640-722 Q&As

Implementing Cisco Unified Wireless Networking Essentials v2.0

Pass Cisco 640-722 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/640-722.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

Which Cisco program for WLAN client vendors helps to ensure that their devices are interoperable with Cisco WLAN infrastructure?

A. CCX

B. CCMP

C. ASDM

D. WLSE

Correct Answer: A

IEEE and industry standards define how a Wi-Fi radio interoperates with a wireless LAN infrastructure, and the Wi-Fi CERTIFIEDTM seal ensures interoperability. For many organizations that rely on mobile computers, however, Wi-Fi CERTIFIED is not enough. These organizations need assurance that their mobile computers will interoperate with a Cisco wireless LAN infrastructure and support Cisco wireless LAN innovations for enhanced security, mobility, quality of service, and network management. The Cisco Compatible seal gives organizations the assurance that they seek. A mobile computer earns the Cisco Compatible seal through a program called Cisco Compatible Extensions, or CCX. Like the Wi-Fi certification program, CCX:

Includes a specification that defines a set of features that must be implemented in the hardware and software for a Wi-Fi radio or a device that uses a Wi-Fi radio.

Requires compliance testing conducted by an independent lab that is approved by the organization that manages the program.

Requires that a submitted radio or device pass all tests to be approved.

The CCX specification is a superset of that used for Wi-Fi certification. In fact, a device cannot be certified for CCX unless it, or the Wi-Fi radio inside it, is Wi-Fi CERTIFIED.

Reference: http://www.digikey.com/Web%20Export/Supplier%20Content/Laird_776/PDF/laird-wireless-value-cisco-compatible-extenstion.pdf?redirected=1

QUESTION 2

Refer to the exhibit.

What is the meaning of the inverted orange triangle (marked "0") in the Alarm Summary tab of Cisco WCS?

A. number of major alarms

B. number of minor alarms

C. number of critical alarms

D. number of system alarms

Correct Answer: A

Alarms are color coded as follows:

Red -- Critical Alarm

Orange -- Major Alarm

Yellow -- Minor Alarm The Alarm Summary displays the number of current critical, major, and minor alarms. Reference: http://www.cisco.com/c/en/us/td/docs/wireless/wcs/6-0/configuration/guide/WCS60cg/6_0event.html

QUESTION 3

Which option describes why most wireless phones and tablets do not use 802.11a/n and 40 MHz channels?

A. a lack of radio range when using these radios

B. a lack of device battery capacity to operate concurrent a/b/g/n radios

C. a lack of cooling in the device necessary to operate these radios

D. These radios would require the devices to be larger.

Correct Answer: B

A different receiver is needed for each 802.11a, b, g, and n radios, so using all simultaneously would severely impact the overall battery life of a mobile device.

QUESTION 4

When using multiple SSIDs on a lightweight AP, how does the traffic of each SSID reach the 802.3 network?

