Cisco

Exam 400-351

CCIE Wireless (v3.1)

Verson: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Exam Set 1	5
Topic 2: Exam Set 2	5

Topic 1, Exam Set 1

Question No : 1 - (Topic 1)

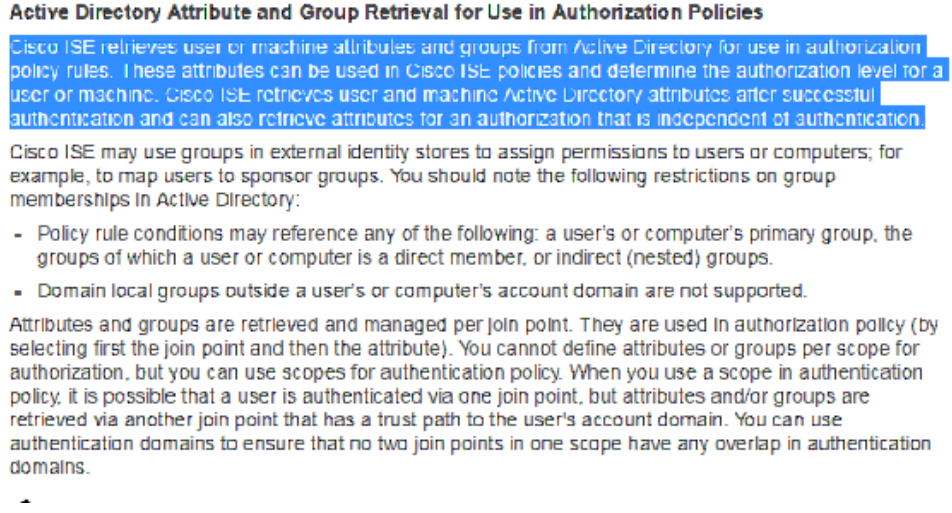
Which option in the Cisco Identity Services Engine checks that the user authentication comes from a domain computer?

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 check.

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_ISE-ADIntegration.html

Question No : 2 - (Topic 1)

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

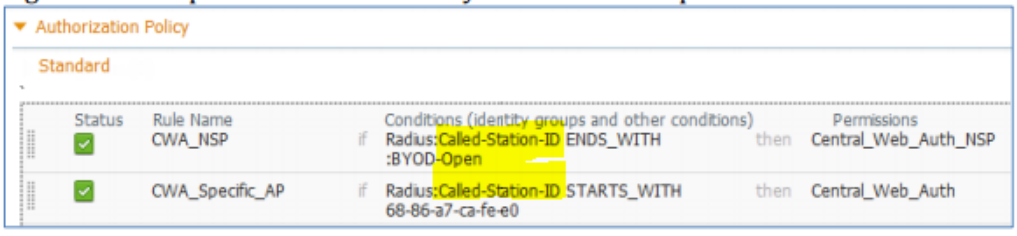
A. RADIUS attribute [31] Calling-Station-Id

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: D,F

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

Question No : 3 - (Topic 1)

With the introduction of mDNS policies in AireOS release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in which location. Based on user 802.lx authentication. aAAA server/lSE can be configured to return which two possible values in the form of a "CISCO-AV-PAIR"? (Choose two.)

A. Client-role
B. User-role
C. User-ID
D. Bonjour-profile
E. Client-location

Answer: B,D

Explanation:

Information about Bonjour gateway based on access policy

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself for which you need not even enable multicast on the controller. The WLC explores all Bonjour discovery packets and does not forward them on AIR or Infra network.

Bonjour is Apple's version of Zeroconf - it is Multicast Domain Name System (mDNS) with DNS-SD (Domain Name System-Service Discovery). Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique). To address this issue Cisco WLC acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc) from the source/host e.g. AppleTV and responds to Bonjour clients when they ask/request for a service.

Bonjour gateway has inadequate capabilities to filter cached wired or wireless service instances based on the credentials of the querying client and its location.

