



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

Instant Download After Purchase

100% Money Back Guarantee

- 😳 365 Days Free Update
- 800,000+ Satisfied Customers





#### **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.

	Alarm St	ummary 😳	🔺 <u>2</u>	<b>8</b> 0	<u> </u>
cisco				.co.	
<b>a</b>	Monitor 🔻	<u>R</u> eports 🔻	<u>C</u> onfigure •	Administratio	n <del>v</del> <u>T</u> ools <del>v</del> <u>H</u> elp <del>v</del>
WCS Hon	ne		0.9		



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

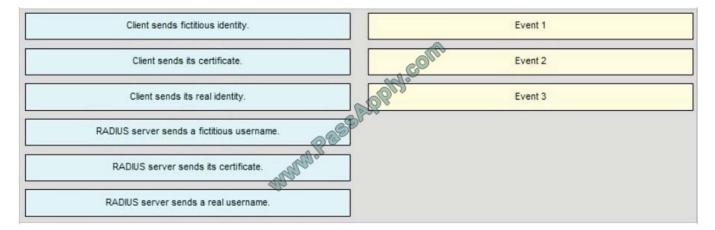


### **QUESTION 5**

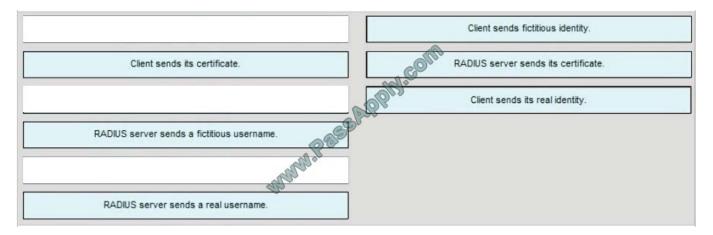
#### DRAG DROP

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.



cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT
Commands Download File Upload File	Config Boot Image	14.	jor		
Reboot Config Boot Scheduled Reboot Reset to Factory	Primary Image Backup Image Config Boot Image	.Q.V	Code 7.0.11 Code 5.1.16	.6.0 (default) :3.0	(active)
Default Set Time Login Banner	Image		Primary 👻 Primary Backup		

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.

ISCO		
<b>क</b> ≜	<u>1</u> onitor <del>▼</del> <u>R</u> eports ▼	Configure - Administration - Tools - Help -
	gging Options ing Options	SysLog Options Administration > Logging Options > SysLog
SysLog Options		SysLog Settings
		Enable SysLog
		SysLog Host 10.108.184.5
		SysLog Facility LOCAL7 -
		Save

