Cisco.300-430.v2026-03-31.q161

Exam Code:	300-430
Exam Name:	Implementing Cisco Enterprise Wireless Networks
Certification Provider:	Cisco
Free Question Number:	161
Version:	v2026-03-31
# of views:	237
# of Questions views:	1610
https://www.freepdfdumps.com/Cisco.300-430.v2026-03-31.q161.html	

NEW QUESTION: 1
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 (LEAVE A REPLY)
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:
https://www.cisco.com/c/en/us/support/docs/wireless/aironet-602-officeextend-access- point/117540-configure-splittunneloeap-00.html

NEW QUESTION: 2
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. MLS AVVID UP
B. MLS Trust DSCP
C. MLS AVVID 1P
D. MLS Trust COS
Answer: (SHOW ANSWER)
For FlexConnect APs with locally switched SSIDs, voice QoS based on Layer 2 markings relies on the 802.1p CoS value in the VLAN tag. The switchport connected to the AP must therefore trust CoS so that the AP's Layer 2 markings (CoS) are honored and used for QoS decisions, which corresponds to MLS Trust COS.

NEW QUESTION: 3
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. Enable Office Extend AP on the Flex Profile.
B. Configure Remote LAN under the Remote LAN.
C. Enable Local Switching under the WLAN.
D. Configure NAT on the physical interface.
E. Create a Flex Group and add the AR
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 4
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: (SHOW ANSWER)
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.

NEW QUESTION: 5
An engineer enabled Cisco Centralized Key Management (CKM) on a WLAN with local and FlexConnect mode APs. The engineer notices that Cisco CKM is not working for the FlexConnect APs when looking at roaming, but it works for local mode APs. Which change must be made on the controller for the configuration to work properly?
A. Configure VLAN-based central switching.
B. Enable Cisco FlexConnect Central Assoc.
C. Use local authentication.
D. Place APs in a Cisco FlexConnect group.
Answer: D (LEAVE A REPLY)
FlexConnect groups are responsible for sharing services between APs in the group. For example, the following services are shared within a FlexConnect group:
Cisco Centralized Key Management (CCKM) / Opportunistic Key
Caching (OKC) fast roaming keys
Local/backup RADIUS server keys
Local EAP (Extensible Authentication Protocol) authentication
Smart Image upgrade

FlexConnect AVC (Application Visibility and Control)
AAA-Override for local switching

NEW QUESTION: 6
An engineer is setting up a new unique NAD on a Cisco ISE. Which two parameters must be configured? (Choose two.)
A. device hostname
B. device password
C. RADIUS fallback
D. device IP address
E. RADIUS shared secret
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 7
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. Reboot all APs before the upgrade.
B. Remove the APs from the group
C. Do not set any master APs.
D. Allocate the master APs to different groups
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 8
Clients on access points within an AP group are not receiving multicast traffic after roaming to another AP within the AP group. Which action maintains multicast connectivity?
A. Enable an ACL on the router that serves the VLAN or subnet.
B. Enable IGMP snooping.
C. Enable a unique NAS-ID for the AP group.
D. Enable NAC out-of-band support.
Answer: (SHOW ANSWER)

NEW QUESTION: 9
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 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. Classify the rogue as malicious in Cisco Prime.

D. Update the status of the rogue in Cisco Prime to contained.

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 10

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 (LEAVE A REPLY)

The checkbox to enable local profiling is called Device Classification.

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless- controllers/215661-in-depth-look-into-client-profiling-on-9.html and logging into my own 9800.

NEW QUESTION: 11

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 Snooping

B. mDNS policy

C. service advertisement

D. AAA Override

Answer: D (LEAVE A REPLY)

