



# 640-722<sup>Q&As</sup>

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 two algorithms are available in RRM? (Choose two.)

- A. coverage-hole detection
- B. dynamic channel assignment
- C. RSSI normalizer
- D. transmitting channel expander
- E. rogue detection

Correct Answer: AB

Here is how Cisco RRM works from a high level:

Wireless LAN Controllers (WLCs) are provisioned with a consistent RF Group Name. This is an ASCII name to identify those WLCs and APs that are all part of the same wireless system.

APs periodically send out RRM Neighbor Messages to each other that are passed up to the Wireless LAN controllers as well. These messages are authenticated for security purposes and provide the controllers with a complete picture of all of the devices in the RF Group. From these devices an RF Group Leader is elected.

Note that these RRM Neighbor Messages play a critical role in other Cisco Unified Wireless Network capabilities such as Over-the-Air Provisioning (OTAP) and Rogue AP Classification.

Once the RF Group is understood, a series of algorithms are run to optimize AP configurations in the RF Group. It is the RF Group Leader that is responsible for these periodic math assignments. (This sounds like a great job for our own Petr Lapukhov!) You should also note that RRM with its RF Grouping is separate and distinct from Mobility Grouping.

What are the algorithms that the RF Group Leader will be busy with?

Dynamic Channel Assignment Algorithm using metrics of load measurements, noise, interference, signal strength

Transmit Power Control Algorithm

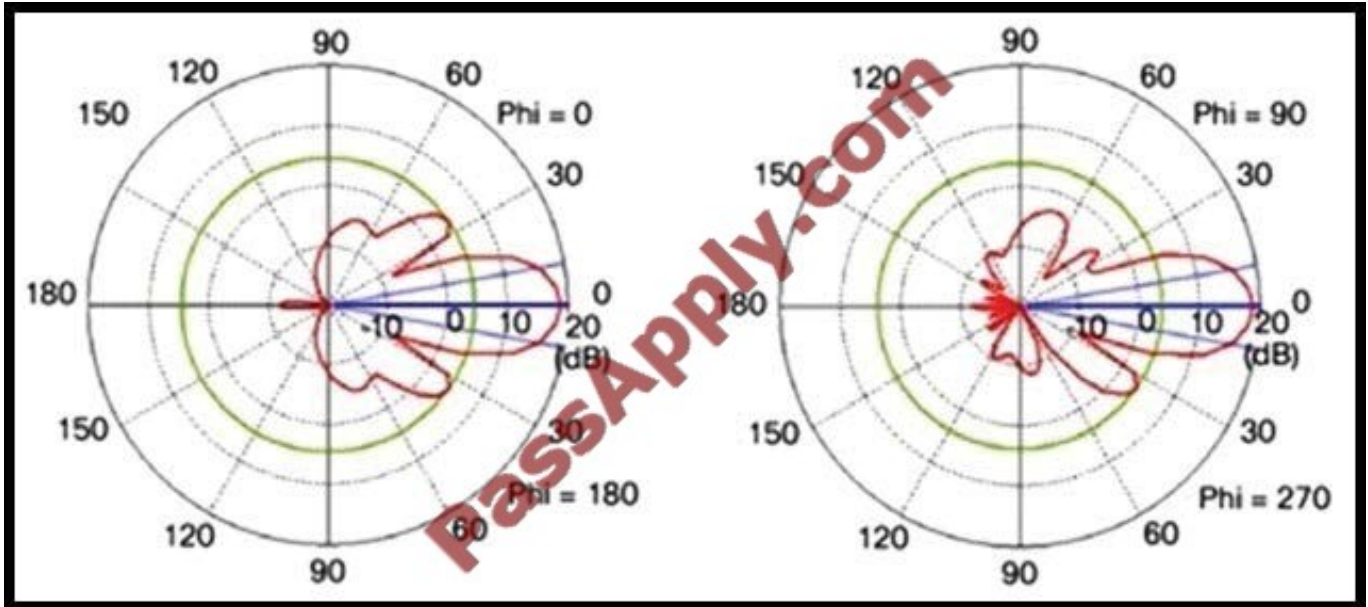
Coverage Hole Detection and Correction Algorithm

Reference: <http://blog.ine.com/2010/10/08/cisco-radio-resource-management-rrm/>

---

### QUESTION 2

Refer to the exhibit.



