



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.pass4lead.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





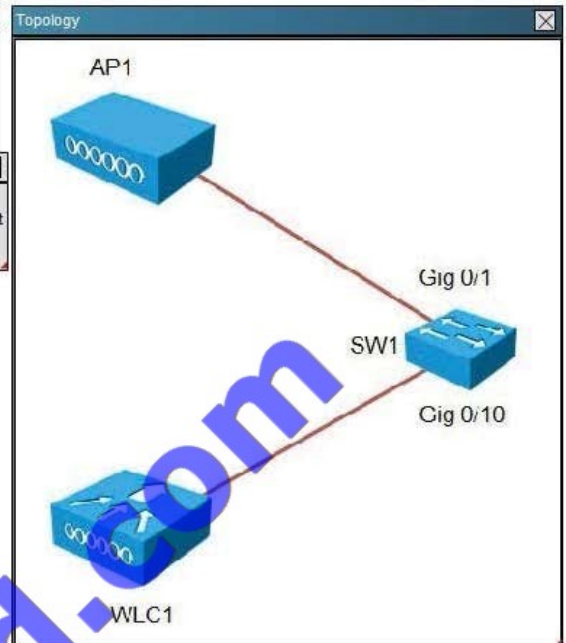
QUESTION 1

Instructions

- Refer to the exhibits to answer the questions related to this task.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- To access the multiple-choice question, click on the numbered box 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.



WLC1 - Monitor Clients

CISCO

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Monitor

- Summary
- ▶ Access Points
- ▶ Cisco CleanAir
- ▶ Statistics
- ▶ CDP
- ▶ Rogues
- Clients
- Multicast

Clients > Detail

Client Properties		AP Properties	
MAC Address	00:1d:e3:46:f3:2d	AP Address	3c:ce:73:6c:c6:d0
IP Address	10.10.10.130	AP Name	AP1
Client Type	Regular	AP Type	802.11bn
User Name		WLAN Profile	HoHo
Port Number	1	Status	Associated
Interface	management	Association ID	-
VLAN ID	0	802.11 Authentication	Open System
CCX Version	CCXv4	Reason Code	-
E2E Version	E2Ev1	Status Code	0
Mobility Role	Local	CF Pullable	Not Implemented
Mobility Peer IP Address	N/A	CF Poll Request	Not Implemented
Policy Manager State	RUN	Short Preamble	Implemented
Management Frame Protection	No	P3CC	Not Implemented
UpTime (Sec)	112	Channel Agility	Not Implemented
Power Save Mode	ON	Timeout	1800
Current TxRateSet	m15	WEP State	WEP Disable
Data RateSet	1.0,2.0,5.5,11.3,6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0		



WLC1 - Intf Mgt

MONITOR WLANs CONTROLLER WIRELESS SECURITY

Controller

General
Inventory
Interfaces
Interface Groups
Multicast
Internal DHCP Server
Mobility Management
Ports
NTP
CDP
Advanced

Interfaces > Edit

General Information

Interface Name: management
MAC Address: d0:c2:82:e0:53:80

Configuration

Quarantine:
Quarantine Vlan Id:

NAT Address

Enable NAT Address:

Interface Address

VLAN Identifier:
IP Address:
Netmask:
Gateway:

Physical Information

Port Number:
Backup Port:
Active Port:
Enable Dynamic AP Management:

DHCP Information

Primary DHCP Server:
Secondary DHCP Server:

Access Control List

ACL Name: none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

```

!
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

```

WLC1 - WLAN

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs

WLANs
WLANs
Advanced

WLANs > Edit 'ExamSSID'

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:
P2P Blocking Action:
Client Exclusion: Enabled 60
Timeout Value (secs):
Maximum Allowed Clients:
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:
DTIM Period (in beacon intervals):
802.11a/g (1 - 255):
802.11b/g/n (1 - 255):

NAC

NAC State:
Load Balancing and Band Select:
Client Load Balancing:
Client Band Select:



In setting up the wireless network, it is desired that the DHCP server that is configured in WLC1 provides IP addressing to the WLAN. When devices attempt to join the network, they fail to receive an IP address in the range provided by the DHCP server in WLC1, but they do receive an IP address from the DHCP server in SW1. What is causing this issue?

