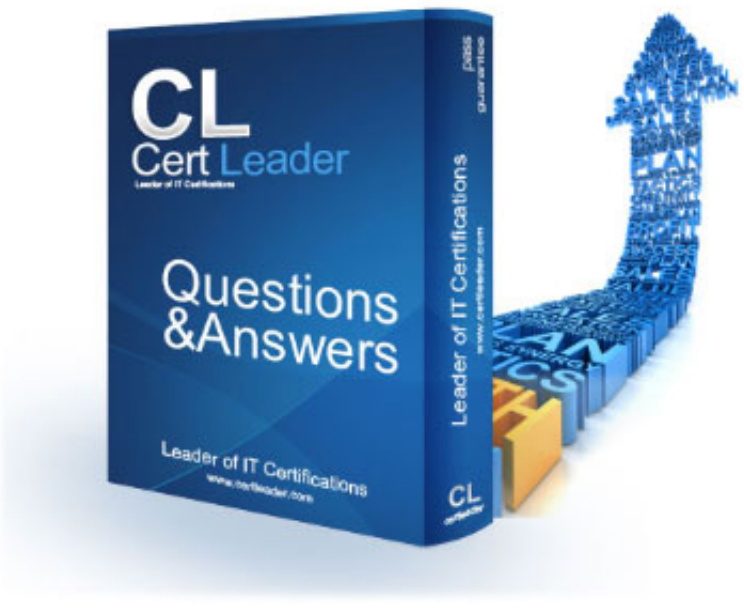
300-375 Dumps

Securing Cisco Wireless Enterprise Networks

https://www.certleader.com/300-375-dumps.html



NEW QUESTION 1
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 clien

Answer: CD

Explanation:

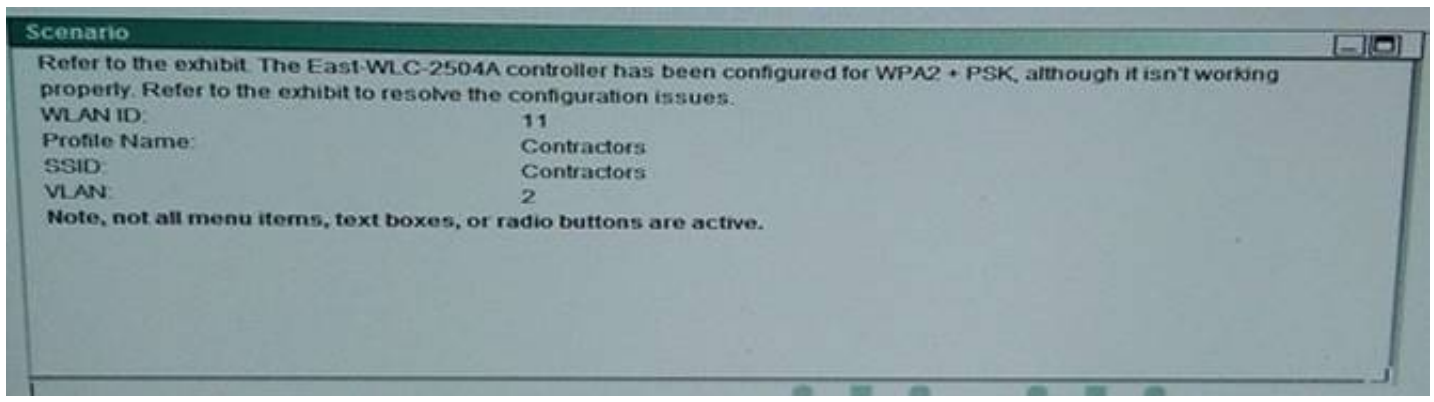
NEW QUESTION 2
Which mobility mode must a Cisco 5508 wireless Controller be in to use the MA functionality on a cisco catalyst 3850 series switch with a cisco 550 Wireless Controller as an MC?

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

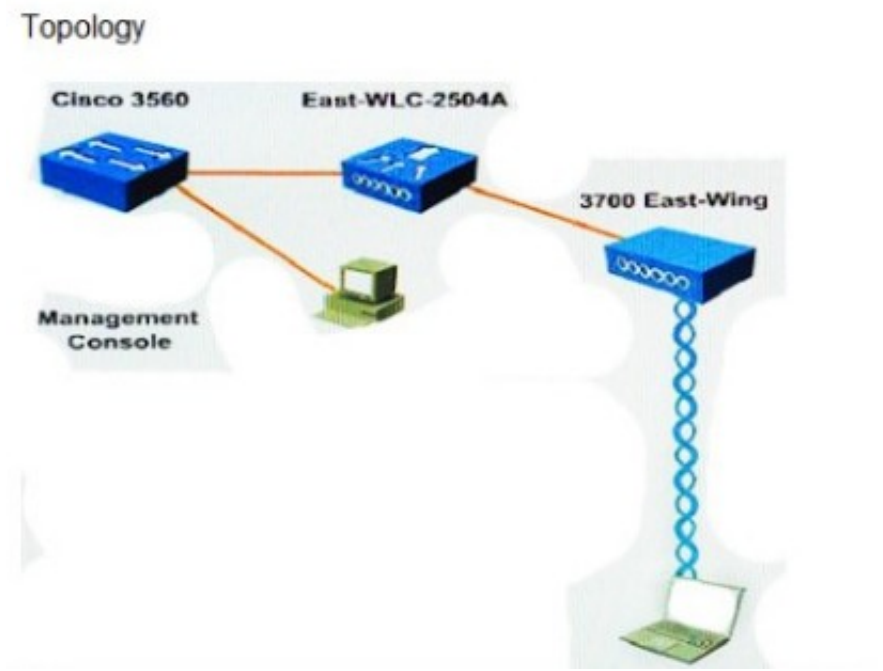
Answer: C

Explanation:

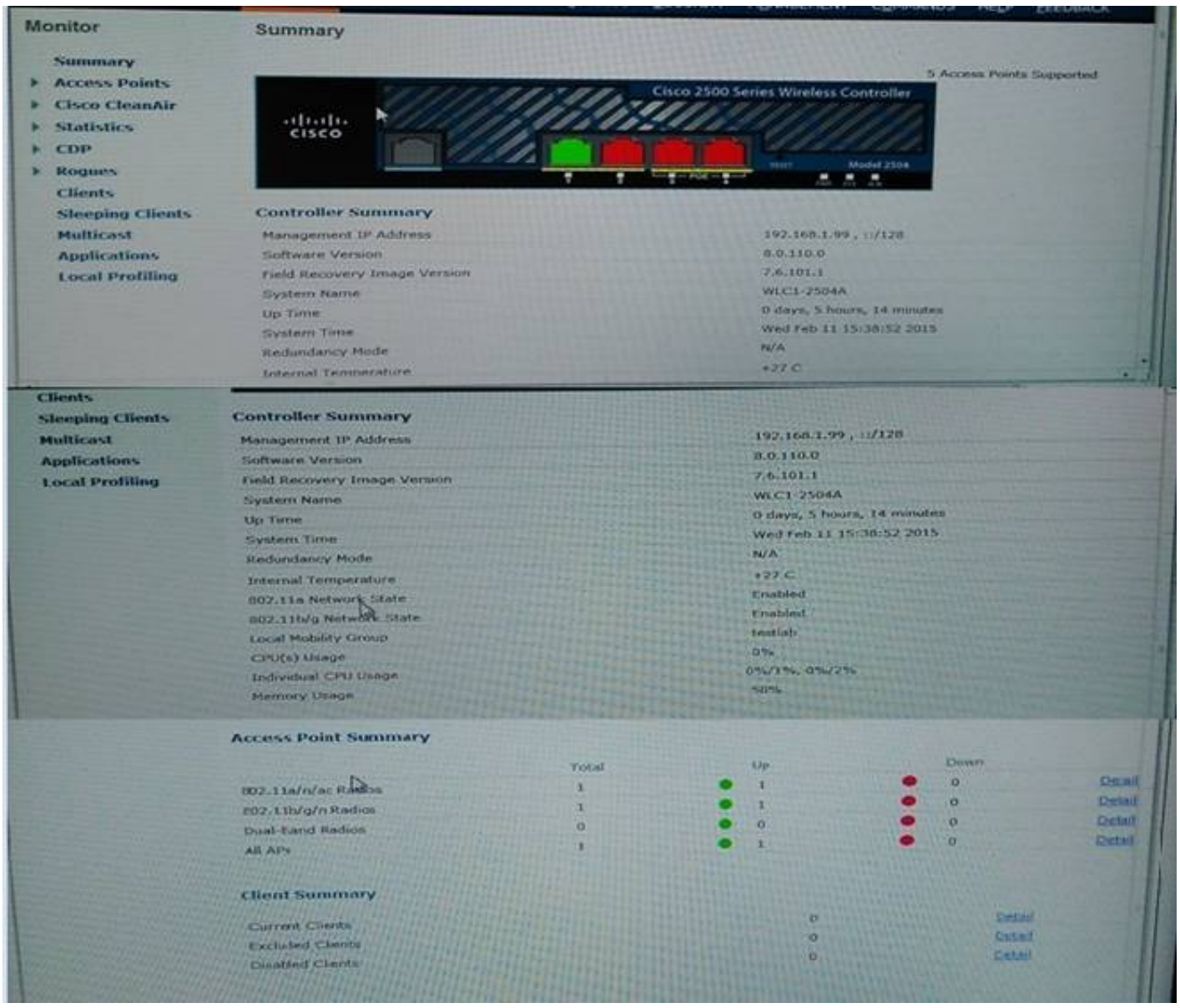
NEW QUESTION 3
Scenario



TOPOLOGY

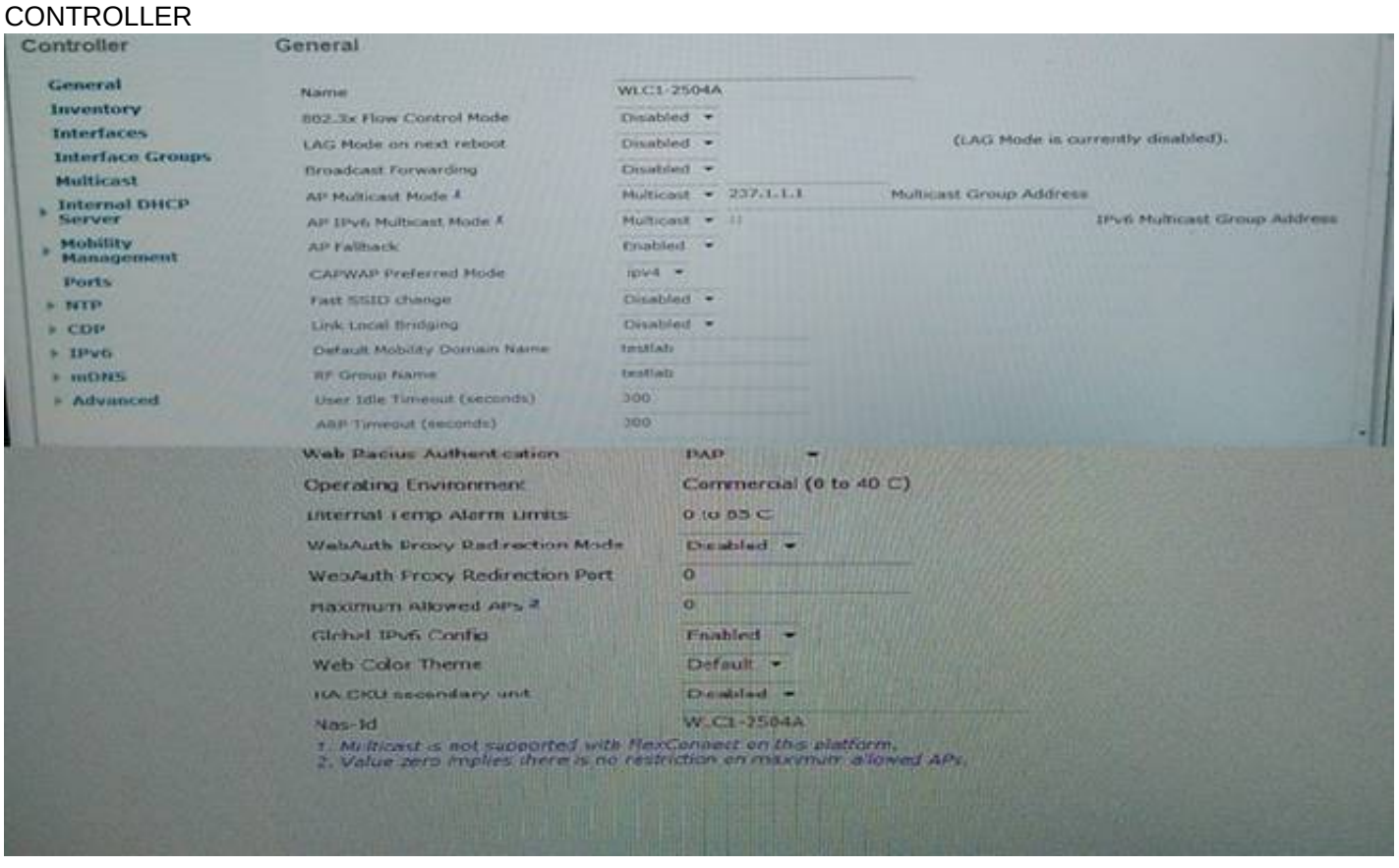


MONITOR



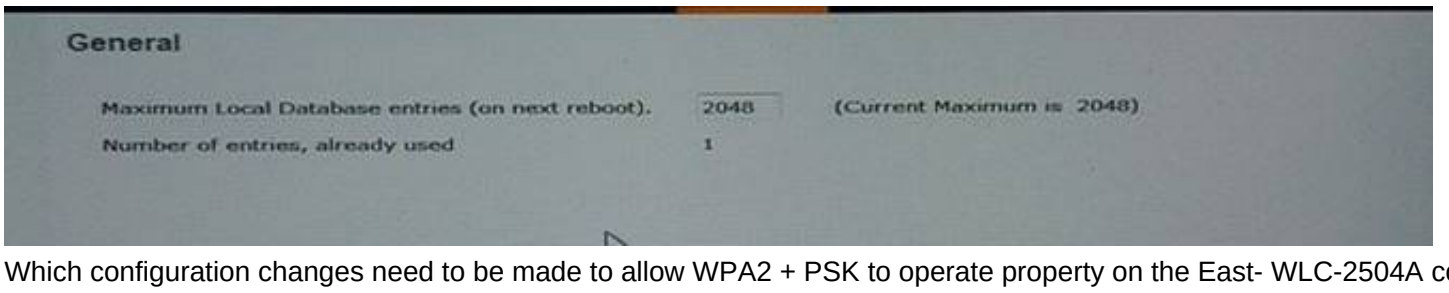
WLAMS

CONTROLLER



WIRELESS

SECURITY



Which configuration changes need to be made to allow WPA2 + PSK to operate property 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 bo

Answer: BFIJ

Explanation:

NEW QUESTION 4
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

Explanation:

NEW QUESTION 5
After receiving an alert regarding a rogue AP, a network engineer logs into Cisco Prime 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 the rogue device is actually inside the campus. The engineer determines the rogue to be a security threat and decides to stop it 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 on WLAN controller resembling the SSID of the rogue to spoof it and 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 containe

Answer: C

Explanation:

NEW QUESTION 6
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

Explanation:

NEW QUESTION 7
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

Explanation:

NEW QUESTION 8
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 controlle

Answer: AB

Explanation:

NEW QUESTION 9
Which security method does a Cisco guest wireless deployment that relies on Cisco ISE guest portal for user authentication use?

A. Layer 2 and Layer 3
B. Layer 2 only
C. No security methods are needed to deploy CWA
D. Layer 3 only

Answer: B

Explanation:

NEW QUESTION 10
Which two options are types of MFP that can be performed? (Choose two.)

A. message integrity check
B. infrastructure
C. client
D. AES-CCMP
E. RSN

Answer: BC

Explanation:

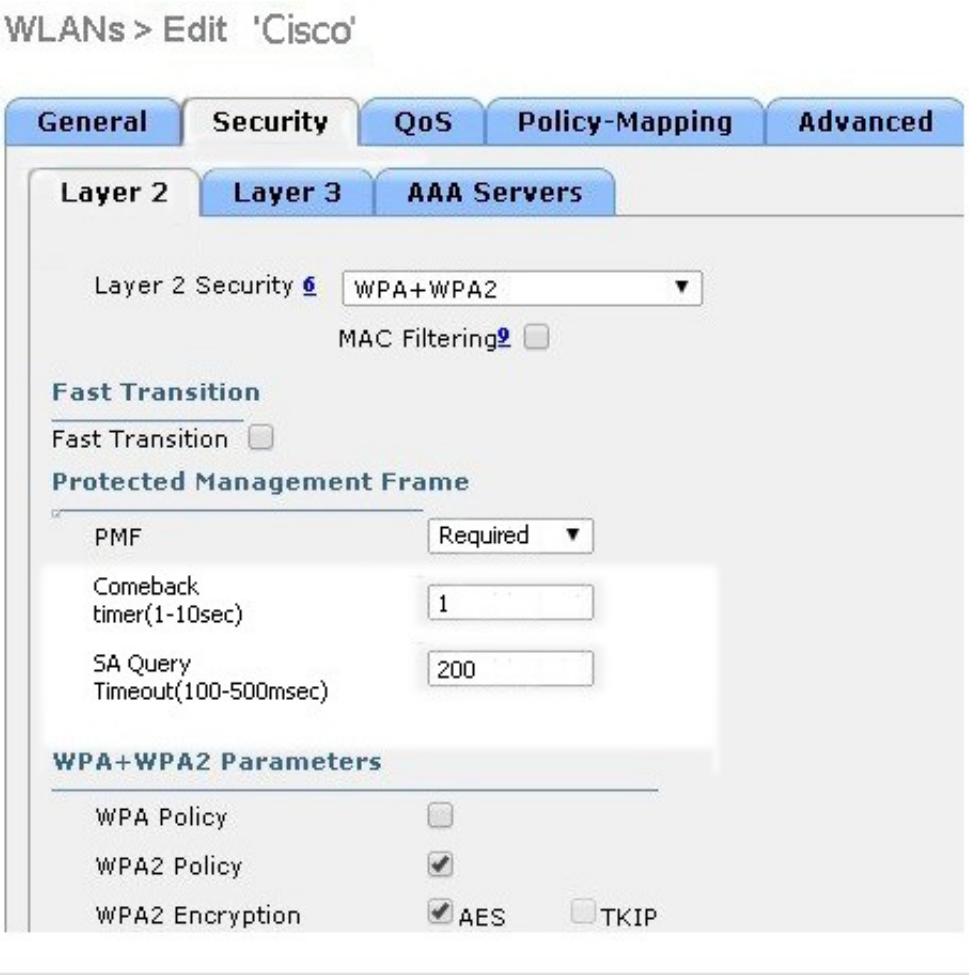
NEW QUESTION 10
An engineer requires authentication for WPA2 that will use fast rekeying to enable clients to roam from one access point to another without going through the controller. Which security option should be configured?

A. PSK
B. AES
C. Cisco Centralized key Management
D. 802.1x

Answer: C

Explanation:

NEW QUESTION 15
Refer to the exhibit.



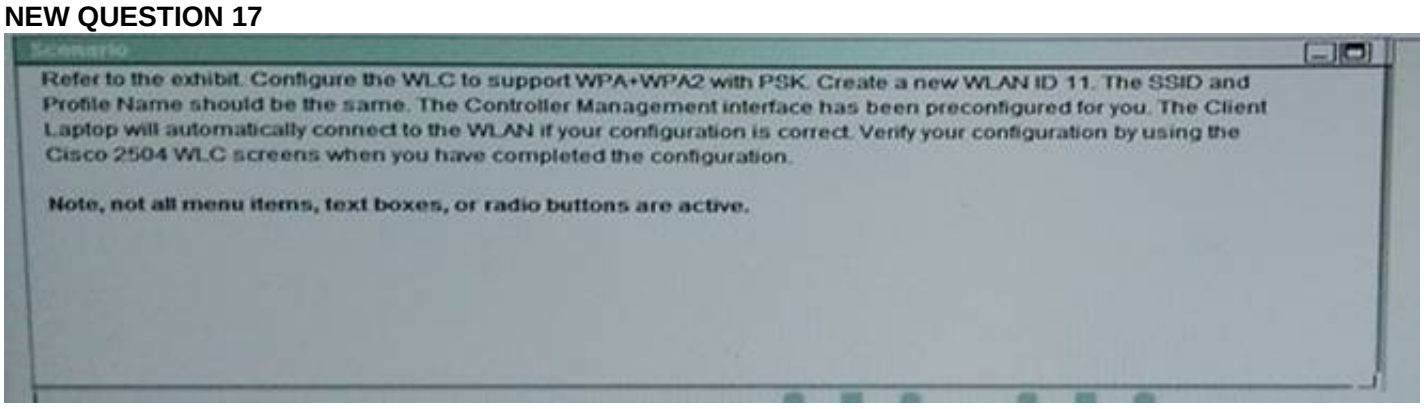
A customer is having problems with clients associating to me wireless network. Based on the configuration, which option describes the most likely cause of the issue?

