := Cisco Prime Infrastructure Reports User Guide

Reference: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/reps.html

Question: 121

What is the maximum time range that can be viewed on the Cisco DNA Center issues and alarms page?

A. 3 hours

B. 24 hours

C. 3 days

D. 7 days

Answer: B

Explanation:

The maximum time range that can be viewed on the Cisco DNA Center issues and alarms page is 24 hours. This allows network administrators to monitor and troubleshoot recent issues and alarms within a one-day period. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 122

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:

When configuring access control on a WLC using a TACACS+ server for centralized authentication on network devices, the role value that must be configured under the shell profile on the TACACS+ server for a user with read-only permissions is "MONITOR". This role restricts the user to monitoring functions without the ability to make changes to the configuration. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 123

The CTO of an organization wants to ensure that all Android devices are placed into a separate VLAN on their wireless network. However, the CTO does not want to deploy ISE. Which feature must be implemented on the Cisco WLC?

A. WLAN local policy

B. RADIUS server overwrite interface

C. AAA override

D. custom AVC profile

Answer: A

Explanation:

To ensure that all Android devices are placed into a separate VLAN on their wireless network without deploying ISE, the feature that must be implemented on the Cisco WLC is “WLAN local policy”. This feature allows the network administrator to create policies that can classify and segregate devices based on their operating system, in this case, Android devices, into a designated VLAN. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 124

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?

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: 125

What must be configured on the Global Configuration page of the WLC for an AP to use 802.1x to authenticate to the wired infrastructure?

A. local access point credentials

B. RADIUS shared secret

C. TACACS server IP address

D. supplicant credentials

Answer: B

Explanation:

On the Global Configuration page of a Wireless LAN Controller (WLC), for an Access Point (AP) to use IEEE 802.1X for authenticating to the wired infrastructure, it is necessary to configure a RADIUS shared secret. This secret will be used by the AP as part of its credentials when communicating with a RADIUS server during the authentication process. Reference: (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 126

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:

When an engineer enables CPU ACLs on a Cisco device through Security > Access Control Lists > CPU Access Control Lists menu, this change applies immediately to both wireless and wired traffic directed towards the CPU of the device. This includes all management traffic destined for control plane services within the device itself, providing an additional layer of security against potential threats. Reference: (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 127

Refer to the exhibit.

An engineer is creating an ACL to restrict some traffic to the WLC CPU. Which selection must be made from the direction drop- down list?

A. It must be Inbound because traffic goes to the WLC.

B. Packet direction has no significance; it is always Any.

C. It must be Outbound because it is traffic that is generated from the WLC.

D. To have the complete list of options, the CPU ACL must be created only by the CLI.

Answer: A

Explanation:

When configuring an Access Control List (ACL) to restrict traffic to the Wireless LAN Controller (WLC) CPU, the direction of the traffic is crucial. Since the ACL is meant to control traffic that is destined for the WLC CPU, it should be set as "Inbound". This means that any rules applied within this ACL will affect incoming traffic towards the WLC, which is necessary when aiming to restrict certain types of traffic from reaching and potentially overwhelming the controller's processing capabilities.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 128

An engineer must implement a CPU ACL that blocks web management traffic to the controller, but they also must allow guests to reach a Web Authentication Redirect page. To which IP address is guest client HTTPS traffic allowed for this to work?

A. DNS server IP

B. controller management IP

C. virtual interface IP

D. client interface IP

Answer: C

Explanation:

For guests to reach a Web Authentication Redirect page while blocking web management traffic to the controller, guest client HTTPS traffic must be allowed to a specific IP address that does not interfere with management access. The virtual interface IP on a Cisco Wireless LAN Controller serves as a DHCP relay and is used for web authentication processes. Therefore, allowing HTTPS traffic to this IP enables guests to reach the redirect page without granting them access to manage the controller. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 129

An engineer needs to configure an autonomous AP for 802.1x authentication. To achieve the highest security an authentication server is used for user authentication. During testing, the AP fails to pass the user authentication request to the authentication server. Which two details need to be configured on the AP to allow communication between the server and the AP? (Choose two.)

A. username and password

B. PAC encryption key

C. RADIUS IP address

D. shared secret

E. group name

Answer: C, D

Explanation:

When configuring an autonomous Access Point (AP) for 802.1x authentication using an external authentication server like RADIUS, it's essential that AP knows where to send authentication requests and has a secure method of communicating with it. The RADIUS server's IP address must be configured on AP so it knows where to forward user credentials for verification. Additionally, a shared secret must be set up between AP and RADIUS server as part of their secure communication protocol; without this shared secret, they cannot trust each other's communications. Reference:
CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 130

A customer wants the APs in the CEO's office to have different usernames and passwords for administrative support than the other APs deployed throughout the facility. Which feature must be enabled on the WLC and APs to achieve this goal?

A. local management users

B. HTTPS access

C. 802.1X supplicant credentials

D. override global credentials

Answer: A

Explanation:

In Cisco Wireless LAN Controller (WLC) environments, the feature that allows for different usernames and passwords for administrative support on specific APs is the local management users. This feature enables the configuration of unique credentials on individual APs, separate from the global credentials used for the rest of the network. By enabling local management users, the APs in the CEO's office can have distinct administrative access controls, ensuring a higher level of security and customization. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 131

An engineer configured a Cisco AireOS controller with two TACACS+ servers. The engineer notices that when the primary TACACS+ server fails, the WLC starts using the secondary server as expected, but the WLC does not use the primary server again until the secondary server fails or the controller is rebooted. Which cause of this issue is true?

A. Fallback is enabled

B. Fallback is disabled

C. DNS query is disabled

D. DNS query is enabled

Answer: B

Explanation:

The issue described occurs when the fallback feature is disabled on the Cisco AireOS controller. When fallback is disabled, the controller does not attempt to reconnect to the primary TACACS+ server after it becomes available again following a

failure. Instead, it continues to use the secondary server until it fails or the controller is rebooted. Enabling fallback would allow the controller to periodically attempt to reconnect to the primary server. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 132

An engineer is implementing RADIUS to restrict administrative control to the network with the WLC management IP address of 192.168.1.10 and an AP subnet of 192.168.2.0/24. Which entry does the engineer define in the RADIUS server?

A. administrative access defined on the WLC and the network range 192.168.2.0/255.255.254.0

B. NAS entry of the virtual interface and the network range 192.168.2.0/255.255.255.0

C. shared secret defined on the WLC and the network range 192.168.1.0/255.255.254.0

D. WLC roles for commands and the network range 192.168.1.0/255.255.255.0

Answer: B

Explanation:

For RADIUS to restrict administrative control effectively, the engineer needs to define a Network Access Server (NAS) entry that corresponds to the WLC's management IP address and the AP subnet. The correct entry would be the NAS IP of the virtual interface (typically used for RADIUS communications) and the specific network range of the AP subnet, which is 192.168.2.0 with a subnet mask of 255.255.255.0. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 133

A customer requires wireless traffic from the branch to be routed through the firewall at corporate headquarters. A RADIUS server is in each branch location. Which Cisco FlexConnect configuration must be used?

A. central authentication and local switching

B. central authentication and central switching

C. local authentication and local switching

D. local authentication and central switching

Answer: B

Explanation:

To route wireless traffic from the branch through the firewall at corporate headquarters, the correct Cisco FlexConnect configuration is central authentication and central switching. This setup ensures that both user authentication and data traffic are handled centrally at the corporate headquarters, allowing the firewall to inspect and route the traffic accordingly. Local RADIUS servers in each branch can still be used for redundancy or other purposes, but the central control of traffic is maintained.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 134

Refer to the exhibit.

An engineer must restrict some subnets to have access to the WLC. When the CPU ACL function is enabled, no ACLs in the drop-down list are seen. What is the cause of the problem?

A. The ACL does not have a rule that is specified to the Management interface.

B. No ACLs have been created under the Access Control List tab.

C. When the ACL is created, it must be specified that it is a CPU ACL.

D. This configuration must be performed through the CLI and not though the web GUI.

Answer: C

Explanation:

The issue described in the scenario occurs because when creating an Access Control List (ACL) to be used for managing traffic to the Wireless LAN Controller's (WLC) CPU, it must be explicitly defined as a CPU ACL. If this specification is not made during the creation process, the ACL will not appear in the drop-down list when enabling the CPU ACL function. This is necessary because CPU ACLs are used to protect the WLC against potential Denial-of-Service (DoS) attacks by filtering incoming packets directed at the management interface before they are processed by the CPU. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 135

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 (Extensible Authentication Protocol) allows wireless LAN controllers to directly authenticate clients using an internal database, which can be useful when external RADIUS servers are unreachable. By enabling local EAP, client devices can still connect to wireless networks even if communication with RADIUS servers fails, ensuring continuous network access for users. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 136

An IT team is growing quickly and needs a solution for management device access. The solution must authenticate users from an external repository instead of the current local on the WLC, and it must also identify the user and determine what level of access users should have. Which protocol do you recommend to achieve these goals?

A. network policy server

B. RADIUS

C. TACACS+

D. LDAP

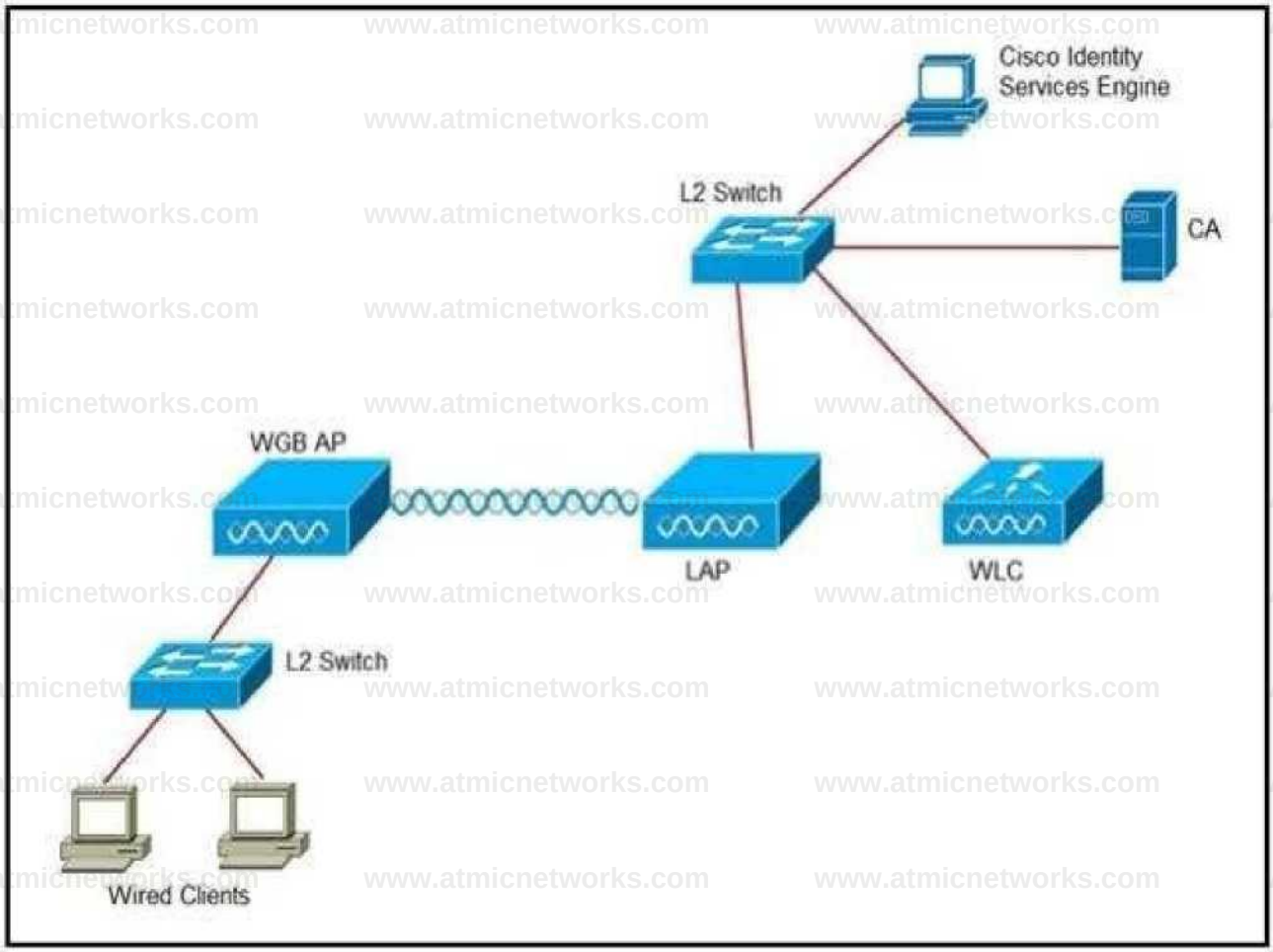
Answer: C

Explanation:

TACACS+ (Terminal Access Controller Access-Control System Plus) is recommended for managing device access as it provides a more granular level of control over user authentication and authorization than RADIUS. It allows for different levels of access based on user identity by interfacing with external repositories such as Active Directory or LDAP. This protocol helps in distinguishing between different users and assigning appropriate access rights based on their roles within an organization. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 137

Refer to the exhibit.



An engineer must connect a fork lift via a WGB to a wireless network and must authenticate the WGB certificate against the RADIUS server. Which three steps are required for this configuration? (Choose three.)

A. Configure the certificate, WLAN, and radio interface on WGB.

B. Configure the certificate on the WLC.

C. Configure WLAN to authenticate using ISE.

D. Configure the access point with the root certificate from ISE.

E. Configure WGB as a network device in ISE.

F. Configure a policy on ISE to allow devices to connect that validate the certificate.

Answer: A, E, F

Explanation:

To connect a Workgroup Bridge (WGB) to a wireless network and authenticate its certificate against a RADIUS server like ISE, the following steps are necessary:

A . Configure the certificate, WLAN, and radio interface on WGB: This is essential because the WGB needs to have the correct certificate to present to the RADIUS server for authentication. Additionally, the WLAN and radio interface must be configured to ensure proper communication with the wireless network.

E . Configure WGB as a network device in ISE: By configuring the WGB as a network device within ISE, it becomes a recognized entity that can be authenticated and authorized accordingly.

F . Configure a policy on ISE to allow devices to connect that validate the certificate: This step ensures that only devices with a validated certificate, such as the WGB, can connect to the network, enhancing security.

Question: 138

During the EAP process and specifically related to the client authentication session, which encrypted key is sent from the RADIUS server to the access point?

A. WPA key

B. session key

C. encryption key

D. shared-secret key

Answer: B

Explanation:

During the Extensible Authentication Protocol (EAP) process, the RADIUS server generates an encrypted session key after the client's identity is authenticated. This session key is sent to the access point to encrypt data frames between the client and the access point. It ensures that each session has a unique encryption key, enhancing security. Reference: Look for information on EAP and RADIUS in the CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide.

Question: 139

A network is set up to support wired and wireless clients. Both types must authenticate using 802.1X before connecting

to the network. Different types of client authentication must be separated on a Cisco ISE deployment. Which two configuration items achieve this task? (Choose two.)

A. device profiles

B. policy sets

C. separate networks

D. policy groups

E. policy results

Answer: B, D

Explanation:

To separate different types of client authentication on a Cisco ISE deployment, policy sets and policy groups can be used. Policy sets allow the creation of policies based on conditions such as device type, while policy groups categorize clients for the application of specific policies. Reference: Cisco ISE documentation on policy sets and policy groups will have detailed information.

Question: 140

An engineer is troubleshooting a Cisco CMX high-availability deployment and notices that the primary and backup Cisco CMX servers are both considered primary. Which command must the engineer run on the backup server?

A. cmxha convert backup

B. cmxha backup convert

C. cmxha secondary convert

D. cmxha convert secondary

Answer: A

Explanation:

The command cmxha convert backup is used on the backup Cisco CMX server to designate it as the secondary server in a high-availability deployment. This command helps to resolve the issue where both servers are considered primary. Reference: Cisco CMX high-availability documentation will provide more details on this command.

Question: 141

A network administrator managing a Cisco Catalyst 9800-80 WLC must place all iOS connected devices to the guest SSID on VLAN 101. The rest of the clients must connect on VLAN 102 distribute load across subnets. To achieve this configuration, the administrator configures a local policy on the WLC. Which two configurations are required? (Choose two.)

