

Exams-Boost



- ✓ Online Tool, Convenient, easy to study.
- ✓ Instant Online Access
- ✓ Supports All Web Browsers
- ✓ Practice Online Anytime
- ✓ Test History and Performance Review
- ✓ Supports Windows / Mac / Android / iOS, etc.



- ✓ Installable Software Application
- ✓ Simulates Real Exam Environment
- ✓ Builds Exam Confidence
- ✓ Supports MS Operating System
- ✓ Two Modes For Practice
- ✓ Practice Offline Anytime



- ✓ Printable PDF Format
- ✓ Prepared by IT Experts
- ✓ Instant Access to Download
- ✓ Study Anywhere, Anytime
- ✓ 365 Days Free Updates
- ✓ Free PDF Demo Available



Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.



Money Back Guarantee

Full refund if you fail the corresponding exam in 90 days after purchasing. And Free get any another product.



Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

<http://www.exams-boost.com/>

Provides everything you need to prepare and quickly pass the certification exam a first attempt.

Exam : **300-375**

Title : **Securing Wireless Enterprise Networks**

Vendor : **Cisco**

Version : **DEMO**

NO.1 A new MSE with wIPS service has been installed and no alarm information appears to be reaching the MSE from controllers.

What protocol must be allowed to reach the MSE from the controllers?

- A. SOAP/XML
- B. NMSP
- C. CAPWAP
- D. SNMP

Answer: A

NO.2 Which feature should an engineer select to implement the use of VLAN tagging, QoS, and ACLs to clients based on RADIUS attributes?

- A. per-WLAN RADIUS source support
- B. AAA override
- C. client profiling
- D. captive bypassing
- E. identity-based networking

Answer: B

NO.3 An engineer with ID 338860948 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.

Which option is the resulting ACL when a Human Resources user connects?

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

Answer: A

NO.4 You are implementing Cisco Identity Based Networking Services on a Cisco Catalyst 3850 Series Switch that uses downloadable service templates. What is the default password that must be configured on the RADIUS server?

- A. cisco
- B. Cisco
- C. cisco123
- D. Cisco123

Answer: C

NO.5 What is the maximum number of clients that a small branch deployment using a four-member Cisco Catalyst

3850 stack (acting as MC/MA) can support?

- A. 1000
- B. 10000

- C. 2000
- D. 500
- E. 5000

Answer: E

NO.6 WPA2 Enterprise with 802.1x is being used for clients to authenticate to a wireless network through an ACS server. For security reasons, the network engineer wants to ensure only PEAP authentication can be used. The engineer sent instructions to clients on how to configure their supplicants, but users are still in the ACS logs authentication using EAP-FAST. Which option describes the most efficient way the engineer can ensure these users cannot access the network unless the correct authentication mechanism is configured?

- A.** Enable AAA override on the SSID and configure an access policy in ACS that denies access to the list of MACs that have used EAP-FAST.
- B.** Enable AAA override on the SSID and configure an access policy in ACS that allows access only when the EAP authentication method is PEAP.
- C.** Enable AAA override on the SSID and configure an access policy in ACS that puts clients that authenticated using EAP-FAST into a quarantine VLAN.
- D.** Enable AAA override on the SSID, gather the usernames of these users, and disable their RADIUS accounts until they make sure they correctly configured their devices.

Answer: C

NO.7 WPA2 Enterprise with 802.1x is being used for clients to authenticate to a wireless network through an ISE server. For security reasons, the network engineer wants to ensure only PEAP authentication can be used. The engineer sent instructions to clients on how to configure their supplicants, but users are still in the ISE logs authentication using EAP-FAST. Which option describes the most efficient way the engineer can ensure these users cannot access the network unless the correct authentication mechanism is configured?

- A.** Enable AAA override on the SSID, gather the usernames of these users, and disable their RADIUS accounts until they make sure they correctly configured their devices.
- B.** Enable AAA override on the SSID and configure an access policy in ACS that puts clients that authenticated using EAP-FAST into a quarantine VLAN.
- C.** Enable AAA override on the SSID and configure an access policy in ACS 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 ACS that allows access only when the EAP authentication method is PEAP.

Answer: D

NO.8 An engineer has configured passive fallback mode for RADIUS with default timer settings. What will occur when the primary RADIUS fails then recovers?

- A.** RADIUS requests will be sent to the secondary RADIUS server until the secondary fails to respond.
- B.** After the inactive time expires the controller will send RADIUS to the primary.
- C.** Once RADIUS probe messages determine the primary controller is active the controller will revert back to the primary RADIUS.
- D.** The controller will immediately revert back after it receives a RADIUS probe from the primary

server.

Answer: B

NO.9 An engineer must change the wireless authentication from WPA2-Personal to WPA2-Enterprise. Which three requirements are necessary? (Choose three.)

- A. 802.11u
- B. EAP
- C. fast secure roaming
- D. 802.11i
- E. 802.1x
- F. per-shared key
- G. RADIUS

Answer: B,D,G

NO.10 An administrator receives reports of many interferers in the wireless network and wants to get the location of these interferers from the maps in Cisco Prime Infrastructure. When looking at the floor plans/maps, the administrator does not see any interferers, but can see all wireless clients located successfully. Which two statements define the cause of the issue? (Choose two.)

- A. NSMP communication is inactive with the WLC.
- B. Interferer tracking is not enabled on the MSE.
- C. Context Aware Service tracking limit has already been reached with tracking other elements.
- D. SNMP between Cisco Prime Infrastructure and the WLC is failing.
- E. MSE is not added to Cisco Prime infrastructure and synchronized.

Answer: B,E

NO.11 Refer to the exhibit.

WLANs > Edit 'Cisco'

General	Security	QoS	Policy-Mapping	Advanced
<div style="display: flex; justify-content: space-between;"> Layer 2 Layer 3 AAA Servers </div>				
Layer 2 Security 6 WPA+WPA2 ▼ MAC Filtering 9 <input type="checkbox"/>				
Fast Transition Fast Transition <input type="checkbox"/>				
Protected Management Frame				
PMF Required ▼				
Comeback timer(1-10sec) 1				
SA Query Timeout(100-500msec) 200				
WPA+WPA2 Parameters				
WPA Policy <input type="checkbox"/>				
WPA2 Policy <input checked="" type="checkbox"/>				
WPA2 Encryption <input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP				

A customer is having problems with clients associating to me wireless network. Based on the configuration, which option describes the most likely cause of the issue?

- A. PME is set to "required"
- B. Both AES and TKIP must be enabled
- C. MAC Filtering must be enabled
- D. Comeback timer is set too low
- E. SA Query Timeout is set too low

Answer: C

NO.12 You plan to implement Cisco Identity Based Networking Services on a Cisco Catalyst 3850 Series Switch.

Which switch command is required when configuring downloadable ACLs?

- A. dot1x system-auth-control
- B. ip device tracking
- C. authentication display new-style

D. aaa session-id common

Answer: B