300-375.exam

Number: 300-375
Passing Score: 800
Time Limit: 120 min

http://www.gratisexam.com/

CISCO

300-375

Securing Wireless Enterprise Networks

Exam A

QUESTION 1
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: In 802.11, management frames such as (de)authentication, (dis)association, beacons, and probes are always unauthenticated and unencrypted. In other words, 802.11 management frames are always sent in an unsecured manner, unlike the data traffic, which are encrypted with protocols such as WPA, WPA2, or, at least, WEP, and so forth.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/82196-mfp.html#climfp

QUESTION 2
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

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Explanation: WLAN reliability and efficiency depend on the quality of the radio frequency (RF) media. Each RF is susceptible to RF noise impact. An attacker using this WLAN vulnerability can perform two types of DoS attacks:
• **Disrupt WLAN service —** At the 2.4 GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4 GHz or 5 GHz

spectrum with a high-gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a 1-kW jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same 1-kW jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.
• **Physically damage AP hardware —** An attacker using a high-output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough RF power to damage electronics in the access point putting it being permanently out of service. Such High Energy RF (HERF) guns are effective and are inexpensive to build.

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/5-2/wIPS/configuration/guide/msecg_wIPS/msecg_appA_wIPS.html

QUESTION 3
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

1. **ap name** *ap-name* **ap-group-name** *ap-group*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ap name** *ap-name* **ap-group-name** *ap-group* Example: `Switch# ap name 1240-101 ap-groupname apgroup_16`	Assigns the access point to the access point group. The keywords and arguments are as follows: • **name**—Specifies that the argument following this keyword is the name of an AP that is associated to the switch. • *ap-name*—AP that you want to associate to the AP group. • **ap-group-name**—Specifies that the argument following this keyword is the name of the AP group that is configured on the switch. • *ap-group*—Name of the access point group that is configured on the switch.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_multibook_config_guide_wireless_3850_chapter_0110.html

QUESTION 4
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 ID must be enabled.
D. The mobility group keepalive must be configured.
E. The indicated WLAN ID must be present on the controller.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
A customer has deployed PEAP authentication with a Novell eDirectory LDAP Server. Which authentication method must be configured on the client to support this deployment?

A. PEAP(EAP-MSCHAPv2)
B. PEAP(EAP-TTLS)
C. PEAP(EAP-GTC)
D. PEAP(EAP-WPA)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: PEAP-GTC is the current authentication requirement for the majority of the K-12 schools. WLC does not support MSCHAPv2 for Local EAP Authentication. As a result, you must choose GTC for the EAP Authentication type on the client.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/112137-novell-edirectory-00.html

QUESTION 6
Access points at branch sites for a company are in FlexConnect mode and perform local switching, but they authenticate to the central RADIUS at headquarters. VPN connections to the headquarters have gone down, but each branch site has a local authentication server. Which three features on the wireless controller can be configured to maintain network operations if this situation reoccurs? (Choose three.)

A. Put APs in FlexConnect Group for Remote Branches.
B. Set Branch RADIUS as Primary.
C. Put APs in AP Group Per Branch.
D. Put APs in FlexConnect Group Per Branch.

E. Set Branch RADIUS as Secondary.
F. Set HQ RADIUS as Primary.

Correct Answer: AEF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html

QUESTION 8
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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

Reference:http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/82196-mfp.html#climfp

QUESTION 9
An engineer has determined that the source of an authentication issue is the client laptop. Which three items must be verified for EAP-TLS authentication? (Choose three.)

A. The client certificate is formatted as X.509 version 3.
B. The validate server certificate option is disabled.
C. The client certificate has a valid expiration date.
D. The user account is the same in the certificate.
E. The supplicant is configured correctly.
F. The subject key identifier is configured correctly.

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_white_paper09186a008009256b.shtml

