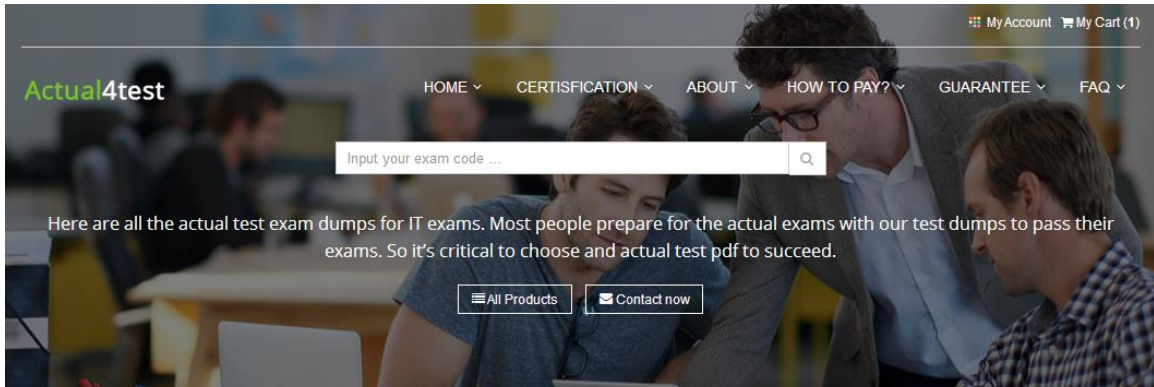


# Actual4Test



## QUALITY AND VALUE

Actual4test Practice Exams are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development - no all dumps.



## TESTED AND APPROVED

We are committed to the process of vendor and third party approvals. We believe professionals and executives alike deserve the confidence of quality coverage these authorizations provide.



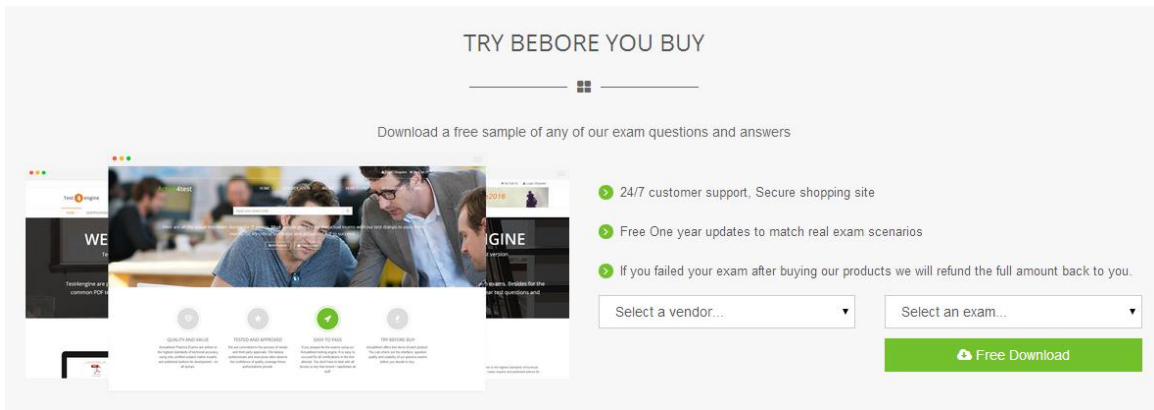
## EASY TO PASS

If you prepare for the exams using our Actual4test testing engine, it is easy to succeed for all certifications in the first attempt. You don't have to deal with all dumps or any free torrent / rapidshare all stuff.



## TRY BEFORE BUY

Actual4test offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.



<http://www.actual4test.com>

Actual4test - actual test exam dumps-pass for IT exams

**Exam** : **400-351**

**Title** : **CCIE Wireless**

**Vendor** : **Cisco**

**Version** : **DEMO**

**NO.1** Which two statement about a Cisco WLC (5500/7500/8500 Series/WiSM-2) High Availability setup running code 8.0 are true? (Choose two)

- A. Certificates are downloaded only to the primary WLC, which then pushes them to the secondary instance
- B. You can have one active WLC and multiple standby-hot
- C. It is possible to achieve HA between two Cisco Wireless Services Module 2 (WiSM2) platforms only if the controllers have been deployed on a single chassis
- D. Enabling HA requires only a reboot of the primary controller
- E. Before you enable HA, ensure that both controllers are physically connected through the redundant port using an Ethernet cable
- F. The IP addresses of the redundancy management interface and the management interface must be in the same subnet for the primary and secondary Cisco WLCs

**Answer:** E,F

**NO.2** Refer to the exhibit. At which rate are the multicast frames transmitted by an autonomous AP configured with these data rates, considering the client on the AP is a 802.11b client?