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

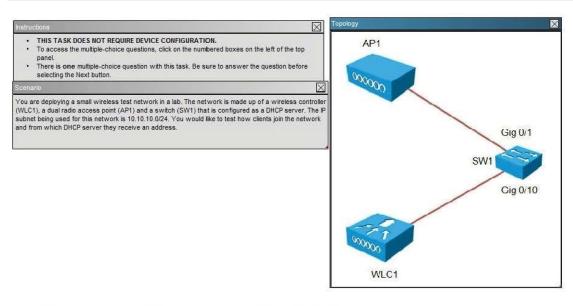


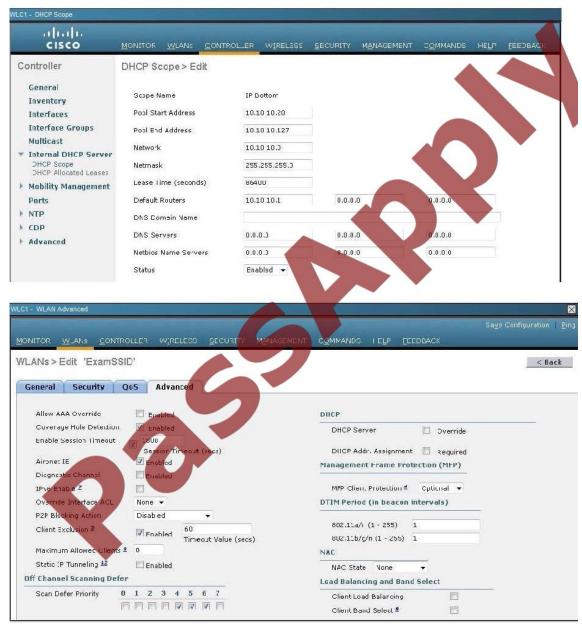
Alarm Summar	ry 🕀	🔺 🔻 🧿 🖌 Wirele	ss Control System SECONTROL Search
ISCO			<u>Advanced Search   Saved Search</u> User: <u>rout</u> @ Virtual Dumain: rcut
n Monitor 🔻 <u>R</u> eports	▼ <u>C</u> or	igure 🔻 Services 🔻 Administration 🔻 Tools 👻 Help 🔻	👝 🛛 😗 🤯 占 Logout
Properties	۲	AP Username Password	
System	۲	Configure > <u>Controllers</u> > <u>10.1.5.28</u> > System > <b>AP Username Passwor</b>	d Contraction
General Commands Interfaces Spanning Tree Protocol Nobility Groups Network Time Protoco OS Profiles OS Profiles DHCP Scopes User Roles AP Username Passwo Multicast		AP Username Password  AP UserName  AP Password  Confirm AP Password  Enable Password  Confirm Enable Password  Save Audit  Footnotes:  1. Enable Password is applicable only for Cisco IOS APs	
WLANs	۲		
H-REA <sup>9</sup>	۲		
Security	۲		
Access Points	۲		
802.11	۲		
802.11a/n	۲		
802.11b/g/n	۲		
Mesh	۲		
Ports	۲		
Management	(je)		
Location Configuration	۲		

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 AP 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** 









#### SWI#show runnning-configuration Building configuration...

rrent configuration : 2429 bytes rsion 12.2 service pad rvice timestamps debug uptime rvice timestamps log uptime service password-encryption stname SV r no aaa new-model systom etu routing 1500 ij subnet-zero no ij demain-lookup ij dhep excluded-aaddress 10.10.10.1 10.10.10.128 dbcp pool Management network 10.10.10.0 255.255.255.0 dofault-router 10.10.10.1 spanning-tree mode post spanning-tree extend system-id lan internal allocation policy ascending interface FastEthernetØ no ip address terface 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 GigabitEthernetA/1A interface GigabitEthernet@/11 interface GigabitEthernet@/12 interface GigabitEthernet0/13 interface GigabitEthernet0/14 interface GigabitEthernet0/15 interface GigabitEthernet0/16 interface GigabitEthernet0/17 interface GigabitEthernet@/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 GigabitEthernet@/32 interface GigabitEthernet@/33 interface GigabitEthernet0/34 interface GigabitEthernet@/35 interface GigabitEthernet0/36 interface GigabitEthernetU/37 interface GigabitEthernet0/38 interface GigabitEthernet0/39 interface GigabitEthernet0/40 interface GigabitEthernet0/41 interface GigabitEthernet@/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 GigabitELenent8/51 interface GigabitELenent8/51 interface TenGigabitELenent8/51 interface TenGigabitELenent8/1 interface Juni 19 address 10.10.10.1 255/255.255 interface Juni 10 classless 10 http server 5 http server 10 h 5