A. Assign a policy map under global security policy settings.

B. Add local profiling policy under global security policy settings.

C. Create a service template.

D. Allow HTTP and DHCP profiling under policy map.

E. Enable device classification on global wireless settings.

Answer: C, E

Explanation:

To segregate iOS devices to the guest SSID on VLAN 101 and distribute the rest of the clients on VLAN 102, creating a service template and enabling device classification are required. The service template specifies the VLAN assignment, while device classification identifies the type of device connecting to the network. Reference: Cisco Catalyst 9800-80 WLC documentation on local policies and device classification.

Question: 142

An engineer is assembling a PCI report for compliance purposes and must include missed best practices that are related to WLAN controllers. The engineer has access to all WLCs, Cisco MSE, and Cisco Prime Infrastructure. Which method

most efficiently displays a summary of inconsistencies?

A. WLC running-config

B. Cisco Prime Infrastructure monitoring

C. Cisco Prime Infrastructure reporting

D. WLC logs

Answer: C

Explanation:

Cisco Prime Infrastructure reporting provides a comprehensive summary of inconsistencies and missed best practices related to WLAN controllers. It aggregates data from all WLCs, Cisco MSE, and itself to generate detailed reports.
Reference: Cisco Prime Infrastructure reporting features documentation.

Question: 143

An engineer is ensuring that, on the IEEE 802.1X wireless network, clients authenticate using a central repository and local credentials on the Cisco WLC. Which two configuration elements must be completed on the WLAN? (Choose two.)

A. TACACS+

B. MAC authentication

C. local EAP enabled

D. web authentication

E. LDAP server

Answer: C, E

Explanation:

On a WLAN that uses IEEE 802.1X for wireless network authentication, enabling local EAP allows clients to authenticate

using locally stored credentials on the Cisco Wireless LAN Controller (WLC), which is useful in scenarios where the external RADIUS server is unavailable. The LDAP server option is used to authenticate clients against a central repository, such as an LDAP directory. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 144

An engineer must enable LSS for the AppleTV mDNS service only when ORIGIN is set to Wired. Which action meets this requirement?

A. Set ORIGIN to Wired. Enable LSS by using the config mdns service Iss All command.

B. Set ORIGIN to Wired. Enable LSS by using the config mdns service Iss AppleTV command.

C. Set ORIGIN to either Wireless or All. Enable LSS by using the config mdns service Iss All command.

D. Set ORIGIN to either Wireless or All. Enable LSS by using the config mdns service Iss enable AppleTV command.

Answer: B

Explanation:

Link-Local Service (LSS) filtering for mDNS (Multicast Domain Name System) is used to control the propagation of mDNS services across the network. To enable LSS for the AppleTV mDNS service only when ORIGIN is set to Wired, the correct action is to set ORIGIN to Wired and enable LSS specifically for the AppleTV service. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 145

A Cisco 8540 WLC manages Cisco Aironet 4800 Series Aps and sends AoA data to a Cisco CMX 3375 Appliance for Hyperlocation. The load from the WLC is distributed to another virtual CMX server using CMX grouping. The virtual CMX server shows location RSSI data and not Hyperlocation. No AoA metrics are shown on the metrics page of the CMX virtual appliance under System > Metrics > Location Metrics. How must the network administrator resolve this issue?

A. Enable Wireless > Access Points > Global Configuration> Enable Hyperlocation on the WLC.

B. Enable the HALO module on the CMX appliance for the data collection.

C. Allow port 2003 for AoA packets to flow through between the CMX appliances.

D. Use one Hyperlocation-enabled WLC and CMX for AoA data.

Answer: C

Explanation:
The issue described indicates that the Angle of Arrival (AoA) data is not being transmitted between the Cisco Wireless LAN Controller (WLC) and the virtual CMX server. To resolve this, the network administrator must ensure that port 2003 is allowed for AoA packets to flow through between the CMX appliances, which is necessary for Hyperlocation data transmission. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 146

An engineer completes the setup of a two-node Cisco ISE deployment for a guest portal. When testing the portal, the engineer notices that sometimes there is a certificate CN mismatch. Which certificate type helps resolve this issue?

A. Public-Signed Root

B. Public-Signed SAN

C. Self-Signed Wildcard

D. Self-Signed Standard

Answer: B

Explanation:
A Public-Signed SAN (Subject Alternative Name) certificate allows multiple domain names to be protected with a single certificate. This is useful in a distributed environment like a guest portal on Cisco ISE, where there may be multiple nodes with different Common Names (CNs). Using a SAN certificate can prevent CN mismatch errors during SSL/TLS handshakes. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official

Question: 147

On a Cisco Catalyst 9800 Series Wireless Controller, an engineer wants to prevent a FlexConnect AP from allowing wireless clients to connect when its Ethernet connection is nonoperational. Which command set prevents this connection?

A. config terminal

wireless flexconnect profile [profile name]

ethernet-fallback-enable

end

B. config terminal

wireless flexconnect profile [profile name]

fallback-radio-shut

end

C. config terminal

wireless profile flex [profile name]

fallback-radio-shut

end

D. config terminal

wireless profile flex [profile name]

ethernet-fallback-enable

end

Answer: B

Explanation:

On a Cisco Catalyst 9800 Series Wireless Controller, the command set that prevents a FlexConnect AP from allowing

wireless clients to connect when its Ethernet connection is nonoperational is the fallback-radio-shut command within the FlexConnect profile configuration. This command disables the radios on the AP, thus preventing client connections during Ethernet link failure. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 148

The security policy mandates that only controller web management traffic is allowed from the IT subnet. In testing, an engineer is trying to connect to a WLAN with Web Authentication for guest users, but the page is timing out on the wireless client browser. What is the cause of the issue?

A. The implemented CPU ACL on the controller is blocking HTTP/HTTPS traffic from the guest clients.

B. Web Authentication Redirect is not supported with CPU ACLs.

C. The DNS server that is configured on the controller is incorrect.

D. Web Authentication Redirect is supported only with Internet Explorer, and the client is using Google Chrome.

Answer: A

Explanation:

The issue is likely caused by the CPU ACL on the controller, which is blocking HTTP/HTTPS traffic from the guest clients. When a WLAN with Web Authentication is used, the wireless client's browser is redirected to a web page for authentication. If the CPU ACL is configured to only allow controller web management traffic from the IT subnet, it may inadvertently block the necessary HTTP/HTTPS traffic for the Web Authentication process, leading to a timeout on the wireless client browser. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, specifically the sections discussing CPU ACLs and their impact on network traffic.

Question: 149

A controller shows that an AP in your environment is detecting interference, but the AP health score in Cisco DNA Center is unaffected. What are two reasons that Cisco DNA Center is ignoring the interference? (Choose two.)

A. The interference is less than or equal to 30% on the 2.4 GHz radio.

B. The interference is less than or equal to 50% on the 2.4 GHz radio.

C. Cisco DNA Center includes only Cisco CleanAir interferers in the AP health score.

D. The interference is less than or equal to 30% on the 5 GHz radio.

E. Cisco DNA Center does not include interference in the AP health score.

Answer: C, D

Explanation:

Cisco DNA Center is likely ignoring the interference detected by the AP because it includes only Cisco CleanAir interferers in the AP health score (option C), and the interference is less than or equal to 30% on the 5 GHz radio (option D). Cisco DNA Center's AP health score algorithm may not consider interference that falls below a certain threshold or interference that is not identified as a CleanAir event. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, particularly the chapters on Cisco DNA Center and CleanAir technology.

Question: 150

An engineer must control administrative access to the WLC using their Active Directory without being concerned about RBAC after the admin user is authenticated. Which two features does the engineer configure to accomplish this task? (Choose two.)

A. Device Admin Policy Set

B. User Access Mode: ReadWrite

C. ACL

D. RADIUS server

E. TACACS server

Answer: D, E

Explanation:

To control administrative access to the WLC using Active Directory without concern for RBAC postauthentication, the engineer would configure a RADIUS server (option D) and a TACACS server (option E). These servers can integrate with Active Directory to authenticate users, and once authenticated, the admin user's access level can be determined without the need for additional rolebased access control configurations within the WLC. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, focusing on the integration of WLC with RADIUS and TACACS servers for administrative access control.

Question: 151

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:

To segregate all iPads on the guest WLAN to a separate VLAN without using Cisco ISE, the engineer can create a local policy on the WLC (option A). This local policy can be configured to identify iPad devices and assign them to a specific VLAN based on their device profile or other identifying characteristics. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, especially the sections that cover local policies and device profiling on the WLC.

Question: 152

In a Cisco WLAN deployment, it is required that all Aps from branch1 remain operational even if the control plane CAPWAP tunnel is down because of a WAN failure to headquarters. Which operational mode must be configured on the APs?

A. disconnected

B. standalone

C. lightweight

D. connected

Answer: B

Explanation:

In a Cisco WLAN deployment where it is required that all APs from branch1 remain operational even if the control plane CAPWAP tunnel is down, the operational mode that must be configured on the APs is standalone (option B). In standalone mode, the APs can continue to function and provide network access to clients even without a connection to the WLC, which is essential during a WAN failure to headquarters. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, with a focus on AP operational modes and their behavior during network disruptions.

Question: 153

An engineer added more APs to newly renovated areas in building. The engineer is now receiving Out-of-Sync alarms on Cisco Prime Infrastructure. Which two actions resolve this issue? (Choose two.)

A. Manually synchronize from Cisco Prime Infrastructure.

B. Manually synchronize from MSE.

C. Enable automatic synchronization on Cisco Prime Infrastructure.

D. Enable automatic synchronization on MSE.

E. Add new APs to maps on Cisco Prime Infrastructure.

Answer: A, C

Explanation:

The Out-of-Sync alarms in Cisco Prime Infrastructure typically indicate that there is a discrepancy between the

configuration of the APs as known by Prime Infrastructure and their actual configuration. To resolve this issue, the engineer can either manually synchronize the APs from Cisco Prime Infrastructure (A) or enable automatic synchronization on Cisco Prime Infrastructure © to ensure that the AP configurations are updated automatically. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 154

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?

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: 155

A customer is concerned that their wireless network is detecting spurious threats from channels that are not being used by their wireless infrastructure. Which two technologies must they deploy?
(Choose two.)

A. FlexConnect mode

B. monitor mode

C. sniffer mode with no submode

D. local mode with WIPS submode

E. rogue detector mode

Answer: B, D

Explanation:

To address concerns about detecting spurious threats from channels not used by the wireless infrastructure, deploying APs in monitor mode (B) and local mode with WIPS submode (D) would be beneficial. Monitor mode allows APs to listen to the wireless spectrum and identify potential threats, while WIPS (Wireless Intrusion Prevention System) submode enhances the ability to detect and mitigate wireless threats. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 156

A network engineer created a new wireless network that will be used for guest access. The corporate network must utilize all rates. The guest network must use only lower rates instead of 802.11n data rates. To what must the WMM policy of the WLAN be set to accomplish this task?

A. required

B. allowed

C. disabled

D. mandatory

Answer: C

Explanation:

To ensure that the guest network uses only lower rates instead of 802.11n data rates, the WMM (WiFi Multimedia) policy of the WLAN should be set to disabled ©. This will prevent the use of 802.11n data rates, which require WMM to be enabled. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 157

Refer to the exhibit.

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

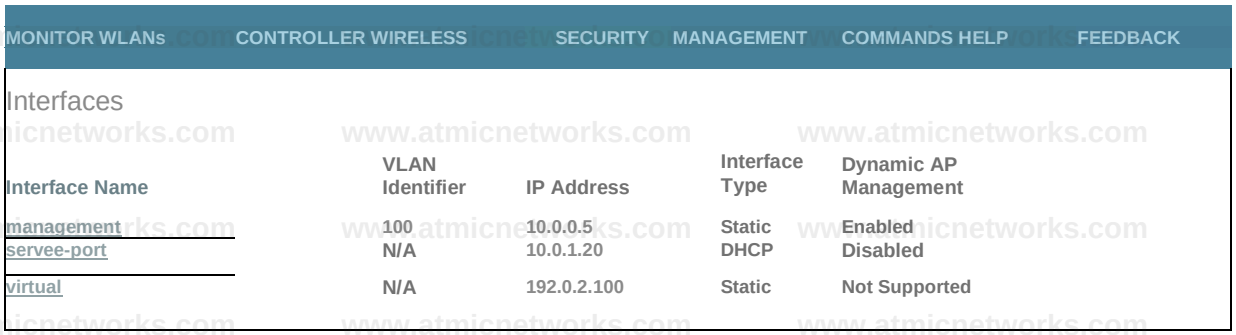
Access Control Lists > Edit

General

Access Lst Name secure 0

Deny Counter*

Seq	Action	Source IP	Mask	Destination IP	Mask	Protocol	Source Port	Best Port	DSCP	Direction
J.	Deny	0000	/oooo	10005	7 255 255 255 255	TCP	Any	HTTPS	Any	Any
X	Deny	0000	/oooo	10005	/255 255 255 255	TCP	Any	22	Any	Any



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	100	10.0.0.5	Static	Enabled
servee-port	N/A	10.0.1.20	DHCP	Disabled
virtual	N/A	192.0.2.100	Static	Not Supported

An engineer implemented the CPU ACL on your Cisco 5520 Series Wireless LAN Controller, and the controller is no longer manageable via the network. What must be changes on this CPU ACL to enable it to manage the controller again?

A. Permit statements must be added to the top of the ACL in both directions, which specify the network to be managed from and the virtual interface of the controller.

B. Line 1 must be set to a destination port of HTTP.

C. Permit statements must be added to the top of the ACL, which specify the network to be managed from.

D. Line 1 must be set to the inbound direction.

Answer: A

Explanation:

If the Cisco 5520 Series Wireless LAN Controller is no longer manageable via the network after implementing a CPU ACL,

permit statements must be added to the top of the ACL in both directions (A). These statements should specify the network from which management is allowed and the virtual interface of the controller to ensure proper management access. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 158

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, C

Explanation:

To offer indoor directions to patient rooms using the existing wireless infrastructure, the hospital would need to install Cisco MSE (B) and Cisco CMX Visitor Connect ©. Cisco Mobility Services Engine (MSE) provides advanced location services, including tracking for Wi-Fi clients, which is essential for indoor navigation. Cisco CMX Visitor Connect, part of the Cisco Connected Mobile Experiences (CMX) solutions, allows for the customization of visitor experiences, such as indoor navigation. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 159

When configuring a large, high-availability wireless network, which change to a mobility group creates less load on the controllers and maintains the same mobility messages?

A. Configure mobility group multicast messaging.

B. Remove unnecessary controllers from the mobility group.

C. Configure the controllers into separate RF groups from the mobility groups.

D. Separate the controllers into different mobility groups per controller.

Answer: B

Explanation:

Removing unnecessary controllers from the mobility group (B) would create less load on the controllers while maintaining the same mobility messages. This is because each controller in a mobility group shares its client database with other controllers, which can lead to increased overhead. By minimizing the number of controllers in the group, the load is reduced. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 160

A healthcare organization notices many rogue APs and is concerned about a honeypot attack. Which configuration must a wireless network engineer perform in Cisco Prime Infrastructure to prevent these attacks most efficiently upon detection?

A. Set the auto containment level to 0 and select the Using Our SSID containment option.

B. Set the manual containment level to 4 and select the Ad Hoc Rogue AP containment option.

C. Set the auto containment level to 0 and select the Ad Hoc Rogue AP containment option.

D. Set the auto containment level to 4 and select the Using Our SSID containment option.

Answer: D

Explanation:

To prevent honeypot attacks most efficiently, the wireless network engineer should set the auto containment level to 4 and select the Using Our SSID containment option (D). This configuration allows the system to automatically contain rogue APs that are spoofing the organization's SSID, which is a common tactic in honeypot attacks. Reference: CCNP Enterprise Wireless Design ENWLSD 300425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 161

An engineer is configuring a new wireless network for guest access. The Facebook page of the company must be viewed by the guest users before they get access to the network. A Cisco MSE is used as a wireless component. Which URL must be used in the configuration as the external redirection URL?

A. http://<MSE>:8083/visitor/login.do
B. http://<MSE>:8083/fbwifi/forward
C. http://<MSE>:8084/visitor/login.do
D. http://<MSE>:8084/fbwifi/forward

Answer: B

Explanation:

The correct URL to be used in the configuration as the external redirection URL for guests to view the company's Facebook page before accessing the network is http://<MSE>:8083/fbwifi/forward (B). This URL is associated with the Cisco MSE's Facebook Wi-Fi feature, which facilitates the redirection process. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 162

An IT administrator deployed an OEAP to the home of a remote user, but the OEAP cannot reach the WLC. Which two configuration settings must be completed before an OEAP is deployed successfully? (Choose two.)