- A. 36.0 mbps
- B. 11.0 mbps
- C. 12.0 mbps
- D. 5.5 mbps
- E. 2 mbps

**Answer:** B

**NO.3** Which two configurations are required on the Cisco 5760 WLC to ensure that APs will successfully join the Cisco WLC? (Choose two)

- A. Ensure accurate configuration of the correct time and date on the wireless LAN controller.
- B. Enable ip dhcp snooping trust on the wireless controller port-channel interface.
- C. Ensure that Port-Fast is enabled on each access point switch port.
- D. Activate the appropriate Right-to-Use AP license on the wireless LAN controller.

**Answer:** A,D

**NO.4** Which three statements about 802.11ac are true? (choose three)

- A. MU-MIMO is supported in wave 1
- B. MU-MIMO allows one AP to transmit unique data to multiple stations simultaneously
- C. when using MU-MIMO up to 8 devices can transmit data at the same time
- D. 802.11 a/b/g/n device are able to connect to 802.11ac radios
- E. it IS possible to reach 160 MHz by combining two discontinuous 80 MHz channel block
- F. 802.11 ac is supported in the 2.4- and 5-Ghz radio band

**Answer:** B,D,E

**NO.5** Which two statement are true about adding identity services engines 1.3 to prime infrastructure 2.2?(choose two)

- A. You need to use super user credential on ISE for PI integration to work.
- B. A maximum of three ISEs can be added to PI.
- C. )If you add two ISEs one should be primary and the other should be standby.
- D. configuration templates within PI can be used to set up ISE.

**Answer:** A,C

Explanation: Section: 7.0 Prime Infrastructure and MSE

**NO.6** You are the network administrator for ACME corporation. Your organization has deployed a single Cisco 5500 Series Wireless Controller with 100 Cisco Aironet 3500 Series Aps. A new IT member is worried that most of these Aps are working at a power level 3 on the 5GHz radio specially. As this power level setting is causing issues in your wireless network.

Which option describes the likely cause of this behavior?

- A.** The WLC has been recently rebooted, which causes the TPC algorithm to set power level 3 on all APs for 90 seconds.
- B.** The controller TPC algorithm seems to have a problem. It might have been set to work in TPCv2 mode instead of TPCv1.
- C.** The WLC is misconfigured because the static power of level 3 has been set for all the APs under TPC settings.
- D.** Cisco 7925 wireless IP Phones are in use and the DTPC feature is enabled on the 5 GHz radio.

**Answer:** D

Explanation:

Tx Power

Num Of Supported Power Levels ..... 5

Tx Power Level 1 ..... 18 dBm

Tx Power Level 2 ..... 15 dBm

Tx Power Level 3..... 12 dBm

Tx Power Level 4 ..... 9 dBm

Tx Power Level 5 ..... 6 dBm

<https://supportforums.cisco.com/discussion/11635606/power-level-wlc>

**NO.7** Which description is correct with regard to the operation of an access point in Rogue Location discovery Protocol Mode?

- A.** The AP uses the existing wireless infrastructure in order to scan for rogue AP's. Once discovered, these rogues are added to a local list that includes the rogue's BSSIDs, MAC addresses and any discovered security provisions (WPA, WEP etc)
- B.** The AP moves to the rogue channel and attempts to connect to the rogue as a client. The AP then tries to obtain an IP address and forwards a UDP packet to the controller through the rogue. If the controller receives this packet, the network administrator is notified that a rogue AP has been discovered on the wired network
- C.** The AP detects a rogue client and then the network administrator is able to contain both the rogue AP and the rogue clients. This can be achieved because 802.11 deauthentication packets are sent to clients that are associated to rogue APs so threats such as holes are mitigated
- D.** The AP determines whether or not a rogue access point is on a trusted network. It does not provide RF service of any kind but rather receives periodic rogue access point reports from the controller and sniffs all ARP packets. If it finds a match between an ARP request and a MAC address it receives from the controller. It generates a rogue access point alert to the controller