NEW QUESTION: 12

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?

```
from ncclient import manager

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

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


<timeout>10</timeout>

A. <priority1>true</priority1>
<timeout>10</timeout>

B. <single-connection>true</single-connection>
<timeout>priority1</timeout>

C. <single-connection>port49</single-connection>
<timeout>10</timeout>

D. <port49>true</port49>

Answer: A (LEAVE A REPLY)

In TACACS+ server configuration on the Cisco Catalyst 9800 via NETCONF, the timeout value specifies the wait time for server responses, and priority1 ensures the server is treated as the primary authentication server. This matches the requirement that the TACACS+ server at 192.168.1.100 must be the primary for both GUI and CLI access.

NEW QUESTION: 13

An engineer configures QoS on an AireOS WLC v8.5. The engineer configures a WLAN for voice traffic and must set the data rates within the QoS profile. How should the data rates be configured to ensure that the QoS profile allows traffic to and from the wireless client?

A. The burst data rate should be set to a non-zero value.

B. Data rates should be applied per AP radio.

C. The burst data rate should be greater than or equal to the average data rate.
D. The burst data rate should be configured before the average data rate.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 14
An engineer is setting up web authentication for the public Wi-Fi. The installation will take place in a retail store. The existing Facebook page to log in to the captive portal must be used. The engineer already paired the Cisco MSE to the Facebook page. Which two actions complete the configuration? (Choose two.)
A. Configure access control lists.
B. Pair Cisco MSE to Cisco Prime Infrastructure.
C. Configure the client for authentication.
D. Configure Cisco MSE to allow mobile authentication.
E. Configure WLAN for authentication.
Answer: A,E (LEAVE A REPLY)
Workflow to Setup the CMX Facebook Wi-Fi
Step 1: Configure Access Control Lists
Step 2: Configure WLAN for authentication
Step 3: Creating a Facebook page
Step 4: Creating and pairing a default Facebook page
Step 5: Pairing MSE and specific locations with the Facebook page
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/CMX_Facebook_Wi-Fi.html

NEW QUESTION: 15
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 (LEAVE A REPLY)
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.

NEW QUESTION: 16
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 (LEAVE A REPLY)
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.

NEW QUESTION: 17
Refer to the exhibit. 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 controller provided, why is the client unable to connect?

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

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

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


A. The client is falling to accept certificate.

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

C. The user is using invalid credentials.

D. The Cisco WLC local EAP profile is misconfigured.

Answer: D (LEAVE A REPLY)

User is configured for PEAP authentication. WLC starts EAP-FAST context (Line 3). -> EAP Profile on the WLC needs to be corrected to use PEAP.

NEW QUESTION: 18

A network engineer is configuring a Cisco AireOS 8.2 WLC, Cisco MSE, and Cisco PI with Cisco 3700 Series APs and Cisco Hyperlocation modules. The engineer configures and enables a WLAN with Hyperlocation. During testing, the engineer notices that the Hyperlocation module cannot be seen on the WLC. Which action resolves the issue?

A. Configure the APs to be in monitor mode.

B. Enable Hyperlocation in the Global Configuration settings of the WLC.

C. Add the key hash that is used to add the Hyperlocation module to the WLC.

D. Enable the NTP server that is connected to the Hyperlocation module.

Answer: (SHOW ANSWER)

Step 1
Choose Wireless > Access Points > Global Configuration.
Step 2
In the Hyperlocation Config Parameters section:
Check the Enable Hyperlocation check box.
Based on AP and installed module, checking the Enable Hyperlocation check box enables different location service (PRL-based or AoA-based).
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-2/config-guide/b_cg82/b_cg82_chapter_011010.html#config-hyperlocation-global:~:text=Check%20the%20Enable%20Hyperlocation%20check%20box.

NEW QUESTION: 19
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 Allow AAA Override to Enabled.
B. Select DHCP Profiling.
C. Set DHCP Addr. Assignment to Required.
D. Set NAC State to Radius NAC.
E. Select Enable Session Timeout.
Answer: (SHOW ANSWER)
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.

NEW 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. WME
B. QBSS
C. Voice VLAN
D. QoS routing
Answer: C (LEAVE A REPLY)
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.

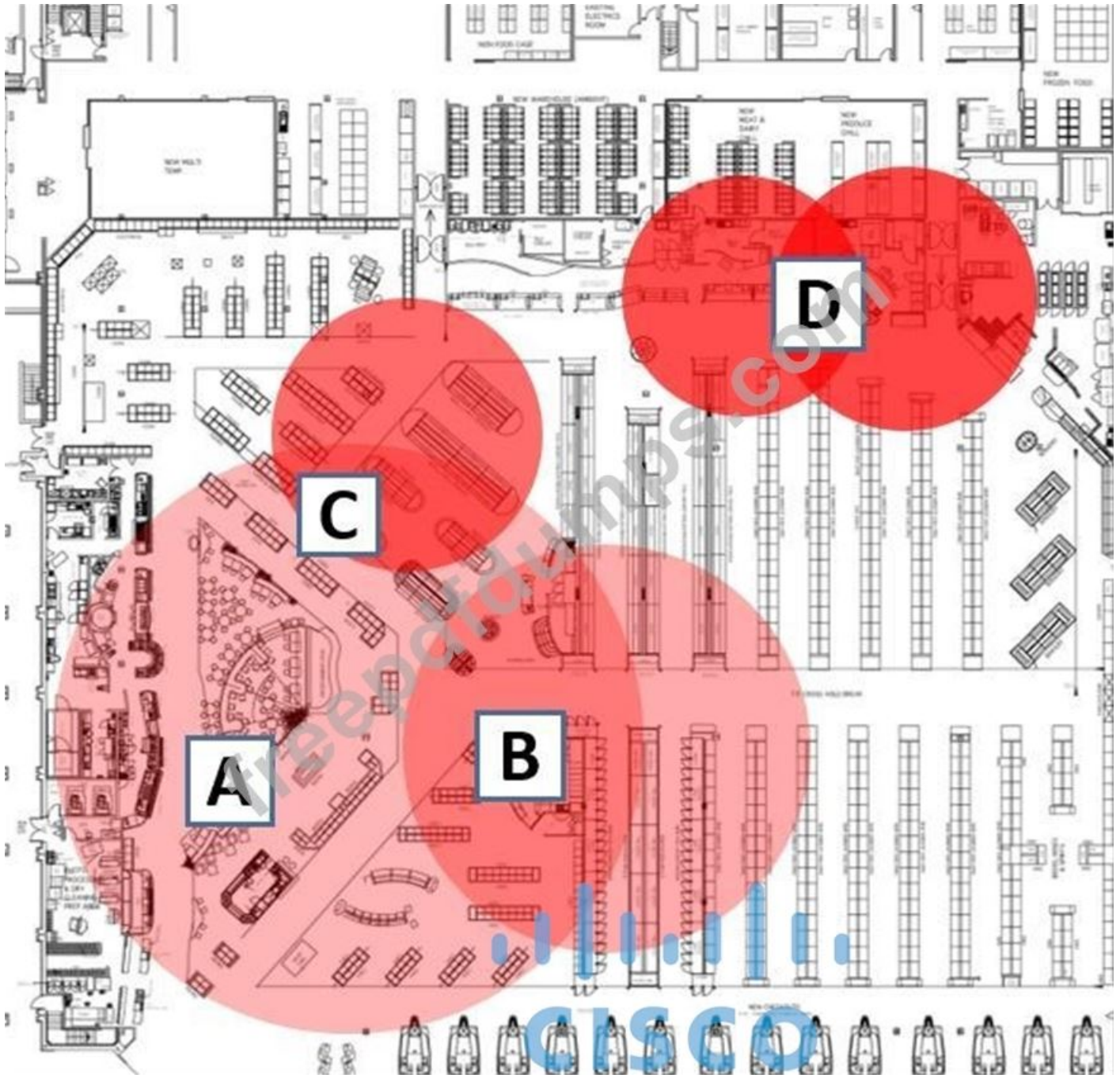
NEW QUESTION: 21
An engineer is configuring wireless guests using Cisco CWA. When a device connects, it must be redirected to the WebAuth, but this was failing. What must be configured for the device to be redirected correctly?
A. Allow ICMP toward the portal.
B. Enabled DHCP option 7.
C. Remove the CN entry from the SAN.

D. Configure the ACL name on the anchor controller.
Answer: (SHOW ANSWER)

NEW QUESTION: 22
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 must be configured under the shell profile on the TACAS+ server for a user with ready-only permissions?
A. MANAGEMENT
B. MONITOR
C. ADMIN
D. READ
Answer: B (LEAVE A REPLY)
Usage: In order to grant the user read-only access, the <username> value must be set to monitor. In order to grant the user read-write access, the <username> value must be set to admin.
https://www.cisco.com/c/en/us/support/docs/security/secure-access-control-system/115926- tacacs-radius-devices-00.html

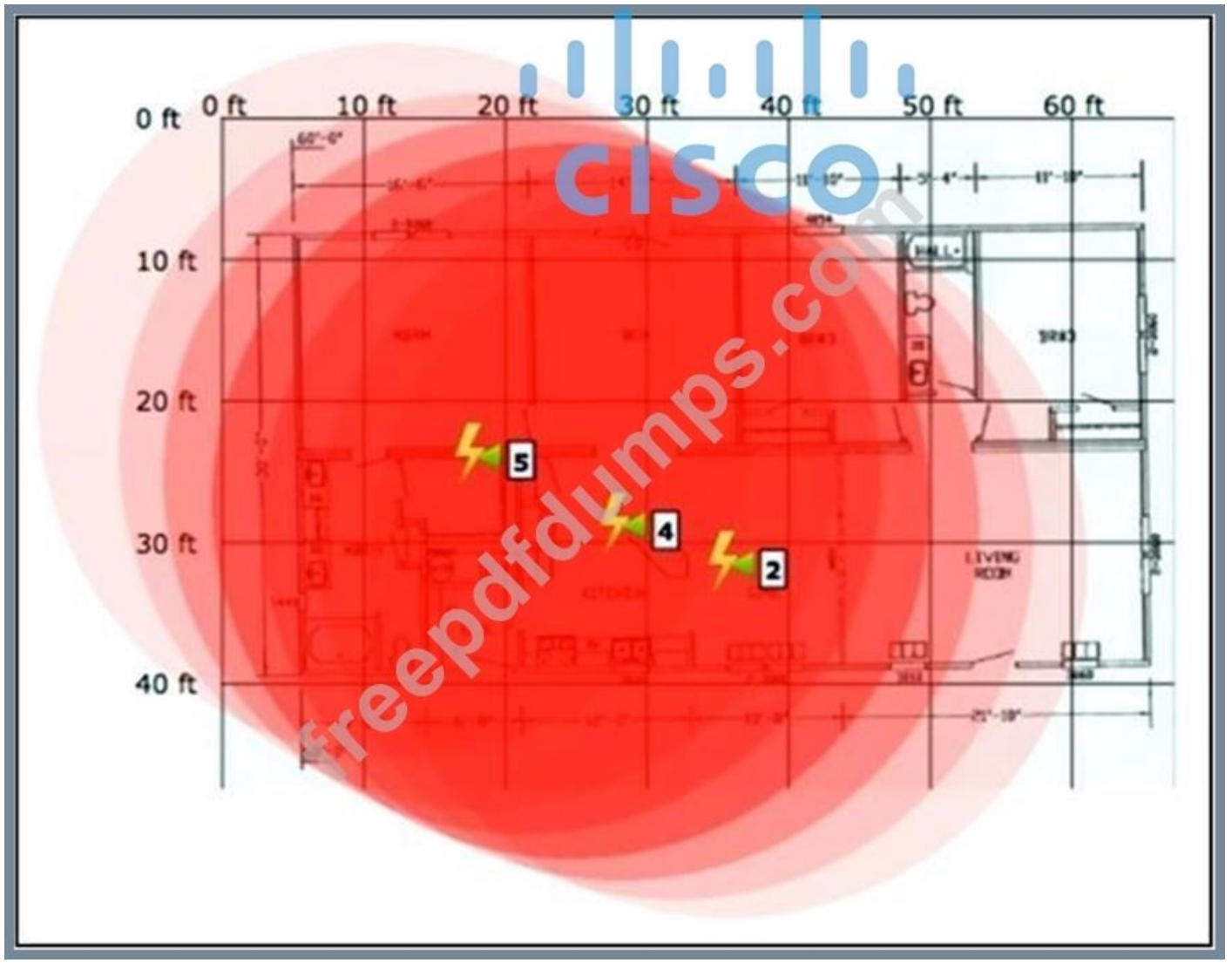
NEW QUESTION: 23
When using a Cisco Catalyst 9800 Series Wireless Controller, which statement about AutoQoS is true?
A. It has a set of predefined profiles that you cannot modify further
B. It matches traffic and assigns each matched packet to QoS groups
C. It automates deployment of wired QoS and makes wireless QoS implementation easier
D. It allows the output policy map to put specific QoS queues into specific subgroups
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 24
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. Option A
B. Option D
C. Option B
D. Option C
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Refer to the exhibit. An engineer needs to manage non-802.11 interference.
What is observed in the output on PI?



A. Several light interferers are collectively impacting connectivity at this site.
B. The three Individual clusters shown Indicate poor AP placement.
C. At least one strong interferer is impacting connectivity at this site.
D. RF at this site is unable provide adequate wireless performance.
Answer: (SHOW ANSWER)
Lightning bolts display an RF interferer source.
The opacity of the circle displays the severity. If several light interferers overlap, the circles opacity becomes 'dark'. Look at the outlines of the circles, there are 5 light interferers and only 3 have been identified as uniques.

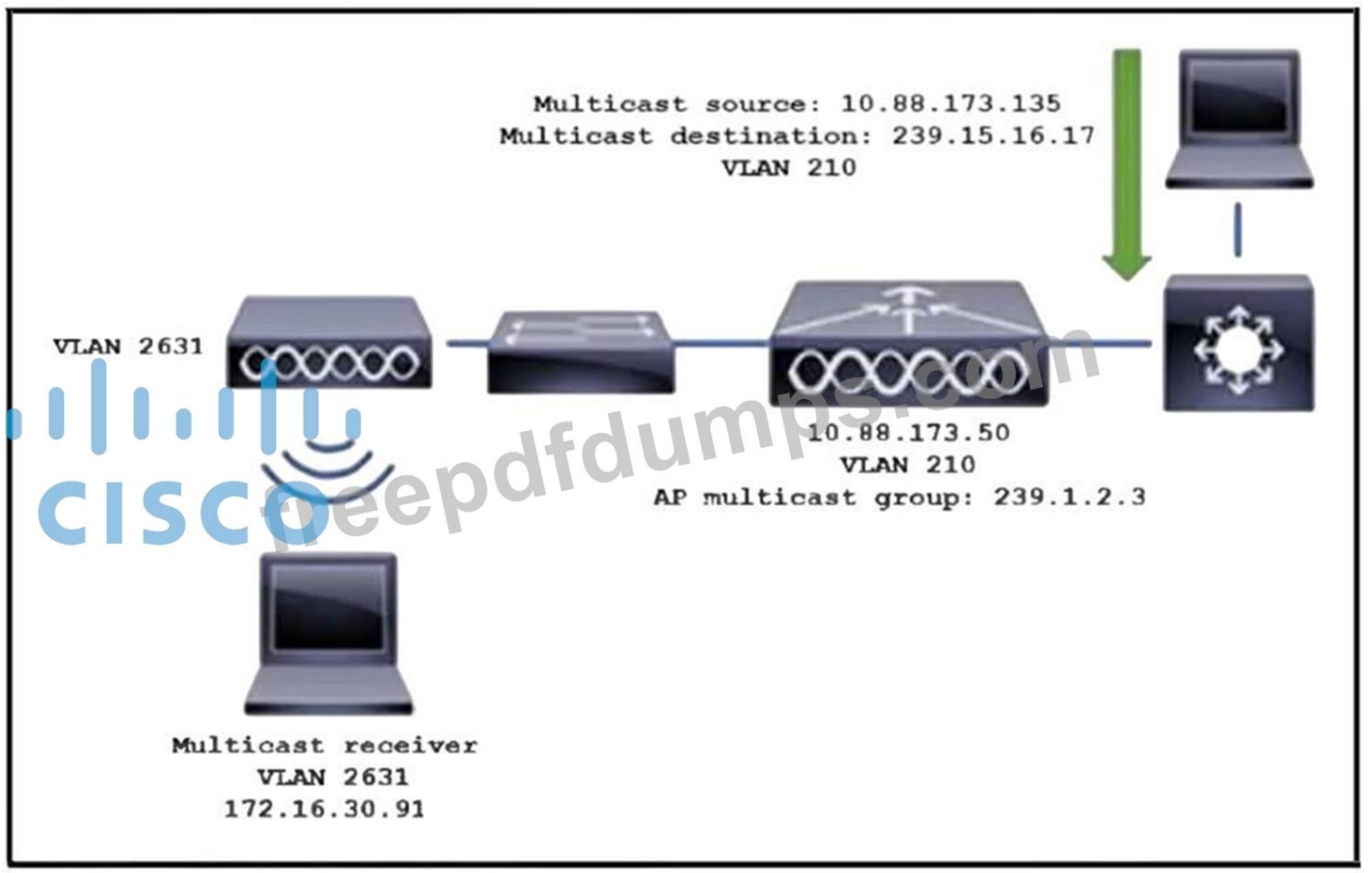
NEW QUESTION: 26
A corporation has recently implemented a BYOD policy at their HQ. Which two risks should the security director be concerned about? (Choose two.)
A. network analyzers
B. malware
C. lost and stolen devices
D. keyloggers
E. unauthorized users
Answer: B,C (LEAVE A REPLY)

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.

NEW QUESTION: 27
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 (LEAVE A REPLY)
When IGMP snooping is enabled, multicast traffic is sent only to the ports which sent IGMP joins.
If IGMP snooping is disabled, then traffic is flooded to all the ports in that VLAN.

NEW QUESTION: 28
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. IPP
C. WMM UP
D. DSCP
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 29
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 IGMP v3 support to support AP IOS-based access points.
B. Enable multicast routing on VLAN 210 for the wireless management VLAN.
C. Enable IGMP support across multicast hosts, routers, and multilayer switches.
D. Enable multicast routing on VLAN 2631 for the wireless client VLAN.
E. Configure the CAPWAP multicast group address to enable multicast mode on the device.
Answer: B,C (LEAVE A REPLY)
Multicast-direct requires the AP's management VLAN to receive the multicast stream; enable multicast routing on VLAN 210 so the AP can join and receive the group.
IGMP must be enabled end-to-end so joins from the AP reach the source and multicast forwarding is established.

NEW QUESTION: 30
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 (LEAVE A REPLY)
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.

NEW QUESTION: 31
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. Disable the Cisco ISE password policy that disables accounts for unchanged passwords.
B. Remove APs from the exclusion list, due to authentication failures.
C. Upgrade Cisco ISE to a newer version due to bugs.
D. Install a valid EAP certificate on Cisco ISE for the APs.
Answer: A (LEAVE A REPLY)
When APs are configured as local users in Cisco ISE (using MAC addresses), they rely on fixed credentials that typically never change. If the password policy in ISE enforces account expiration or disables accounts with unchanged passwords, APs will fail authentication after reboot until re-enabled. Disabling this password policy ensures AP MAC-based local user accounts remain active and APs can consistently rejoin the controller.

NEW QUESTION: 32
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: (SHOW ANSWER)
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.

NEW QUESTION: 33
An engineer manages the wireless network for a government agency. The wireless network is used for access to the corporate network. The wireless network must include the latest wIPS/wIDS detection definitions. Which action does the engineer take to ensure that this requirement is met?
A. Update the Cisco MSE software.
B. Configure Cisco Prime Infrastructure to push new definitions to the APs.
C. Update the Cisco WLC software.
D. Configure the Cisco WLC to repoll the Cisco MSE for update definitions.
Answer: (SHOW ANSWER)

In a Cisco wireless infrastructure, Wireless Intrusion Prevention System (wIPS) and Wireless Intrusion Detection System (wIDS) signatures and definitions are primarily handled by the Cisco Mobility Services Engine (MSE) or Cisco DNA Spaces (in newer deployments). These definitions include the logic and patterns used to detect rogue devices, spoofing, DoS attacks, and more.

NEW QUESTION: 34
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: D (LEAVE A REPLY)
There is no "wireless flexconnect" command. Use the "wireless profile Policy" command.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/cmd- ref/b_wl_17_1_cr/configuration-commands-g-to-z.html#wp5169136690
There is no "Local switching" command. Use the "no central switching" command.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-1/cmd- ref/b_wl_17_1_cr/configuration-commands-a-to-f.html#wp3034709985

NEW QUESTION: 35
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?

```
import requests

url = "https://<catalyst-center-ip>/dna/intent/api/v1/event/webhook"

payload = {
    "name": "ReportWebhook",
    "url": "https://example.com/webhook",
    [redacted]
}

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

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


"method": "PUT",

A. "trustCert": true

"method": "POST",

B. "trustCert": true

"method": "POST",

C. "trustCert": false

"method": "PUT",

D. "trustCert": false

Answer: (SHOW ANSWER)

When configuring a webhook in Cisco Catalyst Center using the API, the HTTP method must be POST because events are sent from Catalyst Center to the webhook endpoint. Since the destination URL uses HTTPS with a self-signed certificate, the trustCert must be set to true to allow the connection despite the untrusted certificate. This ensures the webhook works properly for delivering Security Advisories Data reports.

NEW QUESTION: 36

What is characteristic of multicast mode that affects the wireless network when configured on a Cisco WLC?

A. The controller sends multicast packets to a user group.

B. Packet replication is performed on the network.

C. Packet replication is performed on the controller.

D. The controller sends every multicast packet associated APS.

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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 MSE.

B. Enable automatic synchronization on MSE.

C. Add new APs to maps on Cisco Prime Infrastructure.
D. Enable automatic synchronization on Cisco Prime Infrastructure.
E. Manually synchronize from Cisco Prime Infrastructure.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
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?

A.

```
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 url1.dns.com
Device(config-urlfilter-params)# end
```

B.

```
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::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

C.

```
Device# configure terminal
Device(config)# urlfilter list
    urllist_flex_pre
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4
    8.8.8.8
Device(config-urlfilter-params)# redirect-server-ipv6
    2001:300:8::81
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

D.

```
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
```

Answer: (SHOW ANSWER)

To enforce DNS-based ACLs using URL filtering on a Cisco Catalyst 9800 WLC, the administrator must apply the pre-auth and post-auth URL filter lists directly under the policy profile. Chosen option shows the correct configuration, where urllist_local_preauth and urllist_local_postauth are both bound to the default-policy-profile. This ensures the ACL is enforced for clients before and after authentication, meeting the requirement to block access to restricted teacher URLs.

NEW QUESTION: 39

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 (LEAVE A REPLY)

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.

NEW QUESTION: 40

Refer to the exhibit. 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?

