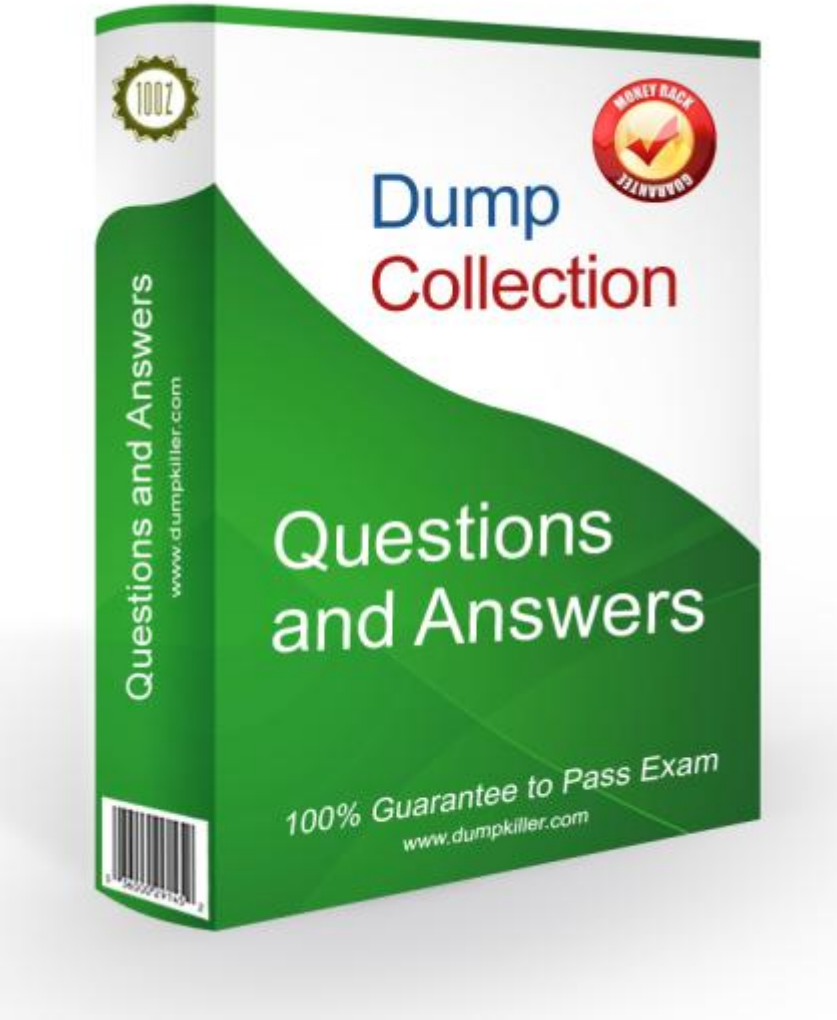
DumpCollection

IT Exam Training online / Bootcamp



http://www.dumpcollection.com

PDF and Testing Engine, study and practice

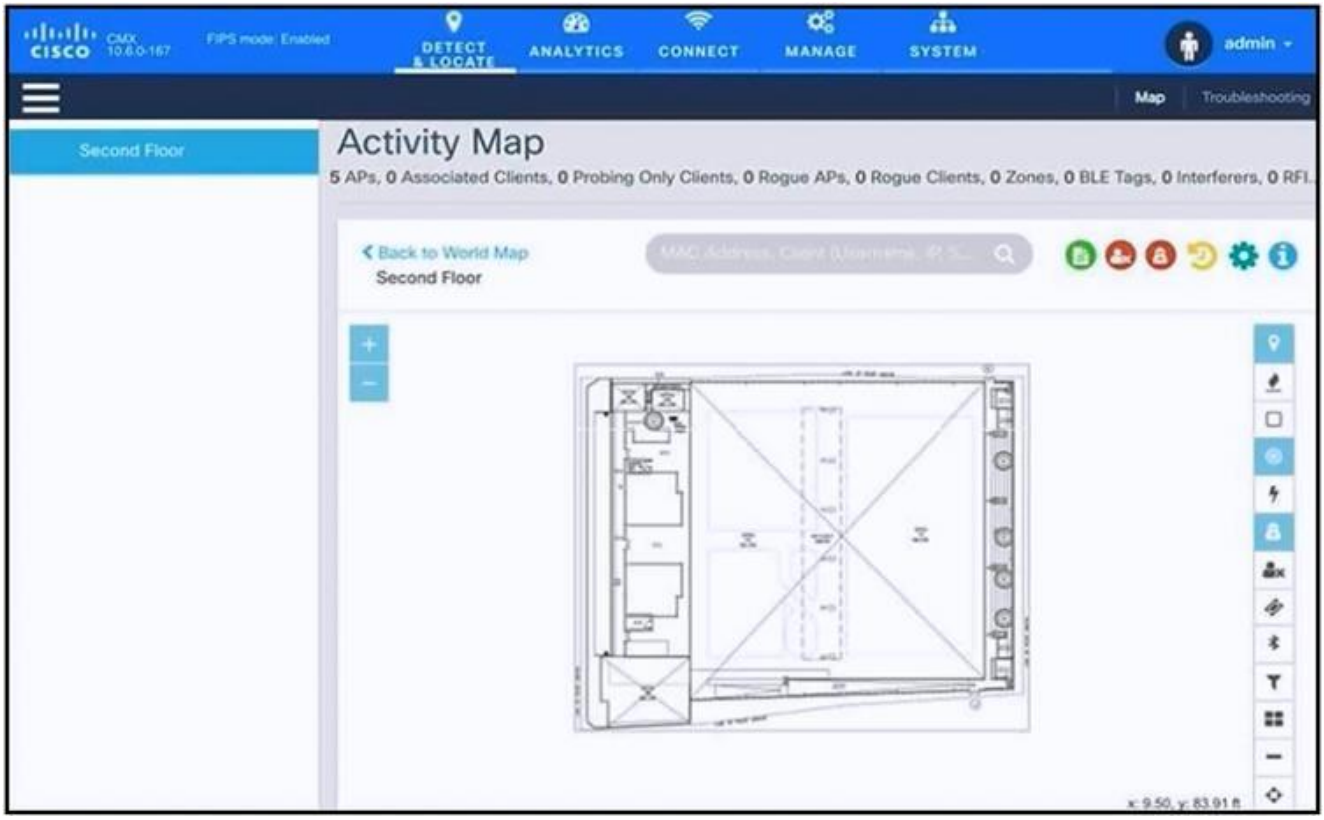
Exam : **300-430**

Title : Implementing Cisco Enterprise Wireless Networks

Vendor : Cisco

Version : DEMO

QUESTION NO: 1
Refer to the exhibit. An engineer has deployed the Cisco CMX solution to track and detect the number of users who visit the office each day. The CMX dashboard is not showing any data.
Which action resolves this issue?



A. Configure Single Sign-On authentication.
B. Add the WLCs to CMX.
C. Copy the exported Maps from CMX server to PI using SCP.
D. Install an evaluation license to CMX server.
Answer: B
Explanation:
The issue with the Cisco CMX dashboard not showing any data can be resolved by integrating the Wireless LAN Controllers (WLCs) with the CMX system. The CMX solution relies on data from the WLCs to track and detect users' presence in the office area. Without the WLCs being added to CMX, the system cannot collect the necessary analytics and location data for its operations.

QUESTION NO: 2
Branch wireless users report that they can no longer access services from head office but can access services locally at the site.
New wireless users can associate to the wireless while the WAN is down.
Which three elements (Cisco FlexConnect state, operation mode, and authentication method) are seen in this scenario? (Choose three.)
A. authentication-local/switch-local
B. WPA2 personal

C. authentication-central/switch-central
D. lightweight mode
E. standalone mode
F. WEB authentication
Answer: ABE

QUESTION NO: 3
A multitenant building contains known wireless networks in most of the suites. Rogues must be classified in the WLC. How are the competing wireless APs classified?
A. adhoc
B. friendly
C. malicious
D. unclassified
Answer: B

QUESTION NO: 4
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 configured before the average data rate.
B. The burst data rate should be greater than or equal to the average data rate.
C. Data rates should be applied per AP radio.
D. The burst data rate should be set to a non-zero value.
Answer: B

QUESTION NO: 5
An engineer must configure MSE to provide guests access using social media authentication. Which service does the engineer configure so that guests use Facebook credentials to authenticate?
A. Visitor Connect
B. Client Connect
C. Social Connect
D. Guest Connect
Answer: C
Explanation:
To provide guests access using social media authentication, the engineer must configure the "Social Connect" service. This service allows guests to use their Facebook credentials, among other social media platforms, to authenticate and gain network access. It simplifies the guest access process by leveraging existing social media accounts for authentication.

QUESTION NO: 6
An engineer has implemented advanced location services for a retail wireless deployment. The marketing department wants to collect user demographic information in exchange for guest WLAN access and to have a customized portal per location hosted by the provider.

Which social connector must be tied into Cisco CMX to provide this service?