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

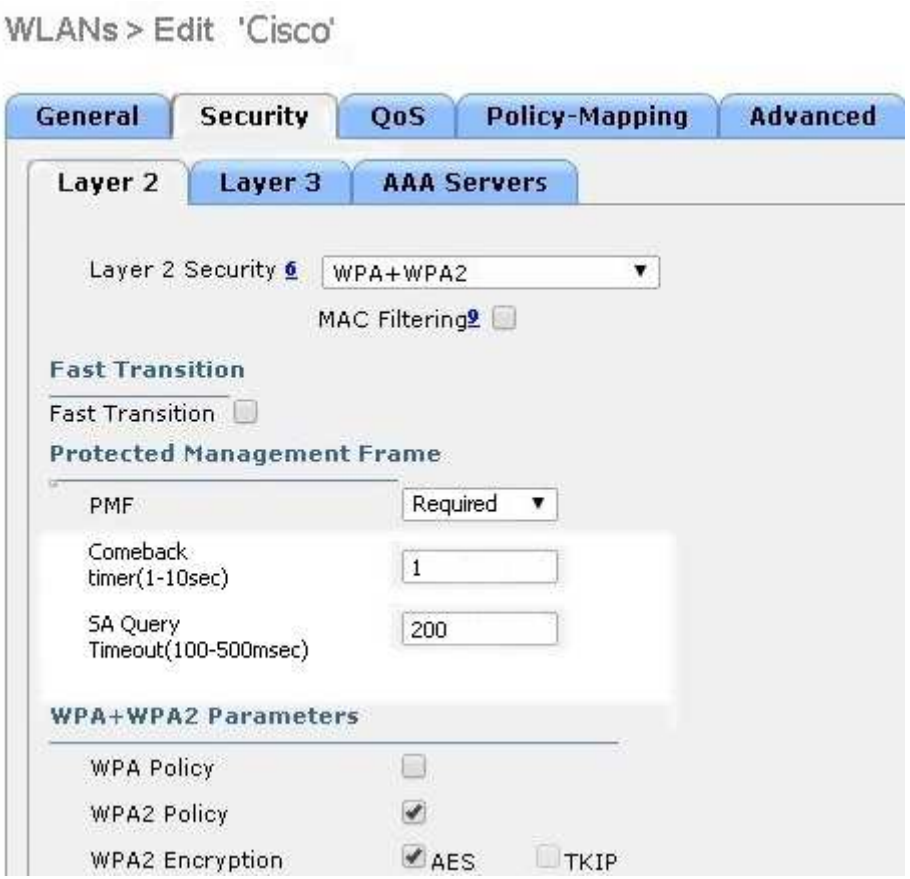
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Cisco Centralized Key Management (CCKM) is the first fast-secure roaming method developed and implemented on enterprise WLANs, created by Cisco as the solution used in order to mitigate the delays explained thus far, when 802.1X/EAP security is used on the WLAN. As this is a Cisco proprietary protocol, it is only supported by Cisco WLAN infrastructure devices and wireless clients (from multiple vendors) that are Cisco Compatible Extension (CCX)-compatible for CCKM.
CCKM can be implemented with all of the different encryption methods available for WLANs, to include: WEP, TKIP, and AES. It is also supported with most of the

802.1X/EAP authentication methods used for WLANs, dependent upon the CCX version supported by the devices.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc8

QUESTION 11
Refer to the exhibit.



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

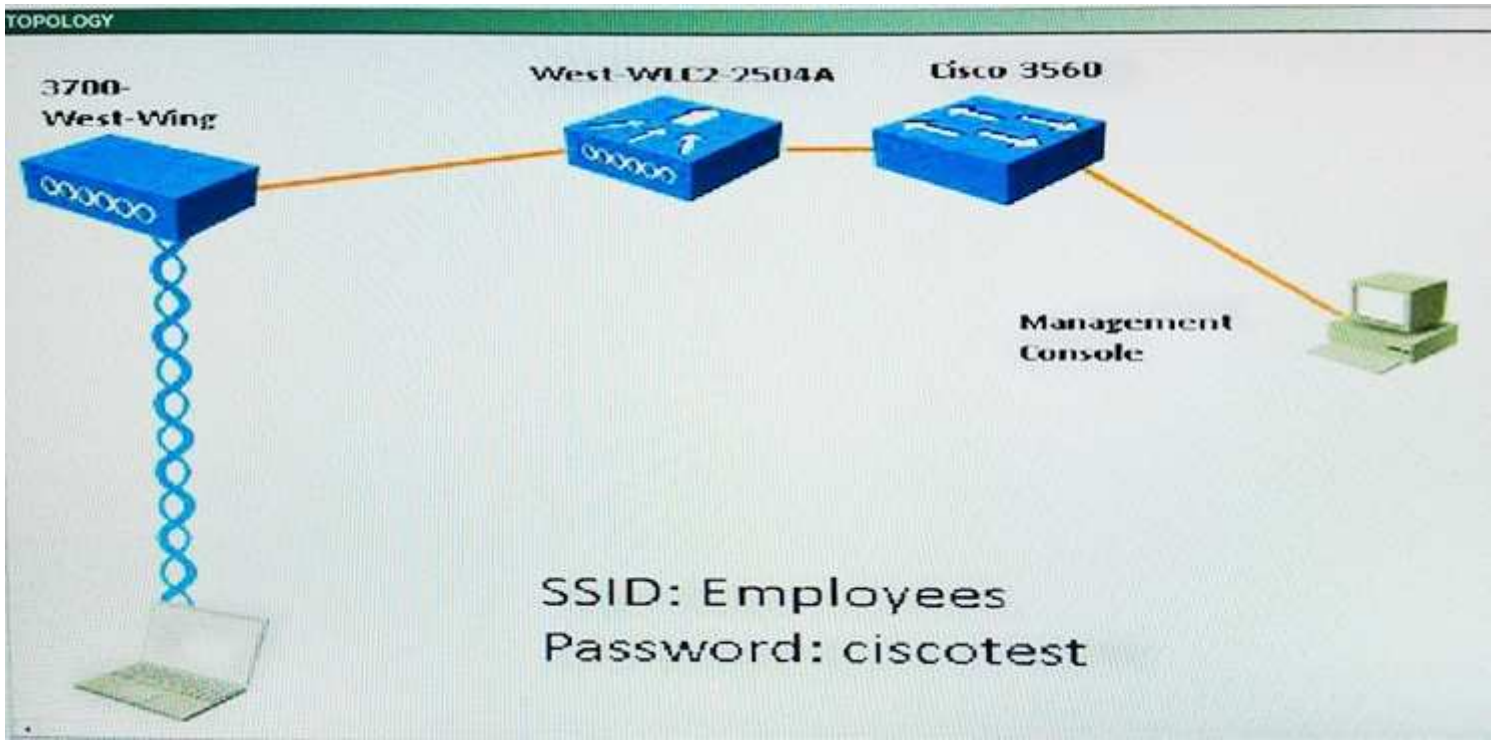
A. Both AES and TKIP must be enabled.
B. SA Query Timeout is set too low.
C. Comeback timer is set too low.
D. PMF is set to “required”.
E. MAC Filtering must be enabled.

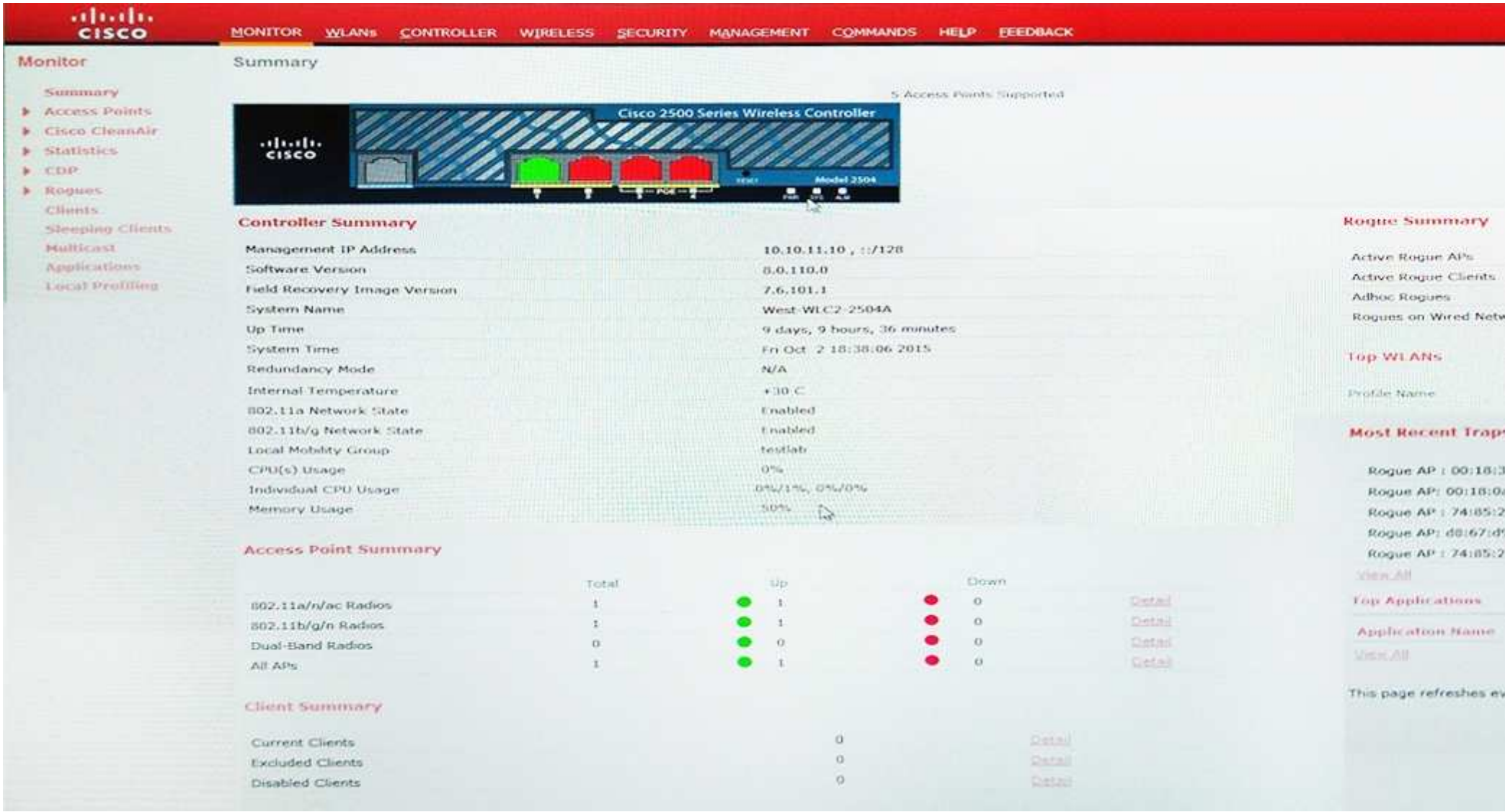
Correct Answer: E
Section: (none)
Explanation

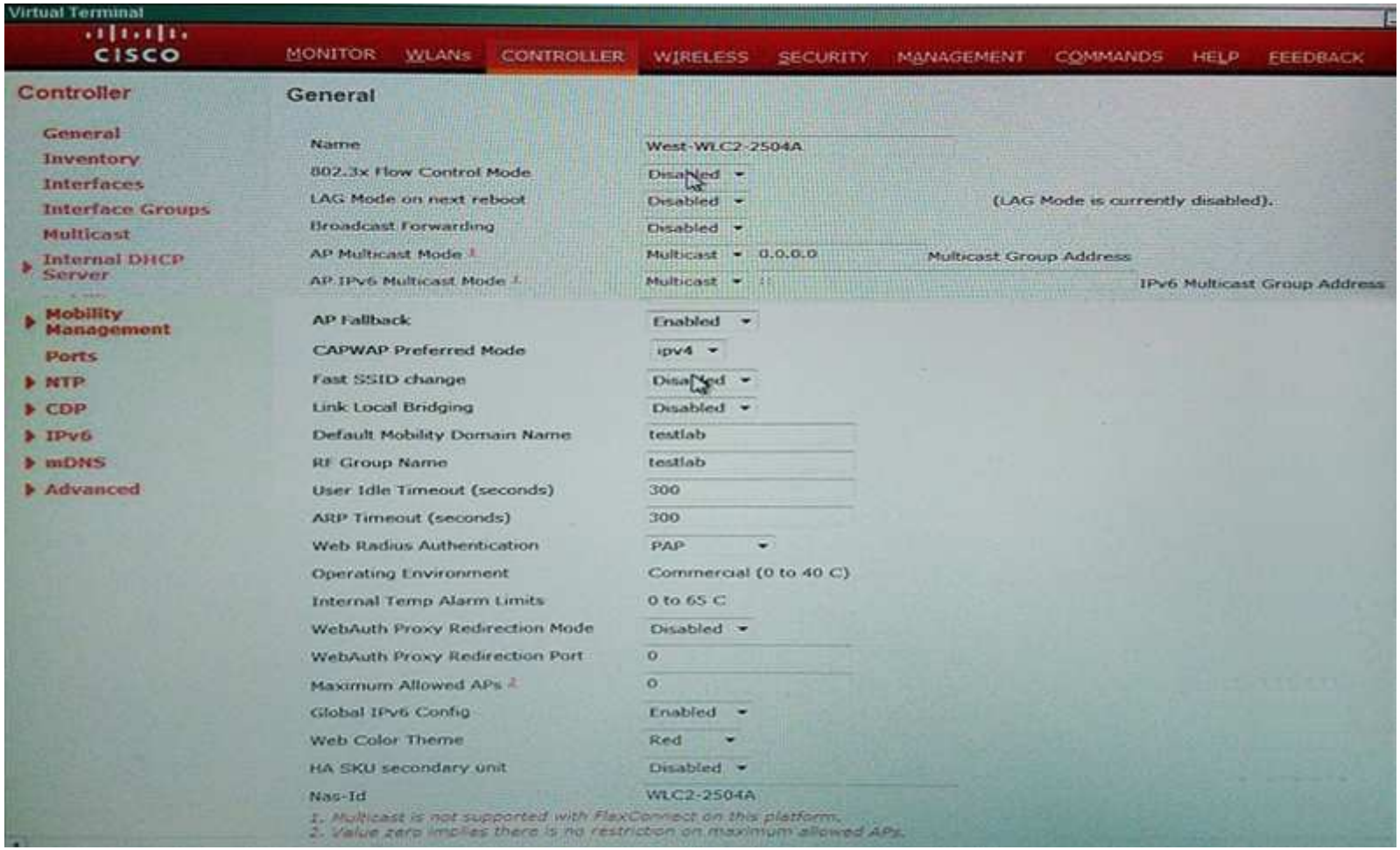
Explanation/Reference:

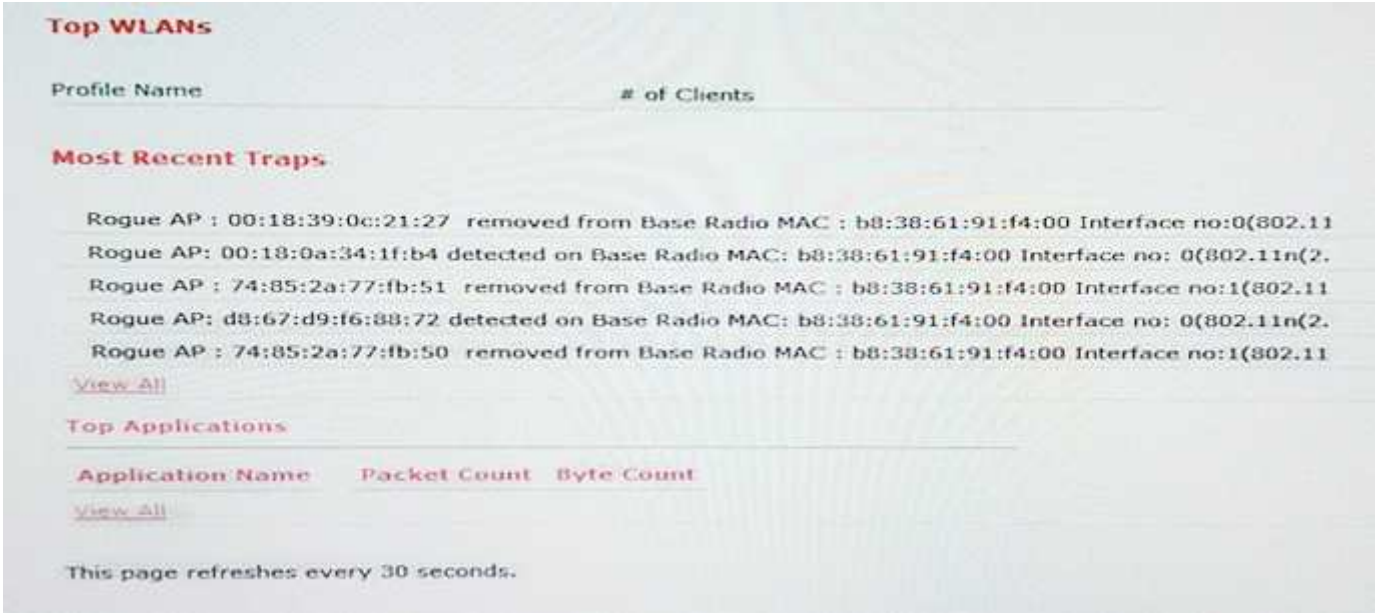
QUESTION 12
SIMULATION
Scenario
Refer to the exhibit. Configure the WLC to support WPA+WPA2 with PSK. Create a new WLAN ID 11. The SSID and Profile Name should be the same. The Controller Management interface has been preconfigured for you. The Client Laptop will automatically connect to the WLAN if your configuration is correct. Verify your configuration by using the Cisco 2504 WLC screens when you have completed the configuration.