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 → 2003 Len=104
3	1.087479	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
4	2.733577	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
5	2.999859	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
6	3.001227	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
7	4.355249	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
8	5.999538	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
9	6.000959	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
10	8.999418	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
11	9.000791	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
12	9.262904	10.48.39.214	10.48.71.21	UDP	146	9999 → 2003 Len=104
13	10.894785	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
14	11.995126	10.48.39.251	10.48.71.21	UDP	194	9999 → 2003 Len=152
15	11.999193	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
16	14.994902	10.48.39.251	10.48.71.21	UDP	178	9999 → 2003 Len=136
17	14.996368	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
18	17.994857	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
19	17.996231	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
20	18.102843	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
21	21.098408	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
22	21.099952	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
23	24.098574	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
24	24.099804	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
25	27.098099	10.48.39.251	10.48.71.21	UDP	162	9999 → 2003 Len=120
26	27.099839	10.48.39.251	10.48.71.21	UDP	130	9999 → 2003 Len=88
27	28.880307	10.48.39.164	10.48.71.21	UDP	146	9999 → 2003 Len=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	UDP	178	9999 → 2003 Len=136
30	30.097812	10.48.39.251	10.48.71.21	UDP	146	9999 → 2003 Len=104
31	30.513451	10.48.39.214	10.48.71.21	UDP	130	9999 → 2003 Len=88
32	30.515926	10.48.39.164	10.48.71.21	UDP	130	9999 → 2003 Len=88

> Frame 1: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
> Ethernet II, Src: CiscoInc_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Vmware_99:4e:19 (00:50:56:99:4e:19)
> Internet Protocol Version 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 2f 44 f0 00 00 b4 5f ef 06 fd cb b7 6c 03 c7 ...
[Length: 120]

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 (LEAVE A REPLY)
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.

NEW QUESTION: 41
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 (LEAVE A REPLY)
Protocol Independent Multicast-Sparse Mode (PIM-SM or PIM) is the routing protocol most suited to get multicast routing up and running within a single domain.
http://www.telfor.rs/telfor2002/radovi/2-19.pdf

NEW QUESTION: 42
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 (LEAVE A REPLY)
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.

NEW QUESTION: 43
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. local authentication and central switching
C. central authentication and central switching
D. local authentication and local switching
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 44
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. Allow UDP ports 5246 and UDP port 5247 on the firewall.
C. Allow UDP ports 12222 and 12223 on the firewall.
D. Enable NAT Address on the 5520 with an Internet-routable IP address.
E. Configure a static IP on the OEAP 1810.
Answer: B,C (LEAVE A REPLY)
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

NEW QUESTION: 45
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 (LEAVE A REPLY)
https://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/datasheet- c78-734648.html

The major steps involved in setting up a Hyperlocation system are:

1. Assemble the APs and mount them to the ceiling, recording the exact X, Y, height, and orientation of the devices.
2. Install Cisco WLC and connect the APs to Cisco WLC.
3. Enable the functions that are required, including Hyperlocation, in Cisco WLC.
4. Import Cisco WLC into Cisco PI.
5. Place the AP on the map in Cisco PI.
6. Save and export the map from Cisco PI to a local storage point.
7. Install Cisco CMX.
8. Configure and enable Hyperlocation.
9. Import the map from the local storage point.
10. Verify that the system is showing the clients correctly on the map and that the APs are placed and orientec correctly.
11. Complete Location Accuracy testing of static clients to determine the level of accuracy obtained.

NEW QUESTION: 46

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: (SHOW ANSWER)

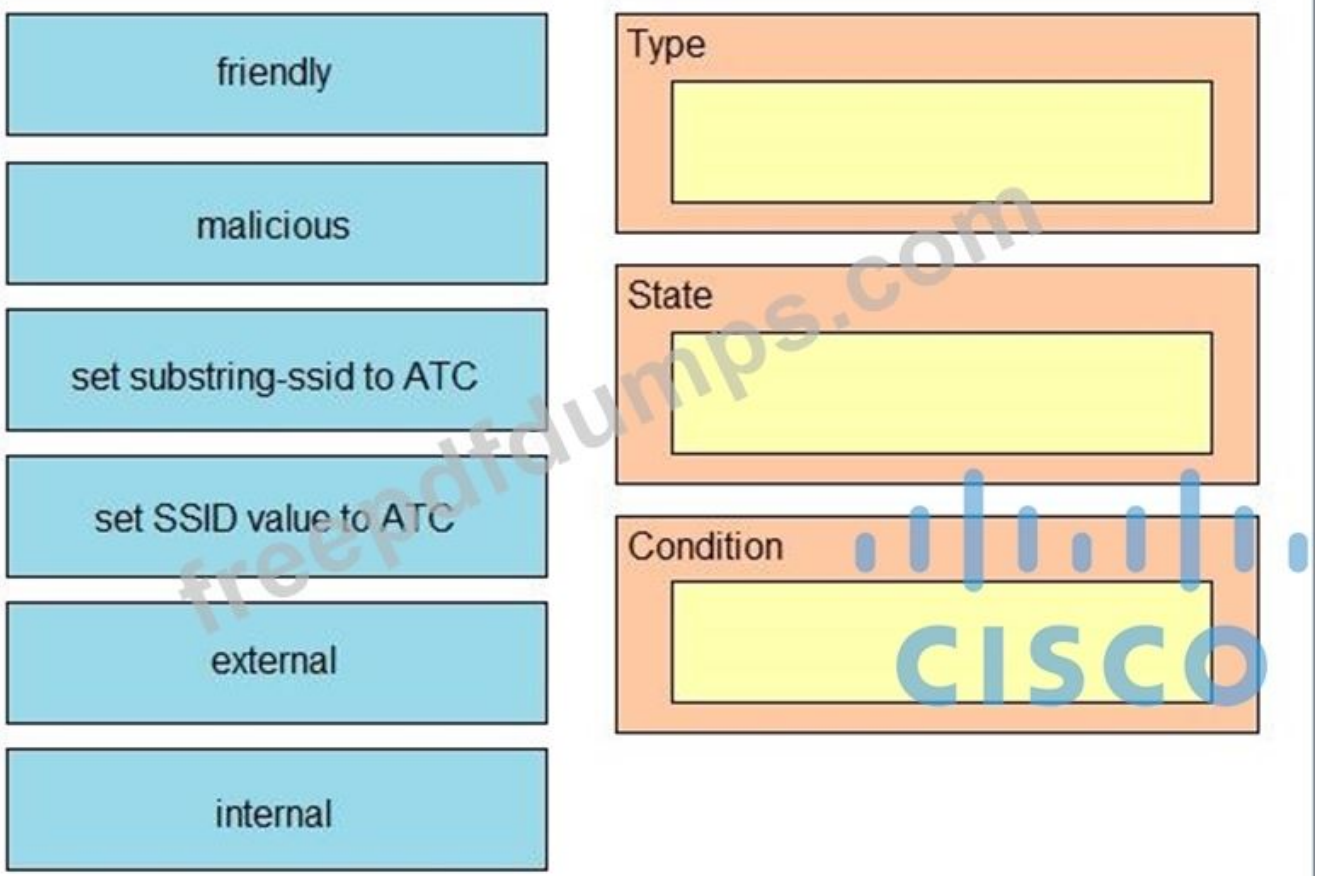
EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) is an EAP method that an Access Point (AP) can use to authenticate to the wired network. EAP-TLS is considered one of the most secure EAP methods because it uses mutual authentication, where both the client and the server authenticate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

NEW QUESTION: 47

Drag and Drop Question

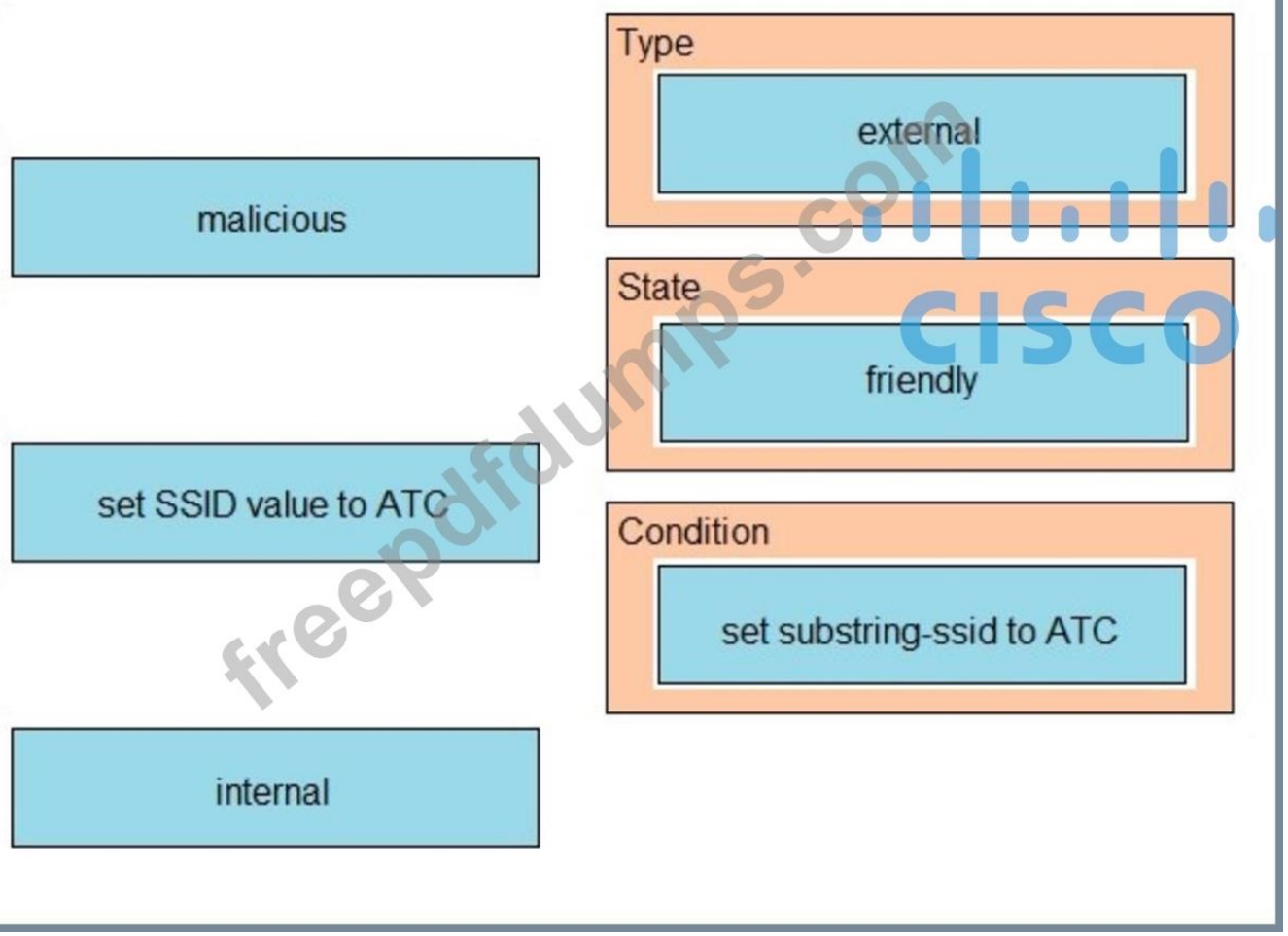
The network management team in a large shopping center has detected numerous roque APs from local coffee shops that are broadcasting SSIDs. All of these SSIDs have names starting with ATC (for example. ATC302. ATC011. and ATC566). A wireless network engineer must appropriately classify these SSIDs using 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 Area



Answer:

Answer Area



Explanation:
https://community.cisco.com/t5/wireless/wildcard-or-regex-in-rogue-ap-rules/td-p/2620976

NEW QUESTION: 48
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 (LEAVE A REPLY)
A FlexConnect group can have one primary AP per AP model. If a primary AP is not selected manually, the AP that has the least MAC address value is automatically chosen as the primary AP for that model.

NEW QUESTION: 49
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. open SSID
C. dual SSID
D. single SSID

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 50

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 a preshared key on the corporate WLAN
B. Use Novell eDirectory
C. Use SAML
D. Use the internal database of the RADIUS server.

Answer: (SHOW ANSWER)

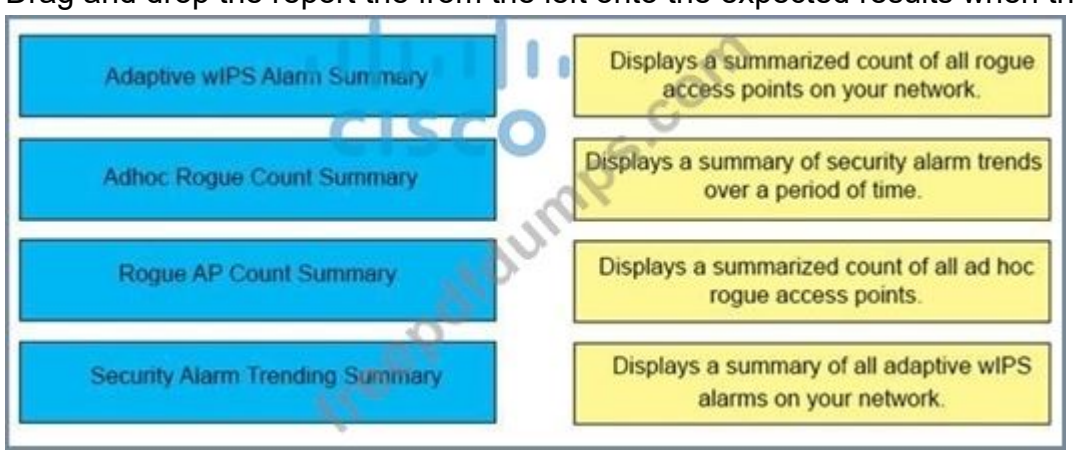
LDAP Identity Source provides access to Active Directory, Sun Directory Server, Novell eDirectory or CUSTOM.
No LDAP really means thta there IS NO directory server (NO Microsoft, NO SUN, NO Novell) Reference:
https://www.cisco.com/c/en/us/td/docs/security/ise/2-4/admin_guide/b_ISE_admin_guide_24/m_extrnal_identity_store.html#reference_922CCDAF80684CDEB02D88C3525B3F89