Which antenna would produce the given radiation pattern?

- A. patch
- B. Yagi
- C. parabolic dish
- D. dipole
- E. omni-directional

Correct Answer: A

### QUESTION 3

Which protocol helps the administrator to determine whether a detected rogue AP is in the network of the organization?

- A. RLDP
- B. RCP
- C. RDP
- D. RAPP

Correct Answer: A

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 deauthentication messages to all connected clients and then shuts down the radio interface. Then, it will associate 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.



Reference: <https://supportforums.cisco.com/discussion/10941011/rd-rogue-detector-or-rldp-rogue-location-discovery-protocol>

#### QUESTION 4

Instructions

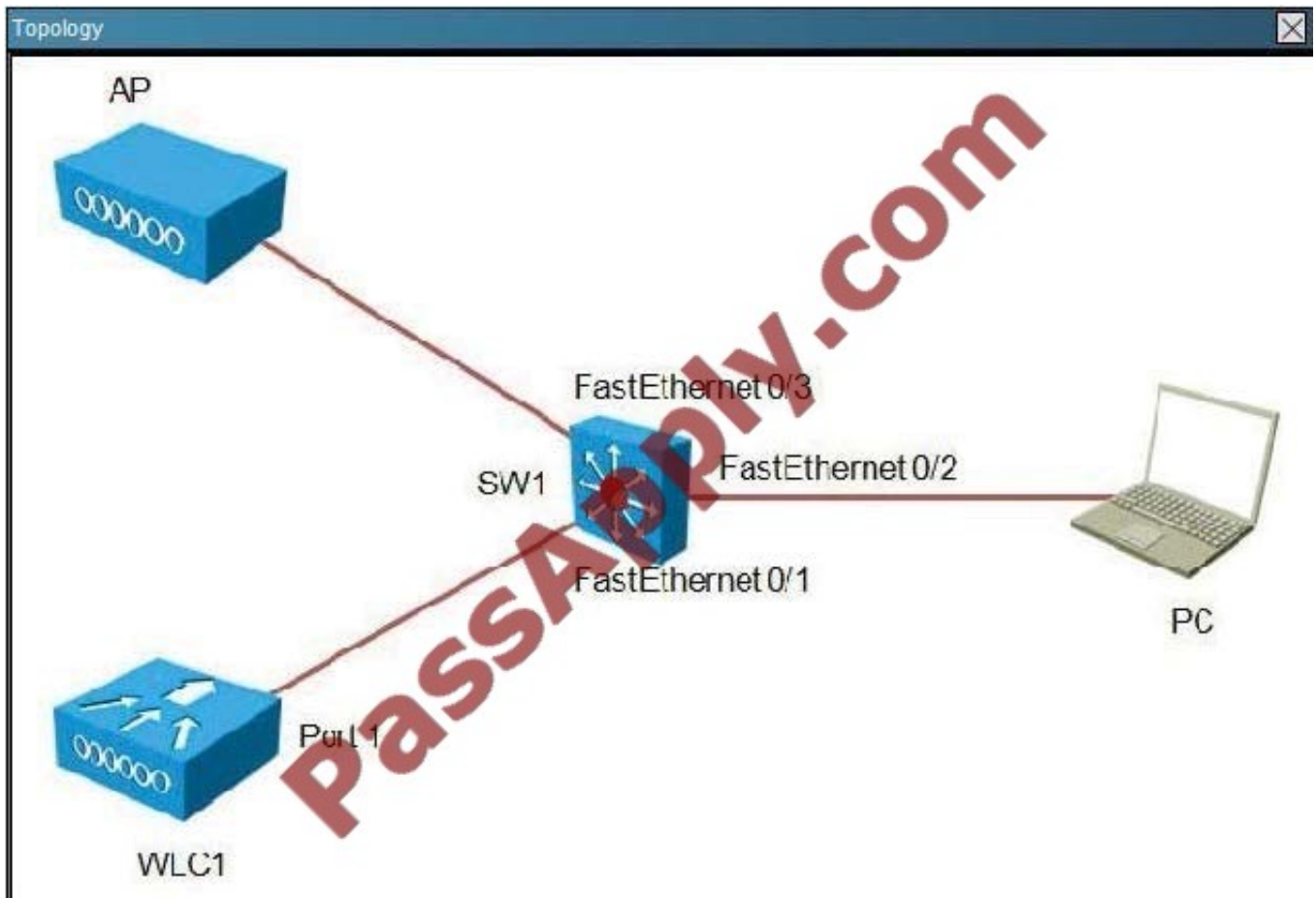
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.