A. provide routing between them at the core so that the SSIDs can reach the internet

B. configure 802.11q trunking on the Ethernet switch port that is connected to the AP

C. configure ACLs at the switch port that will allow all desired SSIDs to pass traffic

D. configure the SSIDs on the WLC and it will regulate the traffic based on traffic type

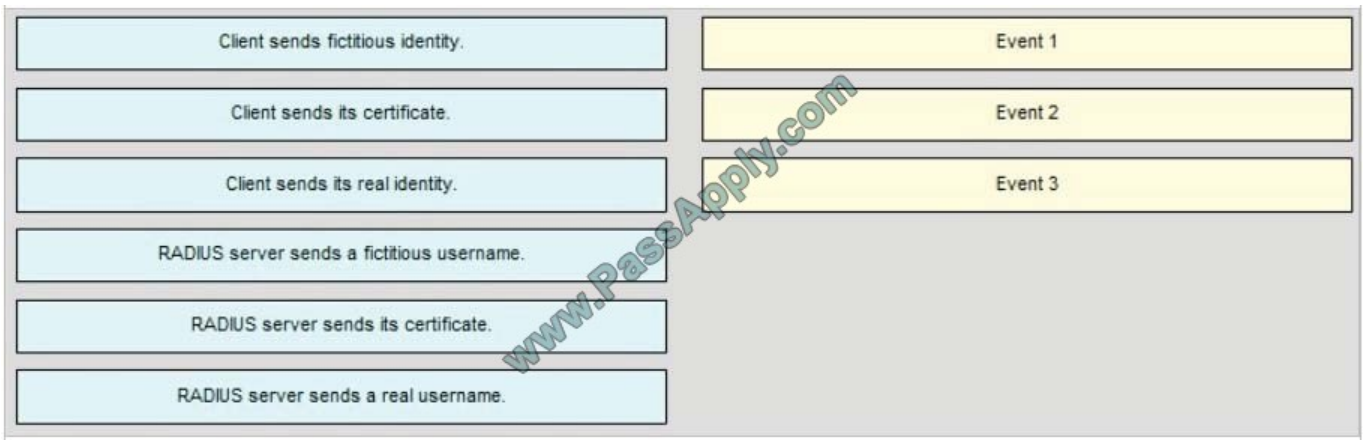
Correct Answer: B

QUESTION 5

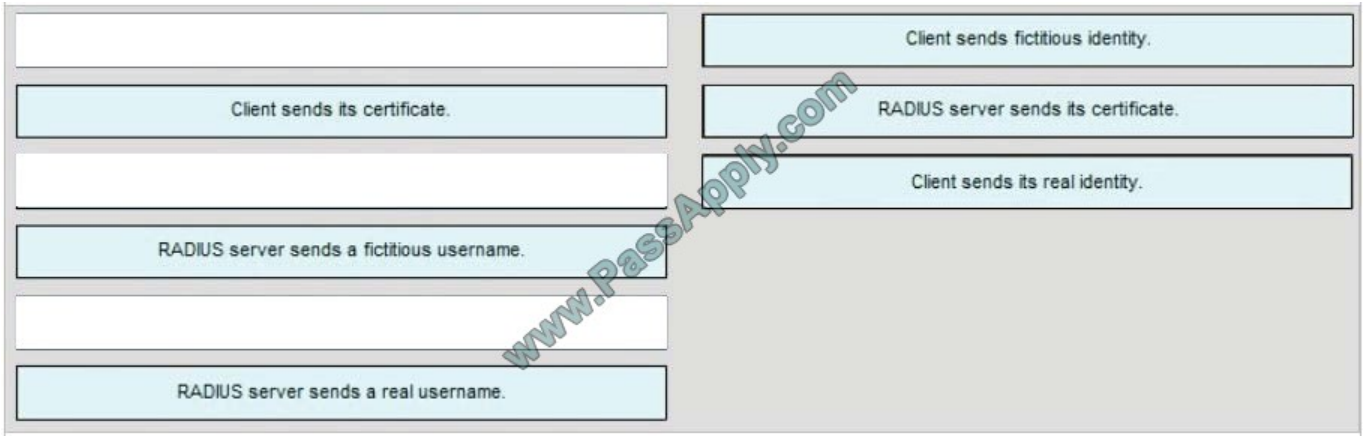
DRAG DROP

Drag the appropriate EAP descriptions on the left and drop them in the correct sequence of events for PEAP on the right.

Select and Place:



Correct Answer:



QUESTION 6

Which two statements about the Cisco WLC and AP code upgrade when 7.0 is running are true? (Choose two.)

A. The AP can download and run new code only after a Cisco WLC reboot causes the AP discovery and join.

B. The AP can download new code before the Cisco WLC reboot, but only if the AP is configured the CLI via SSH.

C. The AP can download new code before Cisco WLC reboot if it is configuring the Cisco WLC directly using the GUI via HTTP or HTTPS.

D. The Cisco WLC defaults to booting newer code, but it can boot older backup code only from the CLI configuration.

E. The Cisco WLC can boot either primary or backup code configured from the GUI.

F. The Cisco WLC can download only a single code at a time for reboot.

Correct Answer: CE

Each Cisco WLC can boot off the primary, last-loaded OS image or boot off the backup, earlier- loaded OS image. In order to change a Cisco WLC boot option, issue the config boot command. By default, the primary image on the controller

will be chosen as the active image.

Examples

> config boot primary

> config boot backup

In order to configure the boot order using the WLC GUI, complete these steps:

From the WLC GUI, navigate to the Commands page.

From the Commands on the left, click Config Boot. The Config Boot Image page appears.

This page displays the Primary and Backup images presently available on the controller, and also indicates the Active image. In order to change the Active image, select the desired image from the image drop-down menu and click Apply.

