

ExamsLabs

ExamsLabs

HOME

ALL VENDORS

GUARANTEE

FAQ

TESTIMONIALS

CART (0)

Pass Your Next Certification Exam Fast!

Everything you need to prepare, learn & pass your certification exam easily.

365 days free updates. First attempt guaranteed success.



Select a vendor...

Select an test...

Your email address

Free Download Demo

Try **Online Engine** before you buy

Online Test Engine: Online Tool, Convenient, easy to study. Instant Online Access. Supports All Web Browsers.

PDF format: Easy to read and print learning materials, our products are available in PDF file format.

Desktop Test Engine: Installable Software Application. Simulates Real Exam Environment. Practice Offline Anytime.

What Client's Say

"I passed today with score 80%. I confirm that it's valid in UK. Focus on "Correct answer" and forget the "Answer X from real test". I had free new questions.



Sebastian
★★★★★

"Questions from this HPE0-S51 dump are 100% valid... not all answers. I passed this exam a few days ago (in France) and got these results.



Wayne
★★★★★

<http://www.examslabs.com/>

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **300-370**

Title : Troubleshooting Cisco
Wireless Enterprise Networks

Vendor : Cisco

Version : DEMO

NO.1 Which two non-802.11 devices cause the least interference on 802.11 networks? (Choose two.)

- A. microwave oven
- B. electro-mechanical generator
- C. wireless game controller
- D. dual-tech motion detector
- E. cellular mobile phone (nonsmartphone)

Answer: A,C

NO.2 An engineer is troubleshooting client issues and has found that DHCP proxy is enabled on the Cisco WLC by default. The Cisco WLC unicasts the packet to the DHCP server on the WLAN, but the DHCP server does not support the DHCP proxy. Which action fixes this issue?

- A. Ensure that the switch ports that are connected to the Cisco WLC and the DHCP server are configured as a trunk.
- B. Disable DHCP proxy on the Cisco WLC.
- C. Ensure that the IP subnet of the WLAN is defined on the DHCP server.
- D. Ensure that the DHCP clients are directly connected to the interface of the server.

Answer: B

NO.3 A WLAN was installed at a high AP density. DTPC is lowering the transmit power of many APs too low. Which change in the DTPC transmit power threshold must be made to allow APs to globally increase AP transmit power by 3dBm?

- A. from -70 dBm to -73 dBm
- B. from 70 dBm to 73 dBm
- C. from -70 dBm to -67 dBm
- D. from 70 dBm to 67 dBm

Answer: C

NO.4 An engineer has received an alarm on a wireless LAN controller and is unsure of its meaning. The engineer attempted to ping the wireless LAN controller interfaces. Which troubleshooting methodology does this action demonstrate?

- A. bottom-up
- B. top-down
- C. shoot from the hip
- D. divide and conquer
- E. follow the path

Answer: D

NO.5 Two 5508 Wireless Lan Controllers are managing all Access Points throughout the network. The WLCs are located in different locations to provide geographical redundancy. A Mobility Group has been configured on both WLCs and has a UP status on both Controllers. The APs in location A are statically configured to use Controller A as the Primary and Controller B as the Secondary. If the WLC in location A goes offline, the APs successfully join the WLC in location B but they do not failover to

their Primary configured Controller What configuration task will fix this issue'

- A. Use DHCP Option 43 and specify WLC in location A as Primary.
- B. Configure the WLC in location A as Primary using the CAPWAP AP Controller IP Address command on all the location A Access Points.
- C. Change the AP Failover Priority to critical.
- D. Enable AP Fallback globally on the WLC.

Answer: B

NO.6 Some users are experiencing inconsistent performance on their mobile devices as they move throughout the building when browsing the Internet. Which feature provides a more consistent user experiences?

- A. 802.11r
- B. low RSSI check
- C. RX-SOP
- D. optimized roaming

Answer: D

NO.7 Refer to the exhibit.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cf8)
2	0.000026000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cf8)
3	0.003835000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cf9)
4	0.003864000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cf9)
5	0.021887000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cfa)
6	0.021909000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cfa)
7	0.028005000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cfb)
8	0.028033000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cfb)
9	0.045915000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cfc)
10	0.045951000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cfc)
11	0.053857000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cfd)
12	0.053879000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cfd)
13	0.070381000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=0, ID=5cfe)
14	0.070406000	192.168.0.13	24.244.31.72	IPv4	1514	Fragmented IP protocol (proto=UDP 17. off=1480, ID=5cfe)

Wireless users notify the helpdesk of poor wireless performance. Based on the packet capture from a client PC, what is the cause of the connectivity issue?

