

## 300-375.exam

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



<http://www.gratisexam.com/>

CISCO

**300-375**

**Securing Wireless Enterprise Networks**

<http://www.gratisexam.com/>

## 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](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	<p><code>ap name ap-name ap-group-name ap-group</code></p> <p>Example:</p> <p>Switch# <code>ap name 1240-101 ap-groupname apgroup_16</code></p>	<p>Assigns the access point to the access point group. The keywords and arguments are as follows:</p> <ul style="list-style-type: none"><li>• <b>name</b>—Specifies that the argument following this keyword is the name of an AP that is associated to the switch.</li><li>• <b>ap-name</b>—AP that you want to associate to the AP group.</li><li>• <b>ap-group-name</b>—Specifies that the argument following this keyword is the name of the AP group that is configured on the switch.</li><li>• <b>ap-group</b>—Name of the access point group that is configured on the switch.</li></ul>

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](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.)



<http://www.gratisexam.com/>

- 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](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.

WLANs > Edit 'Cisco'

The screenshot shows the 'Security' tab of the 'WLANs > Edit 'Cisco'' configuration page. The 'Layer 2' sub-tab is selected. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2'. The 'MAC Filtering' checkbox is unchecked. The 'Fast Transition' checkbox is unchecked. The 'Protected Management Frame' section is expanded, showing 'PMF' set to 'Required', 'Comeback timer(1-10sec)' set to '1', and 'SA Query Timeout(100-500msec)' set to '200'. The 'WPA+WPA2 Parameters' section is also expanded, showing 'WPA Policy' unchecked, 'WPA2 Policy' checked, and 'WPA2 Encryption' checked with 'AES' selected and 'TKIP' unchecked.

Section	Parameter	Value
Layer 2 Security	Layer 2 Security	WPA+WPA2
	MAC Filtering	<input type="checkbox"/>
Fast Transition	Fast Transition	<input type="checkbox"/>
	Protected Management Frame	
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