A. Configure Secondary Controller Name and Management IP address in the High Availability tab.
B. Configure LSC to authorize the OEAP.
C. Configure the AP mode to FlexConnect and check the box for Office Extend AP.

D. Configure the WLC with an external IP address on the virtual interface.

E. Configure Primary Controller Name and Management IP address in the High Availability tab.

Answer: C, E

Explanation:

Before deploying an OEAP successfully, the IT administrator must configure the AP mode to FlexConnect and check the box for Office Extend AP ©, and configure the Primary Controller Name and Management IP address in the High Availability tab (E). These settings ensure that the OEAP can establish a connection to the WLC and function correctly in a remote user's home. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide.

Question: 163

An IT administrator deploys Cisco 2802i APs in all office locations, including main campus and branch offices. The WLC that manages the APs is located at the data center on the main campus. The APs on the main campus are configured to use Local mode and the APs in the branches use FlexConnect mode. Which configuration must be applied to the APs for corporate devices on the main campus to be mapped to the local LAN switch on different VLANs according to the VLAN tag ID and WLAN?

A. Enable Central DHCP Processing.

B. Disable FlexConnect Local Auth

C. Enable FlexConnect Local Switching.

D. Disable VLAN-based Central Switching.

Answer: C

Explanation:

In a FlexConnect deployment, enabling FlexConnect Local Switching allows branch office APs to map client traffic directly onto the local LAN, bypassing the need to tunnel all traffic back to the WLC at the main campus. This is essential for corporate devices at branch offices to access local resources efficiently and to be mapped to the correct VLANs according

to their VLAN tag ID and WLAN. This setting is not relevant for APs in Local mode at the main campus, as they already switch traffic locally by default.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 164

An engineer is in the process of implementing Fastiane on a wireless network with a Mobility Express AP installed and Apple end-user devices. Due to a security concern, the IT department has updated all the iPads to version 14.5.423551943. Which QoS profile must the engineer configure on the user WLAN?

A. Platinum

B. Best Effort

C. Bronze

D. Silver

Answer: A

Explanation:

Fastlane is a feature developed by Apple and Cisco that provides a higher-quality user experience for critical business applications. To implement Fastlane, the WLAN must use the Platinum QoS profile, which is designed to prioritize business-critical traffic and applications. Since the IT department has updated the iPads to a specific version, it is important to ensure that the QoS settings align with the requirements of Fastlane to maintain application performance and security.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 165

An engineer wants to upgrade the APs in a Cisco FlexConnect group. To accomplish this upgrade, the FlexConnect AP

Upgrade setting will be used. One AP of each model with the lowest MAC address in the group must receive the upgrade directly from the controller. Which action accomplishes this direct upgrade?

A. Remove the APs from the group.

B. Reboot all APs before the upgrade.

C. Allocate the master APs to different groups.

D. Do not set any master APs.

Answer: D

Explanation:

The FlexConnect AP Upgrade feature allows for a selective upgrade process within a FlexConnect group. By not setting any master APs, the WLC will automatically select one AP of each model with the lowest MAC address to receive the upgrade directly from the controller. This ensures that the upgrade is distributed efficiently across different AP models in the group without manual intervention.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 166

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?

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.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 167

Refer to the exhibit.

Data Rates *

1 Mbps	Disabled ▼
2 Mbps	Disabled *
5.5 Mbps	Disabled ▼
6 Mbps	Supported
9 Mbps	Mandatory *
11 Mbps	Disabled
12 Mbps	Mandatory *
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	I Supported *

An engineer is configuring a Cisco wireless LAN controller and needs wireless multicast to use the 54Mbps rates.

Which action meets this requirement?

A. Change the 24 Mpbs to Supported.

B. Set all data rates below 54 Mbps to Supported.

C. Change the 54 Mpbs to Mandatory.

D. Set all data rates below 54 Mbps to Disable.

Answer: C

Explanation:

In a Cisco wireless LAN controller, setting a specific data rate to 'Mandatory' means that all wireless clients must be able to communicate at this rate. To ensure that multicast uses the 54Mbps rates, one must set the 54Mbps data rate to 'Mandatory'. This configuration will make it so that all multicast traffic is transmitted at this minimum set data rate, thus meeting the requirement specified by the engineer.

Question: 168

DRAG DROP

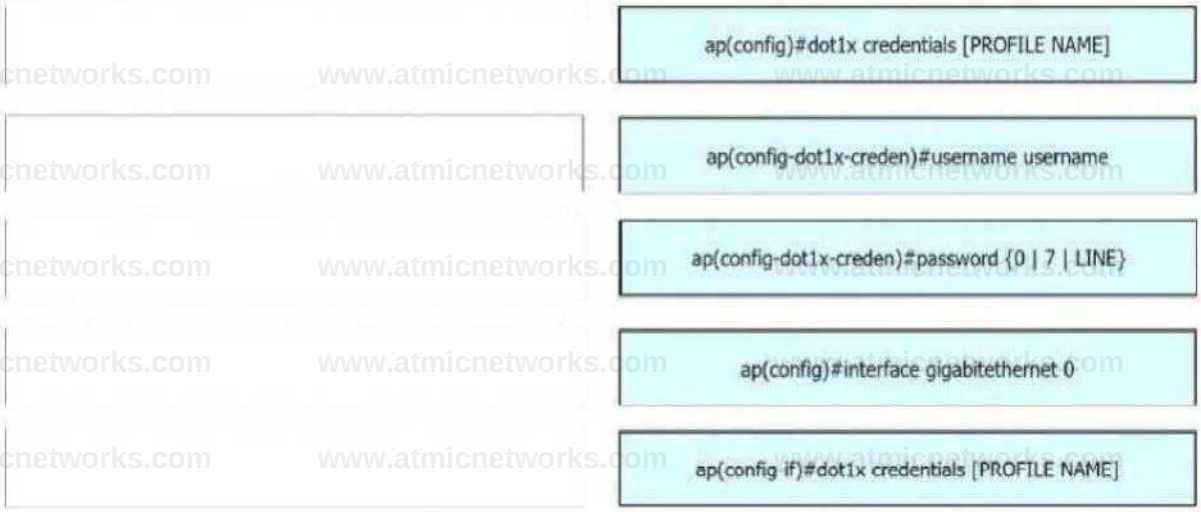
A network engineer must get an autonomous AP to authenticate to the upstream switch via IEEE 802.1 X. Drag and drop the commands from the left onto the right to complete the configuration.

Answer Area

Answer:

Explanation:

Answer Area



Question: 169

A network administrator managing a Cisco Catalyst 9800 WLC must place all iOS-connected devices to the guest SSID on VLAN 101. The rest of the clients must connect on VLAN 102 to distribute load across subnets. To achieve this configuration, the administrator configures a local policy on the WLC.

Which two configurations are required? (Choose two.)

A. Assign a policy map under global security policy settings.

B. Add local profiling policy under global security policy settings.

C. Create a service template.

D. Allow HTTP and DHCP profiling under policy map.

E. Enable device classification on global wireless settings.

Answer: B, E

Explanation:

To segregate iOS-connected devices onto a guest SSID on VLAN 101 and the rest of the clients on VLAN 102, specific configurations are needed on the Cisco Catalyst 9800 Wireless LAN Controller (WLC). The correct configurations

required are:

Add local profiling policy under global security policy settings (Option B): This allows the WLC to profile devices based on their operating system. By identifying iOS devices, a local profiling policy can then direct these devices to the appropriate VLAN.

Enable device classification on global wireless settings (Option E): Device classification is necessary for the WLC to differentiate between device types. Once enabled, it can apply different policies based on whether a device is recognized as an iOS device or not.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 170

An engineer is planning an image upgrade of the WLC, and hundreds of APs are spread across remote sites with limited WAN bandwidth. The engineer must minimize the WAN utilization for this upgrade. Which approach must be used for the AP image upgrade?

A. Predownload the new code to the APs.

B. Use the Smart AP image upgrade feature.

C. Allow the APs to download their code after WLC reboot.

D. Execute parallel TFTP code upgrade on the APs via SSH.

Answer: A

Explanation:

When planning an image upgrade for a large number of Access Points (APs) across remote sites with limited WAN bandwidth, it's crucial to minimize WAN utilization. The best approach in this scenario is:

Predownload the new code to the APs (Option A): This method involves sending the new firmware image to all APs before actually rebooting them with the new image. It allows APs to download firmware when network usage is low, thus minimizing impact during peak hours.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert

Guide)

Question: 171

Refer to the exhibit.

(Test-1) >show network summary Fir-Network Name..... . .... Test-1
Web Mode..... .....Disable
Secure Web Mode..... Enable
Secure Web Mode Cipher-Option High .....Disable
Secure Web Mode Cipher-Option SSLv2.....Disable
Secure Web Mode RC4 Cipher Preference .....Disable
OCSP..... Disabled
OCSP responder URL ..... Secure Shell (ssh) Enable
Telnet .....Disable
Ethernet Multicast Forwarding.....Disable
Ethernet Broadcast Forwarding.....Disable
IPv4 AP Muiticast/Broadcast Mode .....Unicast
IGHP snooping .... Disabled
IGHP timeout..... 60 seconds
IGHP Query Interval..... 20 seconds
HLD snooping... .... Disabled
HLD timeout ..... 60 seconds
HLD query interval ..... 20 seconds
User Idle Timeout .... 3600 seconds
ARP Idle Timeout..... 3600 seconds
Cisco AP Default Master .....Disable
AP Join Priority..... ... Disable

WebPortal Online Client 0
■DNS snooping .... Disabled
■DNS Query Interval..... 15 minutes

(Test-1) >show mdns service summary Humber of Services..... 5

Service-Name	LSS	Origin	No SP	Service-string
AirPrint	No	All	0	_ipp._tcp. local.
AppleTV	No	All	0	_airplay. tcp. local.
HP PhotosmartPrinter 1	No	All	0	universal, sub. ipp. _tcp.local. HP Photosmart Printer 2
	No	All	0	cups. sub. ipp. tcp. local. Printer
	No	All	0	_printer. tcp.local.

An engineer configured a BYOD policy that allows for printing on the WLAN using Bonjour services. However, the engineer cannot get printing to work. The WLC firmware is 8.x. What must be implemented on the controller?

A. Enable mDNS and IGMP snooping.

B. Activate location-specific services.

C. Configure Secure Web Mode Cipher-Option SSLv2.

D. Increase the IGMP Query Interval value

Answer: A

Explanation:

For printing services using Bonjour in a WLAN environment where mDNS services are utilized, especially with WLC firmware version 8.x, it's essential that:

Enable mDNS and IGMP snooping (Option A): Multicast DNS or mDNS needs to be enabled for Bonjour services to function correctly as they rely on this protocol for service discovery within local networks. IGMP snooping improves network efficiency by ensuring multicast traffic is only forwarded to nodes that have explicitly requested it.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 172

A network administrator just completed the basic implementation of Cisco CMX and tries to implement location tracking. The administrator is having trouble establishing connectivity between one of the WLCs through NMSP. What must be configured to establish this connectivity? (Choose two.)

A. Add permanent licenses on the Cisco CMX server.

B. Allow on the firewall port 16113 between Cisco CMX and the WLC.

C. Enable NMSP on the WLC.

D. Reboot Cisco CMX after adding the WLC for the first time.

E. Add to the WLC the MAC address and SSC key for the Cisco CMX server.

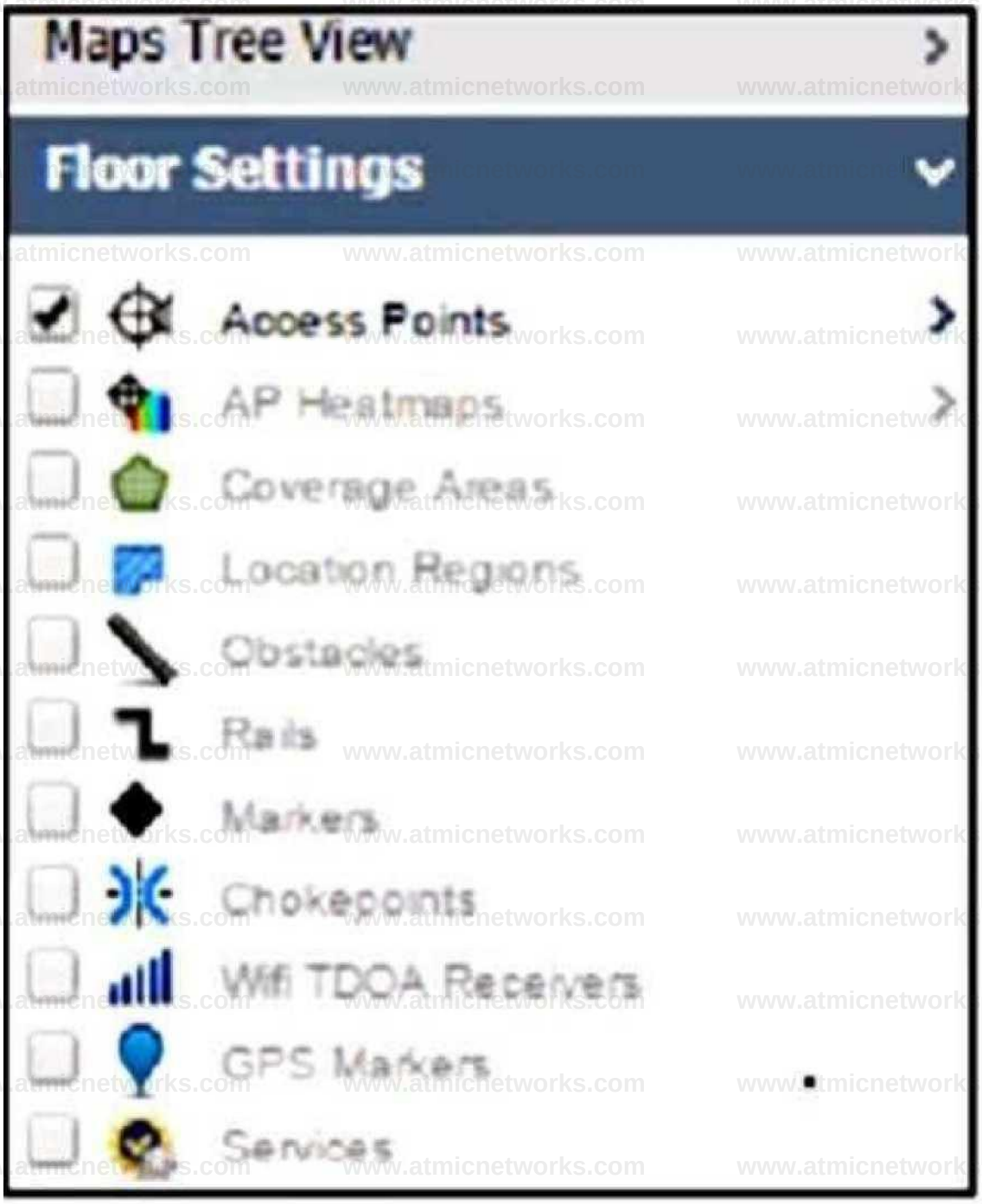
Answer: C, E

Explanation:

To establish connectivity between a Wireless LAN Controller (WLC) and Cisco's Connected Mobile Experiences (CMX) through Network Mobility Services Protocol (NMSP), it is essential to enable NMSP on the WLC, which facilitates communication with location-based services like CMX. Additionally, for secure communication, it is necessary to add the MAC address of the Cisco CMX server to the WLC along with its SSC (Self-Signed Certificate) key, ensuring that both devices can authenticate each other and establish a trusted connection. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 173

Refer to the exhibit.



An engineer must provide a position of rogue APs on a floor map using Cisco PI 3.0, but no rogue AP options are showing on the left-hand navigation menu under Maps. What is the reason for this omission?

A. An assurance license is not installed.

B. The controller operational status background task is disabled.

C. The Show Detected Interferers feature under the AP option is disabled.

D. Cisco MSE has not been added to Cisco PI.

Answer: D

Explanation:

The absence of rogue AP options in the navigation menu under Maps in Cisco Prime Infrastructure (PI) version 3.0 indicates that there is an issue with integrating location services, which are provided by Mobility Services Engine (MSE). Without adding MSE to PI, location-based services such as tracking rogue access points cannot be utilized or displayed within PI's interface. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 174

WPA2 Enterprise with 802.1X is being used for clients to authenticate to a wireless network through a Cisco ISE server. For security reasons, the network engineer wants to ensure that only PEAP authentication is used. The engineer sent instructions to clients on how to configure the supplicants, but the ISE logs still show users authenticating using EAP-FAST. Which action ensures that access to the network is restricted for these users unless the correct authentication mechanism is configured?