- A. MSS mismatch
- B. UDP retransmissions
- C. TCP retransmissions
- D. MTU mismatch

Answer: D

NO.8 An engineer performed a packet capture of the wireless network and found very high retry rates in a high density 802.11 ac WLAN deployment due to overlapping basic service sets. Which change reduces the impact of this issue without creating possible coverage problems?

- A. Disable data rates below 12 Mbps.
- B. Utilize RxSOP.
- C. Reduce the channel bandwidth.
- D. Lower the 802.11a radio power.

Answer: C

Explanation:

<https://www.bartleby.com/essay/Improving-the-Overlapping-Basic-Service-Set-Problem-P3LVW6AVJ>
For 802.11ac to be effective, it requires minimum 80 MHz wide channel with optionally up to 160 MHz.

The increase in bandwidth leads to problems like OBSS. OBSS problem occur when two or more BSSs operate in same channel and are close to hear each other.

NO.9 Refer to the exhibit.

```
(Cisco Controller) > show ap join state detailed 00:ab:00:ab:00:ab

Discovery phase statistics
- Discovery requests received ..... 2
- Successful discovery responses sent ..... 1
- Unsuccessful discovery request processing..... 2234562
- Reason for last unsuccessful discovery attempt.....
  Discovery request received on unsupported VLAN
- Time at last successful discovery attempt.....
  Mar 06 19:03:50.779
- Time at last unsuccessful discovery attempt.....
  Mar 06 19:03:50.782

Join phase statistics
- Join requests received..... 1
- Successful join responses sent..... 0
- Unsuccessful join request processing..... 1
- Reason for last unsuccessful join attempt.....
  Certificate payload in join request contains
  invalid certificate
- Time at last successful join attempt.....
  Not applicable
- Time at last unsuccessful join attempt.....
  Mar 06 19:04:00.810

Configuration phase statistics
- Configuration requests received..... 2
- Successful configuration responses sent ..... 0
- Unsuccessful configuration request processing..... 0
- Reason for last unsuccessful configuration attempt....
  Not applicable
- Time at last successful configuration attempt.....
  Not applicable
- Time at last unsuccessful configuration attempt.....
  Not applicable

Last AP message decryption failure details
- Reason for last message decryption failure.....
  Not applicable

Last AP disconnect details
- Reason for last AP connection failure.....
  Not applicable

Last join error summary
- Type of error that occurred last.....
  Lvapp join request rejected
- Reason for error that occurred last.....
  Certificate payload in join request contains invalid
  certificate
- Time at which the last join error occurred.....
  Mar 06 19:04:00:810
```

Which statement about the join process of the access point is true?

- A. The AP moved from this controller to its primary controller.
- B. The AP failed to join because the self-signed certificate of the AP was not correct on the controller.
- C. The time on the controller is outside of the certificates validity time interval so the join phase failed.
- D. The AP successfully joined the controller.

Answer: C

NO.10 An engineer wants to run the Voice Audit tool in PI and wants to be able to verify that clients will be capable of having static IPs whether or not Call Admission Control is enabled

Which two rules field descriptions must be checked in the report? (Choose two.)

- A. DHCP assignment
- B. CAC: max bandwidth
- C. ACM
- D. DTTPC
- E. load-based CAC

Answer: A,E

Reference:

https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/reference/guide/pi_ref.pdf

NO.11 An engineer is trying to prime a lightweight access point running 8.2 code using the CLI with an IP address of 10.10.10.100/24. Which command set must the engineer input to manually configure this access point?

A. configure terminal

interface Dot11Radio0

ip address 10.10.10.100 255.255.255.0

B. configure terminal

interface BVI 1

ip address 10.10.10.100 255.255.255.0

C. enable

capwap ap ip address 10.10.10.100 255.255.255.0

D. enable

iwapp ap ip address 10.10.10.100 255.255.255.0

Answer: C

NO.12 An engineer is troubleshooting AP join issues on a wireless infrastructure. While gathering debugs, the engineer notices that one of the commands may generate an excessive amount of data on the console. Which command causes this to occur?