Currently the limitations are:

- Location-Specific Services (LSS) filters the wireless service instances only while responding to a query from wireless clients. The filtering is based on the radio neighborhood of the querying client.
- LSS cannot filter wired service instance because of no sense of location.
- LSS filtering is per service type and not per client. It means that all clients receive the location based filtered response if LSS is enabled for the service type and clients cannot override the behavior.
- There is no other filtering mechanism based on client role or user-id.

The requirement is to have configuration per service instance.

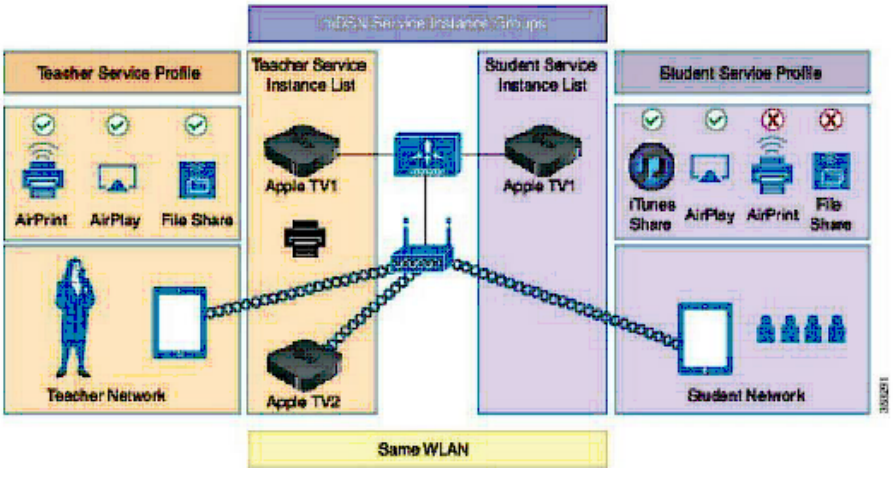
Following are the three criteria of the service instance sharing:

- User-id
- Client-role
- Client location

Introduction to Bonjour Policies and New Requirements

Enterprise credentials of Bonjour are poor and hence the advent of Bonjour gateway. Bonjour gateway snoops and caches Bonjour services across VLANs and periodically refreshes the same. WLC acts as a proxy for all Bonjour services published by wireless and wired devices. Bonjour gateway as of release prior to 8.0 had inadequate capabilities to filter cached wired / wireless service instances based on the credentials of the querying client and its location.

With introduction of the Bonjour policies in the release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in what location (all this applies to the same WLAN). With introduction of the Bonjour policies, the administrator does not need to create multiple WLANs to select which services are allowed or should be used on specific WLAN. Based on user 802.1x authentication, the AAA server or ISE can be configured to return USER-ROLE or BONJOUR-PROFILE in the form of the "CISCO-AV-PAIR". This value gets plumbed into the policy created on the wireless controller. Based on the user authentication, a configured policy and profile are applied to a specific user on the same WLAN.



http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/WLAN-Bonjour-DG.html

Question No : 4 - (Topic 1)

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 control.

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

220352

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/emob41dg-wrapper/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/c41ccfg.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%