A. Gmail

B. Google+

C. Facebook

D. MySpace

Answer: C

Explanation:

- Facebook Wi-Fi:
  - Allows the administrator of a facility to enable the facility's Facebook page as a free Wi-Fi hotspot for visitors
  - Allows visitors to access free Wi-Fi after accessing the facility's Facebook page.
  - Provides insight into a facility's customer base through demographic reports.

QUESTION NO: 7

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

A. Enable Management Frame Protection on the SSIDs broadcasted using third-party AP.

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

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

D. Upload the MAC addresses of the third-party APs to Cisco Catalyst Center using a wIPS workflow.

Answer: D

Explanation:

In Cisco SD-Access with Fabric-enabled wireless, unknown APs are flagged as rogue by default.

To prevent third-party APs used for testing from being classified as high-threat rogue and contained, their MAC addresses must be added as exceptions in Cisco Catalyst Center via the wIPS workflow. This whitelists the devices, allowing interoperability testing without triggering containment actions.

QUESTION NO: 8

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

A. wired and wireless devices

B. wireless devices

C. wired devices

D. Cisco certified wireless devices

Answer: A

Explanation:

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

Q. What devices can be tracked with the Cisco Context Aware Services?

A. The Cisco Context-Aware Services allows you to track and locate IP enabled devices both wired and wireless with the Cisco Unified Wireless Network and Wired network.

QUESTION NO: 9

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

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

A. COS of 5 to DSCP 46
B. COS of 3 to DSCP 26
C. COS of 6 to DSCP 46
D. COS of 7 to DSCP 48

Answer: A

Explanation:

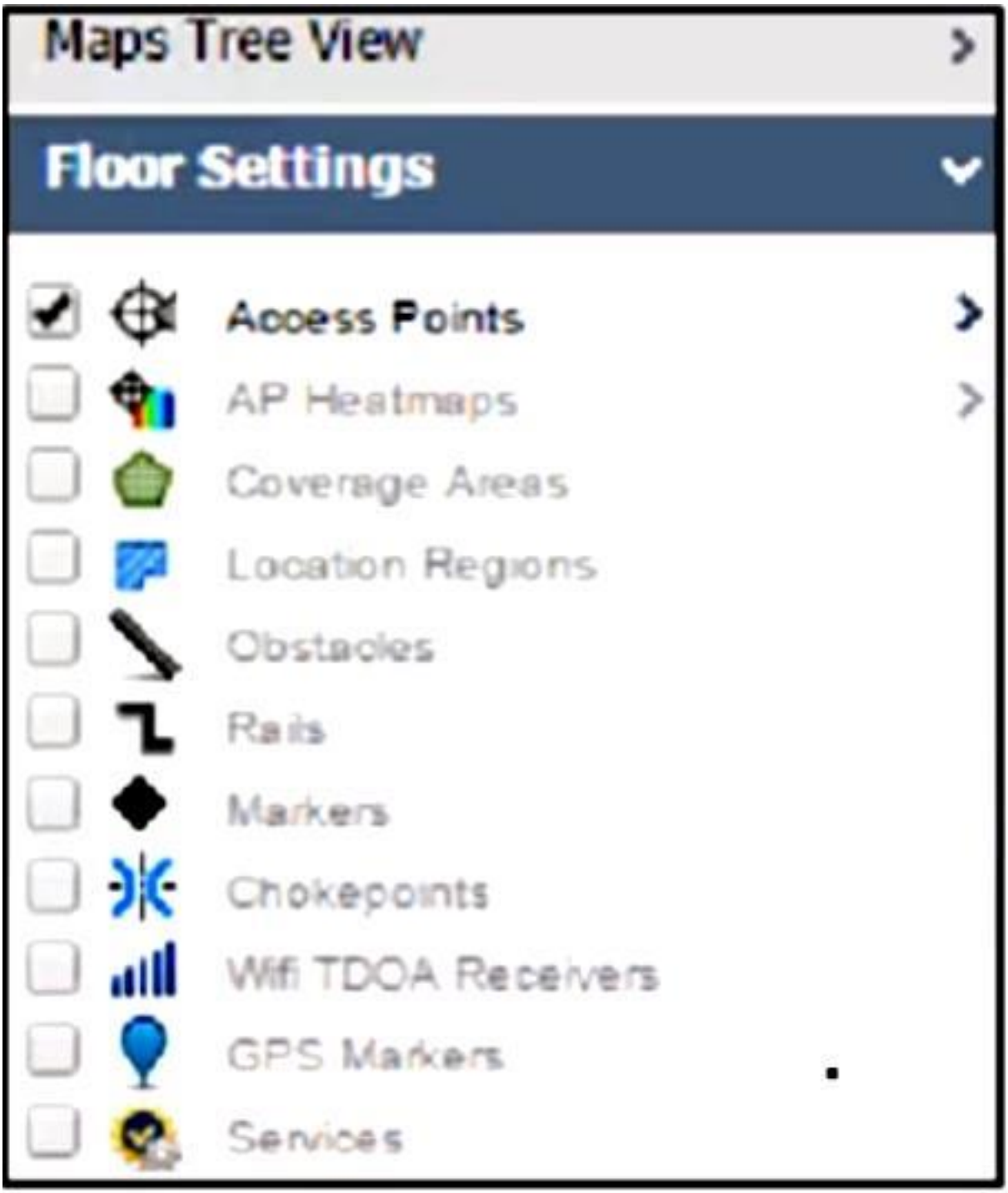
In Quality of Service (QoS) for networking, Class of Service (COS) and Differentiated Services Code Point (DSCP) are used for traffic classification and prioritization. Voice traffic is generally given high priority due to its sensitivity to delay and requires proper tagging to maintain quality over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