A. debug capwap packet enable

B. debug capwap events enable

C. debug capwap info enable

D. debug capwap errors enable

E. debug capwap detail enable

F. debug capwap payload enable

Answer: A

NO.13 All corporate-issued devices in your network have been configured with EAP-TLS authentication. They authenticate via wireless to an instance of Cisco ISE and AD authorization for the user profiles is un-configured. Which impact occurs to the authentication when a user's Active Directory username and password expires?

A. WLAN connectivity is not impacted because EAP-TLS uses certificates.

B. The user must change the password manually on their WLAN profile.

C. The ISE prompts the user for the new password.

D. The WLAN profile must be forgotten and reconfigured.

Answer: A

NO.14 Refer to the exhibit.

```

*Mar 1 02:50:43.508: dot11_auth_dot1x_parse_aaa_resp: Received server response:
GET_CHALLENGE_RESPONSE
*Mar 1 02:50:43.508: dot11_auth_dot1x_parse_aaa_resp: found eap pak in server response
*Mar 1 02:50:43.508: dot11_auth_dot1x_parse_aaa_resp: found session timeout 120 sec
*Mar 1 02:50:43.509: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 001e.be26.0f2a
*Mar 1 02:50:43.509: dot11_auth_dot1x_send_response_to_client: Forwarding server message
to client 001e.be26.0f2a
*Mar 1 02:50:43.509: dot11_auth_dot1x_send_response_to_client: Started timer
client_timeout 120 seconds
*Mar 1 02:50:43.519: dot11_auth_parse_client_pak: Received EAPOL packet from
001e.be26.0f2a
*Mar 1 02:50:43.519: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 001e.be26.0f2aStarted timer-client_timeout 120
seconds
*Mar 1 02:50:43.769: dot11_auth_parse_client_pak: Received EAPOL packet from
001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_send_response_to_server: Sending client
001e.be26.0f2a data to server
----- 02:50:43.769: AAA/AUTHN/PPP (00000021): Pick method list 'eap_methods'
----- started timer
001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_send_response_to_server: Sending client
001e.be26.0f2a data to server
----- 02:50:43.769: AAA/AUTHN/PPP (00000021): Pick method list 'eap_methods'
----- started timer
001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 001e.be26.0f2a
*Mar 1 02:50:43.769: dot11_auth_dot1x_send_response_to_server: Sending client
001e.be26.0f2a data to server
----- 02:50:43.769: AAA/AUTHN/PPP (00000021): Pick method list 'eap_methods'
----- started timer
001e.be26.0f2a
*Mar 1 02:50:44.698: AAA/AUTHN/PPP (00000021): Pick method list 'eap_methods'
*Mar 1 02:50:44.698: dot11_auth_dot1x_send_response_to_server: Started timer
server_timeout 60 seconds
*Mar 1 02:50:44.709: dot11_mgmt: dot11_mgmt_sta_del (ref=0, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:44.709: dot11_mgmt: 001e.be26.0f2a have already been removed from said fsewp
tree
*Mar 1 02:50:44.709: %DOT11-7-AUTH_FAILED: Station 001e.be26.0f2a Authentication failed
*Mar 1 02:50:45.664: dot11_mgmt: add a new station 001e.be26.0f2a
*Mar 1 02:50:45.664: dot11_mgmt: dot11_mgmt_sta_add (ref=1, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:45.664: dot11_mgmt: insert 001e.be26.0f2a into said[] tree
*Mar 1 02:50:45.664: dot11_mgmt: dot11_mgmt_sta_ref (ref=1, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:45.664: dot11_mgmt: dot11_mgmt_sta_ref (ref=2, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:45.664: dot11_mgmt: dot11_mgmt_sta_deref (ref=1, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:46.536: dot11_mgmt: dot11_mgmt_sta_ref (ref=2, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:46.536: dot11_mgmt: dot11_mgmt_sta_del_all_children sta_ptr 0x8f991c0
*Mar 1 02:50:46.536: dot11_mgmt: dot11_mgmt_sta_tree_cleanup, 0x8f991c0
*Mar 1 02:50:46.536: dot11_mgmt: finish remove 001e.be26.0f2a and its children
*Mar 1 02:50:46.536: dot11_mgmt: dot11_mgmt_sta_deref (ref=3, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)
*Mar 1 02:50:46.539: dot11_mgmt: dot11_mgmt_sta_ref (ref=0, sta_ptr=0x8f991c0,
mac=001e.be26.0f2a)

```

What is a possible reason why the non-root AP fails to associate to the root AP?