	cisco	MONITOR WLANE CON	TROLLER WIRELESS	SECURITY	
Inventory       Interfaces         Interfaces       Interfaces         Multicast       Interface Sname         Interface Groups       WAC Address         Multicast       Uncentral Information         Interface Name       management         Multicast       Uncentral Information         Ports       Onfiguration         Outpart       Quarantike         Interface Address       Uncentral         Interface Address       Interface Address         MAX Address       Enabe NAT Address         Enabe NAT Address       Interface Address         VLAN Identifier       0         IP Actress       10.10.10.0         IP Actress       10.10.10.0         Backup Port       0         Advise Port       1         Backup Port       1	Controller	Interfaces > Edit			
Interfaces       General Information         Interfaces Groups       Interfaces Name       management         Walticast       d0:d2:82:60:53:80         Interface Name       management         WAC Address       d0:d2:82:60:53:80         Interface Name       management         Walticast       Guarantine         Ports       Quarantine         ODP       NAT Address         Advanced       Interface Address         VLAN Identifier       0         IP Address       10:10:10:10         Ports       10:10:10:10         Geteway       10:10:10:10         Advise Port       1         Backup Port       0         Actives Port       1         Backup Port       1         Baceordary DHCP Elerver       10:10:10:1	General				
Interfaces       Interface Sname management         Multicast       PAC Address         Multicast       PAC Address         Mobility Management       PAC Address         Mobility Management       Quarantive         Ports       Quarantive Viant Id         CDP       NAT Address         Advanced       Enabe NAT Address         Pactes       10.10.10.0         Interface Address       0         VLN Identifier       0         IP Actress       10.10.10.0         Pacters       10.10.10.0         Pacters       10.10.10.0         Physical Information       Physical Information         Part Humber       1         Backup Port:       0         Advise Port       1         Backup Port:       0         Actives Port       1         Backup Port:       0         Actives Port       1         Backup Port:       0         Actives Port       1.10.10.10         Backup Port:       1.10.10.10         Backup Port:       1.10.10.10         Baceodary OticP Server       1.0.10.10.1         Access Control List       Access Control List         Act. N		Conoral Information			
Multicas Multi		and the second s	Column Column		
<ul> <li>Triteraal DHCP Server</li> <li>Mobility Management Purits</li> <li>CDP</li> <li>Advanced</li> <li>MAT Address</li> <li>Enable NAT Address</li> <li>Interface Address</li> <li>VLAN Identifier</li> <li>D</li> <li>Physical Information</li> <li>Part Number</li> <li>Backup Port</li> <li>Cadeway</li> <li>D.10.10.1</li> <li>Physical Information</li> <li>Part Number</li> <li>Backup Port</li> <li>Enable Dynamic AP Management</li> <li>DHCP Information</li> <li>Phimary DHCP Server</li> <li>D.10.10.1</li> <li>DHCP Information</li> <li>Phimary DHCP Server</li> <li>D.10.10.1</li> <li>DHCP Information</li> <li>DHCP Server</li> <li>D.10.10.1</li> <li>Beackup ICP Server</li> <li>D.10.10.1</li> <li>DHCP Information</li> </ul>					
Ports       Quarantitie         Purts       Quarantitie Vien Id         COP       Advanced         HAT Address       Interface Address         VLAN Identifier       0         IP Address       Interface Address         VLAN Identifier       0         IP Address       13.10.10.0         Network       255.255.0         Gateway       13.10.10.1         Physical Information       Physical Information         Pat Number       1         Eabe Dynamic AP       0         Advagementi       1         Eabe Dynamic AP       0         Primary DHCP Server       13.10.10.10         Eaccess Control List       Access Control List         Active Tomaging the Interface parameters causes the WAANs to be         Note: Charging the Interface parameters causes the WAANs to be					
<ul> <li>NIP</li> <li>Quarandile Vian Id</li> <li>Quarandile Vian Id</li> <li>Advanced</li> <li>HAT Address</li> <li>Enable NAT Address</li> <li>Interface Address</li> <li>Interface Address</li> <li>VLAN Identifier</li> <li>IP Acdress</li> <li>10.10.10.0</li> <li>IP Acdress</li> <li>10.10.10.0</li> <li>Physical Information</li> <li>Part Number</li> <li>Backup Port</li> <li>B</li></ul>		Configuration			
Advanced  Advanced  HAT Address Enabe NAT Address Enabe NAT Address Enabe NAT Address  Linterface Address VLAN Identifier  Interface Address VLAN Identifier  Interface Address VLAN Identifier  Interface Address Interface Addres		Quarantine	20		
Advanced       NAT Address       Enable RNT Address       Interface Address       Interface Address       VLAN Identifier       IP Acdress       10.10.10.10       IP Acdress       10.10.10.10       Physical Information       Part Number:       1       Backup Port       1       Eable Dynamic AP       Winnay DHCP Enver       10.10.10.10       Primary DHCP Server       10.10.10.10       Access Control List       Active Inner Interface parameters causes the WAARs to be homeganerity for the set of the function of the set of the se	NIP .	Quarantine Ylan Id	0		