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.

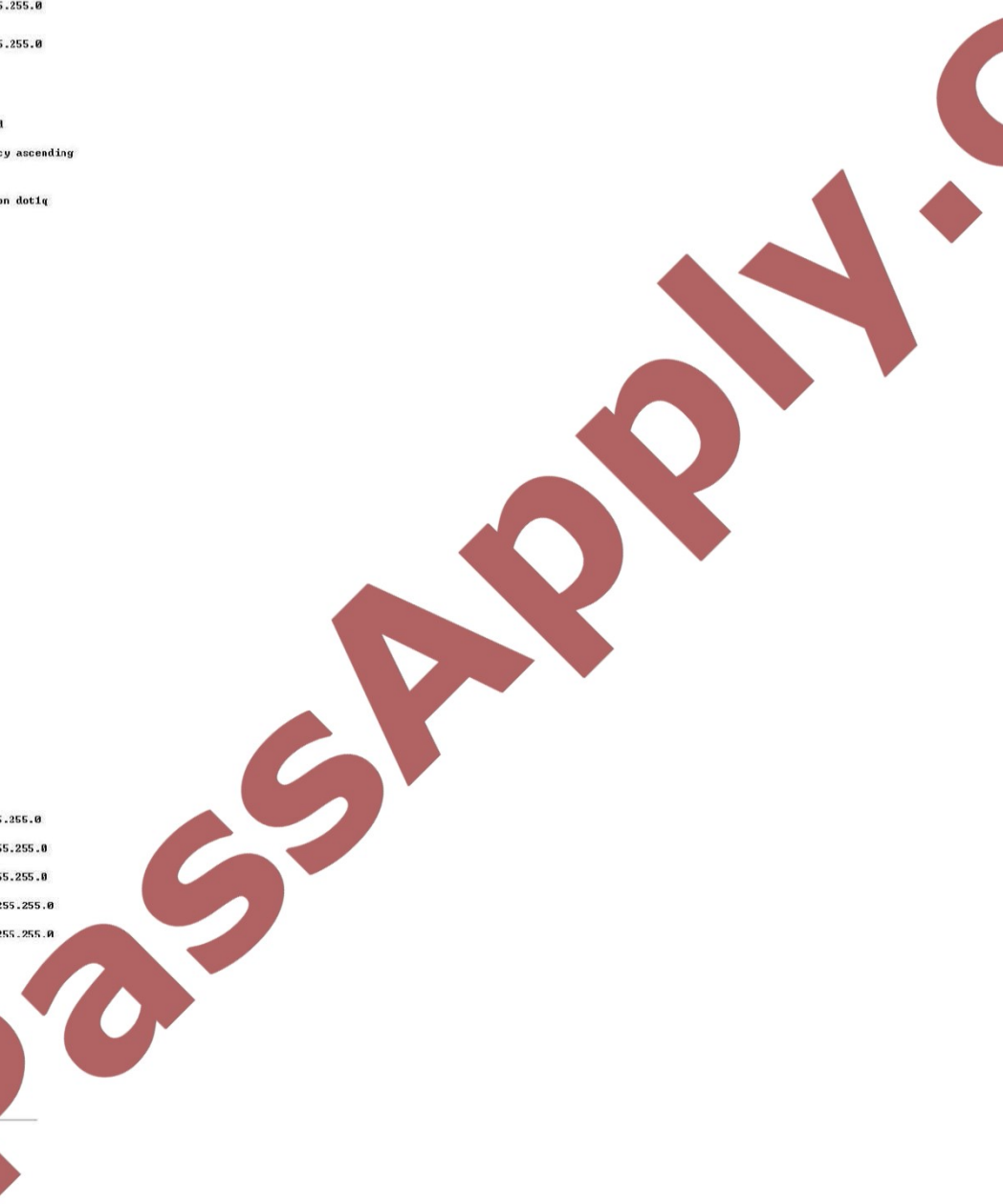
Scenario

You have just finished configuring a WLC2504 through the console CLI. The WLC is attached to an existing production network switch. However, you are not able to reach the WLC via `https://10.10.10.10`.





```
SW1# Show Run
SW1#
SW1# run
Building configuration...
Current configuration : 4504 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Wp4r$xs.h0p1IAFTKdNlgR3oxe1
!
!
no aaa new-model
system mtu routing 1500
ip routing
ip dhcp excluded-address 10.10.10.1 10.10.10.50
ip dhcp excluded-address 192.168.14.1 192.168.14.50
ip dhcp excluded-address 192.168.25.1 192.168.25.50
ip dhcp excluded-address 172.16.12.1 172.16.12.50
ip dhcp excluded-address 172.16.23.1 172.16.23.50
!
ip dhcp pool vlan1
network 10.10.10.0 255.255.255.0
default-router 10.10.10.1
!
ip dhcp pool vlan40
network 192.168.14.0 255.255.255.0
default-router 192.168.14.1
!
ip dhcp pool vlan50
network 192.168.25.0 255.255.255.0
default-router 192.168.25.1
!
ip dhcp pool vlan20
network 172.16.12.0 255.255.255.0
default-router 172.16.12.1
!
ip dhcp pool vlan30
network 172.16.23.0 255.255.255.0
default-router 172.16.23.1
!
!
no ip domain-lookup
!
!
spanning-tree mode pwt
spanning-tree extend system-id
!
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
description VACL
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface FastEthernet0/2
description PC
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/3
description AP
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/4
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/5
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/6
switchport access vlan 20
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
!
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/8