**Answer:** B

**NO.8** Which two statements about accessing the GUI and CLI of Cisco WLC are true?

- A.** Use the config domain add -N command on the Cisco WLC.
- B.** The wireless client can access the Cisco WLC only when the option "Enable controller wireless Management to be accessible from wireless client is checked"

C. The feature management using dynamic interface can be applied to one of the dynamic interfaces only.

D. Add the country code for Panama (PA) through the Cisco WLC web GUI.

**Answer:** B,C

**NO.9** Your customer needs the list of all the guest client that connected to Wi-Fi successfully but have not yet authenticated. The customer decides to create an advanced filter in Cisco Pounder monitor >client and user which two conditions should be included in the filter? (Choose two)

A. PEM state =WebauthReqD

B. On Network= Yes

C. Status =Associated

D. Type =Lightweight client

**Answer:** C,D

**NO.10** You are designing a wireless network for a museum. One of their requirements is to track people inside the museum and push a notification into their tablet device as soon as they step in front of a painting with information about the artist and the painting. This information must be delivered in real time. You are using regular probe request-based tracking and during testing. You notice that although the tablet is connected to the museum Wi-Fi network, the location is not updating in real time as you move. It can take almost 2 minutes for the location to be updated. Which option is the likely reason for this issue?

A. Cisco MSE does not perform a new location calculation for certain elements if the resulting position is not at least 5 meters different than the previous location.

B. Probe request-based tracking is bound to delay due to the broadcast type of traffic that is not acknowledged over the air and could be lost.

C. CCXv4 S60 is disabled by default. You must enable CCXv4 S60, which is compatible with all Wi-Fi clients. This feature comes out location updates more frequently.

D. Probe request-based tracking is device dependent. The tablet might not send a probe request if it is maintaining a good Wi-Fi signal, which can cause slower location updates.

**Answer:** C

Explanation:

From.



## Q. What are the challenges for RSSI based location systems?

A. The common challenges are:

- **Wrong channel problem (WCP)**—When the AP is on a particular channel it is possibly able to receive packets transmitted from adjacent channels albeit at a lower received power. Thus the AP then reports the packet with lower RSSI value, which would cause the location of the client to be estimated further than actual in the location server. This is observed in 2.4 GHz band due to AP filter limitations and 802.11b modulation techniques, even for 802.11g/n clients, as they use 802.11b for probe requests. S60 client driver can eliminate such problems.
- **Antenna diversity issues (ADI)**—It was also observed that the same packet was received on the 2 AP antennas at considerably different power. This can be due to challenges of gathering reliable RSSIs with antenna diversity. The AP must listen on one antenna during start of packet then switch to a different antenna during packet reception in order to get better reception, all within a few micro seconds.
- **Client concerns and environmental issues**—Client transmission, which are frequency and transmit power levels, are dictated by client drivers. These can be augmented by the use of CCXv4, but tests today cannot take advantage of this CCX standard. The high ceiling and metal racks presents a challenging RF environment. See the **How RF propagation helps (and hinders) Location** question for more information on RF environment challenges.
- **Missing RSSIs**—Due to client/driver behavior, AP traffic and RF environment issues, not all APs, get RSSI readings. In a typical high ceiling environment, APs can hear neighboring APs stronger than the clients on the floor. This along with the metal racks can worsen the hidden node problems, wherein the clients on the floor try to communicate with the closest AP which can see packets from neighboring APs on the same channel. The client is unaware of these packets due to the poor RSSI from the neighbor AP at its end. During some readings, not all APs receive RSSI measurements. Thus the location calculation is carried out with an incomplete set of APs, and results in poor location accuracy. S36 and S60 force the client to send more packets frequently and thus overcome this problem.

**Note:** S36 and S60 are client drivers compatible with specific Cisco Compatible Extensions. S36 is compatible with CCXv2 or later. S60 is compatible with CCXv4 or later.

<http://www.cisco.com/c/en/us/support/docs/wireless/context-aware-software/110836-cas-faq.html>

## Configuring CCX Radio Management

### Configuring CCX Radio Management (GUI)

- Step 1** Choose **Wireless > 802.11a/n or 802.11b/g/n > Network** to open the 802.11a/n (or 802.11b/g/n) Global Parameters page.
- Step 2** Under **CCX Location Measurement**, select the **Mode** check box to globally enable CCX radio management. This parameter causes the access points connected to this Cisco WLC to issue broadcast radio measurement requests to clients running CCX v2 or later releases. **Provisioning mode: disabled** (or unselected).
- Step 3** If you selected the **Mode** check box in the previous step, enter a value in the **Interval** text box to specify how often the access points are to issue the broadcast radio measurement requests.
- The range is 60 to 32400 seconds.  
The default is 60 seconds.
- Step 4** Click **Apply**.
- Step 5** Click **Save Configuration**.
- Step 6** Follow the instructions in **Step 2** of the **Configuring CCX Radio Management (CLI)** section below to enable access point customization.
- Note** To enable CCX radio management for a particular access point, you must enable access point customization, which can be done only through the Cisco WLC CLI.
- Step 7** If desired, repeat this procedure for the other radio band (802.11a/n or 802.11b/g/n).

<http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4>

[/configuration/guides/consolidated/b\\_cg74\\_CONSOLIDATED/b\\_cg74\\_CONSOLIDATED\\_chapter\\_010000111.html](http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010000111.html)



## Context-Aware Software Features

This section summarizes the features for Context-Aware Software and contains the following topics:

- **S60 Enhancement**
- **Cisco Tag Engine**

### S60 Enhancement

Currently, client probes are used to extract RSSI information that enables location tracking of these clients. CCXv4 specification included a mandatory S60 component that was later made optional in CCXv5. At the time of this writing, the only 802.11a/b/g Wireless Card Bus Adapter which supported the optional S60 features in compliance to CCXv5 is the Cisco AIR-CB21AG-A-K9 (Kitty Hawk). Therefore, all S60 feature related testing will be tested with the AIR-CB21AG-A-K9. The S60 feature creates a Pathloss Measurement (PLM) request by an AP to be sent to the client which then causes the clients to send bursts of Pathloss Measurement frames, at regular intervals, back to the AP. The packets contain information about the channel and the tx power information. These help sort out the following issues:

- Off channel readings pollute the location calculation. It is not possible to determine with certainty off channel probes.
- Once a client associates, the probes are sent less frequently thus there is less information to calculate location more frequently. Additionally, some clients, by design, send few or no probe requests, and probe requests on channels subject to DFS rules are initially prohibited.
- Some specific client information, such as tx power, is missing from probes.

[http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/release/notes/mse7\\_0\\_220-0.html#pgfId-1128560](http://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/release/notes/mse7_0_220-0.html#pgfId-1128560)

#### 1. Re: MSE Location tracking - how fast should it update?

Hi DaneBlack,

The behavior that you are seeing is due to the probe rate of the device. All WiFi devices probe at different intervals based on factors such as battery life, whether associated or probing etc. The device vendors decide and implement different probe rate algorithms based on what they believe to be most important. That being said, in general, Android devices probe more frequently than iPhones/iPads, and laptops probe more frequently than either. Also the more probes the more battery drain, so as I mention, some vendors are more focused on battery life while others may not view this as important. The MSE does the location calculation very quickly and is able to return those location updates/result quickly. So in the scenario you describe it is not an MSE tracking issue but a client device probing issue.

The impact this has on location updates and accuracy is that we, the AP/WLC/MSE, only sees the device when it is probing. If the device is in one location and it moves to another location we will not know about the movement until the device probes from the second location.

This behavior causes the location inaccuracy and also creates jitter in the location application (blue dot display on the application).

I can say that we are working to implement ways to circumvent the device probe rate limitation. These methods will be available in subsequent product releases.

 Like (0)  Reply (Login Required)

<https://communities.cisco.com/thread/41579?start=0&tstart=0>

## Information About Configuring Location Settings

The switch determines the location of client devices by gathering Received Signal Strength Indication (RSSI) measurements from access points all around the client of interest. The switch can obtain location reports from up to 16 access points for clients, RFID tags, and rogue access points.

You can configure the path loss measurement (**S60**) request for normal clients or calibrating clients to improve location accuracy.

Configures the path loss measurement (**S60**) request for calibrating clients or non-calibrating.