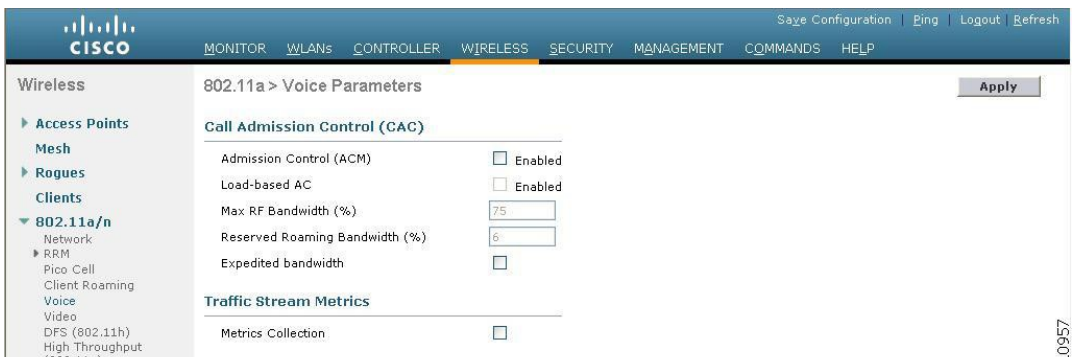
To enable expedited bandwidth requests, check the Expedited Bandwidth check box. The default value is disabled.

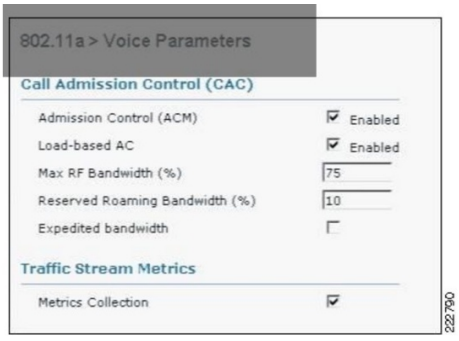
To enable TSM, check the Metrics Collection check box. The default value is disabled. Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.

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.pdfQUESTION NO:

Question No : 5 - (Topic 1)

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 controller. This information is not available on the controller policy type. Access VLAN. VLAN name, supported rates. Encryption ciphter.
B. In connected mode, the access point provides minimal information about the locally authenticated client to the controller. However, this information is available to the controller policy type., access VLAN, VLAN name, supported rates, encryption cipher.
C. 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.
D. 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.
E. Local authentication in connected mode does not require any WLAN configuration.
F. Local authentication can be enabled only on the WLAN of a FlexConnect AP that is in

local switching mode.

Answer: A,C,F

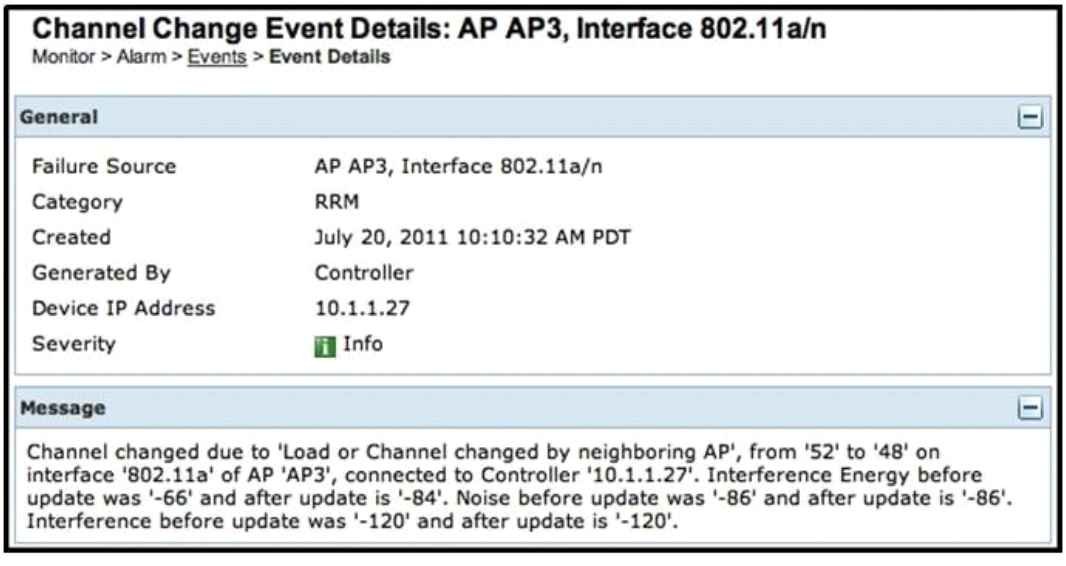
Explanation:

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

Topic 2, Exam Set 2

Question No : 6 - (Topic 2)

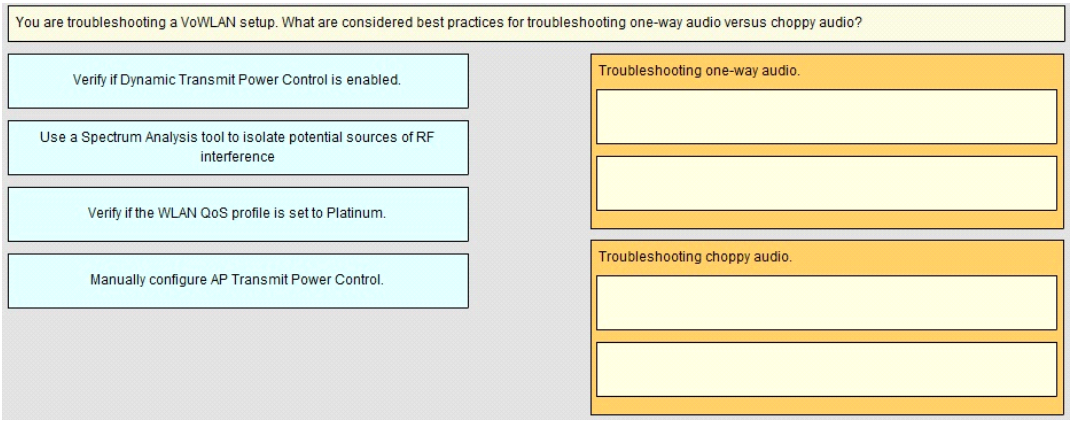
Refer to the exhibit. Which statement about the Cisco WCS RRM event message is true?



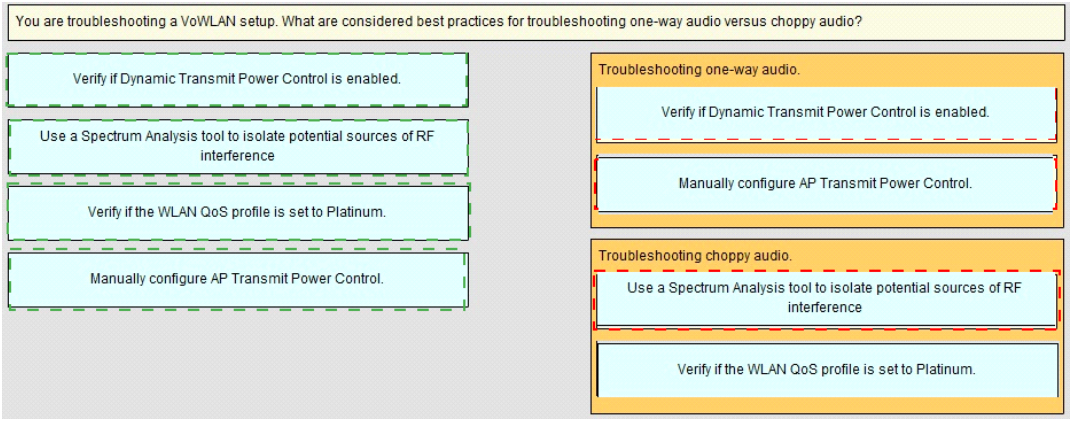
A. Excessive non-802.11 interference caused the channel change.
B. An event-driven RRM caused the channel change.
C. A CleanAir AP detected a persistence interferer and forced an RRM channel reassignment.
D. Two adjacent APs on the same channel caused a signal collision.