A. Enable AAA override on the SSID, gather the usernames of these users, and disable the RADIUS accounts until the devices are correctly configured.

B. Enable AAA override on the SSID and configure an ACL on the WLC that allows access to users with IP addresses from a specific subnet.

C. Enable AAA override on the SSID and configure an access policy in Cisco ISE that denies access to the list of MACs that have used EAP-FAST.

D. Enable AAA override on the SSID and configure an access policy in Cisco ISE that allows access only when the EAP authentication method is PEAP.

Answer: D

Explanation:

To ensure that only PEAP authentication is used for network access through a wireless network using WPA2 Enterprise with 802.1X, enabling AAA override on an SSID allows individual client authentication requests to be modified by RADIUS server responses dynamically. By configuring an access policy in Cisco Identity Services Engine (ISE) that permits access solely when PEAP is used as the EAP authentication method, any user attempting to authenticate using EAP-FAST will be denied network access until their devices are configured correctly for PEAP usage. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 175

Refer to the exhibit.

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

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.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 176

A wireless engineer deployed all remote sites as FlexConnect. The client VLAN assignment on these sites is configured manually mapped by WLAN and using local switching. Dynamic VLAN assignment is provided by the newly deployed Cisco ISE. Which IETF attribute must be configured on the AAA server to send that VLAN ID?

A. Tunnel-Medium-Type

B. Tunnel-Client-Endpoint

C. Tunnel-Assignment-ID

D. Tunnel-Private-Group-ID

Answer: D

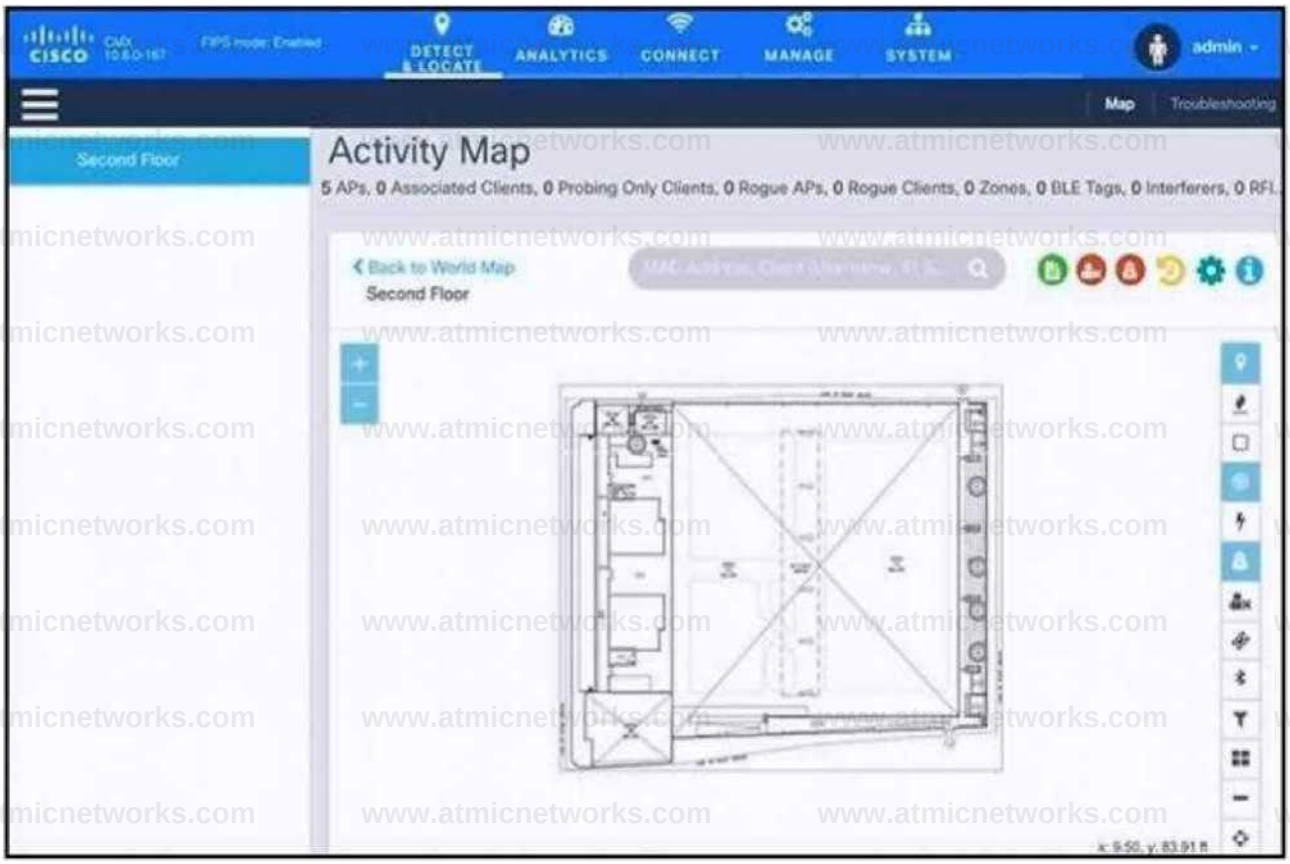
Explanation:

In FlexConnect deployments with local switching, dynamic VLAN assignments are facilitated by Cisco ISE through the use of specific RADIUS attributes. The Tunnel-Private-Group-ID attribute is essential for communicating the VLAN ID to the access point, which then applies it to the wireless client after successful authentication.

Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 177

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?

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: 178

Refer to the exhibit.

```
aaa new-model
aaa local authentication default authorization default
aaa group server radius rad-group server name ise-lab272
aaa authentication login default local

wireless profile policy test profiling accounting-list acct method
  radius-profiling
```

A network architect configured the Cisco Catalyst 9800 Series Controller to find out information on client types in the wireless network. RADIUS profiling is enabled so that the controller forwards the information about clients to a Cisco ISE server through vendor-specific RADIUS attributes. The ISE server is not profiling any data from the controller. Which configuration must be added in the blank in the code to accomplish the profiling on the Cisco 9800 Series controller?

A. aaa accounting identity acct_method start-stop group rad-group

B. aaa accounting network acct_method start-stop group rad-group

C. aaa accounting exec acct_method start-stop group rad-group

D. aaa accounting commands acct_method start-stop group rad-group

Answer: B

Explanation:

In the context of Cisco Catalyst 9800 Series Wireless Controllers, RADIUS profiling requires the correct AAA (Authentication, Authorization, and Accounting) configuration to collect and forward details about clients to a RADIUS server such as Cisco ISE (Identity Services Engine). The correct command in this scenario is "aaa accounting network acct_method start-stop group rad-group" which enables accounting of network services. This command starts gathering accounting information for all network-related service requests and sends start and stop records to the RADIUS server specified in the 'rad-group'. This allows the controller to forward information about clients' activities on the wireless network to Cisco ISE for profiling.

Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300430 Official Cert Guide)

Question: 179

Company XYZ recently migrated from AireOS to IOS XE 9800 WLCs. The Internet bandwidth must be limited to 5 Mbps for each guest client as per the global standard. In which configuration on the Cisco Catalyst 9800 WLC must the QoS requirement be added?

A. table map

B. policy map

C. service policy

D. class map

Answer: B

Explanation:

The correct configuration for limiting Internet bandwidth for each guest client on a Cisco Catalyst 9800 WLC is through a

policy map. A policy map allows the creation of policies that can manage traffic within a network. By setting a bandwidth limit within the policy map, the WLC can enforce the required QoS for guest clients. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 180

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:

To rename access points and add them to the correct AP groups on a wireless controller, the minimum custom attributes required using Cisco ISE TACACS is role1=WIRELESS. This role provides the necessary permissions for read/write access to wireless-related configurations. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 181

An engineer set up a VoWLAN with QoS on the WLC and a class map on the switch, but the markings are not being preserved correctly in the end-to- end traffic flow. Which two configurations on the wired network ensure end-to-end QoS? (Choose two.)

A. trust boundaries

B. access lists

C. policy maps

D. QoS licenses

E. NetFlow

Answer: A, C

Explanation:

To ensure end-to-end QoS and preserve markings correctly in the VoWLAN setup, the configurations needed on the wired network are trust boundaries and policy maps. Trust boundaries define where the network trusts the QoS markings on packets, and policy maps are used to enforce QoS policies on the network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 182

An engineer is in the process of implementing Fastlane on a wireless network with a Mobility Express AP installed. The network must support voice and video applications for Apple devices. Due to a security concern, all iPhones are updated to version 14.5.432302546. Which QoS profile must the engineer configure on the user WLAN?

A. Bronze

B. Best Effort

C. Silver

D. Platinum

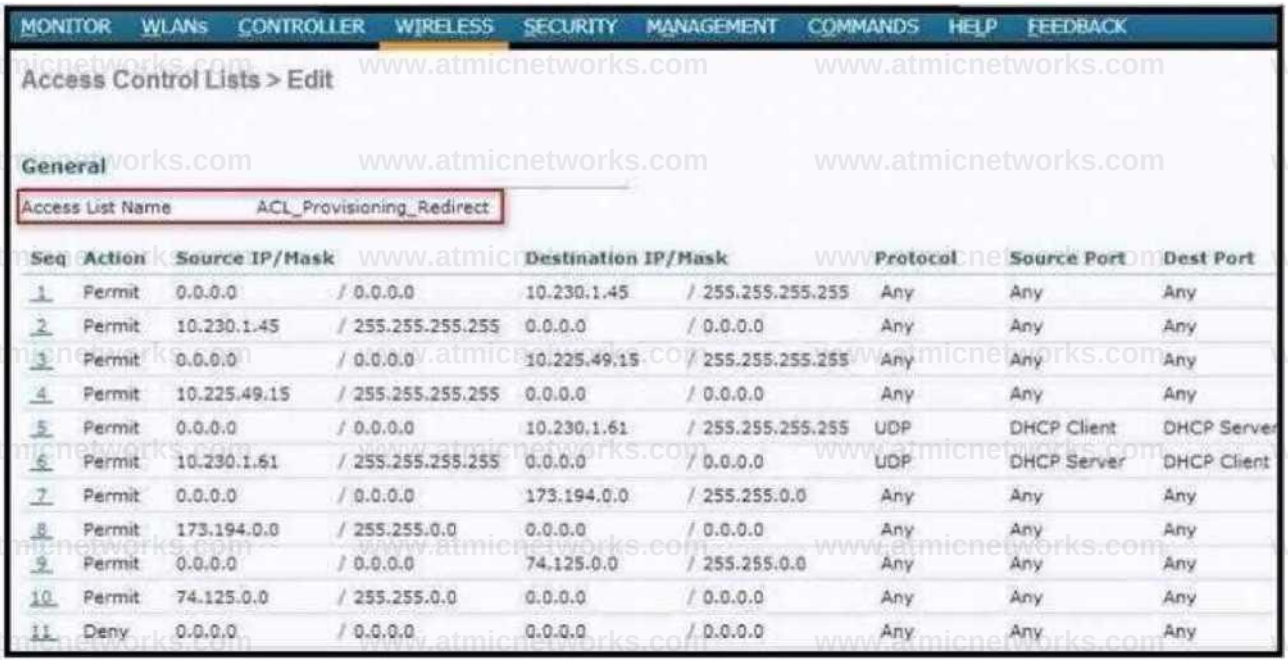
Answer: D

Explanation:

For a wireless network supporting voice and video applications for Apple devices, especially with Fastlane implementation, the QoS profile to configure on the user WLAN for iPhones updated to version 14.5.432302546 is Platinum. This profile provides the highest level of QoS, ensuring priority for voice and video traffic. Reference:= (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 183

Refer to the exhibit.



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Access Control Lists > Edit

General

Access List Name ACL_Provisioning_Redirect

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.45	/ 255.255.255.255	Any	Any	Any
2	Permit	10.230.1.45	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
3	Permit	0.0.0.0	/ 0.0.0.0	10.225.49.15	/ 255.255.255.255	Any	Any	Any
4	Permit	10.225.49.15	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	Any	Any	Any
5	Permit	0.0.0.0	/ 0.0.0.0	10.230.1.61	/ 255.255.255.255	UDP	DHCP Client	DHCP Server
6	Permit	10.230.1.61	/ 255.255.255.255	0.0.0.0	/ 0.0.0.0	UDP	DHCP Server	DHCP Client
7	Permit	0.0.0.0	/ 0.0.0.0	173.194.0.0	/ 255.255.0.0	Any	Any	Any
8	Permit	173.194.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
9	Permit	0.0.0.0	/ 0.0.0.0	74.125.0.0	/ 255.255.0.0	Any	Any	Any
10	Permit	74.125.0.0	/ 255.255.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any
11	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any

An ACL is configured to restrict access for BYOD clients. The ACL must redirect devices to the guest portal. To which two devices on the local network must the ACL allow access other than the DHCP server? (Choose two.)

A. RADIUS server

B. DNS server

C. Cisco ISE

D. SNMP server

E. WLC

Answer: A, C

Explanation:

An ACL configured for BYOD clients to redirect to a guest portal must allow access to the RADIUS server and Cisco ISE. The RADIUS server is crucial for authentication services, a core component of network access control for BYOD. Cisco ISE integrates with the network infrastructure to provide comprehensive security, including guest access management, thus its accessibility is essential for the redirection process to function correctly. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 184

A wireless administrator receives this information to complete a CMX deployment in high availability by using version 10.6 to gather analytics.

IP address of the primary server

IP address of the secondary server

failover mode to be configured as automatic

root password of the secondary server

email ID for NOC notifications

Enabling high availability fails when these parameters are used. Which action resolves the issue?

A. Insert the cmxadmin password of the secondary server.

B. Use IP protocol 4242 for the controller to reach the CMX server.

C. Place primary and secondary servers in different subnets.

D. Enable the virtual IP address of the primary server.

Answer: D

Explanation:

For CMX high availability deployment, enabling the virtual IP address of the primary server is critical. This virtual IP facilitates seamless failover to the secondary server without requiring DNS updates or manual intervention, ensuring uninterrupted service during primary server outages. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425

and Implementation ENWLSI 300-430 Official Cert Guide)

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-6/cmx_config/b_cg_cmx106/managing_cisco_cmx_system_settings.html#task_35253AFE18234DDA8C6E04C297D725F5:~:text=Primary%20and%20Secondary.-,Enabling%20High%20Availability%20for%20Cisco%20CMX%20Using%20the%20Web%20UI,-

Procedure

Question: 185

Which role does an engineer configure for administrative access to the wireless infrastructure, using Cisco ISE, to allow configuration of the WLC syslog configuration?

A. MANAGEMENT

B. SECURITY

C. CONTROLLER

D. WIRELESS

Answer: A

Explanation:

The MANAGEMENT role should be configured for administrative access to the wireless infrastructure using Cisco ISE. This role allows the configuration of WLC syslog settings, among other management tasks, ensuring proper logging and monitoring of the wireless network. Reference := (CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide)

Question: 186

Refer to the exhibit.

```
•radiusTransportThread: May 20 13:04:02.658: AuthorizationResponse: 0xl489ad70
•radiusTransportThread: May 20 13:04:02.658: structuresize..............577
•radiusTransportThread: May 20 13:04:02.658: resultcode.................0
•radiusTransportThread: May 20 13:04:02.658: protocolUsed.......... ......  0x00000001
•radiusTransportThread: May 20 13:04:02.658: proxystate.............  00:0b:0a:0c:Od:0e-02:06
•radiusTransportThread: May 20 13:04:02.658:        Packet contains 9 AVPs:
•radiusTranspor tThread: May 20 13:04:02.658:       AVP[01] User- Name. ...-Oser 1 (11 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[02]
State.....................................ReauthSession:c0a80a0600000003573f5190 (38 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[03]
Class..........................CACS:c0a80a0600000003573f5190:ISE01/253088040/17 (50 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[04] EAP-
Message..............................   0x038a0004   (59375620) (4 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[05] Message
Authenticator..................... DATA (16 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[06] Cisco / Url-
Redirect..................... DATA (133 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[07] Cisco / Uri-Redirect-
Acl.............. BLACKHOLE (9 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[08) Microsoft / MPPE-Send-
Key.............. DATA (32 bytes)
•radiusTransportThread: May 20 13:04:02.658:        AVP[09] Microsoft / MPPE-Recv-
Key   ............ .  -DATA (32 bytes)
•Dotlx_NW_Msgrask_2: May 20 13:04:02.658: 00:0b:0a:0c:Od:Oe Applying new AAA override for station
00:0b:Oa:0c:Od:Oe
*Dotlx_NW_MsgTask_2: May 20 13:04:02.658: 00 : 0b: 0a : 0c: Od: Oe Override values for station
94:bl:0a:c2:3a:4a source: 4, valid bits: 0x0 qosLevel: -1, dscp: Oxffffffff, dotlpTag: Oxffffffff,
sessionTimeout: -1
•Dotlx_NW_MsgTask_2: May 20 13:04:02.658: 00:0b:0a:0c:Od:Oe Override values (cont..) dataAvgC: -1,
rTAvgC: -1, dataBurstC: —1, rTimeBurstC: -1
          vlanlfName: '', vlanld:0, aclName: ', ipv6AclName: , avcProfileName: '
```

An engineer is troubleshooting a client connectivity issue. The client is in the RUN state, and no traffic is passed after authenticating by using Cisco ISE. Which action resolves the problem?

