Exam Code: 351-050

Exam Name: CCIE Wireless Beta Written Exam

Vendor: CISCO

Version: DEMO

Part: A

1: Refer to the exhibit.

Given this debug output, which two statements are correct? (Choose two.)

```
(Cisco Controller) >debug client 001B.7705.4AB9

(Cisco Controller) >show debug

MAC address ................................. 00:1b:77:05:4a:b9

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  pem events enabled.
  pem state enabled.


(Cisco Controller) >Fri Jun  6 19:49:24 2008: 00:1b:77:05:4a:b9 Adding mobile on LWAPP AP 00:1d:a1:91:34:70(0)
Fri Jun  6 19:49:24 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 23) in 5 seconds
Fri Jun  6 19:49:24 2008: 00:1b:77:05:4a:b9 apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:05:4a:b9 on AP
00:1d:a1:91:34:70 from Idle to Probe
Fri Jun  6 19:49:29 2008: 00:1b:77:05:4a:b9 apfMsExpireCallback (apf_ms.c:433) Expiring Mobile!
Fri Jun  6 19:49:29 2008: 00:1b:77:05:4a:b9 pemApfDeleteMobileStation2: caller=apfMsExpireMobileStation line=4474 Role=Unassoc
Fri Jun  6 19:49:29 2008: 00:1b:77:05:4a:b9 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [00:1d:a1:91:34:70]
Fri Jun  6 19:49:29 2008: 00:1b:77:05:4a:b9 Deleting mobile on AP 00:1d:a1:91:34:70(0)
Fri Jun  6 19:49:31 2008: 00:1b:77:05:4a:b9 Adding mobile on LWAPP AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:31 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 23) in 5 seconds
Fri Jun  6 19:49:31 2008: 00:1b:77:05:4a:b9 apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:05:4a:b9 on AP
00:1c:f6:63:94:e0 from Idle to Probe
Fri Jun  6 19:49:31 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:33 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:33 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:34 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:34 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:39 2008: 00:1b:77:05:4a:b9 apfMsExpireCallback (apf_ms.c:433) Expiring Mobile!
Fri Jun  6 19:49:39 2008: 00:1b:77:05:4a:b9 pemApfDeleteMobileStation2: caller=apfMsExpireMobileStation line=4474 Role=Unassoc
Fri Jun  6 19:49:39 2008: 00:1b:77:05:4a:b9 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [00:1c:f6:63:94:e0]
Fri Jun  6 19:49:39 2008: 00:1b:77:05:4a:b9 Deleting mobile on AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:41 2008: 00:1b:77:05:4a:b9 Adding mobile on LWAPP AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:41 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 23) in 5 seconds
Fri Jun  6 19:49:41 2008: 00:1b:77:05:4a:b9 apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:05:4a:b9 on AP
00:1c:f6:63:94:e0 from Idle to Probe
Fri Jun  6 19:49:41 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:44 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:44 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 apfMsExpireCallback (apf_ms.c:433) Expiring Mobile!
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 pemApfDeleteMobileStation2: caller=apfMsExpireMobileStation line=4474 Role=Unassoc
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [00:1c:f6:63:94:e0]
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 Deleting mobile on AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 Adding mobile on LWAPP AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 23) in 5 seconds
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:05:4a:b9 on AP
00:1c:f6:63:94:e0 from Idle to Probe
Fri Jun  6 19:49:41 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:44 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:44 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 apfMsExpireCallback (apf_ms.c:433) Expiring Mobile!
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 pemApfDeleteMobileStation2: caller=apfMsExpireMobileStation line=4474 Role=Unassoc
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 0.0.0.0 START (0) Deleted mobile LWAPP rule on AP [00:1c:f6:63:94:e0]
Fri Jun  6 19:49:49 2008: 00:1b:77:05:4a:b9 Deleting mobile on AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 Adding mobile on LWAPP AP 00:1c:f6:63:94:e0(0)
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 23) in 5 seconds
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 apfProcessProbeReq (apf_80211.c:4057) Changing state for mobile 00:1b:77:05:4a:b9 on AP
00:1c:f6:63:94:e0 from Idle to Probe
Fri Jun  6 19:49:51 2008: 00:1b:77:05:4a:b9 Scheduling deletion of Mobile Station:  (callerId: 24) in 5 seconds
```

A.The station (STA) with MAC address 00:1d:a1:91:34:70 is passing traffic towards the wired network.

