Cisco

Exam Questions 400-351

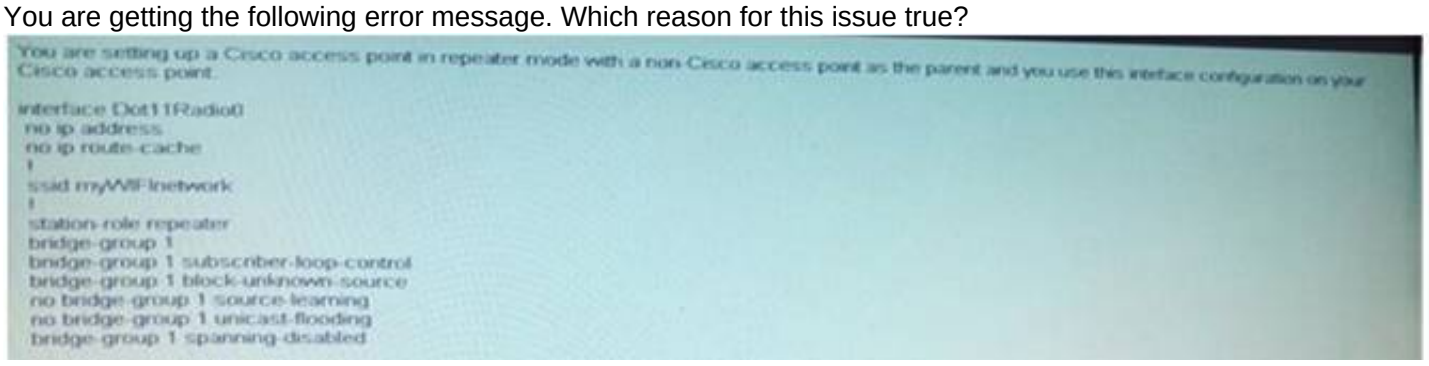
CCIE Wireless Written Exam

NEW QUESTION 1
Which four options are the HTTP methods supported by a reset API?

A. RETRIEVE
B. GET
C. PUT
D. DELETE
E. COPY
F. POST
G. SET

Answer: BCDF

NEW QUESTION 2
You are getting the following error message. Which reason for this issue true?



%DOT11-4-CANT_ASSOC Interface Dot 11 Radio0. Cannot associate NO Aironet Extension IE.

A. “dot11 extension ” is missing under the interface Dot11Radio 0 interface.
B. When repeater mode is used, unicast-flooding must be enabled to allow Aironet IE communications.
C. The parent AP MAC address has not been defined.
D. Repeater mode only works between Cisco access poin

Answer: A

Explanation:

This example shows how to set up a repeater acess point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-2_11_JA/configuration/guide/b12211sc/s11rep.html

NEW QUESTION 3
You are installing Converged Access controllers that run Cisco IOS-XE and you are ready to implement QoS. From the below, choose all the possible QoS target levels that would apply to downstream
traffic (toward the client)?

A. Client, SSID, Radio, Port
B. Client, SSID, Radio
C. Client, Radio
D. Client, SSID

Answer: A

Explanation:

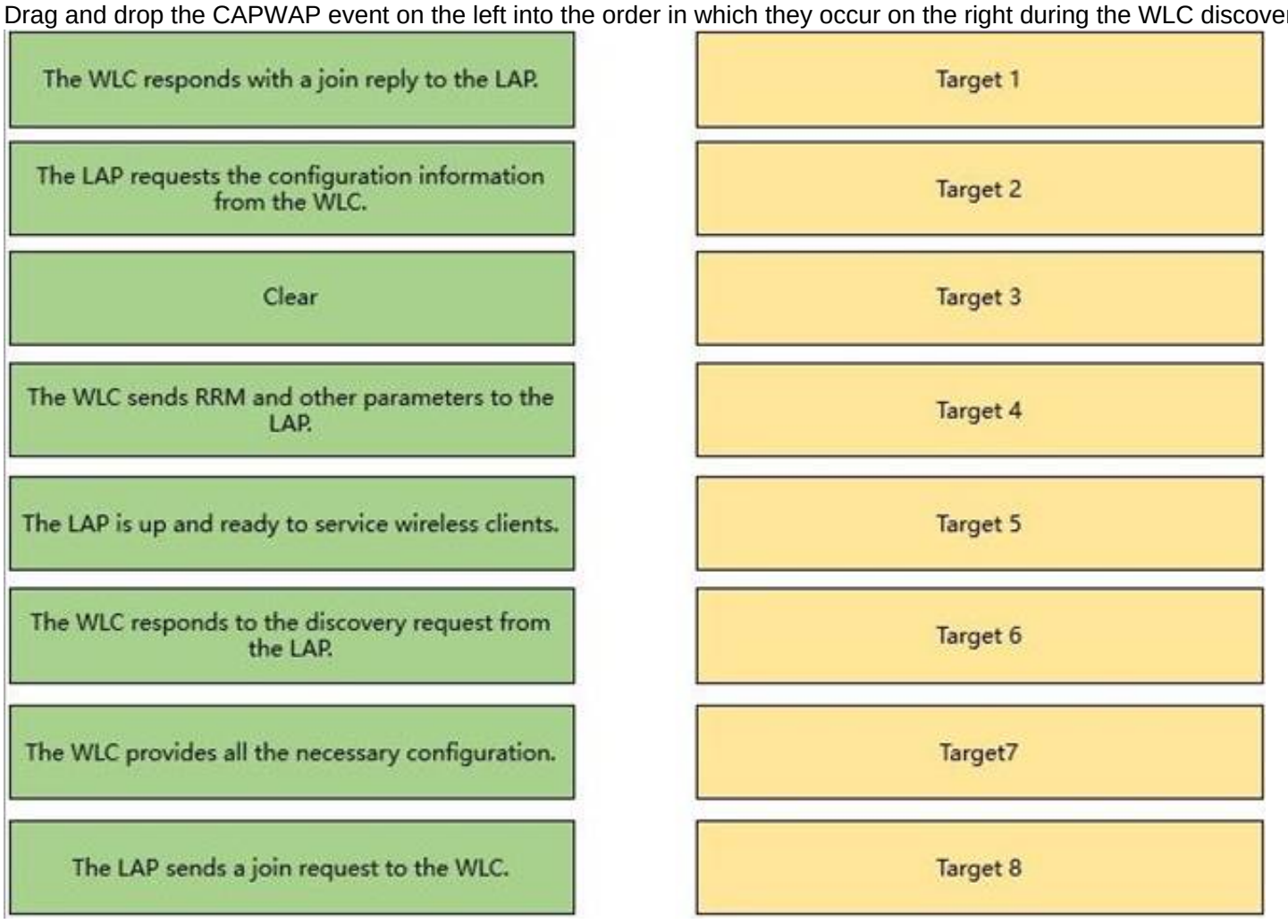
Restrictions for Wireless QoS

General Restrictions

- A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port, client, or VLAN. A wireless target can be either a port, SSID, client, or radio. Wireless QoS policies for p[illegible]are applied in the downstream direction. That is, when traffic is flowing from the switch to wireless client. Only port, SSID, and client (using AAA and Cisco IOS command-line interface) policies are user-configurable. Radio policies are set by the wireless control module and are not user-configurable.
- Port and radio policies are applicable only in the downstream direction (traffic flowing from a wired source to a wireless target).
- SSID and client support non-queuing policies in the upstream direction. SSID and client targets can be configured with marking and policing policies.
- One policy per target per direction is supported.
- For marking rules for access points associated with the switch, the following rules apply:
  - Policing at the access point is not supported.
  - Client policies that are passed to the access points in the upstream direction are not supported.
  - The following rules apply for QoS at the SSID:
    - One table map is supported at the ingress policy.
    - Up to three table maps can be configured in the egress direction for SSID when a QoS-group is involved.

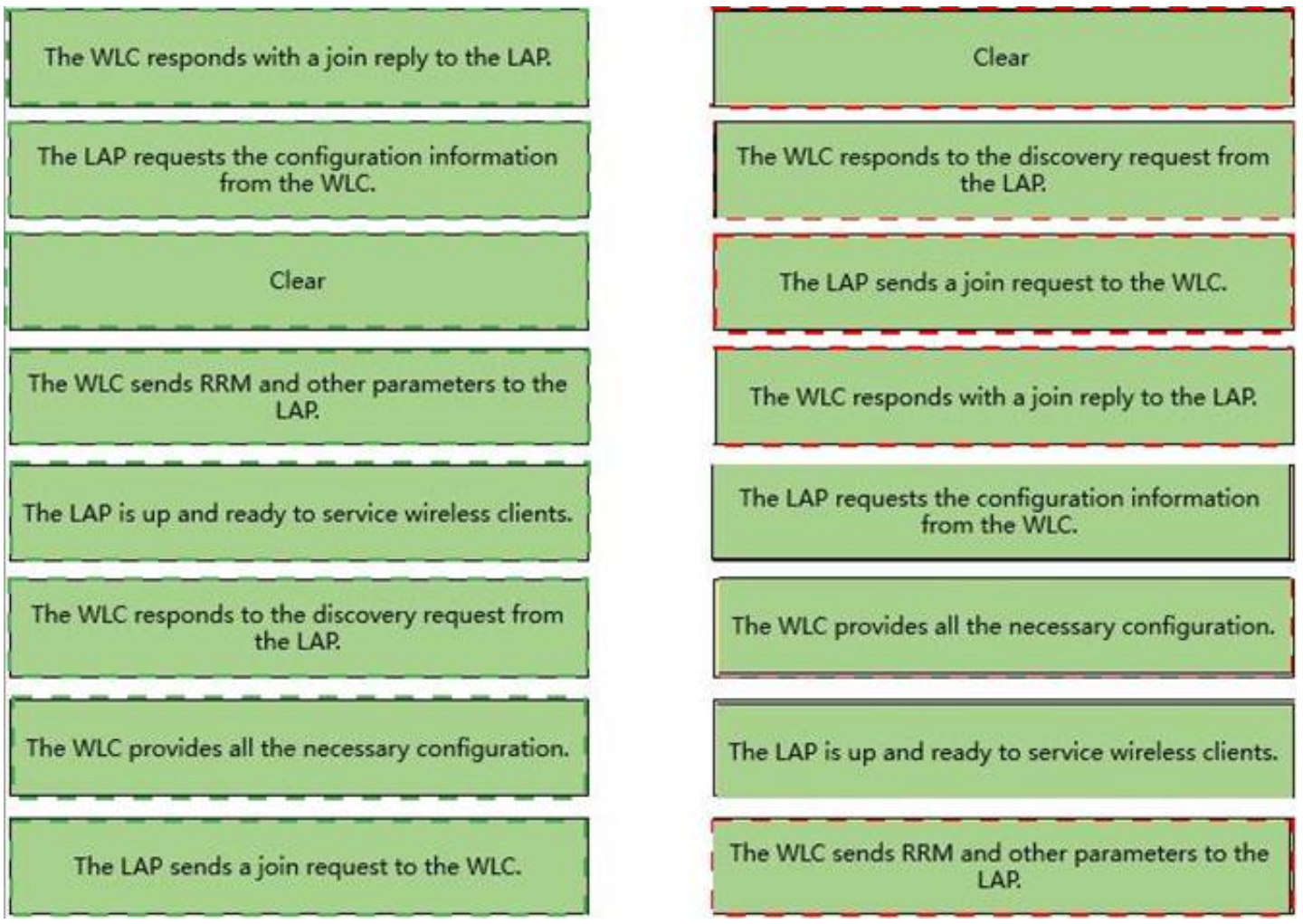
http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_010010.html

NEW QUESTION 4
DRAG DROP
Drag and drop the CAPWAP event on the left into the order in which they occur on the right during the WLC discovery and join processes.



Answer:

Explanation:



NEW QUESTION 5
Which memchanism incorporates the channel capacity into the CAC determination and gives a much more accurate assessment of the current call carrying capacity of the AP?

A. Static CAC.
B. Reserved roaming bandwidth(%).
C. Expedited bandwidth.
D. Metrics collection.
E. Load-based AC.
F. Max RF bandwidth (%).
G. Admission contro

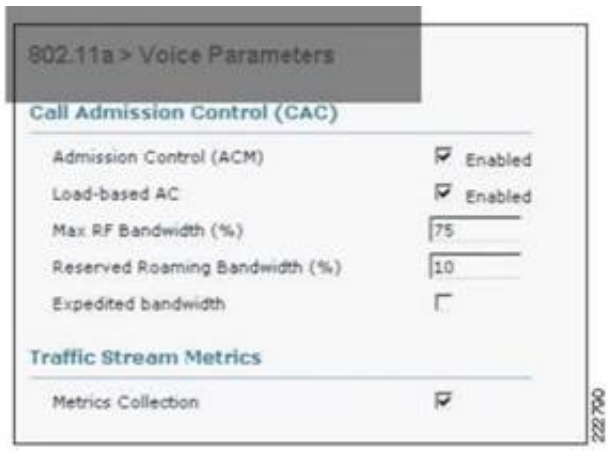
Answer: E

Explanation: AP Call Capacity
A key part of the planning process for a VoWLAN deployment is to plan the number of simultaneous voice streams per AP. When planning the voice stream capacity of the AP, consider the following points:
Note: A call between two phones associated to the same AP counts as two active voice streams.
The actual number of voice streams a channel can support is highly dependent on a number of issues, including environmental factors and client compliance to WMM and the Cisco Compatible Extension specifications. Figure 9-11 shows the Cisco Compatible Extension specifications that are most beneficial to call quality and channel capacity. Simulations indicate that a 5 GHz channel can support 14-18 calls. This means a coverage cell can include 20 APs, each operating on different channels, with each channel supporting 14 voice streams. The coverage cell can support 280 calls. The number of voice streams supported on a channel with 802.11b clients is 7; therefore, the coverage cell with three APs on the three non-overlapping channels supports 21 voice streams. Figure 9-11 Cisco Compatible Extension VoWLAN Features

How Cisco Compatible Extensions Benefits VoWLAN Call Quality	
Feature	**Benefit**
CCKM Support for EAP-Types	Locally Cached Credentials Means Faster Roams
Unscheduled Automatic Power Save Delivery (U-APSD)	More Channel Capacity and Better Battery Life
TSPEC-Based Call Admission Control (CAC)	Managed Call Capacity for Roaming and Emergency Calls
Voice Metrics	Better and More Informed Troubleshooting
Neighbor List	Reduced Client Channel Scanning
Load Balancing	Calls Balanced Between APs
Dynamic Transmit Power Control (DTPC)	Clients Learn a Power to Transmit At
Assisted Roaming	Faster Layer 2 Roams

210352

Call Admission Control (CAC) also benefits call quality and can create bandwidth reservation for E911 and roaming calls.
The 802.11e, WMM, and Cisco Compatible Extension specifications help balance and prevent the overloading of a cell with voice streams. CAC determines whether there is enough channel capacity to start a call; if not, the phone may scan for another channel. The primary benefit of U-ASPD is the preservation of WLAN client power by allowing the transmission of frames from the WLAN client to trigger the forwarding of client data frames that are being buffered at the AP for power saving purposes. The Neighbor List option provides the phone with a list that includes channel numbers and channel capacity of neighboring APs. This is done to improve call quality, provide faster roams, and improve battery life.
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dgwrapper/ preface41.html
Understanding Static CAC
As mentioned previously, there are two types of Admissions Control. Static CAC is based on a percentage of the total Medium Times available and is measure in increments of 32 microseconds. In this section, we will cover how to configure Static and Load-Based CAC and also how to debug it.
http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan
_troubleshoot/5_Troubleshooting_CAC_Rev1-2.html
Load-Based CAC on the other hand is significantly more difficult to debug. LBCAC is dynamic with
regard to the algorithm used to decrement Medium Times from the total that is available. LBCAC takes into consideration different metrics, such as load, Co-channel interference, SNR, etc. and will therefore yield different results when tested. From our experience, it is very difficult to yield consistent results as RF fluctuates and changes within the given environment. Results tend to vary from one cell area to another and even in cell areas that yield the same signal strength.
http://www.cisco.com/c/en/us/td/docs/wireless/controller/4-1/configuration/guide/ccfig41/c 41ccfg.html
o enable video CAC for this radio band, check the Admission Control (ACM) check box. The default value is disabled.
n the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients.
Range: 0 to 25%
Default: 0%
in the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.
Range: 0 to 25%
Default: 6%
To enable expedited bandwidth requests, check the Expedited Bandwidth check box. The default value is disabled.
To enable TSM, check the Metrics Collection check box. The default value is disabled. Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.
In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.
Range: 40 to 85%
Default: 75%



For best performance, the most accurate assessment of call capacity—*Load-based AC*—should be enabled. *Admission Control* enabled by itself uses the APs capacity to calculate the Call Admission Control (CAC). Load-based AC incorporates the channel capacity into the CAC determination and gives a much more accurate assessment of the current call-carrying capacity of the AP. Settings for the *Max RF bandwidth* and *Reserved Bandwidth* values depend on the VoWLAN handsets, the data rates used, and the other sources of the WLAN load. However, the Max RF Reservation should not be greater than 60 percent. At levels greater than 60 percent, the IEEE 802.11 protocol itself can start to be under stress with increases in retransmission. This can impact call quality even if WMM is being used, particularly if the is a number of voice calls are already in progress. Testing with the Cisco Unified IP Phone 7921G in both the 2.4 GHz and 5 GHz bands using the recommended signal levels and SNR suggests that the minimum value for the *Maximum Bandwidth Reservation* parameter of between 40 to 60 percent is also the best setting for this specific phone. Call quality starts to deteriorate when the ***Max RF Bandwidth*** is set at or below these levels.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book/vowlan_ch8.pdf

NEW QUESTION 6

On a Cisco 5760 WLC, which of the below is not part of the initial setup script?

A. Wireless management interface
B. Host name
C. HTTP server login account
D. SNMP Network Management
E. NTP server
F. Enable password
G. Default routing protocol

Answer: G

Explanation: From:
CT5760 Controller and Catalyst3850 Switch Configuration Example -
Cisco http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/116342-config-wlc-00.html
5760 WLC Initial Configuration
This section outlines the steps to succesfully configure the 5760 WLC in order to host wireless services.
Configure Setup Script
--- System Configuration Dialog --- Enable secret warning

In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the intial configuration dialog, or if you exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode- enable secret 0 <cleartext password>

Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: yes Configuring global parameters:
Enter host name [Controller]: w-5760-1
The enable secret is a password used to protect access to privileged EXEC and configuration modes.
This password, after entered, becomes encrypted in the configuration. Enter enable secret: cisco
The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images. Enter enable password: cisco
The virtual terminal password is used to protect access to the router over a network interface. Enter virtual terminal password: cisco Configure a NTP server now? [yes]: Enter ntp server address : 192.168.1.200 Enter a polling interval between 16 and 131072 secs which is power of 2:16 Do you want to configure wireless network? [no]: no
Setup account for accessing HTTP server? [yes]: yes Username [admin]: admin
Password [cisco]: cisco Password is UNENCRYPTED.
Configure SNMP Network Management? [no]: no Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration Interface IP-Address OK? Method Status Protocol
Vlan1 unassigned NO unset up up GigabitEthernet0/0 unassigned YES unset up up Te1/0/1unassigned YES unset up up Te1/0/2unassigned YES unset down down Te1/0/3unassigned YES unset down down Te1/0/4unassigned YES unset down down Te1/0/5unassigned YES unset down down Te1/0/6unassigned YES unset down down
Enter interface name used to connect to the
management network from the above interface summary: vlan1 Configuring interface Vlan1:
Configure IP on this interface? [yes]: yes IP address for this interface: 192.168.1.20
Subnet mask for this interface [255.255.255.0] : 255.255.255.0 Class C network is 192.168.1.0, 24 subnet bits; mask is /24 Wireless management interface needs to be configured at startup It needs to be mapped to an SVI that's not Vlan 1 (default) Enter VLAN No for wireless management interface: 120
Enter IP address :192.168.120.94 Enter IP address mask: 255.255.255.0
The following configuration command script was created: w-5760-1
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY^Q enable password cisco line vty 0 15
password cisco
ntp server 192.168.1.200 maxpoll 4 minpoll 4 username admin privilege 15 password cisco no snmp-server
!
no ip routing

!i
nterface Vlan1 no shutdown
ip address 192.168.1.20 255.255.255.0
!i
nterface GigabitEthernet0/0 shutdown no ip address
!i
nterface TenGigabitEthernet1/0/1
!i
nterface TenGigabitEthernet1/0/2
!i
nterface TenGigabitEthernet1/0/3
!i
nterface TenGigabitEthernet1/0/4
!i
nterface TenGigabitEthernet1/0/5
!i
nterface TenGigabitEthernet1/0/6 vlan 120
interface vlan 120
ip addr 192.168.120.94 255.255.255.0 exit
wireless management interface Vlan120
!
end
[0] Go to the IOS command prompt without saving this config. [1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit. Enter your selection [2]: 2
Building configuration...
Compressed configuration from 2729 bytes to 1613 bytes[OK]
Use the enabled mode 'configure' command to modify this configuration. Press RETURN to get started!

NEW QUESTION 7
A Cisco Unified 7925G Wireless IP Phone is operating on the 5 GHz band and transmitting at a power level of 40 mW. Which configuration must be done on the controller to avoid one-way audio?

A. In DCA, enable UNH-1 channels only.
B. Set the maximum power level assignment to 26 dBm.
C. In DCA, enable UNII-II channels only.
D. Set the maximum power level assignment to 16 dB

Answer: D

Explanation: https://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-wireless-ip-phone-7925g/200032-How-to-get-your-792x-wireless-phones-per.html

NEW QUESTION 8
Refer to the exhibit.

You are troubleshooting location accuracy problems on a customer deployment. You have done the wireless design and you are sure that the As are correctly placed on the Cisco Prime map. Everything is correctly synchronized between WLC, PI, and MSE but, you are sometimes getting elements tracked on the wrong floor. After you get this debug output from MSE, which step is next?

A. Reduce the confidence level on MSE when the last heard value is higher than 150 seconds.
B. Run a new calibration model and ensure that it is applied on the floor.
C. Discard RSSI values lower than – 75 dbm.
D. Check it the AP with MAC address 001c 0f 4c 45 60 is physically located on the floor where the element was wrongly located and if the inter-floor attenuation is weak.

Answer: C

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/1- 3/configuration/guide/pi_13_cg/maps.pdf

Q. When Devices are shown on the wrong floor, what is the Interfloor debug checklist/procedure?

A. The floor determination is carried out based on the RSSIs received by APs on different floors. So if APs are incorrectly placed on floors this can lead to Interfloor. Also, verify the current location of the device under consideration; make sure it has not moved to a different floors by another user.

Is the deployment correct?—Incorrectly placed APs on the WCS maps can cause interfloor and in general lead to poor location accuracy. Check if the APs physical location is consistent with the APs position marked on WCS maps.

Does the deployment comply with the deployment guidelines?—Inconsistency in these deployment guidelines between floors can also lead to interfloor problems. Refer to the user guide on deployment guidelines.

Does the problem only occur in some area or everywhere?—Due to building structure and RF characteristics, APs on adjacent floors can hear a device more strongly than the APs on the current floor. From software release 5.2, new algorithms were added to mitigate against such scenarios. The addition of few APs in such regions usually provides the information needed by the system to correct such problems.

NEW QUESTION 9
Which three conditions can trigger a client exclusion policy?(Choose three.)

A. Excessive 802.11 probe request failures
B. Excessive 802.lx authorization failures
C. IP theft or IP reuse
D. Excessive 802.lx authentication failures
E. Excessive 802.11 association failures
F. Excessive 802.11 packet retries

Answer: CDE

Explanation: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/117714-technoteaireoswlc- 00.html

NEW QUESTION 10
Which two features were added as part of the 802.llh amendment?

A. Dynamic Frequency Selection and Direct Link Setup.
B. Dynamic Frequency Selection and Transmit Power control.
C. Dynamic Frequency Selection and Wireless Performance Prediction.
D. Dynamic Frequency Selection and Inter-Access Point Protoco

Answer: B

Explanation:

Introduction

This document is an overview about a subpart of the wireless 802.11 standard : 802.11h and the impact of this amendment on wireless deployments and what it translates to in terms of configuration. This amendment was meant to bring two main features : Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC). DFS, as spectrum management (mainly to co-operate with radars) and TPC, to limit the overall RF "pollution" of wireless devices.

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/80211/200069-Overview-on-802-11h-Transmit-Power-Cont.html
http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/Enterprise-Mobility-8-1-Design- Guide/Enterprise_Mobility_8-1_Deployment_Guide/wlanrf.html

NEW QUESTION 10
VLAN Trunking Protocol is a Cisco proprietary protocol that propagates the definition of VLANs over the local area network. Which two statements are true?(Choose two.)

A. VTP requires access mode interfaces to propagate.
B. VTP requires trunk mode interfaces to propagate.
C. VTP transparent mode forwards VTP packets and can act as a client or a server.
D. VTP config revision increases base on switch uptime.
E. When Cisco switches are started from scratch, they are in server mode and their domain is set to null.

Answer: BE

NEW QUESTION 12
Which statement about Wired Guest Access is true?

A. The guest traffic can terminate on the foreign WLC, but egress interface must be defined on theguest SSID
B. Wired Guest Access is not supported in the Cisco 5760 WLC
C. The wired guest traffic terminates only on the anchor Cisco WLC
D. The Cisco 5760 WLC supports Wired Guest Access only in conjunction with the converged access switches.

Answer: C

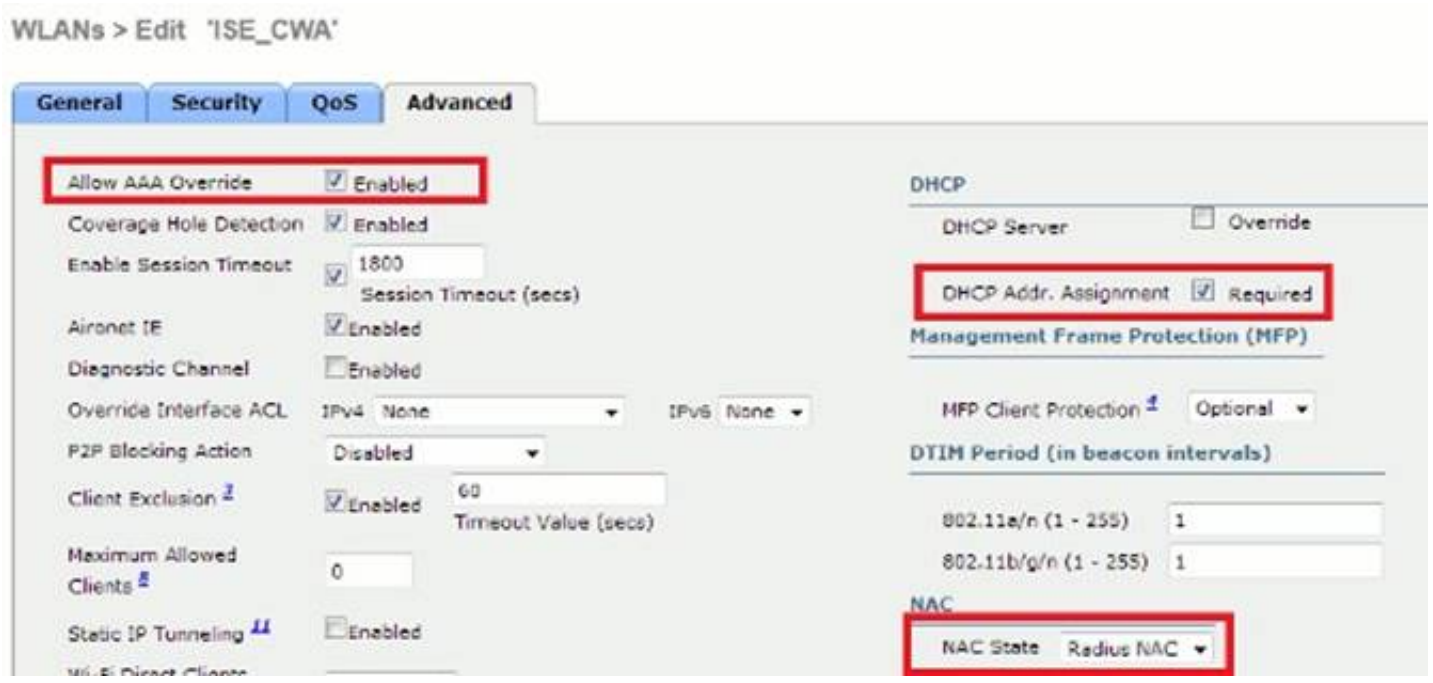
Explanation: http://www.cisco.com/c/en/us/support/docs/wireless/5700-series-wireless-lan-controllers/118810- technote-wlc-00.html

NEW QUESTION 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 RADIU

Answer: D

Explanation:



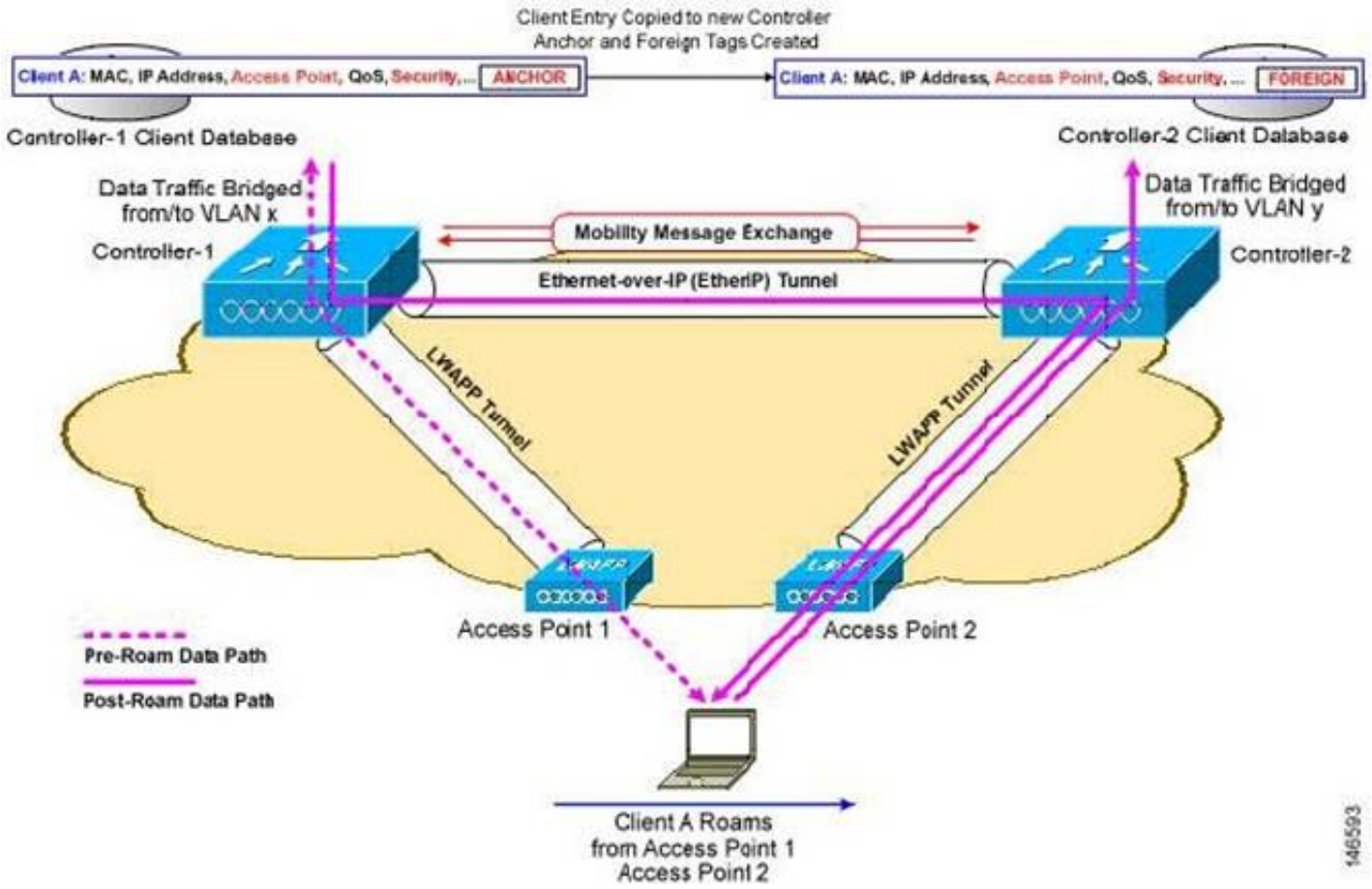
http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-webauth- 00.html

NEW QUESTION 20
If a guest anchor controller is used outside the firewall. Which firewall ports must you open for guest access including SNMP and mobility failover features to work in a Cisco Unified Wireless Network?

A. UDP 16666. IP protocol 90. UDP 162 163
B. UDP 16667. IP protocol 97. UDP 500 501
C. UDP 16666. IP protocol 97. UDP 161 162
D. UDP 12223. IP protocol 97. UDP 161 162
E. UDP 12222. IP protocol 90. UDP 161 162

Answer: C

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configurationguide/b_cg80/b_cg80_chapter_010011.html

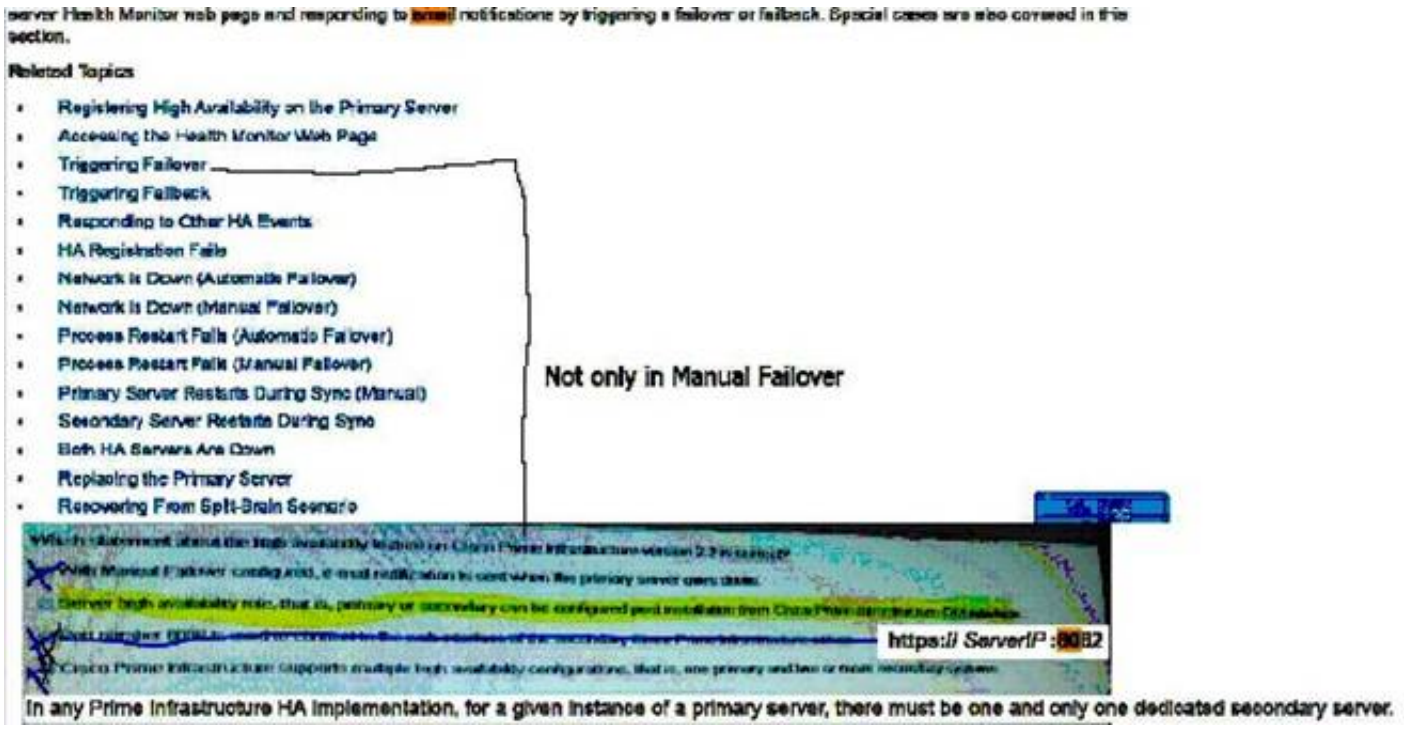


NEW QUESTION 21
Which statement about the high availability feature on Cisco Prime Infrastructure version 2.2 is correct?

A. With Manual Failover configure
B. e-mail notification is sent when the primary server goes down.
C. Server high availability role, that is , primary or secondary can be configured post installation formCisco Prime Infrastructure GUI interface.
D. Port number 8088 is used to connect to the web interface of the secondary Cisco Prime Infrastructure Server.
E. Cisco Prime Infrastructure supports multiple high availability configurations, that is, one primary and two or more secondary systems.

Answer: A

Explanation:



http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-2/administrator/guide/PIAdminBook/config_HA.html

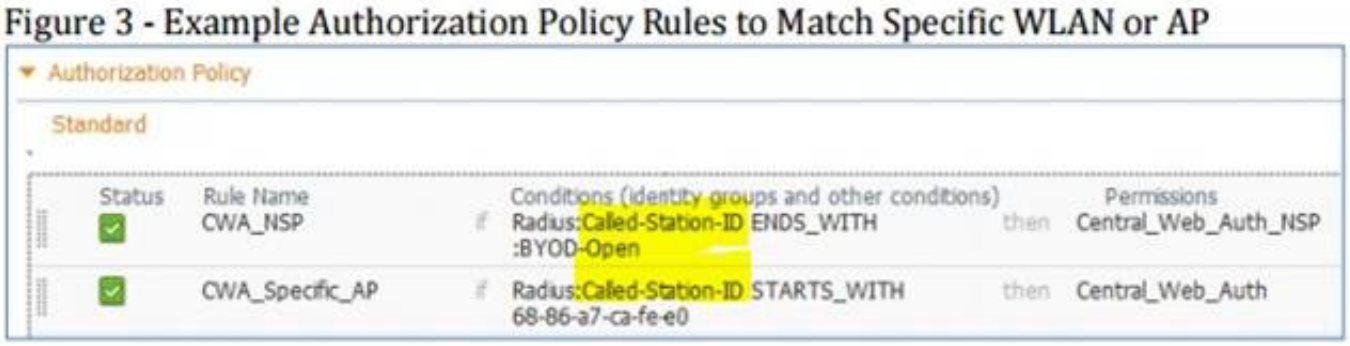
NEW QUESTION 25
Which two IETF RADIUS attributes sent by the Cisco WLC can be used to differentiate authentication requests based on the user location?(Choose two.)

A. RADIUS attribute [31] Calling-Station-Id
B. RADIUS attribute [4] NAS-IP-Address
C. RADIUS attribute [95] NAS-IPv6-Address
D. RADIUS attribute [32] NAS-Identifier
E. RADIUS attribute [303] Source-IP
F. RADIUS attribute [30] Called-Station-Id

Answer: DF

Explanation:

Figure 3 - Example Authorization Policy Rules to Match Specific WLAN or AP



https://supportforums.cisco.com/sites/default/files/ise_location-based_web_portals-v2.pdf

NEW QUESTION 27
Which three statements about enabling the wireless feature on Cisco Catalyst 4500E Supervisor Engine 8-E are true?(Choose three.)

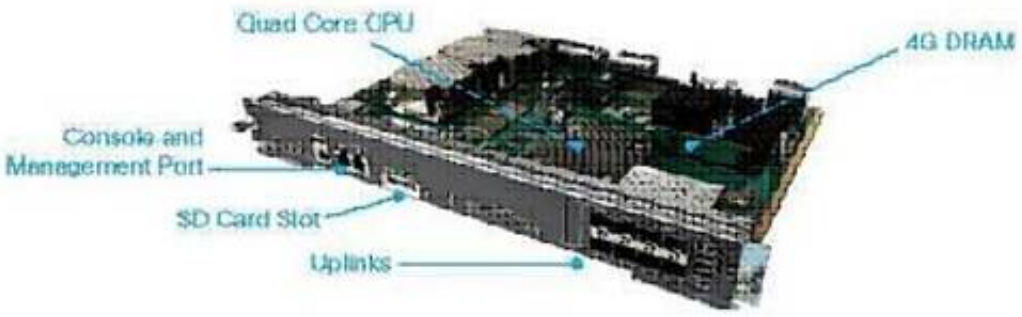
A. Only the install boot method is supported.
B. Access points must terminate on the same chassis/SUP to join the wireless controller.
C. Visual Switching System must be disabled.
D. Maximum number of access points that can join the wireless controller is 200, and the maximum number of wireless clients that can be supported by wireless controller is 4000.
E. Bundle and install boot modes are supported.
F. Virtual Switching System must be enable

Answer: ABC

Explanation:

Introduction

This Document is written by "Viten Patel", is working as Technical Marketing Engineer (Converged Access) at Cisco. He was working as Wireless Escalation Engineer - Cisco TAC and holds many wireless certification like CCIE Wireless, CCNP Wireless, CCNA Wireless, CWNA, CWSP, CWAP, CWNE#146.
This document explains things we need to take care before getting the 4500 SUP8E up and running for Wireless.
The Cisco Catalyst® 4500E Supervisor Engine 8-E is the next generation of enterprise-class switching engine that provides full convergence between wired and wireless networks on a single platform. This new Cisco® Unified Access Data Plane (UADP) application-specific integrated circuit (ASIC) powers the wireless convergence and helps enable uniform wired-wireless policy enforcement, application visibility, flexibility, and application optimization.



Requirements

To get Wireless up and running on this box we have to make sure the below requirements are satisfied

1. Check Rommon version
2. Image should be K9 - Crypto
3. VSS not supported
4. Switch should run install mode
5. License should be Entservices or IP base
6. In Bundle Mode Daughter card will not come up (only in install mode)
7. Max supported APs -50 / Max supported Clients – 2000
8. AP should terminate on the same chassis / SUP
9. Once you get the above up, rest of the config is similar to any 3850 / 5760

https://supportforums.cisco.com/document/12515266/sup8e-4500-wireless-installation

3. Verify VSS

Pre 3.8 behavior :

If VSS enabled wireless commands will not be present and the vice-versa if Wireless is enabled VSS commands are not present

4500-2#sh switch virtual
Switch Mode : Standalone
Not in Virtual Switch mode due to:
Domain ID is not configured

Starting IOS XE 3.8 and later :

Dual-Sup VSS is supported with Wireless operations. However Quad-Sup VSS is not supported with wireless.

http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4500-series-switches/200082-Getting-Started-with-SUP8E-4500-Wireless.html

Cisco Catalyst 4500 Supervisor Engine 8-E Wireless Mode Quick-Start Guide

Download Print

Updated: Jan 23, 2015

Introduction

The new Cisco Catalyst® 4500 Supervisor Engine 8-E helps to enable the Cisco® Converged Access solution on the world's most widely deployed modular access switches: the Cisco Catalyst 4500E Series Switches. These switches bring the best of wired and wireless technologies together while preserving your investment on existing wired infrastructure. Cisco Catalyst 4500 Supervisor Engine 8-E supports a built-in wireless controller with a single software image for wired and wireless infrastructure. Cisco Catalyst Supervisor Engine 8-E supports up to 20 Gbps wireless throughput, 50 access points, and 2000 wireless clients on a single system.

For detail on converged access and wireless modes, see the following white paper on converged access.
Cisco Unified Access Technology Overview - Converged Access White Paper

This document describes the requirements and procedure required to start a Cisco Catalyst 4500E Series Switch with Supervisor Engine 8-E in wireless mode.

Prerequisite for Wireless on a Cisco Catalyst 4500 Series Switch

Hardware: Cisco Catalyst 4500 Supervisor Engine 8-E

Cisco Catalyst 4500 Supervisor Engine 8-E has a daughter card with Cisco Unified Access™ Data Plane application-specific integrated circuit (ASIC), which enable the capability of wireless in the Cisco Catalyst 4500 Supervisor Engine 8-E.

Software requirement: Wireless mode is supported only in Cisco Catalyst 4500 Supervisor Engine 8-E cat4500es8-universalk9* (Crypto) images.

Cisco IOS® XE 3.7.0E and Cisco IOS ROMMON Software Version 16.1(1r)SG4, or later. Make sure that you have the Cisco Catalyst 4500 Supervisor Engine 8-E started with Cisco IOS ROMMON Software Version 15.1(1r)SG4, or later. The updated IOS ROMMON Software is available for download at Cisco.com. For the detailed steps to upgrade the Cisco Catalyst 4500 Supervisor Engine 8-E, see http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/release/note/OL_30306-01.html.

License Requirement: Supported only in IP Base, and EntServices licenses.

Note :

- [redacted]
- In wireless mode no line card is supported in the 10th slot of the Cisco Catalyst 4510R-E chassis.

Starting Cisco Catalyst 4500 Supervisor Engine 8-E in Wired and Wireless Mode.

Traditionally the Cisco Catalyst 4500 Supervisor Engine 8-E is started with a .bin image, which is called a "bundle boot."

To start wireless mode, additional steps are required, which is called the "install boot." Both of these startup methods are explained in the following.

获取支持

询价

电邮 | 电话

寻找本地经销商

致电 4006 680 680
或 4008 100 110
其他国家/地区

Viewers of This Document Also Viewed

- Cisco Catalyst 4500E Supervisor Engine 8-E: Wired and Wireless Convergence Data Sheet
- Getting Started with SUP8E 4500 Wireless: Initial Installation and Troubleshooting
- Introducing Cisco Catalyst 4500E Supervisor Engine 8-E with Wired and Wireless Convergence

+ Show 8 More

Was this Document Helpful?

Yes No × Feedback

Share

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/guidec07- 733704.html

Cisco Catalyst 4500E Supervisor Engine 8-E Feature Highlights

The Cisco Catalyst 4500E Supervisor Engine 8-E is the first Cisco Catalyst supervisor engine to bring wired and wireless convergence to a single platform. In addition, the enterprise-class Cisco Catalyst 4500E Supervisor Engine 8-E offers the following:

- Performance and capability
  - Up to 928 Gbps wired switching capacity with 250 Mpps of throughput
  - Up to 20 Gigabits of wireless termination capacity for a wireless controller-less design. Support for up to 50 access points and 2000 wireless clients on each switching entity (software roadmap)
  - Support of 250 access points and 4000 wireless clients in wireless controller-less deployments with multiple Catalyst 4500E systems forming a wireless domain (software roadmap)
  - Up to eight nonblocking 10 Gigabit Ethernet uplinks (Small Form-Factor Pluggable Plus [SFP+])

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-seriesswitches/data_sheet_c78-728191.html

Converged Wired and Wireless Access

Cisco Catalyst Supervisor 8-E extends wired features to wireless, including infrastructure, resiliency, quality of service (QoS), and scalability. One common set of network capabilities and context-aware intelligence work across wired and wireless networks. You also get:

- A built-in wireless controller with a single software image for the wired and wireless infrastructure
- Support for up to 20 Gbps wireless throughput, 50 access points, and 2000 wireless clients on single system
- Support for up to 250 access points and 4000 clients in a multi-switch controllerless deployment
- Networkwide application visibility and control, and consistent QoS and security, on both wired and wireless networks
- Nonstop Forwarding with Stateful Switchover (NSF/SSO) extended to wireless traffic

http://www.cisco.com/c/en/us/products/switches/catalyst-4500-series-switches/index.html

- In wireless mode no line card is supported in the 10th slot of the Cisco Catalyst 4510R-E chassis.

Starting Cisco Catalyst 4500 Supervisor Engine 8-E in Wired and Wireless Mode.

Traditionally the Cisco Catalyst 4500 Supervisor Engine 8-E is started with a .bin image, which is called a "bundle boot."

To start wireless mode, additional steps are required, which is called the "install boot." Both of these startup methods are explained in the following.

Bundle Boot

Wired customers always use the bundle boot method, which is basically starting the Cisco IOS XE 3.07.0E image file. The daughter card is disabled in the bundle boot method, and daughter-card-related packages are not copied to the running system.

Install Boot

Wireless customers use the install boot method, in which the bundle image is installed first. Then the packages.conf file is installed in bootflash. The install boot is supported only from bootflash, as per installer design. The daughter card is enabled by default in the install boot method.

Note: The startup time in wired mode (bundle boot) is comparable to the startup time of Cisco IOS XE 3.6.0E (approximately 6 to 7 minutes), and wireless mode takes approximately 9 to 10 minutes to start.

Following are the steps to perform a bundle boot and install boot. To perform the install boot for the first time, you must perform a bundle boot first.

Step 1. (bundle boot): Start system with the copied image from bootflash:

Sup8E# boot system flash bootflash:cat4500es8-universalk9.SSA.03.17.51.PI4.152-3.1.51.PI4.bin

Step 2. Reload the switch to start the switch in Cisco IOS XE 3.7.0E wired mode.

To complete the install boot for a wireless mode setup, follow these additional steps:

Step 1. Expand and install the target image from bootflash. (This step copies the necessary packages file in bootflash.)

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/guidec07- 733704.html

NEW QUESTION 31
Which action is needed to edit the settings of an RF profile?

A. Disable both radio networks
B. Disable custom power level settings for all APs within the group to which the profile is linked.
C. Remove the desired RF profile from all AP groups
D. RF profiles cannot be edite
E. They must be removed and recreated with the desired value

Answer: C

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configurationguide/b_cg80/b_cg80_chapter_01011101.html

NEW QUESTION 34
When connecting an autonomous access point in workgroup bridge mode to a WLAN configured on a Cisco WLC. Which two options are true? (Choose two.)

A. The WGB mode allows to connect only one wired client behind the WGB to the WLAN.
B. The WGB cannot serve wireless clients.
C. The traffic of the wired client behind the WGB can be tunneled only to the Cisco WLC on the VLAN configured for the dynamic interface of the WLAN.
D. The traffic of the wired client tagged on a specific VLAN behind the WGB can be tunneled to the same VLAN behind the the Cisco WLC.
E. The WGB creates a network extension for the wired clients.
F. The WGB could serve wireless clients only on the other radio not connecting to the WLA

Answer: BC

Explanation:
http://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/RolesWGB.html

NEW QUESTION 35
Which enhancement was introduced in 802.11ac Wave 2 and was not present in 802.lln?

A. 64 QAM
B. 128 QAM
C. MU-MIMO
D. 40MHz channel width
E. four spatial streams
F. SU-MIMO

Answer: C

Explanation:

Table 1. Comparing 802.11ac Wave 2, Wave 1, and 802.11n

	802.11n	802.11n IEEE Specification	802.11ac Wave 1 Today	802.11ac Wave2 WFA Certification Process Continues	802.11ac IEEE Specification
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz	5 GHz	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)	Multi User (MU)	Multi User (MU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps	2.34 Gbps - 5.47 Gbps	6.9 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
Modulation	64 QAM	64 QAM	256 QAM	256 QAM	256 QAM
Spatial Streams	3	4	3	3-4	8
MAC Throughput*	293 Mbps	390 Mbps	845 Mbps	1.52 Gbps- 2.26 Gbps	4.45 Gbps

* Assuming a 65% MAC efficiency with highest MCS

Q. What's the functional difference between 802.11ac Wave 1 and Wave 2?

A. Wave 1 products have been in use in the market for about 2.5 years. Wave 2 builds upon Wave 1 with some very significant enhancements:

- Supports speeds to 2.34 Gbps (up from 1.3 Gbps) in the 5 GHz band
- Supports multiuser multiple input, multiple output (MU-MIMO)

http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ac-solution/q-and-ac67- 734152.html

NEW QUESTION 39
For "Local mode" APs, which multicast mode is recommended when configuring Media Stream on a Cisco WLC?

A. Multicast-multicast
B. Multicast-unicast
C. Multicast-routing
D. Multicast-direct

Answer: A

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configurationguide/b_cg80/b_cg80_chapter_01111.html

NEW QUESTION 43
Which event happens when a wireless client connects to a Cisco 5760 Converged Access Controller with a WLAN configured for AAA override enabled and an invalid VLAN (not configured on the Cisco 5760) is returned as part of RADIUS accept message by the Cisco ISE server?

A. The client is marked as associated and DHCP required state.
B. The client is marked as authenticated but does not get an IP address.
C. The client is put in exclusion list by the WLC.
D. The client is put in the RUN state and is mapped to the wireless management VLA

Answer: B

Explanation:

Users Are Assigned to Incorrect VLAN During Network Access Sessions	
Symptoms or Issue	Client machines are experiencing a variety of access issues related to VLAN assignments.
Conditions	Click on the magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following lines: • %AUTHMGR-5-FAIL: Authorization failed for client (001b.a912.3782) on Interface Gi0/3 AuditSessionID 0A000A7600000008D4C69994E • %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN 666 to 802.1x port FastEthernet1/9 You can also run the troubleshooting workflow for the authentication. This workflow compares the ACL authentication log that contains RADIUS switch responses with the switch message database. Logging configuration (global) details may also be displayed: • Mandatory Expected Configuration Found On Device • logging monitor informational Missing • logging origin-id ip Missing • logging source-interface <interface_id> Missing • logging <syslog_server_IP_address_x> transport udp port 20514 Missing **Note** The network device must send syslog messages to the Monitoring ISE node server port 20514.
Possible Causes	The switch is missing (or contains the incorrect) name and numbers on the switch.
Resolution	Verify VLAN configuration(s) on the network access/enforcement points (switches) in your deployment.

http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_troubleshooting.html#wp104 3599

NEW QUESTION 48
Which three statements about 802.11ac are true? (Choose three.) Which three statements about 802.11ac are true? (Choose three.)

A. When using MU-MIMO, up to 8 devices can transmit data at the same time.
B. MU-MIMO allows one AP to transmit unique data to multiple stations simultaneously.
C. MU-MIMO is supported in Wave1.
D. 802.11 a/b/g/n devices are able to connect to 802.11 ac radios.
E. 802.11ac is supported in the 2.4- and 5-GHz radio band.
F. It is possible to reach 160 MHz by combining two discontiguous 80MHz channel block

Answer: BDF

Explanation: https://meraki.cisco.com/blog/2013/08/4-things-you-need-to-know-about-802-11ac/

NEW QUESTION 53
When configuration an autonoumous access point, which configuration broadcasts two SSIDs?

A. dot11 ssid data1 vlan 10 authentication openauthentication key-managerment wpa version 1 wpa-psk ascii cisco123end!dot11 ssid data2 vlan 11 authentication openauthentication key-management wpa version 2 wps-psk accii Cisco12345end
B. dot11 ssid data1 vlan 10 authentication openauthentication key-management wpa version 1 wpa-psk ascii cisco123mbssid guest-mode end!dot11 ssid data2 vlan 11 authentication openauthentication key-management wpa version 2 wpa-psk accii Cisco12345mbssid guest-mode end
C. mbssid!dot11 ssid data1 vlan 10 authentication openauthentication key-management wpa version 1 wpa-psk ascii cisco123end!dot11 ssid data2 vlan 11authentication openauthentication key-management wpa version 2 wpa-psk accii Cisco12345end
D. dot11 ssid data1 vlan 10 authentication openauthentication key-management wpa version 1 wpa-psk ascii cisco123guest-mode end!dot11 ssid data2 vlan 11 authentication openauthentication key-management wpa version 2 wpa-psk ascii cisco12345guest-mode end
E. dot11 ssid data1 vlan 10 authentication openauthentication key-management wpa version 1 wpa-psk ascii cisco123mbssid end!dot11 ssid data2 vlan 11 authentication openauthentication key-management wpa version 2 wpa-psk accii Cisco12345mbssid end

Answer: B

Explanation:

CLI Configuration Example

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is included in beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
router(config)# interface dot11 0
router(config-if)# mbssid
router(config-if)# exit
router(config)# dot11 ssid visitor
router(config-ssid)# mbssid guest-mode
router(config-ssid)# exit
router(config)# interface dot11 0
router(config-if)# ssid visitor
```

You can also use the **dot11 mbssid** global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

http://www.cisco.com/c/en/us/td/docs/routers/access/1800/wireless/configuration/guide/awg/s37 ssid.pdf

NEW QUESTION 56
You are the wireless administrator for ACME corporation. You must configure a Cisco Catalyst 3850 Series Switch to work as mobility agent to allow access point association to this switch. Which statement about this scenario is true?

A. Access points must be connected to an access port that has the access VLAN configured to be the same as the service port VLAN on the Catalyst 3850 switch.Access points must be connected to a trunk port with the native VLAN set to 1 in order to join the WLC on the Catalyst 3850 switch.
B. Access points must be connected to an access port with the access VLAN configured to the same as the wireless management VLAN on the Catalyst 3850 switch.
C. Access points must be connected to an access port that has the access VLAN configured to be the same as the management VLAN for the switch stack.
D. Access points must be connected to an access port with the access VLAN configured to be any VLAN that has a Layer 3 interface (SVI) on the Catalyst 3850 switch.

Answer: C

Explanation: https://mrncciew.com/2013/09/29/getting-started-with-3850/

2. **Wireless management vlan & AP management vlan should be identical**. If you configure vlan 21 as wireless management in 3850 switch all your APs connected to this switch should be on access vlan 21.

AP------> WLC Connectivity

In order for Access Points to join the controller, the switchport configuration **must be set as an access port** in the wireless management vlan:

If using vlan 100 for wireless management interface:

```
sw-3850-1(config)#interface gigabit1/0/10
sw-3850-1(config-if)#switchport mode access
sw-3850-1(config-if)#switchport access vlan 100
```

Wireless Pre-requisites

To enable wireless services, the 3850 must be running an **ipservices or ipbase** license

Enable Wireless on the Switch

Note: The Access Points will need to be connected to access mode

switchports in the same VLAN!

- Enable Wireless Management

  sw-3850-1(config)#wireless management interface vlan <1-4095>

- Define Mobility Controller

  A Mobility Controller (MC) must be defined in order to allow Access Points to join

  a. If this 3850 will be the Mobility Controller

  sw-3850-1(config)#wireless mobility controller

  Note: This configuration change will require a reboot!

  b. If this 3850 will operate as a Mobility Agent (MA). Then please point it to the MC IP address using the following

  command

  sw-3850-1(config)#wireless mobility controller ip a.b.c.d

  And on the MC

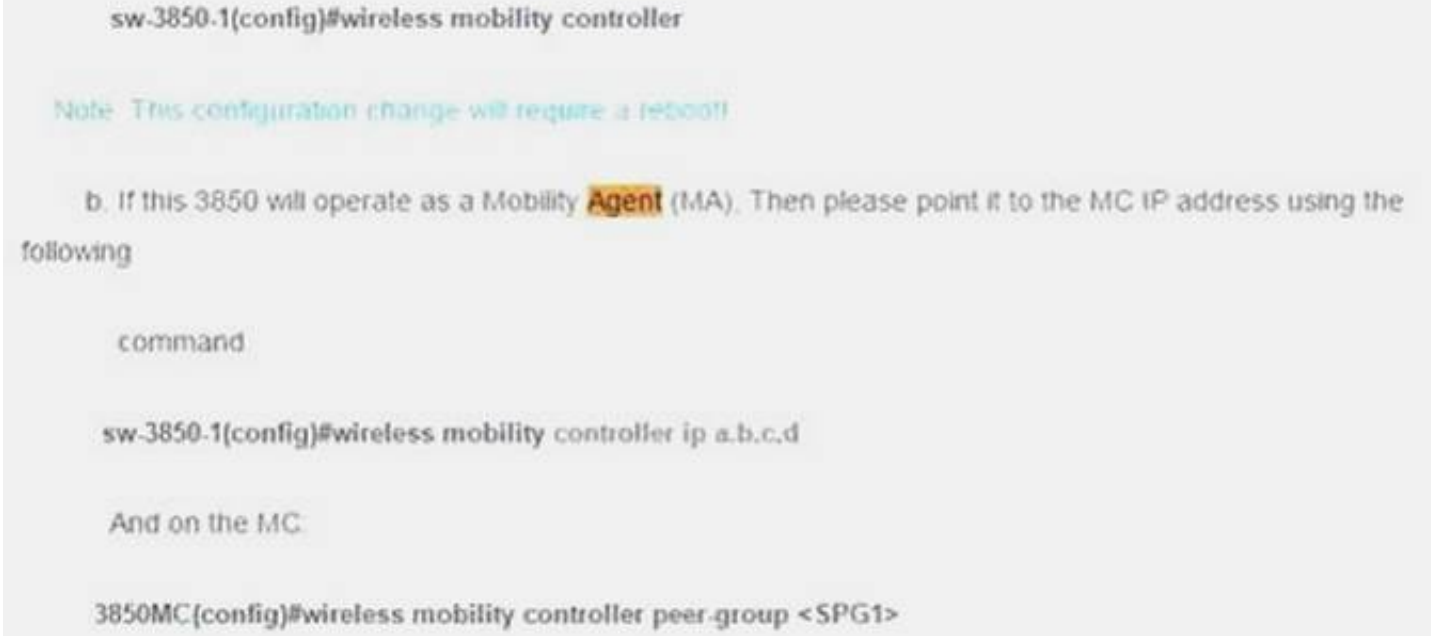
  3850MC(config)#wireless mobility controller peer-group <SPG1>

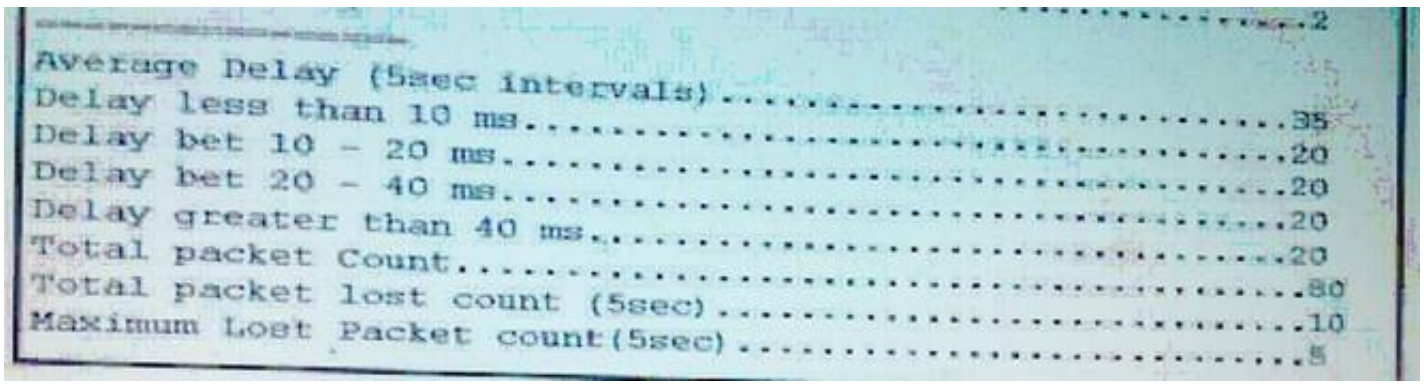
  3850MC(config)#wireless mobility controller peer-group <SPG1> member ip w.x.y.z

License Verification

https://supportforums.cisco.com/document/146996/getting-started-wlc-5760-and-3850

NEW QUESTION 59
Refer to the exhibit.





Which feature (and associated show output) is seen here?

A. Controller>show client tsm 802.11a 00:01:02:03:04:05 all
B. Controller>show client wmm 802.11a 00:01:02:03:04:05 all
C. Controller>show ap stats 802.11a00:01:02:03:04:05
D. Controller>show client detail 00:01:02:03:04:05

Answer: A

Explanation:

Step 4 See the TSM statistics for a particular client and the access point to which this client is associated by entering this command:
show client tsm {802.11a | 802.11b} *client_mac* {*ap_mac* | all}
The optional all command shows all access points to which this client has associated. Information similar to the following appears:

```
Client Interface Mac:                00:01:02:03:04:05
Measurement Duration:                90 seconds

Timestamp                            1st Jan 2006, 06:35:80
  UpLink Stats
  ---------------
     Average Delay (5sec intervals).....35
     Delay less than 10 ms.....20
     Delay bet 10 - 20 ms.....20
     Delay bet 20 - 40 ms.....20
     Delay greater than 40 ms.....20
    Total packet Count.....80
    Total packet lost count (5sec).....10
    Maximum Lost Packet count(5sec).....5
    Average Lost Packet count(5secs).....2
  DownLink Stats
  ================
     Average Delay (5sec intervals).....35
     Delay less than 10 ms.....20
     Delay bet 10 - 20 ms.....20
     Delay bet 20 - 40 ms.....20
     Delay greater than 40 ms.....20
    Total packet Count.....80
    Total packet lost count (5sec).....10
    Maximum Lost Packet count(5sec).....5
    Average Lost Packet count(5secs).....2
```

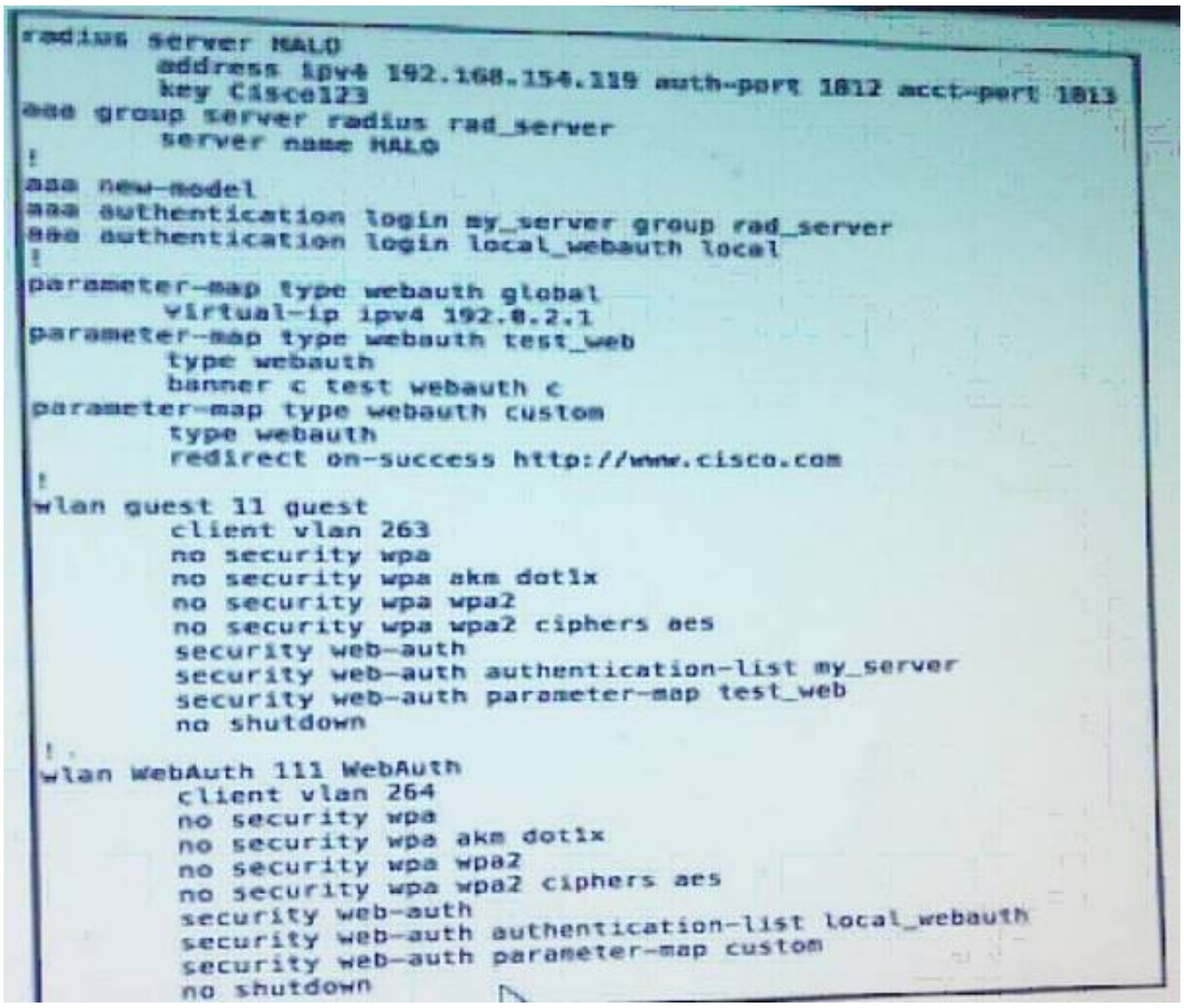
http://www.cisco.com/c/en/us/td/docs/wireless/controller/7- 4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010000.html

NEW QUESTION 61
You have configured VideoStream on a Cisco WLC and users are now viewing the company video broadcast over the wireless network. How can you verify you have VideoStream configured and working in the Cisco WLC GUI?

A. The Multicast Status shows "Normal Multicast" in the Multicast Group Details.
B. The Multicast Status shows "MediaStream Ongoing" in the Client detail page.
C. The Multicast Status shows "Multicast-direct Allowed" in the Multicast Group Details.
D. The Multicast Status shows "MediaStream Allowed" in the Multicast Group Detail

Answer: C

NEW QUESTION 66
Refer to the exhibit,



which is a configuration snippet of a Cisco 5760 controller running code IOS XE 3.6.3. Which statement about wlan 11 is true?

A. This configuration is for external WebAuth with an external RADIUS server.
B. This configuration is for WebAuth with local authentication.
C. This configuration is for custom WebAuth with local authentication.
D. This configuration is for WebAuth with an external RADIUS server.
E. This configuration is for custom WebAuth with an external RADIUS serve

Answer: D

Explanation:

WLAN Configuration Commands

Use the following commands to configure WLAN:

```
wlan webauth 11 local_webauth
 client vlan 263
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list ext_ise ------> calling auth method ext_ise which points to ise
 security web-auth parameter-map test_web
 no shutdown
```

http://www.cisco.com/c/en/us/td/docs/switches/lan/Denali_16-1/ConfigExamples_Technotes/Techzone_Articles/Example_and_Technotes_Denali_16_1_1/Example_and_Technotes_Denali_16_1_1_chapter_010010.html

NEW QUESTION 70
Which two statements about accessing the GUI and CLI of Cisco WLC are true? (Choose two.)

A. The feature "Management using Dynamic Interfaces" can be applied to one of the Dynamic Interfaces only.
B. Wireless management access is only possible through the default management WLAN "thazz"
C. The wireless clients can access the Cisco WLC only when the option " Enable Controller Management to be accessible from Wireless Clients" is checked.
D. The feature "Management using Dynamic Interfaces" can be configured in CLI onlyWireless management access is only possible through the default management WLAN - WLAN ID
E. Wired clients |can have only CLI access with the dynamic interface of the Cisco WLC, while wireless clients have both CLI and GUI access with the dynamic interface when the feature "Management using Dynamic Interfaces" is enabled.

Answer: AC

NEW QUESTION 74
In which direction does Application Visibility and Control mark the DSCP value of the original packet in the wireless LAN controller?

A. In both directions, upstream and downstream.
B. In one direction, downstream only.
C. In one configured direction, either upstream or downstream.
D. In one direction, upstream onl

Answer: A

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configurationguide/b_cg80/b_cg80_chapter_011001.htmlQUESTION NO:

NEW QUESTION 77
Which statement about network automation and/or network orchestration is true?

A. Automation focuses on coordinating multiple tasks at the same time.
B. Orchestration and automation focus on a single task at a time.
C. Orchestration focuses on coordinating multiple tasks at the same time.
D. Automation and orchestration focus on coordinating multiple tasks at the same tim

Answer: C

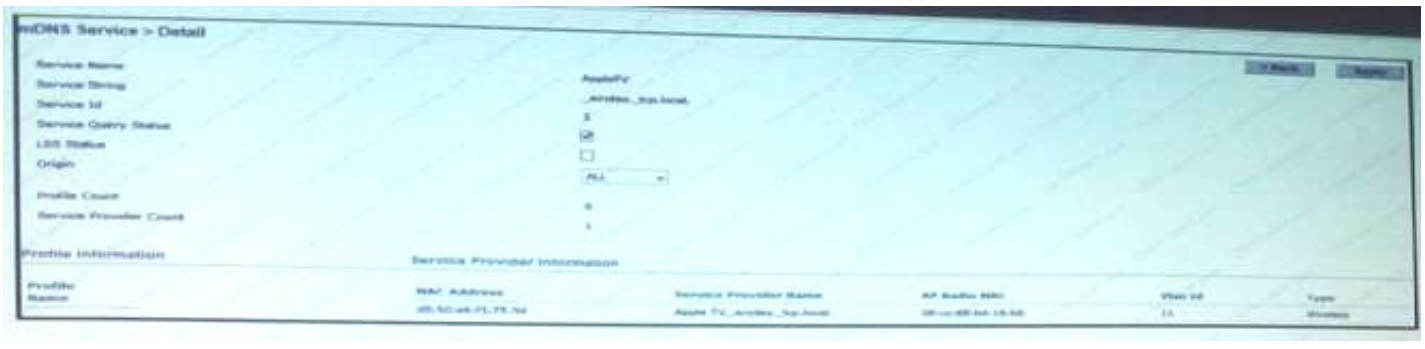
NEW QUESTION 79
Which three statements about the high availability configuration on the Cisco 5760 WLCs are true? (Choose three.)

A. Cisco WLC with more reboots is elected as active when the default stack priority is in use.
B. EtherChannel bundles all ports on both active and standby Cisco WLC on a logical port.
C. Cisco 5760 WLC uses a dedicated high availability port for high availability and configuration synchronization.
D. High availability switchover is triggered when one of the ports on the active Cisco WLC EtherChannel bundle fails.
E. Active Cisco WLCs in a pair can be identified using LED state without issuing any command on the Cisco WLC console.
F. Cisco WLC with the highest priority in a stack are elected as the active Cisco WLC during the election process.
G. All configuration including certificates are automatically synced between active and standby Cisco WLC.

Answer: BEF

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/technology/5760_deploy/CT5760_Controller_Depl oyment_Guide/High_Availability.html

NEW QUESTION 84
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 i

Answer: C

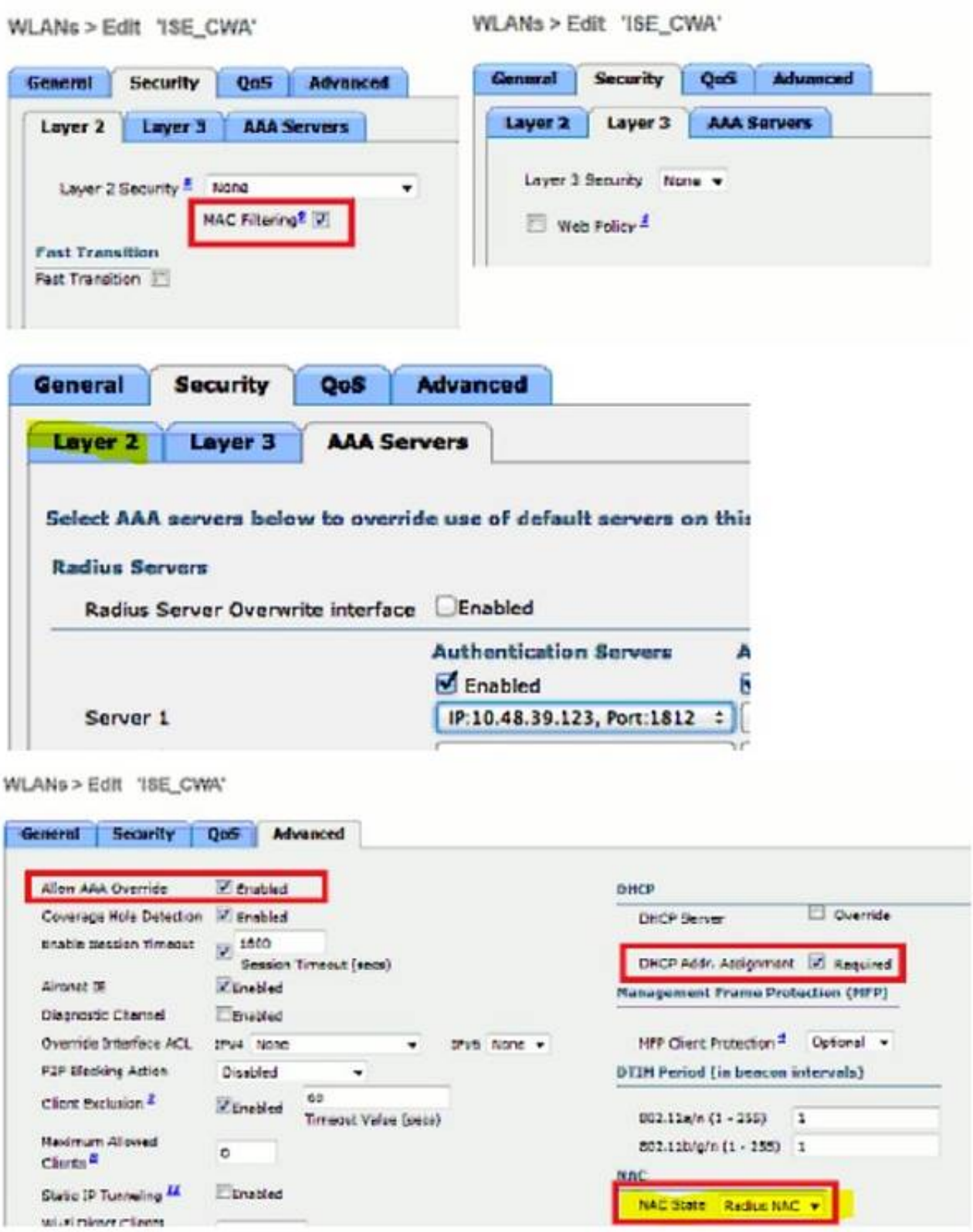
Explanation: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/ BYOD_Design_Guide/BYOD_Bonjour.html

NEW QUESTION 85
While troubleshooting a failed central web authentication configuration on Cisco WLC, you discover that the Cisco WLC Policy Manager State is showing RUN for new clients and not CENTRAL_WEB_AUTH. Which of the below is most likely causing this issue?

A. The WLAN NAC state should be set to RADIUIS NAC.
B. The WLAN Layer 2 security should be set to WPA+WPA2.
C. The WLAN Layer 3 security should be set to Web Policy with Conditional Web Redirect.
D. The Web Login Page under the Cisco WLC security settings should be set to External(Redirect to external server).

Answer: A

Explanation:



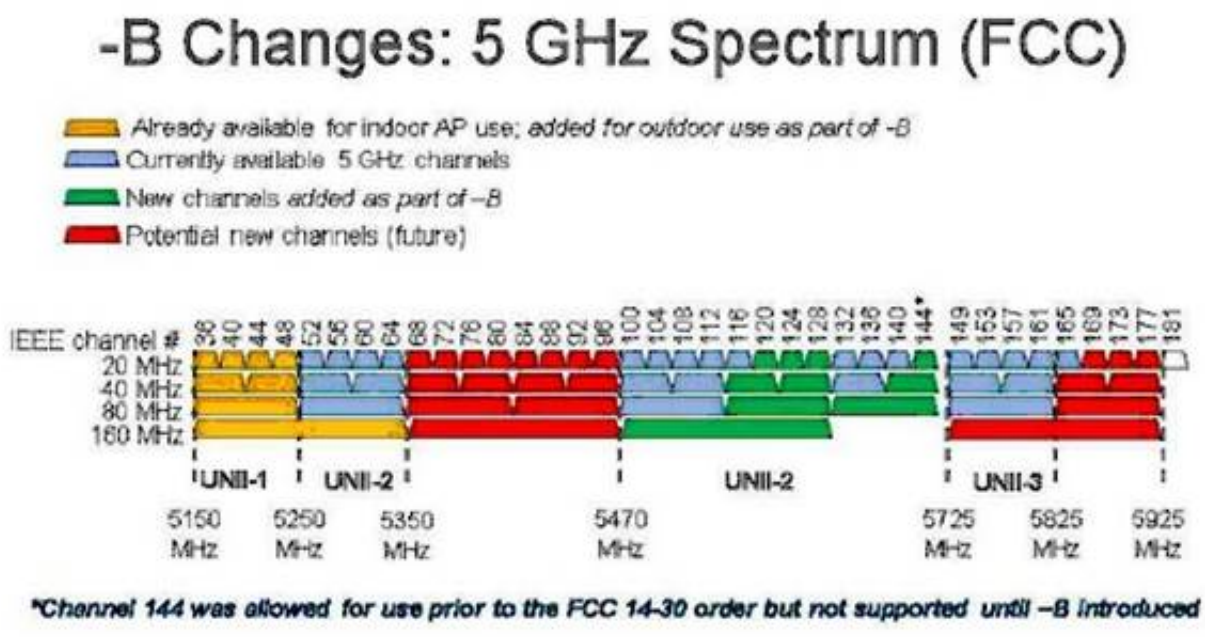
http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-webauth- 00.html
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69340-web-authconfig. html

NEW QUESTION 86
DRAG DROP
Drag and drop the channel lists on the left onto the corresponding UNII bands on the right, as applicable in the new-B Regulatory Domain for US. Not allow options are used.

Channels:32.36,40,44	UNII-1
Channels:36,40.44,48	UNII-2
Channels:52,56,60,64	UNII-2 extended
Channels:100,104,108,112,116,120,124,128,132,136 140,144	UNII-3
Channels:100,104,108,112,116,132,136,140,144,148	
Channels:148,152,156,160	
Channels:149.153,157,161,165	
Channels:56,60,64,68	

Answer:

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-3/b_cisco_aironet_series_2800_3800_access_point_deployment_guide/b_cisco_aironet_series_2800_3800_access_point_deployment_guide_chapter_01011.pdf



NEW QUESTION 88
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 controlle

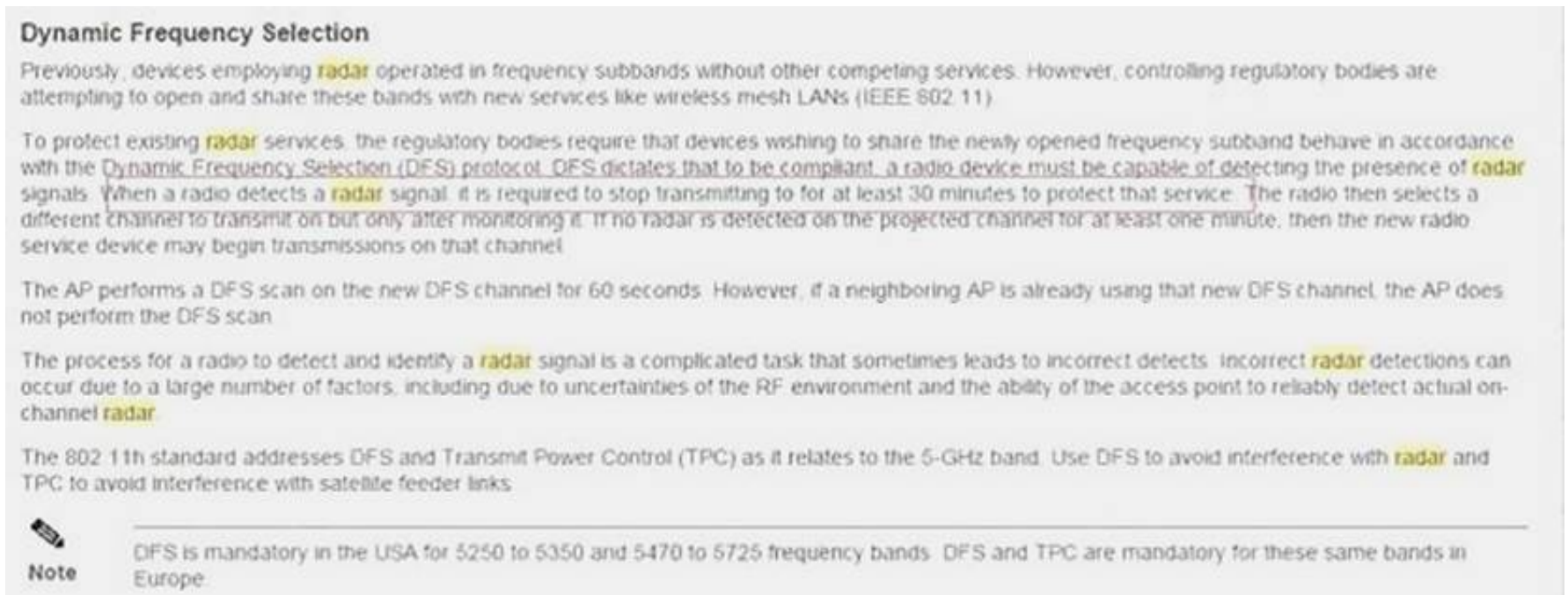
Answer: AD

NEW QUESTION 90
Which statement about a Cisco Mesh Network when a radar event is detected by the MAP on a mesh tree when coordinated channel change is enabled Is true?

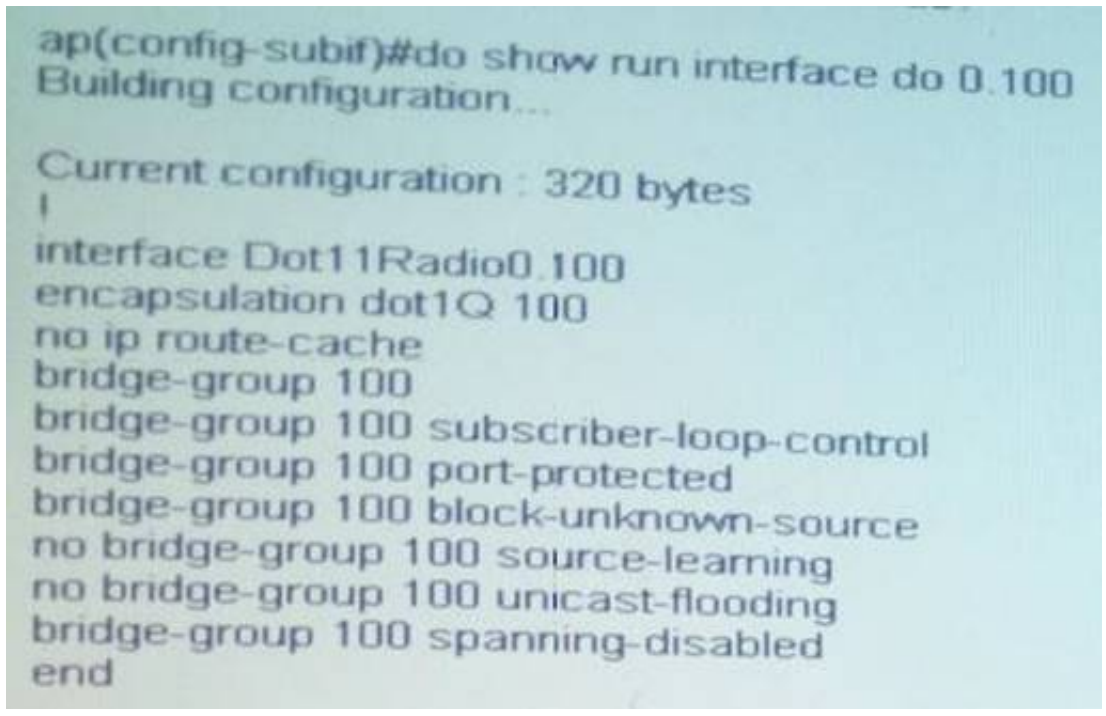
A. The MAP immediately stops transmission of the current channel and joins the parent again after 30 minutes after the channel is marked as clean.
B. The MAP continues transmission of the beacons and probes for 10 seconds after the radar detection and suspends operation for the next 30 mins.
C. The MAP propagates radar event information to the RAP in the same BG
D. Searchs for a different parent working on a nono-dfs channel and join there.
E. The MAP propagates the radar event information to the RAP and the whole sector moves to the new channel.

Answer: B

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-3/b_mesh_83/Troubleshooting.html



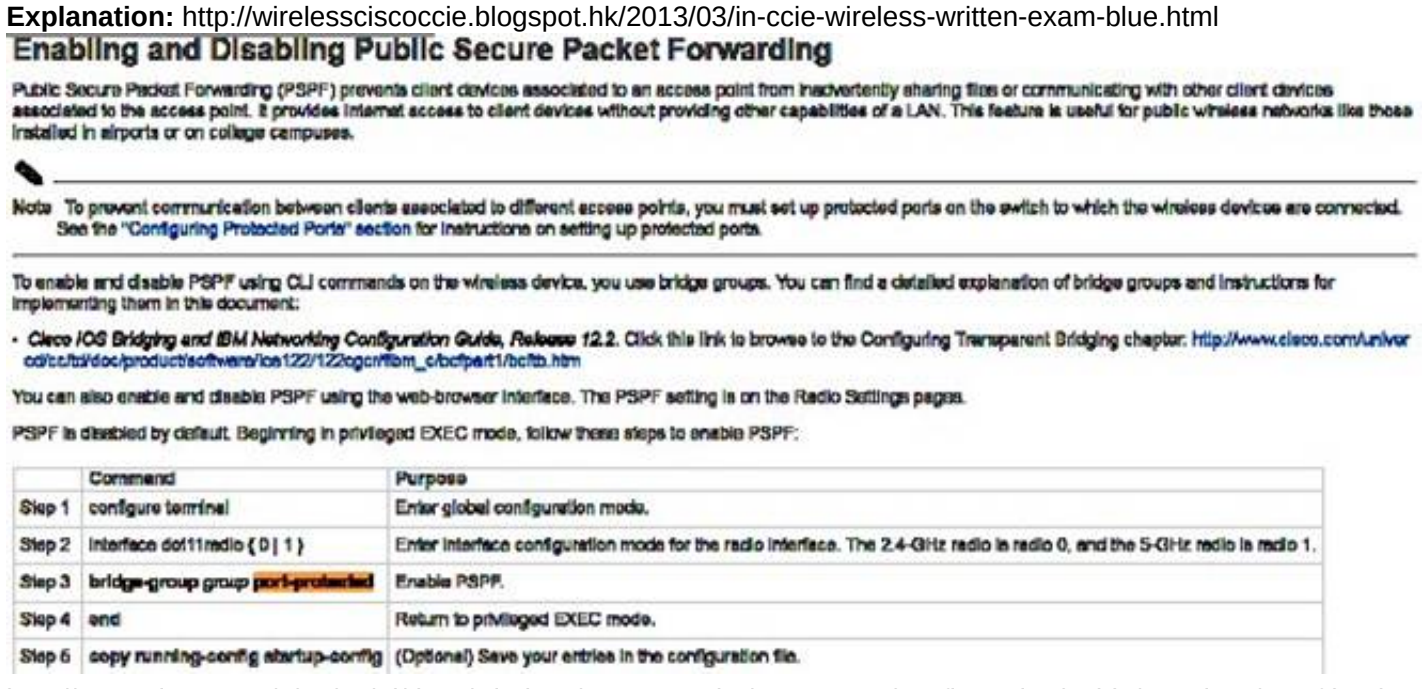
NEW QUESTION 91
Two wireless IP phones are never able to call each other when connected to the same autonomous AP. However, they can place calls to other wireless IP phones that are connected to other APs or to wired IP phones. The wireless phones are operating on VLAN 100. Based on this output, which statement about the problem is true?



A. P2P blocking is enabled via the bridge-group 100 block-unknow-source command.
B. P2P blocking is enabled via the no bridge-group 100 unicast-floodin
C. command.
D. P2P blocking is enabled via the bridge-group 100 port-protecte
E. command.
F. P2P blocking is enabled via the no bridge-group 100 source-learning command.
G. P2P blocking is enabled via the bridge-group 100 subscriber-loop-control comman

Answer: C

Explanation: http://wirelessciscoccie.blogspot.hk/2013/03/in-ccie-wireless-written-exam-blue.html



http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-3_8_JA/configuration/guide/1238jasc/s38rf.html

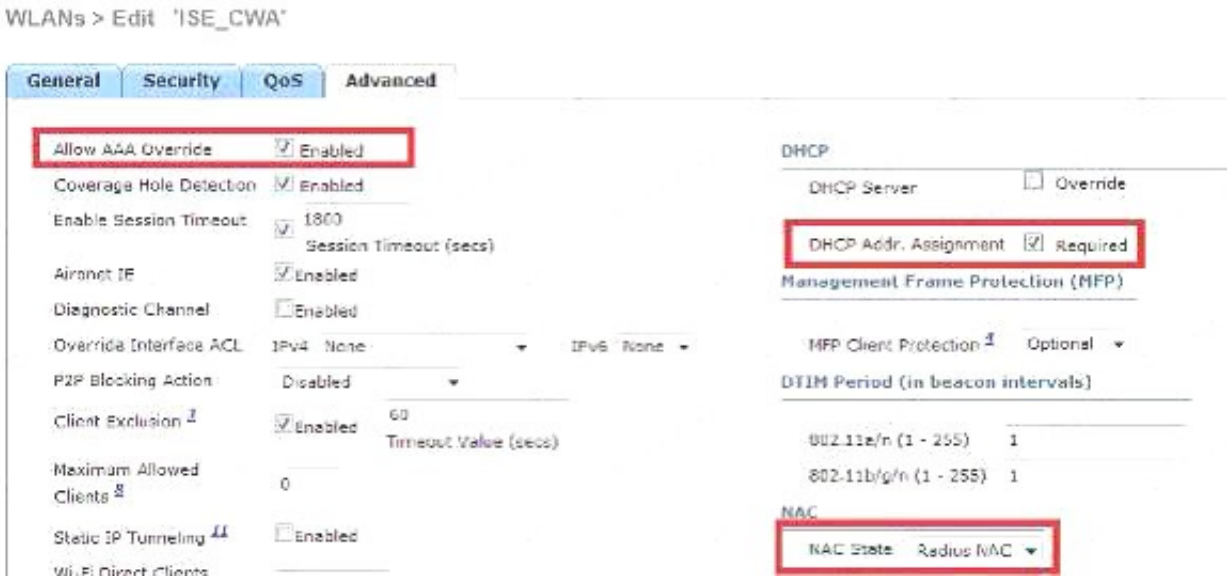
NEW QUESTION 94

Which two advanced WLAN options are required when deploying central web authentication with Cisco ISE? (Choose two.)

A. P2P Blocking Action set to Drop.
B. NAC State RADIUS NAC
C. NAC State SNMPNAC.
D. DHCP Add
E. Assignment disabled.
F. Allow AAA override enable

Answer: BE

Explanation: From



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

NEW QUESTION 95

Refer to the exhibit. You have been asked to troubleshoot why VTP is not distributing new VLANs to a VTP client switch. Which option is the most likely root cause of this VTP problem.

A. The VTP password is not set to level 15 on the client switch.
B. The VTP password encryption level is not set on the client switch.
C. The VTP encryption level does not match on the client switch.
D. The VTP password is incorrect on the client switch.
E. The client switch is set to transparent mod
F. Which ignores VLAN configuration updates from VTP servers.

Answer: D

Explanation: From:
Each sw, and issue the command:
No vtp password

Enable debugging of VTP events to find the exact issue. Notice the message "MD5 digest failing".

```
SW3#debug sw-vlan vtp events

SW3#
00:20:00: VTP LOG RUNTIME: Summary packet received, domain = packet6.c

00:20:00: VTP LOG RUNTIME: Validate TLVs : #tlvs 1, max blk size 4
00:20:00: VTP LOG RUNTIME: Validate TLVs : #00, val 6, len 4
00:20:00: VTP LOG RUNTIME: Summary packet rev 1 greater than domain pa

00:20:00: VTP LOG RUNTIME: Domain packet6.com currently not in updatin

00:20:00: VTP LOG RUNTIME: pdu len 80, #tlvs 1

00:20:00: VTP LOG RUNTIME: Subset packet received, domain = packet6.co

00:20:00: VTP LOG RUNTIME: MD5 digest failing
calculated = 34 15 83 F3 BC 0E B3 E6 F7 E2 E9 DD 5D 0C 9D 95
transmitted = 08 7A 2F C0 1E 76 81 E4 06 90 23 67 94 19 07 9F
```

Let's configure the password on SW3.

```
SW3#conf t
SW3(config)#vtp password cisco
SW3(config)#end
```

https://www.packet6.com/configuring-vtp-on-cisco-switches/ http://www.sunpenguin.net/?p=283

NEW QUESTION 99
Which of the below characteristics of RPL is true?

A. RPL is designed 1)or lossy networks.
B. RPL is an IPv6 link-state routing protocol.
C. RPL can send only messages in secured mode.
D. RPL uses hello messages to send routing updates to its neighbor

Answer: A

Explanation: From:
http://www.openmote.com/standards/ietf-rpl.html
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/rpl/configuration/15-mt/rpl-15-mt-book.html https://datatracker.ietf.org/doc/rfc6550/?include_text=1

NEW QUESTION 100
You have been hired to install new Cisco switches at ACME Corporation. The company has an existing Cisco network comprised of access layer switches that use multiple VLANs and VLAN trunking protocol to distribute the VLANs to the switches throughout the network. Which two methods are best to accomplish your task? (Choose two.)

A. Configure the VLAN Trunking Protocol pruning on the new switches because they may not need all of the VLANs.
B. Prior to installation, ensure that all switches are running the same Cisco IOS software version as the VTP server.
C. Ensure that all the new Cisco switches have their VTP domain name set to the default value of null
D. Configure one of the new switches as a VTP server to distribute the VLANs appropriately.
E. Ensure that all switches have the same VLAN Trunking Protocol password and encryption level.
F. Configure all new switches as VTP clients and relocated switches as VTP server because the already have all the VLANs in their database.
G. Ensure that all switches are running the same VTP versio

Answer: EG

Explanation: From:

VTP Configuration Guidelines and Restrictions

Follow these guidelines and restrictions when implementing VTP in your network:

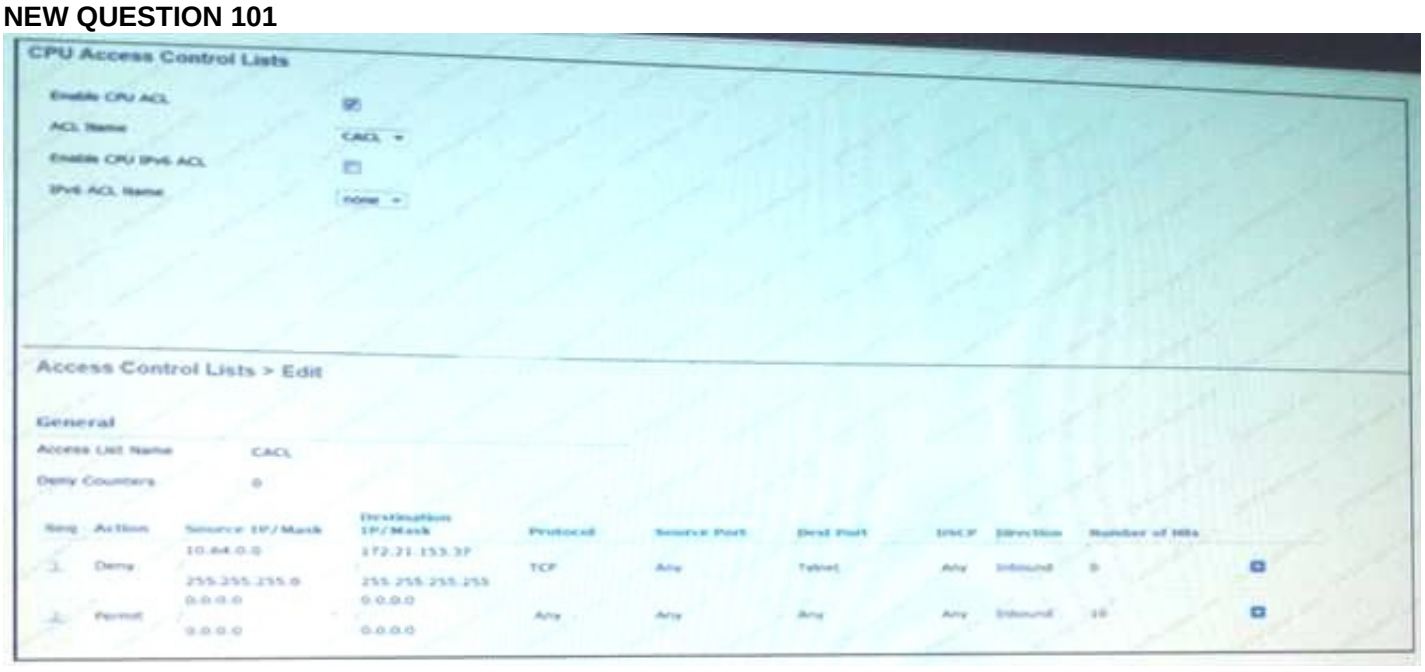
- All network devices in a VTP domain must run the same VTP version.
- You must configure a password on each network device in the management domain when VTP is in secure mode.

⚠

Caution If you configure VTP in secure mode, the management domain will not function properly if you do not assign a management domain password to each network device in the domain.

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vtp.html#wp1034490

NEW QUESTION 101

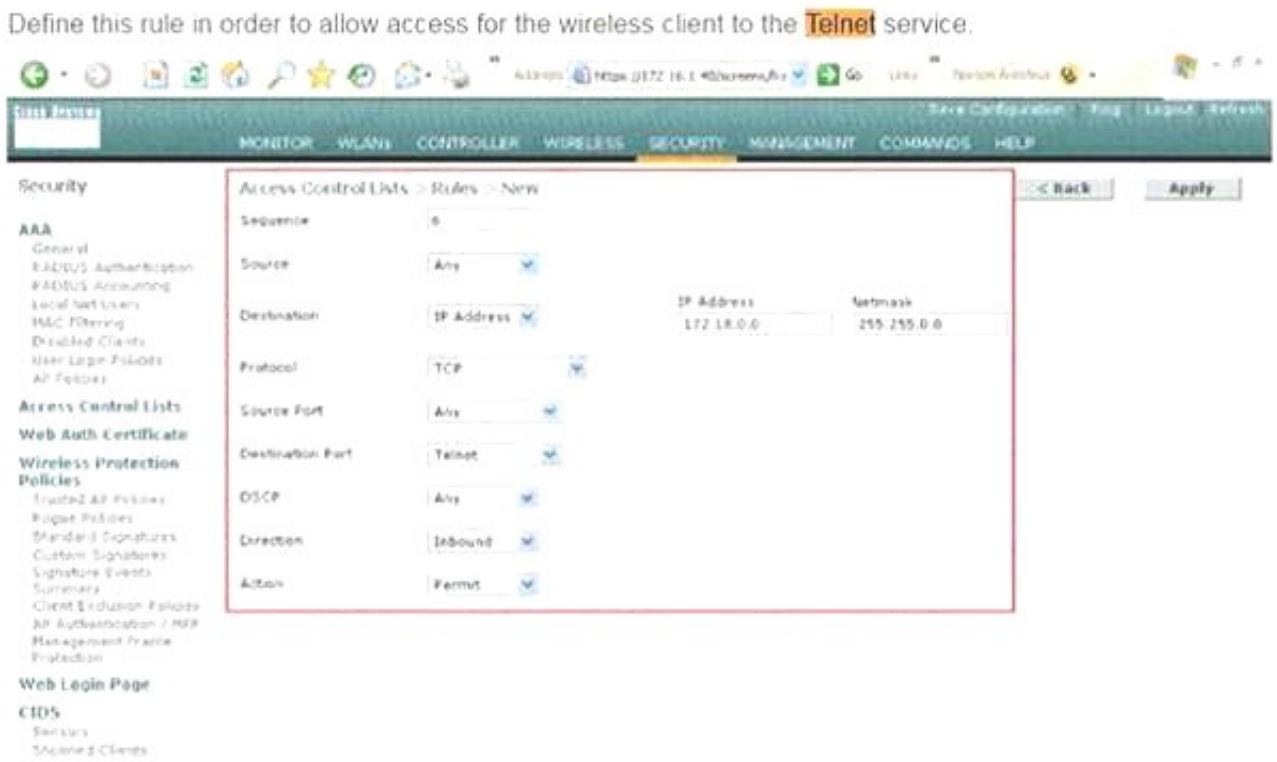


Refer to the exhibit. Which statement about this CPU ACL is correct?

A. This CPU ACL is used as a redirection aCLto redirect all traffic except Telnet to 172.21.153.37.
B. A user on the 10.64.0.0/24 network can use Telnet to access the WLC IP address on 172.21.153.37.
C. A user on the 10.64.0.0/24 network cannot use Telnet to access the WLC IP address on 172.21.153.37.
D. A user on the 10.64.0.0/24 network cannot use HTTPS to 172.21.153.37.
E. No subnets other than 10.64.0.0/24 can manage the WL

Answer: C

Explanation: From:
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71978-acl-wlc.html

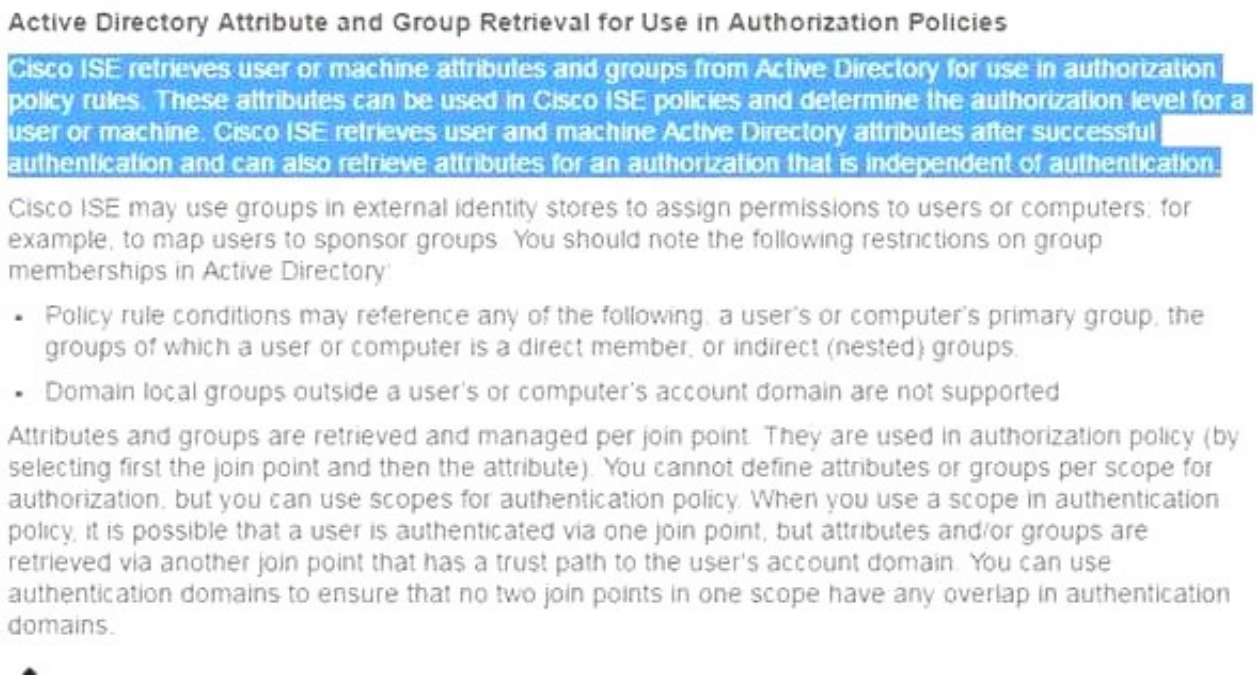


NEW QUESTION 102
Which option in the Cisco Identity Services Engine checks that the user authentication comes from a domain computer?

A. It is not possible to validate the computer domain membership through ISE.
B. Machine Access Restriction
C. Machine Access Restriction
D. Active Directory Attributes.
E. An identity source sequence can be used to perform this chec

Answer: C

Explanation: From:


Active Directory Attribute and Group Retrieval for Use in Authorization Policies

Cisco ISE retrieves user or machine attributes and groups from Active Directory for use in authorization policy rules. These attributes can be used in Cisco ISE policies and determine the authorization level for a user or machine. Cisco ISE retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

Cisco ISE may use groups in external identity stores to assign permissions to users or computers; for example, to map users to sponsor groups. You should note the following restrictions on group memberships in Active Directory:

- Policy rule conditions may reference any of the following: a user's or computer's primary group, the groups of which a user or computer is a direct member, or indirect (nested) groups.
- Domain local groups outside a user's or computer's account domain are not supported

Attributes and groups are retrieved and managed per join point. They are used in authorization policy (by selecting first the join point and then the attribute). You cannot define attributes or groups per scope for authorization, but you can use scopes for authentication policy. When you use a scope in authentication policy, it is possible that a user is authenticated via one join point, but attributes and/or groups are retrieved via another join point that has a trust path to the user's account domain. You can use authentication domains to ensure that no two join points in one scope have any overlap in authentication domains.

http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/ISE-ADIntegrationDoc/b_ISEADIntegration. html

NEW QUESTION 107
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 standar

Answer: CD

Explanation: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dgbook/ vowlan_ch2.html
http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troub leshoot/5_Troubleshooting_CAC_Rev1-2.html#wp1053384

NEW QUESTION 109
FlexConnect APs have already been deployed in a branch office for local switching. Currently the WLAN in the large auditorium is proposed to change to a high-density design and thus some low data rates are proposed to be disabled while keeping the data rates in other areas under the same Cisco WLC. Which two configuration settings must be modified in the Cisco WLC to achieve this configuration? (Choose two.)

A. RF Profiles
B. Mobility Groups
C. FlexConnect Groups
D. AP Groups
E. Fape profil

Answer: AD

Explanation: From:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/7- 4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010001111.html

NEW QUESTION 111
You are setting up a Cisco access point in repeater mode with a non-Cisco access point as the parent and you use this interface configuration on your Cisco access point.

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid myWIFInetwork
 !
 station-role repeater
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
```

You are getting the following error message. Which reason for this issue is true?

A. %D0Tll-4-CANT_A$S0C:lnterface DotllRadioO, cannot associate:No Aironet Extension IE.
B. "dotll extension aironet" is missing under the interface DotllRadio 0 interface When repeater mode is used, unicast-flooding must be enabled to allow Aironet IE

communications.
C. The parent AP MAC address has not been defined.
D. Repeater mode only works between Cisco access point

Answer: A

Explanation: From:

This example shows how to set up a repeater acess point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-2_11_JA/configuration/guide/b12211sc/s11rep.html

NEW QUESTION 115
When a Flex Connect AP is in the "local authentication, local switching" state, it handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode. Which three statements about a FlexConnect AP are true? (Choose three).

A. In connected mode, the AP provides minimal information about the locally authenticated client to the controlle
B. This information is not available on the controller policy typ
C. Access VLA
D. VLAN name, supported rate
E. Encryption ciphter.
F. In connected mode, the access point provides minimal information about the locally authenticated client to the controlle
G. However, this information is available to the controller policy type., access VLAN, VLAN name, supported rates, encryption cipher.
H. Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit no smaller than 576 bytes.
I. Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 150 ms and the maximum transmission unit no higher than 500 bytes.
J. Local authentication in connected mode does not require any WLAN configuration.
K. Local authentication can be enabled only on the WLAN of a FlexConnect AP that is in local switching mode.

Answer: ACF

Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7- 2/configuration/guide/cg/cg_filexconnect.html

NEW QUESTION 117
Heartbeats are used to maintain the high-availability status of an application. Which factor is most important?

A. Bandwidth
B. Latency
C. Routing
D. Round-trip time

Answer: D

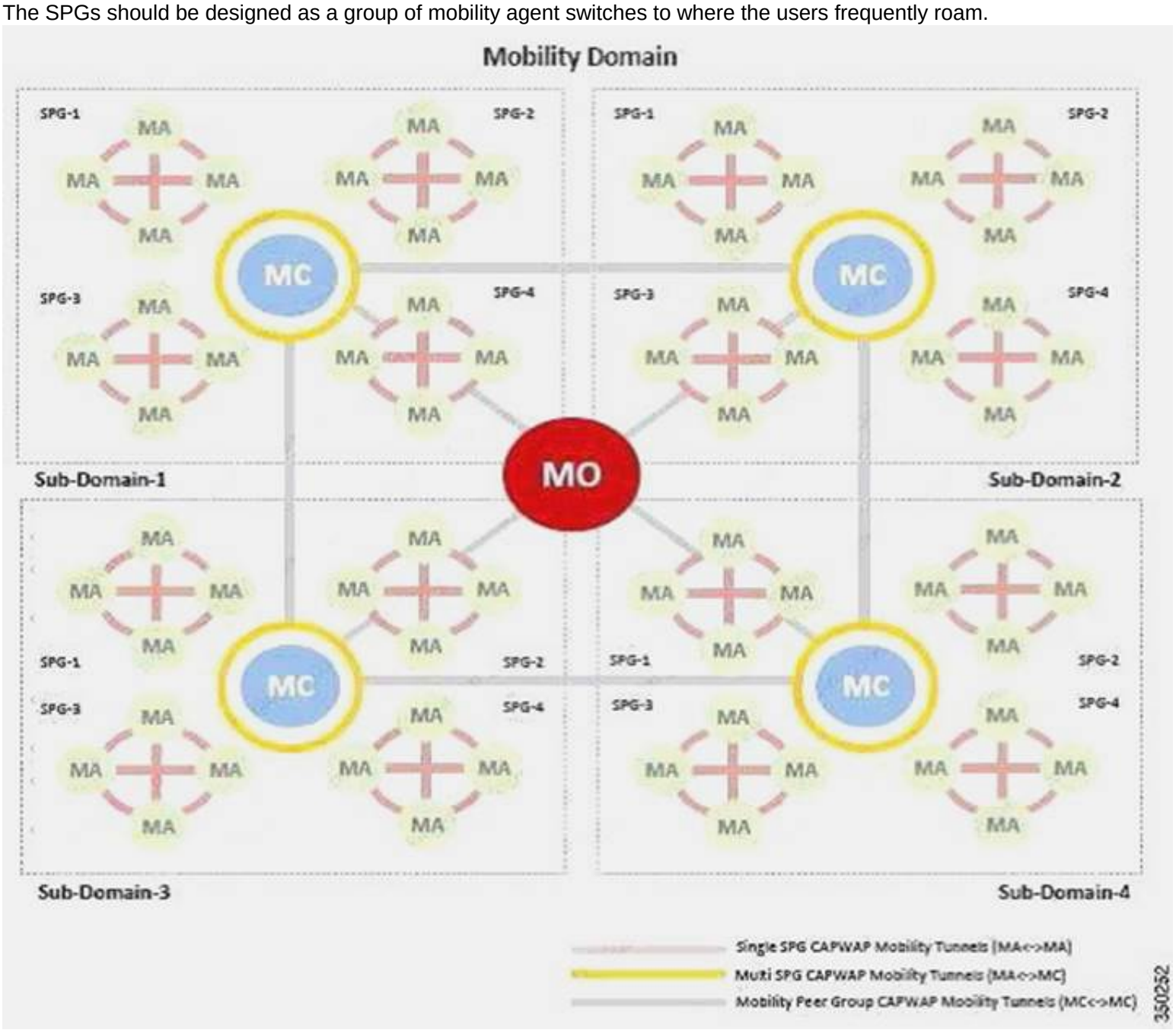
Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_011 11101.html
https://books.google.com.hk/books?id=YLHvHGGx5AEC&pg=PT66&lpg=PT66&dq=wlc+heatbeat+round+trip+time&source=bl&ots=ClFsWOm0RH&sig=5NO_zaiDBOmHlDzXfLiLgrkgpP0&hl=zh-TW&sa=X&ved=0ahUKEwjb0M31vdLPAhUT9mMKHRJkDv4Q6AEIWDAH#v=onepage&q=wlc%20heat beat%20round%20trip%20time&f=false
Cisco Prime Infrastructure 3.1.3 Administrator Guide - Configuring High Availability [Cisco Prime Infrastructure] - Cisco
http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-1- 3/administrator/guide/PIAdminBook/config_HA.html
Health Monitor (HM) detects failure conditions using the heartbeat messages that the two servers exchange. If the primary server is not responsive to three consecutive heartbeat messages from the secondary, it is considered to have failed. During the health check. HM also checks the application process status and database health; if there is no proper response to these checks, these are also treated as having failed.
The HA system takes approximately 10 to 15 seconds to detect a process failure on the primary server and initiate a failover. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.
High Availability FAQ –Cisco. http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1130-ag-series/qa_c67- 714540.html
Q. What are the recommendations for the network between the primary and secondary controllers connected via RP over Layer 2 VLAN/fiber to achieve client SSO?
A. The Layer 2 network
for RP connectivity needs to follow these recommendations to ensure appropriate performance in case of a switchover:
• Round-trip time (RTT) latency on the redundancy link: 80 ms or less for the default keep-alive timeout or 80 percent of the configured keep-alive timeout
• Preferred maximum transmission unit (MTU) on the redundancy link: 1500 or above
• Bandwidth on the redundancy link: 60 Mbps or more

NEW QUESTION 122
In a converged access deployment, which two statements about mobility agents are true? (Choose two.)

A. It maintains a client database of locally served clients.
B. It manages mobility-related configuration.
C. It handles RF functions.
D. It is the first level in the converged access hierarchy.
E. It is a mandatory element in the converged access desig

Answer: AD

Explanation: From:
CT5760 Controller Deployment Guide - Mobility Architecture [Cisco 5700 Series Wireless LAN Controllers] – Cisco
http://www.cisco.com/c/en/us/td/docs/wireless/technology/5760_deploy/CT5760_Controller_Depl oyment_Guide/Mobility_Architecture.html
Mobility Agent
A mobility agent manages AP connectivity, CAPWAP tunnel terminations from APs and builds a database of client stations (endpoints) that are served locally as well as roamed from an Anchor WLC. Mobility agent can be either a Catalyst 3850 or a CT5760 mobility controller with an internal mobility agent running on it.
Mobility Controller:
A mobility controller provides mobility management tasks including inter-SPG roaming, RRM, and guest access. Mobility roaming, where a wireless client moves from one physical location to another without losing connectivity and services at any time, can be managed by a single mobility controller if roaming is limited to a mobility sub-domain. Roaming beyond a mobility sub-domain can be managed by multiple mobility controllers in a mobility group. The mobility controller is responsible for caching the Pairwise Master Key (PMK) of all clients on all the mobility controllers, enabling fast
roaming of the clients within its sub-domain and mobility group. All the mobility agents in the subdomain form CAPVVAP mobility tunnels to the mobility controller and report local and roamed client
states to the mobility controller. The mobility controller builds a database of client stations across all the mobility agents.
Mobility Oracle
Mobility oracle further enhances mobility scalability and performance by coordinating roaming activities among multiple mobility groups, which removes the need for N2 communications between mobility controllers in different mobility groups to improve efficiency and performance.
Mobility Sub-domain
Multiple SPGs can be grouped together and collectively managed as a mobility sub-domain. One mobility controller is required for each mobility sub-domain.
Switch Peer Group
The Converged Access deployment defines an SPG as a logical group of mobility agents within one mobility controller (or mobility sub-domain). The main advantage of configuring SPGs is to constrain the roaming traffic to switches that form the SPG. When the mobility agents are configured in one SPG on the mobility controller, the software automatically forms full mesh CAPWAP tunnels between the mobility agent switches. These CAPWAP tunnels can be formed in a multi-layer network design (where the mobility agent switches are L2 adjacent on a VLAN spanned across) or a routed access design (where the mobility agent switches are L3 adjacent).
The SPGs should be designed as a group of mobility agent switches to where the users frequently roam.



NEW QUESTION 124
Which statement about 802.11h is true?

A. DFS feature works irrespective of whether the channel setting on WLC is set to auto or manual.
B. 802.llh is not a mandatory standard under FCC regulations.

C. The FCC does not require 802.llh to be supported in the 5 GHz band.
D. When the radio detects a radar, it can use the channel for only 20 minutes at a tim

Answer: A

Explanation: From:
EEE
802 .llh-2003-Wikipedia, the free encyclopedia https://en.wikipedia.org/wiki/IEEE_802.11h-2003
The standard provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a PHY. It has been integrated into the full IEEE 802.11-2007 standard.
FCC Regulations Update –Cisco http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1300-series/prod_white_paper0900aecd801c4a88.html https://supportforums.cisco.com/document/52376/tpc-and-dfs-overview

NEW QUESTION 126
Which option is a feature of a Cisco Autonormous AP that prevents over-the-air direct P2P communication, which forces all traffic to hit the first-hop router where security policy is enforced?

A. Wi-Fi Direct Client Policy
B. P2P Secure Packet Public
C. Secure Packet Forwarding
D. P2P Blocking Action

Answer: C

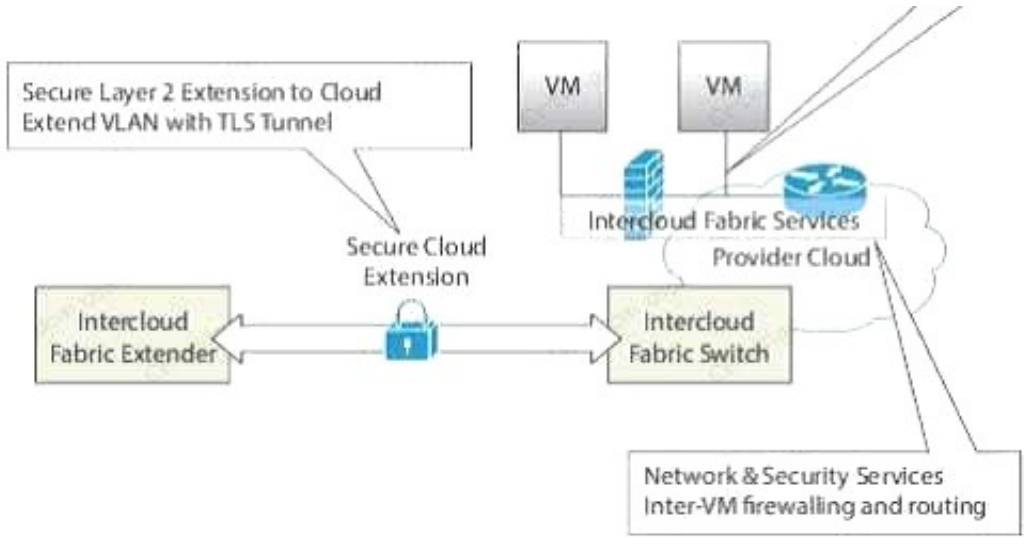
Explanation: http://docwiki.cisco.com/wiki/Wireless_Technologies Cisco Aironet Access Points
http://www.cisco.com/web/techdoc/wireless/access_points/online_help/eag/123- 02.JA/1400BR/h_ap_network-if_802-11_c.html
Public Secure Packet Forwarding
Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN.
No exchange of unicast, broadcast, or multicast traffic occurs between protected ports. Choose Enable so that the protected port can be used for secure mode configuration.
PSPF must be set per VLAN.
Note: To prevent communication between clients associated to different access points on your wireless LAN, you must set up protected ports on the switch to which your access points are connected.
Wi-Fi Direct Client Policy | Security and Network Management J Cisco Support Community https://supportforums.cisco.com/discussion/11851216/wi-fi-direct-client-policy Information About the Wi-Fi Direct Client Policy
Devices that are Wi-Fi Direct capable can connect directly to each other quickly and conveniently to do tasks such as printing, synchronization, and sharing of data. Wi-Fi Direct devices may associate
with multiple peer-to-peer (P2P) devices and with infrastructure wireless LANs (WLANs) concurrently. You can use the controller to configure the Wi-Fi Direct Client Policy, on a per WLAN basis, where you can allow or disallow association of Wi-Fi devices with infrastructure WLANs, or disable Wi-Fi Direct Client Policy altogether for WLANs. http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_010 00011.html

NEW QUESTION 127
Which option describes the function of the Intercloud Fabric Extender?

A. It provides the network overlay functionality between the used clouds or cloud models.
B. It establishes a secure site-to-site tunnel to the intercloud fabric agent in the private cloud.
C. It applies network policies and collects and reports VEM-related intercloud statistics.
D. It establishes a secure site-to-site tunnel to the intercloud fabric switch in the provider clou

Answer: D

Explanation: From:



Intercloud Fabric Extender

The Intercloud Fabric Extender is a virtual machine that runs in the private cloud. It is responsible for establishing a secure tunnel for interconnecting the Intercloud Fabric components in the private cloud with the provider cloud. The main functions of the Intercloud Fabric Extender are as follows:

- Establishes a secure tunnel to interconnect all of the cloud resources.
- Interacts with the virtual switch, such as the Cisco Nexus 1000V, at the private cloud.

Cisco Intercloud Fabric Agent

The Cisco Intercloud Fabric Agent (ICA) provides a network overlay for the VMs in the cloud. It secures the guest VM traffic in the cloud and abstracts the cloud infrastructure. It is deployed in the provider cloud as a secure tunnel driver that runs within the cloud VM's operating system. It also redirects network traffic to the secure overlay network as follows:

- Establishes a secure tunnel to connect to an Intercloud Fabric Switch that allows VMs in the cloud to communicate with private cloud VMs and provider cloud VMs.
- Collects secure overlay-related statistics.

Intercloud Fabric Switch

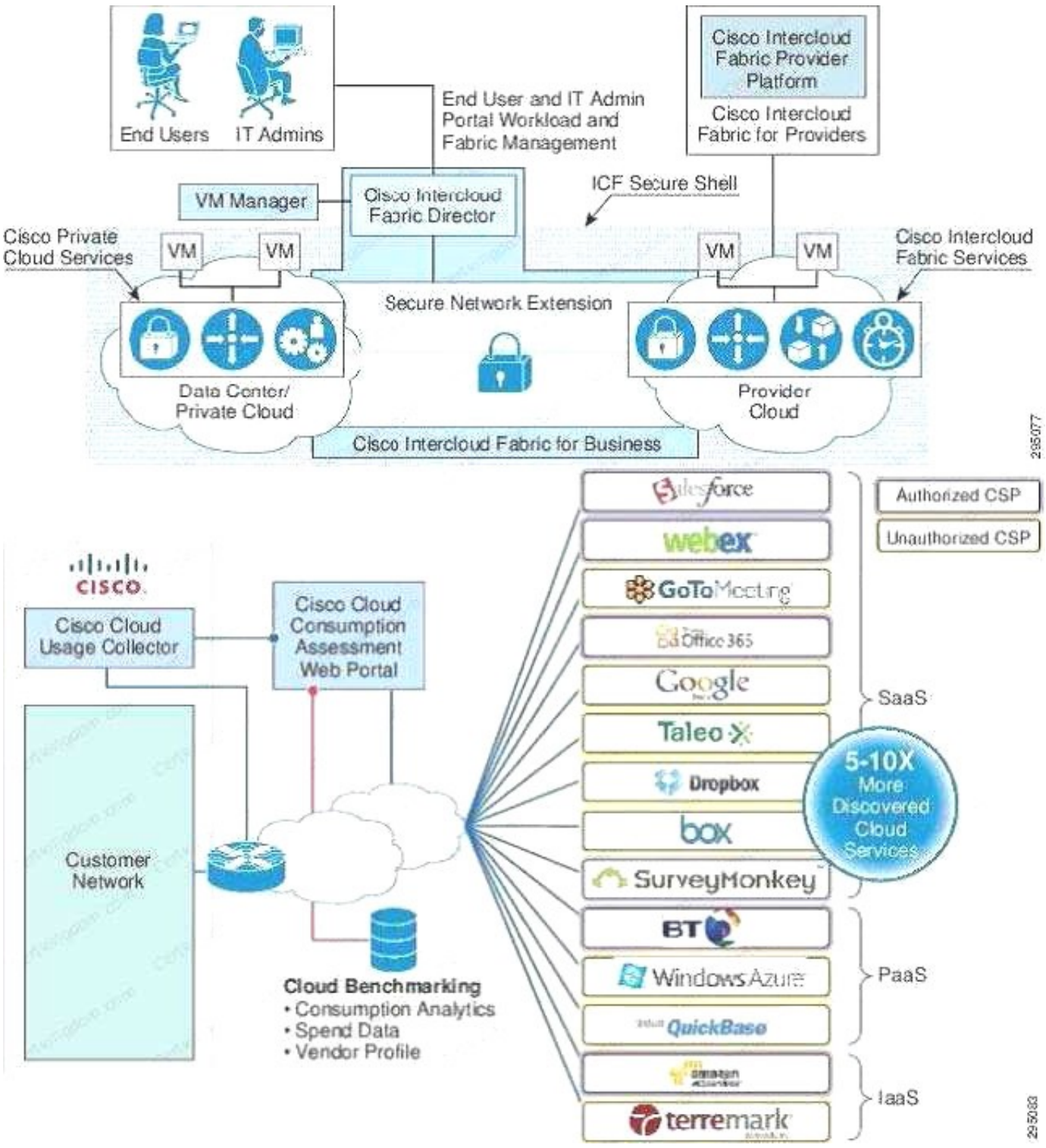
The Intercloud Fabric Switch is a virtual machine that runs in the provider cloud. It is responsible for establishing secure tunnels for connecting VMs in the provider cloud to the private cloud VMs and other VMs in the cloud. The main functions of the Intercloud Fabric Switch are as follows:

- Runs the Virtual Ethernet Module (VEM) to provide the Cisco Nexus 1000V functions.
- Establishes a secure tunnel to connect the VEM with Intercloud Fabric Extender.
- Establishes secure tunnels to connect all of the cloud VMs.
- Monitors and reports statistics of VMs in the cloud.
- Monitors and reports any component failures in the cloud to Cisco Prime Network Services Controller (PNSC).

The VEM is embedded in the Intercloud Fabric Switch and is responsible for the following:

- Communicates with the Virtual Supervisor Module (VSM) function that runs at the private cloud for retrieving VM-specific network policies such as port profiles.
- Switches the network traffic between cloud VMs.
- Switches the network traffic between cloud VMs and the private cloud.
- Applies network policies to any switching network traffic.
- Collects and reports VEM-related statistics.

http://www.cisco.com/c/en/us/td/docs/cloud-systems-management/cisco-intercloud-fabric/ciscointercloud- fabric-for-business/2-3-1/getting-startedguide/b_Cisco_Intercloud_Fabric_Getting_Started_Guide_Release_2_3_1/b_Cisco_Intercloud_Fabric_Getting_Started_Guide_Release_2_3_1_chapter_00.pdf Cisco Inter cloud Fabric Architectural Overview - Cisco
http://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Interc loud_Fabric_2.html
Cisco Intercloud Fabric Secure Extension
All data in motion is cryptographically isolated and encrypted within the Cisco Intercloud Fabric Secure Extender. This data includes traffic exchanged between the private and public clouds (site to site) and the virtual machines running in the cloud (VM to VM). A Datagram Transport Layer Security (DTLS) tunnel is created between these endpoints to more securely transmit this dat
A. DTLS is a User
Datagram Protocol (UDP)-based highly secure transmission protocol. The Cisco Intercloud Fabric Extender always initiates the creation of a DTLS tunnel.
The encryption algorithm used is configurable, and different encryption strengths can be used depending on the level of security desired.
The encryption algorithm used is configurable, and different encryption strengths can be used depending on the level of security desired.



NEW QUESTION 131
Which two options are new features that are supported by IGMPv3compared to IGMPv2.(Choose two)

A. It extends IGM
B. which allows for an explicit maximum response time field.
C. It adds support for source filtering.
D. Router can now send a group-specific query.
E. It adds support for IGMP Leave Message.
F. It supports the link local address 224.0.0.22. which is the destination IP address for membership reports.

Answer: BE

Explanation: Do not understanding difference between IGMPv2 and v3 | LAN, Switching and Routing | Cisco Support Community
https://supportforums.cisco.com/discussion/10948466/do-not-understanding-difference-betweenigmpv2- and-v3
IGMP Version 3 Cisco http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_igmp.html Feature Overview
Internet Group Management Protocol (IGMP) is a protocol used by IPv4 systems to report IP multicast memberships to neighboring multicast routers.
This feature module introduces support for Version 3 of IGMP. In previous versions of Cisco IOS software only Version 1 and Version 2 were supported. IGMP Version 3 (IGMPv3) adds support for "source filtering," which enables a multicast receiver host to signal to a router which groups it wants to receive multicast traffic from, and from which source(s) this traffic is expected. This membership information enables Cisco IOS software to forward traffic only from those sources from which receivers requested the traffic.
IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:
INCLUDE mode—In this mode, the receiver announces membership to a host group and provides a
list of IP addresses (the INCLUDE list) from which it wants to receive traffic. EXCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of IP addresses (the EXCLUDE list) from which it does not want to receive traffic. This indicates that the host wants to receive traffic only from other sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, like in the case of the Internet Standard Multicast (ISM) service
model, a host expresses EXCLUDE mode membership with an empty EXCLUDE list. IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in
Source Specific Multicast (SSM). SSM was introduced in Cisco IOS Release 12.1(3)1, however SSM support for IGMPv3 was introduced in 12.1(5)T. For SSM to rely on IGMPv3; IGMPv3 must be available in last hop routers and host operating system network stacks, and be used by the applications running on those hosts.
In SSM deployment cases where IGMPv3 cannot be used because it is not supported by the receiver host or the receiver applications, there are two Cisco-developed transition
solutions that enable the immediate deployment of SSM services: URL Rendezvous Directory (URD) and IGMP Version 3 lite (IGMP v3lite). Both of these features are documented in the Cisco IOS Release 12.0(15)S Source Specific Multicast with IGMPv3, IGMP vSlite, and URD feature module.
IGMP
Version Description IGMPvl

Provides the basic query-response mechanism that allows the multicast
router to determine which multicast groups are active and other processes that enable hosts to join and leave a multicast group. RFC 1112 defines the IGMPvl host extensions for IP multicasting. IGMPv2
Extends IGMP. allowing such capabilities as the IGMP leave process, group-specific queries, and an explicit maximum response time field. IGMPv2 also adds the capability for routers to elect the IGMP querier without dependence on the multicast protocol to perform this task. RFC 2236 defines IGMPv2.
IGMPv3
Provides for source filtering. which enables a multicast receiver host to
signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. In addition, IGMPv3 supports the link local address 224.0.0.22. which is the destination IP address for IGMPv3 membership reports; all IGMPv3-capable multicast routers must listen to this address. RFC 3376 defines IGMPv3.

NEW QUESTION 135
Which two statement about local profiling on a Cisco WLC running AireOS are true? (Choose two)

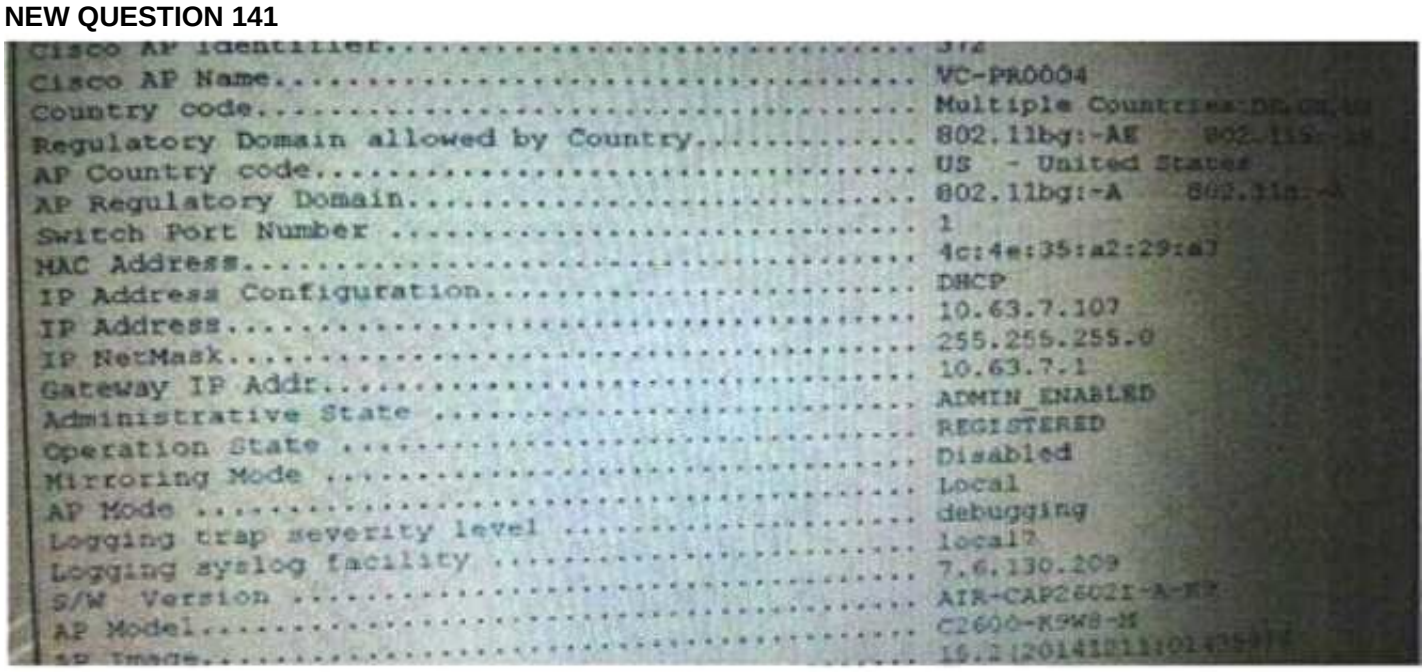
A. Profiling is performed on IPV4 and IPV6 client.
B. When local profiling is enabled , RADIUS profiling is allowed.
C. Wired clients behind the workgroup bridge are profiled and a policy action is taken
D. Profiling is performed only on IPV4 clients.
E. Wired clients behind the workgroup bridge are not profiled and no policy action is take

Answer: DE

NEW QUESTION 139
Which two impact dose TSPEC admission controlhave as it relates to 802.11e clients? (choose two)

A. Enforce airtime entitlement for wireless voice applications.
B. Ensure that call quality dose not degrade for existing VoWLAN calls.
C. Deny client access to the WLAN that do not meet the standard.
D. Allow access only for VoWLAN traffic when interference is detecte

Answer: AB

NEW QUESTION 141


Refer to the exhibit which syslog logging facility and severity level is enabled on this AP ?

A. logging trap severity 6, logging syslog facility local7
B. logging trap severity 3,logging syslog facility sys 10
C. logging trap severity 5,logging syslog facility local14
D. logging trap severity 7, logging syslog facility local 7
E. Logging trap severity 9,logging syslog facility kernel

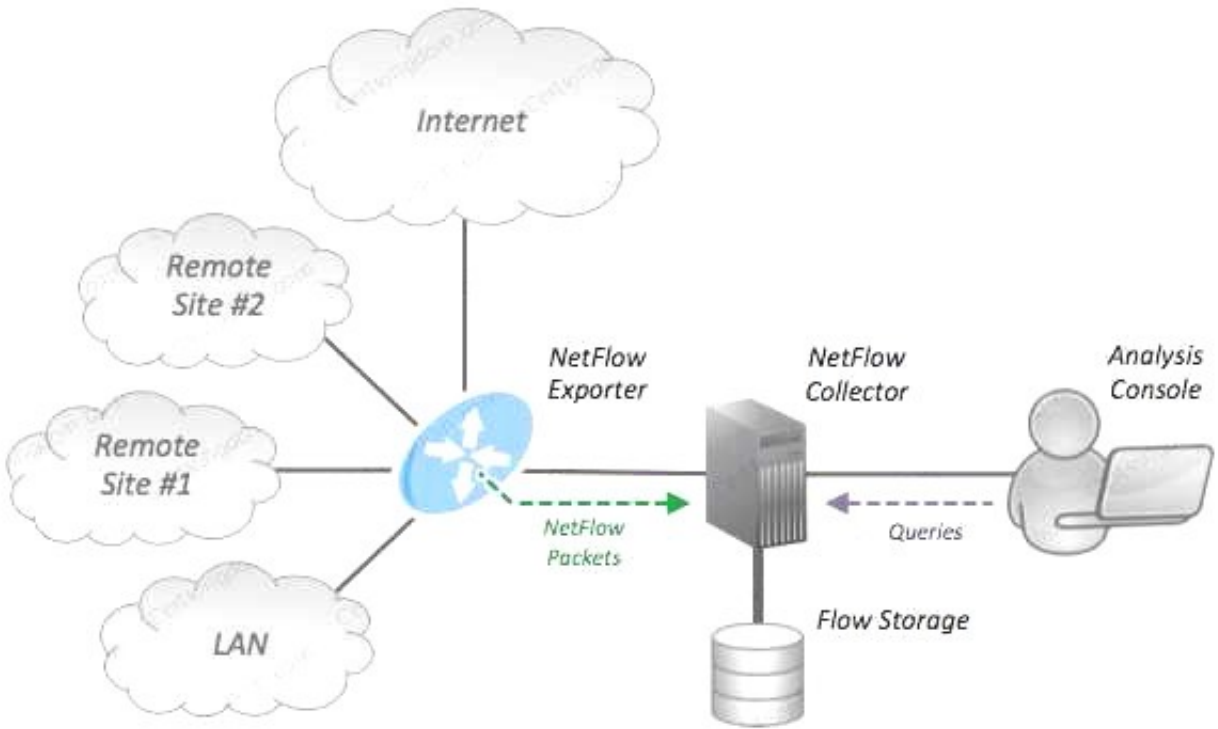
Answer: D

NEW QUESTION 144
DRAG DROP
Drag and drop the AVC configuration feature on the left to their respective function on the right.?

Enable AVC	Select Application Action for DROP or MARK
NetFlow Exporter	Mapped to WLAN for action enforcement
NetFlow Monitor	Network entity that exports the template with the IP traffic information.
AVC Profile	Classifies application and provides applicaton-level visibility and control (Qos) in Wireless network.
AVC Rule	ASsigned to WLAN to export IP traffic information to collector.

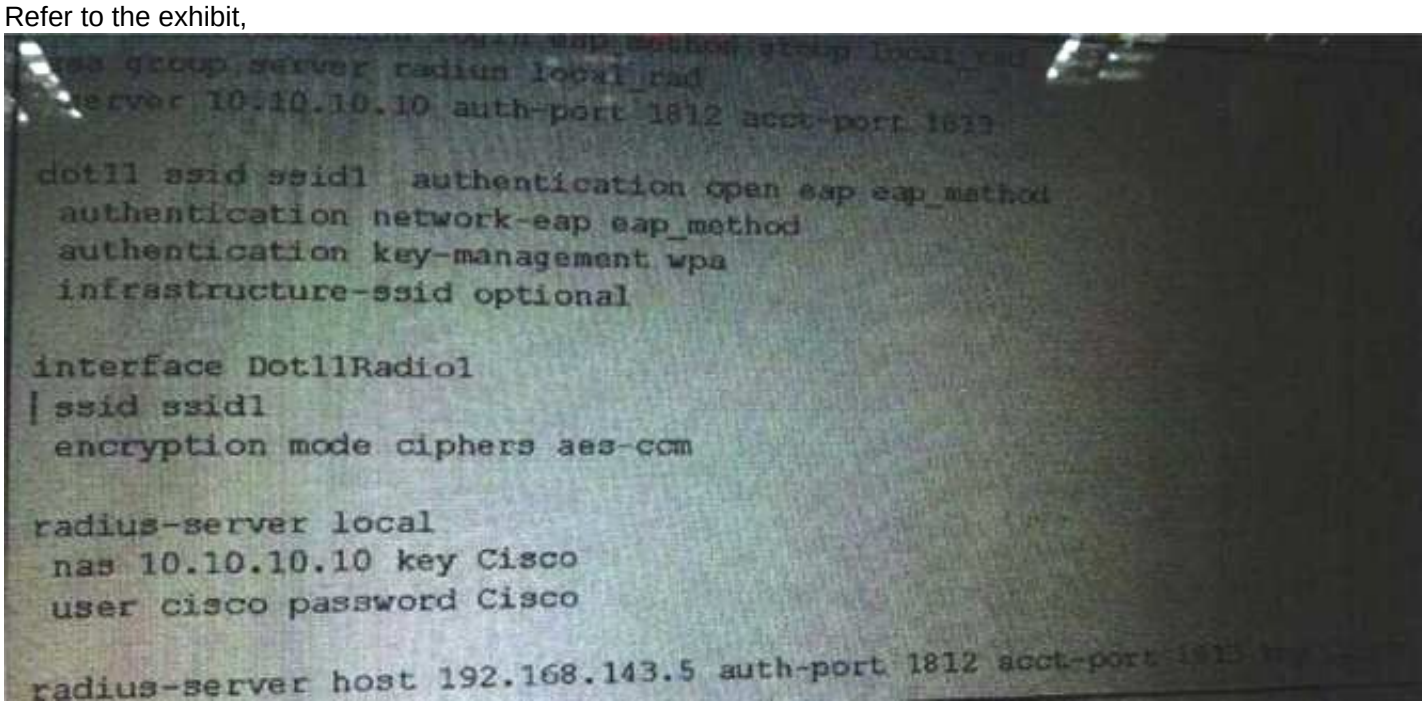
Answer:

Explanation: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/primeinfrastructure/ solution_overview_c22-728972.html
http://mrncciew.com/2013/02/13/who-really-support-wlc-netflow/ http://mrncciew.com/2013/10/07/3850-filexible-netflow/
http://docwiki.cisco.com/wiki/AVC:AVC_Tech_Overview https://en.wikipedia.org/wiki/NetFlow



http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/7- 5/AVC_dg7point5.html#pgfId-50665

NEW QUESTION 145
Refer to the exhibit,



based upon the given configuration which two statement are true? (choose two)

A. local RADIUS server is used
B. No password is required everyone can join wireless network
C. Users will be required to provide a username and password for authentication
D. User will be required to provide a password only order to get access
E. Remote RADIUS servers is used

Answer: AC

NEW QUESTION 147
Given the IPV6 address and subnet 2001:adcb:3257:9048::/64,which option list the start and ending IP address of this subnet?

A. 2001:adcb:3257:9048: ,2001:adcb:3257:9048:0000:0000:0000:ffff
B. 2001:adcb:3257:9048:0:0:0:0 .2001:adcb:3257:9048:0000:ffff:ffff:ffff
C. 2001:adcb:3257:9048:0:0:0:0 ,2001:adcb:3257:9048: ffff'ffff:ffff:ffff
D. 2001:adcb:3257 9048 0 0 0 0 ,2001adbc: 3257 9048 0000:0000:0000:ffff
E. 2001:adcb:3257:9048 :0:0:0:0, 2001:adcb:3257: 9048: 0000:0000:ffff: ffff
F. 2001:adcb:3257:9048:0::, 2001:adcb:3257:9048:0000:0000:0000:ffff

Answer: C

NEW QUESTION 152
which two types of interface events are common for cleanAir?(choose two)

A. Microwave interference
B. Co-channel interference

C. Spontaneous interference
D. Persistent mterference

Answer: CD

NEW QUESTION 153
Flexconnect APs have already deployed in a branch office for local switching.Currently the WLAN in the large auditorium is proposed to change to high-density design and thus some low data rates are proposed to be disabled while keeping the data rates in other areas under the same Cisco WLC.
Which configuration settings must be modified in the Cisco WLC to achieve this configuration?(choose two)

A. FlexconnectgroupS
B. Mobility groups
C. AP Groups
D. RF profiles

Answer: CD

NEW QUESTION 157
Which two AP join process are supported by the cisco 5760 WLC ?(choose Two)

A. Layer 2 CAPWAP discovery
B. Remotely stored controller IP address discovery
C. DNS discovery
D. Layer 3 CAPWAP discovery

Answer: CD

NEW QUESTION 162
Prime infrastructure will trigger alarms indicating that the prime infrastructure physicalor virtual server is low on disk space as the administrator which three actions can you take to increase disk space immediately upon receiving a major alert (60 percent disk usage)? (choose three)

A. Change the disk controller RAID
B. Enable corn job on ade for disk clean up using $ du-sh
C. Compacting the PI database using the NCS CLEANUP command
D. Reduce the storage load on the local disk by setting up and using remote buckuprepostttories
E. Reduce the length of time you store client association data and related events.
F. Compacting the PI database using the NCS DATABASE PURGE command

Answer: CDE

NEW QUESTION 163
Which two cisco ISE option simplify the use of EAP-TLS authentication in a BYOD environment using PKI? (choose two)

A. Simple Certificate Enrollment Protocol
B. Lightweight Directory Access Protocol
C. Online Certificate Stats Protocol
D. Native Supplicant Provisioning
E. Certificate Signing Reques

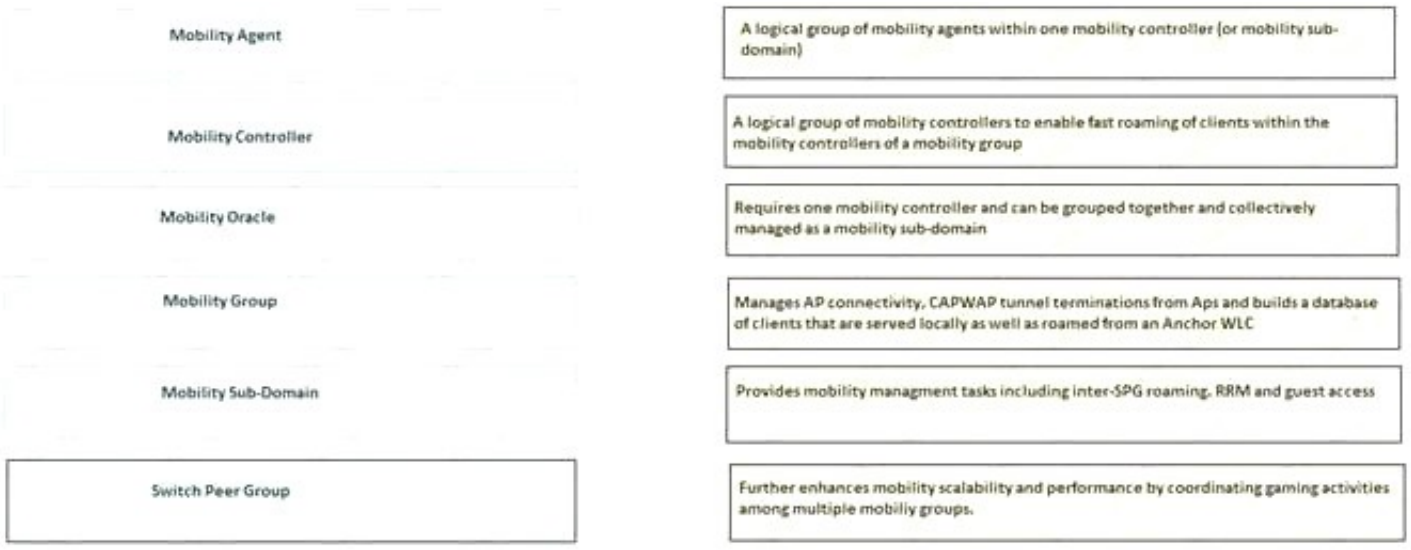
Answer: AE

NEW QUESTION 167
what are two differences between wireless QoS and wired QoS on an autonomous AP?(choose two)

A. WirelessQoS dose FIFO and RED on Ethernet egress ports
B. WirelessQoS can prioritize packet based on DSCP,TOS, COS or EXP values.
C. WirelessQoS MQC policy-maps support only set cos act1on
D. WirelessQoS carries out WMM type of queuing on the radio egress port
E. WirelessQoS support ISL 802.10 and 802.1p tagged packet

Answer: BC

NEW QUESTION 170
DRAG DROP
Drag and drop the mobility architecture components on the left to their primary function on the right?



Answer:

Explanation:

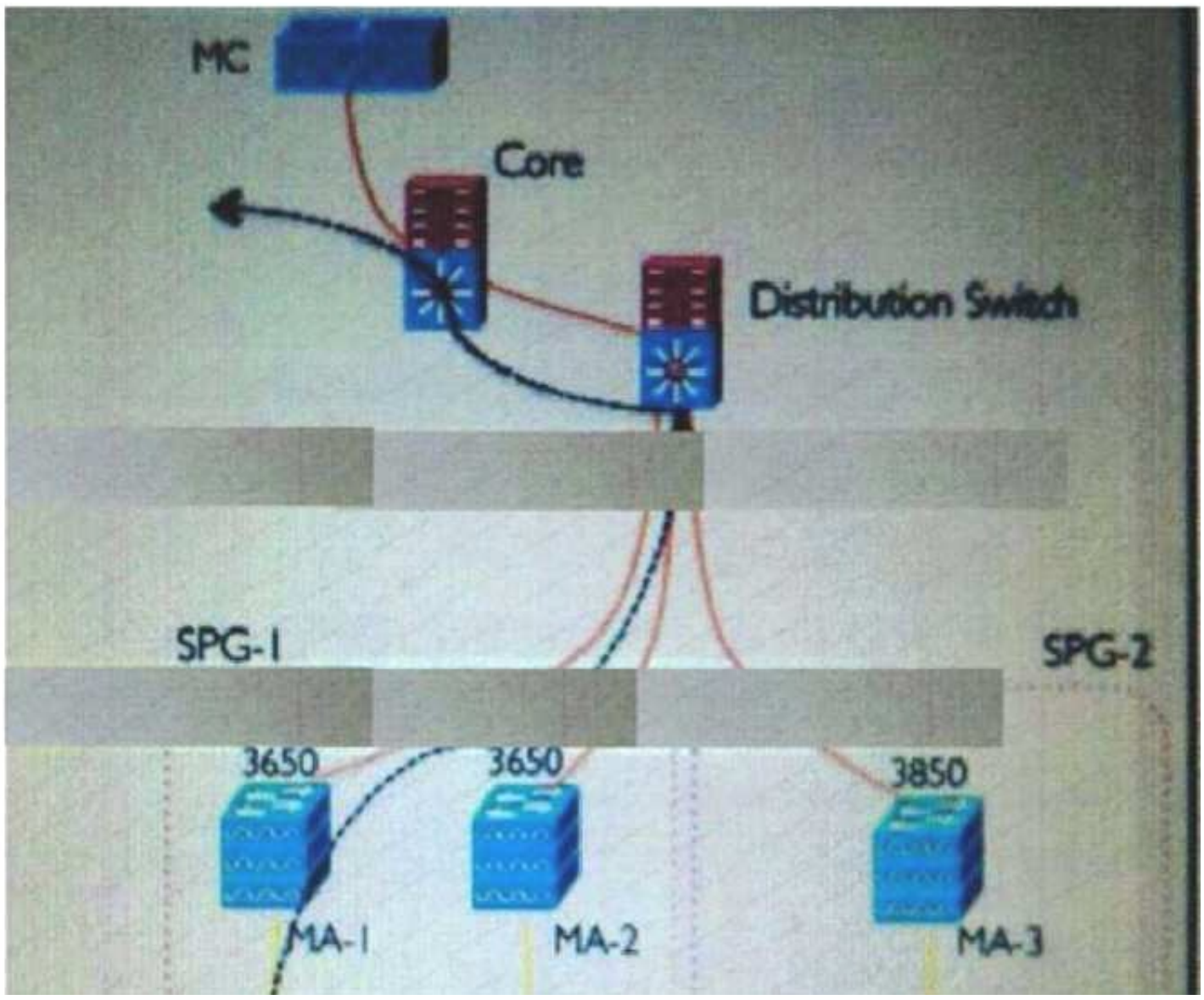
Mobility Agent	4	Manages AP connectivity, CAPWAP tunnel terminations from Aps and builds a database of clients that are served locally as well as roamed from an Anchor WLC
Mobility Controller	5	Provides mobility managment tasks including inter-SPG roaming, RRM and guest access
Mobility Oracle	6	Further enhances mobility scalability and performance by coordinating roaming activities among multiple mobility groups
Mobility Group	2	A logical group of mobility controllers to enable fast roaming of clients within the mobility controllers of a mobility group
Mobility Sub-Domain	3	Requires one mobility controller and can be grouped together and collectively managed as a mobility sub-domain
Switch Peer Group	1	A logical group of mobility agents within one mobility controller (or mobility sub-domain)

NEW QUESTION 172
Which Cisco WLC configuration option should be used if you do not want to require guest user to re authenticate via local web authentication when their device has not been associated to the cisco WLC for a longer period?

A. Condition Web Redirect
B. Client user idle timeout
C. Session Timeout
D. Sleeping Client

Answer: D

NEW QUESTION 175
Refer the exhibit.



A Wireless user has roamed tram an AP connected to MA-l to an AP connected to MA·.:S. The traffic flow for the user before the roam is shown. Which option shows the traffic flow for the user after roam, considering default sticky anchoring is disabled on the WLAN, and WLAN to VLAN mapping and roaming domain IDs are identical on both sides?

A. MA-3 >Distribution Switch> MA-l> Distribution Switch> Core
B. MA-3 > Distribution Switch > MA-2 > MA-1> Distribution Switch > Core
C. MA-3 >Distribution Switch> MA-2 >MA-l> Distribution Switch> Core
D. MA-3 > Distribution Switch > Core

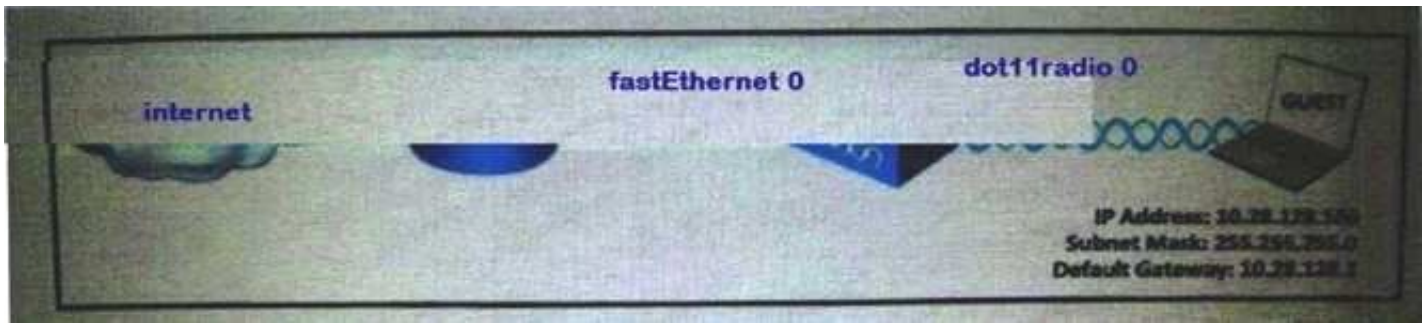
Answer: D

NEW QUESTION 177
Which two features require Network Time Protocol synchronization on the Cisco 5760 WLC?(Choose two)

A. AP CAPWAP multicast
B. SNMPv3
C. AP authentication
D. Band Select

Answer: BC

NEW QUESTION 181
Refer to the exhibit



the autonomous AP has a corporate and guest SSID configured . The security team requested that you limit guest user traffic to DHCP ,DNS, and web browsing on the AP. which configuration best satisfies the request?

A. access-list 101permit udp any any eq 67 access-list 101permit udp 10.28.128.0 0.0.0.255 host 10128.10.15 eq 53 access-list 101 permit tcp 10.28.128.0.0.0.0.255 any eq 80 access-list 101 deny ip any any interface dot11radio 0 ip access-group 101 in
B. access-list 101permit udp any any eq 67 access-list 101permit udp 10.28.128 0.255.255.255 host 10128.10.15 eq 53 access-list 101permit tcp 10.28.128 0.255.255.255 any eq 80 access-list 101deny ip any any interface dot11radio 0 ip access-group 101in
C. access-list 101 perm1t udp any any eq 67 access-list 101 per mit udp 10.28.128.0 0.0.0.255 host 10128.10.15 eq 53 access- l1st 101 permit tcp 10.28.128.0 0.0.0.255 any eq 80 access-list 101 deny ip any any interface fast Ethernet 0 ip access-group 101 in
D. access-list 101 permit udp any anyeq 67 access-list 101 permit udp 10.28.128 0.255.255.255 host10128.10.15 eq 53 access-list 101 permit tcp 10.28.128 0.255.255.255 any eq 80 access-list 101 deny ip any any interface fast Ethernet 0 ip access-group 101 in

Answer: C

NEW QUESTION 185
Refer to the exhibit.

```
ip dhcp pool vlan 2100
 network 10.63.7.0 255.255.255.0
 default-router 10.63.7.1
 option 43 hex f104.18f4.1cd8
```

APs on VLAN 2100 can get IP address but cannotregister to the WLC The iP address of the WLC management interface is 24.244.4.227 which option is the correct DHCP option 43 configuration.?

A. f10412f41cd9
B. f10418f404227
C. f10818f41cd0a181cf4a01c
D. f10418f404e3
E. f1040a3f0701

Answer: D

NEW QUESTION 190
Which option in the cisco identity service engine allows for authorization based on Active Directory user and domain computer login?

A. Machine access restriction
B. Active directory group
C. Active directory attributes
D. Identity source sequences

Answer: A

NEW QUESTION 193
While troubleshooting a failed central web authentication configuration on cisco WLC you discover that the Cisco WLC policy manager state is showing RUN For new client and not CENTRAL_WEB_AUTH what is most likely the issue.?

A. The WLAN Layer 2 security should be sent to WPA+WPA2
B. The WLAN NAC state should be set to RADIUS NAC
C. The web login page under the cisco WLC security should be set to external (redirect to external server)
D. The WLAN layer 3 security should be set to web page policy with condition web redirec

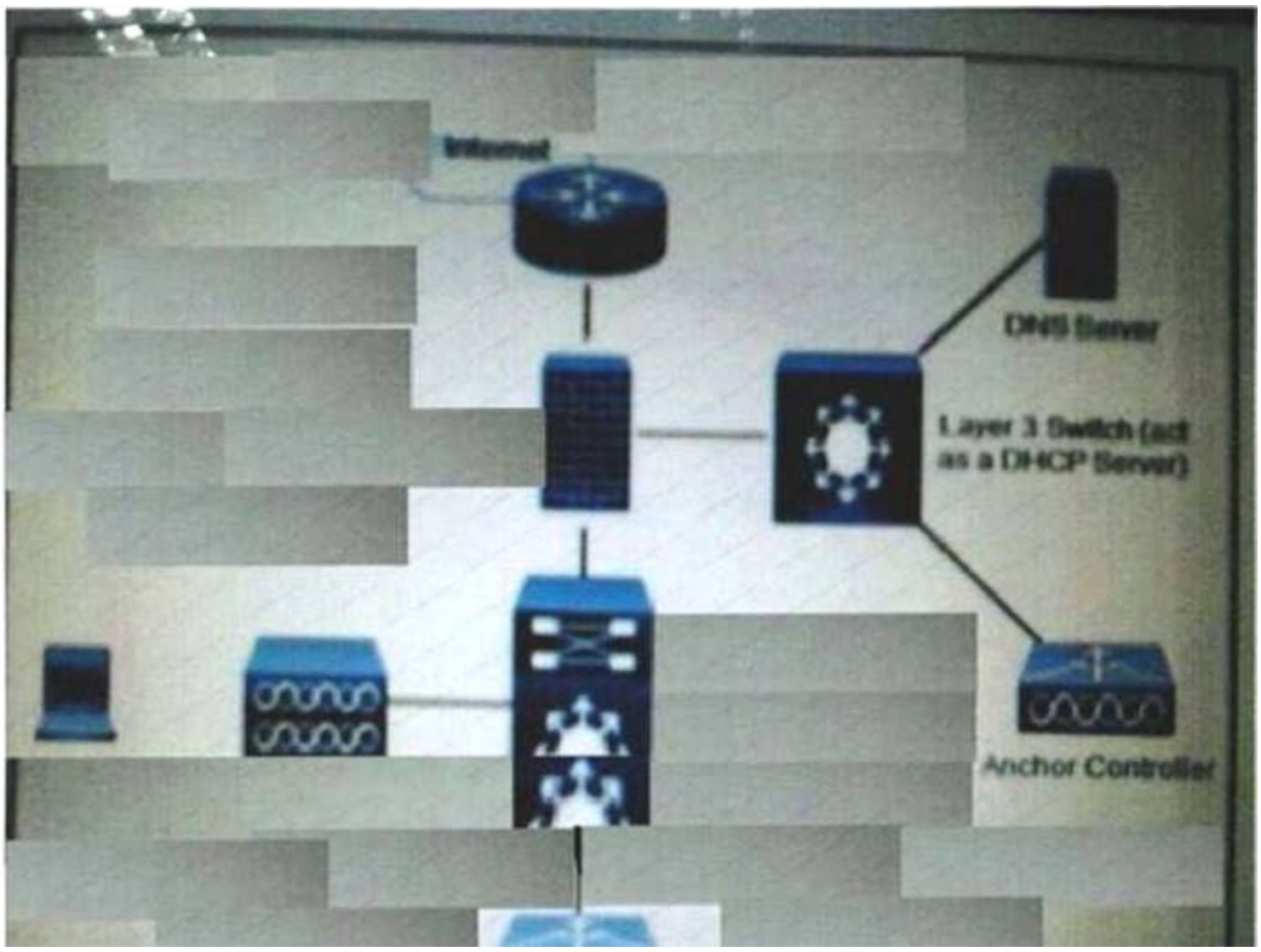
Answer: B

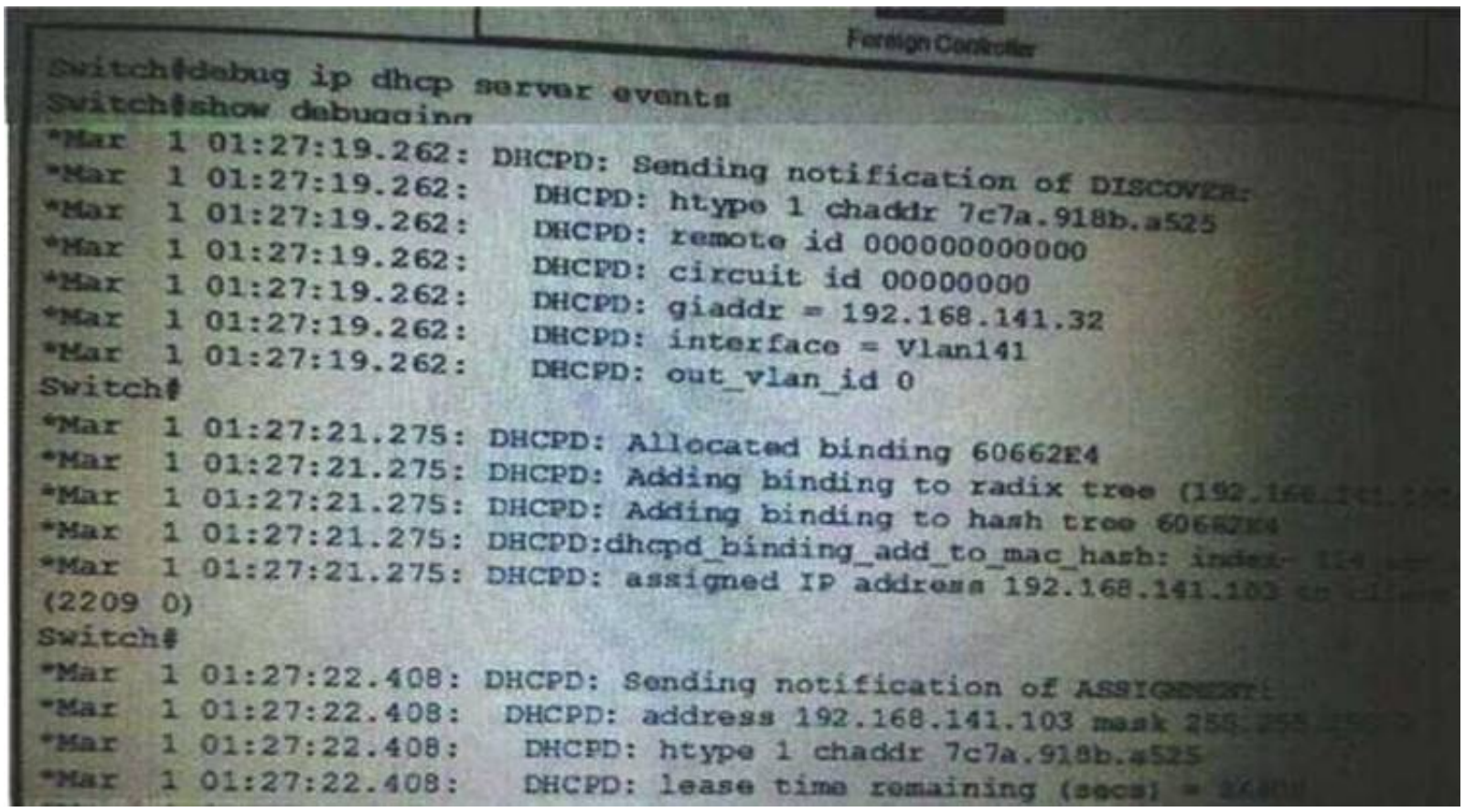
NEW QUESTION 196
Two autonomous Aps are connected to a switch on the same VLAN both APS are configured with the same SSID and WPA2-PSK. After making configuration changes to one of the APs .spanning tree disabled one of the switch ports into which AP was plugged.? Which two options describe possible reasons that spanning tree disabled a port? (choose Two)

A. One of the Aps was configured as a universal workgroup bridge.
B. It is not possible for spanning tree to disable a por
C. The bridging loop must have been coincidental
D. Spanning tree was disabled on both Aps
E. PortFast was enabled on all ports
F. One of the APs was configured as a standard workgroup bridg

Answer: AE

NEW QUESTION 201
Refer to the exhibit.





Your colleague a junior network engineer is struggling to enable DHCP option 82 in the layer 3 switch which is in the DMZ for a mobile client under a guest anchor Cisco wireless LAN controller deployment . What is your answer.?

A. DHCP proxy must be enabled for DHCP option 82 to operate correctly . All Cisco WLCsthat will be in the setup must have the same DHCP proxy setting.
B. DHCP option 82 must be enabled on the dynamic interface with which theWLANis associated
C. DHCP option 82 is not supported when it is used with auto-anchor mobility
D. The mobility tunnel datapath control path or both between the anchor cisco WLC and foreign WLC are down.

Answer: C

NEW QUESTION 206
RX-SOP is configured for SGHz radio with value set as "High Threshold". Which two clients will associate to the AP? (Choose Two)

A. client with RSSI-75 dBm
B. client with RSSI-79d8m
C. client with RSSI-77dBm
D. client with RSSI-73dBm

Answer: AD

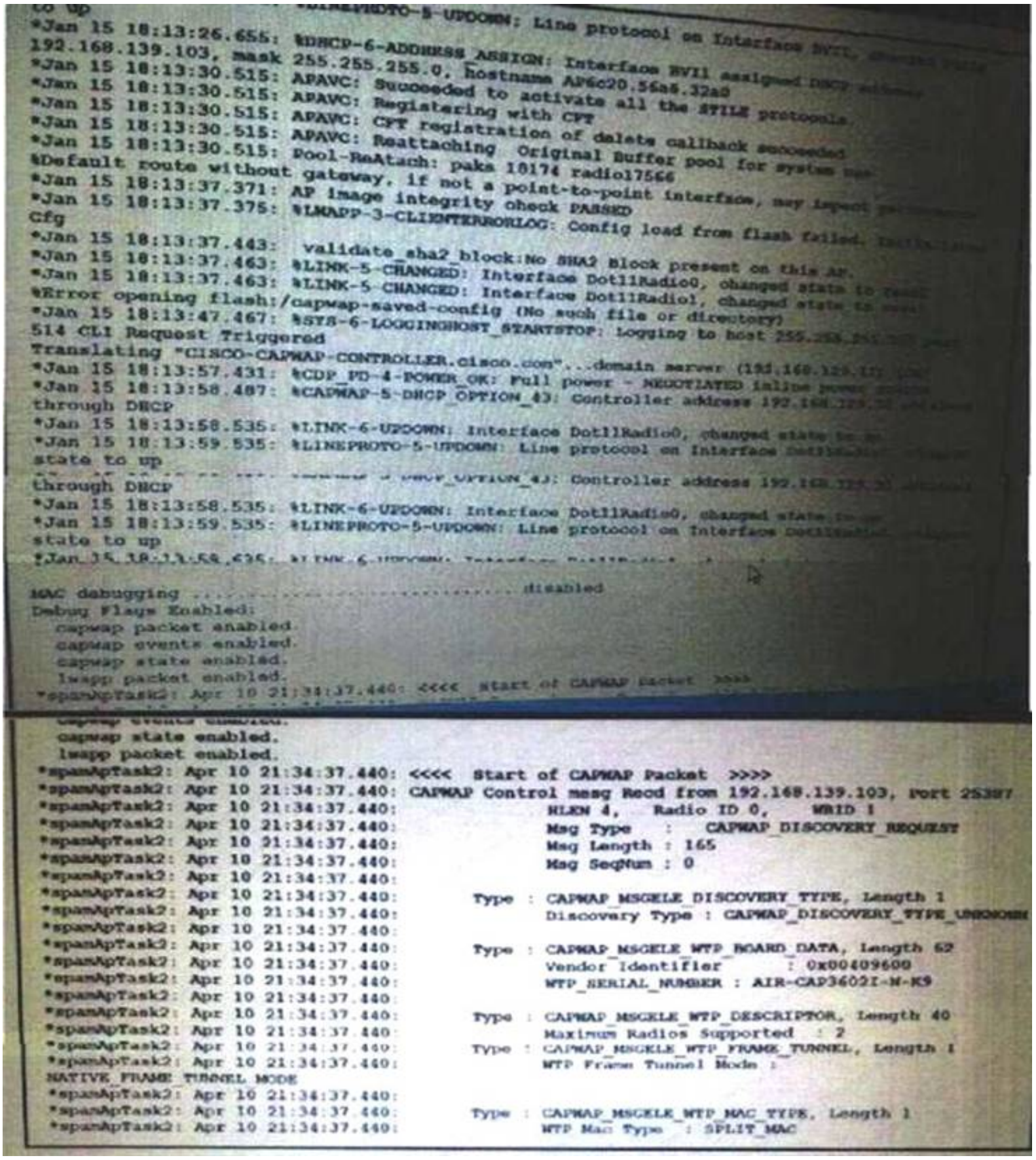
NEW QUESTION 211
Which port does cisco JSE use by default to send RADIUS CoA messages to the Cisco WLC?

A. UDP 3799

B. UDP 1813
C. UDP 1700
D. TCP 1812

Answer: C

NEW QUESTION 213
Refer to the exhibit .

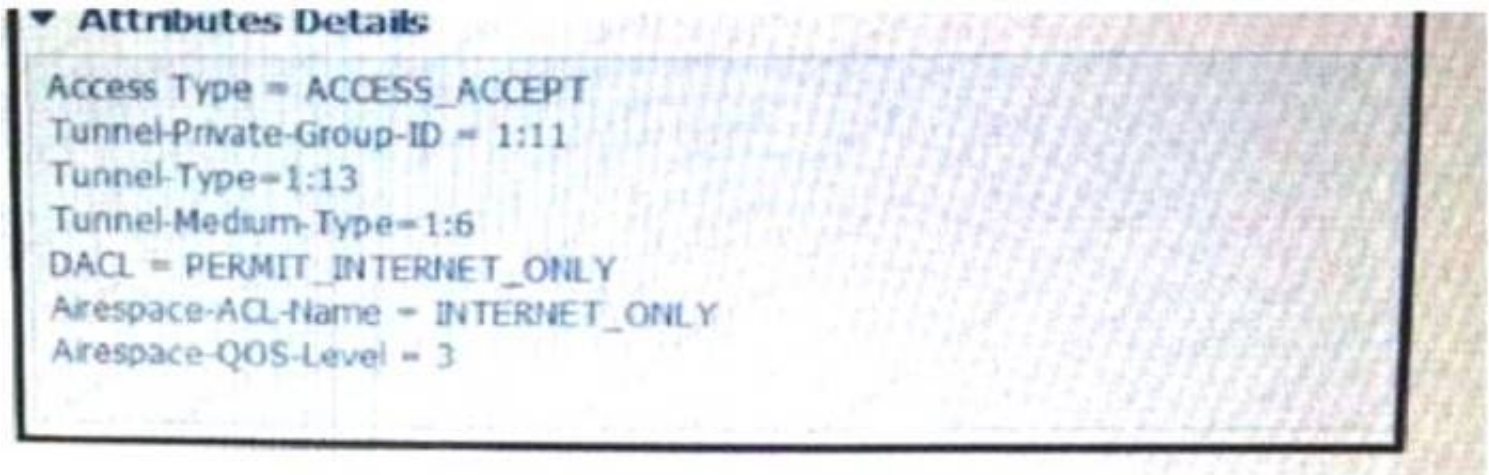


According to the debugs and logn the Cisco WLC and Cisco LAP which WLC discovery Algorithm is used by the LAP to join the Cisco WLC?

A. DHCP server LAP sends a layer 3 CAPWAP discover request to the Cisco WLC that is listed m the DHCP option 43.
B. configured LAP sends a uncast layer 3 CAPWAP discover request to the Cisco WLC IP address that the LAP has in its NVRAM
C. Broadcast lap broadcasts a layer 3 CAPWAP discover massage on the local ip subnet
D. DNS lap resolve the DNS Name CISCO-CAPWAP-CONTEOLLER cisco to the Cisco WLC ip address then it sends a uncast layer 3 CAPWAP discovery request to the Cisco WLC

Answer: A

NEW QUESTION 214
Refer to the exhibit.



Which AAA attribute is not used by the Cisco WLC running AireOS 8.0 ?

A. Tunnel-Pnvate-Group-10
B. Tunnel-Type
C. Airespace-QOS-Level
D. DACL

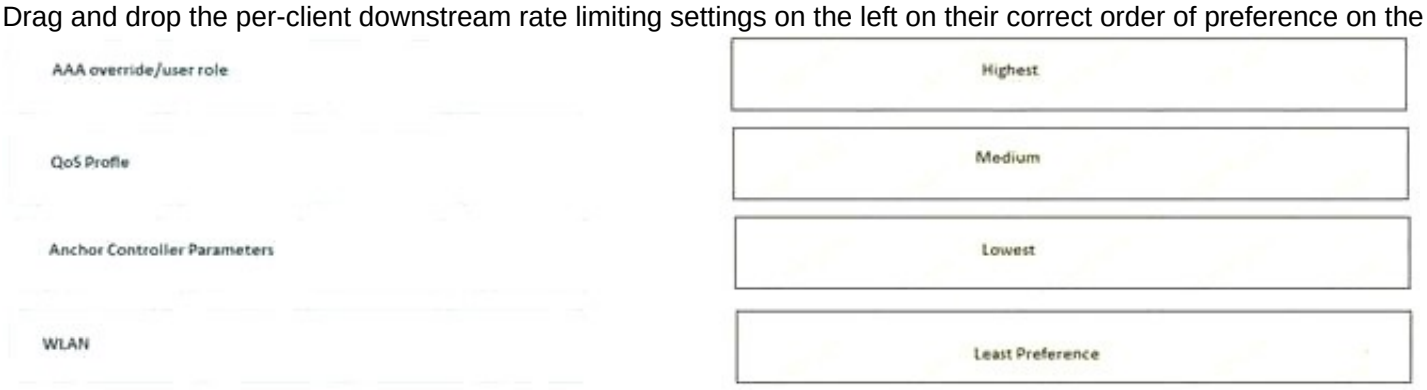
Answer: D

NEW QUESTION 215
When creating a guest account on Cisco identity Services Engine .Which option in the sponsor portal allows for the guest credentials to be used for RADIUS authentication without requiring the guest user to log into the guest portal?

A. Set the Guest role to Guest
B. Set the Guest role to Activated guest
C. Set the Time Profile to Radius 1Day
D. Check the box to send email not send email notification id the guest user name is based on the email address.

Answer: B

NEW QUESTION 218
DRAG DROP
Drag and drop the per-client downstream rate limiting settings on the left on their correct order of preference on the right.



Answer:

Explanation:

Anchor Controller Parameters	Highest
AAA override / user role	Medium
WLAN	Lowest
QoS Profile	Least Preference

NEW QUESTION 219
Which two statements about 802.11are true? (Choose two}

A. MIC is appended for robust management frame.
B. IGTK is used to protect robust broadcast and multicast management frames
C. Association and disassociation frames are protected.
D. PKC is used to protect robust unicast management frames .
E. Association responses are not protected

Answer: BE

NEW QUESTION 223
Your customer has high availability Clint SSO configure using a pair of Cisco 5508 WlCs running 8.0 code. The primary unit failed over and the secondary unit is now active. Which two statement are true. (Choose two)

A. Both controller RMIcan be in different subnets.
B. Only the clients that are in the run state are maintained during failover
C. Clients that are in transition such as roaming are dissociated
D. New mobility is supported

Answer: BC

NEW QUESTION 228
Which three AP modes are supported by Converged Access WLC (3650/3850/5760) in cisco ISO-XE software 3.6E? (Choose three)

A. sniffer
B. local
C. Fiexconnect
D. monitor
E. office extend
F. Mesh

Answer: ABD

NEW QUESTION 233
Refer to the exhibit

Which statements about this CPU ACL is true?

A. A user on the 10.64.0.0/24 network can use SSH to access the WLC.
B. A User on the 10.64.0.0/24 network cannot use HTTPS to access the WLC GUI
C. A user on the 10.64.0.0/24 network cannot use telnet to access the WLC 172.21.159..37
D. Any user on any other subnet can access the WL

Answer: C

NEW QUESTION 234
Which two statements about 802.11r are true? (Choose two)

A. A PTK is generated before the client roams to the target AP.
B. Non-802.11r clients cannot associate to WLANs that have 802 llr enabled on WLC AireOS code 8.0
C. 802.11r IS supported only on OPEN and WPA2 WLANs.
D. This protocol uses the four-way handshake for the key management upon roamin

Answer: BC

NEW QUESTION 235
Your customer is having wireless VoIP problems. When the Cisco 7925 phones roam from APtlo AP2, the voice drops out and comes back. The phones are set up for PEAP/WPA2-AES with CCKM to an external RADIUS server .The APs and WLAN are setup in FlexConnect mode. Which statement explains the issue?

A. PEAP with WPA2-AES is not supported with Cisco Centralized Key Management, use EAP-FAST.
B. The APs have not been added to the FlexConnectgroup .
C. PEAP with WPA2-AES is not supported with Cisco Centralized Key Management, use LEAP.
D. The APs have been added to the FlexConnectgroup .

Answer: B

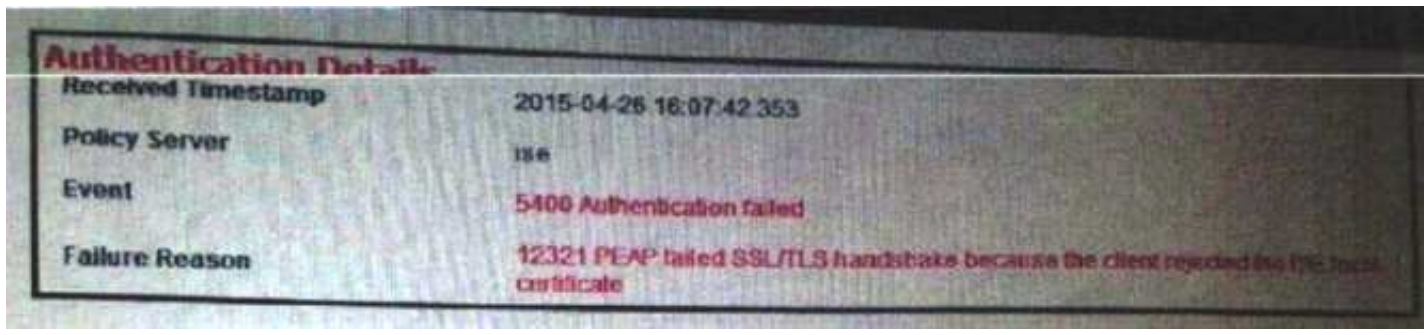
Explanation: http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configurationguide/b_cg80/b_cg80_chapter_0101110.html https://supportforums.cisco.com/discussion/11396831/vowlan-cckm-792x-series http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/100397- peap-ias.html

NEW QUESTION 238
In Cisco Wireless LAN Controller .the transmit power level of an AP radio is assigned an integer value inserted of a value in mW or dBm. Which two statements about the power level are true (Choose two)

A. The integer corresponds to a power level that vanes depending on the regulatory domain in which the access points are deployed
B. Each successive lower power level always represents 50% of the previous power level.
C. Power Level 1 is always the minimum power level allowed per country code setting.
D. There are always eight power levels for configuratio

Answer: AB

NEW QUESTION 242
Refer to the exhibit.



What is the best way to resolve this issue?

A. Install a publicity 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

NEW QUESTION 243
An autonomous AP is configured with the infrastructure –client command. What is this command used for?

A. to allow more than 20 client associations
B. to send reliable multicast traffic
C. to enable multiple VLANs to cross the bridge link
D. to allow only infrastructure device associations

Answer: B

NEW QUESTION 248
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

NEW QUESTION 251
Which two configuration are required on the Cisco 5760 WLC to ensure that APs will successfully join the Cisco WLC? (Choose two)

A. Enable IP DHCP SNOOPING TRUST on the wireless controller port-channel interface
B. Activate the apocopate Right-to-use AP license on the wireless LAN controller
C. Ensure that port-fast is enabled on each access point switch port
D. Ensure accurate configuration of the correct time and date on the wireless LAN controller

Answer: BD

NEW QUESTION 253
Which two option describe implication of deploying autonomous APs in repeater mode? (Choose two)

A. The Ethernet port is disabled in repeater mode
B. You can configure multiple VLANs on repeater access point

C. You should disable Cisco Aironet extensions on the parent(root) AP and on the repeater APs
D. The infrastructure SSID should be assigned to the native VLAN

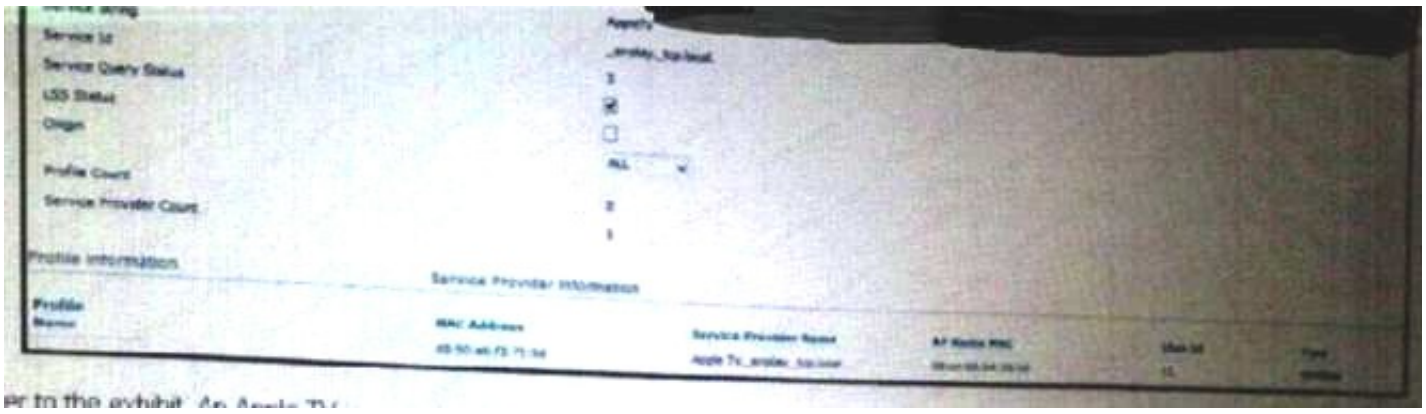
Answer: AD

NEW QUESTION 258
You want to set up Prime infrastructure to be notified when a device configuration has changed. Which option is available in prime infrastructure 2.2 ?

A. Set up prime infrastructure to send an email containing the device configuration change(s} on regularly scheduled.
B. Set up prime Infrastructure to send an email containing the change audit report immediately after the configuration change is detected
C. Set up prime infrastructure to send an email containing the change audit report on a regularscheduled basis
D. Set up prime infrastructure to send an email containing the configuration change(s) immediately after the configuration change is detected.

Answer: C

NEW QUESTION 259
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

NEW QUESTION 261
In a VWLAN deployment, what autonomous ISO command should be used to ensure that VWLAN performance is not adversely impacted by an unexpected channel change resulting from a DFS event triggered by a nearby airport radar system?

A. ap(config-if)#DFs band 1block
B. ap(config-if)#DFs band 23 block
C. ap(config-if)#DFs band 123 block
D. ap(config-if)#DFs band 13 block
E. ap(config-if)#DFs band 2 block

Answer: B

NEW QUESTION 263
Which two statement about AP local authentication by FlexConnect AP in standalone mode are true?(choose two)

A. Only LEAP,EAP F AST,PEAP and EAP-TLS authentication are supported
B. Only the vendor certificate authority (CA) certificate has to be downloaded to the Cisco wireless LAN controller for EAP-TLS authentication
C. Cisco wireless LAN controller must generate a certificate signing request by itself for submitting to a certificate authority for signing.
D. A filexconnect group must be created so that the cisco wireless LAN Controller can push the certificate to the filexconnect AP in the Flexconnect group.

Answer: AD

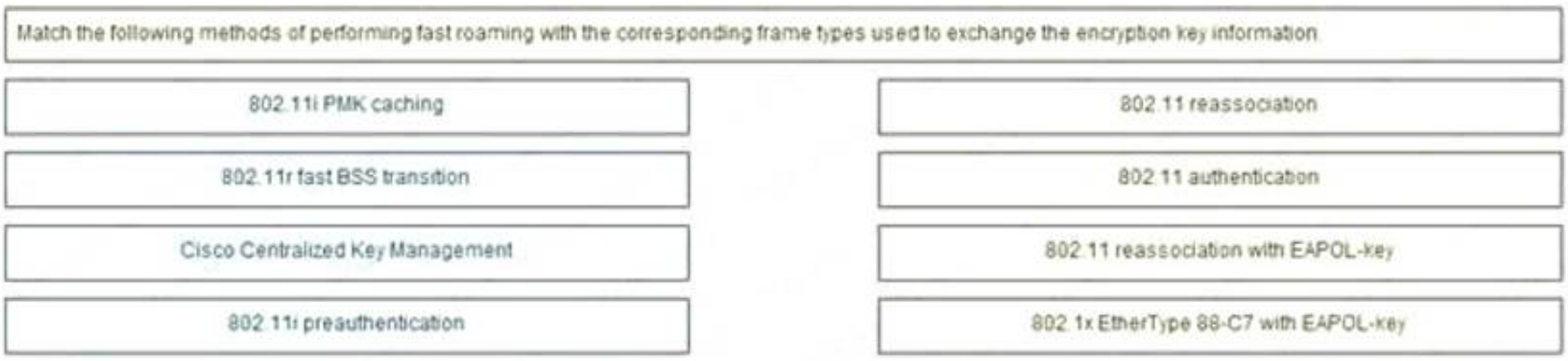
NEW QUESTION 265
You are working on a deployment that uses two Cisco APs as wireless bridges. One of the bridges is configured as a root bridge and the second bridge is configured as a nonroot bridge. Client A associates to the root bridge and client B associates to the nonroot bridge. Which two statements about this scenario are true? (Choose two)

A. The default setting of a bridge is nonroot bridge.
B. For two bridges to communicate with each other, one of the bridges must be in root mode and the other bridge must be in nonroot mode.
C. Only one device can connect to the Ethernet port of a nonroot bridge.
D. Two bridges that are in root mode can talk to each other.
E. In point-to-multipoint bridging, WGB is not recommended with the root bridg
F. WGB must be associated to the root AP in point-to-multipoint bridging setup.

Answer: AE

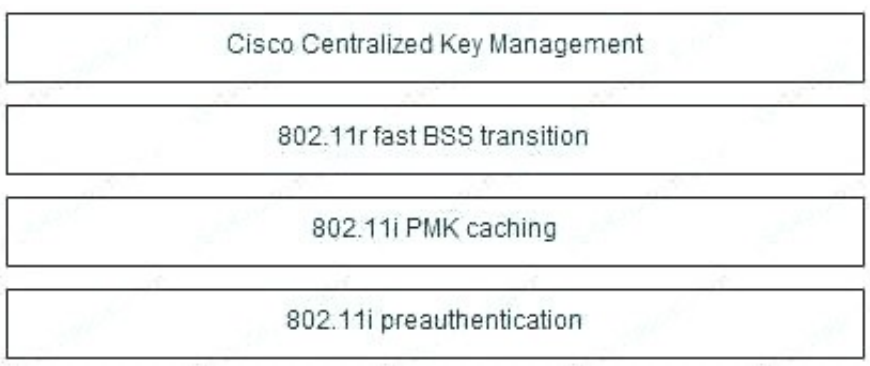
Explanation: http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/16041-bridgefaq. html
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/22950-br-ts- 22950.html#reset
http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3- 3/cg15-3-3-chap6-radio.html

NEW QUESTION 268
DRAG DROP

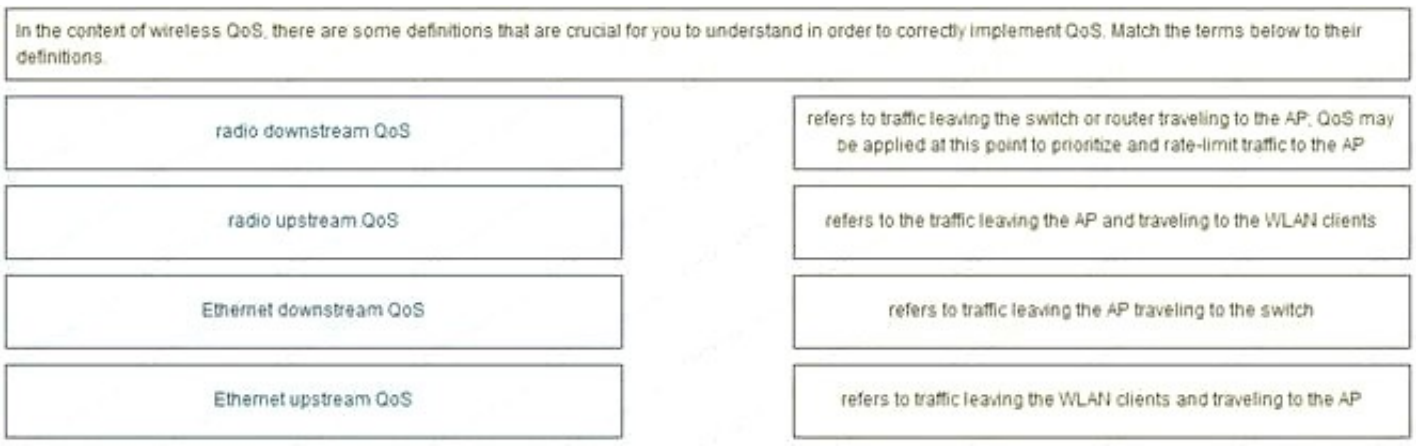


Answer:

Explanation:

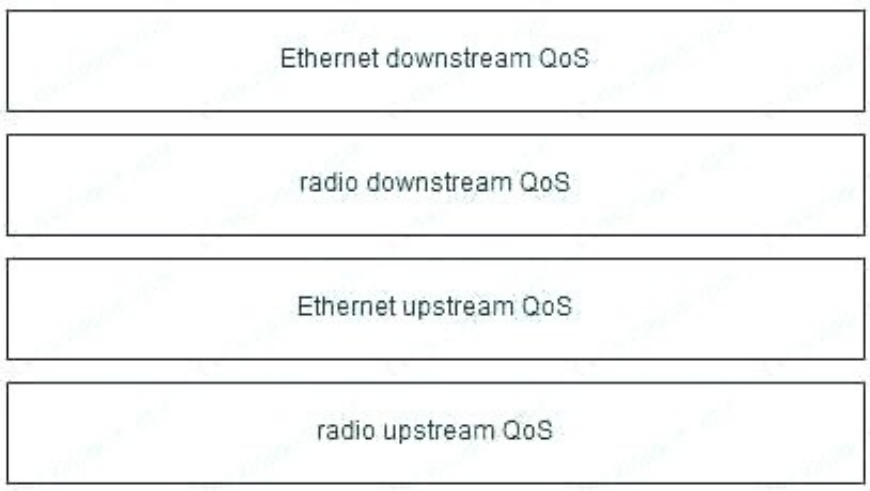


NEW QUESTION 273
DRAG DROP

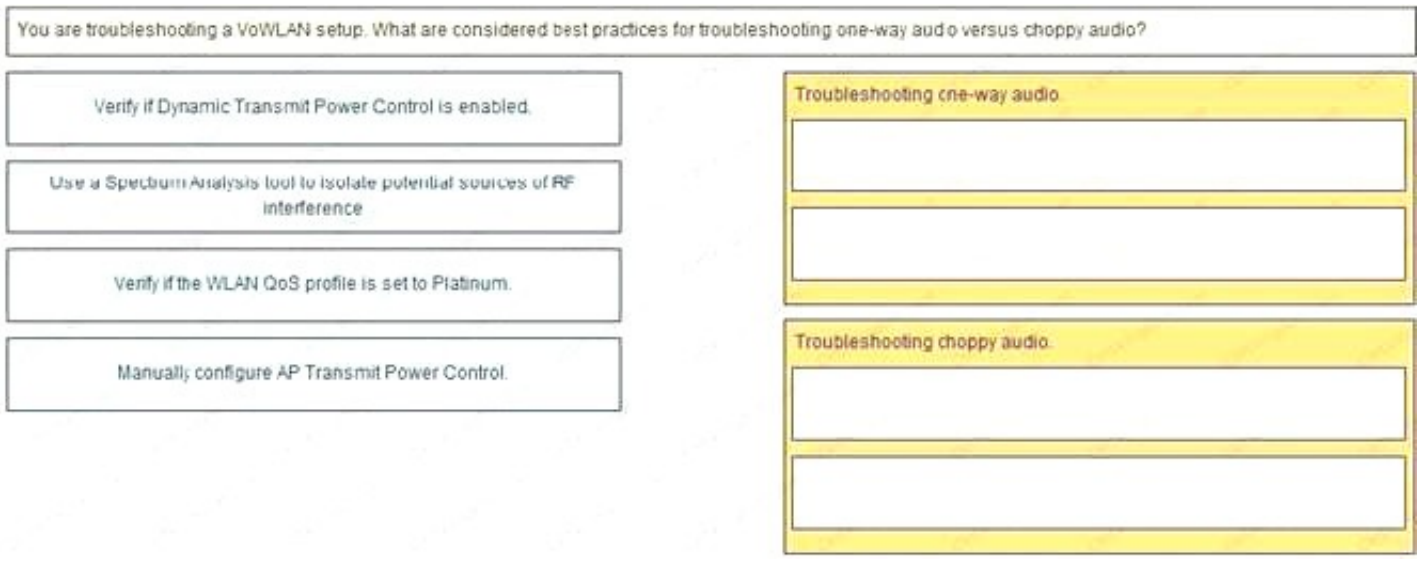


Answer:

Explanation:

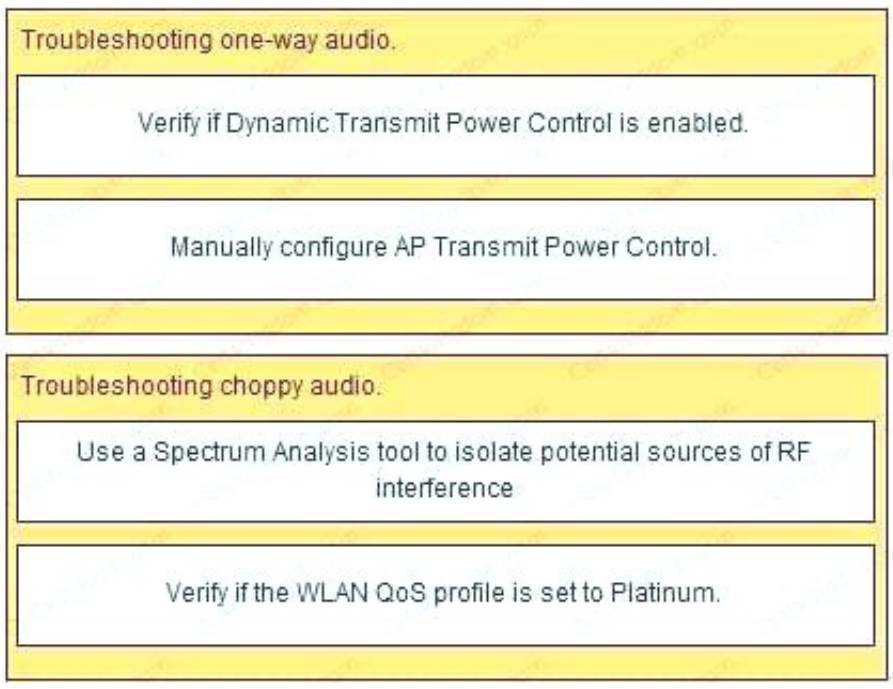


NEW QUESTION 276
DRAG DROP

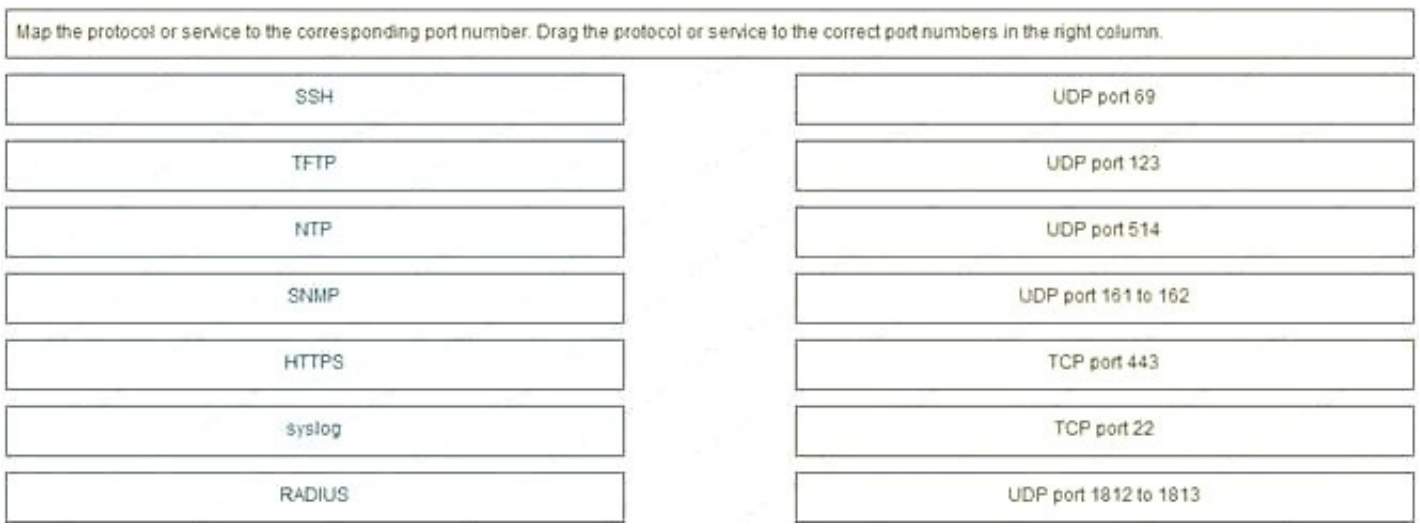


Answer:

Explanation:



NEW QUESTION 279
DRAG DROP



Answer:

Explanation:

TFTP

NTP

syslog

SNMP

HTTPS

SSH

RADIUS

NEW QUESTION 282
DRAG DROP

Map the WLC interfaces on the left to their correct functionality description in the right column.

management interface	This interface is not available on all Cisco WLCs.
AP-manager interface	Within a mobility group, the same IP address must be used for this interface in order for intercontroller roaming to work without losing connectivity.
virtual interface	If the service port is in use, this interface must be on a different subnet than the service-port interface.
service port interface	Cisco recommends using tagged VLANs for these types of interfaces.
dynamic interface	This interface is used for all Layer 3 communications between the controller and lightweight access points after the access points have joined the controller.

Answer:

Explanation:

service port interface

virtual interface

management interface

dynamic interface

AP-manager interface

NEW QUESTION 284
DRAG DROP

Map the common status error message seen on a Cisco Unified Wireless IP Phone 7900 Series, in the left column, to its possible cause, in the right column.

Network Busy	The phone is attempting to obtain network parameters such as its IP address, or the IP address of the gateway or router from the DHCP server.
Leaving Service Area	The phone cannot detect any beacons from the AP. The phone is either out of range of an AP or the AP may have unexpectedly stopped sending beacons.
Locating Network Services	CAC is enabled and the available bandwidth (Medium Times) has been reached per AP or channel.
Configuring IP	The phone is searching all beacons and scanning for a channel and SSID to use.

Answer:

Explanation:

Configuring IP

Leaving Service Area

Network Busy

Locating Network Services

NEW QUESTION 289
DRAG DROP

Regarding mesh access points, map the bridge group name characteristics on the left to the maximum BGN length and BGN of an out-of-the-box AP on the right.

10 characters

32 characters

DEFAULT

NULL

maximum BGN length
Target

BGN of an out-of-the-box AP
Target

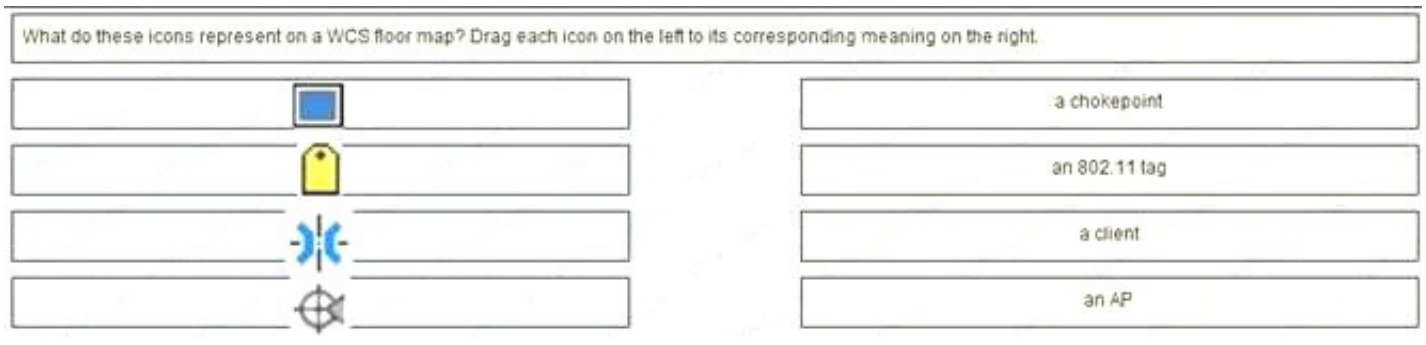
Answer:

Explanation:

maximum BGN length
10 characters

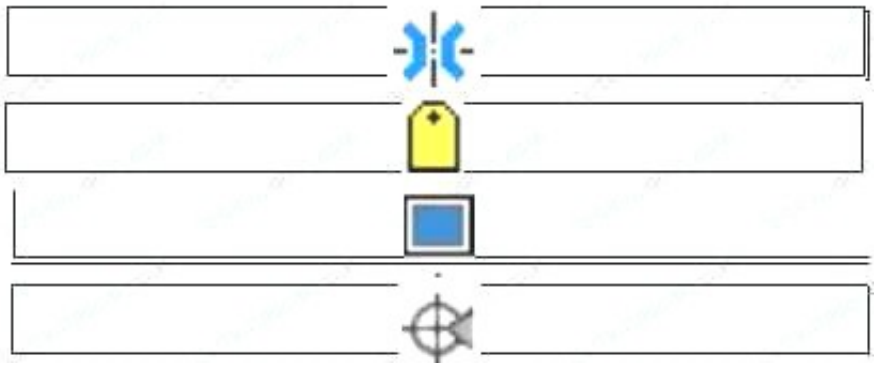
BGN of an out-of-the-box AP
NULL

NEW QUESTION 294
DRAG DROP

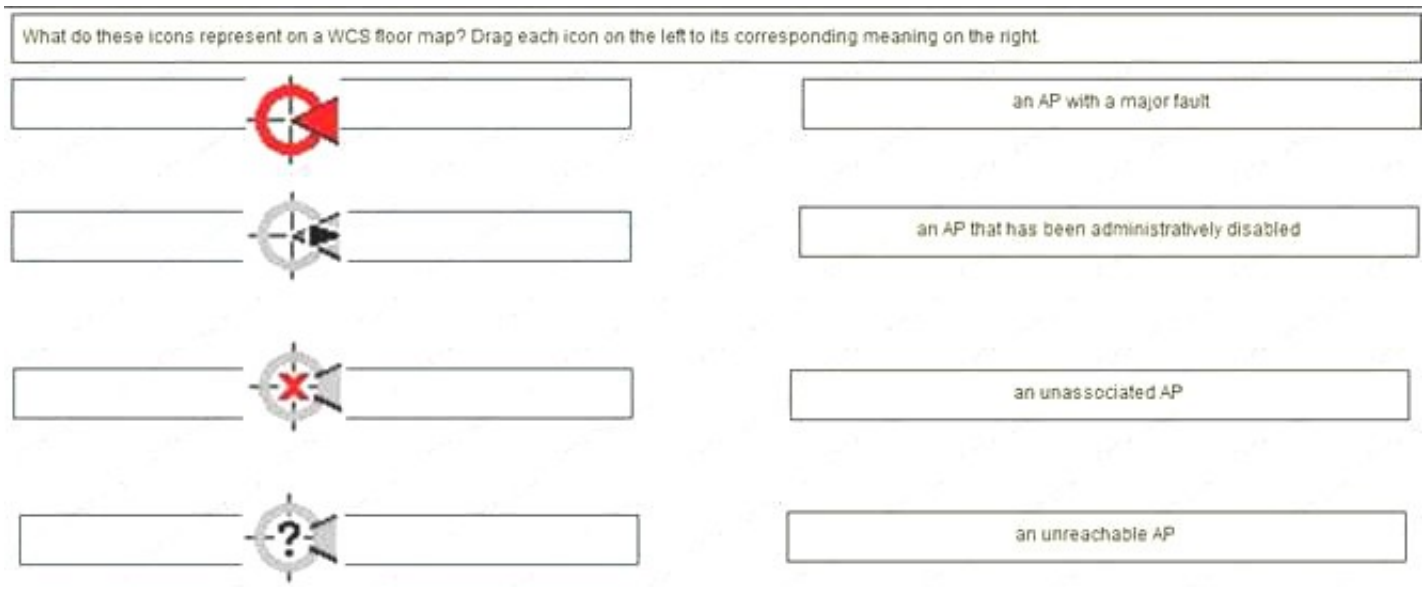


Answer:

Explanation:



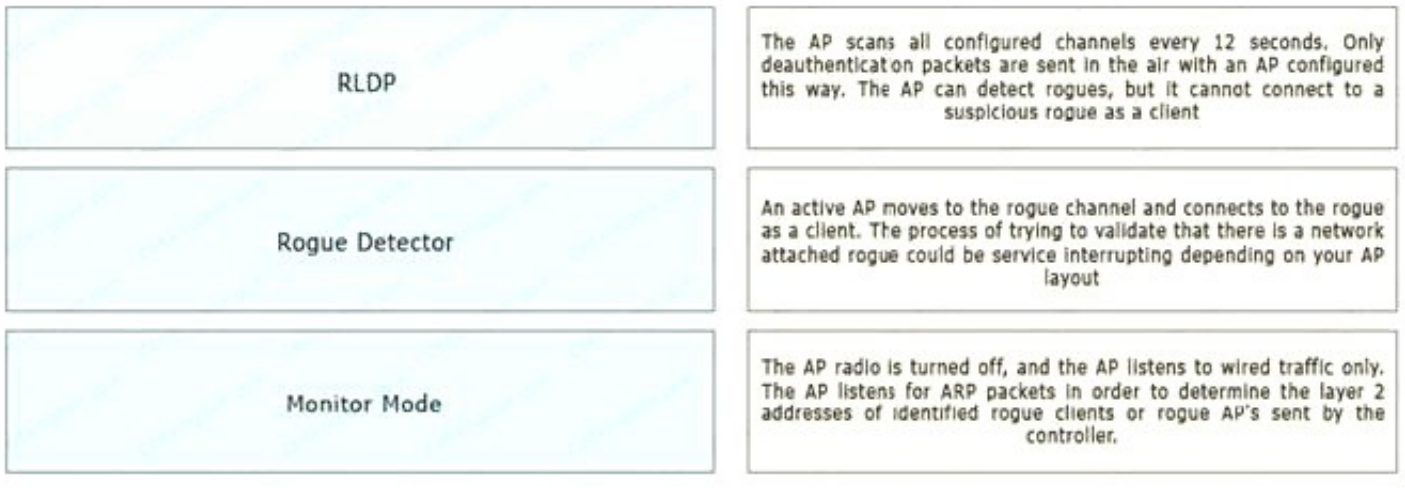
NEW QUESTION 296
DRAG DROP



Answer:

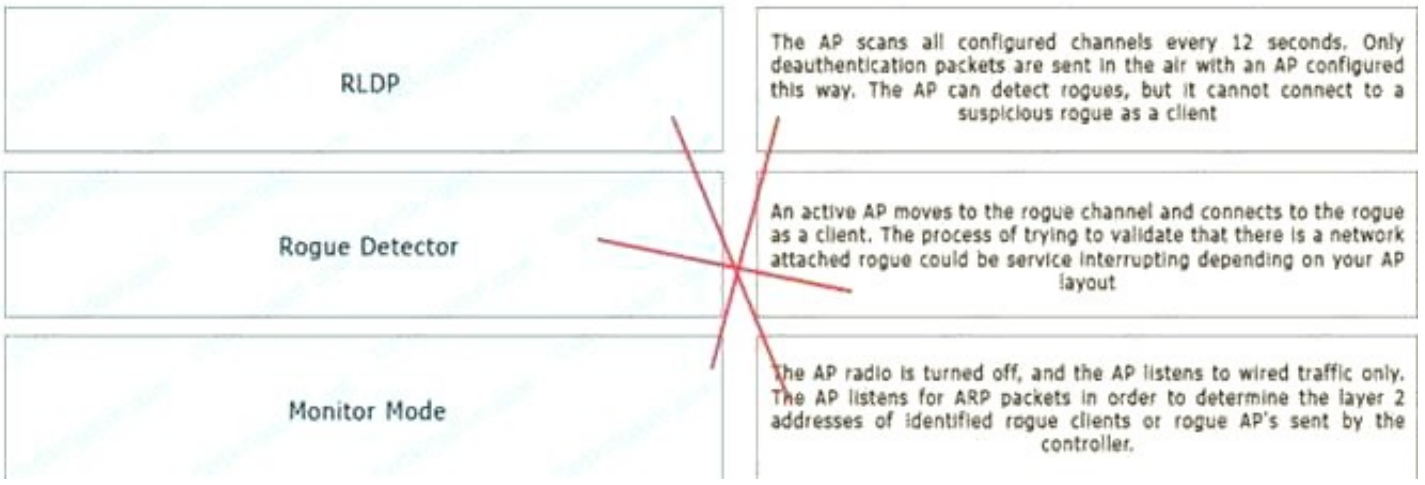
Explanation:
Reference: http://www.cisco.com/en/US/docs/wireless/wcs/7.0MR1/configuration/guide/maps.html#wp10758 63

NEW QUESTION 298
DRAG DROP
Drag and drop the rogue detection “technique” on the left to the appropriate description on the right.

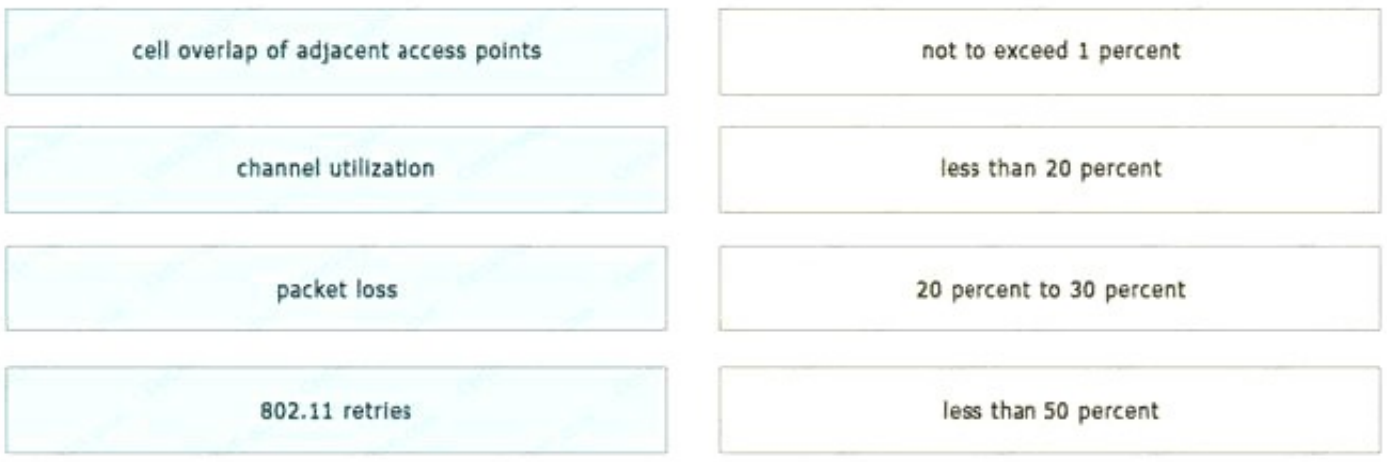


Answer:

Explanation:

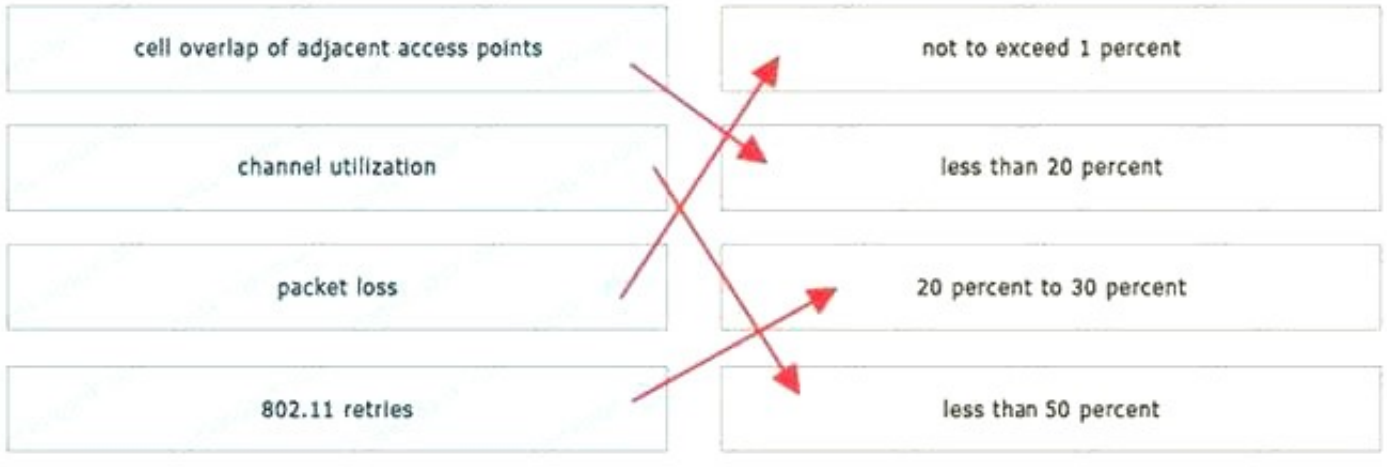


NEW QUESTION 301
DRAG DROP
Drag and drop the RF performance metric on the left to the threshold that is recommended to provide good voice over wireless performance on the right.



Answer:

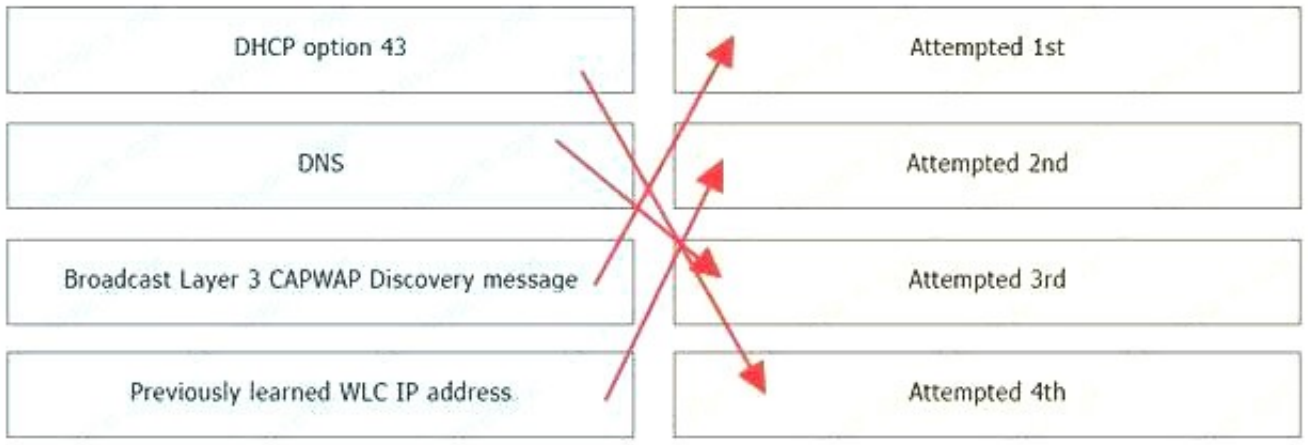
Explanation:



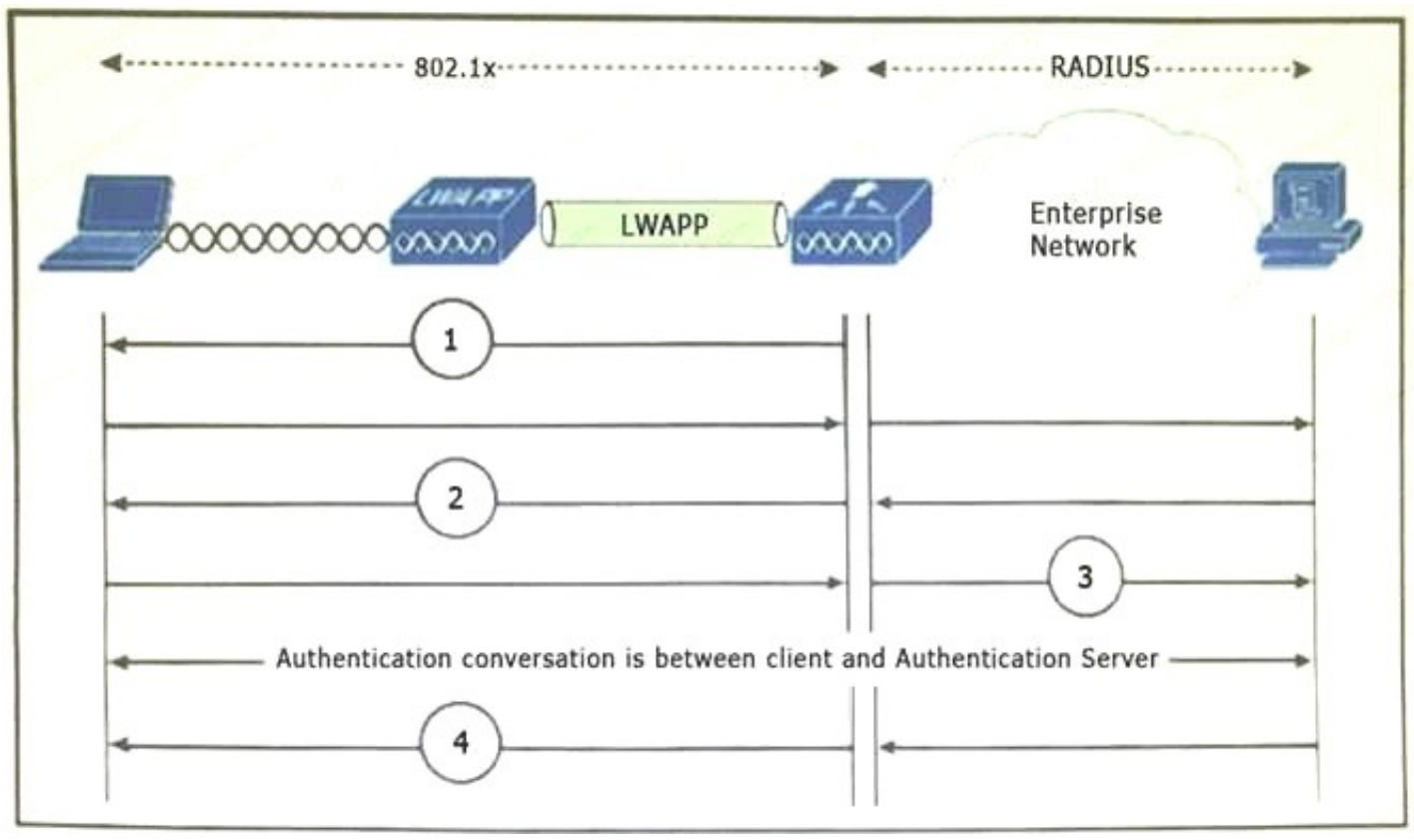
NEW QUESTION 303
DRAG DROP
Drag and drop the Cisco WLC discovery attempt method on the left to the correct order on the right.

Answer:

Explanation:



NEW QUESTION 305
DRAG DROP
Refer to the exhibit.

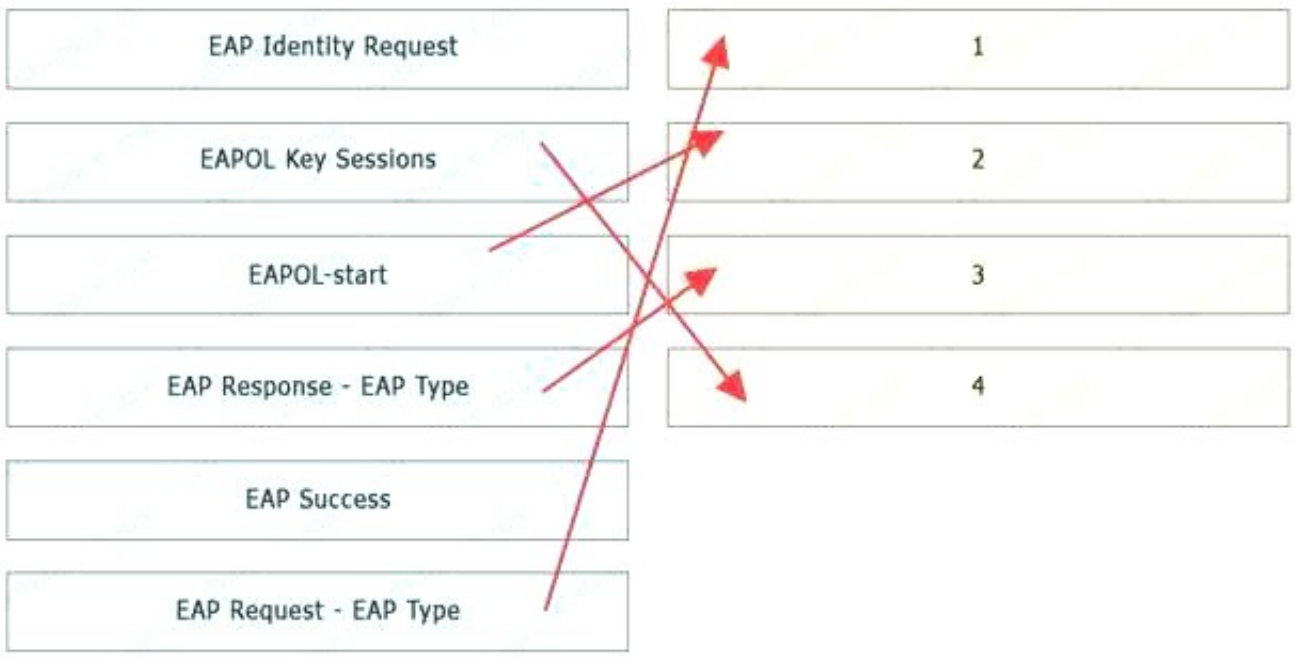


Drag and drop steps of the 802.1x authentication process on the left to the corresponding number on the right.