switchport access vlan 30
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/9
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/10
switchport access vlan 40
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/11
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/12
switchport access vlan 50
switchport mode access
spanning-tree portfast
!
interface Vlan1
ip address 10.10.10.1 255.255.255.0
!
interface Vlan20
ip address 172.16.12.1 255.255.255.0
!
interface Vlan30
ip address 172.16.23.1 255.255.255.0
!
interface Vlan40
ip address 192.168.14.1 255.255.255.0
!
interface Vlan50
ip address 192.168.25.1 255.255.255.0
!
!
ip classless
ip http server
ip http secure-server
!
ip sla enable reaction-alerts
!
!
line con 0
line vty 0 4
password cisco
login
line vty 15
login
!
end
```





SW1 Show Intf Switchport

```
SW1#show int faste0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-100
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
SW1#
```

SW1 Show Interface

```
SW1#sh int faste0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 2c36.f866.a701 (bia 2c36.f866.a701)
Description: WLC1
MTU 1500 bytes, BW 100000 kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 10Cmb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout: 04:00:00
Last input 00:00:05, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 1000 bits/sec, 3 packets/sec
 15220 packets input, 5567664 bytes, 0 no buffer
  Received 978 broadcasts (76 multicasts)
  0 runs, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 756 multicast, 0 pause input
  0 input packets with dribble condition detected
108786 packets output, 1021445 bytes, 0 underruns
  0 output errors, 0 collisions, 1 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier, 0 pause output
  0 output buffer failures, 0 output buffers swapped out
SW1#
```