B.The station (STA) with MAC address 00:1b:77:05:4a:b9 is passing traffic towards the wired network.

C.The wireless client is not receiving an IP address via DHCP, and therefore gets disconnected after five seconds.

D.The wireless client "hangs" in probes (does not proceed with 802.11 authentication and

association). It is likely that the "encryption" or "key-management" advertised in the probe response does not match.

E.Since the AP receives a probe request from the wireless client, the Access Point Functions state for the machine changes from "Idle" to "Probe."

F.The wireless client uses a static IP address, so "0.0.0.0 START (0)" can be found in the logs.

G.The wireless client has been successfully authenticated. Reauthentication is set to occur on an extremely aggressive schedule (every five seconds).

Correct Answers: D E

2: Which two statements about RTS/CTS are correct? (Choose two.)

A.When the transmitted packet is equal to or larger than the RTS threshold, an RTS packet is sent. The destination node must respond with a CTS packet before the originator can send the real data packet.

B.The sender sends an RTS packet with the predicted sending time in the duration field. If the receiver grants this time it replies with the same value in the duration field of the CTS packet.

C.The RTS/CTS sequence allows a STA or AP to assemble several frames, reserve the medium, and send them in one burst.

D.The RTS and CTS are small and, if lost in a collision, they can be retried more quickly and with less overhead than if the whole packet must be retried.

E.Since the introduction of EDCA (WMM and 802.11e), the RTS/CTS sequence has been rendered unnecessary.

F.802.11d replaced the RTS/CTS sequence with CTS to Self.

Correct Answers: A D

3: You see the following message on a Cisco WCS:

AP 'floor-1-lobby', interface '802.11b/g' on Controller '10.1.1.1'. Noise threshold violated.

There is also a correlation between the occurrence of the message and user complaints. What action should be taken?

A.Increase the interference threshold from the default 10%.

B.Seek out the source of the noise with a spectrum analyzer.

C.Check the logs for rogues in the area, then turn on rogue mitigation.

D.Manually increase the power of the AP to overcome the interference.

Correct Answers: B

4: It is recommended that you prime or stage your lightweight access points in a convenient location, rather that after they have been installed in locations that may be difficult to reach. When priming a lightweight AP prior to deployment, you should use the controller CLI, controller GUI, or Cisco WCS to configure which three of these? (Choose three.)

A.to configure the lightweight access point with primary, secondary, and tertiary controller names

B.to configure the Controller Mobility Group name, if the lightweight access point is in a Controller Mobility Group

C.to configure dhcp option 43

D.to configure dhcp option 60

E.to configure the access-point-specific LED blink sequence

F.to configure the access-point-specific 802.11a, 802.11b, and 802.11g network settings
Correct Answers: A B F

5: When viewed from the side (H-plane), how can the radiation pattern of patch and Yagi antennas be described?
A.the patch patterns are egg-shaped, the Yagi patterns are conical
B.the patch patterns are conical, the Yagi patterns are egg-shaped
C.the patch patterns are doughnut-shaped, the Yagi patterns are conical
D.the patch patterns are conical, the Yagi patterns are doughnut-shaped
Correct Answers: A

6: Which statement is correct about wireless voice traffic?
A.Voice traffic is more latency-sensitive.
B.Wireless voice devices cannot share APs with wireless data NIC cards.
C.1Mb/s and 2Mb/s data rates are required for the phones, but not for the wireless data traffic.
D.Wireless voice traffic must be on a dedicated channel apart from wireless data.
Correct Answers: A

7: Which functionality, as defined by IEEE 802.11e, does WWM certify as part of the tests for QoS done by the WiFi Alliance?
A.EDCA
B.Direct Link Setup
C.S-APSD
D.HCCA
Correct Answers: A