In this example, Backup is selected.

Save the configuration and reboot.

When the WLC reboots and comes back up, it will boot with the backup image.

Reference: http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/107530-backup-image-wlc.html

QUESTION 7

When a wireless client is authenticated in a controller-based wireless network, which three pieces of source identification information can be used by the controller for an Access-Request message that is sent to an external RADIUS server? (Choose three.)

A. wireless client IP address

B. controller IP address

C. AP IP address

D. wireless client MAC address

E. controller MAC address

F. AP MAC address

Correct Answer: BEF

From the Call Station ID Type drop-down list, choose IP Address, System MAC Address, or AP MAC Address to specify whether the IP address, system MAC address, or AP MAC address of the originator will be sent to the RADIUS server in the Access-Request message.

Reference:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70sol.html#wp1389032 (Step 3)

QUESTION 8

Refer to the exhibit.

Which syslog facility option is shown?

A. an information field, which is added to every message that comes from the WLC

B. a security feature, which is set on the syslog server

C. the type of syslog server

D. the Cisco WLC identifier for this syslog server

Correct Answer: A

A facility level is used to specify what type of program is logging a message. This lets the configuration file specify that messages from different facilities will be handled differently. Local7 maps to Facility level 23, which is local so the WLC will add this information to syslog messages when sending to the syslog server.

QUESTION 9

Refer to the exhibit.

What does the yellow shield with the exclamation mark indicate?

A. The network uses open authentication and no encryption.

B. The network uses an unsupported channel.

C. The signal is too distorted to connect.

D. The AP that is transmitting this SSID uses the wrong RF domain.

E. This is the ad-hoc network.

Correct Answer: A

an exclamation mark inside a yellow shield is displayed if the SSID has no security [Open authentication, no encryption]), clicking Connect and completing the security parameters when applicable.

QUESTION 10

Which two statements about the requirements to configure inter-controller roaming are true? (Choose two.)

A. The same mobility domain names are configured across controllers.

B. The same RF group names are configured across controllers.

C. The same controller hardware version is configured across controllers.

D. The same AP manager interface is configured across controllers.

E. The same virtual interface is configured across controllers.

F. The same controller software version is configured across controllers.

Correct Answer: AE

All controllers must be configured with the same mobility group name.

All controllers must be configured with the same virtual interface IP address.

If necessary, you can change the virtual interface IP address by editing the virtual interface name on the Controller > Interfaces page. If all the controllers within a mobility group are not using the same virtual interface, inter- controller roaming

may appear to work, but the handoff does not complete, and the client loses connectivity for a period of time.

Reference: http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-0/configuration/guide/c70/c70mobil.html

QUESTION 11

What tab contains access point configuration in the WCS?