The path loss measurement request improves the location accuracy. You can configure the **burst\_interval** parameter for the normal, noncalibrating client from zero through 3600 seconds, and the default value is 60 seconds.

You can configure the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio or on the associated 802.11a/b/g radio.

If a client does not send probes often or sends them only on a few channels, its location cannot be updated or cannot be updated accurately. The **location plm** command forces clients to send more packets on all channels. When a CCXv4 (or higher) client associates, the SwitchControllerDevice sends it a path loss measurement request, which instructs the client to transmit on the bands and channels that the access points are on (typically, channels 1,

[http://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\\_01010.pdf](http://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_01010.pdf)

### NO.11 DRAG DROP

When a client associates to an H-REAP access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication and data packets, the WLAN can be in any one of the following states, depending on the configuration and state of controller connectivity. Map the states on the left to the correct description on the right.

central authentication, central switching	In this state, the WLAN rejects any new clients trying to authenticate, but it continues sending beacon and probe responses to keep existing clients alive.
central authentication, local switching	This state is useful where you cannot maintain the criteria for a remote office setup with a minimum bandwidth of 128 kb/s, roundtrip latency no greater than 100 ms, and MTU no smaller than 500 bytes.
local authentication, local switching	In this state, the controller handles client authentication, and all client data tunnels back to the controller.
authentication down, switching down	In this state, the controller handles client authentication, and the H-REAP access point switches data packets locally. This state is applicable only in connected mode.
authentication down, local switching	In this state, the WLAN disassociates existing clients and stops sending beacon and probe responses.

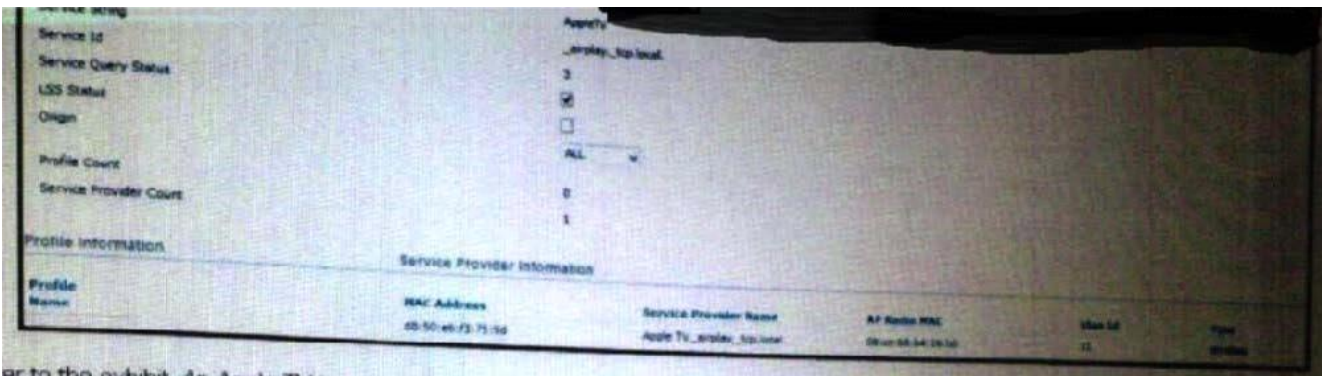
**Answer:**



When a client associates to an H-REAP access point, the access point sends all authentication messages to the controller and either switches the client data packets locally (locally switched) or sends them to the controller (centrally switched), depending on the WLAN configuration. With respect to client authentication and data packets, the WLAN can be in any one of the following states, depending on the configuration and state of controller connectivity. Map the states on the left to the correct description on the right.

central authentication, central switching	authentication down, local switching
central authentication, local switching	local authentication, local switching
local authentication, local switching	central authentication, central switching
authentication down, switching down	central authentication, local switching
authentication down, local switching	authentication down, switching down

**NO.12** Refer to the exhibit.







Refer to the exhibit. An Apple TV is associated to the wireless network wireless attempt to connect to it but they report that cannot discover the apple TV on their devices what is most likely the root cause?

- A. The mDNS origin is not set to wireless
- B. The mDNS globalsnooping is disabled
- C. The mDNS service provider is not associated to a profile
- D. The mDNS profile is not associated to the wlan

**Answer:** D









**NO.13** DRAG DROP

What do these icons represent on a WCS floor map? Drag each icon on the left to its corresponding meaning on the right.