A. Configure a different client VLAN after authentication.

B. Disable the ACL that prevents traffic from being allowed.

C. Apply a lower WMM QoS.

D. Enable rate-limiting to the client.

Answer: B

Explanation:

When a client is authenticated but cannot pass traffic in the RUN state, it indicates that an ACL may be blocking the traffic post-authentication. Disabling or modifying this ACL to allow traffic can resolve the connectivity issue, ensuring that the client's traffic flows correctly after authentication with Cisco ISE.

Question: 187

An engineer is deploying a virtual MSE. The network has 3000 APs and needs 7000 IPS licenses.

To which size server does the engineer scale it?

A. virtual

B. standard

C. high end

D. low end

Answer: C

Explanation:

For a network with 3000 APs and 7000 IPS licenses, scaling to a high-end server is appropriate. This will provide the necessary resources and capabilities to support the large number of APs and the extensive licensing requirements for the Intrusion Prevention System.

Question: 188

The marketing department creates a promotion video for the branch store. Only interested hosts must receive the video over wireless multicast. What allows this feature?

A. TPC

B. DCA

C. WMM

D. WMF

Answer: D

Explanation:

Wireless Multicast Forwarding (WMF) is the feature that allows the delivery of multicast content, such as a promotional video, to only interested hosts over a wireless network. It optimizes the use of network resources by ensuring that only the hosts that have expressed interest in the multicast group receive the data.

Question: 189

The security learn is concerned about the access to all network devices, including the Cisco WLC. To permit only the admin subnet to have access to management, a CPU ACL is created and applied. However, guest users cannot get to the web portal. What must be configured to permit only admins to have access?

A. The guest portal must be configured on the CPU ACLs on the Cisco WLC.

B. Access to Cisco ISE must be allowed on the pre authentication ACL.

C. Management traffic from the guest network must be configured on the ACL rules. D. Traffic toward the virtual interface must be permitted.

Answer:B

To ensure that only admins have access to network device management while allowing guest users to reach the web portal, access to Cisco ISE must be permitted on the pre-authentication ACL. This configuration allows guests to interact with the portal without granting them broader network access.

Question: 190

A customer is deploying local web authentication. Which software application must be implemented on Cisco ISE to utilize as a directory service?

A. Solaris Directory Service

B. LDAP

C. SAML

D. Novell eDirectory

Answer: B

Explanation:

LDAP (Lightweight Directory Access Protocol) is a protocol used for accessing and maintaining distributed directory information services over an IP network. In the context of Cisco ISE (Identity Services Engine), LDAP can be utilized as a directory service to authenticate and authorize users during local web authentication processes. LDAP supports a wide range of directory services, including Microsoft Active Directory, which is commonly used in enterprise environments.

Question: 191

An engineer must achieve the highest level of location accuracy possible for a new mobile application. Which technology must be implemented for this use case?

A. Time Difference of Arrival

B. Bluetooth Low Energy

C. RSS lateration

D. ToA lateration

Answer: B

Explanation:

Bluetooth Low Energy (BLE) is renowned for its ability to provide precise location services, especially in the context of indoor positioning systems. BLE beacons can be strategically placed throughout a facility, and when used in conjunction with a mobile application, they can deliver the high level of location accuracy required for various use cases, including navigation, asset tracking, and contextual marketing.

Question: 192

Which two configurations are applied on the WLC to enable multicast, check multicast stream subscriptions, and stream content only to subscribed clients? (Choose two)

A. Enable IGMP snooping

B. Set the IGMP timeout to 180 seconds

C. Enable broadcast forwarding

D. Enable 802.3x flow control mode.

E. Set the AP multicast to 238.255.255.255

Answer: A, E

Explanation:

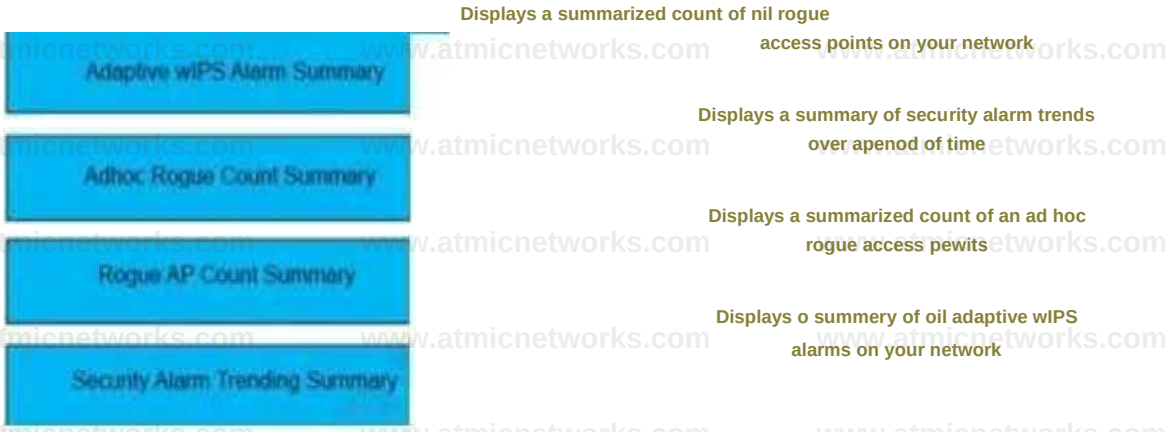
IGMP snooping is a feature that allows a network switch to listen to the Internet Group Management Protocol (IGMP) network traffic. This feature enables the switch to identify the multicast streams to which hosts are interested and to forward multicast traffic intelligently. By enabling IGMP snooping on the Wireless LAN Controller (WLC), it ensures that multicast streams are only forwarded to the access points (APs) where clients are subscribed to them. Setting the AP multicast mode to a specific multicast address, such as 238.255.255.255, allows the WLC to send

multicast traffic to APs using this address, which helps in efficient distribution of the multicast stream.

Question: 193

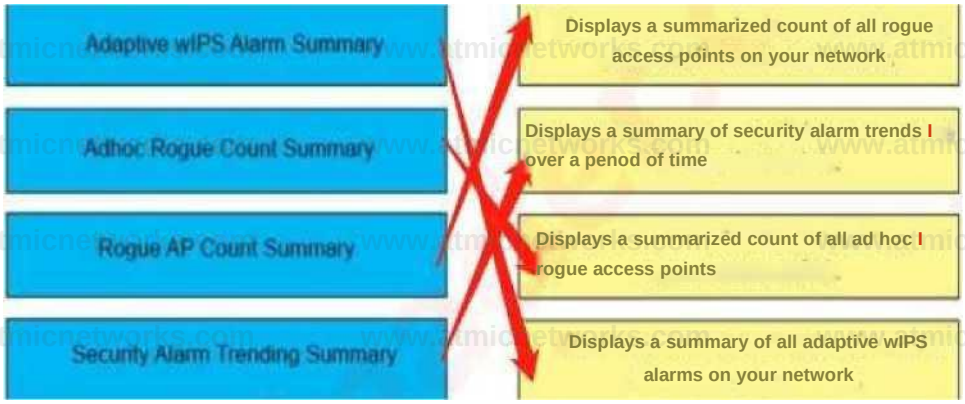
DRAG DROP

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:

Explanation:



Question: 194

Which condition introduce security risk to a BYOD policy?

A. enterprise-managed MDM platform used for personal devices

B. access to LAN without implementing MDM solution

C. enforcement of BYOD access to internet only network

D. enterprise life-cycle enforcement of personal device refresh

Answer: B

Explanation:

Allowing access to the Local Area Network (LAN) without implementing a Mobile Device Management (MDM) solution poses a significant security risk to a Bring Your Own Device (BYOD) policy. Without MDM, the organization lacks control over the personal devices that connect to its network, which could lead to unauthorized access to sensitive data, potential data breaches, and the inability to enforce security policies.

Question: 195

An engineer has configured the wireless controller to authenticate clients on the employee SSID against Microsoft Active Directory using PEAP authentication.

Which protocol does the controller use to communicate with the authentication server?

A. EAP

B. 802.1X

C. RADIUS

D. WPA2

Answer: C

Explanation:

When a wireless controller is configured to authenticate clients against Microsoft Active Directory using PEAP (Protected Extensible Authentication Protocol), it uses RADIUS (Remote Authentication Dial-In User Service) as the protocol to communicate with the authentication server. RADIUS is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service.

Question: 196

An engineer is setting up a new unique NAD on a Cisco ISE.

Which two parameters must be configured? (Choose two.)

A. device host name
B. device password
C. RADIUS fallback
D. device IP address
E. RADIUS shared secret

Answer: E, D

Explanation:

When setting up a new Network Access Device (NAD) on Cisco ISE, it is essential to configure the device's IP address and the RADIUS shared secret. The device IP address is used to identify the NAD within the network, and the RADIUS shared secret is a password used between the ISE and the NAD to ensure secure communication.

Question: 197

An engineer is considering an MDM integration with Cisco ISE to assist with security for lost devices.

Which two functions of MDM increase security for lost devices that access data from the network? (Choose two.)

A. PIN enforcement

B. Jailbreak/root detection

C. data wipe

D. data encryption

E. data loss prevention

Answer: B, C

Explanation:

Mobile Device Management (MDM) integration with Cisco ISE increases security for lost devices by providing functions such as data wipe and jailbreak/root detection. Data wipe allows the remote erasure of sensitive information from lost devices, preventing unauthorized access. Jailbreak/root detection helps identify compromised devices that may bypass standard security measures, ensuring that they do not access network resources.

Question: 198

Which EAP method can an AP use to authenticate to the wired network?

A. EAP-GTC

B. EAP-MD5

C. EAP-TLS

D. EAP-FAST

Answer: C

Explanation:

EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is an EAP method that an Access Point (AP) can use to authenticate to the wired network. EAP-TLS is considered one of the most secure EAP methods because it uses mutual authentication, where both the client and the server authenticate each other using certificates.

Question: 199

A wireless engineer has performed a Wireshark ccapture on an 802.1x authentication process to troubleshoot a connectivity issue.

Which two types of packet does the EAP contain? (Choose two.)

A. EAP complete

B. EAP response

C. EAP failure

D. EAP request

E. EAP reply

Answer: B, D

Explanation:

The Extensible Authentication Protocol (EAP) is an authentication framework frequently used in wireless networks and Point-to-Point connections. During the EAP authentication process, EAP Request and EAP Response packets are exchanged between the supplicant (client device) and the authenticator (network). These packets are used to transport messages for the authentication process. An EAP Request packet is sent by the authenticator requesting identity information from the supplicant, while an EAP Response packet is sent by the supplicant in reply to the request. The other options, such as EAP complete, EAP failure, and EAP reply, are not standard EAP packet types. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 200

You enter the command or a Cisco Catalyst 3850 Series Switch that runs Cisco ISO XE. What does the command do?

A. It defines the user identity or the device identity to be validated by the RADIUS server.

B. It captures information on the length of the authorized session, as well as the bandwidth usage of the client.

C. It defines the RADIUS server used to track which sessions are still active.

D. It defines the level of access of the user or the device.

Answer: C

Explanation:

The command in question is typically used to configure the switch to interact with a RADIUS server for session tracking purposes. The RADIUS server keeps track of authenticated sessions, ensuring that they are still active and monitoring for any changes in status. This is crucial for maintaining network security and ensuring that only authorized users have access to network resources.

Question: 201

Which CLI command do you use to shut down the 2.4 GHz radio of the Floor1_AP1 AP on a Cisco 3850 Switch?

A. ap name Floor1_AP1 dot11 shutdown 24ghz

B. ap name Floor1_AP1 dot11 5ghz shutdown

C. ap name Floor1 AP1 dot11 24ghz shutdown

D. ap name Floor1_AP1 shutdown dot11 24ghz

Answer: C

Explanation:

The correct command to shut down the 2.4 GHz radio on a specific AP on a Cisco 3850 switch is ap name Floor1_AP1 dot11 24ghz shutdown. This command specifies the AP by name (Floor1_AP1), the radio frequency band (dot11 24ghz), and the action to be taken (shutdown). The other commands listed either reference the wrong frequency band, use incorrect syntax, or are not valid Cisco IOS commands for managing AP radios. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 202

You plan to implement Cisco Identity Based Networking Services on a Cisco Catalyst 3850 Series Switch. Which switch command is required when configuring downloadable ACLs?

A. authentication display new-style

B. ip device tracking

C. dot1x system-auth-control

D. aaa session-id common

Answer:D

The 'aaa session-id common' command is essential when implementing Cisco Identity Based Networking Services (IBNS) with downloadable ACLs on a Cisco Catalyst 3850 Series Switch. This command configures the switch to use a common session identifier for all AAA (Authentication, Authorization, and Accounting)

transactions. This is important for downloadable ACLs because it ensures that the correct policies are applied consistently across different sessions and services.

Question: 203

An administrator receives reports of many interferers in the wireless network and wants to get the location of these interferers from the maps in Cisco Prime Infrastructure.

When looking at the floor plans/maps, the administrator does not see any interferers, but can see all wireless clients located successfully.

Which two statements define the cause of the issue? (Choose two.)

A. MSE is not added to Cisco Prime infrastructure and synchronized.

B. Interferer tracking is not enabled on the MSE.

C. SNMP between Cisco Prime Infrastructure and the WLC is failing.

D. Context Aware Service tracking limit has already been reached with tracking other elements.

E. NSMP communication is inactive with the WLC.

Answer:A,B

If the administrator is unable to see interferers on the Cisco Prime Infrastructure maps, it could be due to the MSE (Mobility Services Engine) not being added and synchronized with Cisco Prime Infrastructure, which is essential for tracking and locating devices, including interferers. Additionally, if interferer tracking is not enabled on the MSE, it would not track or display the location of interferers on the maps. The other options, such as SNMP failure, reaching the Context Aware Service tracking limit, or inactive NSMP communication, would affect other aspects of network visibility but not specifically the tracking and display of interferers. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 204

An engineer is adding APs to an existing VolMLAN to allow for location based services. Which option will the primary change be to the network?

A. increased transmit power on all APs

B. moving to a bridging model

C. AP footprint

D. cell overlap would decrease

E. triangulation of devices

Answer: C

Explanation:

The primary change to the network when adding APs for location-based services, such as VolMLAN, would be the AP footprint. This refers to the physical coverage area of the access points. Increasing the AP footprint enhances the ability to perform location-based services by improving the accuracy of triangulation and location tracking of devices. This is because a denser AP footprint allows for more precise determination of a device's location within the network. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, specifically the sections discussing location-based services and AP deployment strategies for optimal coverage and location tracking.

Question: 205

A network engineer is configuring a Cisco AireOS WLC environment for central web authentication using Cisco ISE.

The controllers are configured using auto-anchor for the guest network.

Which three components must be implemented for the foreign WLC?(Choose three.)

A. DHCP RADIUS profiling enabled.

B. HTTP RADIUS profiling enabled.

C. UDP/1812-1813 open to ISE

D. downloadable preauth ACL on ISE

E. local preauth ACL on WLC

F. WLAN Layer 2 security

Answer: C, D, E

Explanation:

For central web authentication with Cisco ISE in a Cisco AireOS WLC environment using auto-anchor for the guest network, the foreign WLC must have UDP ports 1812 and 1813 open to ISE for RADIUS authentication and accounting. Additionally, a downloadable preauth ACL on ISE is required to define the permissions for the guest user before authentication, and a local preauth ACL on the WLC is needed to restrict or allow traffic prior to authentication. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, particularly the chapters on WLC configuration for guest access and integration with Cisco ISE for security and access control.