NEW QUESTION: 51

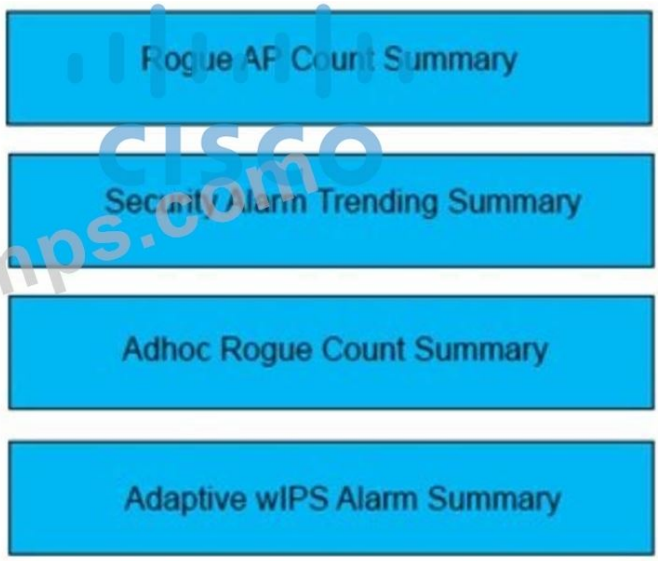
Drag and Drop Question

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:

Report	Description	Customizable?	Multiple Subreports?	Report Views	Data Field Sorting?
Adaptive wIPS Alarm Summary	This report displays a summary of all adaptive wIPS alarms on your network.	Yes	No	Both	No
Adhoc Rogue Count Summary	This report displays a summarized count of all ad hoc rogue access points.	No	No	Both	No
Rogue AP Count Summary	This report displays a summarized count of all rogue access points on your network.	No	No	Both	No
Security Alarm Trending Summary	This report displays a summary of security alarm trends over a period of time.	No	No	Graphical	No

NEW QUESTION: 52

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. port
B. bounce
C. preauth
D. no CoA
E. reauth
Answer: E (LEAVE A REPLY)

NEW QUESTION: 53
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 (LEAVE A REPLY)
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.

NEW QUESTION: 54
An engineer must create an account to log in to the CLI of an access point for troubleshooting.

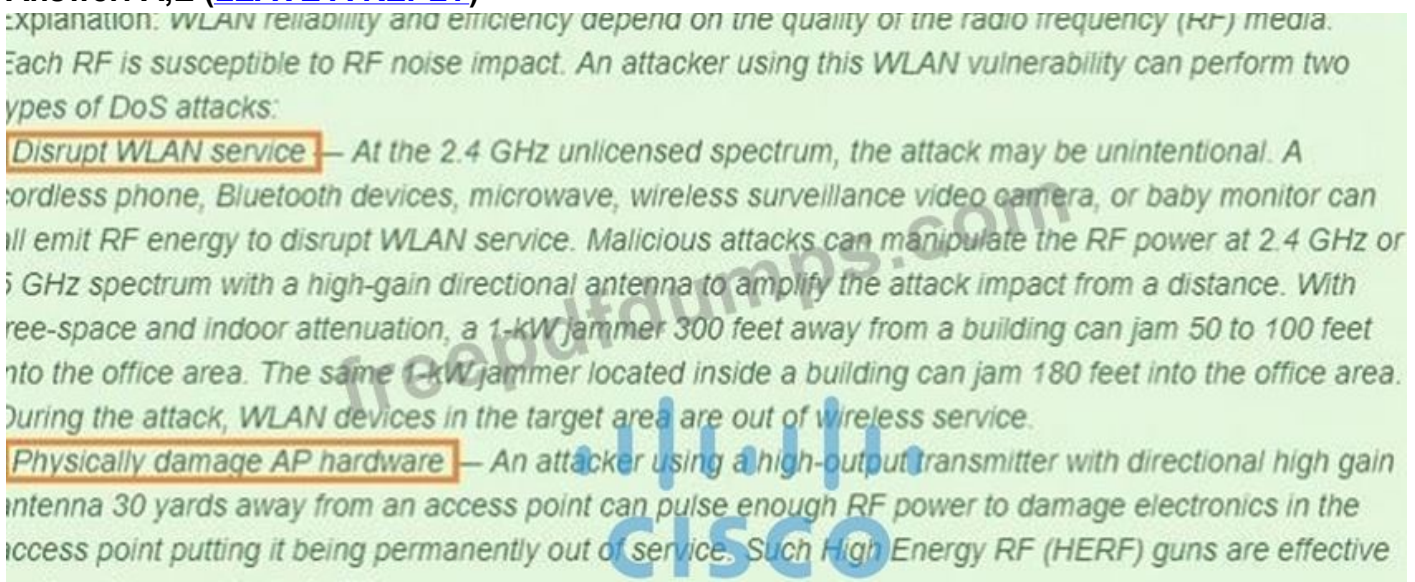
Which configuration on the WLC will accomplish this?
A. ReadWrite User Access Mode
B. Global Configuration Enable Password
C. SNMP V3 User
D. Allow New Telnet Sessions
Answer: A (LEAVE A REPLY)
To create an account for CLI access to an access point for troubleshooting, the WLC must be configured to allow 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.

NEW QUESTION: 55
ALLAR 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. Enable RADIUS DHCP profiling on the WLAN.
B. Create a local policy on the WLC.
C. Use an mDNS profile for the iPad device.
D. Use 802.1x authentication to profile the devices
Answer: B (LEAVE A REPLY)
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. 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.

NEW QUESTION: 56
The IT department creates a video containing instructions for employees who have just joined the company. Newcomers need to join the wireless network named NEW4501999110. The WLAN name will be changed daily by IT support. Only new employees must receive the video over wireless multicast. What allows this feature?
A. WMF
B. WMM
C. TPC
D. DCA
Answer: A (LEAVE A REPLY)
Wireless Multicast Forwarding (WMF) is designed to efficiently forward multicast traffic on wireless networks by sending multicast frames only to the interested clients who have joined the multicast group, using IGMP to track group membership.
This is ideal for scenarios like delivering instructional videos via multicast only to specific users (new employees) connected to a particular WLAN, even if the WLAN name changes daily.
WMF improves wireless performance and reliability for multicast streaming by converting multicast frames to unicast frames for targeted delivery, reducing unnecessary traffic and improving quality.

NEW QUESTION: 57
Which two events are outcomes of a successful RF jamming attack? (Choose two.)
A. disruption of WLAN services
B. unauthentication association

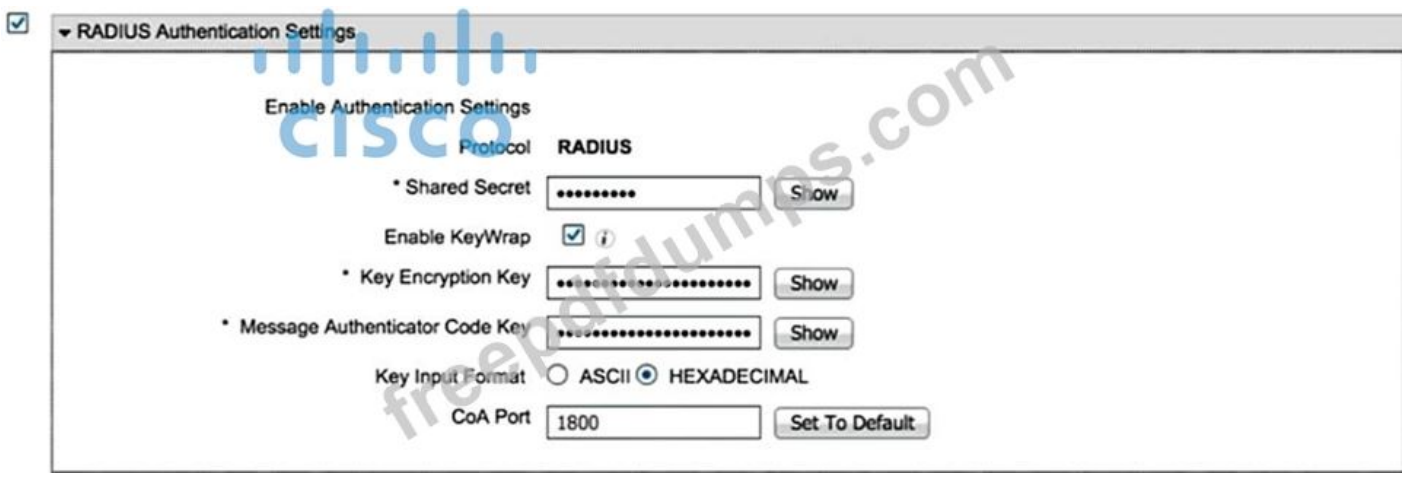
C. deauthentication broadcast
D. deauthentication multicast
E. physical damage to AP hardware
Answer: A,E (LEAVE A REPLY)



NEW QUESTION: 58
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. This configuration must be performed through the CLI and not though the web GUI
B. No ACLs have been created under the Access Control List tab.
C. The ACL does not have a rule that is specified to the Management interface.
D. When the ACL is created, it must be specified that it is a CPU ACL.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
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 can 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. Change the CoA Port

C. Correct the shared secret.

D. Use ASCII for the key input format

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 60

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. NAS Prompt

B. Administrative

C. Call Check

D. Callback Login

Answer: (SHOW ANSWER)

Since, in this example, user acsreadonly needs to have read-only access, choose NAS Prompt from the Service-Type pull-down menu and click Submit.

This ensures that this particular user has read-only access to the WLC.

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71989-manage-wlc- users-radius.html#toc-hId--1799525129

NEW QUESTION: 61

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: WIPS

B. Ap mode: monitor, Ap submode: WIPS

C. Ap mode: monitor, Ap submode: none

D. Ap mode: local, Ap submode: none

Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 62
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 (LEAVE A REPLY)
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.

NEW QUESTION: 63
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. Each WLC management address must be in a different multicast grou
D. Both WLCs must be assigned the same multicast group address
Answer: A (LEAVE A REPLY)
Choose Controller > General to configure AP multicast mode (multicast or unicast) & CAPWAP multicast group address(only for multicast mode). Use private multicast IP (239.0.0.0/8) for the group address, but avoid 239.0.0.x or 239.128.0.x as these overlap with the link local MAC addresses & flood out all switch ports. This group address cannot be used for any application in your network. If you have multiple controllers, configure different group address for different controllers.
https://mrncciew.com/2012/11/17/configuring-multicast-on-wlc/

NEW QUESTION: 64

A customer uses a Cisco Catalyst 9800 Series Wireless Controller and Cisco 802.11ax APs. 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. DHCP
B. wireless supplicant
C. RADIUS
D. MAC Address OUI
E. IP address
Answer: (SHOW ANSWER)

NEW QUESTION: 65
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 (LEAVE A REPLY)
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.

NEW QUESTION: 66
An engineer configures an AireOS WLC v8.2 that has Cisco Aironet 3700 Series APs and Cisco Hyperlocation modules. The engineer deploys and enables a WLAN that has Hyperlocation.
During testing, the engineer notices poor location accuracy when the packets arrive. Which action resolves the issue?
A. Open SNMP port 161 and NMSP port 16113 on the WLC.
B. Enable Hyperlocation in the Global Configuration settings of the WLC.
C. Wait 60 to 90 minutes for RRM to settle before recording location measurements.
D. Install the software code for the WLC that supports the Hyperlocation module.
Answer: C (LEAVE A REPLY)
Troubleshooting HyperLocation Deployment Issues
Hardware
Poor location accuracy when packets arrive:
Ensure NTP server is up and running.
Ensure the same NTP server is used for syncing time for WLC, MSE and PI.
Ensure that any tilt of APs is recorded accurately within PI maps.
Ensure the accurate azimuth angle is recorded within PI.
Allow 60-90 minutes for RRM to settle before recording location measurements.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_hyperLocation_best_practices_and_troubleshooting_guide.html#id_12692

NEW QUESTION: 67
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. Install a trusted certificate.
B. Enter the correct credentials.
C. Restart the ISE service.
D. Configure NTR.
Answer: D (LEAVE A REPLY)
The "clock skew" error in Cisco ISE occurs when there is a time synchronization mismatch between ISE, the WLC, and Active Directory. To resolve this, NTP must be configured so that all devices use the same time source, ensuring proper certificate validation and successful 802.1X authentication.