EAP Identity Request	1
EAPOL Key Sessions	2
EAPOL-start	3
EAP Response - EAP Type	4
EAP Success	
EAP Request - EAP Type	

Answer:

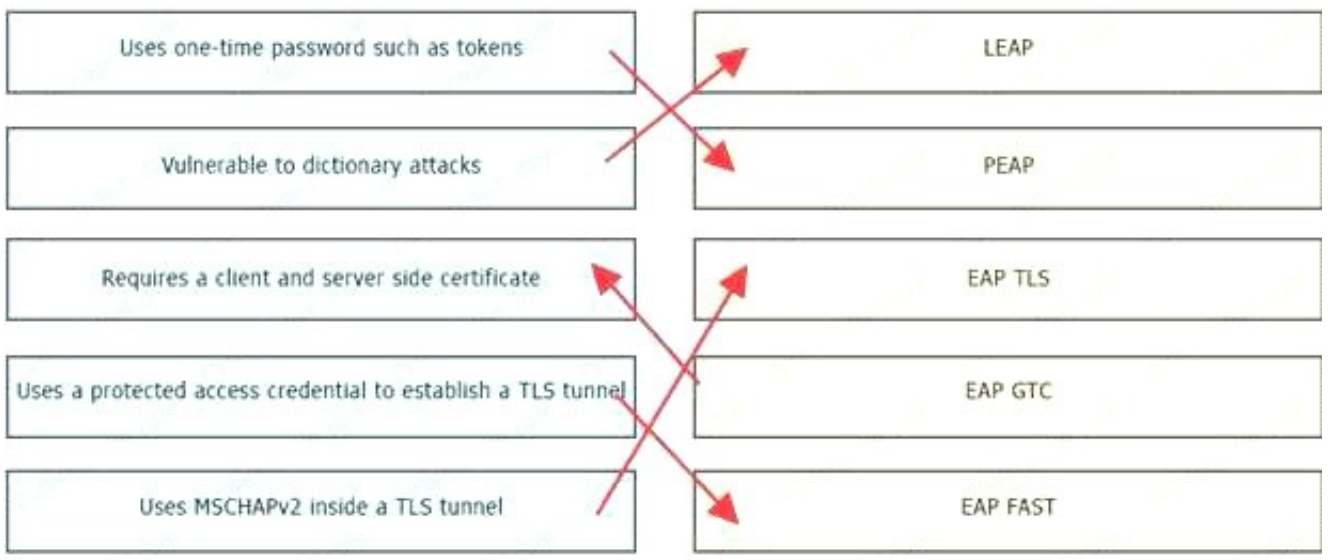
Explanation:



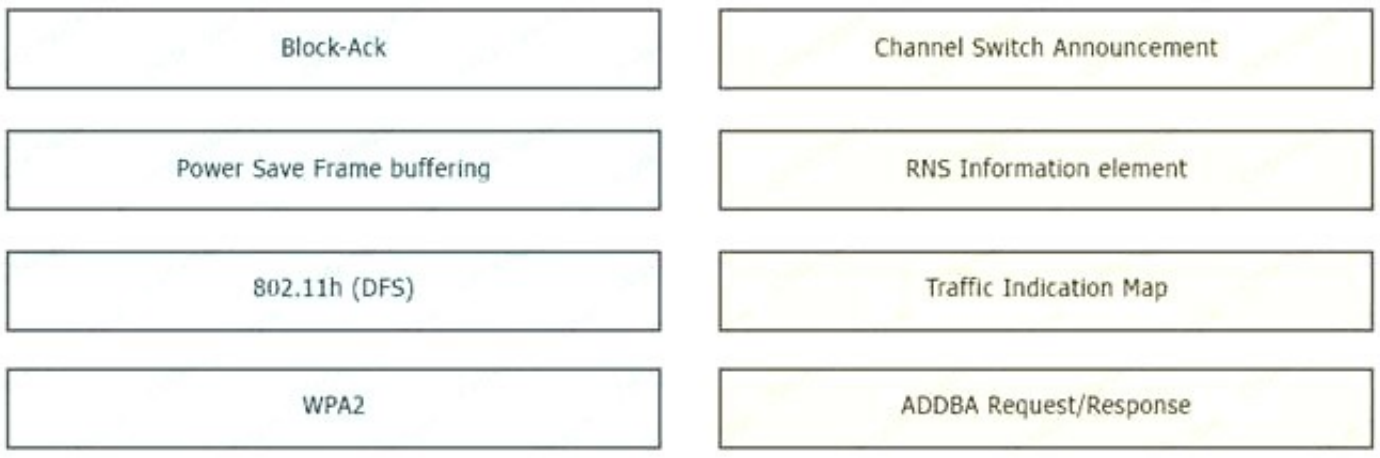
NEW QUESTION 306
DRAG DROP
Drag and drop the characteristic on the left to the appropriate EAP type on the right.

Answer:

Explanation:

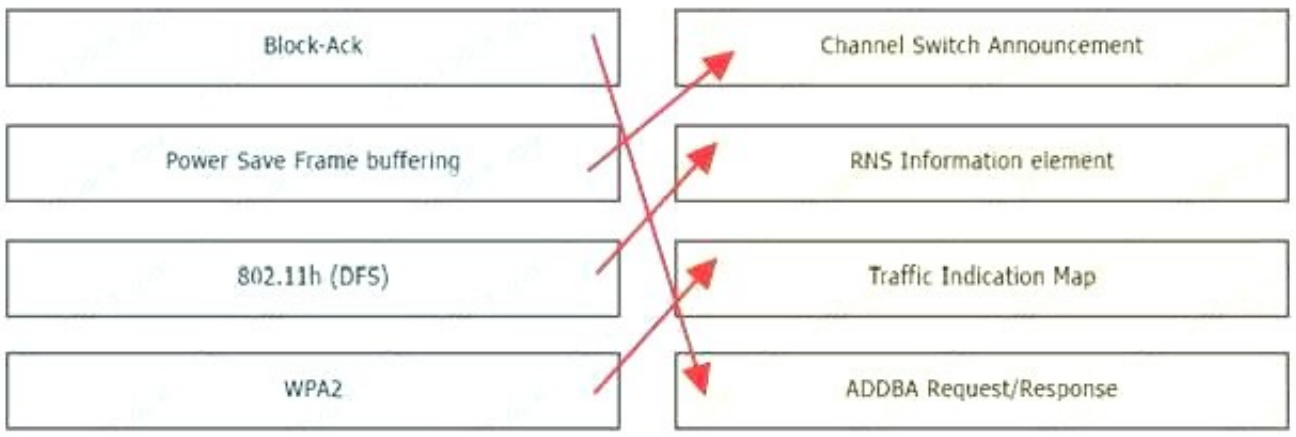


NEW QUESTION 307
DRAG DROP
Drag and drop the 802.11 technology feature on the left to the related frame type and IE on the right.

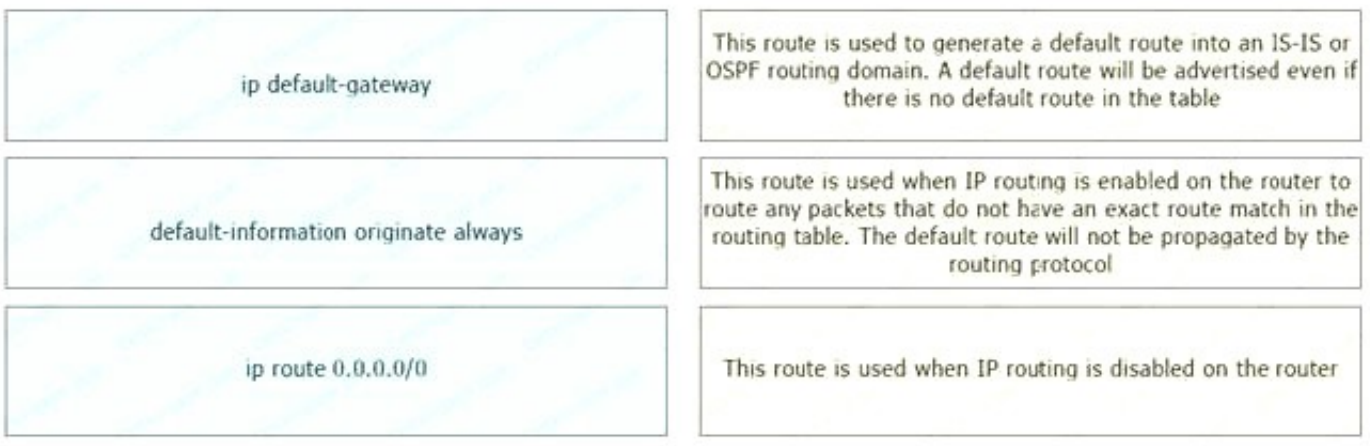


Answer:

Explanation:

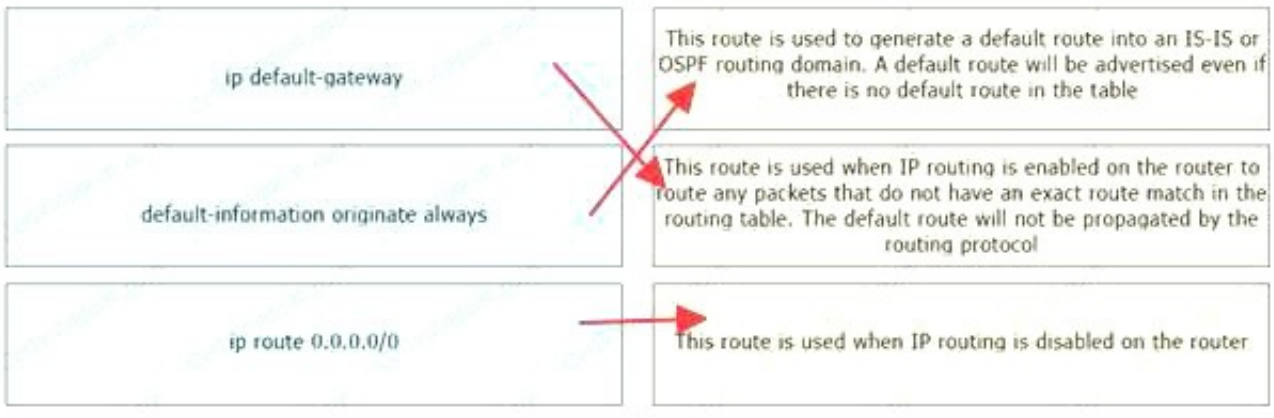


NEW QUESTION 308
DRAG DROP
Drag and drop the route type on the left to their intended usage on the right.



Answer:

Explanation:



NEW QUESTION 311
Refer to the exhibit.

```
(WLC) >show media-stream group details test

Media Stream Name..................................... test
Start IP Address...................................... 239.4.5.6
End IP Address........................................ 239.4.5.6
RRC Parameters
Avg Packet Size (Bytes)............................... 1200
Expected Bandwidth (Kbps)............................. 1500
Policy................................................ Admit
RRC re-evaluation..................................... periodic
QoS................................................... Video
Status................................................ Multicast-dir
Usage Priority........................................ 1
Violation............................................. drop
```

Which two statements are true based upon the output in the exhibit? (Choose two.)

A. Operation will be effective only if the video profile on the WLC is mapped to the 802.1p protocol with a tagged value of 5.
B. It is recommended to configure IP multicast on the WLC in multicast-multicast mode.
C. CAC must be enabled to avoid channel oversubscription and guarantee the configured media bandwidth.
D. In case of a violation after an RRC re-evaluation, the stream is demoted to the best-effort clas

Answer: B

NEW QUESTION 316
Which three options are valid AP modes for lightweight APS in the WLC 7.0.116 release? (Choose three.)

A. SE-Connect
B. WPS
C. RAM
D. OEAP
E. Rogue Detector
F. Sniffer

Answer: AEF

Explanation:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/7- 0MR1/configuration/guide/wlc_cg70MR1.pdf

NEW QUESTION 319
Which data rate mode allows the transmission of both unicast and multicast packets on a Cisco AP?

A. disabled mode
B. enabled mode
C. mandatory mode
D. multicast mode
E. supported mode

Answer: B

NEW QUESTION 324
Refer to the exhibit. Which two statements about this output are true? (Choose two.)

```
R1(config)# class-map match-any class1
R1(config-cmap)# match access-group 101
R1(config-cmap)# match protocol ip

R1(config-cmap)# exit
R1(config)# class-map class2
R1(config-cmap)# match access-group 102
R1(config-cmap)# match not protocol ip
R1(config-cmap)# exit
```

A. Unclassified traffic belongs to the traffic class default, and packets in this class are treated as FIFO.
B. For traffic to match class1, the traffic that is being evaluated must match one of the specified criteria.
C. For traffic to match class1, the traffic that is being evaluated must match both of the specified criteria.

D. Unclassified traffic will be dropped because no default class is create

Answer: B

NEW QUESTION 326
Why would you enable the RFC 3578 option when adding a new RADIUS authentication server to a WLC?

A. you want to run both RADIUS and TACACS
B. to support Disconnect and Change of Authorization
C. to encrypt communications between the WLC and the RADIUS server
D. to support RADIUS key wrapping

Answer: B

Explanation: If you are configuring a new RADIUS authentication server, choose Enabled from the Support for RFC 3576 drop-down list to enable RFC 3576, which is an extension to the RADIUS protocol that allows dynamic changes to a user session, or choose Disabled to disable this feature. The default value is Enabled. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session and supports disconnect and change-of-authorization (CoA) messages. Disconnect messages cause a user session to be terminated immediately where CoA messages modify session authorization attributes such as data filters.

NEW QUESTION 329
Refer to the exhibit. A wireless engineer at ACME Company is troubleshooting a wireless client that is unable to associate to a WLAN. What is likely the cause of the problem?

```
00:1b:77:42:07:69 Adding mobile on LWAPP AP 00:1c:b0:ea:5f:c0(0)
00:1b:77:42:07:69 Scheduling deletion of Mobile Station: (callerId: 24) in  5 seconds
00:1b:77:42:07:69 Association received from mobile on AP 00:1c:b0:ea:5f:c0
00:1b:77:42:07:69 STA - rates (8): 130 132 139 150 12 18 24 36 0 0 0 0 0 0 0 0
00:1b:77:42:07:69 STA - rates (12): 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
00:1b:77:42:07:69 Processing WPA IE type 221, length 24 for mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state AUTHCHECK (2)
00:1b:77:42:07:69 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state 8021X_REQD 3)
00:1b:77:42:07:69 apfPemAddUser2 (apf_policy.c:209) Changing state for mobile 00:1b:77:42:07:69: on AP
00:1c:b0:ea:5f:c0 from Probe to Associated
00:1b:77:42:07:69 Stopping deletion of Mobile Station: (callerId: 48)
00:1b:77:42:07:69 Sending Assoc Response to station on BSSID 00:1c:b0:ea:5f:c0 (status 0)
00:1b:77:42:07:69 apfProcessAssocReq (apf_80211.c:3838) Changing state for mobile 00:1b:77:42:07:69 on AP
00:1c:b0:ea:5f:c0 from Associated to Associated
00:1b:77:42:07:69 Creating a new PMK Cache Entry for station 00:1b:77:42:07:69 (RSN 0)
00:1b:77:42:07:69 Initiating WPA PSK to mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 dot1x - moving mobile
00:1b:77:42:07:69 into Force Auth state
00:1b:77:42:07:69 Skipping EAP-Success to mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 Sending EAPOL-Key Message to mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 Received EAPOL-KEY from mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 Received EAPOL_key in PKT_START state (message 2) from mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 Received EAPOL-key M2 with invalid MIC from mobile 00:1b:77:42:07:69
00:1b:77:42:07:69 802.1x 'timeoutEvt' Timer expired for station 00:1b:77:42:07:69
00:1b:77:42:07:69 Sent Deauthenticate to mobile on BSSID 00:1c:b0:ea:5f:c0 slot 0(caller 1x_ptsm.c:462)
00:1b:77:42:07:69 0.0.0.0 8021X_REQD (3) Change state to START (0) last state 8021X_REQD (3)
00:1b:77:42:07:69 0.0.0.0 START (0) Reached FAILURE: from line 3522
```

A. The AP CAPWAP tunnel is down, and is unable to handle any new connections.
B. The client is providing a wrong credential for dot1x authentication.
C. The WPA PSKs do not match.
D. The client uses WPA, but the AP is advertising only WPA2 support.
E. A firewall is blocking the ports that are necessary for the AP to join the WL

Answer: B

NEW QUESTION 330
You need to open the appropriate firewall port for RLDP. Which port must you open?

A. UDP 6352
B. UDP 5246
C. TCP 37540
D. TCP 8443
E. TCP 16113
F. UDP 16666

Answer: A

Explanation: Rogue Location Discovery Protocol (RLDP) is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs
an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends de-authentication messages to all connected clients and then shuts down the radio interface. Then, it associates to the rogue AP as a client. The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature.

NEW QUESTION 331
Refer to the exhibit. Which WLAN IDs will be advertised by an out-of-the-box AP that joins the WLC for the first time?

```
(Cisco Controller) >show wlan summary


Number of WLANs .....................................7
WLAN ID                 WLAN Profile Name / SSID                Status     Interface Name
-------     ------------------------------------             -------    -------------

5           Hidden / Hidden                                  Enabled      Vlan5
8           Guest / Guest                                    Enabled      Vlan8
12          Contractors/Contractors                          Disabled     Vlan12
15          IT / IT                                          Enabled      Vlan15
17          Finance / Finance                                Enabled      Vlan17
512         Marketing / Marketing                            Enabled      Vlan512
```

A. 5,8,12,15
B. 5,8,15
C. 8,15
D. 17,512
E. 8,15,17,512
F. 5,8,15,17,512

Answer: F

NEW QUESTION 332
Which two options are valid mobility roles in which a controller can operate in during a client mobility session? (Choose two.)

A. local
B. auto anchor
C. export anchor
D. mobility announcer

Answer: AC

NEW QUESTION 335
You are implementing a WLC at a remote site and want to make sure that you are able to sync up with the Cisco WCS at the central site. Which two statements about this process are true? (Choose two.)

A. If the WLC is behind a firewall, you must make sure that UDP ports 161 and 162 are open.
B. The Cisco WCS server does not need direct IP connectivity to the WLC.
C. Cisco WCS will not be able to communicate with the WLC if the WLC is behind a NAT device.
D. If the WLC is behind a NAT device, the WLC's dynamic AP-manager interface must be configured with the external NAT IP address.

Answer: AC

NEW QUESTION 338
You are conducting a site survey for a customer that is about to deploy Cisco wireless phones.
Which three recommendations apply? (Choose three.)

A. Minimum SNR should be 15 dB.
B. The minimum recommended wireless signal strength for voice applications is -71 dBm.
C. Minimum SNR should be 25 dB.
D. Wireless cell overlap should be 20 percent.
E. Minimum SNR should be 35 dB.
F. The minimum recommended wireless signal strength for voice applications is -57 dBm.
G. Wireless cell overlap should be 10 percent.
H. The minimum recommended wireless signal strength for voice applications is -67 dB

Answer: ADF

NEW QUESTION 341
Which two platforms provide hypervisor virtualization? (Choose two.)

A. DevStack
B. Docker
C. KVM
D. OpenStack
E. Xen

Answer: CE

NEW QUESTION 345
Which two characteristics of an IoT network are true? (Choose two.)

A. The transmission rate in an IoT network is consistent.
B. IoT networks must be designed for low-powered devices.
C. IoT networks use IS-IS for routing.
D. IoT networks are 100% reliable

E. loT networks are bandwidth constrained

Answer: BE

NEW QUESTION 347
In a typical three-node OpenStack deployment, which two components are part of the controller node? (Choose two)

A. Neutron Layer 3 agent
B. Neutron DHCP agent
C. Identity service
D. Neutron Layer 2 agent
E. Neutron server plugin

Answer: AD

NEW QUESTION 348
Which option is the common primary use case for tools such as Puppet. Chef. Ansible, and Salt?

A. network function visualization
B. policy assurance
C. Configuration management.
D. network orchestratio

Answer: C

NEW QUESTION 351
Which two actions will happen when a wireless client deploys a Layer 2 roam between two WLCs with management IP addresses on different IP subnets but dynamic interfaces in the same VLAN? (Choose two.)

A. The new WLC exchanges mobility messages with the original WLC and the client database entry is moved to the new WLC.
B. The original WLC marks the client with an "Anchor" entry in its own client database.
C. The client database entry is maintained on both the original and newWLCs.
D. The client database entry is removed from the original WLC once it has been entered into the new WLC.

Answer: AD

NEW QUESTION 355
Given: LAG bundles all distribution ports on a WLC into a single 802.3ad port channel.The system load-balances access points transparently to the user. question Which two items should be taken into consideration when configuring the neighbor Ethernet switch? (Choose two.)

A. The Cisco WLC relies on the neighbor switch to load-balance traffic across the EtherChanne
B. The Cisco WLC does not perform any EtherChannel load-balancing on its own.
C. LAG requires theEtherChannel to be configured for the "on" mode on the Catalyst switch.
D. LAG requires that the Catalyst switch be configured with CiscoPAg
E. Link Aggregation Control Protocol is not supported.
F. The load-balancing method configured on the Catalyst switch must be based on Layer 2, not Layer 3. Failure to follow this recommendation may result in problems with access point associatio

Answer: AB

NEW QUESTION 357
Which one of the following commands could limit WLC output from subsequent debug commands to show only information associated with a specific wireless client device that has the MAC address 00:0c:41:07:33:a6?

A. Debug mobility addr 00:0c:41:07:33:a6 enable
B. Debug mac addr 00:0c:41:07:33:a6
C. Debug mac addr 00-0c-41-07-33-a6 enable
D. Debug mobility addr 00:0c:41:07:33:a6

Answer: B

NEW QUESTION 360
Which description is true about NIC cards certified by Cisco Compatible Extensions?

A. They support Cisco Standards such as LEAP and EAP-FAST but not PEAP-MSCHAP
B. They are compliant with Cisco Compatible Extensions, but not with Wi-Fi
C. They support Cisco WLAN technology enhancements
D. They support 802.11 standards plus power management only

Answer: C

NEW QUESTION 362
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. DTPC
C. DCA and TPC
D. AKM

Answer: B

NEW QUESTION 366
For the following cipher suites, which were defined in the IEEE 802.11i-2004 standard and then again in the 802.11-2007 standard? Select all that apply.

A. TKIP
B. WEP-40
C. TCP-IP
D. WEP-104
E. AES-CCMP

Answer: ABDE

NEW QUESTION 369
While configuring Wireless Domain Services, which port is used for traffic between infrastructure APs and the WDS AP?

A. Generic Routing Encapsulation GRE which is IP protocol 47
B. UDP destination and source protocol Port 1812 (0x0714)
C. UDP destination and source protocol port 2887 (0x0B47) or Ethernet Type 34605 (0x872D)
D. UDP destination and Source Protocol Port 1645 (0x066D)

Answer: C

NEW QUESTION 373
Harry is a network engineer for a company, he is now upgrading a large autonomous WLAN deployment to LWAPP operation. He has successfully imported a X.509 self-signed certificate into the WLC. But, when he tries to add additional self-signed certificates, the WLC GUI reports a "Failed to Add entry" error.
Which command can diagnose the root cause of this problem?

A. Show wps summary
B. Show database summary
C. Show exlusionlist
D. Show sysinfo

Answer: B

NEW QUESTION 375
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'
B. 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)
C. The AP moves to the rogue channel and attempts to connect to the rogue as a clien
D. The AP then tries to obtain an IP address and forwards a UDP packet to the controller through the rogu
E. If the controller receives this packet, the network administrator is notified that a rogue AP has been discovered on the wired network
F. The AP detects a rogue client and then the network administrator is able to contain both the rogue AP and the rogue client
G. 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
H. The AP determines whether or not a rogue access point is on a trusted networ
I. It does not provide RF service of any kind but rather receives periodic rogue access point reports from thecontroller and sniffs all ARP packet
J. If it finds a match between an ARP request and a MAC address it receives from the controlle
K. It generates a rogue access point alert to the controller

Answer: B

NEW QUESTION 376
In order to provide end-to-end QoS, how to send traffic classification information between the LWAPP AP and the WLAN Controller?

A. LWAPP APs map the WMM CoS values of the client traffic to the Ethernet frames and the CoS value of the Ethernet frames sent to the AP to the WMM access categor
B. The switch upstream from the AP is responsible for converting between 802.1D classification and DSCP
C. LWAPP packets from the controller and the AP are marked by DSCP based on the DSCP of the tunneled traffi
D. This DSCP is converted to a CoS by a table in the A
E. The access category used for each frame depends on the table CoS and QoS profile of the WLAN
F. There is no end-to-end QoS, only WMM on the WLA
G. This is all that is required, because campus networks typically have greater than 1 Gb/s backbones and WLANs operate at only 11 or 54 Mb/s
H. The WMM CoS values are carried within the LWAPP tunnels and translated from CoS to DSCP to ensure that the correct priority is given to different LWAPP packets

Answer: B

NEW QUESTION 380
Which three devices historical locations can be tracked by the Cisco Location Appliance? (Choose three.)

A. Remote sources of ISM interference
B. Rogue access points
C. 802.11-based RFID Asset tags
D. Trusted and Rogue clients

Answer: BCD

NEW QUESTION 385
Assuming that the antenna system characteristics (for example, gain VSWR, polarization and beam width) are similar for a 5-GHz and 2.4-GHz radio. While conducting a dual band site survey, how to configure the 5-GHz radio, relative to the 2.4-GHz radio, in order to achieve similar cell size?

A. The 5-GHz radio power level should be higher than the 2.4-GHz radio
B. The 5-GHz radio should use BPSK modulation and the 2.4 GHz radio should use CCK modulation
C. The 5-GHz radio power level should be lower than the 2.4-GHz radio
D. The 5-GHz radio should use CCK modulation and the 2.4-GHz radio should use BPSK modulation

Answer: A

NEW QUESTION 388
Which organization is a consortium of industry leaders in switching and wireless, silicon, and other technology areas working to deliver Multigigabit Ethernet speeds over existing cabling?

A. Ethernet Alliance
B. Wi-Fi Alliance
C. mGig Consortium
D. NBASE-T Alliance

Answer: D

NEW QUESTION 390
In a Cisco Prime Infrastructure High Availability deployment which model allows the use of a single IP address for system management and allows network devices to use that single IP address for SNMP trap and other notifications?

A. campus
B. local
C. branch
D. remote

Answer: A

NEW QUESTION 394
You must configure user management access on Cisco Prime Infrastructure Each user that requires access belongs to a department and each department needs to have specific access. Which configuration in Cisco Prime is the best way to easily administer these users?

A. Configure user groups
B. Create one user account for each department and each department shares it internally
C. Create virtual domains
D. Configure access for each user individually

Answer: C

NEW QUESTION 398
With RF group "auto mode", the Cisco WLCs dynamically form an RF neighborhood and elect an RF group leader to maintain a master power and channel scheme for the group For this to work access points on different Cisco WLCs must hear validated neighbor messages at a minimal signal strength What is the minimum signal strength?

A. -67dBm
B. -70 dBm
C. -80dBm
D. -90 dBm

Answer: C

NEW QUESTION 399
A corporation has hired you to understand more about the Fastlane feature on the Cisco wireless LAN controller because the majority of the clients in their network are iOS and Mac OS devices Which statement do you mark as a correct explanation of this feature, on software version 8 3 or above?

A. Enabling Fastlane on a SSID automatically creates a new EDCA profile named "Fastlane" which applies to the 5 GHz band only
B. Enabling Fastlane on a SSID automatically creates a new AVC profile which ensures appropriate QoS marking for well-known applications such as Lync and WebEx
C. Enabling Fastlane on a SSID automatically creates and applies a new AVC profile which ensures appropriate QoS marking for well-known applications such as Jabber and WebEx
D. An EDCA profile must be manually set to Voice and Video optimized when the Fastlane feature is enabled on a SSID

Answer: A

NEW QUESTION 400
You notice error messages that say that the broadcast'multicast queue on your Cisco 5508 WLC is full You have several gateways present in the client subnet and this subnet is IPv6-enabled No multicast application is being used You want to fix this problem without reducing the amount of features on your network Which action can help mitigate this problem?

A. Enable RA throttling on the WLC
B. Disable broadcast on the WLC
C. Disable multicast on the WLC
D. Enable mDNS snooping on the WLC

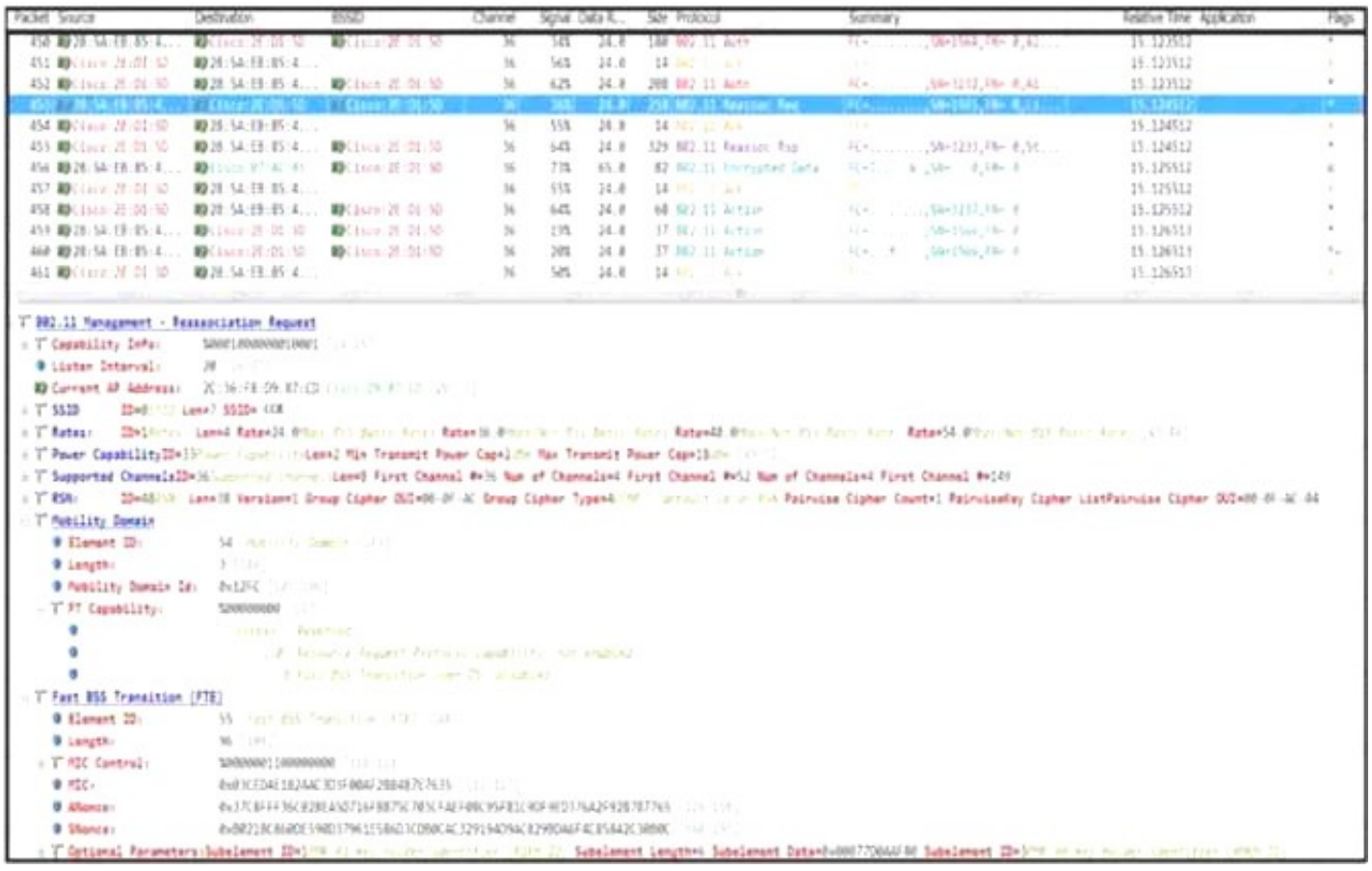
Answer: A

NEW QUESTION 403
A wireless engineer has completed the configuration of the QoS profiles on the WLC and has assigned them to the WLANs The engineer applies the profiles, tests them, and notices that traffic is blocked for some of the WLANs. Which problem is true?

A. The QoS profiles have 802 1p tagging disabled and the WLANs that are assigned use tagged interfaces on the controller.
B. The QoS profiles and the traffic restrictions of the WLANs are different
C. The QoS profiles have 802 1p tagging configured, and the WLANs that are assigned use untagged interfaces on the controller.
D. AVC must be enabled for the QoS profiles to work property

Answer: A

NEW QUESTION 407
Refer 10 the exhibit.



You are the network administrator at a corporation and you are trying to troubleshoot a Fast BSS transition issue for a client You have received the snapshot of the packet capture Based on your analysis of this packet capture which statement is true?

A. The packet capture shows that client cannot use any Fast BSS transition methods
B. The packet capture is for the initial association of the client with an AP supporting 802 11r-based Fast BSS transition
C. The packet capture shows the Fast BSS transition over the air
D. The packet capture shows Fast BSS transition over the DS, authentication packets are sent at basic rate of 36 Mbps.

Answer: D

NEW QUESTION 411
A wireless engineer must configure bandwidth-based admission control on the company WLC for video applications. After applying the necessary configuration changes to the corporate WLAN, the engineer notices that the bandwidth is not being allocated correctly Which problem is true"?

A. Only CCX v2 clients were connected to the WLAN at the time of the testing
B. An AVC profile must be assigned to the WLAN for the admission control to work properly
C. Admission control cannot work with 802.1X security
D. The WLAN must have gold QoS configured

Answer: D

NEW QUESTION 415
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

400-351 Practice Exam Features:

* 400-351 Questions and Answers Updated Frequently

* 400-351 Practice Questions Verified by Expert Senior Certified Staff

* 400-351 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 400-351 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year