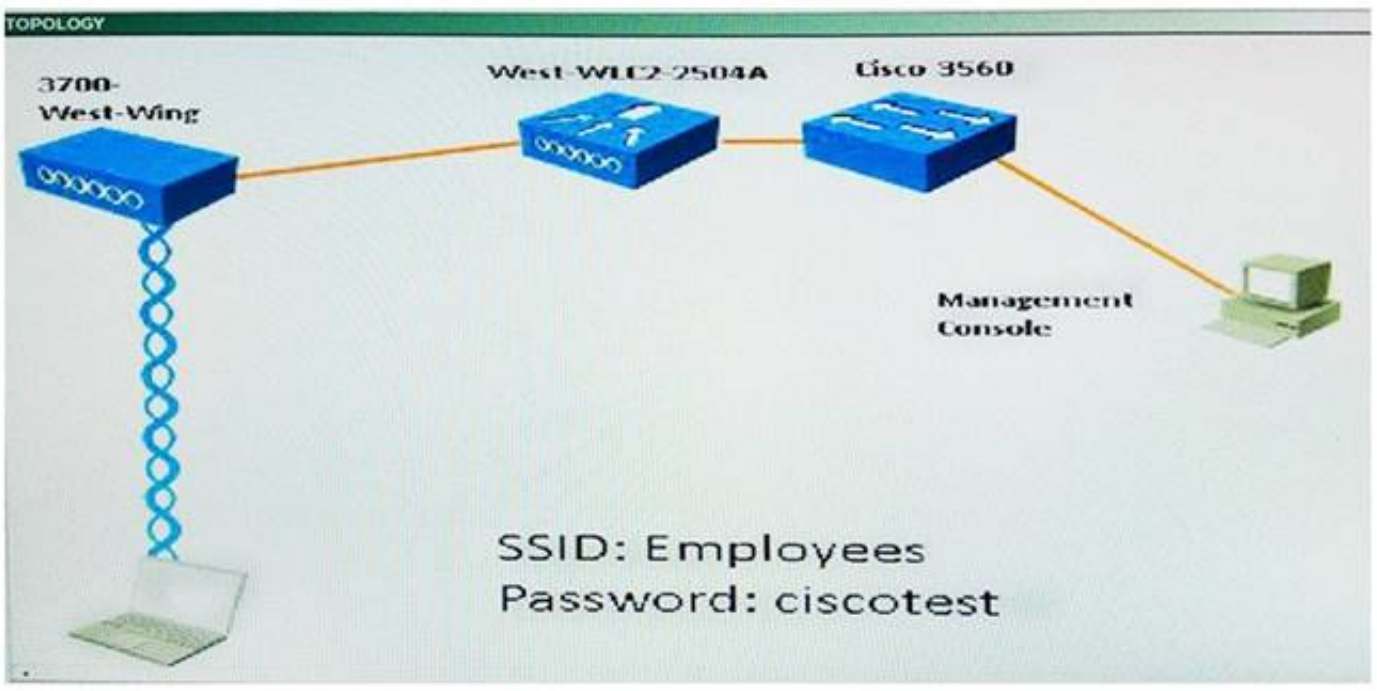
A. Both AES and TKIP must be enabled
B. SA Query Timeout is set too low
C. Comeback timer is set too low
D. PME is set to "required"
E. MAC Filtering must be enabled

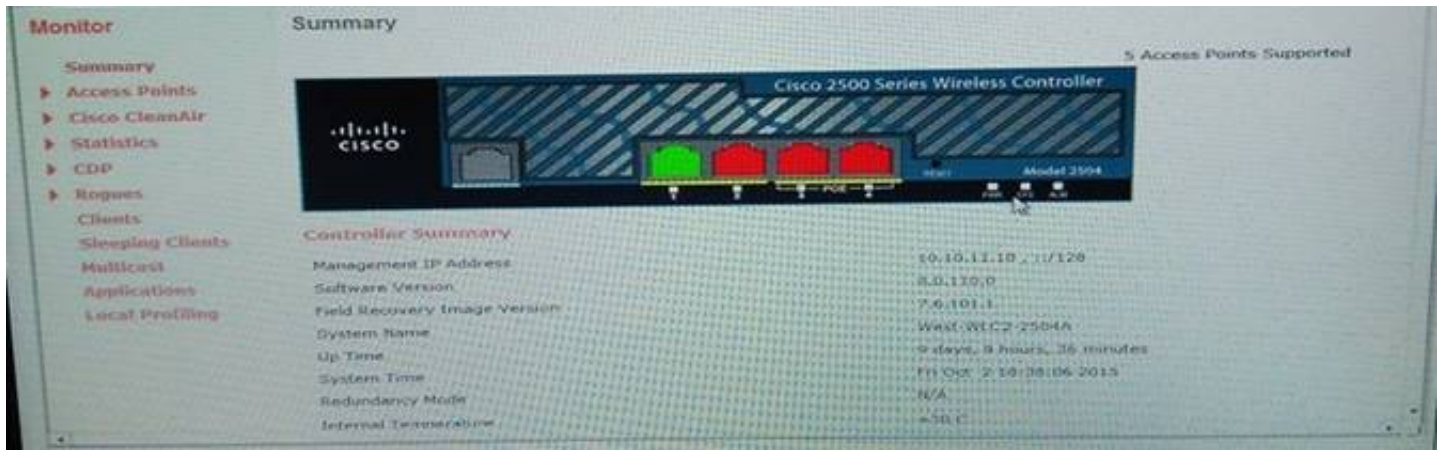
Answer: E

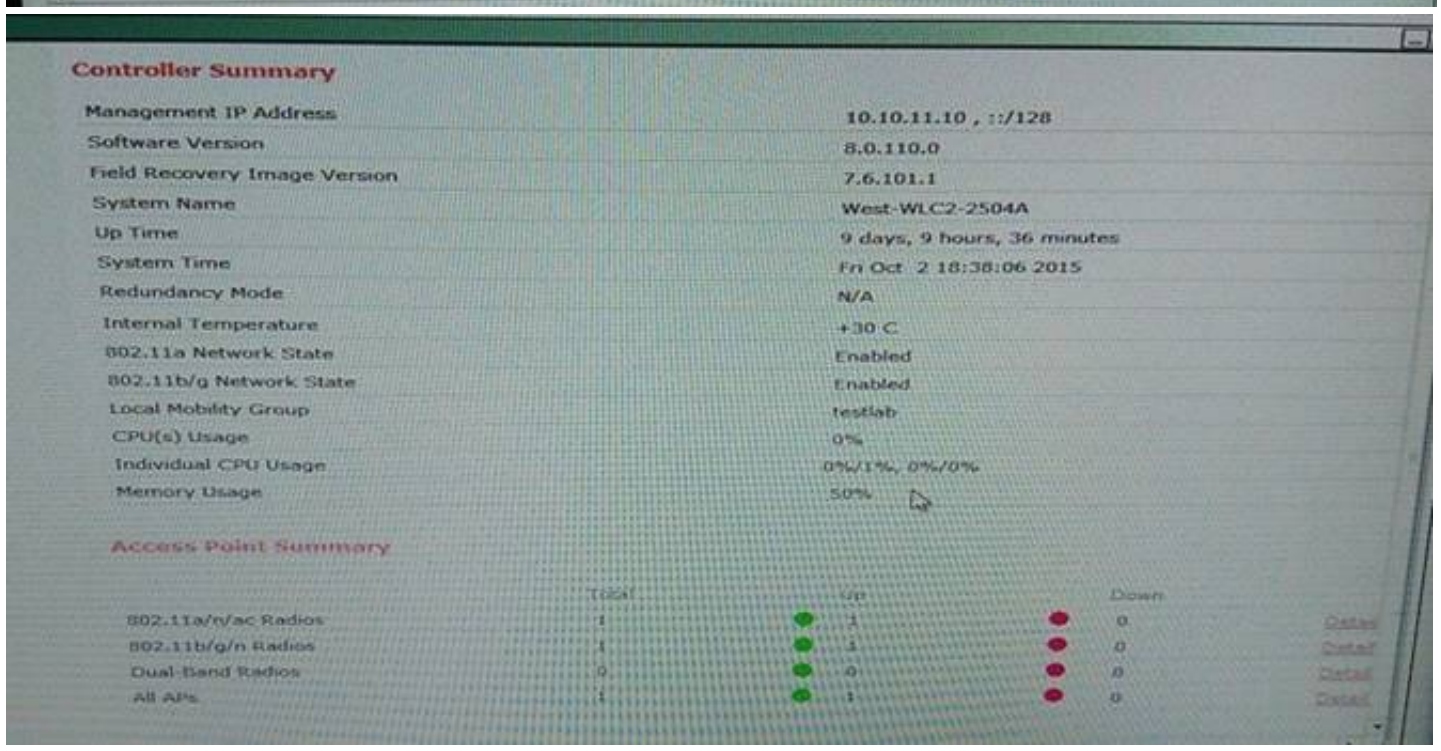
Explanation:

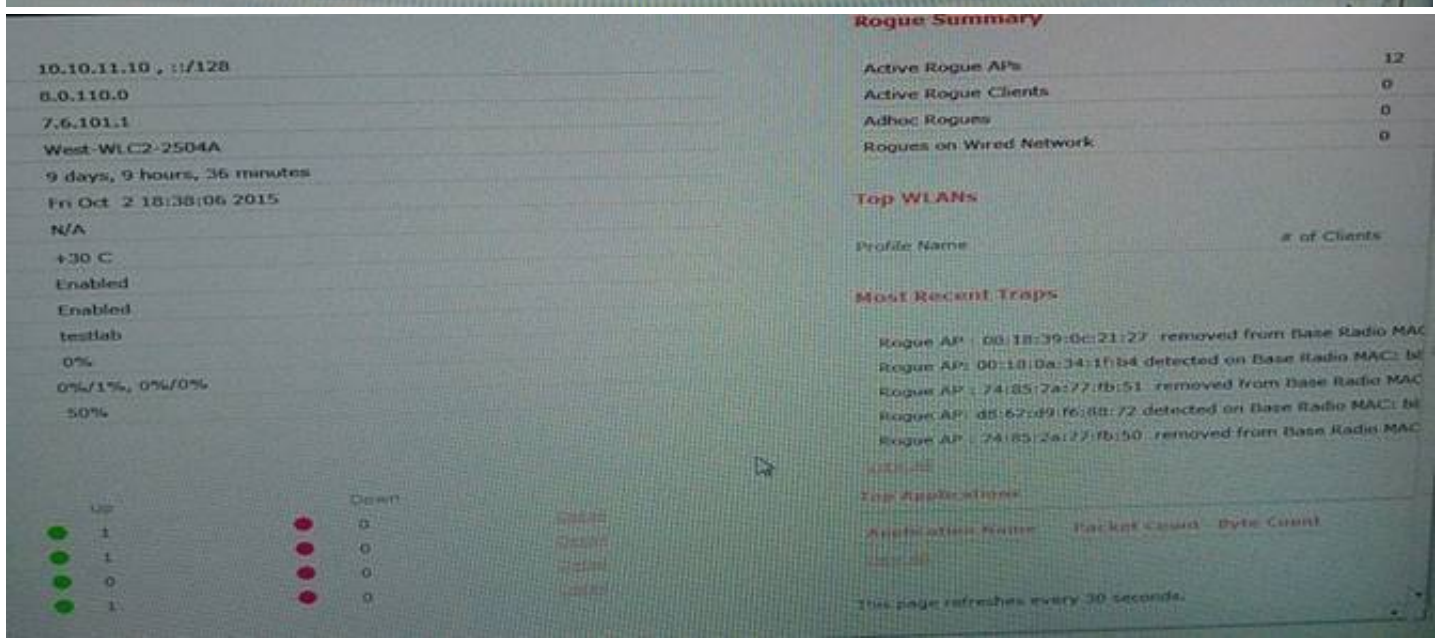
NEW QUESTION 17



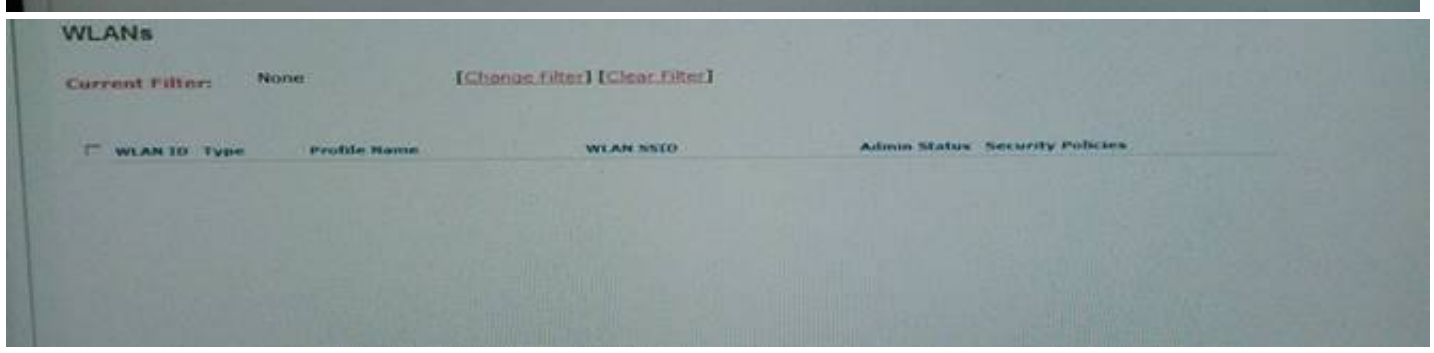


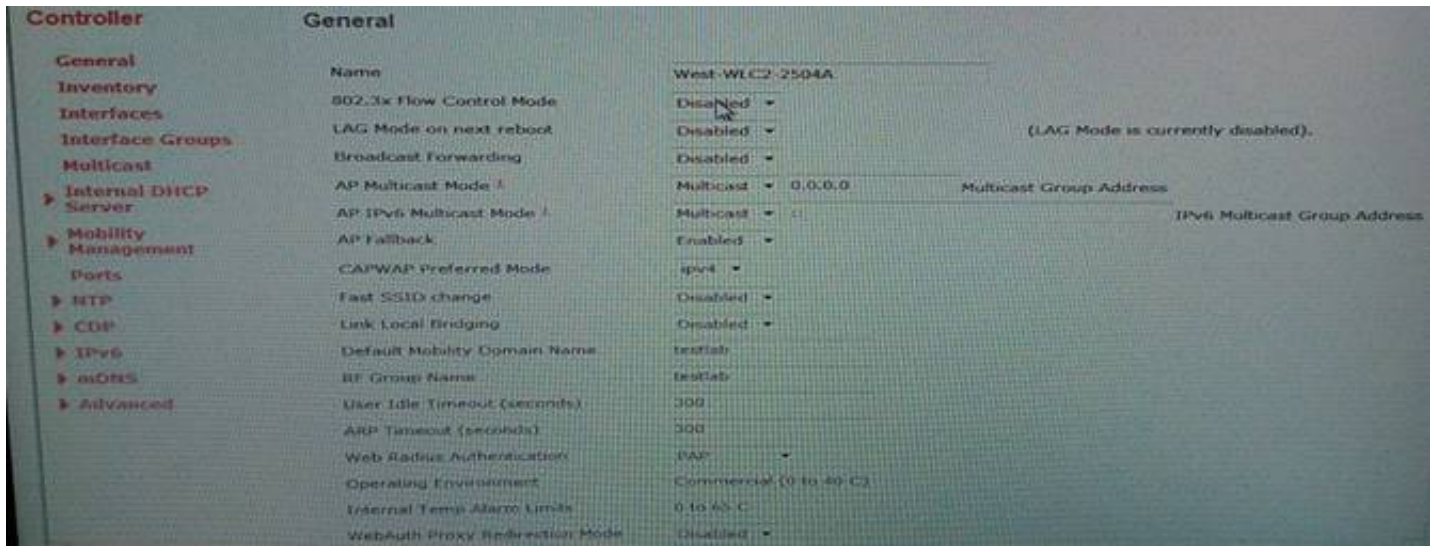

Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Sleeping Clients
Multicast
Applications
Local Profiling
Summary
5 Access Points Supported
Cisco 2500 Series Wireless Controller
Controller Summary
Management IP Address
Software Version
Field Recovery Image Version
System Name
Up Time
System Time
Redundancy Mode
Internal Temperature

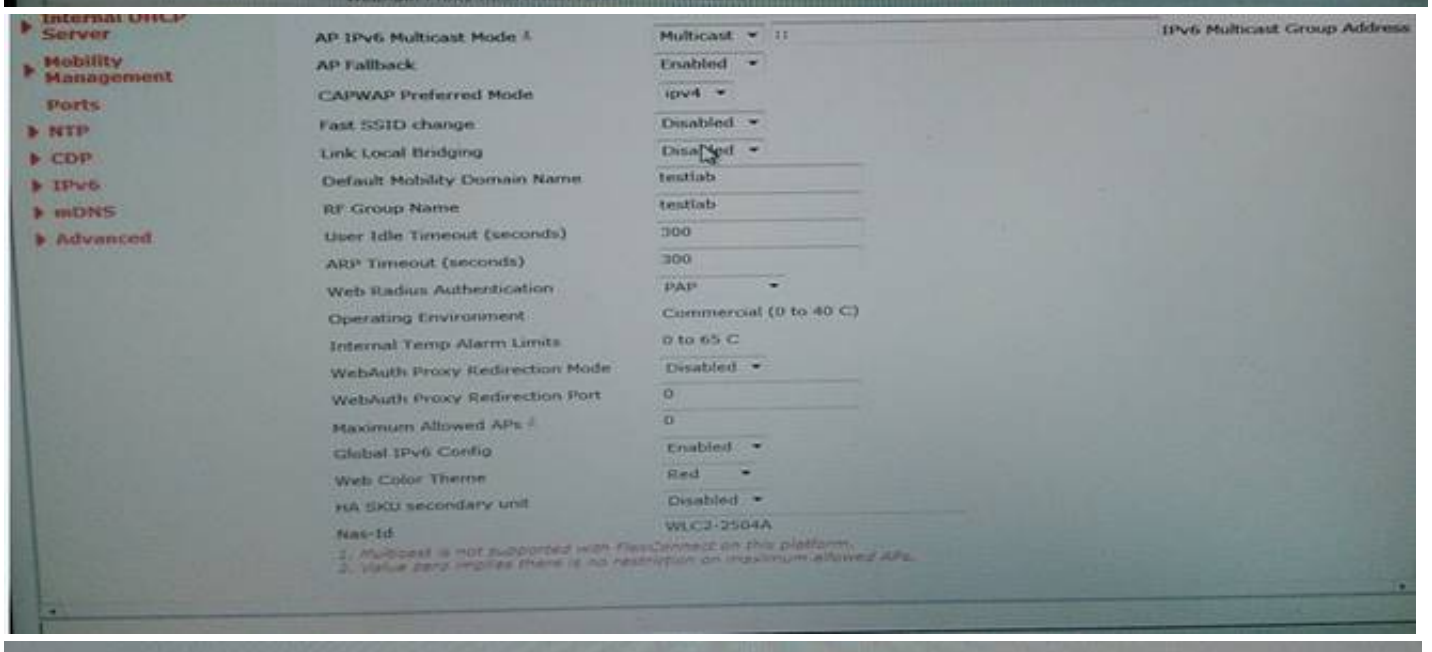

Controller Summary
Management IP Address 10.10.11.10 , ::/128
Software Version 8.0.110.0
Field Recovery Image Version 7.6.101.1
System Name West-WLC2-2504A
Up Time 9 days, 9 hours, 36 minutes
System Time Fri Oct 2 18:38:06 2015
Redundancy Mode N/A
Internal Temperature +30 C
802.11a Network State Enabled
802.11b/g Network State Enabled
Local Mobility Group testlab
CPU(s) Usage 0%
Individual CPU Usage 0%/1%, 0%/0%
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


10.10.11.10 , ::/128
8.0.110.0
7.6.101.1
West-WLC2-2504A
9 days, 9 hours, 36 minutes
Fri Oct 2 18:38:06 2015
N/A
+30 C
Enabled
Enabled
testlab
0%
0%/1%, 0%/0%
50%
Rogue Summary
Active Rogue APs 12
Active Rogue Clients 0
Adhoc Rogues 0
Rogues on Wired Network 0
Top WLANs
Profile Name # of Clients
Most Recent Traps
Rogue AP : 00:18:39:0c:21:27 removed from Base Radio MAC
Rogue AP: 00:18:0a:34:1f:b4 detected on Base Radio MAC: bl
Rogue AP : 74:85:2a:77:fb:51 removed from Base Radio MAC
Rogue AP: d8:67:d9:f6:88:72 detected on Base Radio MAC: bl
Rogue AP : 74:85:2a:77:fb:50 removed from Base Radio MAC
Top Applications
Application Name Packet Count Byte Count
This page refreshes every 30 seconds.


Internal Temperature +30 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%/0%
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


WLANs
Current Filter: None [Change Filter] [Clear Filter]
WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies





Answer:

Explanation: Please refer the link below in Explanation to configure this simulation.
Example:
Use this link to configure all the steps for this simulation : http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-configwpa2-psk-00.html

NEW QUESTION 20
Which Cisco feature must an engineer configure on a cisco WLC to enable PCI specification compliance for communication of neighbor radio information?

A. RF Grouping
B. MFP
C. Rogue Access Point Detection
D. RRM NDP
E. Off Channel Scanning

Answer: D

Explanation:

NEW QUESTION 25

MFP is enabled globally on a WLAN with default settings on single controller wireless network. Older client devices are disconnected from the network during a deauthentication attack. What is the
cause of this issue?

A. The client devices do not support WPA.
B. The client devices do not support CCXv5.
C. The MFP on the WLAN is set to optional
D. The NTP server is not configured on the controlle

Answer: C

Explanation:

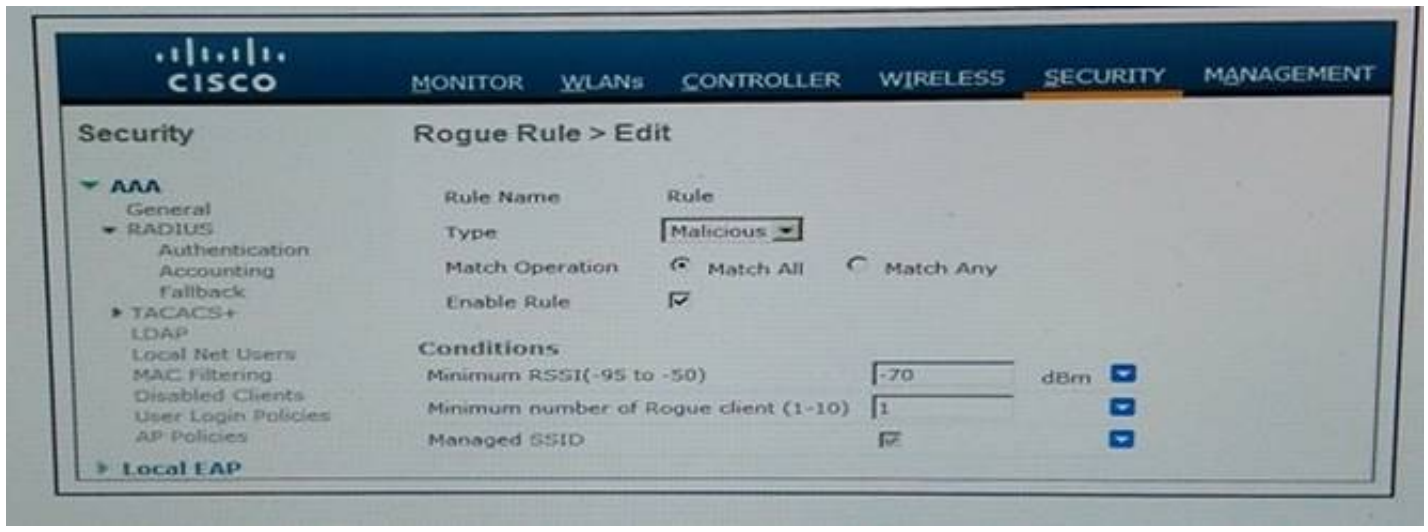
NEW QUESTION 27
An engineer must enable EAP on a new WLAN and is ensuring that the necessary components are available. Which component uses EAP and 802.1x to pass user authentication to the authenticator?