NEW QUESTION: 68
What is an indication of having multiple wireless controllers within the same CAPWAP multicast group?
A. CAPWAP packets are fragmented.
B. Multicast traffic is increased throughout the network.
C. Multicast packets are rate-limited to 128 kbps.
D. ACL filtering are used on the first hop router on all VLANs.
Answer: (SHOW ANSWER)

NEW QUESTION: 69
A municipality customer uses a Cisco 5520 Series Wireless Controller for the wireless network.
The customer intends to move the depot of its stores from using legacy bespoke voice-over-Wi-Fi handsets to a VoIP software package running on 5 GHz-capable laptops, tablets, and smartphones. Bluetooth headsets will be used for any voice communication on any data device.
Assuming that a suitable RF site survey for 5 GHz has already been carried out, which two configuration settings ensure the best possible voice experience? (Choose two.)
A. Configure AVC on the controller to prioritize voice over other applications' traffic on the same device.
B. Remark all traffic coming from the new voice-capable devices with DSCP 46 (EF) at the AP.
C. Assign the Platinum QoS profile to the SSID carrying the new-style voice traffic.
D. Create mobility groups and include all the APs in the high-density areas.
E. Turn off the 2.4 GHz radios on all APs where the voice application is used.
Answer: A,C (LEAVE A REPLY)
With the Cisco AVC solution available on wireless controllers from AireOS 7.4 onward, it is possible to identify applications inside the packet and to have a measure of control over them.
Types of control include the following:
- Marking of DSCP
- Rate-limiting/policing traffic in the upstream or downstream direction
- Dropping certain traffic types

NEW QUESTION: 70
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 mode access
mls qos trust cos
B. switchport encapsulation dotlq
switchport mode trunk
mls qos trust device cisco-phone
C. switchport mode access
mls qos trust device cisco-phone
D. switchport mode access
mls qos trust dscp
Answer: D (LEAVE A REPLY)
Enable DSCP trust for Cisco Access Points
mls qos
!
interface X mls qos trust dscp
Reference:
https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/8821/english/Deployment/8821_wlandg.pdf

NEW QUESTION: 71
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: (SHOW ANSWER)
For 2.4-GHz radio:
If interference is less than or equal to 50 percent, the score is 10.
If interference is more than 50 percent, the score is 0.
For 5-GHz radio:
If interference is less than or equal to 20 percent, the score 10.
If interference is more than 20 percent, the score is 0.
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and- management/dna-center-assurance/2-2-2/b_cisco_dna_assurance_2_2_2_ug/b_cisco_dna_assurance_2_2_2_ug_chapter_0110.html

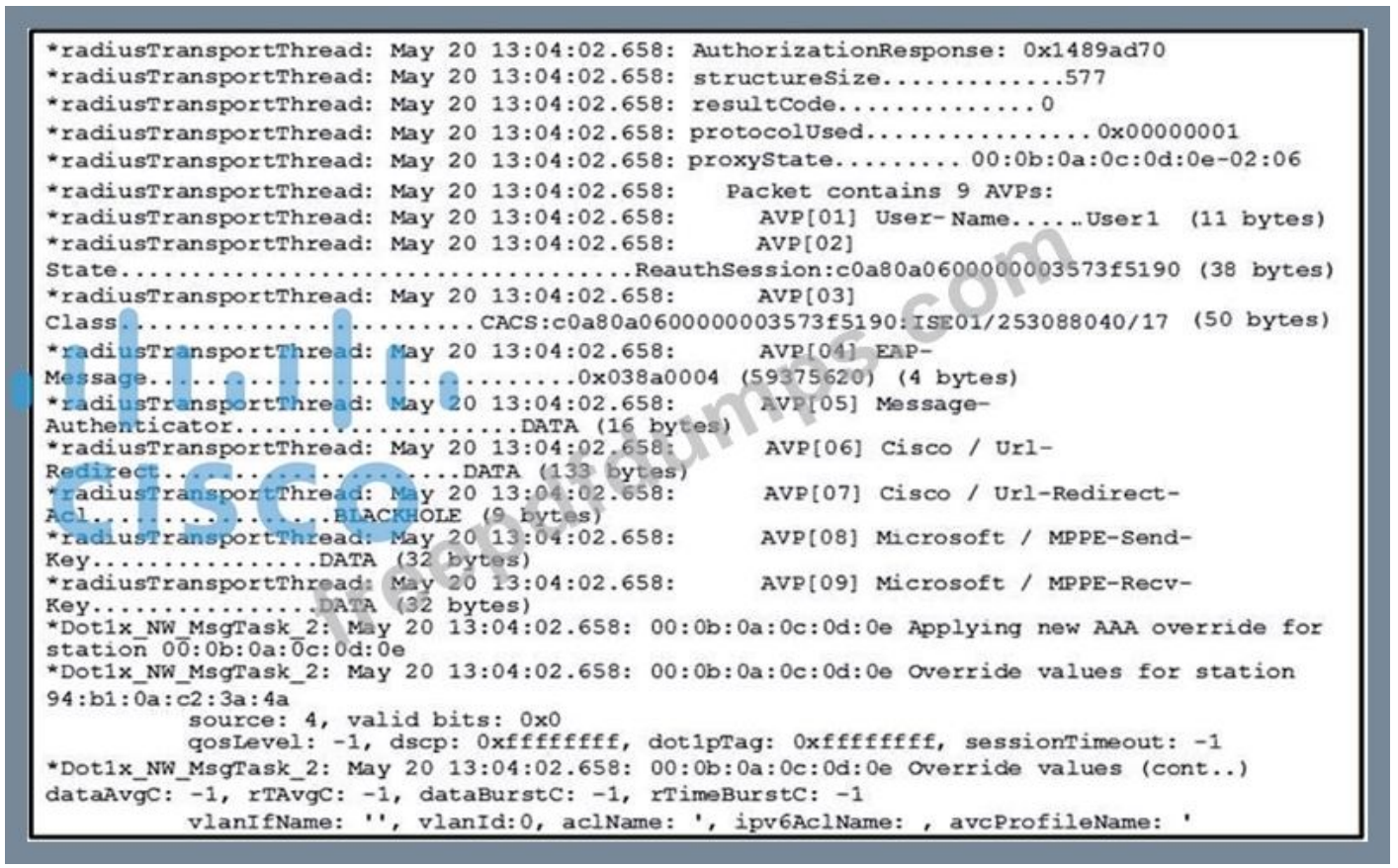
NEW QUESTION: 72
A wireless engineer must implement a corporate wireless network for a large company in the most efficient way possible. The wireless network must support 32 VLANs for 300 employees in different departments. Which solution must the engineer choose?
A. Configure a second WLC to support 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: (SHOW ANSWER)
One of the primary advantage of ISE and 802.1x with COA is to use user groups and put them on the appropriate VLAN after authentication.

NEW QUESTION: 73
An engineer must collect all Cisco CleanAir alarms in a central location for archival purposes.
Which device is configured for collection?
A. Cisco Prime Infrastructure
B. MSE
C. wIPS AP
D. WLC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
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 (LEAVE A REPLY)
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.

NEW QUESTION: 75
Refer to the exhibit. 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 (LEAVE A REPLY)

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.

NEW QUESTION: 76

An engineer configures QoS on an AireOS WLC v8.5. The engineer configures a WLAN for voice traffic and must give a higher priority to WMM clients than to non-WMM clients. Which two configurations should be performed? (Choose two.)

A. Implement the Gold QoS profile.

B. Select Video from the Unicast Default Priority drop-down menu.

C. Implement the Platinum QoS profile.

D. Set Unicast Default Priority to Platinum.

E. Set Multicast Default Priority to Voice.

Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 77
An engineer deploys APs in autonomous mode to provide corporate and guest access in several retail locations. Remote authentication with IEEE 802.1X is configured to ensure a secure wireless connection for corporate users. Which component must be configured as the authenticator?
A. supplicant
B. authentication server
C. APs
D. RADIUS server
Answer: (SHOW ANSWER)

NEW QUESTION: 78
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 (LEAVE A REPLY)
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.

NEW QUESTION: 79
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: (SHOW ANSWER)
Enter the maximum number of Cisco APs to actively contain the rogue client [1-4].
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan- controllers/112045-handling-rogue-cuwn-00.html

NEW QUESTION: 80
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. first the RADIUS server that is mapped for WLAN A, and if authentication fails, it reverts to the RADIUS server that is globally configured
B. RADIUS server that is mapped for WLAN A
C. RADIUS server that is globally configured
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: (SHOW ANSWER)
When a WLAN has a specific RADIUS server mapped, the controller always uses the mapped RADIUS server for client authentication on that WLAN. The globally configured RADIUS server is only used for WLANs that do not have a dedicated server mapping.

NEW QUESTION: 81
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. Bronze
C. Gold
D. Silver
Answer: (SHOW ANSWER)

NEW QUESTION: 82
A wireless network has lightweight APs distributed on multiple buildings and different AP groups.
An administrator reported that AppleTV from one building is discovered in other buildings after it is queried. Why is this happening?
A. AppleTV service is discovered as a wired service provider.
B. mDNS service is configured as a wireless service provider for user access.
C. Lightweight APs incorrectly filter mDNS service for each location.
D. No ACL entry has been deployed to filter mDNS service advertisement between AP groups.
Answer: D (LEAVE A REPLY)
In a wireless network using mDNS (Multicast DNS) for service discovery (like AppleTV), services are typically advertised over multicast. In a controller-based architecture with lightweight APs, mDNS snooping and AP groups help control the visibility and scope of service advertisements.
If AppleTV in one building is being discovered in other buildings after a query, it means the mDNS advertisements are not being filtered or scoped correctly.

NEW QUESTION: 83
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. Install Cisco Spaces Connector on-premises to connect CMX to Cisco Spaces.
C. Download JSON dump of the location hierarchy from CMX and manually upload to Cisco Spaces.
D. Use Cisco WLC Direct Connect feature to connect Catalyst 9800 to Cisco Spaces directly.
E. Establish VPN connection between CMX and Cisco Spaces to transfer the location hierarchy details.
Answer: A,B (LEAVE A REPLY)
The administrator must configure a notification service on CMX that points to Cisco Spaces, so CMX can stream location data to Spaces.
Because the CMX is in a DMZ and not publicly accessible, a Cisco Spaces Connector is required on-premises to securely bridge CMX with Cisco Spaces.
These two steps enable Cisco Spaces to obtain the location hierarchy and provide detect and locate functionality.

NEW QUESTION: 84
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 UDP any any
B. Permit 0.0.0.0 0.0.0.0 any DNS any
C. Permit 0.0.0.0 0.0.0.0 UDP DNS any
D. Permit 0.0.0.0 0.0.0.0 UDP any DNS
E. Permit any any any
Answer: (SHOW ANSWER)

Seq	Action	Source IP/Mask		Destination IP/Mask		Protocol	Source Port	Dest Port
1	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0		UDP	DNS	Any
2	Permit	0.0.0.0 0.0.0.0	/	0.0.0.0 0.0.0.0	/	UDP	Any	DNS

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

NEW QUESTION: 85
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?

```
import requests

url = "https://<catalyst-center-ip>/dna/intent/api/v1/event/webhook"

payload = {
    "name": "APUsageWebhook",
    "url": "https://example.com/webhook?event_type=report_complete",
    [                                                              ]
    },
    "events": [
        {"eventId": "REPORT.COMPLETION"},
        {"eventId": "REPORT.DATA_UPDATE"}
    ],
    "trustCert": True
}

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

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

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

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

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

D.

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

Answer: (SHOW ANSWER)

The requirements are:

- Method must be PUT (webhook creation/update in Catalyst Center API).
- Content-Type must be application/json (payload format).
- X-API-Key must be xyz789 (API key).
- X-Source must be CiscoDNAC (custom identifier).

NEW QUESTION: 86

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 AVVID priority mapping on all the Aps.

Answer: C (LEAVE A REPLY)

In autonomous AP deployments, there is no centralized controller to enforce QoS. To ensure VoWLAN signaling and RTP traffic are prioritized, EDCA (Enhanced Distributed Channel Access) parameters must be configured on each AP. This optimizes wireless access categories for voice and video, ensuring end-to-end QoS between wired and wireless networks.

NEW QUESTION: 87

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 > Client Provisioning > Client Provisioning Policy > Add

C. Policy > Policy Elements > Profiling > Add

D. Policy > Posture > Posture Profile > Add

Answer: A (LEAVE A REPLY)

To group users by their endpoints and assign them to identity groups in Cisco ISE, Profiling Policies are used. The correct configuration path is Policy > Profiling > Profiling Policies > Add, where endpoints can be profiled and associated with identity groups for applying the required policy profiles.

NEW QUESTION: 88

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 (LEAVE A REPLY)

We usually create this type of pre-authentication ACL for web authentication. Such an ACL could be used to allow certain types of traffic before authentication is complete.

NEW QUESTION: 89

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 setting must be enabled for this functionality?

A. Northbound Notification

B. Message of the Day

C. Session Announcement State

D. SNMP Trap Log

Answer: (SHOW ANSWER)

NEW QUESTION: 90

Refer to the exhibit. An administrator configures CPU ACLs on the AireOS WLC to implement security. After configuration, administrative users cannot access the user interface. Where must HTTP and HTTPS traffic be allowed on the ACLs, based on the configuration?