A. Controller > Access Points

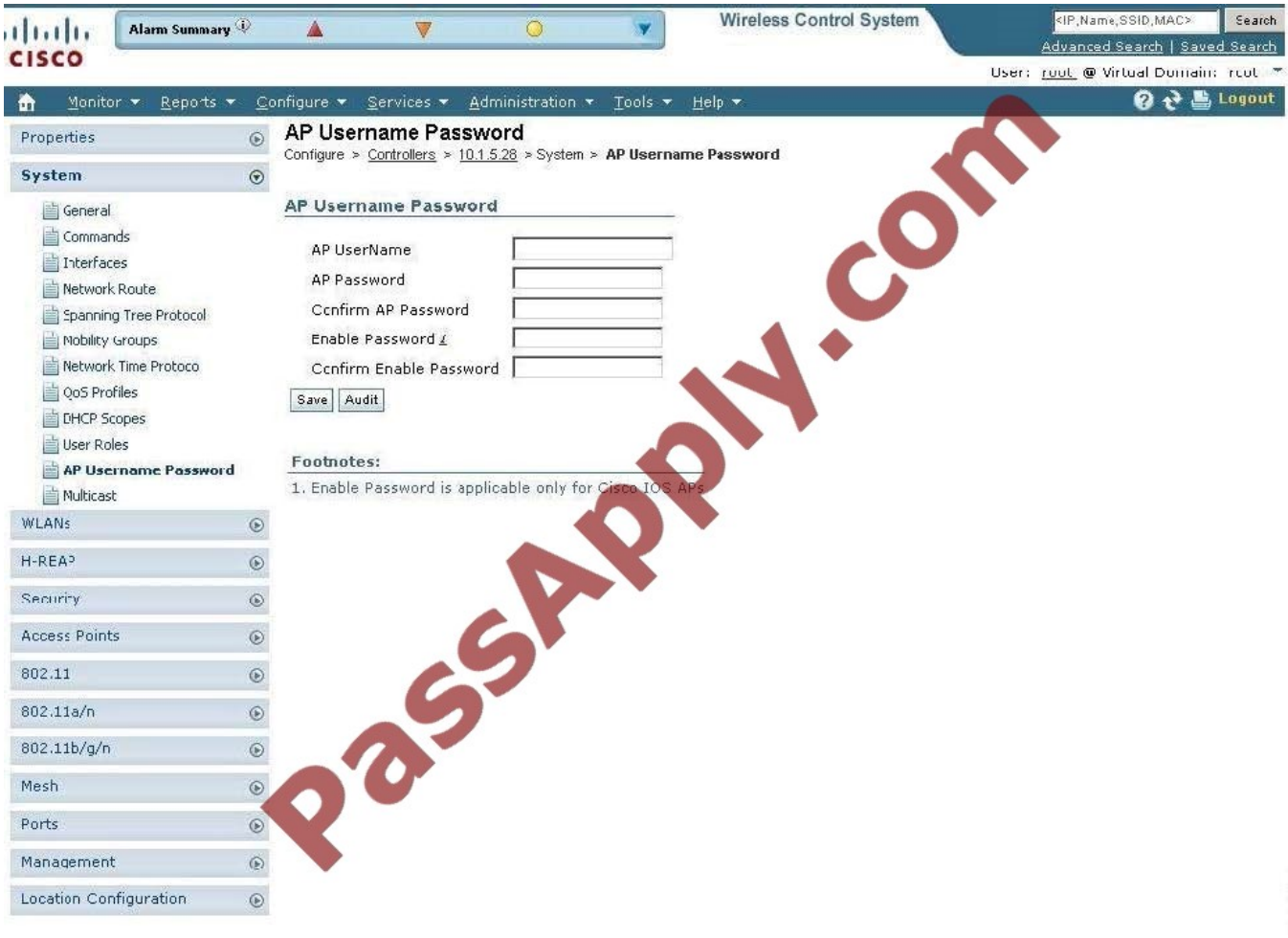
B. Configure > Access Points

C. General > Configure > Access Points

D. System > Configure > Access Points

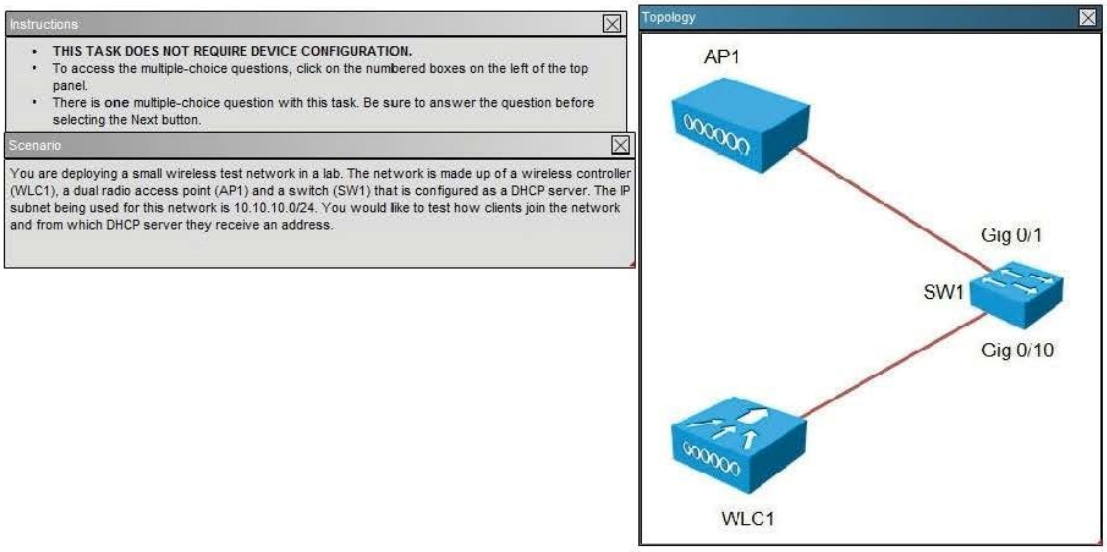
Correct Answer: B

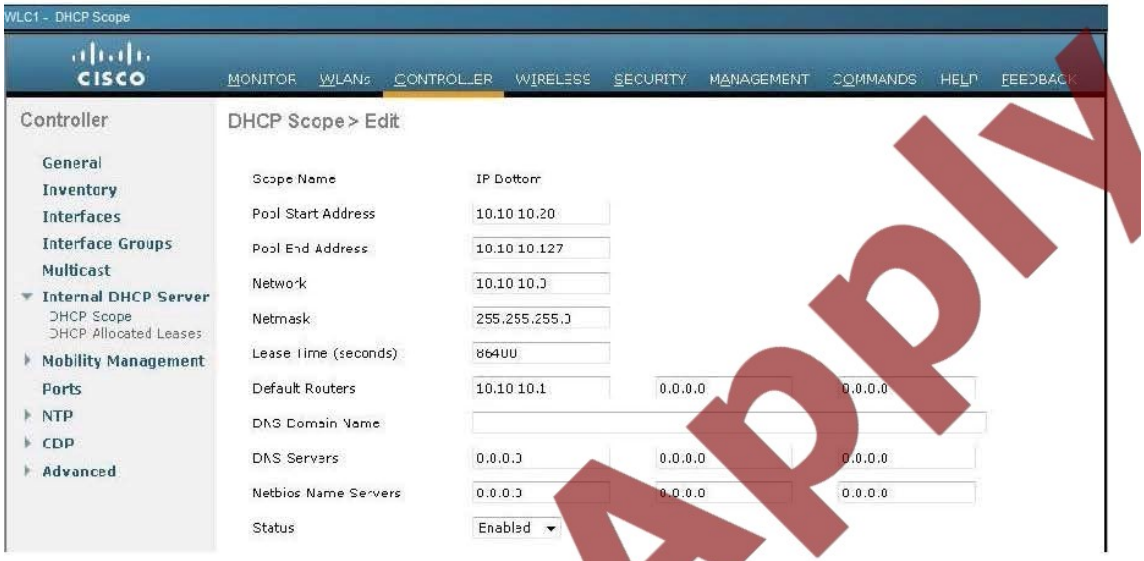
Step 1 - Choose Configure > Controllers or Configure > Access Points. Step 2 - Choose an IP address of a controller with software release 5.0 or later or choose an access point associated with software release 5.0 or later. Step 3 - Choose System > AP Username Password from the left sidebar menu. The AP Username Password page appears AP Username Password Page