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

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

QUESTION NO: 10

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



A. An assurance license is not installed.
B. The controller operational status background task is disabled.
C. The Show Detected Interferers feature under the AP option is disabled.
D. Cisco MSE has not been added to Cisco PI.
Answer: D
Explanation:
Note Depending on whether or not a mobility services engine is present in NCS, some of the floor settings may not display. Clients, 802.11 Tags, Rogue APs, Adhoc Rogues, Rouge Clients and Interferers are visible only if a MSE is present in NCS.

QUESTION NO: 11
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
Explanation:
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.

QUESTION NO: 12
A healthcare organization notices many rogue APs and is concerned about a honeypot attack.
Which configuration must a wireless network engineer perform in Cisco Prime Infrastructure to prevent these attacks most efficiently upon detection?
A. Set the auto containment level to 0 and select the Ad Hoc Rogue AP containment option.
B. Set the auto containment level to 0 and select the Using Our SSID containment option
C. Set the manual containment level to 4 and select the Ad Hoc Rogue AP containment option.
D. Set the auto containment level to 4 and select the Using Our SSID containment option.
Answer: D
Explanation:
Use of our SSID - If a rogue device uses an SSID which is the same as that configured on the controller, it is automatically contained. This feature aims to address a honey-pot attack before it causes damage.
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112045-handling-rogue-cuwn-00.html#toc-hId-715491869

QUESTION NO: 13
An engineer must enable location services using Cisco DNA Space through a DNA Space Connector on a client located in the US. Which two requirements are mandatory for a successful implementation? (Choose two.)
A. Cisco DNA Spaces Connector must connect to the wireless controllers on NMSP port 16113 over TCP and SNMP ports 161/162 over UDP.
B. Cisco DNA Space Connector must be able to reach out to https://connector.dnaspaces.io
C. The wireless controllers must enable Cisco CMX Connector.
D. Ensure that the wireless controller API is accessible for the DNA Space Connector.
E. Cisco DNA Space Connector must be able to connect to the wireless network via CAPWAP ports
5246 and 5247.
Answer: AB

QUESTION NO: 14
An engineer has many different WLANs on a WLC but does not want to broadcast them to every AP in the building. Which group must be configured on the WLC to allow different WLANs on the different APs without creating new interfaces?
A. ACL
B. interface group
C. mobility group
D. AP group
Answer: D
Explanation:
In a Cisco Wireless LAN Controller (WLC), AP groups are used to manage the distribution of WLANs to different access points (APs). By configuring AP groups, an engineer can specify which WLANs are broadcasted by which APs. This allows for the creation of multiple WLANs across different APs without the need to create new interfaces for each WLAN. AP groups provide the flexibility to control WLAN availability based on location or other criteria, ensuring that only the intended WLANs are available through specific APs.

QUESTION NO: 15
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: B
Explanation:
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.

QUESTION NO: 16
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

Explanation:

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.

QUESTION NO: 17

A network engineer is implementing a wireless network and is considering deploying a single SSID for device onboarding. Which option is a benefit of using dual SSIDs with a captive portal on the onboard SSID compared to a single SSID solution?