- A. The external DHCP server in SW1 will always be the preferred DHCP server and WLC1 will always be the secondary DHCP server in the WLAN.
- B. The DHCP server address for SW1 needs to be removed from the DHCP server configuration in WLC1.
- C. The primary DHCP server address in WLC1 is incorrect.
- D. The primary DHCP server configured in WLC1 is not enabled.

Correct Answer: D

This can be verified by the following screen shot, showing the DHCP server is disabled at the bottom:

The screenshot shows the 'DHCP Scope > Edit' configuration page in a network management interface. The 'Status' field is set to 'Disabled'. The 'Access Control List' section shows 'ACL Name' set to 'none'. A note at the bottom of the page reads: 'Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.'

QUESTION 2

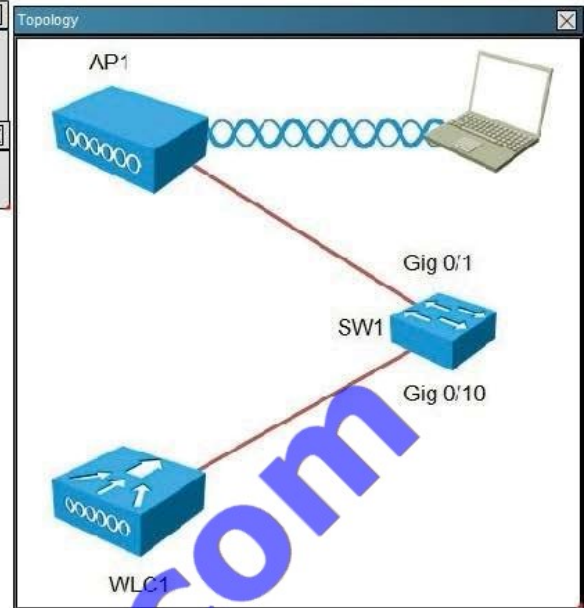


Instructions

- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- To access the multiple-choice question, click on the numbered box 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

A wireless LAN controller, AP, IOS switch, and wireless client have been properly configured. Use the exhibits to answer the question.



WLC1 - Interface Groups

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS

Interface Groups > Edit

Interface Group Name: intgroup

Description: Interface Group

Property: Non-Quarantine

Interface Name: management

Add Interface

Interface Name	Management
vlan20	<input checked="" type="checkbox"/>
vlan40	<input checked="" type="checkbox"/>
vlan50	<input checked="" type="checkbox"/>

WLC1 - Interfaces

MONITOR | WLANs | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	10.10.10.10	Static	Enabled
virtual	N/A	192.0.2.1	Static	Not Supported
vlan20	20	172.16.12.10	Dynamic	Disabled <input checked="" type="checkbox"/>
vlan30	30	172.16.23.10	Dynamic	Disabled <input checked="" type="checkbox"/>
vlan40	40	192.168.14.10	Dynamic	Disabled <input checked="" type="checkbox"/>
vlan50	50	192.168.25.10	Dynamic	Disabled <input checked="" type="checkbox"/>



WLC1 - Monitor Summary

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Summary

5 Access Points Supported



Controller Summary

Management IP Address	10.10.10.10
Software Version	7.0.116.U
Field Recovery Image Version	1.0.0
License Level	base
System Name	WLC1
Up Time	0 days, 4 hours, 13 minutes
System Time	Thu Apr 19 12:44:41 2012
Internal Temperature	+32 C
802.11a Network State	Enabled
802.11h/g Network State	Enabled

Rogue Summary

Active Rogue APs	21	Detail
Active Rogue Clients	0	Detail
Adhoc Rgues	0	Detail
Rouges on Wired Network	0	

Top WLANs

Profile Name	# of Clients	
ExamSSID	1	Detail

WLC1 - WLANs

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANs > Edit 'ExamSSID'

General Security QoS Advanced

Profile Name: ExamSSID
Type: WLAN
SSID: ExamSSID
Status: Enabled

Security Policies: None
(Modifications done Under security tab will appear after applying the changes.)