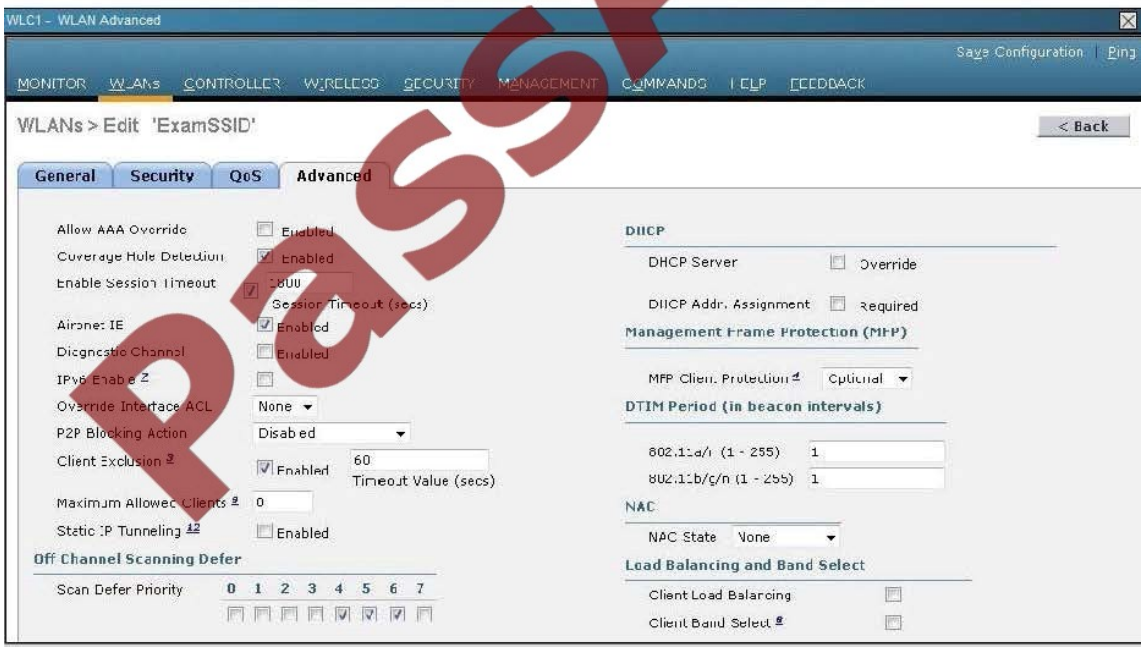


Step 4 - In the AP Username text box, enter the username that is to be inherited by all access points that join the controller. Step 5 - In the AP Password text box, enter the password that is to be inherited by all access points that join the controller. Re-enter in the Confirm AP Password text box. Step 6 - For Cisco autonomous access points, you must also enter and confirm an enable password. In the AP Enable Password text box, enter the enable password that is to be inherited by all access points that join the controller. Re-enter in the Confirm Enable Password text box. Step 7 - Click Save.

QUESTION 12

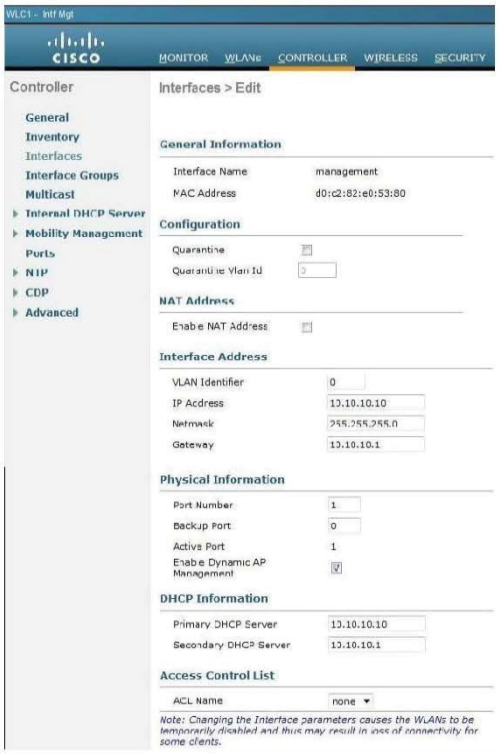

Instructions
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
There is one multiple-choice question with this task. Be sure to answer the question before selecting the Next button.
Scenario
You are deploying a small wireless test network in a lab. The network is made up of a wireless controller (WLC1), a dual radio access point (AP1) and a switch (SW1) that is configured as a DHCP server. The IP subnet being used for this network is 10.10.10.0/24. You would like to test how clients join the network and from which DHCP server they receive an address.
Topology
AP1
Gig 0/1
SW1
Gig 0/10
WLC1


WLC1 - DHCP Scope
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Controller
General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
DHCP Scope
DHCP Allocated Leases
Mobility Management
Ports
NTP
CDP
Advanced
DHCP Scope > Edit
Scope Name IP Bottom
Pool Start Address 10.10.10.20
Pool End Address 10.10.10.127
Network 10.10.10.0
Netmask 255.255.255.0
Lease Time (seconds) 86400
Default Routers 10.10.10.1 0.0.0.0 0.0.0.0
DNS Domain Name
DNS Servers 0.0.0.0 0.0.0.0 0.0.0.0
Netbios Name Servers 0.0.0.0 0.0.0.0 0.0.0.0
Status Enabled