Enabe INAT Address: □  Interface Address:  VLAN Identifier 0 IP Acdress 10.10.10.10 IP Acdress 10.10.10.10 IP Acdress 10.10.10.10 IP Acdress 10.10.10.10 IP Acdress 10.10.10 IP IN Umber 1 Backup Port 0 IP Backup Port 1 Backup Port 1 Backup Port 1 Backup Port 1 Enabe Dynamic AP Menogement AP IP Information  DHCP Information  Primary DHCP Server 10.10.10 Becondary OHCP Server 10.10.10.1 Access Control List Acc Name none  Note: Charging the Informace parameters causes the WAANE to be Becongenity disability and the camp creatil in ose of comparentity for between I and the camp creatil in ose of comparentity for the Information		NAT Address			
VLAN Identifier 0 IP Acdress 10.10.10.10 Netrowsk 255.255.255.0 Gateway 10.10.10.1 Physical Information Part Number 1 Backup Port 0 Active Port 1 Evabe Dynamic AP Management DHCP Information Primary DHCP Server 10.10.10 Secondary DHCP Server 10.10.10.1 Primary DHCP Server 10.10.10.1 Access Control List ACL Name none ▼	Advanced	Enable NAT Address	871		
VLAN Identifier 0 IP Acdress 10.10.10.10 Netrowsk 255.255.255.0 Gateway 10.10.10.1 Physical Information Part Number 1 Backup Port 0 Active Port 1 Evabe Dynamic AP Management DHCP Information Primary DHCP Server 10.10.10 Secondary DHCP Server 10.10.10.1 Primary DHCP Server 10.10.10.1 Access Control List ACL Name none ▼		Interface Address			
IP Acdress 10.10.10.10 Netrowsk 255.255.255.0 Gateway 10.10.10.1 Physical Information Part Number 1 Backup Port 0 Active Port 1 Enable Dynamic AP Managament DHCP Information Primary DHCP Server 10.10.10.10 Secondary DHCP Server 10.10.10.1 Access Control List Access Control List Acc Name none ▼			0		
Netrowsk:     255,255,255,0       Geteway     10,10,10,1       Physical Information        Backup Port     1       Babe Dynamic AP Manogement     I       DHCP Information     I       Primary DHCP Server     10,10,10,10       Secondary DHCP Server     10,10,10,10       Access Control List     I       ACL. Name     none ▼       Note: Charging the Interface parameters causes the WAARs to be Imported and this cam prevail in one soft causes the WAARs to be			P. 1		
Physical Information Part Number  Part Number  Backup Port  Active Port  Charles Port  Charles Port  Charles Port  DHCP Information  Primary DHCP Server  10.10.10.10  Secondary DHCP Server  10.10.10.1  Access Control List  ACL Name none ▼  Note: Charging the Interface parameters causes the WLANe to be Importantly disability for					
Part Number 1 Backup Port 0 Activs Port 1 Enable Dynamic AP Management AP DHCP Information Primary DHCP Server 10.10.10.10 Secondary DHCP Server 10.10.10.10 Access Control List ACL Name none ▼ Note: Changing the Interface parameters causes the WANe to be integrately disability and the image receil in lines of comparisity for		Gateway	10.10.10.1		
Port Number 1 Backup Port 0 Active Port 1 Enable Dynamic AP Manogenerat DHCP Information Primary DHCP Server 10.10.10.0 Secondary OHCP Server 10.10.10.1 Access Control List Acc Name none ▼ Note: Charging the Interface parameters causes the WANe to be Interface and the ican growell in one of comparisity for		Physical Information			
backup Port     0       Activa Port     1       Evable Dynamic AP     ▼       Managament     ▼       DHCP Information     ▼       Primary DHCP Server     13.10.10.10       Secondary DHCP Server     13.10.10.10       Access Control List     Acc Name       Note: Changing the Interface parameters causes the WLANs to be the temporarily disability for		and the second second second			
Active Port 1 Evable Dynamic AP Management DHCP Information Primary DHCP Server 10.10.10.10 Secondary DHCP Server 10.10.10.1 Access Control List ACL Name none ▼ Note: Changing the Interface parameters causes the WLANs to be Importantly disability of the					
Enable Dynamic AP Management DHCP Information Primary DHCP Server 10.10.10.10 Secondary DHCP Server 10.10.10.10 Access Control List Acc. Name none ▼ Note: Changing the Interface parameters causes the WLANs to be Importantly disability of the					
Primary DHCP Server 13.10.10.10 Secondary DHCP Server 13.10.10.10 Access Control List ACL Name none ▼ Note: Changing the Interface parameters causes the W_ANs to be temporarily disability and the camp create lin and a conservity for		Enable Dynamic AP			
Secondary DHC® Server 10:10:10.1 Access Control List ACL Name none ▼ Note: Changing the Interface parameters causes the WLANs to be temporarily disability and the camp year will in case of comparity for		DHCP Information			
Access Control List ACL Name none ▼ Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may rewail in uses of connectivity for		Primary DHCP Server	10.10.10.10		
ACL Name none ▼ Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may cresult in uses of connectivity for		Secondary DHCP Server	10.10.10.1		
Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in joss of connectivity for		Access Control List			
temporarily disabled and thus may result in loss of connectivity for		ACL Name	none 🔻		
		temporarily disabled and thus	parameters causes the WL may result in loss of conn	ANs to be activity for	