Question: 206

An engineer is troubleshooting rogue access points that are showing up in Cisco Prime Infrastructure.

What is maximum number of APS the engineer can use to contain an identified rogue access point in the WLC?

A. 3

B. 4

C. 6

D. 5

Answer: B

Explanation:

In Cisco Prime Infrastructure, the maximum number of APs that can be used to contain an identified rogue access point in the WLC is four (4). This containment process involves using nearby APs to disrupt the rogue AP's signals, thereby preventing it from effectively communicating with client devices. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide, which includes information on rogue AP detection and containment strategies within the WLC and Cisco Prime Infrastructure.

Question: 207

A company is deploying wireless PCs on forklifts within its new 10,000-square-foot(3048-square- rneter) facility.

The clients are configured for PEAP-MS-CHAPv2 with WPA TKIP. Users report that applications frequently drop when the clients roam between access points on the floor. A professional site survey was completed.

Which configuration change is recommended to improve the speed of client roaming?

A. EAP-FAST

B. EAP-TLS

C. WPAAES

D. WPA2AES

Answer: D

Explanation:

To improve the speed of client roaming in a wireless network, especially in scenarios where applications are dropping during roams between access points, it is recommended to switch to WPA2 with AES encryption. WPA2AES provides a more robust and efficient encryption method, which can facilitate faster and more secure client handoffs between APs. This change can help mitigate issues with application drops during roaming. Reference: CCNP Enterprise Wireless Design ENWLSD 300425 and Implementation ENWLSI 300-430 Official Cert Guide, focusing on client roaming optimization and security protocols for wireless networks.

Question: 208

An engineer has configured passive fallback mode for RADIUS with default timer settings. What will occur when the primary RADIUS fails then recovers?

A. RADIUS requests will be sent to the secondary RADIUS server until the secondary fails to respond.

B. The controller will immediately revert back after it receives a RADIUS probe from the primary server.

C. After the inactive time expires the controller will send RADIUS to the primary.

D. Once RADIUS probe messages determine the primary controller is active the controller will revert back to the primary RADIUS.

Answer:C

In passive fallback mode for RADIUS, when the primary RADIUS server fails, the controller will start using the secondary RADIUS server. The default timer settings include an inactive timer, which, upon expiration, prompts the controller to attempt to send RADIUS requests back to the primary server. If the primary server is responsive, the controller will resume sending requests to it. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 209

You are configuring the social login for a guest network. Which three options are configurable social connectors in Cisco CMX Visitor Connect? (Chose three)

A. Linkedn

B. Pinterest

C. Medium

D. Google+

E. Facebook

F. Myspace

Answer: A, D, E

Explanation:

Cisco CMX Visitor Connect supports various social connectors for guest network login. The configurable social connectors include LinkedIn, Google+, and Facebook, but not Pinterest, Medium, or Myspace. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 210

What two actions must be taken by an engineer configuring wireless Identity-Based Networking for a WLAN to enable VLAN tagging? (Choose two.)

A. enable AAA override on the WLAN

B. create and apply the appropriate ACL to the WLAN

C. update the RADIUS server attributes for tunnel type 64, medium type 65, and tunnel private group type 81

D. configure RADIUS server with WLAN subnet and VLAN ID E. enable VLAN Select on the wireless LAN controller and the WLAN

Answer: A, C

Explanation:

To enable VLAN tagging for wireless Identity-Based Networking on a WLAN, an engineer must enable AAA override, which allows for dynamic VLAN assignment. Additionally, the RADIUS server attributes need to be updated to include tunnel type 64, medium type 65, and tunnel private group type 81, which are necessary for VLAN tagging information. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 211

An engineer is designing a high availability wireless network. What mechanism should be the focus for high availability?

A. SNR

B. channel reuse

C. RSSI

D. cell overlap

Answer: D

Explanation:

When designing a high availability wireless network, the focus should be on cell overlap. Adequate cell overlap ensures that if one access point fails, another can provide coverage without service interruption, thus maintaining network resilience and availability. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 212

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. identify service engine

D. Prime Infrastructure

Answer: C

Explanation:

In a BYOD (Bring Your Own Device) deployment strategy that prefers a single SSID model, an Identity Services Engine (ISE) is required. Cisco's ISE is a security policy management platform that automates and enforces context-aware security access to network resources. It allows for the creation of policies that control access to the network based on user identity, device type, device health, and posture compliance, which is essential for a BYOD environment. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 213

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:

The impact of BYOD that should be considered is the potential for increased phishing attacks. BYOD can lead to a greater variety of devices accessing the network, which may not all have the same level of security. This can increase the risk of phishing attacks as attackers may target personal devices that are used to access corporate resources, which might not be as secure as company-owned devices. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 214

A network engineer is implementing a wireless network and is considering deploying a single SSID for device onboarding.

Which option is a benefit of using dual SSIDs with a captive portal on the onboard SSID compared to a single SSID solution?

A. limit of a single device per user

B. restrict allowed devices types

C. allow multiple devices per user

D. minimize client configuration errors

Answer:B

The benefit of using dual SSIDs with a captive portal on the onboard SSID compared to a single SSID solution is the ability to restrict allowed device types. With a dual SSID setup, one SSID can be used for onboarding new devices with a captive portal that can enforce policies and check the device type before allowing access to the main SSID. This helps in maintaining a secure and compliant network environment. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 215

An engineer must perform a Layer 2 survey for a mining facility. Which type of antenna does the engineer use in the mine shaft?

A. dipole

B. omnidirectional

C. patch

D. internal

Answer: C

Explanation:

For a Layer 2 survey in a mining facility, particularly in a mine shaft, a patch antenna is the most suitable choice. Patch antennas are directional and can be used to focus the signal in a specific direction, which is ideal for the long and narrow structure of a mine shaft. This type of antenna can help in providing better coverage and signal strength in challenging environments like mines. Reference: CCNP Enterprise Wireless Design ENWLSD 300-425 and Implementation ENWLSI 300-430 Official Cert Guide

Question: 216

An engineer has many different WLANs on a WLC but does not want to broadcast them to every AP in the building. Which group must be configured on the WLC to allow different WLANs on the different APs without creating new interfaces?

A. ACL

B. interface group

C. mobility group

D. AP group

Answer: D

Explanation:

In a Cisco Wireless LAN Controller (WLC), AP groups are used to manage the distribution of WLANs to different access points (APs). By configuring AP groups, an engineer can specify which WLANs are broadcasted by which APs. This allows for the creation of multiple WLANs across different APs without the need to create new interfaces for each WLAN. AP groups provide the flexibility to control WLAN availability based on location or other criteria, ensuring that only the intended WLANs are available through specific APs.

Question: 217

A university implemented a Cisco Catalyst Center (formerly DNA Center) solution to help its network administrator resolve Wi-Fi issues that are raised by students. A client dashboard must be used to view, monitor, and troubleshoot the captured data packets. Which feature must be used?

A. Intelligent Capture

B. Packet Sniffer

C. Packet Capture

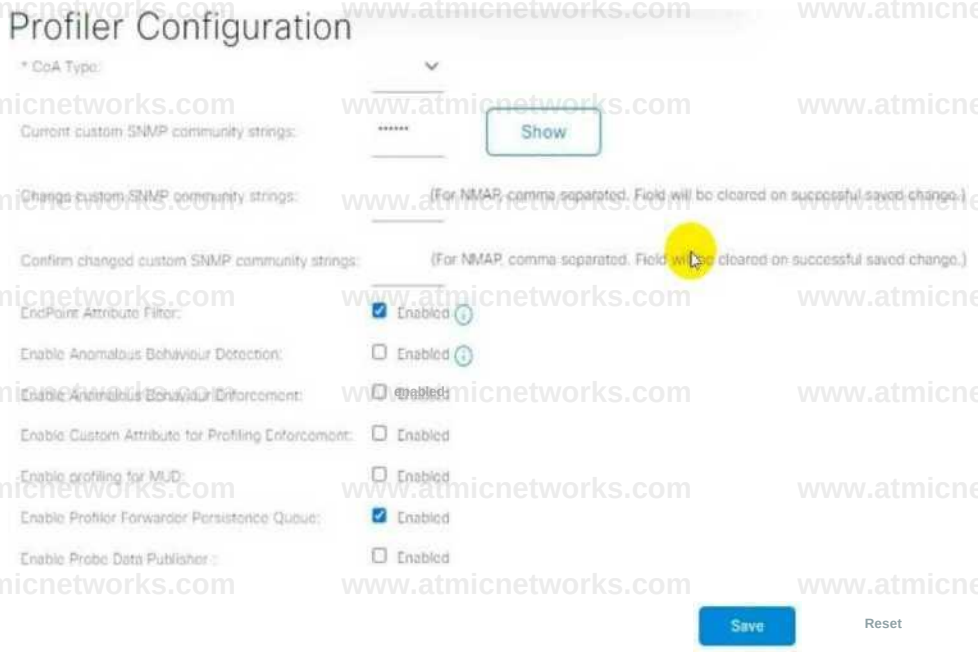
D. Cisco CleanAir

Answer: C

Explanation:

Question: 218

Refer to the exhibit.



Refer to the exhibit. A network administrator must migrate a Cisco Catalyst 9800 WLC from local client profiling to RADIUS profiling through Cisco ISE. The engineer must enable RADIUS CoA based on detecting the client type as Windows to update the access policy based on profile detection immediately. Which CoA type configuration must the engineer apply on Cisco ISE?

A. no CoA

B. reauth

C. port

D. bounce

E. preauth

Answer: B

Explanation:

Question: 219

An engineer is configuring location services within Cisco Spaces (formerly Cisco DNA Spaces). The solution must track interfering devices. Which component of Cisco Spaces must be configured?

A. Proximity Reporting

B. Detect and Locate

C. Cisco DNA Spaces SDK

D. Location Analytics

Answer: B

Explanation:

Question: 220

An engineer has configured Cisco Centralized Key Management for an enterprise that has remote branches. The remote offices are connected back to the data center using a VPN connection with low-bandwidth connections. The goal is to improve roaming. Which type of group must be configured?

A. RF

B. Cisco FlexConnect

C. interlace

D. AP

Answer: B

Explanation:

Question: 221

During discovery, one out of five fabric-enabled WLAN controllers is not being properly discovered The firewall rules are the same for all the controllers Which element is missing?

A. NETCONF

B. SNMP trap

C. YANG

D. SNMP management

Answer: A

Explanation:

Question: 222

A customer configures iPSK for use with a Cisco Catalyst 9800 Series controller. The configuration is complete, but the wireless client fails to authenticate to the network. Which implementation resolves this issue?

A. Enable iPSK on the WLAN.

B. Configure the DHCP Required option on the policy profile.

C. Configure an accounting list on the policy profile.

D. Enable the AAA Override option on the policy profile.

Answer: D

Explanation:

Question: 223

A healthcare organization is using Cisco Catalyst Center integrated with Cisco Spaces to track the movement of medical devices in real time. The IT team notices that location accuracy is significantly reduced in areas where medical trolleys are frequently moved. A site survey revealed that with the trolley in the environment, an insufficient number of APs can detect the client device. The APs are deployed following standard ceiling-mounted guidelines. The IT team already ruled out interference from non-Wi-Fi devices and configured proper RF profiles. Which action must the IT team take to resolve the issue?

A. Lower APs in the affected areas to reduce obstructions and improve the signal path for accurate triangulation

B. Enable spectrum analysis to detect non-Wi-Fi device interference and automatically adjust AP channels.

C. Implement location-based FastLocate features on Cisco Spaces to bypass the need for signal triangulation.

D. Increase the transmit power of all APs in the hospital to compensate for signal interference.

Answer: A

Explanation:

Question: 224

The marketing department in a retail company has created a promotional video for the opening of a new branch store shp-GA4B6C828354AB. The video must be received by interested its only, over wireless multicast What allows this feature?

A. TPC

B. WMF

C. WMM

D. DCA

Answer: B

Explanation:

Question: 225

A university campus uses Cisco Catalyst Center and Cisco Spaces to provide indoor wayfinding for students and guests by leveraging the university mobile app. IT administrators notice that location tracking is

inaccurate in multistory buildings, especially near staircases and elevators. Upon investigation, they find that overlapping signals from APs on different floors are causing triangulation errors. The IT team already ensured that APs are not placed directly above or below each other. However, the problem persists, and location accuracy remains unreliable near vertical structures. Which action must the IT team take to resolve the issue?

A. Increase the maximum allowable client connections per AP to compensate for signal overlap in high-traffic areas.

B. Enable coverage hole detection and mitigation to address areas with inconsistent signal strength near staircases and elevators.

C. Adjust AP transmit power and orientation to minimize vertical signal propagation between floors and optimize coverage for horizontal triangulation

D. Configure all the APs in the building to use the same channel to provide consistent signal coverage across floors.

Answer: C

Explanation:

Question: 226

Refer to the exhibit. A network administrator must use the webhook feature in Cisco DNA Catalyst Center to receive notifications for multiple events related to the AP - Usage and Client Breakdown report. The external service handling these notifications is located at the callback URL https://example.com/webhook and has the requirements:

•An API key is passed in the X-API-Key header with the value xyz789.
•The payload must be in JSON format, specified in the Content-Type header.
•The callback URL must include a query parameter event_type to indicate the type of notification •A custom header X-Source with the value CiscoDNAC to identify the notification source.

Which code snippet must be placed onto the box in the code to complete the Python script that configures the webhook?

```
"method": "POST",
"headers": {
    "Content-Type": "application/json",,
    "X-API-Key": "xyz789",
    "X-Source": "CiscoDNAC"
```

```
"method": "PUT",
"headers": {
    "Content-Type": "json",
    "X-API-Key": "CiscoDNAC",
    "X-Source": "xyz789"
```

```
"method": "POST",
"headers": {
    "Content-Type": "json",
    "X-API-Key": "xyz789",
    "X-Source": "CiscoDNAC"
```

```
"method": "PUT",
"headers": {
    "Content-Type": "application/json",
    "X-API-Key": "xyz789",
    "X-Source": "CiscoDNAC"
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Question: 227

Refer to the exhibit.

```
policy-map BW_Limit
 class BW_Limit1_AVC_UI_CLASS
  police cir 8000
   conform-action drop
   exceed-action drop
 class BW_Limit1_ADV_UI_CLASS
  set dscp af41
 class BW_Limit2_ADV_UI_CLASS
  police cir 50000
   conform-action transmit
   exceed-action drop
 class class-default
  police cir 100000
   conform-action transmit
   exceed-action drop
```

Refer to the exhibit. A university network administrator notices that wireless guest users consume a significant amount of uplink internet bzjjlwidth in the library, which causes throughput issues on staff SSID. To throttle this bandwidth use, the administrator intends to configure a QoS policy for guests that:

- remarks DSCP 46 to 34
- drops Netflix and YouTube traffic
- rate limits a host specified in an ACL to 50 Kbps
- rate limits all other traffic to 100 Kbps

Which class-map configuration must the administrator implement?

class-map match-all BW_Limit1_AVC_UI_CLASS match protocol

youtube match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS match dscp af41
class-map match-all BW_Limit1_ADV_UI_CLASS match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS match protocol youtube match protocol netflix
class-map match-any BW_Limlt1_ADV_UI_CLASS match dscp af41
class-map match-all BW_Limit2_ADV_UI_CLASS match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS match protocol youtube match protocol netflix
class-map match-any BW_Llmit1_ADV_UI_CLASS match dscp af34
class-map match-all BW_Limit2_ADV_UI_CLASS match access-group name specifichostACL

class-map match-all BW_Limit1_AVC_UI_CLASS match protocol youtube match protocol netflix
class-map match-any BW_Limit1_ADV_UI_CLASS match dscp ef
class-map match-all BW_Llmit2_ADV_UI_CLASS match access-group name specifichostACL

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Question: 228

Refer to the exhibit.