WLC1 - WLAN Advanced
Save Configuration | Ping
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs > Edit 'ExamSSID'
< Back
General Security QoS Advanced
Allow AAA Override Enabled
Coverage Hole Detection Enabled
Enable Session Timeout 1800
Session Timeout (secs)
Aironet IE Enabled
Diagnostic Channel Enabled
IPv6 Enable
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion Enabled 60
Timeout Value (secs)
Maximum Allowed Clients 0
Static IP Tunneling Enabled
Off Channel Scanning Defer
Scan Defer Priority 0 1 2 3 4 5 6 7
DHCP
DHCP Server Override
DHCP Addr. Assignment Required
Management Frame Protection (MFP)
MFP Client Protection Optional
DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1
NAC
NAC State None
Load Balancing and Band Select
Client Load Balancing
Client Band Select

```
SW1 Show Run
SW1#show runnning-configuration
Building configuration...

Current configuration : 2429 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.10.1 10.10.10.128
!
ip dhcp pool Managament
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface GigabitEthernet0/25
!
interface GigabitEthernet0/26
!
!
interface GigabitEthernet0/27
!
interface GigabitEthernet0/28
!
interface GigabitEthernet0/29
!
interface GigabitEthernet0/30
!
interface GigabitEthernet0/31
!
interface GigabitEthernet0/32
!
interface GigabitEthernet0/33
!
interface GigabitEthernet0/34
!
interface GigabitEthernet0/35
!
interface GigabitEthernet0/36
!
interface GigabitEthernet0/37
!
interface GigabitEthernet0/38
!
interface GigabitEthernet0/39
!
interface GigabitEthernet0/40
!
interface GigabitEthernet0/41
!
interface GigabitEthernet0/42
!
interface GigabitEthernet0/43
!
interface GigabitEthernet0/44
!
interface GigabitEthernet0/45
!
interface GigabitEthernet0/46
!
interface GigabitEthernet0/47
!
interface GigabitEthernet0/48
!
interface GigabitEthernet0/49
!
!
interface GigabitEthernet0/50
!
interface GigabitEthernet0/51
!
interface GigabitEthernet0/52
!
interface TenGigabitEthernet0/1
!
interface TenGigabitEthernet0/2
!
interface Vlan1
 ip address 10.10.10.1 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
control-plane
!
!
line con 0
line vty 0 4
 login
line vty 5 15
 login
!
end
```



SW1 Show Run

```
SW1#show runnning-configuration
Building configuration...

Current configuration : 2429 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname SW
!
!
no aaa new-model
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.10.1 10.10.10.128
!
ip dhcp pool Management
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface GigabitEthernet0/3
!
!
interface GigabitEthernet0/4
!
interface GigabitEthernet0/5
!
interface GigabitEthernet0/6
!
interface GigabitEthernet0/7
!
interface GigabitEthernet0/8
!
interface GigabitEthernet0/9
!
interface GigabitEthernet0/10
!
interface GigabitEthernet0/11
!
interface GigabitEthernet0/12
!
interface GigabitEthernet0/13
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface GigabitEthernet0/17
!
interface GigabitEthernet0/18
!
interface GigabitEthernet0/19
!
interface GigabitEthernet0/20
!
interface GigabitEthernet0/21
!
interface GigabitEthernet0/22
!
interface GigabitEthernet0/23
!
interface GigabitEthernet0/24
!
interface GigabitEthernet0/25
!
interface GigabitEthernet0/26
!
interface GigabitEthernet0/27
!
interface GigabitEthernet0/28
!
interface GigabitEthernet0/29
!
interface GigabitEthernet0/30
!
interface GigabitEthernet0/31
!
interface GigabitEthernet0/32
!
interface GigabitEthernet0/33
!
interface GigabitEthernet0/34
!
interface GigabitEthernet0/35
!
interface GigabitEthernet0/36
!
interface GigabitEthernet0/37
!
interface GigabitEthernet0/38
!
interface GigabitEthernet0/39
!
interface GigabitEthernet0/40
!
interface GigabitEthernet0/41
!
interface GigabitEthernet0/42
!
interface GigabitEthernet0/43
!
interface GigabitEthernet0/44
!
interface GigabitEthernet0/45
!
interface GigabitEthernet0/46
!
interface GigabitEthernet0/47
!
interface GigabitEthernet0/48
!
interface GigabitEthernet0/49
!
```

All equipment is operational. Through which two methods can a wireless client receive an IP address when associating to the WLAN? (Choose two.)

A. The clients can receive an IP address from SW1.

B. Tie clients can receive an IP address from WLC1.

C. The clients will not receive an IP address from either DHCP server because of overlapping address ranges.

D. The clients can receive an IP address in a round-robin manner from either SW1 or WLC1.

E. The clients can use a static IP address.

Correct Answer: BE

As shown below, the DHCP server functionality has been enabled on the WLC1. Aside from DHCP, all clients can always statically assign themselves an IP address.

[Latest 640-722 Dumps](#) [640-722 Practice Test](#) [640-722 Study Guide](#)