A. AP
B. AAA server
C. supplicant
D. controller

Answer: D

Explanation:

NEW QUESTION 31
Refer to the exhibit.



A WLAN with the SSID "Enterprise" is configured. Which rogue is marked as malicious?

A. a rogue with two clients, broadcasting the SSID "Employee" heard at -50 dBm
B. a rogue with no clients, broadcasting the SSID "Enterprise" heard at -50 dBm
C. a rouge with two clients, broadcasting the SSID "Enterprise" heard at -80 dBm
D. a rogue with two clients, broadcasting the SSID "Enterprise" heard at -50 dBm

Answer: C

Explanation:

NEW QUESTION 34
On which two ports does the RADIUS server maintain a database and listen for incoming authentication and accounting requests? (Choose two.)

A. UDP 1900
B. UDP port 1812
C. TCP port 1812
D. TCP port 1813
E. UDP port 1813

Answer: BE

Explanation:

NEW QUESTION 37
Which command is an SNMPv3-specific command that an engineer can use only in Cisco IOS XE?

A. snmp-server user remoteuser1 group1 remote 10.12.0.4
B. snmp-server host 172.16.1.33 public
C. snmp-server community comaccess ro 4
D. snmp-server enable traps wireless

Answer: A

Explanation:

NEW QUESTION 38
An engineer must provide a graphical trending report of the total number of wireless clients on the network. Winch report provides the required data?

A. Client Summary
B. Posture Status Count
C. Client Traffic Stream Metrics
D. Mobility Client Summary

Answer: D

Explanation:

NEW QUESTION 43
When a wireless client uses WPA2 AES, which keys are created at the end of the four way handshake process between the client and the access point?

A. AES key, TKIP key, WEP key
B. AES key, WPA2 key, PMK
C. KCK, KEK, TK
D. KCK, KEK, MIC key

Answer: A

Explanation:

NEW QUESTION 45
Which customizable security report on Cisco Prime Infrastructure would show rogue APs detected since a point in time?

A. New Rogue APs
B. Rogue AP Events
C. Rogue APs
D. Rogue AP Count Summary
E. Network Summary

Answer: C

Explanation:

NEW QUESTION 50
A corporation has recently implemented a BYOD policy at their HQ. Which three risks should the security director be concerned about? (Choose three.)

A. unauthorized users
B. rogue ad-hocs
C. software piracy
D. lost and stolen devices
E. malware
F. keyloggers

Answer: ACE

Explanation:

NEW QUESTION 51
Which three options are valid client profile probes m Cisco ISE? (Choose three.)

A. DHCP
B. 802.1X
C. CCX
D. NetFlow
E. TACACS
F. HTTP

Answer: ADF

Explanation:

NEW QUESTION 54
A customer is concerned about DOS attacks from a neighboring facility. Which feature can be enabled to help alleviate these concerns and mitigate DOS attacks on a WLAN?

A. PMF
B. peer-to-peer blocking
C. Cisco Centralized Key Management
D. split tunnel

Answer: A

Explanation:

NEW QUESTION 58
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: AC

Explanation:

NEW QUESTION 62
How many mobility peers can a Cisco Catalyst 3850-MC node have?

A. 8
B. 2
C. 6
D. 16
E. 4

Answer: A

Explanation:

NEW QUESTION 63
Which client roam is considered the fastest in a wireless deployment using Cisco IOS XE mobility controllers and mobility agents?

A. Roam within stack members
B. Inter-SPG roam
C. Interdomain roam
D. Intermobility roam
E. lntra-SPG roam

Answer: B

Explanation:
• Inter-SPG, Intra-subdomain roaming?The client roaming between mobility agents in different SPGs
within the same subdomain. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/system_management/configuration_guide/b_sm_3se_3850_cg/b_sm_3se_3850_cg_chapter_0111.pdf

NEW QUESTION 66
An engineer is deploying EAP-TLS as the authentication mechanism for an 802.1X-enabled wireless network. Which network device is responsible for applying the digital signature to a certificate to ensure that the certificate is trusted and valid?

A. supplicant
B. CA server
C. wireless controller
D. authentication server

Answer: B

Explanation:

NEW QUESTION 67
Which EAP type requires the use of device certificates?

A. EAP-TLS
B. EAP-FAST
C. EAP-SSL
D. PEAP
E. LEAP

Answer: A

Explanation:

NEW QUESTION 71
A Cisco WLC has been added to the network and Cisco ISE as a network device, but authentication is failing. Which configuration within the network device configuration should be verified?

A. shared secret
B. device ID
C. SNMP RO community
D. device interface credentials

Answer: A

Explanation:

NEW QUESTION 74
Which three commands are part of the requirements on Cisco Catalyst 3850 series Switch with Cisco IOX XE to create a RADIUS authentication server group? (Choose three.)

A. authentication dot1x default local
B. aaa session-idcommon
C. dot1x system-auth-control
D. aaa new-model
E. local-auth wcm_eap_prof
F. security dot1x

Answer: BCD

Explanation:

NEW QUESTION 79
When a supplicant and AAA server are configured to use PEAP, which mechanism is used by the client to authenticate the AAA server in Phase One?

A. PMK
B. shared secret keys
C. digital certificate
D. PAC

Answer: C

Explanation:

NEW QUESTION 84
What are two of the benefits that the Cisco AnyConnect v3.0 provides to the administrator for client WLAN security configuration? (Choose two.)

A. Provides a reporting mechanism for rouge APs
B. Prevents a user from adding any WLANs
C. Hides the complexity of 802.1X and EAP configuration
D. Supports centralized or distributed client architectures
E. Provides concurrent wired and wireless connectivity
F. Allows users to modify but not delete admin-created profiles

Answer: CD

Explanation:

NEW QUESTION 86
Which two attacks represent a social engineering attack? (Choose two.)

A. using AirMagnet Wi-Fi Analyzer to search for hidden SSIDs
B. calling the IT helpdesk and asking for network information
C. spoofing the MAC address of an employee device
D. entering a business and posing as IT support staff

Answer: BD

Explanation:

NEW QUESTION 88
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. The controller will immediately revert back after it receives a RADIUS probe from the primary server.
C. After the inactive time expires the controller will send RADIUS to the primary.
D. Once RADIUS probe messages determine the primary controller is active the controller will revert back to the primary RADIUS.

Answer: C

Explanation:

NEW QUESTION 93
Clients are failing EAP authentication. A debug shows that an EAPOL start is sent and the clients are then de-authenticated. Which two issues can cause this

problem? (Choose two.)

A. The WLC certificate has changed.
B. The WLAN is not configured for the correct EAP supplicant type.
C. The shared secret of the WLC and RADIUS server do not match.
D. The WLC has not been added to the RADIUS server as a client.
E. The clients are configured for machine authentication, but the RADIUS server is configured for user authentication.

Answer: CD

Explanation:

NEW QUESTION 94
How should the Cisco Secure ACS v4.2 and the Cisco WLC v7.0 be configured to support wireless client authentication?

A. The WLC configured for RADIUS and the Cisco Secure ACS configured for RADIUS (Cisco Airespace)
B. The WLC configured for RADIUS and the Cisco Secure ACS configured for RADIUS (IETF)
C. The WLC configured for TACACS+ and the Cisco Secure ACS configured for TACACS+ (Cisco Airespace)
D. The WLC configured for TACACS+ and the Cisco Secure ACS configured for TACACS+ (Cisco IOS)

Answer: A

Explanation:

NEW QUESTION 98
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. client profiling
C. AAA override
D. captive bypassing
E. identity-based networking

Answer: C

Explanation:

NEW QUESTION 103
802.1X AP supplicant credentials have been enabled and configured on a Cisco WLC v7.0 in both the respective Wireless>AP>Global Configuration location and AP>Credentials tab locations. What describes the 802.1X AP authentication process when connected via Ethernet to a switch?

A. Only WLC AP global credentials are used.
B. Only AP credentials are used.
C. WLC global AP credentials are used first; upon failure, the AP credentials are used.
D. AP credentials are used first; upon failure, the WLC global credentials are use

Answer: B

Explanation:

NEW QUESTION 107
Client Management Frame Protection is supported on which Cisco Compatible Extensions version clients?

A. v2 and later
B. v3 and later
C. v4 and later
D. v5 only

Answer: D

Explanation:

NEW QUESTION 108
Which three items must be configured on a Cisco WLC v7.0 to allow implementation of isolated bonding network? (Choose three.)

A. RADIUS server IP address
B. DHCP IP address
C. SNMP trap receiver IP address
D. interface name
E. SNMP community name
F. ACL name

Answer: ADF

Explanation:

NEW QUESTION 110
Which attribute on the Cisco WLC v7.0 does RADIUS IETF attribute "Tunnel-Private-Group ID" assign?

A. ACL
B. DSCP
C. QoS
D. VLAN

Answer: D

Explanation:

NEW QUESTION 114
What two actions must be taken by an engineer configuring wireless Identity-Based Networking for a WLAN to enable VLAN tagging? (Choose two.)

A. enable AAA override on the WLAN
B. create and apply the appropriate ACL to the WLAN
C. update the RADIUS server attributes for tunnel type 64, medium type 65, and tunnel private group type 81
D. configure RADIUS server with WLAN subnet and VLAN ID
E. enable VLAN Select on the wireless LAN controller and the WLAN

Answer: AC

Explanation:

NEW QUESTION 116
Which three properties are used for client profiling of wireless clients? (Choose Three)

A. MAC OUI
B. IP Address
C. HTTP user agent
D. DHCP
E. hostname
F. OS Version

Answer: ACD

Explanation:

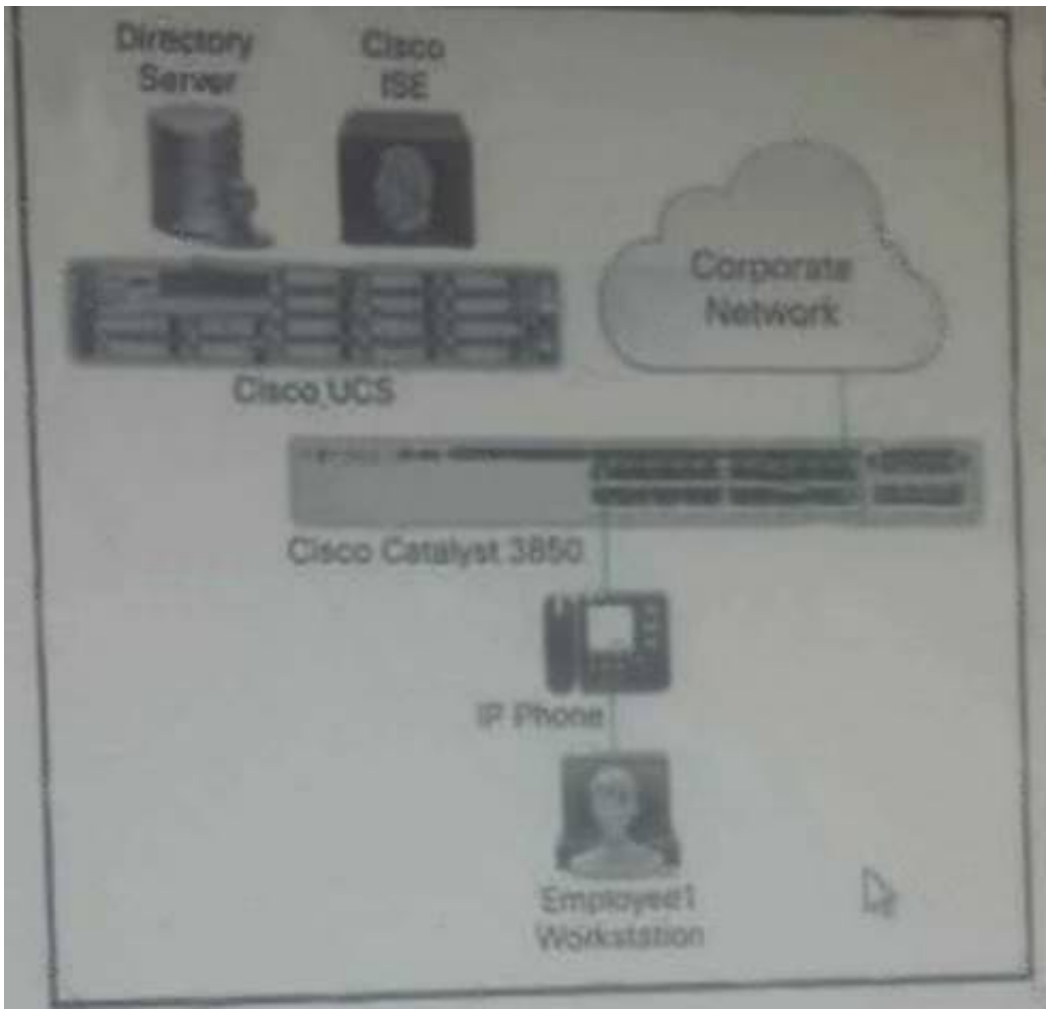
NEW QUESTION 118
A company wants to switch to BYOD to reduce IT support costs for the company. Which option is an impact of BYOD that should be considered?

A. increased VPN connections
B. restricted device enforcement
C. increased phishing attacks.
D. decreased support calls

Answer: A

Explanation:

NEW QUESTION 123
Refer to the exhibit.



In this IBN topology, which device acts as the RADIUS server?

A. directory server
B. Cisco ISE
C. Cisco UCS
D. Cisco Catalyst 3850 Series Switch

Answer: D

Explanation:

NEW QUESTION 127
Regarding the guidelines for using MFP, under what circumstances will a client without Cisco compatible Extensions v5 be able to associate to a WLAN?

A. The DHCP Required box is unchecked.
B. AAA override is configured for the WLAN
C. Client MFP is disabled or optional.
D. WPA2 is enabled with TKIP or AE

Answer: D

Explanation:

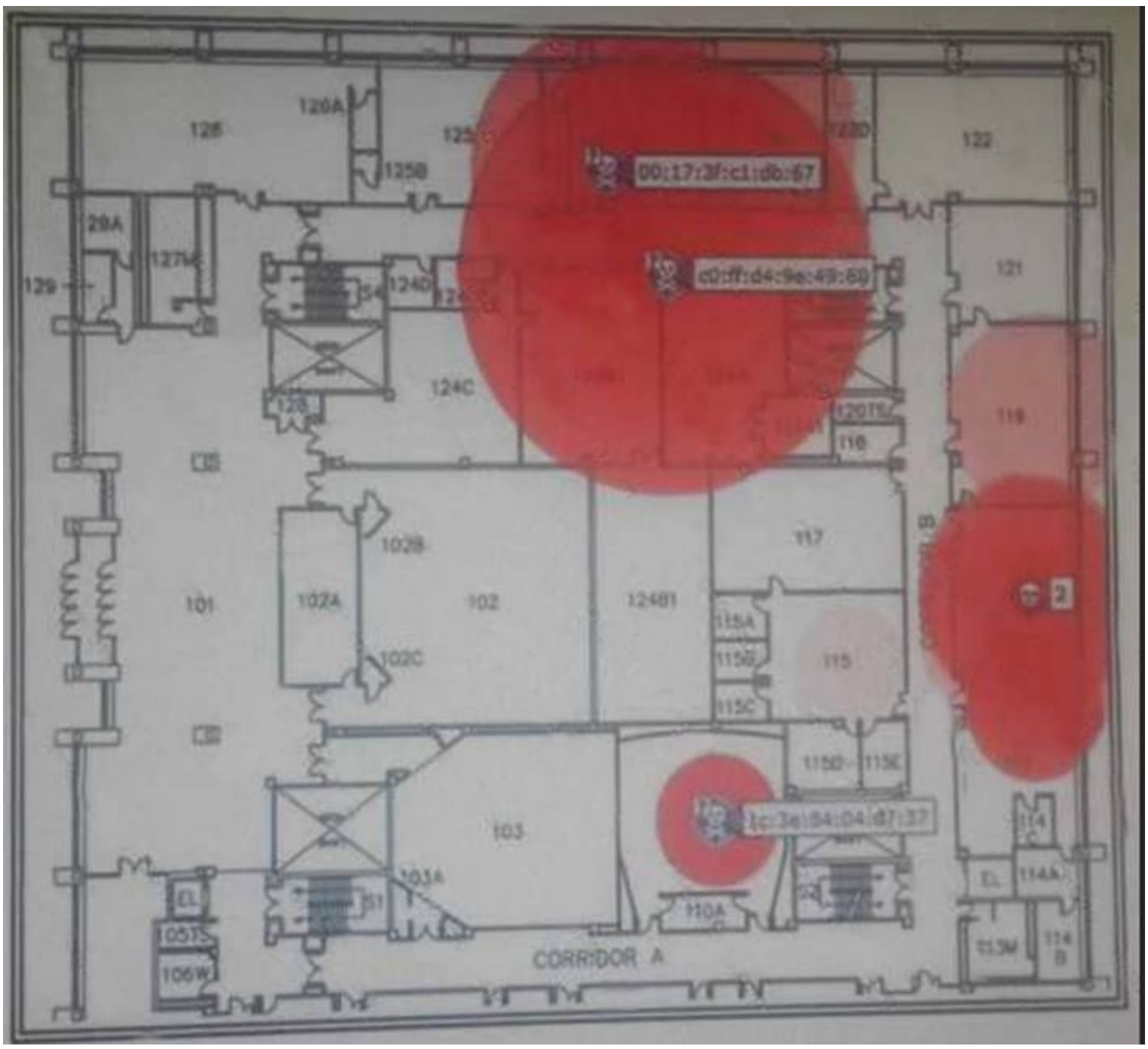
NEW QUESTION 130
An engineer is working on a remote site that is configured using FlexConnect. They are worried that the access points will not send RADIUS requests directly to the authentication server is standalone mode. Which command ensures direct authentication using the default ports as defined on the WLC?

A. config filexconnect group Remote radius server acct add primary 10.10.10.10 1813 Cisco123
B. config filexconnect group Remote radius server auth add primary 10.10.10.10 1813 Cisco123
C. config filexconnect group Remote radius server acct add primary 10.10.10.10 1812 Cisco123
D. config filexconnect group Remote radius server auth add primary 10.10.10.10 1812 Cisco123

Answer: C

Explanation:

NEW QUESTION 135
Refer to the exhibit. What do the red circles represent in the exhibit?



A. detected interferes
B. RSSI cutoff
C. wIPs attackers
D. zones of impact

Answer: C

Explanation:

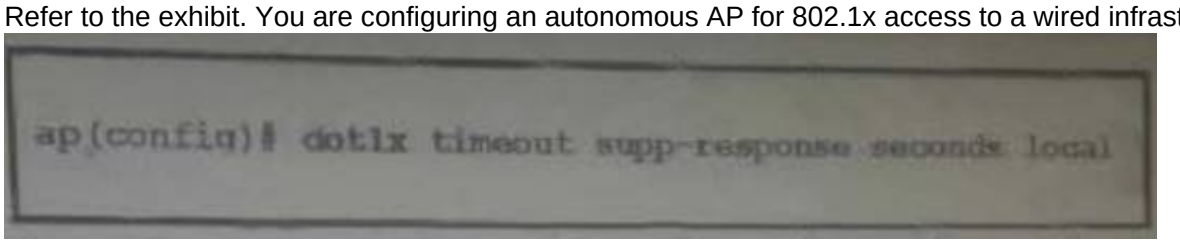
NEW QUESTION 138
An engineer is configuring central web authentication using a Cisco 5508 wireless controller and the Cisco identity Service Engine. Which two attributes must be configured on Cisco ISE to add the controller as a network device? (Choose two.)

A. authentication protocol
B. RADIUS shared secret
C. out-of-band SGA PAC
D. controller IP address
E. controller software version

Answer: DE

Explanation:

NEW QUESTION 143
Refer to the exhibit. You are configuring an autonomous AP for 802.1x access to a wired infrastructure. What does the command do?



A. It enables the AP to override the authentication timeout on the RADIUS server.
B. It configures how long the AP must wait for a client to reply to an EAP/dot1x message before the authentication fails.
C. It enables the supplicant to override the authentication timeout on the client
D. It configures how long the RADIUS server must wait for supplicant to reply to an EAP/dot1x message before the authentication fails.

Answer: C

Explanation:

NEW QUESTION 144
An engineer is troubleshooting rogue access points that are showing up in Cisco Prime Infrastructure. What is the 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: B

Explanation:
https://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010 111001.html

NEW QUESTION 148
When a network engineer plans to implement the client MFP, which three settings should be supported by the client? (Choose three)

A. WPA2 with AES
B. Short Preamble check box
C. WPA2 with TKIP
D. WEP
E. WPA with TKIP
F. Cisco Compatible Extensions v5

Answer: ACF

Explanation:

NEW QUESTION 153
Which two statements describe the requirements for EAP-TLS?