<http://www.gratisexam.com/>

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**

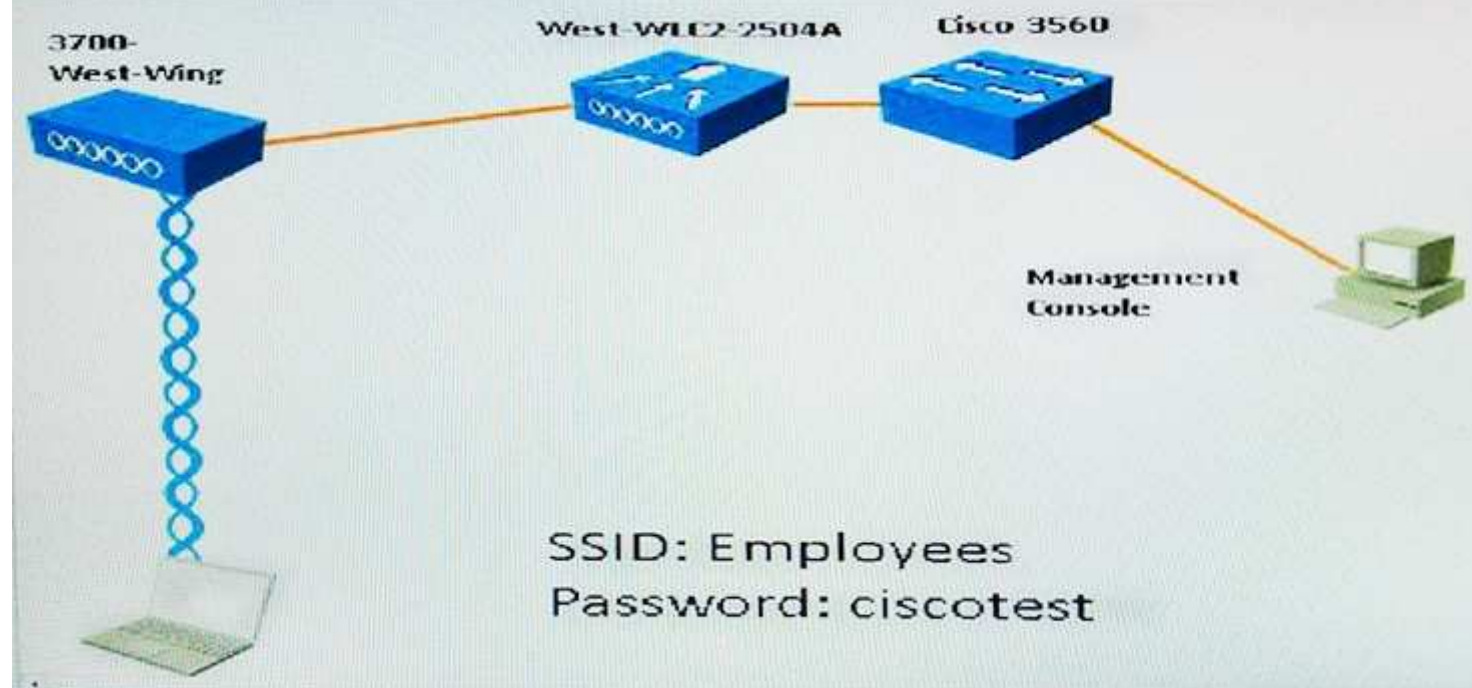
### **SIMULATION**

#### **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.

TOPOLOGY





Monitor

Summary

- Summary
- Access Points
- Cisco CleanAir
- Statistics
- CDP
- Rogues
- Clients
- Sleeping Clients
- Multicast
- Applications
- Local Profiling



5 Access Points Supported

Controller Summary

Management IP Address	10.10.11.10, ::1/128
Software Version	5.0.110.0
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	<a href="#">Detail</a>
802.11b/g/n Radios	1	1	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	1	1	0	<a href="#">Detail</a>

Client Summary

Current Clients	0	<a href="#">Detail</a>
Excluded Clients	0	<a href="#">Detail</a>
Disabled Clients	0	<a href="#">Detail</a>

Rogue Summary

Active Rogue APs  
Active Rogue Clients  
Adhoc Rogues  
Rogues on Wired Netw

Top WLANs

Profile Name

Most Recent Traps

Rogue AP : 00:18:3  
Rogue AP: 00:18:0  
Rogue AP : 74:85:2  
Rogue AP: d8:67:d9  
Rogue AP : 74:85:2

[View All](#)

Top Applications

Application Name

[View All](#)

This page refreshes ev



Virtual Terminal

**CISCO**

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

**Controller**

**General**

**General**  
Inventory  
Interfaces  
Interface Groups  
Multicast  
Internal DHCP Server  
Mobility Management  
Ports  
NTP  
CDP  
IPv6  
mDNS  
Advanced

**General**

Name: West-WLC2-2504A

802.3x Flow Control Mode: Disabled

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

Broadcast Forwarding: Disabled

AP Multicast Mode: Multicast 0.0.0.0 Multicast Group Address

AP IPv6 Multicast Mode: Multicast :: IPv6 Multicast Group Address

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: PAP

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: Red

HA SKU secondary unit: Disabled

Nas-Id: WLC2-2504A

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



Top WLANs

Profile Name

# of Clients

Most Recent Traps

Rogue AP : 00:18:39:0c:21:27 removed from Base Radio MAC : b8:38:61:91:f4:00 Interface no:0(802.11

Rogue AP: 00:18:0a:34:1f:b4 detected on Base Radio MAC: b8:38:61:91:f4:00 Interface no: 0(802.11n(2.

Rogue AP : 74:85:2a:77:fb:51 removed from Base Radio MAC : b8:38:61:91:f4:00 Interface no:1(802.11

Rogue AP: d8:67:d9:f6:88:72 detected on Base Radio MAC: b8:38:61:91:f4:00 Interface no: 0(802.11n(2.

Rogue AP : 74:85:2a:77:fb:50 removed from Base Radio MAC : b8:38:61:91:f4:00 Interface no:1(802.11

View All

Top Applications

Application Name

Packet Count

Byte Count

View All

This page refreshes every 30 seconds.