	<input type="text"/>	an AP with a major fault
	<input type="text"/>	an AP that has been administratively disabled
	<input type="text"/>	an unassociated AP
	<input type="text"/>	an unreachable AP

**Answer:**

What do these icons represent on a WCS floor map? Drag each icon on the left to its corresponding meaning on the right.

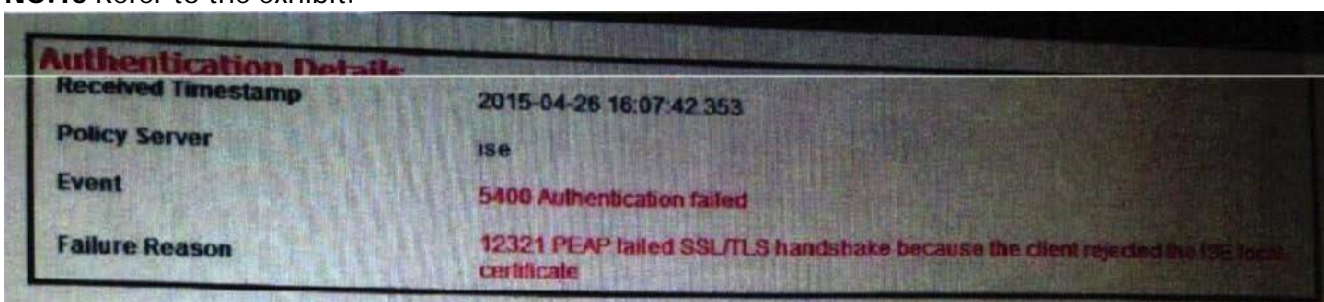
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>
	<input type="text"/>		<input type="text"/>

**NO.14** In the process of deploying a Cisco 7921G wireless IP Phone within the Cisco Unified Wireless Network, which feature will be implemented between the phone and the access point to mitigate one-way audio?

- A. NMSP
- B. DTCP
- C. DCA and TPC
- D. AKM

**Answer:** B

**NO.15** Refer to the exhibit.



What is the best way to resolve this issue?

- A. Install a publicly signed wildcard certificate by a well-known CA on the RADIUS server
- B. Disable certificate checks on the client.
- C. Use the certificate authority on the Cisco identity services Engine.
- D. Install a publicly signed server certificate by a well-known CA on the RADIUS server

**Answer: A**

**NO.16** Which two effects does TSPEC-based admission control have as it relates to WMM clients? (Choose two)

- A. Deny clients access to the WLAN that do not support WMM.
- B. Allow access only for VoWLAN traffic when interference is detected.
- C. Enforce airtime entitlement for wireless voice applications.
- D. Ensure that call quality does not degrade for existing VoWLAN calls.
- E. Deny clients access to the WLAN if then do not comply with the TERP standard.

**Answer: C,D**

Explanation:

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book/vowlan\\_ch2.html](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book/vowlan_ch2.html)

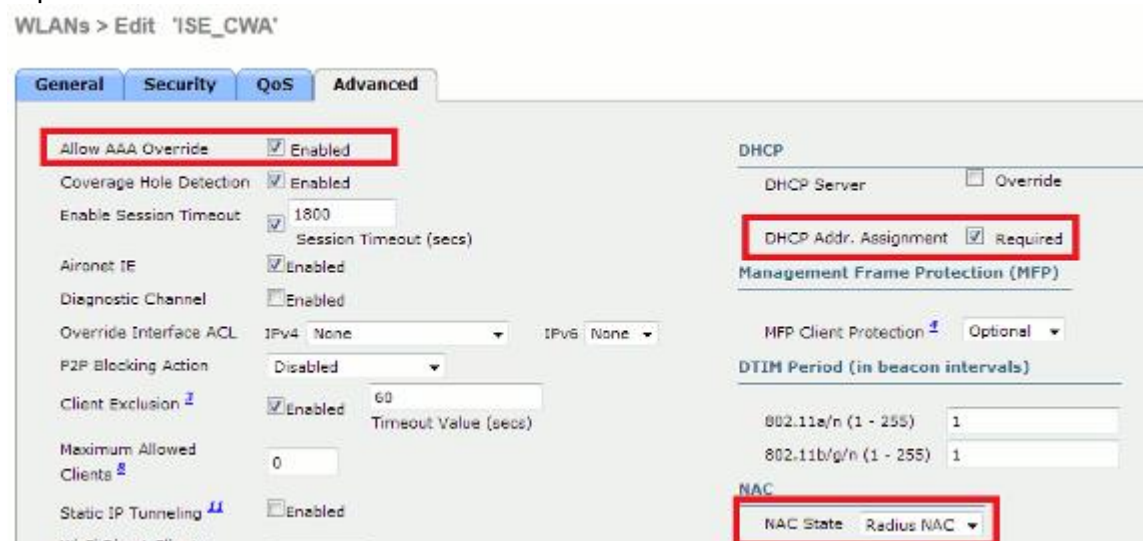
[http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan\\_troubleshoot/5\\_Troubleshooting\\_CAC\\_Rev1-2.html#wp1053384](http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/5_Troubleshooting_CAC_Rev1-2.html#wp1053384)

