



BrainDumps
Collection

Cisco

300-375 Exam

Cisco Securing Wireless Enterprise Networks Exam

Thank you for Downloading 300-375 exam PDF Demo

You can also try our 300-375 practice exam software

Download Free Demo

<https://www.braindumpscollection.com/300-375.html>

DEMO
VERSION

(LIMITED CONTENT)

Questions
& Answers

Version: 12.0

Question: 1

Which two considerations must a network engineer have when planning for voice over wireless roaming? (Choose two.)

- A. Roaming with only 802.1x authentication requires full reauthentication.
- B. Full reauthentication introduces gaps in a voice conversation.
- C. Roaming occurs when a phone has seen at least four APs.
- D. Roaming occurs when the phone has reached -80 dBs or below.

Answer: A, B

Question: 2

Which two 802.11 methods can be configured to protect card holder data? (Choose two.)

- A. CCMP
- B. WEP
- C. SSL
- D. TKIP
- E. VPN

Answer: CE

Question: 3

An engineer is changing the authentication method of a wireless network from EAP-FAST to EAP-TLS. Which two changes are necessary? (Choose two.)

- A. Cisco Secure ACS is required.
- B. A Cisco NAC server is required.
- C. All authentication clients require their own certificates.
- D. The authentication server now requires a certificate.
- E. The users require the Cisco AnyConnect client.

Answer: CD

Question: 4

Which mobility mode must a Cisco 5508 wireless Controller be in to use the MA functionality on a Cisco Catalyst 3850 series switch with a Cisco 550 Wireless Controller as an MC?

- A. classic mobility
- B. new mobility
- C. converged access mobility
- D. auto-anchor mobility

Answer: C

Question: 5

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 authenticating 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 denies access to the list of MACs that have used EAP-FAST.
- C. Enable AAA override on the SSID and configure an access policy in ACS that allows access only when the EAP authentication method is PEAP.
- D. 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.

Answer: D

Question: 6

An engineer is configuring a BYOD deployment strategy and prefers a single SSID model. Which technology is required to accomplish this configuration?

- A. mobility service engine
- B. wireless control system
- C. identify service engine
- D. Prime Infrastructure

Answer: C

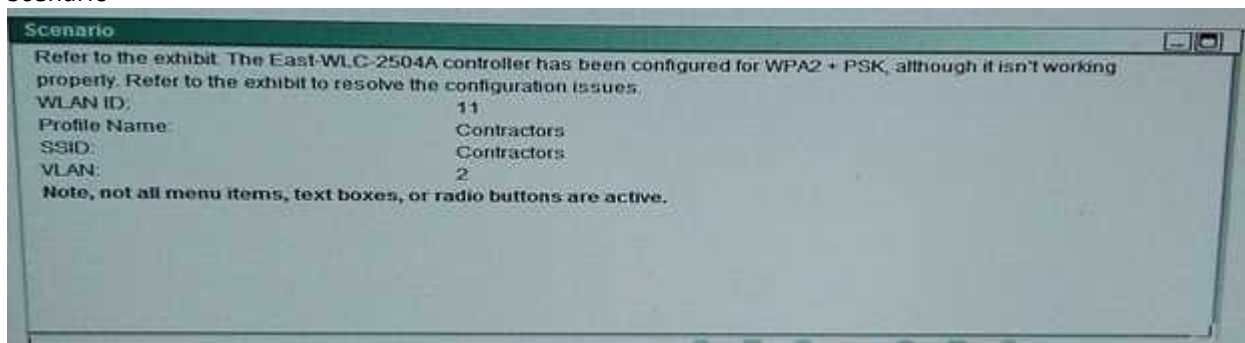
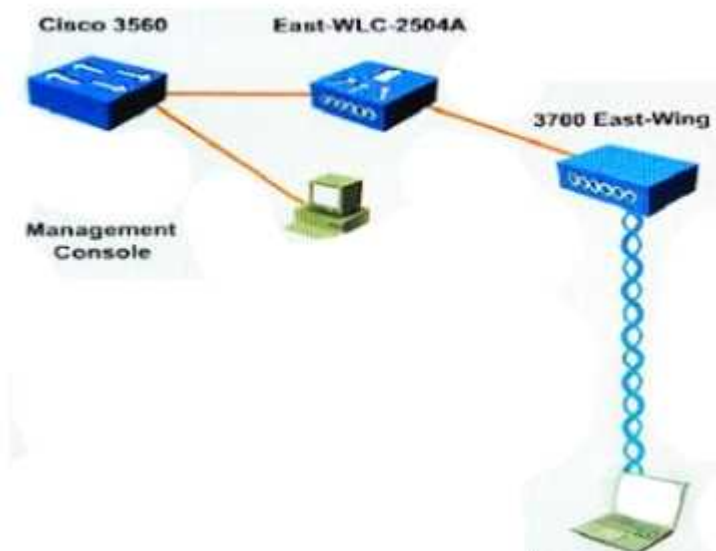
Question: 7

When you configure BYOD access to the network, you face increased security risks and challenges. Which challenge is resolved by deploying digital client certificates?