```
from ncclient import manager

wlc = manager.connect(
     host="192.168.1.10",
     port-830,
     username="admin",
     password="Clscol23", hostkey_verify=False )

<config>
  <native x.mins="http: / /cisco. com/ns/yang/Cis co-IOS-XE-native" > <tacacs>
      <server>
        <name>TACACS-Server</name>
        <address>
          <ipv4>192.168.1.100</ipv4>
        </address>
        <key>Ciscol23</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>
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

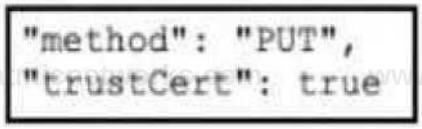
Explanation:

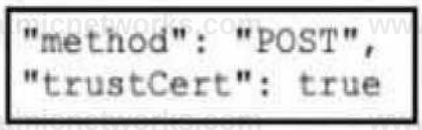
Question: 229

Refer to the exhibit.

```
import requests

url = "https://<ca talys t-cen te r-i p>/dna/intent/api/v1/event/webhook"

payload * {
      "name": "ReportWebhook",
      "url": "https://example.com/webhook",

|

headers = {
      "Content-Type": "application/json", "Authorization": "Bearer <token>"
|

response = requests.post(url, json=payload, headers=headers)
```

Refer to the exhibit. A network administrator must automate notifications for Security Advisories Data reports on the Cisco Catalyst Center v2.3.7 using the Report notification feature. Preferring a programmable approach over UI/CLI, the administrator decides to create a webhook via the Cisco DNA Center API to send real-time HTTP notifications to an external application. The webhook URL https://example.com/webhook uses HTTPS with a self-signed certificate, which requires a specific configuration in the payload to ensure the webhook functions correctly. Which code snippet must be placed onto the box in the code to complete the Python script that configures the webhook to use the self-signed certificate to extract the Security Advisories Data report?





A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Question: 230

A wireless controller has a RADIUS server configured globally. Another RADIUS server is mapped for WLAN A in this controller. Which RADIUS server does the controller use for authenticating clients from WLAN A?

A. RADIUS server that is globally configured

B. first the RADIUS server that is mapped for WLAN A, and if authentication fails, it reverts to the RADIUS server that is globally configured

C. RADIUS server that is mapped for WLAN A

D. first the RADIUS server that is globally configured, and if authentication fails, it reverts to the RADIUS server that is mapped for WLAN A

Answer: C

Explanation:

Question: 231

A consulting engineer must migrate the APs from a Cisco 8540 WLC to a Cisco Catalyst 9800-80 WLC. As part of the migration, the engineer is advised to use a policy map as part of the configuration on the Catalyst 9800-80 WLC to mirror the platinum QoS settings on voice WLAN to accommodate CP- 840 wireless phones. Which configuration must the engineer implement on the voice WLAN?

policy-map voice-policy class cm-dscp-34 set dscp af41 class cm-dscp-45 set dscp 45 class cm-dscp-46 set dscp ef class cm-dscp-47 set dscp 47

policy-map voice-policy class cm-dscp-45 set dscp af41 class cm-dscp-46 set dscp af41 class cm-dscp-47
set dscp af41

policy-map voice-policy class cm-dscp-34 set dscp default class cm-dscp-45 set dscp default class cm-dscp-46 set dscp default class cm-dscp-47 set dscp default

policy-map voice-policy class cm-dscp-0 set dscp cs1 class cm-dscp-34 set dscp cs1 class cm-dscp-45 set dscp cs1 class cm-dscp-46 set dscp cs1 class cm-dscp-47 set dscp cs1

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Question: 232

An engineer is attempting to implement a local MAC authorization list for the APs that are registered to your Cisco Catalyst 9800 Series Wireless Controller. The list of AP MAC addresses has been added, but the controller is not enforcing AP MAC authentication. Where is AP Authorization against MACs enabled?

A. Configuration > Wireless > AP Global Config

B. Configuration > Security > AAA > AAA Advanced > AP Policy

C. Configuration > Tags & Profiles > AP Join > default-ap-profile

D. Configuration > Security > AAA > Authentication > AAA Method List

Answer: D

Explanation:

Question: 233

An engineer implemented AP Authorization with Cisco ISE utilizing AP MAC addresses as local users in Cisco ISE. Everything has been working fine until recently. It has been noticed that APs that reboot are temporarily disconnected from the network and cannot rejoin the controller. Which action completes the implementation?

A. Remove APs from the exclusion list, due to authentication failures.

B. Disable the Cisco ISE password policy that disables accounts for unchanged passwords.

C. Install a valid EAP certificate on Cisco ISE for the APs.

D. Upgrade Cisco ISE to a newer version due to bugs.

Answer: B

Explanation:

Question: 234

A customer is deploying Cisco Catalyst Center (formerly DNA Center) to manage a Cisco Catalyst 9800 Series Wireless Controller Cisco CleanAir is used to address wireless interference Which two configurations must be completed from the Cisco Catalyst Center GUI to manage the interferes? (Choose two)

A. Enable Neighbor List Dual Band on the configured WLANs

B. Disable Persistent Device Propagation in the CleanAir configuration model

C. Configure the RX SOP threshold to be high

D. Enable CleanAir Device Reporting in the CleanAir configuration model

E. The CleanAir configuration model must be applied to a wireless network profile

Answer: D, E

Explanation:

Question: 235

A customer has Cisco FlexConnect APs in all remote branches and requires zero downtime with the FlexConnect Fault Tolerance feature. Which two configurations must be the same in both controllers to connected clients when the APs switch from primary to backup WLC due to WAN failure? (Choose two.)

A. interface configuration

B. virtual interface IP address

C. WLAN ordering

D. AAA server ordering

E. mobility domain

Answer: C, E

Explanation:

Question: 236

A wireless network has two RF groups where Cisco WLCs are joined. APs are associated with different controllers using the round-robin approach. Rogue containment must be deployed v\ all controllers, but the network must not be affected by any RRM neighbor packets sent by friendly APs. Which AP authentication protection type must be enabled?

A. AP Security

B. AP Authentication

C. AP Wireless Protection Rules

D. AP Access Control

Answer: C

Explanation:

Question: 237

A WLC must be configured to allow multiple mDNS profiles based on a user authentication profile configured in Cisco ISE. Which WLAN setting must be configured?

A. mDNS policy

B. mDNS Snooping

C. AAA Override

D. service advertisement

Answer: C

Explanation:

Question: 238

An engineer is working for an organization that recently deployed Cisco SD-Access-based network with all SSIDs working in Fabric-enabled wireless. A recent project requires third-party APs to be connected to the access switches for some interoperability testing. However, Cisco Catalyst Center (formerly DNA Center) detects these APs as rogue on the wire. Which action must the engineer take to avoid reporting third-party APs as high-threat rogue

and containing them?

A. Reduce the power on the third-party APs and create smaller broadcasting cells.

B. Upload the MAC addresses of the third-party APs to Cisco Catalyst Center using a wl PS workflow.

C. Remove specific switches from Cisco Catalyst Center management where third-party APs are connected.

D. Enable Management Frame Protection on the SSIDs broadcasted using third-party APs.

Answer: B

Explanation:

Question: 239

A customer must provide a secure wireless network from a Cisco Catalyst 9800 Series Wireless Controller to a Cisco AP to remote users The corporate WLAN must be provided over the Internet to specific locations and support a locally-installed IP phone Which two actions accomplish this configuration? (Choose two)

A. Configure NAT on the physical interface

B. Enable Local Switching under the WLAN

C. Create a Flex Group and add the AP

D. Enable Office Extend AP on the Flex Profile

E. Configure Remote LAN under the Remote LAN

Answer: DE

Explanation:

Question: 240

A network administrator for a corporation must create a guest SSID for a captive portal redirect powered by Cisco

Catalyst Center (formerly DNA Center). The network includes a Cisco Catalyst 9800-80 WLC, Cisco 9130AXI APs, and Cisco Spaces (formerly Cisco DNA Spaces) using a connector. To support guest client captive portal redirect, the administrator must create a security ACL and an intercept ACL. The ACL requirement is:

ACL WA-v4-int34.235.248.212 must be applied first on traffic coming from the client and keep HTTP(s) traffic toward Cisco DNA Spaces portal IP 34.235.248.212 on the data plane. No drop or forward action, just hand the traffic over to the data plane. Then send it to the CPU for redirection except for virtual IP traffic, which is serviced by the web server for all HTTP(s) traffic. Other types of traffic is given to the data plane.

ACL WA-sec-34.235.248.212 must permit HTTP and HTTPS traffic to the Cisco Spaces portal IP 34.235.248.212 that the administrator configured in the web authentication parameter map. DNS and DHCP traffic must be allowed, but drop the rest. HTTP traffic is intercepted before reaching this ACL and therefore does not need to be covered by this ACL.

Which configuration implements the ACL requirements?

ip access-list extended WA-sec-34.235.248.212 10 permit tcp any host 34.235.248.212 eq www 20 permit tcp any host 34.235.248.212 eq 443 30 permit tcp any any eq domain 40 permit udp any any eq domain 50 permit udp any any eq bootpc 60 permit udp any any eq bootps
70 deny Ip any any exit
ip access-list extended WA-v4-int-34.235.248.212 10 permit tcp any any eq www
20 permit tcp any host 192.0.2.1 eq 443 exit

Ip access-list extended WA-sec-34.235.248.212 10 permit tcp any host 34.235.248.212 eq www 20 permit tcp any host 34.235.248.212 eq 443 30 permit tcp host 34.235.248.212 eq www any 40 permit tcp host 34.235.248.212 eq 443 any 50 deny ip any any exit
Ip access-list extended WA-v4-Int-34.235.248.212 10 deny tcp any host 34.235.248.212 eq www 20 deny tcp any host 34.235.248.212 eq 443 30 permit tcp any host 192.0.2.1 eq 443 exit

O Ip access-list extended WA-sec-34.235.248.212 10 permit tcp any host 34.235.248.212 eq www 20 permit tcp any host 34.235.248.212 eq 443 30 permit tcp host 34.235.248.212 eq www any 40 permit tcp host 34.235.248,212 eq 443 any 50 permit tcp any any eq domain 60 permit udp any any eq domain 70 permit udp any any eq bootpc 80 permit udp any any eq bootps 90 deny ip any any exit
Ip access-list extended WA-v4-Int-34.235.248.212 10 deny tcp any host 34.235.248.212 eq www 20 deny tcp any host 34.235.248.212 eq 443 30 permit tcp any any eq www 40 permit tcp any host 192.0.2.1 eq 443 exit

Q ip access-list extended WA-sec-34.235.248.212 10 permit tcp any host 34.235.248.212 eq www 20 permit tcp any host 34.235.248.212 eq 443 30 permit tcp host 34.235.248.212 eq www any 40 permit tcp host 34.235.248.212 eq 443 any 50 permit

tcp any any eq domain 60 permit udp any any eq domain 70 permit udp any any eq bootpc 80 permit udp any any eq bootps exit
ip access-list extended WA-v4-Int-34.235.248.212 10 deny tcp any host 34.235.248.212 eq www 20 deny tcp any host 34.235.248.212 eq 443 30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443 nvit

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Question: 241

An engineer has eight WLCs in a mobility group and must reduce the bandwidth consumed. Which two configuration items achieve this result? (Choose two.)

A. global symmetric mobility messaging

B. global multicast mode

C. mobility group unicast messaging

D. global unicast messaging

E. mobility group multicast messaging

Answer: B, E

Explanation:

Question: 242

A network engineer recently deployed Cisco Catalyst Center (formerly DNA Center) to a customer site. The customer is being flooded with alarms for wireless clients that fail AAA authentication.

What is the path to disable the alarm in the Cisco Catalyst Center user interface?

A. Assurance > Manage > Sensors

B. Assurance > Manage > Intelligent Capture Settings

C. Assurance > Manage > Issue Settings

D. Assurance > Manage > Health Score Settings

Answer: C

Explanation:

Question: 243

Refer to the exhibit.

```
Please enter controller type [WLC / NGWC] [WLC]: WLC
Please enter controller ip: 0.0.0.0
Please enter the controller version [Optional]:
Please enter controller SNMP version [v1 / v2c / v3] [v2c]: v2c
Please enter controller SNMP write community [private]:
```

Refer to the exhibit. An event company must gather location-tracking details of wireless clients at an event where clients will be given free guest access to the Wi-Fi. A network engineer must integrate a Cisco WLC with a Cisco CMX server. Which command must be run?

```
[cmxadmin@cmx]# cmxctl config controllers floors wlc-ip-address
```

```
[cmxadmin@cmx]# cmxctl config controllers add
```

```
[cmxadmin@cmx]# cmxctl config controllers import
```

```
[cmxadmin@cmx]# cmxctl config controllers activeap
```


A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Question: 244

A company has a Cisco wireless network with Cisco ISE. The company wants to allow employees to use their personal mobile devices on the wireless network. The company wants to allow access to the network only if the devices meet certain criteri

a. To meet the requirement, the company asked a network engineer to create a native supplicant profile. Which two fields must be configured when the profile is created? (Choose two.)

A. Allowed Protocol (PEAP/TLS)

B. Allowed Protocol (Ms-CHAPv2/ EAP-FAST)

C. SSID Name

D. WLC Name

E. Allowed Protocol (LEAP/ EAP-TTLS)

Answer: AC

Explanation:

Question: 245

A customer must use deep-packet inspection on the Cisco Catalyst 9800 Series Wireless Controller. The details must include all wireless client use details. Where must AVC be configured to meet this requirement?

A. RF tag

B. WLAN

C. policy profile

D. join tag

E. AP join

Answer: C

Explanation:

Question: 246

A customer has 10 Cisco 3700 Series APs in autonomous mode installed at a warehouse facility. A new VoWLAN service is being deployed to support Cisco WLAN phones. All wired QoS is configured. The customer requires that all VoWLAN signaling and RTP traffic be prioritized between the wired and wireless networks. Which configuration is required?

A. Apply a Cisco AVC profile for RTP and signaling on all the APs.

B. Switch on Fastlane on all the APs.

C. Set EDCA on all the APs to optimize voice and video.

D. Enable AWID priority mapping on all the APs

Answer: D

Explanation:

Question: 247

An engineer is defining a new Cisco AVC profile with different rules for HR and VIP users. Both user types connect to a single SSID and authenticate by using their Active Directory credentials via a Cisco ISE The engineer wants to apply the AVC profile dynamically to the user types Which Cisco AV pair attribute must be applied to the Cisco ISE?

A. role-name-avc

B. avc-protile-name

C. policy-role-avc

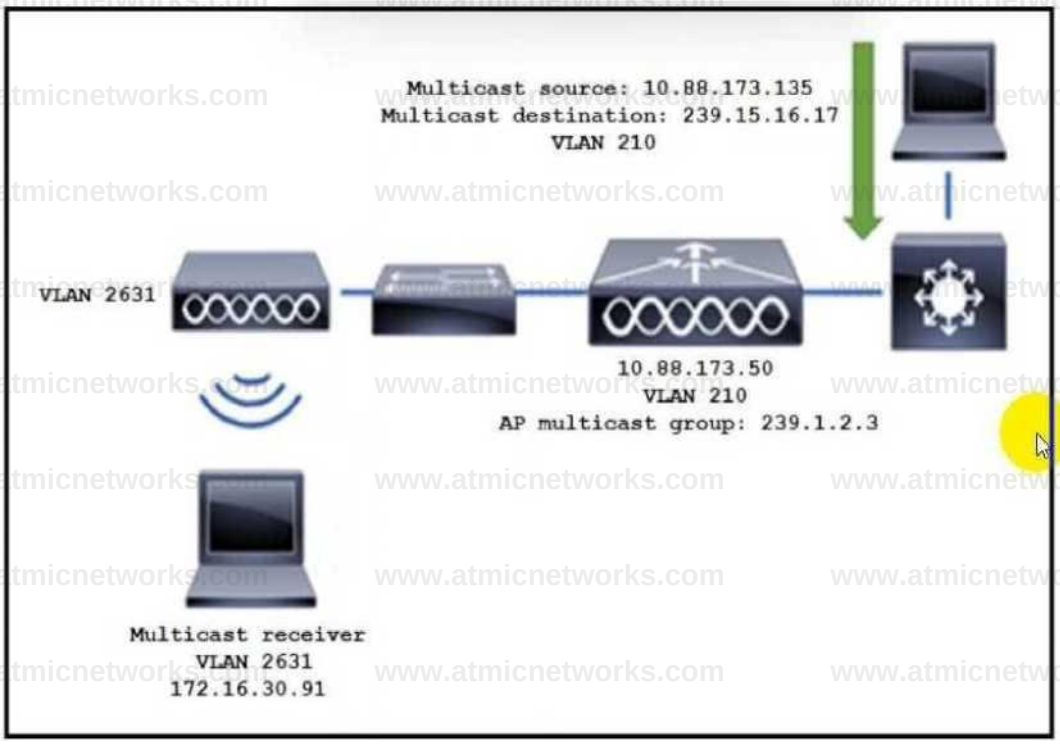
D. policy-avc-role

Answer: B

Explanation:

Question: 248

Refer to the exhibit.