- A. Eap_methods is misconfigured
- B. Invalid credentials are entered
- C. An invalid PSK is configured
- D. The authentication server failed to respond

Answer: A

NO.15 Refer to the exhibit.

```

Packet Number: 104
Flags: 0x00000000
Status: 0x00000001
Packet Length: 281
Timestamp: 15:22:51.446693700 09/22/2014
Data Rate: 48 24.0 Mbps
Channel: 149 5745MHz 802.11a
Signal Level: 74%
Signal dBm: -21
Noise Level: 71%
Noise dBm: -92
[0-23] 802.11 MAC Header Version=0 Type=X00 Management Subtype=X1000 Beacon Duration=0 Microseconds Destinat
802.11 Management - Beacon
Beacon Timestamp: 2993897478 Microseconds [24-31]
Beacon Interval: 102 Time Units (104 Milliseconds, and 448 Microseconds) [32-33]
Capability Info=X000100000000000001
SSID ID=0 SSID Len=3 SSID=ABC
Rates= ID=1 Rates: Len=4 Rate=24.0 Mbps Rate=36.0 Mbps Rate=48.0 Mbps Rate=54.0 Mbps
TIM= ID=5 TIM: Len=7 DTIM Count=0 DTIM Period=1 Bitmap Control=X00000000 Part Virt Bmap=0x02000000
Country ID=7 Country Len=18 Country Code=AU Enviroment=0x20 Any Starting Channel=36 Number of Channels=4 Max I
QBSS= ID=11 QBSS: Len=5 Station Count=1 Channel Utilization=3 % Avail Admission Capacity=23437
HT Cap= ID=45 HT Cap: Len=26
HT Info= ID=61 HT Info: Len=22 Primary Channel=149
Extended Capabilities ID=127 Extended Capabilities Len=8
Cisco Proprietary ID=133 Cisco Proprietary Len=30 OUI=00-00-8F Raytheon Value=0x003F00FF035900 AP Name=TEST-AP
ID=150 Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
VHT Capabilities element ID=191 VHT Capabilities element Len=12
VHT Operation element ID=192 VHT Operation element Len=5
VHT Transmit Power Envelope ID=195 VHT Transmit Power Envelope Len=4 Local Maximum Transmit Power For 20 MHz=
WMM ID=221 WMM Len=24 OUI=00-50-F2 MICROSOFT CORP. OUI Type=2 OUI SubType=1 Parameter Element Version=1
Vendor Specific ID=221 Vendor Specific Len=6 OUI=00-40-96 Cisco Systems Data=(3 bytes)
Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Version=3 CCX Version=5
Vendor Specific ID=221 Vendor Specific Len=5 OUI=00-40-96 Cisco Systems Data=(2 bytes)
Vendor Specific ID=221 Vendor Specific Len=8 OUI=00-40-96 Cisco Systems Data=(5 bytes)

```

What is the highest mandatory rate in Mbps configured for the AP?

- A. 54
- B. 36
- C. 24
- D. 48

Explanation: This is the capture of a Beacon frame. As you can see it is transmitted at 24Mbps (highest mandatory rate configured on 802.11a band). Note that it is advertising VHT - 802.11ac capability

Answer: C

NO.16 Refer to the exhibit. Which option prevents the AP from completing the DTLS join process?

```

*Jan 15 22:29:04.847: AP has SHA2 MIC certificate - Using SHA2 MIC
certificate for DTLS.

*May 8 20:35:13.000: %CAPWAP-5-DTLSREQSEND: DTLS connection
request sent peer_ip: 192.168.10.6 peer_port: 5246
*May 8 20:35:13.207: %DTLS-5-ALERT: Received FATAL : Certificate
unknown alert from 192.168.10.6
*May 8 20:35:13.207: %DTLS-5-SEND_ALERT: Send FATAL : Close notify
Alert to 192.168.10.6:5246

```

- A. The WLC has the incorrect date.
- B. The SSC is not authorized.
- C. The root CA is missing on the WLC.

D. An intermediary CA is missing on the WLC.

Answer: B