Note, not all menu items, text boxes, or radio buttons are active.









Correct Answer: Here is the solution below
Section: (none)
Explanation

Explanation/Reference:
Please refer to this link to configure new WLC:
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116880-config-wpa2-psk-00.html

QUESTION 13
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:
Explanation: The Cisco Neighbor Discovery Packet (NDP) is the fundamental tool for RRM and other wireless applications that provides information about the neighbor radio information. You can configure the Cisco WLC to encrypt neighbor discovery packets. This feature enables you to be compliant with the PCI specifications.
Reference: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80/b_cg80_chapter_01111111.html

QUESTION 14
MFP is enabled globally on a WLAN with default settings on a 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 controller.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Client MFP shields authenticated clients from spoofed frames, which prevents the effectiveness of many of the common attacks against wireless LANs. Most attacks, such as deauthentication attacks, revert to simply degraded performance when they contend with valid clients.
Specifically, client MFP encrypts management frames sent between access points and CCXv5 clients so that both access points and clients can take preventive action and drop spoofed class 3 management frames (that is, management frames passed between an access point and a client that is authenticated and associated). Client MFP leverages the security mechanisms defined by IEEE 802.11i to protect these types of class 3 unicast management frames: disassociation, deauthentication, and QoS (WMM) action. Client MFP can protect a client-access point session from the most common type of denial-of-service attack. It protects class 3 management frames with the same encryption method used for the data frames of the session. If a frame received by the access point or client fails decryption, it is dropped, and the event is reported to the controller.
In order to use client MFP, clients must support CCXv5 MFP and must negotiate WPA2 with either TKIP or AES-CCMP. EAP or PSK can be used to obtain the PMK. CCKM and controller mobility management are used to distribute session keys between access points or Layer 2 and Layer 3 fast roaming.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/82196-mfp.html

QUESTION 15
An engineer must enable EAP on a new WLAN and is ensuing 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

Correct Answer: D
Section: (none)
Explanation

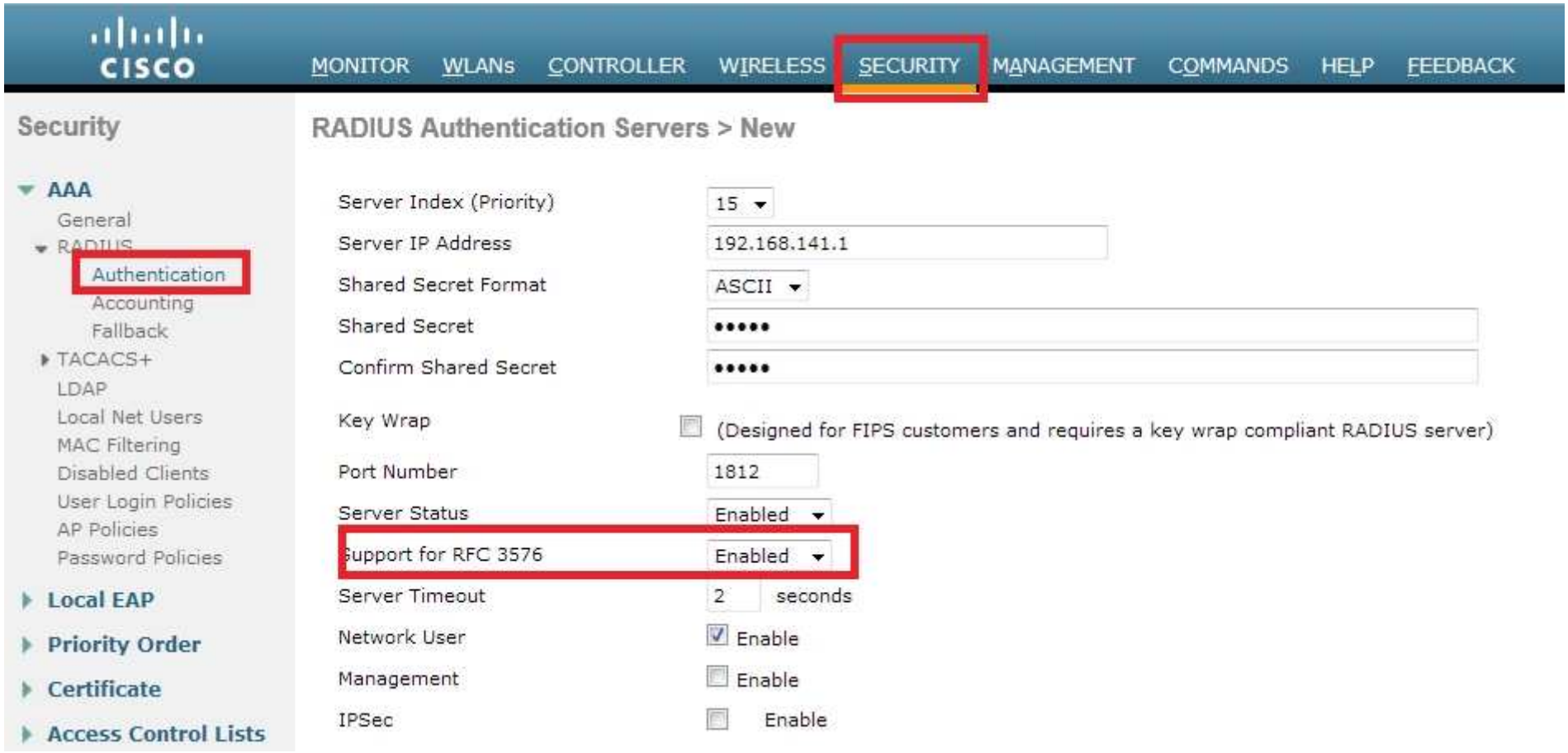
Explanation/Reference:

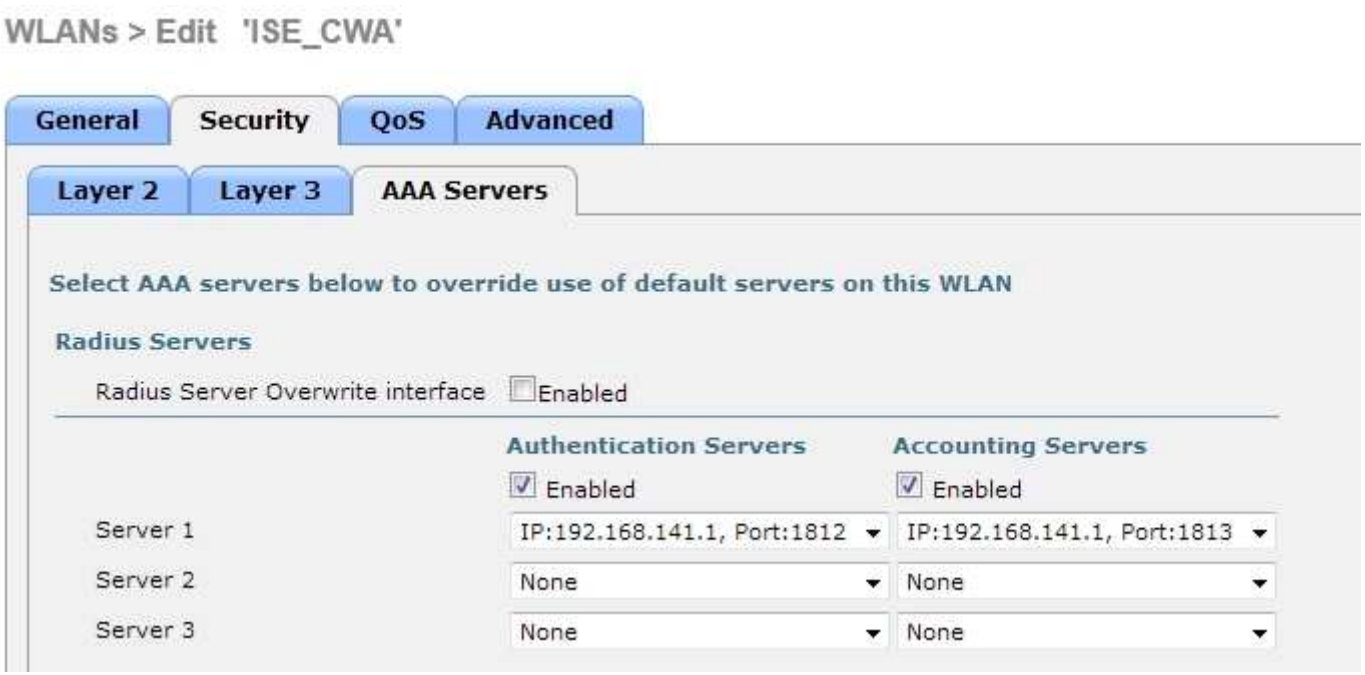
QUESTION 16
Which three configuration steps are necessary on the WLC when implementing central web authentication in conjunction with Cisco ISE. (Choose three.)

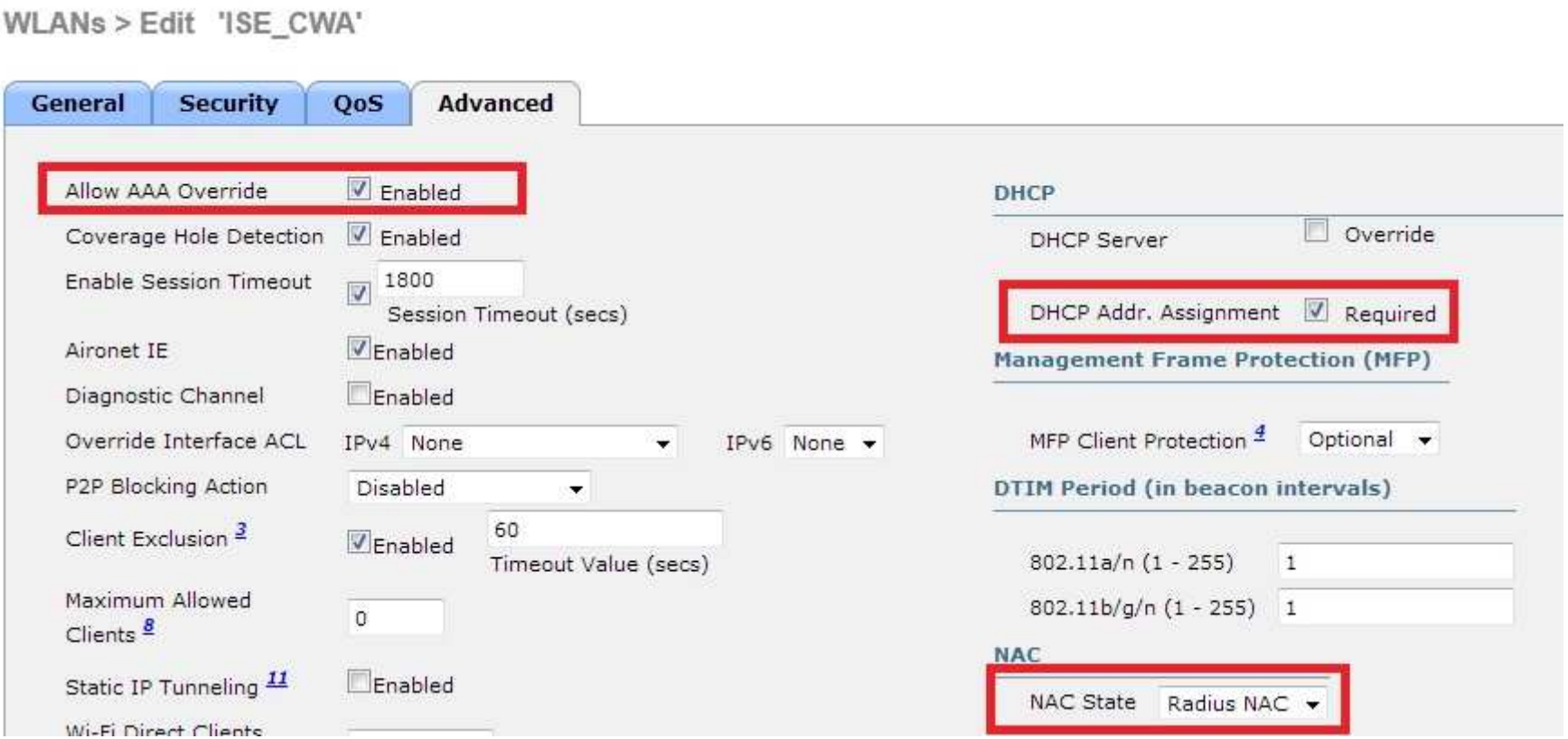
A. Set P2P Blocking Action to Drop.
B. Enable Security Layer 3 Web Policy.
C. Set NAC state to SNMP NAC.
D. Enable Allow AAA override.
E. Enable Security Layer 2 Mac Filtering.
F. Set NAC state to RADIUS NAC.

Correct Answer: DEF
Section: (none)
Explanation

Explanation/Reference:
Explanation:

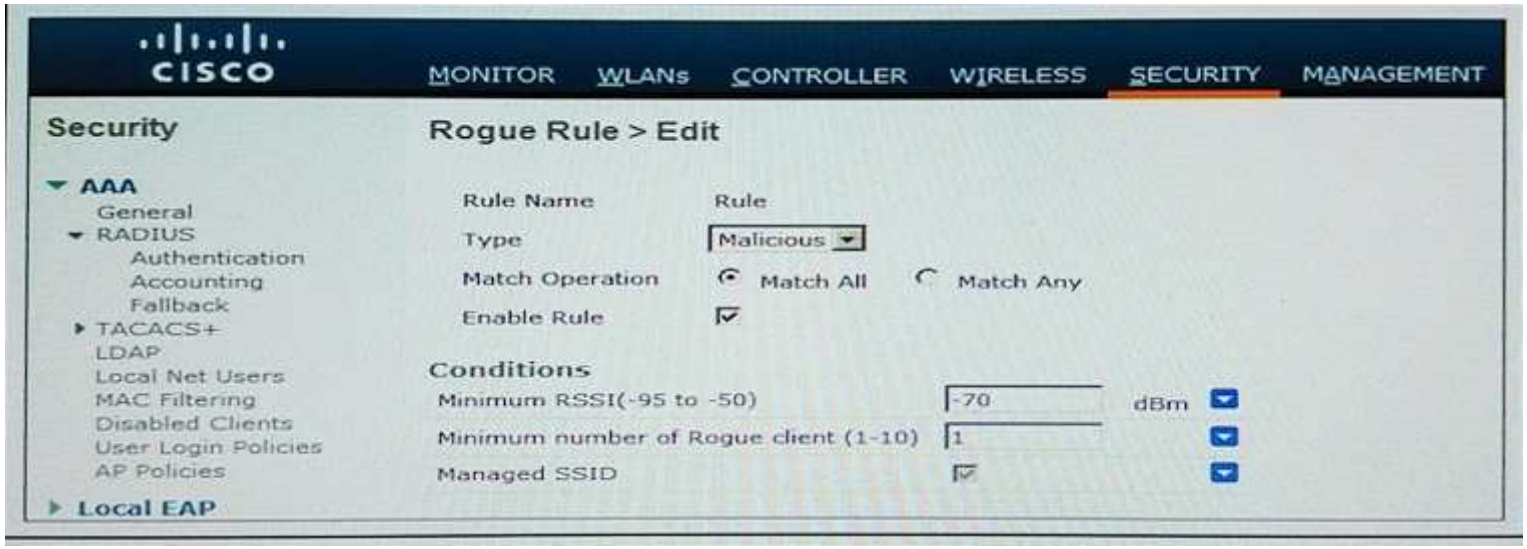






Reference: https://supportforums.cisco.com/document/110031/central-web-authentication-cwa-guests-ise

QUESTION 17
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: **RSSI** — Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the **Minimum RSSI** text box. The valid range is –95 to –50 dBm (inclusive), and the default value is 0 dBm.