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: D, E

Explanation:

Question: 249

An engineer is deploying a Cisco wireless network to support branch offices. All APs are in FlexConnect mode, and

the SSIDs switch traffic locally. The customer requires that all QoS for the VoWLAN service be based on Layer 2 markings. Which configuration is required on the switch ports that connect to the APs?

A. MLSAWID1P

B. MLSAWID UP

C. MLS Trust DSCP

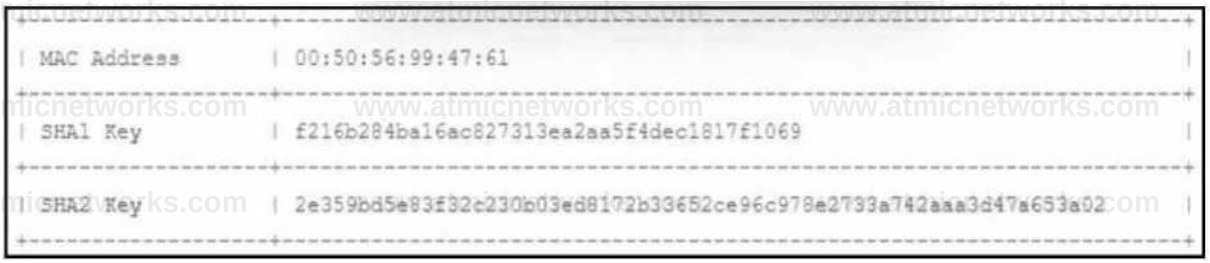
D. MLS Trust COS

Answer: D

Explanation:

Question: 250

Refer to the exhibit.



Refer to the exhibit. A Cisco WLC and Cisco CMX server fail to establish an NMSP tunnel for location services. All required ports are allowed through the firewall. Which command shows the hash key that was pushed from the WLC to the CMX server?

A. nmsp enable

B. show nmsp status

C. show nmsp subscription summary

D. cmxctl conflg controllers show

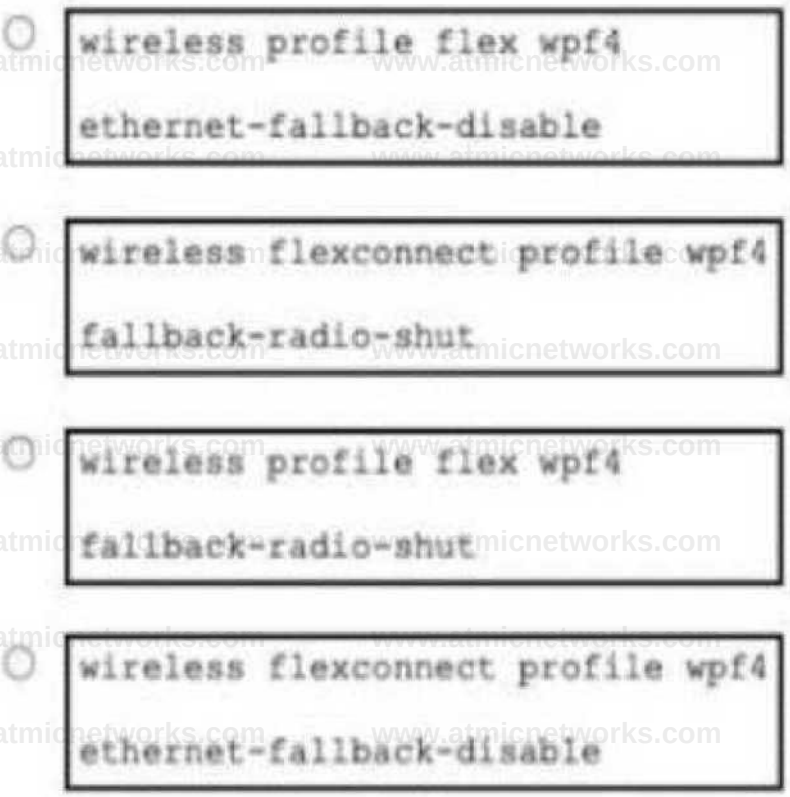
Answer: D

Explanation:

Question: 251

Refer to the exhibit.

Refer to the exhibit A network engineer must deploy a configuration to a Cisco Catalyst 9800 WLC to prevent a FlexConnect AP from allowing wireless clients to connect when its Ethernet connection is down Which code snippet must be added to the box in the code to complete the configuration?



A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Question: 252

A retail company wants to migrate from their existing CMX location services to Cisco Spaces infrastructure for detect and locate functionality. Ports 80 and 443 are opened to establish the connection between the wireless network and Cisco Spaces. However, the CMX is in a DMZ and is not publicly accessible. Which two actions must the administrator take to achieve location hierarchy in Cisco Spaces from CMX? (Choose two.)

A. Configure a new notification service on CMX with Cisco Spaces receiver details.

B. Use Cisco WLC Direct Connect feature to connect Catalyst 9800 to Cisco Spaces directly.

C. Download JSON dump of the location hierarchy from CMX and manually upload to Cisco Spaces.

D. Establish VPN connection between CMX and Cisco Spaces to transfer the location hierarchy details.

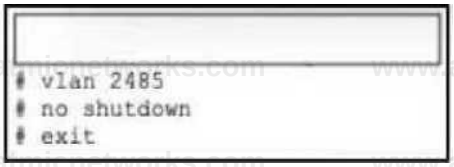
E. Install Cisco Spaces Connector on-premises to connect CMX to Cisco Spaces.

Answer: A, E

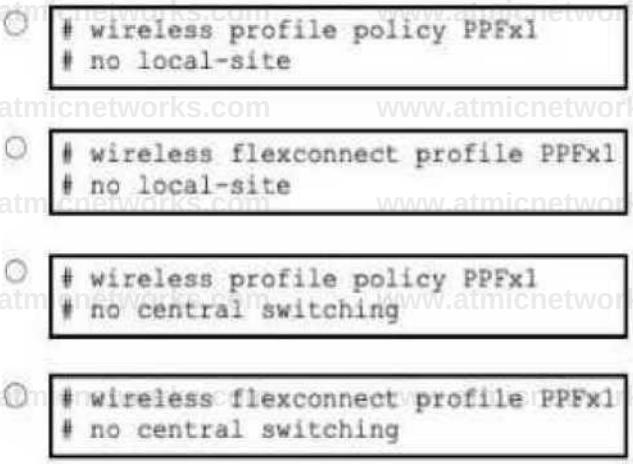
Explanation:

Question: 253

Refer to the exhibit.



Refer to the exhibit A network engineer is using a Cisco Catalyst 9800 Series WLC to deploy a new wireless solution in a branch location Client traffic must be configured to break out locally Which code snippet must be added to the box in the code to complete the policy profile?



A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Question: 254

A network engineer must deploy a Cisco wireless solution tor an event company Cisco ISE will be used for user authentication based on groups Each user group must be placed in its own VLAN after authentication

Where in the Cisco ISE user interface must the configuration be made?

A. Profiling

B. Allowed Protocols

C. Authorization Profiles

D. Client Provisioning

Answer: C

Explanation:

Question: 255

An engineer configures a WLC and 20 Cisco OEAPs. The engineer must configure a remote LAN that uses WPA2 Enterprise security. How should the LAN be configured?

A. on the anchor WLC via the GUI

B. on the OEAP via the GUI

C. on the OEAP via the CLI

D. on the WLC via the CLI

Answer: D

Explanation:

Question: 256

A company wants to utilize the wireless network to push videos to wireless clients. An engineer has been hired to

configure a Cisco WLC to notify users when it cannot provide a video stream while using the Multicast Direct Feature. Which settings must be enabled for this functionality?

A. Session Announcement State

B. Message of the Day

C. SNMP Trap log

D. Northbound Notification

Answer: A

Explanation:

Question: 257

An organization is concerned about site-specific 802.1X authentication in the event of a WAN outage in their Cisco FlexConnect deployment. Which data is needed to accomplish this authentication?

A. local TACACS server shared secret

B. central RADIUS server shared secret

C. central TACACS server shared secret

D. local RADIUS server shared secret

Answer: D

Explanation:

Question: 258

An engineer supports the network infrastructure within a football stadium, and there is a new requirement to send media over wireless. Multicast direct must be used to optimize multicast communication over wireless. Which multicast address must be added in the media stream configuration to meet this requirement?

A. AP multicast address group

B. INESE DUMPS

C. RP multicast address

D. WLC multicast address

E. video server multicast destination address

Answer: D

Explanation:

Question: 259

A company has a Cisco wireless solution and uses Cisco ISE to authenticate corporate users using 802.1X. Users must be grouped by endpoints, and a policy profile must be added and then assigned to an identity group. What is the configuration path in the Cisco ISE user interface?

A. Policy > Profiling > Profiling Policies > Add

B. Policy > Policy Elements > Profiling > Add

C. Policy > Posture > Posture Profile > Add

D. Policy > Client Provisioning > Client Provisioning Policy > Add

Answer: A

Explanation:

Question: 260

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? (Choose two.)

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

Explanation:

Question: 261

An engineer must set up EAP-TLS authentication on all Cisco FlexConnect APs in local authentication mode
Which certificates must be added to allow seamless roaming?

A. client and controller root CA

B. client and AP root CA

C. controller and AP root CA

D. AP and controller root CA

Answer: B

Explanation:

Question: 262

A network administrator of a school district must implement a DNS-based ACL to block students from accessing certain teacher URLs where test papers are hosted. The infrastructure contains a Cisco Catalyst 9800 WLC with 25 9136 APs. The administrator configured the URL Filter List called urllist_flex_pre, applied the URL Filter List to the default Flex Profile, and defined Preauth called urllist_local_preauth and Postauth called urllist_local_postaut URL Filter List. Which configuration must the administrator apply to implement the ACL on the default policy profile?

```
Device# configure terminal
Device(config)♦ urlfilter list
     urllist_local_postauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# filter-type
     post-authentication
Device(config-urlfilter-params)# redirect-server-ipv4
     9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6
     2001:300:8:162
Device(config-urlfilter-params)I url urll.dns.com
Device(config-urlfilter-params)J end
```

```
Device# configure terminal
Device(config)# urlfilter list
     urllist_flex_pre
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4
     £.8.6.9
Device(config-urlfilter-params)♦ redirect—server-ipvo
     2001:300:8::81
Device(config-urlfilter-params)# url urll.das.com
Device(config-urlfilter-params)# end
```

o

```
Device# configure terminal
Device(config)# wireless profile policy
     default-policy-profile
Device(config-wireless-policy)# urlfilter list
     pre-auth-filter urllist_local_preauth
Device(config-wireless-policy)# urlfilter list
     post-auth-filter urllist local_postauth
Device(config-wireless-policy)# end
```

0

```
Device# configure terminal
Device(config)# urlfilter list
     urllist_local_preauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4
     9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6
     2001:300:8::82
Device(config-urlfilter-params)# url urll.dns.com
Device(config-urlfilter-params)# end
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Question: 263

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:

Question: 264

An engineer configures Cisco CMX. which uses Layer 2 high availability on primary and secondary CMX instances, according to these specifications:

· Primary CMX IP address: 192.168.1.4/24

- Secondary CMX IP address 192 168.4.4/24
- Virtual IP address: 192.168.4.1/24

in testing, the engineer discovers that the failover fails. Which action resolves the issue?

A. Place the primary CMX IP address and the virtual IP address in the same subnet

B. Use a virtual IP address with CMX Layer 3 high availability

C. Place the primary CMX IP address and the secondary CMX IP address in the same subnet.

D. Place the primary CMX IP address and the secondary CMX IP address in the same subnet

Answer: D

Explanation:

Question: 265

A wireless engineer completed the configuration of QoS on the WLC and the policy map on the switch that the WLC is connected. During testing, the engineer realizes that the markings are preserved in an incorrect way in the end-to-end traffic flow. What is missing from the configuration?

A. NetFlow

B. class map

C. ACL

D. port channel

Answer: B

Explanation:

Question: 266

An engineer is configuring an autonomous AP to allow 802.1X authentication for users. The policy on the RADIUS server only allows for EAP-TLS authentication. Which authentication method must the engineer select under the Client Authentication Settings for the SSID on the AP?

A. Open

B. Shared

C. Web

D. Network EAP

Answer: A

Explanation:

Question: 267

An engineer must configure rogue AP tracking within Cisco Spaces (formerly Cisco DNA Spaces). The engineer must configure the time after which the RSSI measurement must be considered obsolete and discarded from use in location calculations regardless of the most recent sample. What must be configured to meet the requirement?

A. relative discard RSSI time

B. absolute discard RSSI time

C. location discard RSSI time

D. rogue discard RSSI time

Answer: B

Explanation:

Question: 268

A wireless network uses Cisco ISE to implement 802 1x for user authentication and an Active Directory server as a user database After a power outage, the wireless clients cannot connect to the wireless network The ISE log reports a "clock skew" Which action addresses this issue?

A. Enter the correct credentials

B. Restart the ISE service

C. Install a trusted certificate

D. Configure NTP

Answer: D

Explanation:

Question: 269

An engineer set up RADIUS for WLC management to harden the configuration. Read-only access must be provided to a user. Which Service-Type attribute must be configured on the RADIUS server to meet this requirement?

A. Callback Login

B. Administrative

C. Call Check

D. NAS Prompt

Answer: D

Explanation:

Question: 270

An engineer is configuring wireless guests using Cisco CW

A. When a device connects, it must be redirected to the WebAuth, but this was failing. What must be configured for the device to be redirected correctly?

A. Configure the ACL name on the anchor controller

B. Enabled DHCP option 7.

C. Remove the CN entry from the SAN

D. Allow ICMP toward the portal

Answer: D

Explanation:

Question: 271

A company is concerned about unauthorized APs on their wired and wireless networks. The company implements a Cisco Catalyst Center (formerly DNA Center) solution. Which feature must be enabled?

A. Rogue Management application package

B. Neighbor Assisted Roaming

C. Sniffer package

D. Monitor Mode package

Answer: A

Explanation:

Question: 272

A wireless barcode scanner on a plant floor finds the closest AP that is set to power level 7 statically. However, the scanner has trouble associating and sending dat

a. Which action fixes this issue?

A. Turn on Band Steering in the controller to move the scanner to 5 GHz.

B. Add QoS for the application in the network.

C. Turn on TPC in the controller.

D. Add more APs to the area.

Answer: C

Explanation:

Question: 273

A WLAN is being configured for guest access using the portal on the Cisco CMX. Which Layer 3 security setting must be selected?

A. Web-Policy-Conditional Redirect

B. Web-Policy-Authentication

C. Web-Policy-Splash Page Redirect

D. Web-Policy-Passthrough

Answer: C

Explanation:

Question: 274

An SSID is set up with central web authentication using Cisco ISE The new SSID uses guest tunneling from the foreign controller to the anchor controller. Which device must be configured ISE as the one performing the RADIUS authentication requests for the web authentication method?

A. APs

B. authentication server

C. anchor controller

D. foreign controller

Answer: C

Explanation:

Question: 275

A company is concerned about unauthorized APs on their wired and wireless networks. The company implements a Cisco Catalyst Center (formerly DNA Center) solution. Which feature must be enabled?

A. Rogue Management application package

B. Neighbor Assisted Roaming

C. Sniffer package

D. Monitor Mode package

Answer: A

Explanation:

Question: 276

What is characteristic of Multicast mode that affects the wireless network when configured on a Cisco WLC?

A. Packet replication is performed on the controller

B. The controller sends every multicast packet associated APs

C. Packet replication is performed on the network

D. The controller sends multicast packets to a user group.

Answer: A

Explanation:

Question: 277

A company has an existing Cisco wireless solution deployed to a remote branch location with centrally switched control and data traffic. A new solution is needed to locally switch client traffic when Wi-Fi is used. A new SSID that is used only for voice devices must be mapped to an onsite voice VLAN named VLAN 25. Which configuration on the switch interface that connects to the APs meets the requirement?

A. switchport mode trunk switch trunk native vlan 25

B. switchport mode access switchport access vlan 25 switchport access voice vlan 25 switchport mode trunk

C. switchport trunk allowed vlan add vlan 25

D. switchport mode access switchport access vlan 25

Answer: C

Explanation: