300-430 Q&As

Implementing Cisco Enterprise Wireless Networks (ENWLSI)

Pass Cisco 300-430 Exam with 100% Guarantee

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

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.

Correct Answer: CE

https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/multicast_broadcast_setup.html
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. For locally switched WLANs, all multicast traffic including mDNS is simply bridged between the local VLAN and the SSID.

QUESTION 2

An engineer must implement a BYDD policy with these requirements:

1.

Onboarding unknown machines

2.

Easily scalable

3.

Low overhead on the wireless network

Which method satisfies these requirements?

A. triple SSID

B. open SSID

C. dual SSID

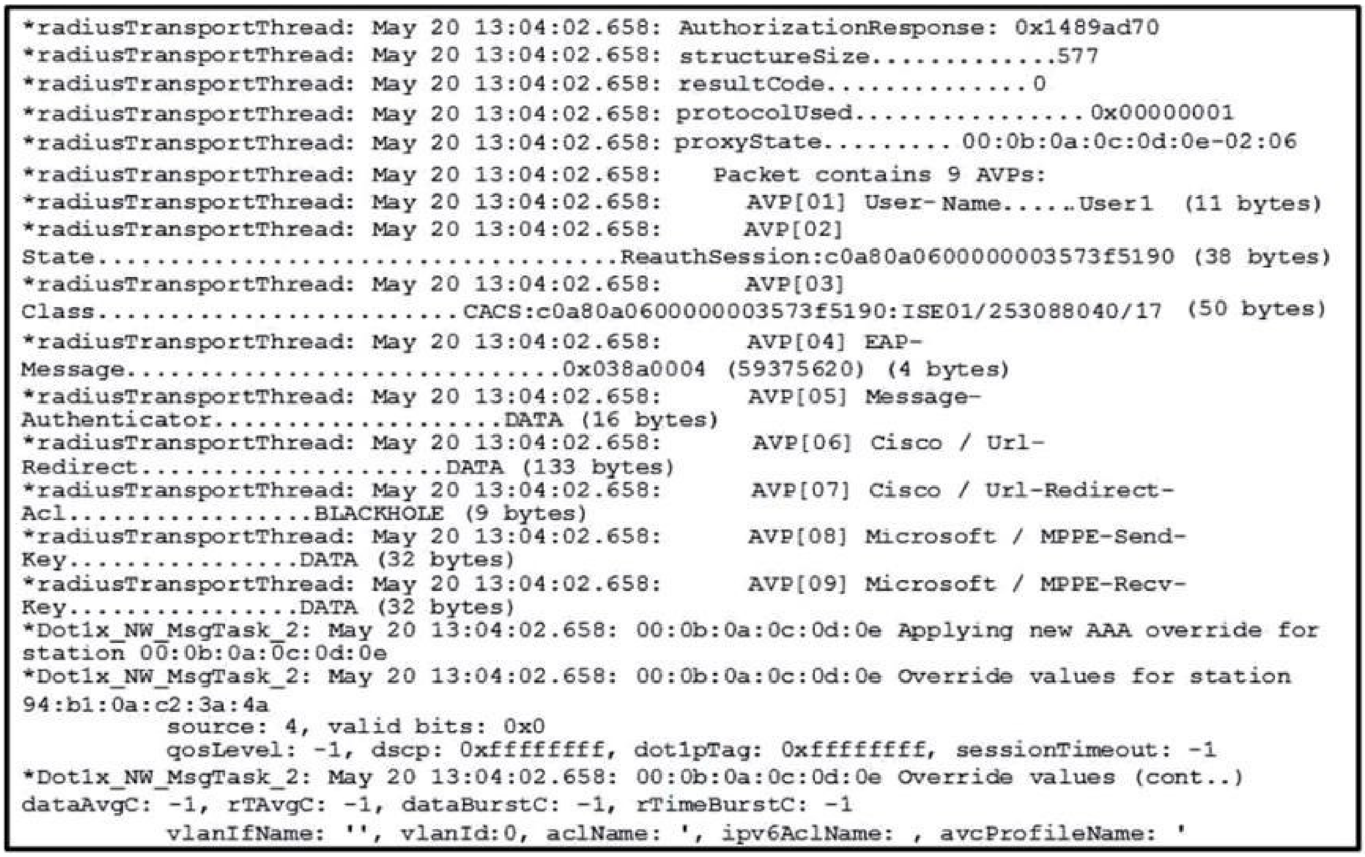
D. single SSID

Correct Answer: D

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Wireless.html

QUESTION 3

Refer to the exhibit.



```
*radiusTransportThread: May 20 13:04:02.658: AuthorizationResponse: 0x1489ad70
*radiusTransportThread: May 20 13:04:02.658: structureSize............577
*radiusTransportThread: May 20 13:04:02.658: resultCode.............0
*radiusTransportThread: May 20 13:04:02.658: protocolUsed...............0x00000001
*radiusTransportThread: May 20 13:04:02.658: proxyState......... 00:0b:0a:0c:0d:0e-02:06
*radiusTransportThread: May 20 13:04:02.658:    Packet contains 9 AVPs:
*radiusTransportThread: May 20 13:04:02.658:      AVP[01] User-Name.....User1  (11 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[02]
State...................................ReauthSession:c0a80a0600000003573f5190 (38 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[03]
Class........................CACS:c0a80a0600000003573f5190:ISE01/253088040/17  (50 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[04] EAP-
Message.............................0x038a0004 (59375620) (4 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[05] Message-
Authenticator....................DATA (16 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[06] Cisco / Url-
Redirect.....................DATA (133 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[07] Cisco / Url-Redirect-
Acl.................BLACKHOLE (9 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[08] Microsoft / MPPE-Send-
Key................DATA (32 bytes)
*radiusTransportThread: May 20 13:04:02.658:      AVP[09] Microsoft / MPPE-Recv-
Key................DATA (32 bytes)
*Dot1x_NW_MsgTask_2: May 20 13:04:02.658: 00:0b:0a:0c:0d:0e Applying new AAA override for
station 00:0b:0a:0c:0d:0e
*Dot1x_NW_MsgTask_2: May 20 13:04:02.658: 00:0b:0a:0c:0d:0e Override values for station
94:b1:0a:c2:3a:4a
          source: 4, valid bits: 0x0
          qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
*Dot1x_NW_MsgTask_2: May 20 13:04:02.658: 00:0b:0a:0c:0d:0e Override values (cont..)
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
          vlanIfName: '', vlanId:0, aclName: ', ipv6AclName: , avcProfileName: '
```

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

A. Configure a different client VLAN after authentication.

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

C. Apply a lower WMM QoS.

D. Enable rate-limiting to the client.

Correct Answer: A

QUESTION 4

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

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

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

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

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

Correct Answer: C

QUESTION 5

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

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

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

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

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

Correct Answer: B

https://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_troubleshooting.html

QUESTION 6

An enterprise started using WebEx as a virtual meeting solution. There is a concern that the existing wireless network will not be able to support the increased amount of traffic as a result of using WebEx. An engineering needs to remark the QoS value for this application to ensure high quality in meetings. Which must be implemented to accomplish this task?

A. WLAN quality of service profile

B. QoS preferred call index

C. AVC profiles

D. UP to DSCP map

Correct Answer: C

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

QUESTION 7

What is an indication of having multiple wireless controllers within the same CAPWAP multicast group?

A. Multicast packets are rate-limited to 128 kbps.

B. Multicast traffic is increased throughout the network.

C. ACL filtering are used on the first hop router on all VLANs.

D. CAPWAP packets are fragmented.

Correct Answer: B

QUESTION 8

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

Correct Answer: B

webex-app-sharing is for sharing traffic only (doesn\\'t include webex-audio or webex-video) for streaming.
https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7-5/AVC_dg7point5.html

QUESTION 9

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

Correct Answer: B

https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/
b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_011 01011.html