A. limit of a single device per user

B. restrict allowed devices types

C. allow multiple devices per user

D. minimize client configuration errors

Answer: D

Explanation:

https://ciscocustomer.lookbookhq.com/iseguidedjourney/byod-configuration

https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=47256

QUESTION NO: 18

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: CE

QUESTION NO: 19

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

A. Manually synchronize from Cisco Prime Infrastructure.

B. Manually synchronize from MSE.

C. Enable automatic synchronization on Cisco Prime Infrastructure.

D. Enable automatic synchronization on MSE.

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

Answer: CE

QUESTION NO: 20

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
Explanation:
In a Cisco WLAN deployment where it is required that all APs from branch1 remain operational even if the control plane CAPWAP tunnel is down, the operational mode that must be configured on the APs is standalone. 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.

QUESTION NO: 21
The marketing department creates a promotion video for the branch store. Only interested hosts must receive the video over wireless multicast. What allows this feature?
A. TPC
B. DCA
C. WMM
D. WMF
Answer: D
Explanation:
Wireless Multicast Forwarding (WMF) is the feature that allows the delivery of multicast content, such as a promotional video, to only interested hosts over a wireless network. It optimizes the use of network resources by ensuring that only the hosts that have expressed interest in the multicast group receive the data.

QUESTION NO: 22
A company wants to switch to BYOD to reduce IT support costs for the company. Which option is an impact of BYOD should be considered?
A. increased VPN connections
B. restricted device enforcement
C. increased phishing attacks
D. decreased support calls
Answer: C
Explanation:
The impact of BYOD that should be considered is the potential for increased phishing attacks.
BYOD can lead to a greater variety of devices accessing the network, which may not all have the same level of security. This can increase the risk of phishing attacks as attackers may target personal devices that are used to access corporate resources, which might not be as secure as company-owned devices.

QUESTION NO: 23
A consulting engineer must migrate the APs from a Cisco 8540 WLC to a Cisco Catalyst 9800-80 WLC. As part of the migration, the engineer is advised to use a policy map as part of the configuration on the Catalyst 9800-80 WLC to mirror the platinum QoS settings on voice WLAN to accommodate CP-840 wireless phones. Which configuration must the engineer implement on the voice WLAN?
A.

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

B.

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

C.

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

D.

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

Answer: D
Explanation:
For Cisco Platinum QoS applied to voice WLANs (supporting Cisco 840 phones), traffic classes must be mapped to appropriate DSCP values for prioritization:
- DSCP 34 (video) → AF41
- DSCP 45 (voice signaling) → DSCP 45
- DSCP 46 (voice bearer) → EF (Expedited Forwarding, highest priority)
- DSCP 47 (call control) → DSCP 47

QUESTION NO: 24
A corporation is spread across different countries and uses MPLS to connect the offices. The senior management wants to utilize the wireless network for all the employees. To ensure strong connectivity and minimize delays, an engineer needs to control the amount of traffic that is traversing between the APs and the central WLC.
Which configuration should be used to accomplish this goal?
A. FlexConnect mode with OfficeExtend enabled
B. FlexConnect mode with local authentication
C. FlexConned mode with central switching enabled
D. FlexConnect mode with central authentication
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/72/configuration/guide/cg/cg_flexconnect.html#wp1241304

Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit (MTU) no smaller than 500 bytes. In local authentication, the authentication capabilities are present in the access point itself. Local authentication reduces the latency requirements of the branch office.

QUESTION NO: 25
An engineer is considering an MDM integration with Cisco ISE to assist with security for lost devices. Which two functions of MDM increase security for lost devices that access data from

the network? (Choose two.)