**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](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 ensuring that the necessary components are available. Which component uses EAP and 802.1x to pass user authentication to the authenticator?



<http://www.gratisexam.com/>

- 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:

<http://www.gratisexam.com/>





## Security

### AAA

General

#### RADIUS

**Authentication**

Accounting

Fallback

#### TACACS+

LDAP

Local Net Users

MAC Filtering

Disabled Clients

User Login Policies

AP Policies

Password Policies

### Local EAP

### Priority Order

### Certificate

### Access Control Lists

## RADIUS Authentication Servers > New

Server Index (Priority)	15 ▼
Server IP Address	192.168.141.1
Shared Secret Format	ASCII ▼
Shared Secret	•••••
Confirm Shared Secret	•••••
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled ▼
Support for RFC 3576	Enabled ▼
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

## WLANs > New

Type	WLAN ▼
Profile Name	ISE_CWA
SSID	ISE_CWA
ID	2 ▼

## WLANs > Edit 'ISE\_CWA'

**General** **Security** QoS Advanced

Layer 2 **Layer 3** AAA Servers

Layer 2 Security <sup>6</sup> None ▼

MAC Filtering <sup>9</sup> ☒

**Fast Transition**

Fast Transition ☐

## WLANs > Edit 'ISE\_CWA'

**General** **Security** QoS Advanced

Layer 2 Layer 3 **AAA Servers**

Layer 3 Security None ▼

☐ Web Policy <sup>1</sup>

## WLANs > Edit 'ISE\_CWA'

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

**Radius Servers**

Radius Server Overwrite interface ☐ Enabled

	<b>Authentication Servers</b>	<b>Accounting Servers</b>
	<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1	IP:192.168.141.1, Port:1812 ▼	IP:192.168.141.1, Port:1813 ▼
Server 2	None ▼	None ▼
Server 3	None ▼	None ▼

## WLANs > Edit 'ISE\_CWA'

General	Security	QoS	Advanced
<b>General</b>			
Allow AAA Override <input checked="" type="checkbox"/> Enabled			
Coverage Hole Detection <input checked="" type="checkbox"/> Enabled			
Enable Session Timeout <input checked="" type="checkbox"/> 1800 Session Timeout (secs)			
Aironet IE <input checked="" type="checkbox"/> Enabled			
Diagnostic Channel <input type="checkbox"/> Enabled			
Override Interface ACL IPv4 None IPv6 None			
P2P Blocking Action Disabled			
Client Exclusion <sup>3</sup> <input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)			
Maximum Allowed Clients <sup>8</sup> 0			
Static IP Tunneling <sup>11</sup> <input type="checkbox"/> Enabled			
Wi-Fi Direct Clients			
<b>DHCP</b>			
DHCP Server <input type="checkbox"/> Override			
DHCP Addr. Assignment <input checked="" type="checkbox"/> Required			
<b>Management Frame Protection (MFP)</b>			
MFP Client Protection <sup>4</sup> Optional			
<b>DTIM Period (in beacon intervals)</b>			
802.11a/n (1 - 255) 1			
802.11b/g/n (1 - 255) 1			
<b>NAC</b>			
NAC State Radius NAC			

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

### QUESTION 17

Refer to the exhibit.

**CISCO**

MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT

**Security**

**Rogue Rule > Edit**

▼ **AAA**

- General
- ▼ **RADIUS**
  - Authentication
  - Accounting
  - Fallback
- ▶ **TACACS+**
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
- ▶ **Local EAP**

Rule Name: \_\_\_\_\_ Rule: **Malicious**

Type: \_\_\_\_\_

Match Operation: ☒ Match All ☐ Match Any

Enable Rule: ☒

**Conditions**

Minimum RSSI (-95 to -50):  dBm ☒

Minimum number of Rogue client (1-10):  ☒

Managed SSID: ☒

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 rogue 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](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](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?



<http://www.gratisexam.com/>

- 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**

<http://www.gratisexam.com/>

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



<http://www.gratisexam.com/>

**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](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/>



<http://www.gratisexam.com/>