- A. managing the increase connected devices
- B. ensuring wireless LAN performance and reliability
- C. providing device choice and support
- D. enforcing company usage policies


Answer: D

Question: 8

Scenario**TOPOLOGY****Topology****MONITOR**

Monitor **Summary**

5 Access Points Supported



Controller Summary

| | |
|------------------------------|-----------------------------|
| Management IP Address | 192.168.1.99, ::1/128 |
| Software Version | 8.0.110.0 |
| Field Recovery Image Version | 7.6.101.1 |
| System Name | WLC1-2504A |
| Up Time | 0 days, 5 hours, 14 minutes |
| System Time | Wed Feb 11 15:38:52 2015 |
| Redundancy Mode | N/A |
| Internal Temperature | +27 C |

Clients

Sleeping Clients

Controller Summary

| | |
|------------------------------|-----------------------------|
| Management IP Address | 192.168.1.99, ::1/128 |
| Software Version | 8.0.110.0 |
| Field Recovery Image Version | 7.6.101.1 |
| System Name | WLC1-2504A |
| Up Time | 0 days, 5 hours, 14 minutes |
| System Time | Wed Feb 11 15:38:52 2015 |
| Redundancy Mode | N/A |
| Internal Temperature | +27 C |
| 802.11a Network State | Enabled |
| 802.11b/g Network State | Enabled |
| Local Mobility Group | testlab |
| CPU(s) Usage | 0% |
| Individual CPU Usage | 0%/1%, 0%/2% |
| Memory Usage | 50% |

Access Point Summary

| | Total | Up | Down | |
|---------------------|-------|----|------|------------------------|
| 802.11a/n/ac Radios | 1 | 1 | 0 | Detail |
| 802.11b/g/n Radios | 1 | 1 | 0 | Detail |
| Dual-Band Radios | 0 | 0 | 0 | Detail |
| All APs | 1 | 1 | 0 | Detail |

Client Summary

| | | |
|------------------|---|------------------------|
| Current Clients | 0 | Detail |
| Excluded Clients | 0 | Detail |
| Disabled Clients | 0 | Detail |

WLAMS

WLANs

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#)

| WLAN ID | Type | Profile Name | WLAN SSID | Admin Status | Security Policies |
|---------|------|--------------|-----------|--------------|----------------------|
| 10 | WLAN | Contractors | Employees | Disabled | [WPA2][Auth(802.1X)] |

CONTROLLER

Controller General

General

Name: WLC1-2504A

802.3x Flow Control Mode: Disabled

LAG Mode on next reboot: Disabled (LAG Mode is currently disabled).

Broadcast Forwarding: Disabled

AP Multicast Mode: Multicast

AP IPv6 Multicast Mode: Disabled

AP Fallback: Enabled

CAPWAP Preferred Mode: ipv4

Fast SSID change: Disabled

Link Local Bridging: Disabled

Default Mobility Domain Name: testlab

RF Group Name: testlab

User Idle Timeout (seconds): 300

ARP Timeout (seconds): 300

Web Radius Authentication

Operating Environment: Commercial (0 to 40 C)

Internal Temp Alarm Limits: 0 to 65 C

WebAuth Proxy Redirection Mode: Disabled

WebAuth Proxy Redirection Port: 0

Maximum Allowed APs: 0

Global IPv6 Config: Enabled

Web Color Theme: Default

HA EKU secondary unit: Disabled

Nas-Id: WLC1-2504A

1. Multicast is not supported with FlexConnect on this platform.
2. Value zero implies there is no restriction on maximum allowed APs.