A. PIN enforcement

B. Jailbreak/root detection

C. data wipe

D. data encryption

E. data loss prevention

Answer: BC

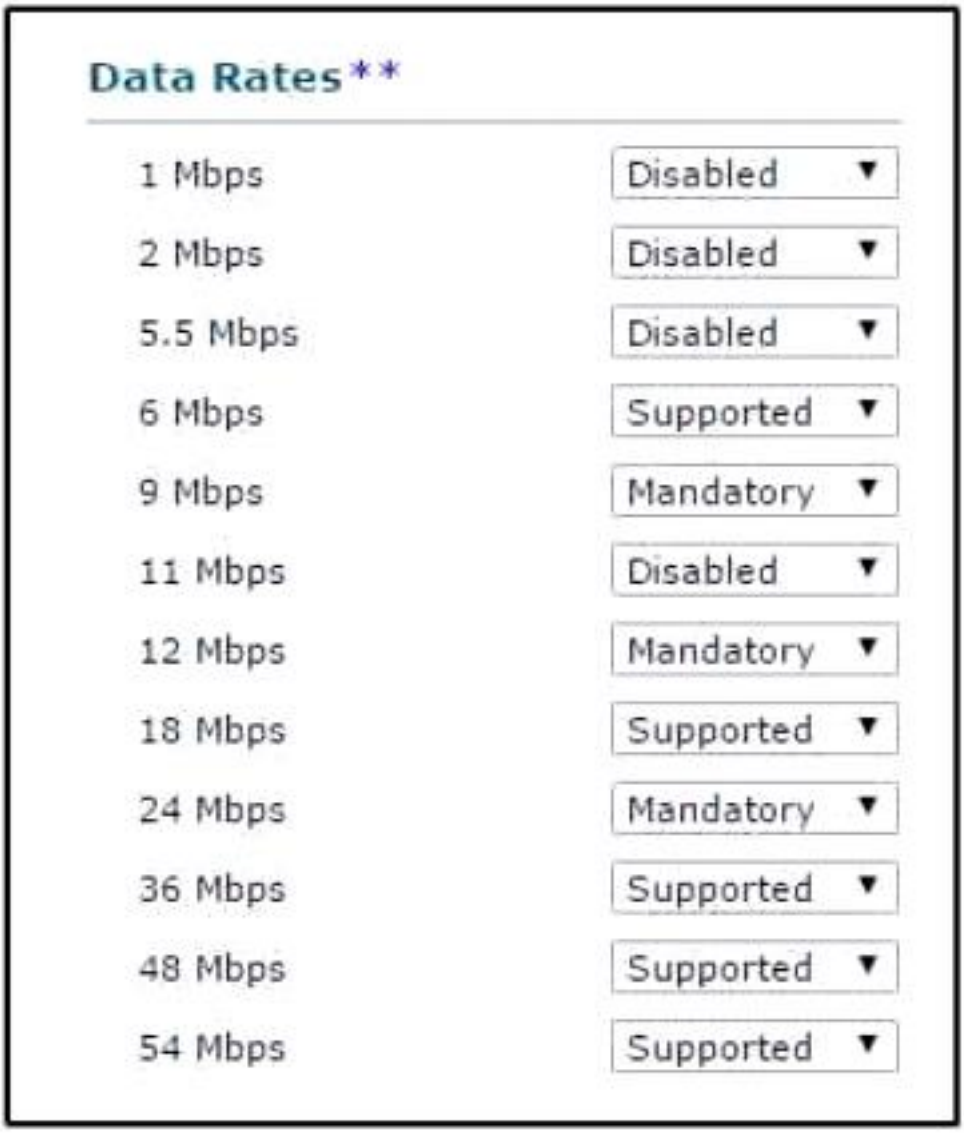
Explanation:

Mobile Device Management (MDM) integration with Cisco ISE increases security for lost devices by providing functions such as data wipe and jailbreak/root detection. Data wipe allows the remote erasure of sensitive information from lost devices, preventing unauthorized access.

Jailbreak/root detection helps identify compromised devices that may bypass standard security measures, ensuring that they do not access network resources.

QUESTION NO: 26

Refer to the exhibit. An engineer is configuring a Cisco wireless LAN controller and needs wireless multicast to use the 54Mbps rates. Which action meets this requirement?



A. Change the 24 Mpbs to Supported.
B. Set all data rates below 54 Mbps to Supported.
C. Change the 54 Mpbs to Mandatory.
D. Set all data rates below 54 Mbps to Disable.
Answer: C
Explanation:
In a Cisco wireless LAN controller, setting a specific data rate to `Mandatory' means that all wireless clients must be able to communicate at this rate. To ensure that multicast uses the 54Mbps rates, one must set the 54Mbps data rate to `Mandatory'. This configuration will make it so that all multicast traffic is transmitted at this minimum set data rate, thus meeting the requirement specified by the engineer.

QUESTION NO: 27
A network administrator just completed the basic implementation of Cisco CMX and tries to implement location tracking. The administrator is having trouble establishing connectivity between one of the WLCs through NMSP. What must be configured to establish this connectivity?
(Choose two.)
A. Add permanent licenses on the Cisco CMX server.
B. Allow on the firewall port 16113 between Cisco CMX and the WLC.
C. Enable NMSP on the WLC.
D. Reboot Cisco CMX after adding the WLC for the first time.
E. Add to the WLC the MAC address and SSC key for the Cisco CMX server.
Answer: BC

QUESTION NO: 28
Refer to the exhibit. A customer implements AVC on the AireOS controllers. All of the NetFlow data is configured for export to Cisco Prime Infrastructure to be analyzed for a specified period.
During testing, no data is reported from the controllers. Which two configurations must be applied for the data to be exported? (Choose two.)