QUESTION 10

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

Correct Answer: C

QUESTION 11

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

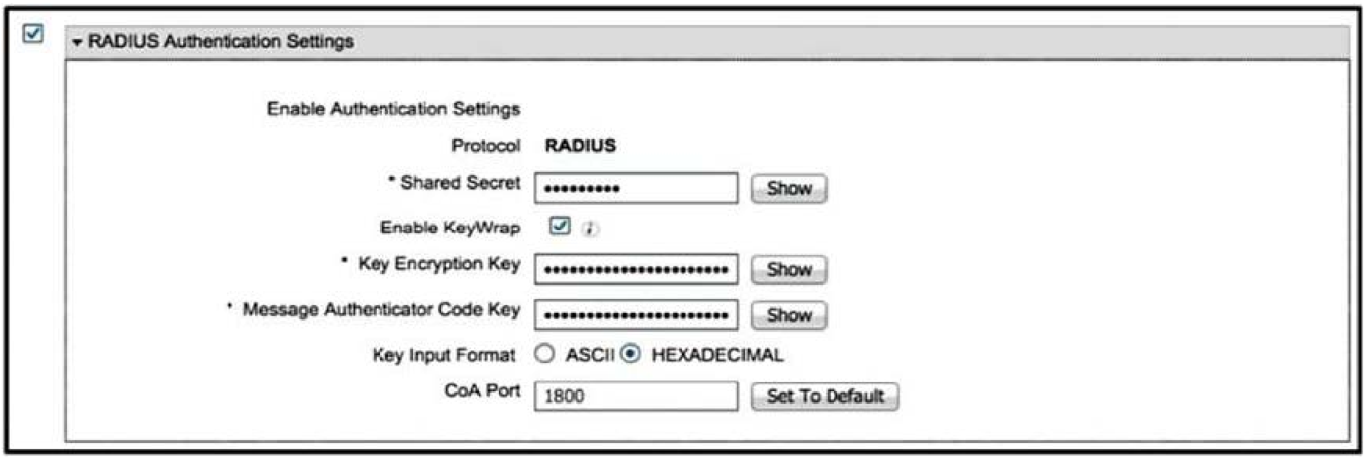
C. 6

D. 5

Correct Answer: B

QUESTION 12

Refer to the exhibit.



☑ ▾ RADIUS Authentication Settings

Enable Authentication Settings
Protocol: RADIUS
* Shared Secret: •••••••••• [Show]
Enable KeyWrap: ☑
* Key Encryption Key: •••••••••••••••••••••••• [Show]
* Message Authenticator Code Key: •••••••••••••••••••••••• [Show]
Key Input Format: ○ ASCII ● HEXADECIMAL
CoA Port: 1800 [Set To Default]

The security team has implemented ISE as a 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

Correct Answer: B

QUESTION 13

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

Correct Answer: B

QUESTION 14

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

A. Configure Secondary Controller Name and Management IP address in the High Availability tab.

B. Configure LSC to authorize the OEAP.

C. Configure the AP mode to FlexConnect and check the box for Office Extend AP.

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

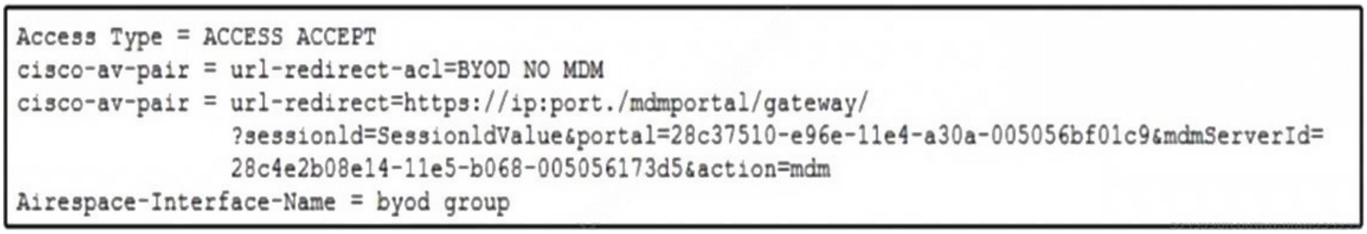
E. Configure Primary Controller Name and Management IP address in the High Availability tab.

Correct Answer: CE

Step 4 and 5: https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_0101111.pdf

QUESTION 15

Refer to the exhibit.



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

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?

A. static IP tunneling

B. allow AAA override

C. RADIUS profiling

D. Aironet IE

Correct Answer: B

300-430 PDF Dumps 300-430 Practice Test 300-430 Study Guide