```
(Cisco Controller) >show interface summary

 Number of Interfaces..... 4

Interface Name                   Port Vlan Id  IP Address      Type    Ap Mgr Guest
-------------------------------- ---- -------- --------------- ------- ------ -----
dead                             3    999      1.2.3.4         Dynamic No     No
labnetwork                       3    272      192.168.172.40  Dynamic No     No
management                       3    10       172.18.254.249  Static  Yes    No
virtual                          N/A  N/A      192.0.2.2       Static  No     No

(Cisco Controller) >
(Cisco Controller) >show acl detailed CPU_ACL_LIST

                 Source                  Destination                Source Port Dest Port
Index  Dir  IP Address/Netmask       IP Address/Netmask        Prot  Range      Range     DSCP  Action  Counter
------ ---- ------------------- ------------------------------ ---- ---------- ---------- ----- ------- -------
     1 Any    0.0.0.0/0.0.0.0    192.168.172.40/255.255.255.255  Any   0-65535    0-65535  Any Permit       0
     2 Any    0.0.0.0/0.0.0.0    172.18.254.249/255.255.255.255    6   0-65535   22-22     Any Permit       0
     3 Any    0.0.0.0/0.0.0.0          0.0.0.0/0.0.0.0           Any   0-65535    0-65535  Any   Deny       0
```

A. on the service port of management traffic

B. on the management interface

C. on the dynamic interface

D. on the virtual interface
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
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. Enable Locally Administered MAC Filtering
C. Enable Location MAC Filtering
D. Duty Cycle Cutoff
Answer: (SHOW ANSWER)
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:
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

NEW QUESTION: 92
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: (SHOW ANSWER)
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.

NEW QUESTION: 93

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 in 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 Wireless Protection Rules

B. AP Security

C. AP Access Control

D. AP Authentication

Answer: D (LEAVE A REPLY)

In a wireless network with multiple controllers and APs, AP Authentication is the appropriate protection type to ensure that rogue containment is deployed without being affected by RRM (Radio Resource Management) neighbor packets sent by friendly APs. AP Authentication ensures that only authorized APs are allowed to join the network, preventing rogue APs from connecting.

AP Authentication verifies the identity of APs attempting to join the network, ensuring they are legitimate and authorized. This prevents rogue APs from being added to the network and ensures that RRM neighbor packets are only sent by trusted APs.

NEW QUESTION: 94

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

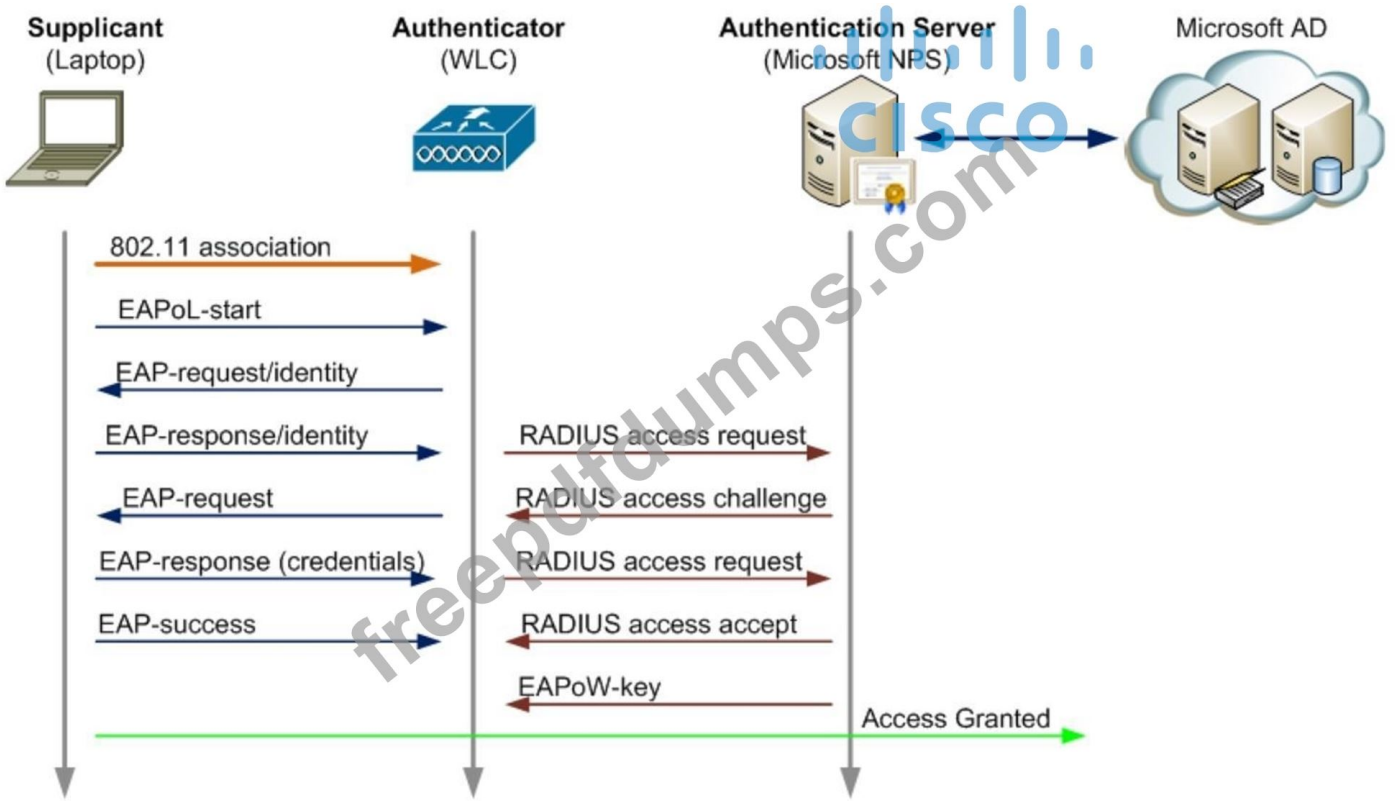
B. 802.1X

C. RADIUS

D. WPA2

Answer: C (LEAVE A REPLY)

EAP is exchanged between supplicant and authenticator and RADIUS Is used between authenticator and Auth server.



NEW QUESTION: 95

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. Enable the virtual IP address of the primary server.

B. Insert the cmxadmin password of the secondary server.

C. Place primary and secondary servers in different subnets.

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

Answer: B (LEAVE A REPLY)

NEW QUESTION: 96

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: D (LEAVE A REPLY)

When you enter the mls qos trust cos command on a port, the switch uses the CoS marking on incoming packets in order to put the packet in the right queue. When the packet is resent, the switch makes the DSCP value correspond to the CoS.
https://www.cisco.com/c/en/us/support/docs/wireless-mobility/voice-over-wireless-lan- vowlan/116056-technote-qos-00.html#anc3

NEW QUESTION: 97
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 on ISE as the one performing the RADIUS authentication requests for the web authentication method?
A. authentication server
B. anchor controller
C. foreign controller
D. APs
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
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. The CleanAir configuration model must be applied to a wireless network profile.
B. Enable Neighbor List Dual Band on the configured WLANs.
C. Configure the RX SOP threshold to be high.
D. Disable Persistent Device Propagation in the CleanAir configuration model.
E. Enable CleanAir Device Reporting in the CleanAir configuration model.
Answer: (SHOW ANSWER)
The CleanAir configuration model must be applied to a wireless network profile so that Cisco Catalyst Center can manage and enforce interference mitigation policies.
Enabling CleanAir Device Reporting ensures that interference information from APs is collected and reported back to Cisco Catalyst Center, allowing visibility and management of interferers.

NEW QUESTION: 99
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. RADIUS server overwrite interface
B. AAA override
C. WLAN local policy
D. custom AVC profile
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 100

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: C (LEAVE A REPLY)

The Cisco CMX Presence Analytics service is a comprehensive analytics and engagement platform that uses APs to detect visitor presence based on their mobile devices' Received Signal Strength Indication (RSSI). The AP detects these client mobile devices irrespective of the latter's wireless association state as long as they are within the specified signal range, and the wireless option is enabled on the mobile device (ability to detect devices wirelessly even if they are not connected to the network

https://www.cisco.com/c/en/us/td/docs/wireless/mse/10-4/cmx_config/b_cg_cmx104/the_cisco_cmx_presence_analytics_service.html

NEW QUESTION: 101

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. SSL

D. LDAP

Answer: A (LEAVE A REPLY)

The controller makes use of the Simple Certificate Enrollment Protocol (SCEP) to forward certReqs generated on the devices to the CA and makes use of SCEP again to get the signed certificates from the CA.

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

NEW QUESTION: 102

A customer recently upgraded the network to Cisco SD-Access. Cisco DNA Center manages the wireless network; all SSIDs are Fabric-enabled. Cisco DNA Center must be able to classify ogue on Wire" APs. Which action must the customer take?

A. Allow SNMPv3 between Cisco DNA Center and access switches.

B. Connect APs to the network using a trunk port with native VLAN.

C. Disable all the DCA channels under RRM on the WLC.

D. Configure all access switches to be managed by Cisco DNA Center.

Answer: (SHOW ANSWER)

NEW QUESTION: 103

An engineer can log in to a WLC but cannot log in to the AP. Which configuration change allows the engineer to log in to the AP without changing the global login policy?

A. Change the WLC password.

B. Set up AAA override.

C. Override the credentials.
D. Reload the WLC.
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which Cisco Prime Infrastructure report does an engineer run to troubleshoot client connectivity issues for a VoWiFi network?
A. Airtime Fairness Statistics
B. Up/Down Statistics
C. Traffic Stream Metrics
D. 802.11 Counters
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
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 (LEAVE A REPLY)
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.

NEW QUESTION: 106
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 (LEAVE A REPLY)
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.

NEW QUESTION: 107
Which two steps are needed to complete integration of the MSE to Cisco Prime Infrastructure and be able 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 configured during set up.
D. Apply a valid license for Wireless Intrusion Prevention System.
E. Apply a valid license for location tracking.
Answer: C,E (LEAVE A REPLY)
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.

NEW QUESTION: 108
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. port channel
C. class map
D. ACL
Answer: (SHOW ANSWER)
In QoS configurations, the class map is required to identify and classify traffic flows before applying a policy map. Without the class map, the policy map has no defined traffic classes to match against, which leads to incorrect or missing QoS markings in the end-to-end traffic flow.

NEW QUESTION: 109
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: (SHOW ANSWER)
Cisco Connected Mobile Experiences (CMX) is a smart Wi-Fi solution that uses the Cisco wireless infrastructure to provide location services and location analytics for consumers' mobile devices.

NEW QUESTION: 110
What must be configured on ISE version 2.1 BYOD when using Single SSID?
A. no authentication
B. WPA2
C. open authentication
D. 802.1x
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 111
An engineer must implement multicast on an AireOS WLC v8.2 that has 200 LWAPs connected.
Reliable reception is a main requirement of this implementation. Which wireless configuration must be performed?
A. Increase the coverage cell.
B. Decrease the coverage cell.
C. Disable lower mandatory data rates.
D. Disable higher mandatory data rates.
Answer: (SHOW ANSWER)

NEW QUESTION: 112
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 connects the issue?
A. controller IGMP snooping
B. multicast AP multicast mode
C. broadcast forwarding
D. unicast AP multicast mode
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 113
An engineer is trying to log in to their lightweight access point joined to a WLC that does not have AP credentials defined. Which credentials does the engineer use?
A. admin/Cisco123
B. Cisco/Cisco
C. TACACS credentials
D. AP Global Configuration configured credentials
Answer: (SHOW ANSWER)

Lab Exercise (9800-CL, 17.3.7):
Configuration > Tags & Profiles > AP Join > edit "AP Join Profile Name" > Management > Device ssh disbaled by default // telnet disbaled by default set to enable leads to the following error message
"Error in Configuring AP JOIN PROFILE - AP SSH access enable config is not allowed with AP user management credentials set to default"
Configuration > Tags & Profiles > AP Join > edit "AP Join Profile Name" > Management > User > fill in user data! (i.e. ap-maneger // Password // Secret) Configuration > Tags & Profiles > AP Join > edit "AP Join Profile Name" > Management > Device > enable ssh // dont enable telnet Login via serial console, use AP Global Configuration configured credentials (i.e. ap-maneger // Password // Secret) --> it works!
Login via ssh, use AP Global Configuration configured credentials (i.e. ap-maneger // Password // Secret) --> it works!

NEW QUESTION: 114
An engineer is configuring the maps on the Cisco Prime Infrastructure, but clients fail to show up on the maps. Which two actions are needed to complete this configuration? (Choose two.)
A. Install wIPS licenses on the Cisco MSE.
B. Install event group services in Cisco Prime Infrastructure.
C. Synchronize the Cisco WLC with Cisco Prime Infrastructure.
D. Synchronize the network designs with the Cisco MSE.
E. Activate the context-aware service on the Cisco MSE.
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 115
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 group BranchA-FCG vlan add 30
C. config flexconnect group BranchA-FCG vlan 30 add
D. config flexconnect BranchA-FCG vlan add 30
Answer: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/flexconnect_groups.html

NEW QUESTION: 116
What is configured to use more than one port on the OEAP to extend the wired network's?
A. AAA override
B. client load balancing
C. remote LAN ACL
D. remote LAN
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 117

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

A. LinkedIn
B. Pinterest
C. Medium
D. Google+
E. Facebook
F. Myspace

Answer: A,D,E (LEAVE A REPLY)

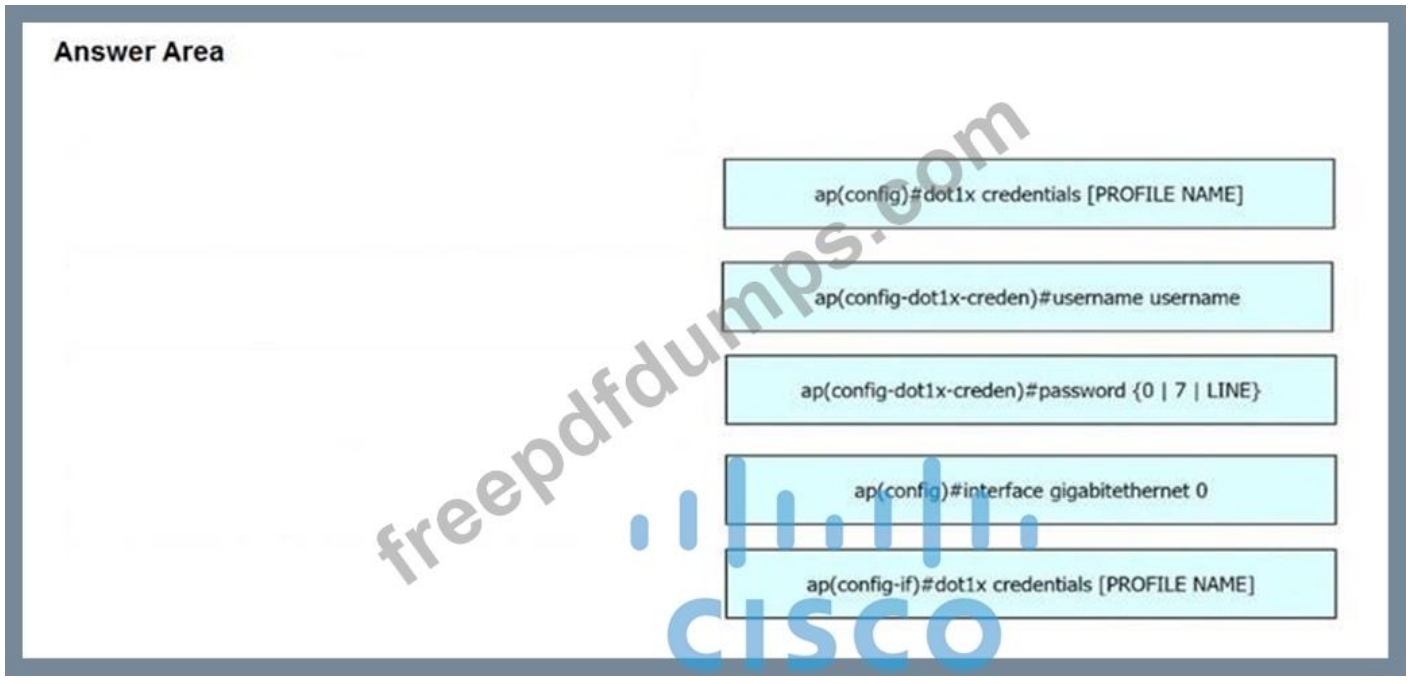
Cisco CMX Visitor Connect supports various social connectors for guest network login. The configurable social connectors include LinkedIn, Google+, and Facebook, but not Pinterest, Medium, or Myspace.

NEW QUESTION: 118

Drag and Drop Question

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:



NEW QUESTION: 119
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 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: (SHOW ANSWER)

NEW QUESTION: 120
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. IPv6 ACL
C. multicast address
D. DNS server
E. DSCP value
Answer: (SHOW ANSWER)
The AAA Override option of a WLAN enables you to configure the WLAN for identity networking.
It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.
AAA Override for IPv6 ACLs
In order to support centralized access control through a centralized AAA server such as the Cisco Identity Services Engine (ISE) or ACS, the IPv6 ACL can be provisioned on a per-client basis using AAA Override attributes. In order to use this feature, the IPv6 ACL must be configured on the controller

and the WLAN must be configured with the AAA Override feature enabled. The actual named AAA attribute for an IPv6 ACL is Airespace-IPv6-ACL-Name, which is similar to the Airespace-ACL-Name attribute that is used for provisioning an IPv4-based ACL. The AAA attribute returned contents should be a string equal to the name of the IPv6 ACL as configured on the controller.

NEW QUESTION: 121
Refer to the exhibit. A company is implementing Cisco ISE and IBN for their WLAN. The pictured IBN profile is applied to BYOD devices that are not registered to the Mobile Device Manager.
Which advanced setting must be enabled on the WLAN to allow the policy to work correctly?