a supervision of the second seco			
Pool Stat 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	C.0.0.0
DNS Dumain Nerrie			
DNS Servers	0.0.0	0.0.0	C.0.0.0
Netblos Name Servars	0.0.0	0.0.0.0	C.O.0.0
Status	Disabled *		

6



SW1#show runnning-configuration Building configuration... Current configuration = 2429 bytes t version 12.2 nn service pad service timestanps debug uptime service timestanps log uptime no service passuord-encryption : hostname SW ro aaa new-model systom mtu routing 1500 ip subnetzero no 1p domain-lookup ip dhop excluded-address 10.10.10.1 10.10.10.128 dhen nool Management network 10.10.10.0 255.255.255.0 default-router 10.10.10.1 spanning-tree mode pust spanning-tree extend system-id vlan internal allocation policy ascending interface FastEthernetØ no ip address interface GigahitEthernet0/1 interface GigabitEthernet0/2 interface GigabitEthernet0/3 interface GigabitEthernet0/1 interface GigabitEthernet@/5 interface GigabitEthernet0/6 interface GigabitEthernet0/7 interface GigabitEthernet0/8 interface GigabitEthernet0/9 interface GigabitEthernet0/10 interface GigabitEthernet@/11 interface GigabitEthernet0/12 interface GigabitEthernet0/13 interface GigabitEthernet0/14 interface GigabitEthernet0/15 interface GigabitEthernet0/16 interface GigabitEthernet0/17 interface GigabitEthernet@/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 GigabitEthernetU/30 interface GigabitEthernet0/31 interface GigabitEthernet0/32 interface GigabitEthernet0/33 interface GigabitEthernet0/34 interface GigabitEthernet@/35 interface GigabitEthernet0/36 interface GigabitEthernetU/37 interface GigabitEthernet0/38 interface GigabitEthernet0/39 interface GigabitEthernet0/40 interface GigabitEthernet0/41 interface GigabitEthernet@/42 interface GigabltEthernot0/43 interface GigabitEthernetU/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



To Read the Whole Q&As, please purchase the Complete Version from Our website.

# Try our product !

100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

#### https://www.passapply.com/allproducts

### **Need Help**

Please provide as much detail as possible so we can best assist you. To update a previously submitted ticket:



#### **One Year Free Update**



Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.



To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of ourchase.

**Money Back Guarantee** 



#### Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Any charges made through this site will appear as Global Simulators Limited. All trademarks are the property of their respective owners. Copyright © passapply, All Rights Reserved.