SW1 Show VLAN

```
SW1#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Gi0/1 Gi0/2
20 vlan20	active	Fa0/5, Fa0/6
30 vlan30	active	Fa0/7, Fa0/8
40 vlan40	active	Fa0/9, Fa0/10
50 vlan50	active	Fa0/11, Fa0/12
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

SW1#



```
WLC1 - Setup
System Name [Cisco_e0:52:04] (31 characters max): WLC1
Enter Administrative User Name (21 characters max): admin
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password : *****

Management Interface IP Address: 10.10.10.10
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 - untagged): 1
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.1

Virtual Gateway IP Address: 192.0.2.1

Mobility/RF Group Name: Mobility

Network Name (SSID): ExamSSID

Configure DHCP Bridging Mode [yes][no]:
Allow Static IP Addresses [YES][no]:
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: no
Enable 802.11a Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

Configuration correct? If yes, system will save it and reset. [yes][no]: yes
.....reboot info deleted.....

User: admin
Password: *****
<Cisco Controller> >ping 10.10.10.1
Send count=3, Receive count=0 from 10.10.10.1

<Cisco Controller> >
```

Which change can correct inband access to the WLC?

- A. change the switch FastEthernetO/1 duplex setting
- B. change the switch FastEthernetO/1 speed setting
- C. enable the switch FastEthernetO/1 spanning-tree port-fast trunk
- D. change the switch FastEthernetO/1 trunk encapsulation
- E. change the WLC management interface to use DHCP
- F. change the WLC management interface VLAN
- G. change the WLC configuration of NTP



H. browse to WLC via http://10.10.10.10

Correct Answer: D

All of the other ports in the network are using the default VLAN (VLAN 1) but port 0/1, which connects to the WLC, is configured as a trunk, so VLAN 1 is not operational.

```
SW1 Show Run
vlan internal allocation policy ascending
interface FastEthernet0/1
description WLC1
switchport trunk encapsulation dot1q
switchport mode trunk

SW1 Show VLAN
SW1#show vlan brief
VLAN Name                Status    Ports
-----
1    default                 active    Fa0/2, Fa0/3, Fa0/4, Gi0/1
                    Gi0/2
20   vlan20                  active    Fa0/5, Fa0/6
30   vlan30                  active    Fa0/7, Fa0/8
40   vlan40                  active    Fa0/9, Fa0/10
50   vlan50                  active    Fa0/11, Fa0/12
1002 fddi-default            act/unsu
1003 token-ring-default    act/unsu
1004 fddinet-default       act/unsu
1005 trnet-default         act/unsu
SW1#

interface FastEthernet0/8
switchport access vlan 20
switchport mode access
spanning-tree portfast
interface FastEthernet0/7
switchport access vlan 30
switchport mode access
spanning-tree portfast
interface FastEthernet0/8
switchport access vlan 30
switchport mode access

User: admin
Password:*****
<Cisco Controller> >ping 10.10.10.1
Send count=3, Receiving count=3 from 10.10.10.1
```

### QUESTION 5

What is the maximum number of access points supported on Cisco WCS with an enterprise license?

- A. 5,000
- B. 10,000
- C. 50,000
- D. 100,000

Correct Answer: C





Enterprise Server License (Multiple Servers) Overview (release 4.1 or later)

License: WCS-ENT-PLUS-K9

License increments: 1000, 2500, 10000, 50000

Single or multiple server deployment (Cisco WCS Navigator included in 10000, and 50000 licenses)

Suitable for customers deploying 500 or more Cisco Aironet lightweight access points

Multiple license files linked to a single PAK certificate

Server decrements available number of access points as licenses are allocated within the network

Reference: [http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product\\_data\\_sheet0900aecd804b4646.html](http://www.cisco.com/c/en/us/products/collateral/wireless/wireless-control-system/product_data_sheet0900aecd804b4646.html)

[Latest 640-722 Dumps](#)

[640-722 Study Guide](#)

[640-722 Braindumps](#)



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:



 <p><b>One Year Free Update</b> 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><b>Money Back Guarantee</b> 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><b>Security &amp; Privacy</b> We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information &amp; 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 © passapply, All Rights Reserved.