Radio Policy: All
Interface/Interface Group(G): intgroup (G)
Multicast Vlan Feature: Enabled
Broadcast SSID: Enabled

When a client associates to ExamSSID, which network address will be assigned?

- A. The IP address assigned will be based on the AP network assignment of 10.10.10.0.
- B. The IP address assigned will be based on the AP network assignment of 172.16.23.0.



C. The IP address will be assigned in a round-robin format based on the 172.16.12.0, 172.16.23.0, 192.168.14.0 address pools.

D. The IP address will be assigned in a round-robin format based on the 172.16.12.0, 192.168.14.0, 192.168.25.0 pools.

E. The IP address will be assigned in a round-robin format based on the 172.16.12.0, 172.16.23.0, 192.168.14.0, 192.168.25.0 pools.

Correct Answer: D

The IP addresses will be assigned round robin to the three interface groups, which we can see are vlan20, vlan40, and vlan50. From the WLC-interfaces tab we see that the IP addresses assigned to these 3 interfaces are 172.16.12.10, 172.16.14.10, and 192.168.25.10, respectively.

QUESTION 3

How can you protect the configuration file from eavesdropping, when uploading from a Cisco WLC?

A. Use the Configuration File Encryption option.

B. Choose an SCP as the transfer method.

C. Connect to the Cisco WLC by using HTTPS.

D. Connect to the Cisco WLC by using SSH.

Correct Answer: A

Uploading the Configuration Files (GUI) Reference:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/configuration/guide/b_cg73/b_wlc-cg_chapter_01010.html



Step 1	Choose Commands > Upload File to open the Upload File from Controller page.
Step 2	From the File Type drop-down list, choose Configuration .
Step 3	Encrypt the configuration file by selecting the Configuration File Encryption check box and entering the encryption key in the Encryption Key text box.
Step 4	From the Transfer Mode drop-down list, choose from the following options: <ul style="list-style-type: none">• TFTP• FTP
Step 5	In the IP Address text box, enter the IP address of the server.
Step 6	In the File Path text box, enter the directory path of the configuration file.
Step 7	In the File Name text box, enter the name of the configuration file.
Step 8	If you are using an FTP server, follow these steps: <ol style="list-style-type: none">In the Server Login Username text box, enter the username to log into the FTP server.In the Server Login Password text box, enter the password to log into the FTP server.In the Server Port Number text box, enter the port number on the FTP server through which the upload occurs. The default value is 21.
Step 9	Click Upload to upload the configuration file to the server. A message appears indicating the status of the upload. If the upload fails, repeat this procedure and try again.

QUESTION 4

When using DHCP option 43, the discovery option supports vendor specific identifiers in order to obtain what IP address?

- A. core router\\'s gateway
- B. closest distribution switch
- C. local WLAN controller
- D. local Radius Server

Correct Answer: C



QUESTION 5

Which module does the Cisco AnyConnect Secure Mobility client integrate into the AnyConnect client package for access to both wired and wireless networks?

- A. Network Access Manager
- B. Telemetry
- C. Web Security
- D. DART

Correct Answer: A

The main components used in IUWNE are the Cisco AnyConnect Mobility Client itself, associated with the Network Access Module (NAM) used to manage existing profiles and provide the wireless connectivity. Reference: CCNA Wireless (640-722 IUWNE) Quick Reference Guide page 73

[640-722 PDF Dumps](#)

[640-722 VCE Dumps](#)

[640-722 Practice Test](#)



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](#)

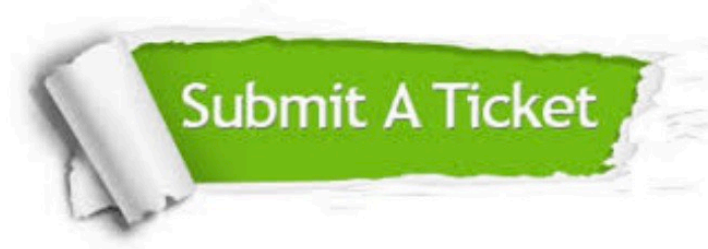
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4lead.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>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.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>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.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4lead, All Rights Reserved.