```
Access Type = ACCESS ACCEPT
cisco-av-pair = url-redirect-acl=BYOD NO MDM
cisco-av-pair = url-redirect=https://ip:port./mdmportal/gateway/
                ?sessionId=SessionIdValue&portal=28c37510-e96e-11e4-a30a-005056bf01c9&mdmServerId=
                28c4e2b08e14-11e5-b068-005056173d5&action=mdm
Airespace-Interface-Name = byod group
```

A. RADIUS profiling
B. allow AAA override
C. Aironet IE
D. static IP tunneling
Answer: B (LEAVE A REPLY)

NEW QUESTION: 122
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. WLAN static IP tunneling
B. FlexConnect local switching
C. OEAP split tunnel
D. OEAP gateway override
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 123

An engineer configures an ACL on a Cisco WLC v8.7. The engineer must control IPv4 traffic to the CPU of the controller. The engineer updates the ACL via the GUI and has to define the direction in which the ACL must be applied. Which value should be applied to the direction option?

A. None

B. Any

C. Outbound

D. Inbound

Answer: D (LEAVE A REPLY)

NEW QUESTION: 124

An engineer just added a new MSE to Cisco Prime Infrastructure and wants to synchronize the MSE with the Cisco 5520 WLC, which is 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 can communicate using NMSP?

A. TCP 1613

B. UDP 16113

C. TCP 16113

D. UDP 1613

Answer: C (LEAVE A REPLY)

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.

NEW QUESTION: 125

A company uses Cisco ACS to provide AAA services to network devices. The company recently replaced Cisco ACS with Cisco ISE that runs TACACS+. An IT administrator notices that the Work Centers option that contains the device administration pages is unavailable. Which action resolves the issue?

A. Configure a shared secret key in Cisco ISE.

B. Enable the Work Centers option for AAA.

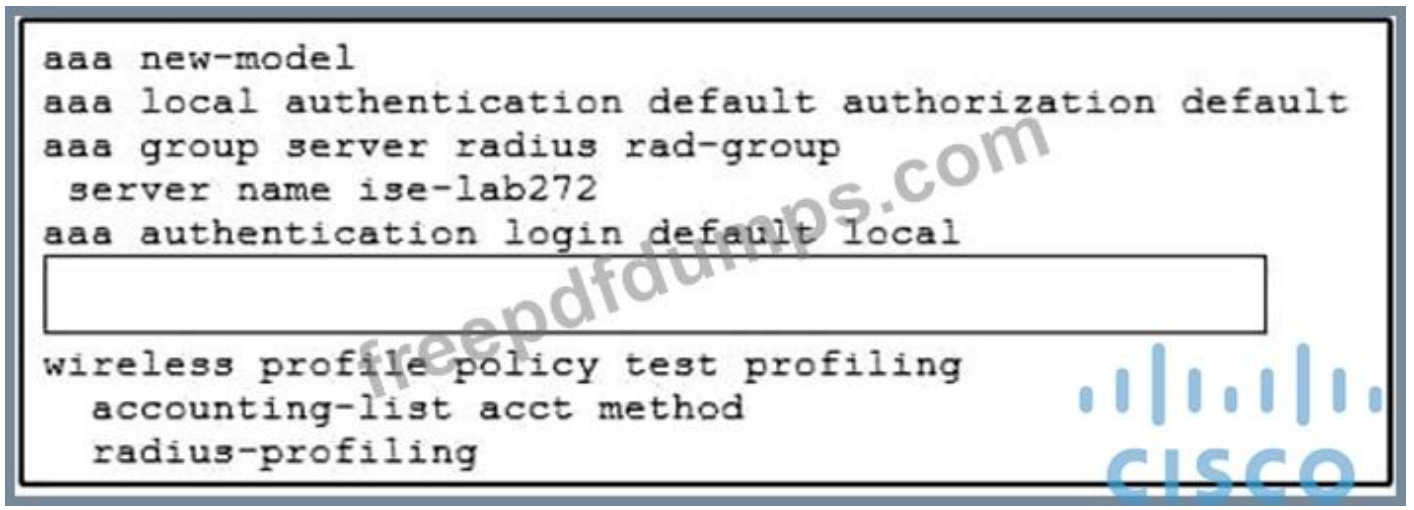
C. Install TACACS+ licenses.

D. Open ports 1812 and 1813.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 126

Refer to the exhibit. 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 (LEAVE A REPLY)
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.

NEW QUESTION: 127
More people are working from home, so an engineer must configure OEAPs to support the users.
The security team already configured NAT with a public IP address that points to the internal WLC IP address. The APs also have been configured with the public WLC IP address, but APs cannot join the controller yet. Which action resolves this issue?
A. Configure the internal WLC IP address on the OEAPs.
B. Create an ACL in WLC to accept the OEAPs.
C. Enable NAT on the WLC to configure the public IP address.
D. Configure the public WLC IP address on the home router.
Answer: C (LEAVE A REPLY)
You need to select the management interface on the WLC and click the NAT checkbox. Then enter the public NAT IP. In this case it would be the public NAT IP that the security team created.

NEW QUESTION: 128
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 as the admin user before restarting ntpd by using service ntpd restart.
B. Log in to the Cisco CMX CLI and issue set ntp server NTP_IP where NTPJP is the IP of the NTP server.
C. 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.
D. Manually edit /etc/ntp.conf using an XML editor before restarting the server by using service restart all services.

Answer: A (LEAVE A REPLY)
https://www.cisco.com/c/en/us/support/docs/wireless/connected-mobile-experiences/200906- Troubleshooting-CMX-connectivity-with-WL.pdf

NEW QUESTION: 129
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 (LEAVE A REPLY)
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.

NEW QUESTION: 130
An engineer must send Cisco OEAPs to the homes of employees. The APs must be able to discover and join the WLC when they connect to each employee home network. Which action accomplishes this task?
A. Use the WLC name and management IP address to configure the OEAPs.
B. Use the OEAP management IP address to listen for discovery broadcasts from the WLC.
C. Use the WLC name and management IP address to configure the DNS server.
D. Use DHCP Option 43 to configure the WLAN name and management IP address.
Answer: (SHOW ANSWER)
Configure one or more controllers for the access point as follows:
Click the High Availability tab.
Enter the name and IP address of the primary controller for this access point in the Primary Controller Name and Management IP Address text boxes.

NEW QUESTION: 131
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 > Security > AAA > Authentication > AAA Method List
B. Configuration > Tags & Profiles > AP Join > default-ap-profile
C. Configuration > Wireless > AP Global Config
D. Configuration > Security > AAA > AAA Advanced > AP Policy
Answer: D (LEAVE A REPLY)
On a Cisco Catalyst 9800 WLC, even after adding AP MAC addresses to the local list, AP Authorization must be explicitly enabled under Security > AAA > AAA Advanced > AP Policy. This ensures that AP join requests are checked against the MAC authorization list before being allowed to register with the controller.

NEW QUESTION: 132

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 (LEAVE A REPLY)

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.

NEW QUESTION: 133

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: (SHOW ANSWER)

FlexConnect Groups is needed for CCKM to work. Flex group needs to be created for CCKM, 11r , and OKC , only then the caching can happen on an AP. The group name must be same between APS for a fast roaming to happen for 11r/CCKM. The group can be different for OKC as final check is done at Cisco WLC.

NEW QUESTION: 134

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?

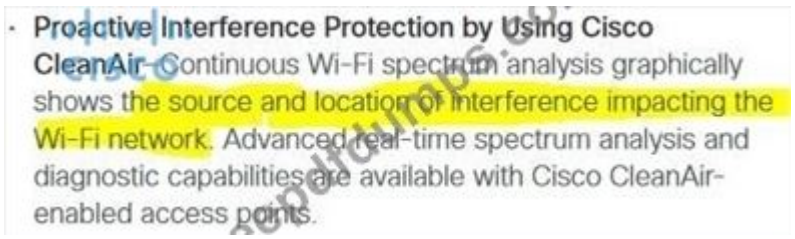
A. CleanAir reports on Cisco Prime Infrastructure

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

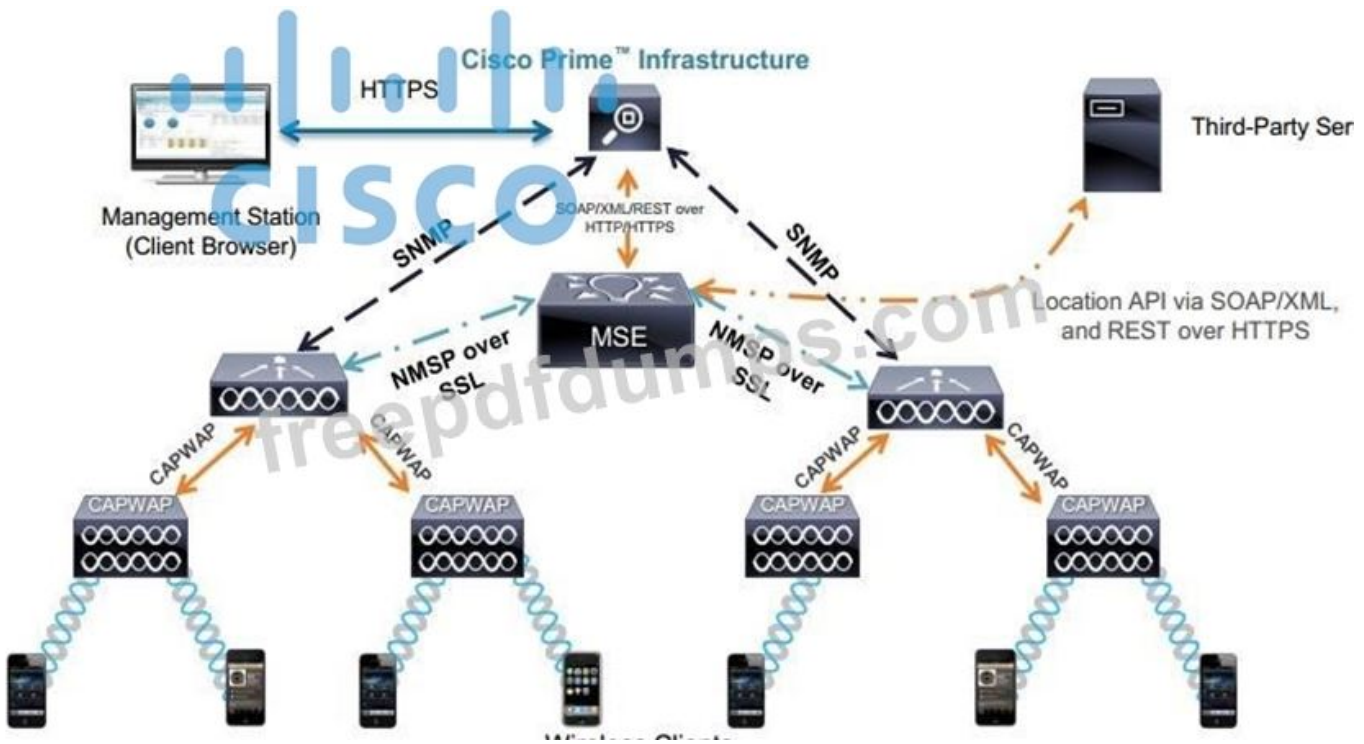
Answer: A (LEAVE A REPLY)



https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Apr2014/CVD-CampusCleanAirDesignGuide-APR14.pdf

NEW QUESTION: 135
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: (SHOW ANSWER)
https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-7/config-guide/b_cg87/flexconnect.html

NEW QUESTION: 136
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,C (LEAVE A REPLY)



NMSP is just used between MSE and WLC.

https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/113344- cuwn-ppm.html#anc5

NEW QUESTION: 137

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. Connected

C. Lightweight

D. Standalone

Answer: D (LEAVE A REPLY)

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. 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.

NEW QUESTION: 138

Refer to the exhibit. An engineer receives a report that a client cannot authenticate via phone in a secure WLAN. The phone uses Layer 2 Security WPA2, and other clients can authenticate successfully. The engineer issues the (CONTROLLER) >debug client 64:89:9a:31:7f:a1 and (CONTROLLER) >debug aaa all enable commands in the controller and sees this output. What are two sources of this issue? (Choose two.)

A. RADIUS is incorrectly configured

B. The incorrect EAP method was configured on the client device.

C. An invalid user account or password was used.

D. The server certificate is expired or not in use

E. Certificate services are not working properly.

Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 139

An engineer implements QoS on an AireOS WLC v8.3. When configuring AVC on a WLAN, the engineer must configure the appropriate AVC profile for a Cisco Wireless IP Phone 8821, Which command must be used?

A. config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 46

B. config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 48

C. config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 56

D. config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 41

Answer: A (LEAVE A REPLY)

NEW QUESTION: 140

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 (LEAVE A REPLY)