Answer: A

Question No : 7 DRAG DROP - (Topic 2)

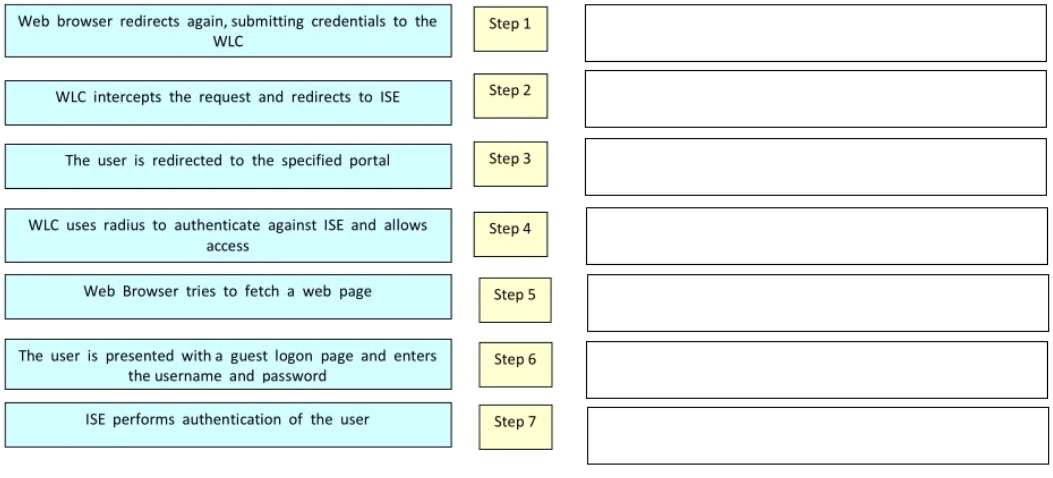


Answer:

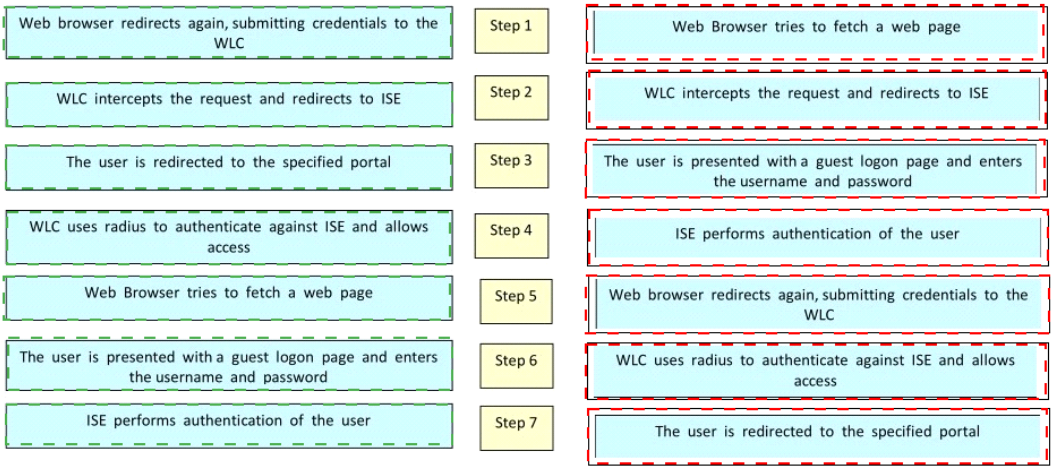


Question No : 8 DRAG DROP - (Topic 2)

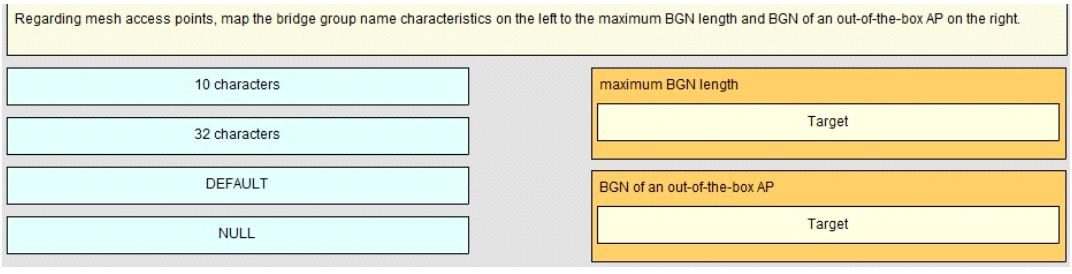
You are authenticating users using LWA and ISE guest portal. Drag and drop the step in the process on the left into the correct order on the right ?