A. It requires client-side and server-side certificates.
B. It uses PAC on the client.
C. It requires PKI.
D. It requires a server side digital certificate on only the RADIUS server
E. It must use AES for encryption and cannot use TKIP for encryptio

Answer: AB

Explanation:

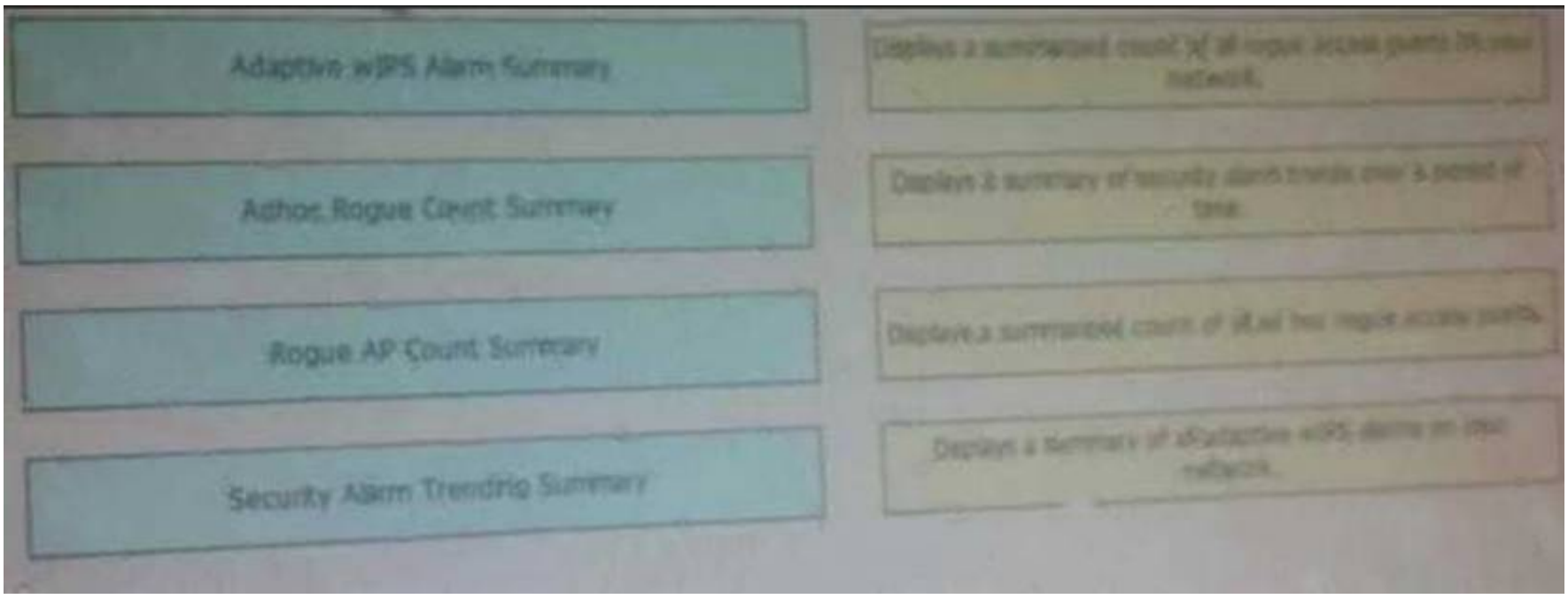
NEW QUESTION 154
An engineer has configured the wireless controller to authenticate clients on the employee SSID against Microsoft Active Directory using PEAP authentication. Which protocol does the controller use to communicate with the authentication server?

A. EAP
B. 802.1x
C. RADIUS
D. WPA2

Answer: A

Explanation:
Define the Layer 2 Authentication as WPA2 so that the clients perform EAP-based authentication (PEAP-MS-CHAP v2 in this example) and use the advanced encryption standard (AES) as the encryption mechanism. Leave all other values at their defaults. https://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/115988-nps-wlc-config-000.html

NEW QUESTION 159
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.



Answer:

Explanation:

NEW QUESTION 162
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 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: C

Explanation:

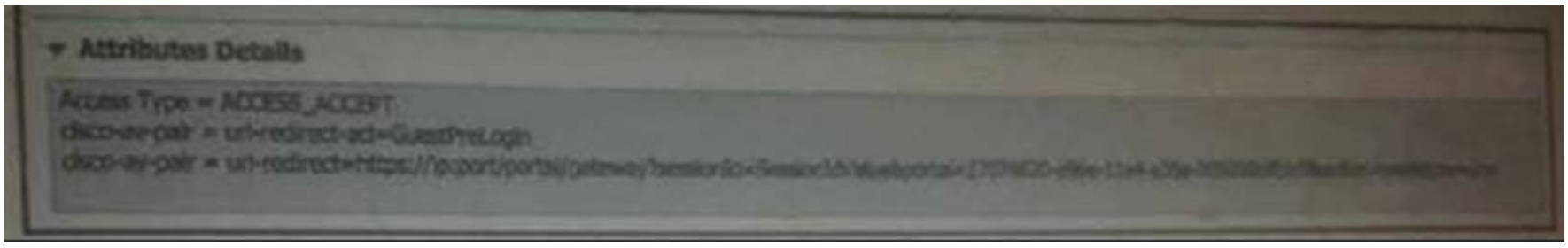
NEW QUESTION 167
An engineer is designing a high availability wireless network. What mechanism should be the focus for high availability?

A. SNR
B. channel reuse
C. RSSI
D. cell overlap

Answer: B

Explanation:
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

NEW QUESTION 170
Refer to the exhibit. The security team has configured an IBN profile on ISE for the guest wireless network to provide captive portal service. Where must the network engineer configure the ACL and portal for the Cisco AireOS controller?



A. GuestPreLogin downloadable ACL on ISE, login portal on ISE
B. GuestPreLogin local ACL on WLC, login portal on WLC
C. GuestPreLogin downloadable ACL on ISE, login portal on WLC
D. GuestPreLogin local ACL on WLC, login portal on ISE

Answer: C

Explanation:
The flow would be the following:
-User associate to the Web Auth SSID
-User starts its browser
-The WLC Redirect to the guest portal (ISE/NGS)
-The user authenticate on the portal
-The Guest Portal redirect back to the WLC with the credentials entered
-The WLC Authenticate the guest user via Radius
-The WLC Redirects back to the original URL.
https://supportforums.cisco.com/t5/wireless-mobility-documents/central-web-authentication-cwafor- guests-with-ise/ta-p/3121101

NEW QUESTION 172
An engineer is configuring EAP-TLS with a client trusting server model and has configured a public root certification authority. Which action does this allow?

A. specifies a second certification authority to trust
B. utilizes two subcertification authority servers
C. creates a PKI infrastructure
D. validates the AAA server

Answer: D

Explanation:
To support EAP-TLS, the AAA server (for example, Cisco Secure ACS) must have a certificate. Either a public certification authority or a private certification authority can be used to issue the AAA server certificate. The AAA server will trust a client certificate that was issued from the same root certification authority that issued its certificate.
https://www.cisco.com/en/US/tech/ CK7 22/ CK8 09/technologies_white_paper09186a008009256b.sht ml

NEW QUESTION 174
An engineer is configuring an autonomous AP for RADIUS authentication. What two pieces of information must be known to configure the AP? (Choose two.)

A. shared secret
B. username and password
C. RADIUS IP address
D. group name
E. PAC encryption key

Answer: AC

Explanation:
You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_rad/configuration/xe-3se/3850/secusr- rad-xe-3se-3850-book/sec-rad-mult-udp-ports.html

NEW QUESTION 179
When implementing secure PCI wireless networks, which two are specific recommendations in the PCI DSS? (Choose two)

A. Use a minimum 12-character random passphrase with WPA
B. Segment logging events with other networking devices within the organization.
C. Use VLAN based segmentation with MAC filters.
D. Change default settings.
E. Implement strong wireless authentication

Answer: DE

Explanation:
Wireless networks that are part of the CDE must comply with all PCI DSS requirements. This includes using a firewall (requirement 1.2.3) and making sure that additional rogue wireless devices have not been added to the CDE (requirement 11.1). In addition, PCI DSS compliance for systems that include WLANs as a part of the CDE requires extra attention to WLAN specific technologies and processes such as:
A. Physical security of wireless devices, B. Changing default passwords and settings on wireless devices, C. Logging of wireless access and intrusion prevention,

D. Strong wireless authentication and encryption, E. Use of strong cryptography and security protocols, and F. Development and enforcement of wireless usage policies. This section will cover each of these requirements sequentially. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

NEW QUESTION 181
An engineer configures 802.1 X authentication for the access points using the config ap 802.1Xuser add username admin password secret AP_01 command. Which EAP method does the access point use to authenticate?

A. EAP-TLS
B. MS-CHAPv2 PEAP
C. LEAP
D. EAP-FAST

Answer: D

Explanation:
Enables or disables Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) authentication. https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/cmdref/b_cr80/config_commands_a_to_i.html

NEW QUESTION 183
Which two requirements must be met to ensure that Cisco ISE can join the Active Directory domain of the company. (Choose two.)

A. If a firewall exists between Cisco ISE and Active Directory domain server, these ports are allowed through UDP 69, 123, and 389; and TCP 88, 389, 445, 464, 636, 3268, and 3269.
B. The hostname of Cisco ISE is less than 20 characters in length.
C. An account has been created in Active Directory for Cisco ISE that has the necessary permissions.
D. The DNS name is configured on Cisco ISE and resolved on the Active Directory domain server
E. Time synchronization between Cisco ISE and Active Directory must be within 10 minute

Answer: CD

Explanation:

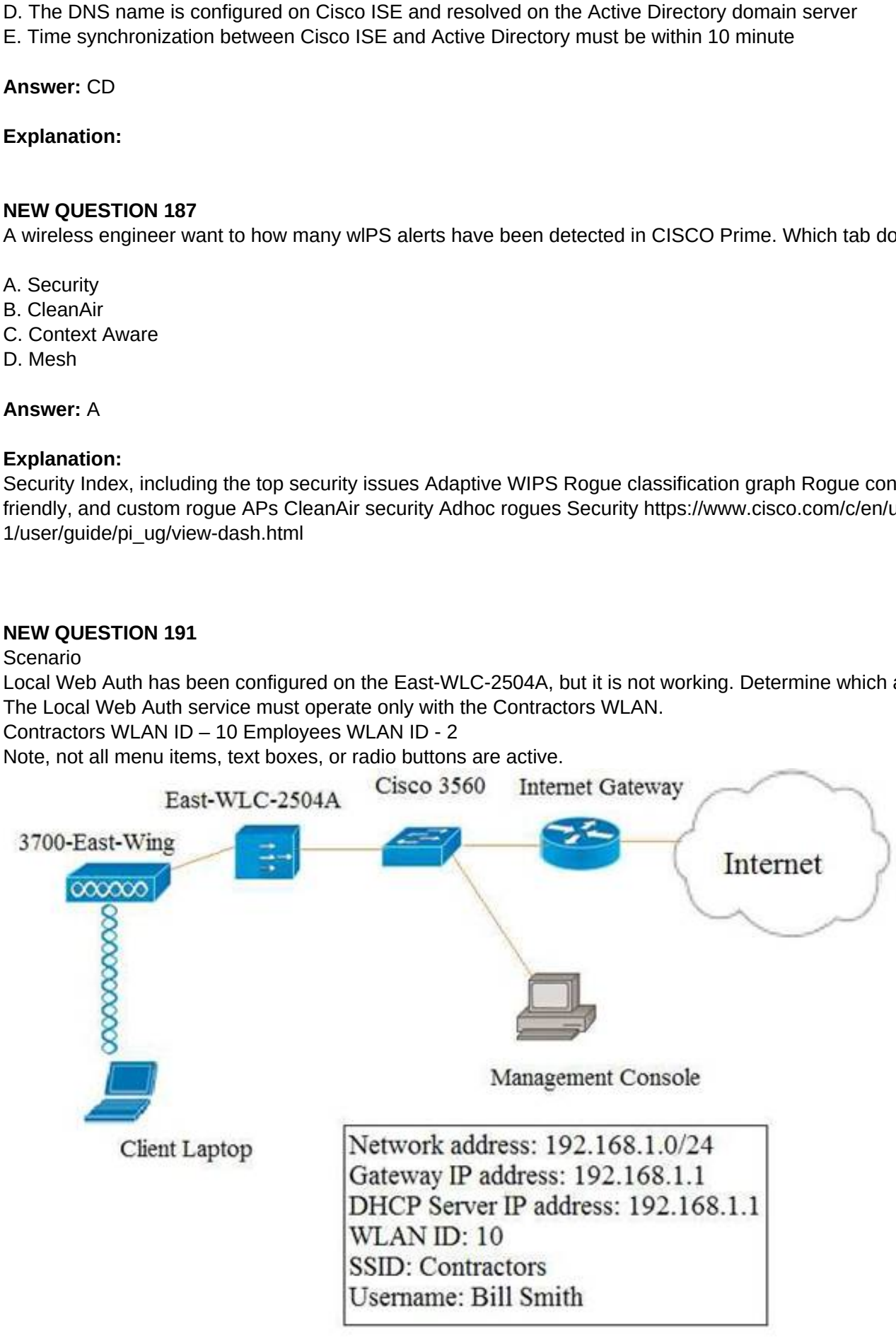
NEW QUESTION 187
A wireless engineer want to how many wlPS alerts have been detected in CISCO Prime. Which tab does the engineer select in the windows dashboard?

A. Security
B. CleanAir
C. Context Aware
D. Mesh

Answer: A

Explanation:
Security Index, including the top security issues Adaptive WIPS Rogue classification graph Rogue containment graph Attacks detected Malicious, unclassified, friendly, and custom rogue APs CleanAir security Adhoc rogues Security https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-1/user/guide/pi_ug/view-dash.html

NEW QUESTION 191
Scenario
Local Web Auth has been configured on the East-WLC-2504A, but it is not working. Determine which actions must be taken to restore the Local Web Auth service.
The Local Web Auth service must operate only with the Contractors WLAN.
Contractors WLAN ID – 10 Employees WLAN ID - 2
Note, not all menu items, text boxes, or radio buttons are active.



Virtual Terminal

Controller Summary

Management IP Address	192.168.1.99, ::/128
Software Version	0.0.110.0
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	+ 27C
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%

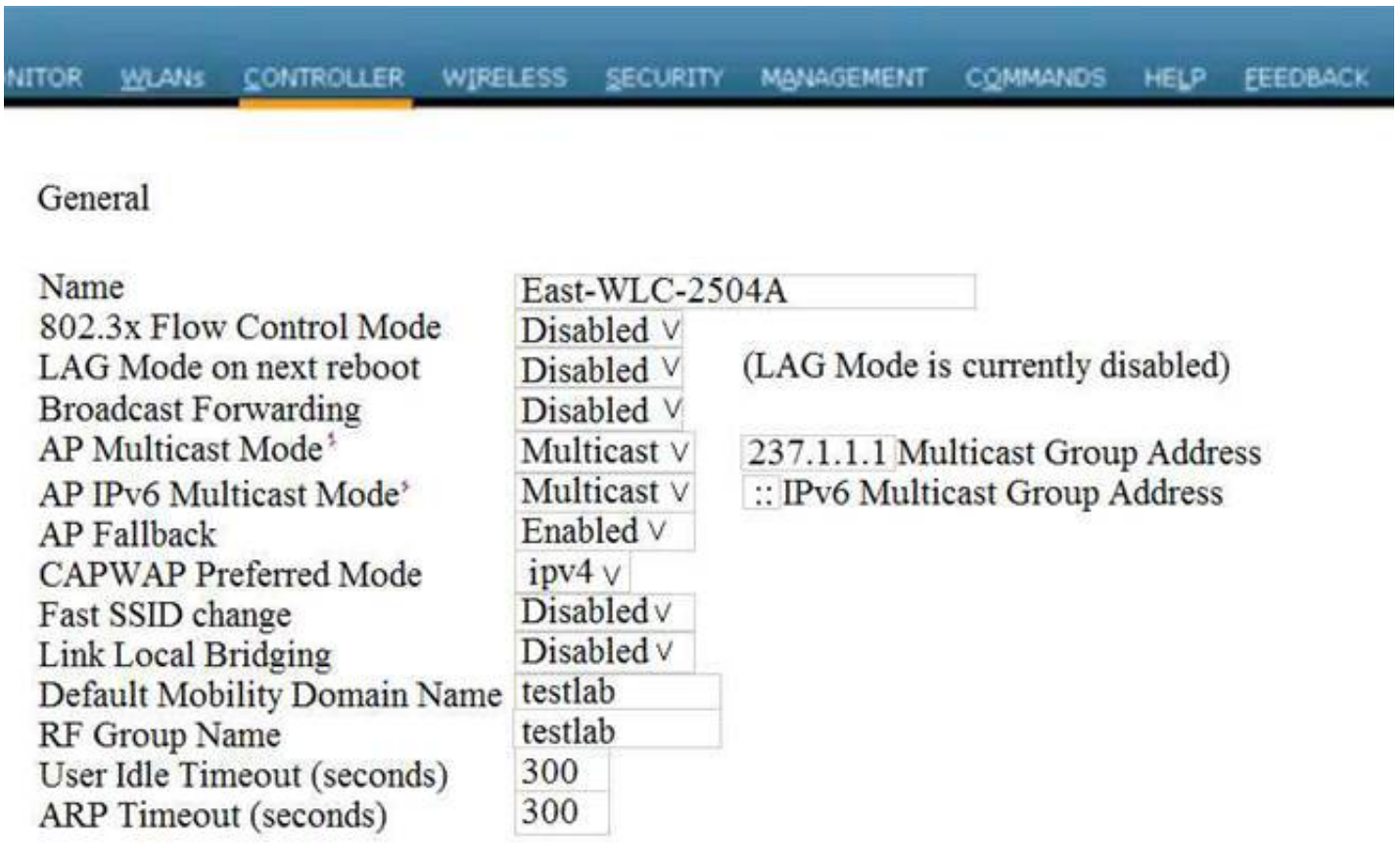
Acces Point Summary

	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

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	TestWLAN	TestWLAN	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Contractors	Contractors	Enabled	[WPA2][Auth(802.1X)]
8	WLAN	Marketing	Marketing	Enabled	[WPA2][Auth(802.1X)]
9	WLAN	Engineering	Engineering	Enabled	[WPA2][Auth(802.1X)]
10	WLAN	Employees	Employees	Enabled	[WPA2][Auth(802.1X)]



Which four changes must be made to configuration parameters to restore the Local Web Auth feature on the East-WLC-2504A? Assume the passwords are correctly entered as “ciscotest”. (Choose four.)

A. Remove the existing Local Net User Bill Smith and add a New Local Net User “Bill Smith” password “ciscotest’, WLAN Profile “Contractors”.
B. Remove WLAN 10 and WLAN 2, replace WLAN 10 with Profile Name Employees and SSID Contractors;replace WLAN 2 with Profile Name Employees and SSID Employees.
C. Remove WLAN 10 and WLAN 2, replace WLAN 10 with Profile Name Contractors and SSID Contractors, replace WLAN 2 with Profile Name Employees and SSID Employees.
D. Change the Layer 2 security to None on the Contractors WLAN.
E. Under Layer 3 Security, change the Layer 3 Security to Web Policy on the Contractors WLAN.
F. Under Security Local Net Users add a New Local Net User “Bill Smith” password “Cisco”, interface/ Interface Group “east-wing”.
G. Change the Layer 2 Security to None + EAP Pass-through on the Contractors WLAN.
H. Under WLANs > Edit “Contractors “change the interface/Interface group to “east-wing”.

Answer: CEFG

Explanation:

NEW QUESTION 196
An engineer is implementing SNMP v3 on a Cisco 5700 Series WLC. Which three commands are the minimum needed to configure SNMP v3? (Choose three.)

A. snmp-server enable traps
B. snmp-server group
C. snmp-server user

D. snmp-server community
E. snmp-server context
F. snmp-server engineID

Answer: BCF

Explanation:

NEW QUESTION 201
Which two fast roaming algorithms will allow a WLAN client to roam to a new AP and re-establish a new session key without a full reauthentication of the WLAN client? (Choose two.)

A. PKC
B. GTK
C. PMK
D. PTK
E. CKM

Answer: AE

Explanation:

NEW QUESTION 206
Which condition introduce security risk to a BYOD policy?

A. enterprise-managed MDM platform used for personal devices
B. access to LAN without implementing MDM solution
C. enforcement of BYOD access to internet only network
D. enterprise life-cycle enforcement of personal device refresh

Answer: B

Explanation:

NEW QUESTION 209
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

Explanation:

NEW QUESTION 212
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:

NEW QUESTION 217
Refer to the exhibit.

```
(Cisco Controller) >show radius summary
Authentication Servers
Idx Type Server Address Port State Tout MgmtTout RFC3576
--- ---- --------------- ------ -------- ---- -------- ---------
1 N 10.10.2.3 1812 Enabled 2 2 Enabled
2 N 10.10.2.4 1812 Enabled 2 2 Enabled

Accounting Servers
Idx Type Server Address Port State Tout MgmtTout RFC3576
--- ---- --------------- ------- ------- ---- -------- ---------
1 N 10.10.2.3 1813 Enabled 2 2 N/A
2 N 10.10.2.4 1813 Enabled 2 2 N/A
```

An engineer utilizing ISE as the wireless AAA service noticed that the accounting process on the server at 10.10.2.3 has failed, but authentication process is still functional.
Which ISE nodes receive WLC RADIUS traffic, using the CLI output and assuming the WLAN uses the servers in their indexed order?

A. authentication to 10.10.2.4, accounting to 10.10.2.3.
B. authentication to 10.10.2.3, accounting to 10.10.2.3.
C. authentication to 10.10.2.4, accounting to 10.10.2.4.
D. authentication to 10.10.2.3, accounting to 10.10.2.4.

Answer: B

Explanation:

NEW QUESTION 218
Refer to the exhibit.

```
Controller(config-wlan)#security pmf
```

You are configuring a controller that runs Cisco IOS XE by using the CLI. Which three configuration options are used for 802.11w Protected Management Frames? (Choose three.)

A. mandatory
B. association-comeback
C. SA teardown protection
D. saquery-retry-time
E. enable
F. comeback-time

Answer: ABD

NEW QUESTION 219
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 300-375 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-375-dumps.html