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:

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

NEW QUESTION: 141

A network engineer must deploy a Cisco wireless solution for 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. Client Provisioning
B. Authorization Profiles
C. Profiling
D. Allowed Protocols
Answer: B (LEAVE A REPLY)
In Cisco ISE, Authorization Profiles define post-authentication policies such as VLAN assignment, ACLs, and QoS. To place different user groups into their own VLANs after authentication, the engineer must configure Authorization Profiles with the appropriate VLAN settings and apply them to the group-based authorization rules.

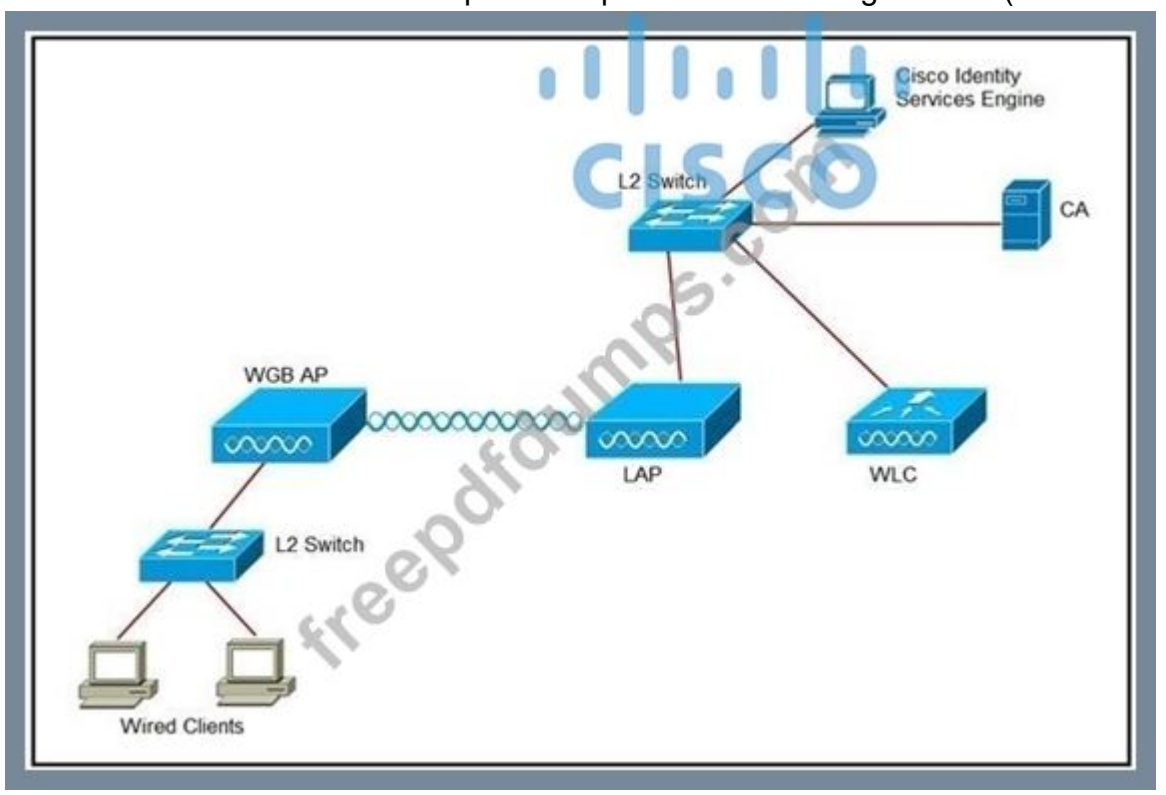
NEW QUESTION: 142
An engineer completes the setup of a two-node Cisco ISE deployment for a guest portal. When testing the portal, the engineer notices that sometimes there is a certificate CN mismatch. Which certificate type helps resolve this issue?
A. Public-Signed Root
B. Self-Signed Standard
C. Public-Signed SAN
D. Self-Signed Wildcard
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 143
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 multicast mode
B. mobility group unicast messaging
C. global unicast messaging
D. mobility group multicast messaging
E. global symmetric mobility messaging
Answer: A,D (LEAVE A REPLY)
Mobility group messaging involves controllers exchanging client context and roaming information.
By default, mobility messages can be sent as unicast or multicast.
Using multicast messaging (both globally and within the mobility group) reduces bandwidth usage because messages are sent once to a multicast group rather than individually to each controller.
Global multicast mode enables multicast forwarding for various wireless services, improving efficiency.

NEW QUESTION: 144
Which QoS level is recommended for guest services?
A. gold

B. bronze
C. platinum
D. silver
Answer: (SHOW ANSWER)
- Platinum (voice): Assures a high QoS for voice over wireless.
- Gold (video): Supports high-quality video applications.
- Silver (best effort): Supports normal bandwidth for clients.
- Bronze (background): Provides the lowest bandwidth for guest services.

NEW QUESTION: 145
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: (SHOW ANSWER)
https://mrncciew.com/2018/05/25/wgb-with-peap/

NEW QUESTION: 146
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: D (LEAVE A REPLY)
https://community.cisco.com/t5/wireless/office-extend-ap-and-external-addresses/td-p/3742395

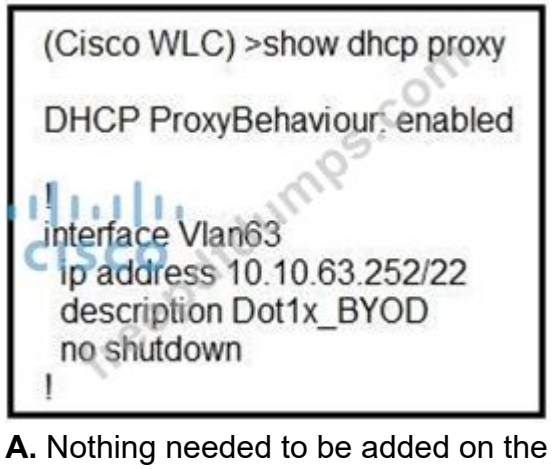
NEW QUESTION: 147
An engineer configures a WLC and 20 Cisco OEAPs. The engineer must configure a remote LAN that uses WPA2 Enterprise security. How should the LAN be configured?
A. on the WLC via the CLI
B. on the OEAP via the GUI
C. on the anchor WLC via the GUI
D. on the OEAP via the CLI
Answer: (SHOW ANSWER)
For Cisco OfficeExtend APs (OEAPs), remote LANs are configured directly on the OEAP itself through the GUI. This allows the administrator to define a wired SSID (Remote LAN) with WPA2 Enterprise security for wired devices connected to the OEAP's LAN ports, independent of the central WLC configuration.

NEW QUESTION: 148
An engineer is adding APs to an existing VoWLAN 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 (LEAVE A REPLY)
With RRM, if more APs were added to an area, the power to each AP would decrease as it would detect that the APs would be talking over each other.

NEW QUESTION: 149
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. Allow HTTP and DHCP profiling under policy map.
B. Enable device classification on global wireless settings.
C. Add local profiling policy under global security policy settings
D. Assign a policy map under global security policy settings.
E. Create a service template
Answer: B,E (LEAVE A REPLY)

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.

NEW QUESTION: 150
Refer to the exhibit. 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 (LEAVE A REPLY)
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.

NEW QUESTION: 151
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 (LEAVE A REPLY)
Describe basic RF deployment considerations related to site survey design of data or VoWLAN applications, common RF interference sources such as devices, building material, AP location, and basic RF site survey design related to channel reuse, signal strength, and cell overlap. If an AP fails, channel reuse in the design is not going to help you if there is no coverage. Cell overlap will, because more than one AP will cover a given area.

NEW QUESTION: 152
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: (SHOW ANSWER)
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.

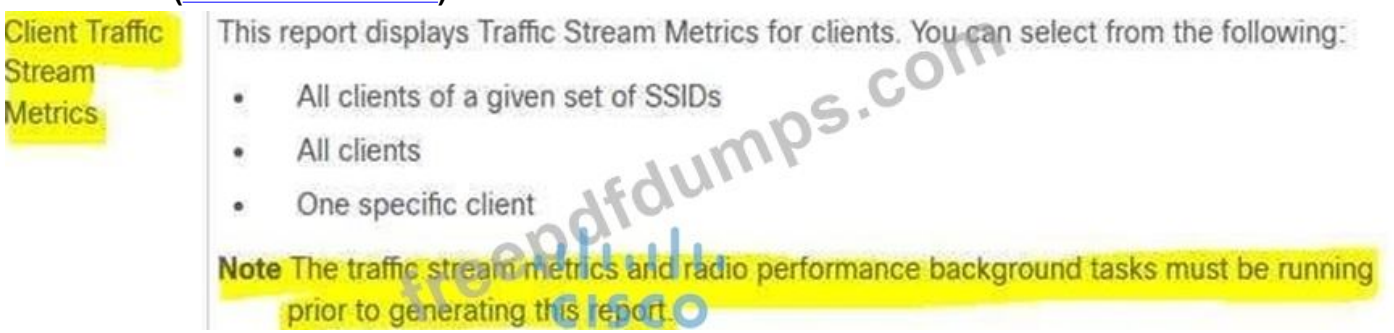
NEW QUESTION: 153
Which two configurations are applied on the WLC to enable multicast, check multicast stream subscriptions, and stream content only to subscribed clients? (Choose two)
A. Enable broadcast forwarding
B. Enable 802.3x flow control mode.
C. Set the IGMP timeout to 180 seconds
D. Enable IGMP snooping
E. Set the AP multicast to 238.255.255.255
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 154
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. RADIUS IP address
B. Username and password
C. Group name
D. Shared secret
E. PAC encryption key
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 155
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 the AAA Override option on the policy profile.
B. Configure the DHCP Required option on the policy profile.
C. Enable iPSK on the WLAN.
D. Configure an accounting list on the policy profile.
Answer: (SHOW ANSWER)
For Identity PSK (iPSK) to function on a Cisco Catalyst 9800 WLC, it must be explicitly enabled on the WLAN. This allows the controller to validate multiple PSKs tied to different client identities, as configured in the RADIUS server. Without enabling iPSK on the WLAN, authentication will fail even if the rest of the configuration is correct.

NEW QUESTION: 156
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. software
D. client status
Answer: B (LEAVE A REPLY)



NEW QUESTION: 157
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: (SHOW ANSWER)

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.

NEW QUESTION: 158
Refer to the exhibit. A wireless engineer has integrated the wireless network with a RADIUS server. Although the configuration on the RADIUS is correct, users are reporting that they are unable to connect. During troubleshooting, the engineer notices that the authentication requests are being dropped. Which action will resolve the issue?

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

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

NEW QUESTION: 159
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,E (LEAVE A REPLY)

Restrictions for Configuring Multicast DNS

- mDNS over IPv6 is not supported.
- mDNS snooping is not supported on access points in FlexConnect mode in a locally switched WLAN and mesh access points multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.
- mDNS is not supported on remote LANs.

NEW QUESTION: 160
An administrator is querying the Cisco CMX server through REST API for active client data to build an application. Cisco CMX supports the use of version 3 of REST API to query for active clients in the network. While testing to retrieve information using the API, no results are received.
Which configuration is required for authentication against the API?
A. cmxos apiserver user add

B. cmxos v3 apiserver user add
C. cmxctl apiserver user add
D. cmxctl v3 apiserver user add
Answer: A (LEAVE A REPLY)

NEW QUESTION: 161
An engineer is concerned that a wireless attack is causing client connectivity issues. Which Cisco Prime Infrastructure report does the engineer run to determine if the user was in an area afflicted by a large number of attacks?
A. AVC Troubleshooting
B. NetFlow v7
C. Adaptive wIPS Top 10 APs
D. New Rogue APs
Answer: (SHOW ANSWER)