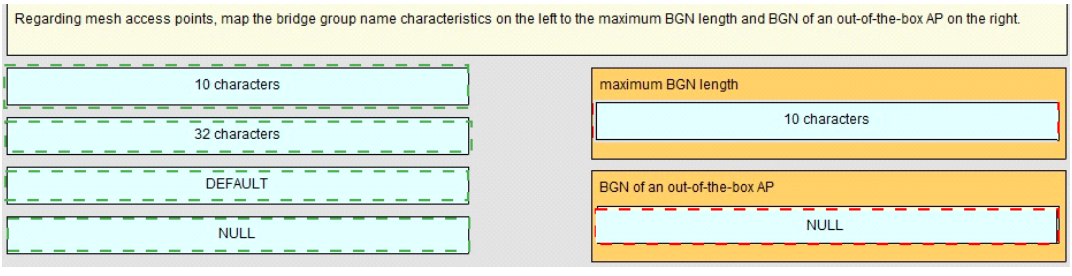
Answer:



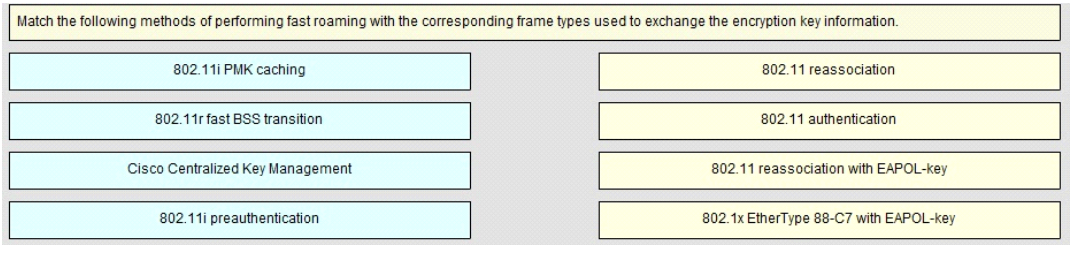
Question No : 9 DRAG DROP - (Topic 2)



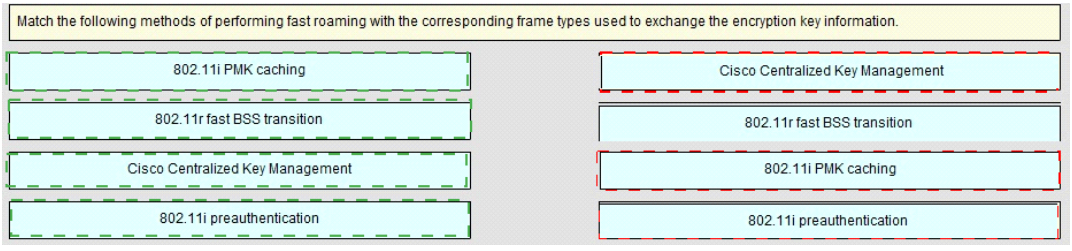
Answer:



Question No : 10 DRAG DROP - (Topic 2)



Answer:


Match the following methods of performing fast roaming with the corresponding frame types used to exchange the encryption key information.
802.11i PMK caching
802.11r fast BSS transition
Cisco Centralized Key Management
802.11i preauthentication
Cisco Centralized Key Management
802.11r fast BSS transition
802.11i PMK caching
802.11i preauthentication