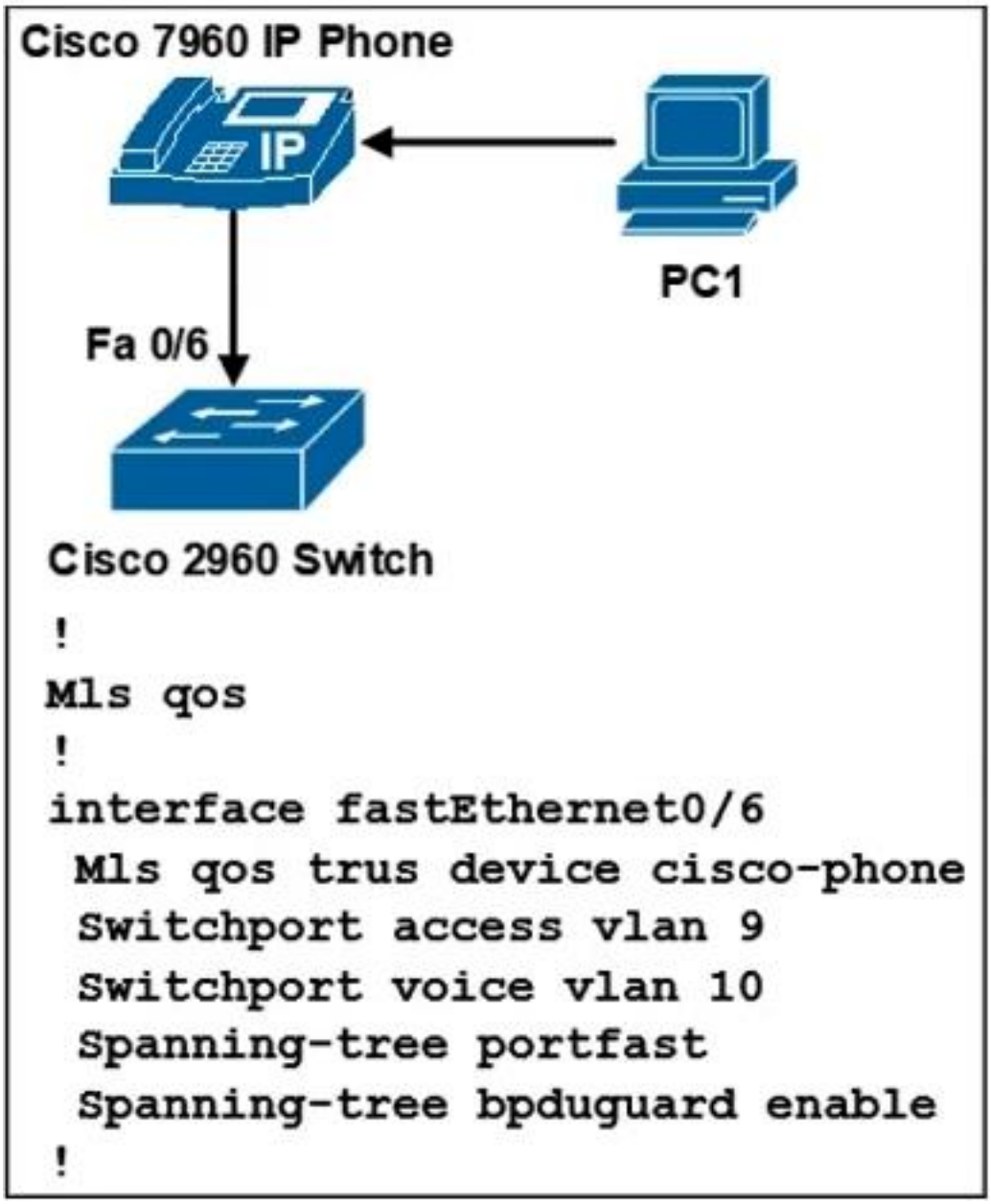
```
(Cisco Controller) >show flow exporter summary

    Exporter-Name  Exporter-IP    Port
    ============   ==========     ====
    Export_to_Prime_Infrastructure 10.20.30.6   8080

(Cisco Controller) >show flow monitor summary

    Monitor-Name        Exporter-Name  Exporter-IP    Port Record Name
    ============        ============== ============   ===  ============
    AVC_Test               -----          -----        -   ipv4_client_app_flow_record
```

A. config flow add monitor AVC_test record ipv4_client_app_flow_record
B. config flow create exporter Export_to_Prime_Infrastructure 10.20.30.6 port 9991
C. config flow create exporter Export_to_Prime_Infrastructure 10.20.30.6 port 8080
D. config flow add monitor Export_to_Prime_Infrastructure exporter AVC_test