WIRELESS

All APs

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

Number of APs: 2

| AP Name | IP Address(Ipv4/Ipv6) | AP Model | AP MAC | AP Up Time | Admin Status | Operational Status | Pol. Status | No. of Clients | Port | AP Mode |
|----------------|-----------------------|---------------|-------------------|----------------|--------------|--------------------|--------------|----------------|------|---------|
| 3700-East-Wing | 192.168.1.128 | AIR-CT5502-K9 | b8:30:61:04:06 | 0d, 01:07m 33s | Enabled | REC | Normal power | 0 | 1 | local |
| 3700-West-Wing | 192.168.1.100 | AIR-CT5502-K9 | b8:30:61:04:05:20 | 0d, 00:22m 31s | Enabled | REC | Normal power | 0 | 1 | local |

SECURITY

General

Maximum Local Database entries (on next reboot): 2048 (Current Maximum is 2048)

Number of entries, already used: 1

Which configuration changes need to be made to allow WPA2 + PSK to operate properly on the East-WLC-2504A controller? (Choose four.)

- A. Disable Dynamic AP Management.
- B. Click on the Status Enabled radio button.
- C. Change the Layer 3 Security to Web Policy.
- D. Change the WPA + WPA2 Parameters to WPA2 Policy-AES.
- E. Change the PSK Format to HEX.
- F. Change the WLAN ID.
- G. Change the VLAN Identifier.
- H. Change the IP Address of the Virtual interface.
- I. Change the SSID name of the WLAN.
- J. Click on the PSK radio button and add the password in the text box.

Answer: B, F, I, J

Question: 9

Refer to the exhibit.



What is the 1.1.1.1 IP address?

- A. the wireless client IP address
- B. the RADIUS server IP address
- C. the controller management IP address
- D. the lightweight IP address
- E. the controller AP-manager IP address
- F. the controller virtual interface IP address

Answer: F

Question: 10

A Customer is concerned about denial of service attacks that impair the stable operation of the corporate wireless network. The customer wants to purchase mobile devices that will operate on the corporate wireless network. Which IEEE standard should the mobile devices support to address the customer concerns?

- A. 802.11w
- B. 802.11k
- C. 802.11r
- D. 802.11h

Answer: A

Question: 11

DRAG DROP

A wireless engineer wants to schedule monthly security reports in Cisco Prime infrastructure. Drag and drop the report title from the left onto the expected results when the report is generated on the right.

| | |
|---------------------------------|---|
| Adaptive wIPS Alarm Summary | Displays a summarized count of all rogue access points on your network. |
| Adhoc Rogue Count Summary | Displays a summary of security alarm trends over a period of time. |
| Rogue AP Count Summary | Displays a summarized count of all ad hoc rogue access points. |
| Security Alarm Trending Summary | Displays a summary of all adaptive wIPS alarms on your network. |

Answer:

| |
|---------------------------------|
| Rogue AP Count Summary |
| Security Alarm Trending Summary |
| Adhoc Rogue Count Summary |
| Adaptive wIPS Alarm Summary |

Question: 12

An engineer is configuring client MFP. What WLAN Layer 2 security must be selected to use client MFP?

- A. Static WEP
- B. CKIP
- C. WPA+WPA2
- D. 802.1x

Answer: C

Question: 13

Which two events are possible outcomes of a successful RF jamming attack? (Choose two.)

- A. unauthentication association
- B. deauthentication multicast
- C. deauthentication broadcast
- D. disruption of WLAN services
- E. physical damage to AP hardware

Answer: DE

Question: 14

Which CLI command do you use on Cisco IOS XE Software to put the AP named Floor1_AP1 back in the default AP group?

- A. ap Floor1_AP1 ap-groupname default-group
- B. ap name Floor1_AP1 apgroup default-group
- C. ap name Floor1_AP1 ap-groupname default-group
- D. ap name Floor1_AP1 ap-groupname default

Answer: C

Question: 15

An engineer is configuring a new mobility anchor for a WLAN on the CLI with the config wlan mobility anchor add 3 10.10.10.10 command, but the command is failing. Which two conditions must be met to be able to enter this command? (Choose two.)

- A. The anchor controller IP address must be within the management interface subnet.
- B. The anchor controller must be in the same mobility group.
- C. The WLAN must be enabled.
- D. The mobility group keepalive must be configured.
- E. The indicated WLAN ID must be present on the controller.

Answer: AB

Thank You for trying 300-375 PDF Demo

To try our 300-375 practice exam software visit link below

<https://www.braindumpscollection.com/300-375.html>

Start Your 300-375 Preparation

Use Coupon "20OFF" for extra 20% discount on the purchase of Practice Test Software. Test your 300-375 preparation with actual exam questions.