**NO.17** You are the network administrator at ACME Corporation and currently troubleshooting a Central Web Authentication issue where the guest users are not being redirected to the ISE guest login portal. You have verified that all configuration on the ISE is correct and that the ISE is sending the redirect URL for the client. Which configuration check can help to resolve the issue?

- A. Verify if DADIUS accounting interim update is enabled on the guest SSID.
- B. Verify if SNMP NAC is enabled on the guest SSID.
- C. Verify if the SSID is configured for VVPA2-AES Layer 2 security.
- D. Verify if AAA override is enabled for the guest SSID.
- E. Verify if the RFC 3567 support is enabled under ISE configuration on the Cisco WLC.
- F. Verify if authentication priority for web-auth is set to RADIUS.

**Answer: D**

Explanation:



<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web->



auth-00.html

**NO.18** What is the minimum VMware ESXi version you need to install Cisco prime infrastructure 2.2 virtual appliance?

- A. ESXi 4.1
- B. ESXi 5.0
- C. ESXi 4.0
- D. ESXi 5.5
- E. ESXi 5.1

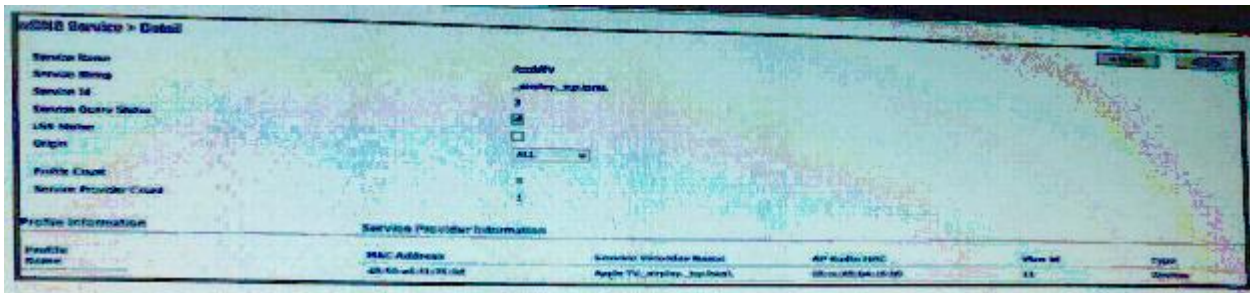
**Answer:** B

**NO.19** How does the Cisco Location Appliance locate a client or rogue access point?

- A. Use Triangulation
- B. Use Time Difference of Arrival
- C. Use RF fingerprinting
- D. Use closest access point method

**Answer:** C

**NO.20** Refer to the exhibit.



An Apple TV is associated to the wireless network. Wireless users attempt to connect to it, but they report that they cannot discover the Apple TV on their devices. What is most likely the root cause?

- A. The mDNS Origin is not set to wireless.
- B. The "Service ID" must be changed to 1 in order to ensure the highest priority for the traffic.
- C. The mDNS Service Provider is not associated to a profile.
- D. The "Service Provider Name" must not include "airplay" on it.

**Answer:** C

Explanation:

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless\\_Networks/Unified\\_Access/BYOD\\_Design\\_Guide/BYOD\\_Bonjour.html](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_Bonjour.html)