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_0111110.html#ID4397

QUESTION 18
Which option describes the purpose of configuring switch peer groups?

A. enforces RF profiles
B. enables location services
C. restricts roaming traffic to certain switches
D. allows template based configuration changes

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference https://supportforums.cisco.com/blog/11939206/converged-access-mobilitynew-mobility-architecture-wlc-5500-and-ngwc-5760-and-3850

QUESTION 19
Which of the following user roles can access CMX Visitor Connect?

A. Administrator
B. Power User
C. Guest User
D. Super Administrator

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
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

Correct Answer: BE

Section: (none)
Explanation

Explanation/Reference:
Explanation: RADIUS messages are sent as User Datagram Protocol (UDP) messages. UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages. Some network access servers might use UDP port 1645 for RADIUS authentication messages and UDP port 1646 for RADIUS accounting messages. By default, IAS supports receiving RADIUS messages destined to both sets of UDP ports.

Reference: https://technet.microsoft.com/en-in/library/cc781821(v=ws.10).aspx

QUESTION 21
Which command is an SNMPv3-specific command that an engineer can use only in Cisco IOS XE?

A. snmp-server user remoteuser1 group1 remote 10.12.8.4
B. snmp-server host 172.16.1.33 public
C. snmp-server community comaccess ro 4
D. snmp-server enable traps wireless

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
SUMMARY STEPS
1. **enable**
2. **configure terminal**
3. **snmp-server group** [*group-name* {**v1** | **v2c** | **v3** [**auth** | **noauth** | **priv**]}] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** *access-list*]
4. **snmp-server engineID** {**local** *engine-id* | **remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engine-id-string*}
5. **snmp-server user** *user-name group-name* [**remote** *ip-address* [**udp-port** *port*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth**{**md5** | **sha**} *auth-password*]} [**access** *access-list*]
6. **end**

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html#GUID-54F1E297-CE1D-45FE-9751-B8D129606010

QUESTION 22
An engineer must provide a graphical trending report of the total number of wireless clients on the network. Which report provides the required data?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation: Mobility Client Summary - This trending report displays the total number of active clients in your wireless network.

Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/reps.html#pgfId-1059688

QUESTION 23
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: When WPA-PSK or WPA2-PSK is performed via Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) for the encryption, the client must go through the process known as the WPA 4-Way handshake for both the initial association and also when roaming. As previously explained, this is basically the key management process used in order for WPA/WPA2 to derive the encryption keys. However, when PSK is performed, it is also used in order to verify that the client has a valid Pre-Shared Key to join the WLAN.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116493-technote-technology-00.html#anc6

QUESTION 24
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation: Prime Infrastructure gets updates about rogues from controllers by using traps or by polling. The Last Seen Time is updated any time a trap for the rogue is received or rogue is seen during the last Prime Infrastructure polling cycles.
This report displays all rogues detected by the access points in your network based on the Last Seen Time of the rogue access points and the selected filtering criteria. The report lists rogue access points based on the time they were last seen.
Note The report includes rogue access point alarms with clear severity.

Reference: http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/user/guide/prime_infra_ug/reps.html

QUESTION 25
A customer is concerned that radar is impacting the access points that service the wireless network in an office located near an airport. On which type of channel should you conduct spectrum analysis to identify if radar is impacting the wireless network?

A. UNII-3 channels
B. UNII-1 channels
C. 802.11b channels
D. 2.4 GHz channels
E. UNII-2 channels
F. channels 1, 5, 9, 13

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
An engineer configures the wireless LAN controller to perform 802.1x user authentication. Which option must be enabled to ensure that client devices can connect to the wireless, even when WLC cannot communicate with the RADIUS?

A. local EAP
B. authentication caching
C. pre-authentication
D. Cisco Centralized Key Management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation: Local EAP is an authentication method that allows users and wireless clients to be authenticated locally on the controller. It is designed for use in remote offices that want to maintain connectivity to wireless clients when the backend system becomes disrupted or the external authentication server goes down. When you enable local EAP, the controller serves as the authentication server and the local user database, so it removes dependence on an external authentication server.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100590-ldap-eapfast-config.html

QUESTION 27
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. 10000
B. 1000
C. 500
D. 2000
E. 5000

Correct Answer: E
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
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

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which three options are valid client profile probes in Cisco ISE? (Choose three.)

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

Correct Answer: ADF
Section: (none)
Explanation

Explanation/Reference:
Explanation: Valid client probes in ISE are:

- NetFlow Probe
- DHCP Probe
- DHCP SPAN Probe
- HTTP Probe
- RADIUS Probe
- DNS Probe

Reference: http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_prof_pol.html

QUESTION 30
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.gigawave.com/2016/05/10/techtip-802-11w-protected-management-frames/