E. config flow add monitor AVC_test exporter Export_to_Prime_Infrastructure
Answer: AE

QUESTION NO: 29
An engineer manages a wireless network for an enterprise. The offices of the enterprise are in a multistory building with other companies. To avoid service loss of the wireless network, jamming devices must be monitored and an alert must be raised when one enters the airspace. Which two parameters must be configured for this alarm to happen? (Choose two.)
A. Jammer is in the "Rogue Devices to Detect"multiple select box.
B. Jammer is selected in the Rogue Policies.
C. Clean Air is enabled.
D. Air Quality Index Trap is enabled.
E. Set the Cisco WLC to trap this type of device.
Answer: CE
Explanation:
CleanAir is required as that enables the AP chipset to detect interference. Then in 9800 you go to Configuration --> Radio Configurations --> CleanAir --> Select Trap Configuration --> Move Jammer to the Interference Types to trap box.

QUESTION NO: 30
Refer to the exhibit. An engineer must preserve a QoS marking sent by the Cisco Jabber software running on PC1. Which marking value must be trusted on port Fa 0/6?



A. DSCP
B. 802.1p
C. CoS
D. IP precedence
Answer: A

QUESTION NO: 31
An engineer is implementing Cisco Identity-Based Networking on a Cisco AireOS controller. The engineer has two ACLs on the controller.
The first ACL, named BASE_ACL, is applied to the corporate_clients interface on the WLC, which is used for all corporate clients.
The second ACL, named HR_ACL, is referenced by ISE in the Human Resources group policy.
What is the resulting ACL when a Human Resources user connects?
A. HR_ACL appended with BASE_ACL

B. HR_ACL only
C. BASE_ACL appended with HR_ACL
D. BASE_ACL only
Answer: B
Explanation:
https://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/98590- Per-User-ACL-WLC.html#configure-acs

QUESTION NO: 32
Refer to the exhibit. An engineer must identify jammer devices on the wireless network. The AP must scan all configured channels. Which AP mode must be configured to accomplish this?


802.11b/g/n Cisco APs >Interference Devices

Entries 1 - 2 of 2

Current Filter: None [Change Filter] [Clear Filter]

AP Name	Radio Slot#	Device Type	Affected Channel	Detected Time	Severity	Duty Cycle(%)	RSSI	DevID
RL-C3700-01-HALO	0		1,2,3,4,5,6,7,8,9,11	Mon May 2 14:32:39 2016	63	54	-35	0x3011

A. Monitor
B. Local
C. FlexConnect
D. Bridge
Answer: A

QUESTION NO: 33
An engineer is configuring a new wireless network for guest access. The Facebook page of the company must be viewed by the guest users before they get access to the network. A Cisco MSE is used as a wireless component. Which URL must be used in the configuration as the external redirection URL?
A. http://<MSE>:8084/vistor/login.do
B. http://<MSE> 8083/visitor/login.do
C. http://<MSE>:8083/fbwifi/forward
D. http://<MSE>:8084/fbwifi/forward
Answer: D
Explanation:
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

QUESTION NO: 34
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.)

```
.....................
*radiusTransportThread: Jan 03 12:54:17.120: [PA] 64:89:9a:31:7f:a1 Access-Reject
received from RADIUS server 147.70.11.241 for mobile 64:89:9a:31:7f:al received = 4
*radiusTransportThread: Jan 03 12:54:17.120: [PA] 64:89:9a:31:7f:a1 [Error] Client
requested no retries for mobile 64:89:9A:31:7F:A1
*radiusTransportThread: Jan 03 12:54:17.120: [PA] 64:89:9a:31:7f:a1 Returning AAA
Error 'Authentication Failed' (-4) for mobile 64:89:9a:31:7f:a1
*radiusTransportThread: Jan 03 12:54:17.120: [PA] AuthorizationResponse:
0x7f13e99ea600
.....................
```

A. An invalid user account or password was used.

B. RADIUS is incorrectly configured

C. The server certificate is expired or not in use

D. Certificate services are not working properly.

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

Answer: AB

QUESTION NO: 35

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

A. learn client IP address

B. FlexConnect local authentication

C. VLAN-based central switching

D. central DHCP processing

Answer: C

Explanation:

VLAN-based central switching is the feature that meets the requirements stated. With this feature, when a subnet assigned to a client is available at the remote site, the traffic is offloaded locally. If the subnet is not available, the traffic is tunneled back to the Wireless LAN Controller (WLC). This setup allows for dynamic assignment of clients to specific IP subnets using Cisco Identity-Based Networking Services with ISE.