8: In an LWAPP system, when an AP's interface goes down and then comes up again, how does the Cisco WCS know what has happened?
A.The AP sends a linkDown then linkUp trap to the Cisco WCS; these are two of the six traps defined in RFC 1215, A Convention for Defining Traps for use with the SNMP.
B.The AP cannot send a linkDown trap, as per RFC 1215, because the link is down; when the link comes back up, the AP sends a linkup trap to the Cisco WLC, which then forwards the trap to the Cisco WCS.
C.The Cisco WCS polls the APs and when the AP is unreachable, reports "Max retransmissions reached on AP <name>".
D.The Cisco WLC sends a trap to the Cisco WCS when it detects that an AP is down.
Correct Answers: D

9: What will happen when a client roams from one controller (controller A) to a new controller (controller B), if the wireless LAN interfaces configured on the different controllers are on different IP subnets (Layer 3 inter-controller roaming)?
A.Controller B will update its client database and all client ingress and egress traffic will transition to the new controller.
B.Controller A will mark the client with an anchor entry in its client database, the database, and

the database entry will be copied to controller B and marked with a foreign entry.

C.Controller A will mark the client's entry in its client database as an anchor, controller B will not update its client database because of the anchored entry in controller A, and all ingress and egress traffic will flow through controller A.

D.Controller A will mark the client's entry in its client database as foreign, controller B will update its client database, all ingress traffic will flow through controller A, and egress traffic will flow through controller B when symmetric tunneling is disabled.

Correct Answers: B

10: Which 802.11i key is used to provide data origin authenticity during the four-way handshake and the group key handshake messages?

A.Key Encryption Key

B.Groupwise Master Key

C.Key Caching Key

D.Key Confirmation Key

Correct Answers: D

11: Which command can be used to determine the health of a RADIUS server on an autonomous AP?

A.show radius statistics

B.show radius table {server_ip}

C.show radius-server {server_ip}

D.debug radius-server

Correct Answers: A

12: When setting up a WLAN for Wireless Domain Services, what must be configured on the APs in order to be able to communicate with the WDS master?

A.username and password valid on the AAA server

B.IP address of the master WDS and any backup master WDS

C.pre-shared key which matches that of the master WDS

D.multicast group for the WDS

Correct Answers: A

13: Which two of these are long-term solutions to hidden node problems? (Choose two.)

A.increase the power or antenna gain on the access point; for example, by using Yagi or parabolic antennas

B.change the RF situation by increasing the power on client work stations (None-AP-STA)

C.set the RTS threshold to 10 or less

D.change the RF situation by adding additional access points

E.enable CTS to Self

F.increase the radio speed to at least 24 Mb/s

Correct Answers: B D

14: A user reports problems authenticating via wireless. Which two Cisco WLC debug commands

would help clarify the issue? (Choose two.)

A.debug mac { addr MAC}

B.debug authentication enable

C.debug dot1x events enable

D.debug client authentication enable

E.debug client events enable

Correct Answers: A C

15: What are the LWAPP data and control port numbers?

A.TCP 12124 and 12134

B.UDP 12124 and 12134

C.TCP 12222 and 12223

D.UDP 12222 and 12223

E.TCP 16666 and 16667

F.UDP 16666 and 16667

Correct Answers: D

16: A VoWLAN user is complaining about bad voice quality. Which three problems are possible factors contributing to this issue? (Choose three.)

A.SNR is greater than 25 dB

B.packet loss is greater than 1%

C.jitter is greater than 30 ms

D.one-way delay is greater than 150 ms

E.round trip delay is greater than 150 ms

F.packet loss is greater than 0.1% but less than 1%

Correct Answers: B C D

17: What is the purpose of a radome?

A.to reduce the mechanical load from wind

B.to increase the gain of an antenna

C.to mitigate interference

D.to indicate which way the antenna is pointing

Correct Answers: A

18: At what distance does the curve of the earth factor into the antenna elevation calculation?

A.greater than 6 miles (~10 km)

B.greater than 26 miles (~42 km)

C.the width of the Fresnel zone, which varies depending on the distance by which the bridges are separated

D.60% of the Fresnel zone

Correct Answers: A

19: Refer to the exhibit. Given a client configured for LEAP authentication, a RADIUS server configured for LEAP, and an autonomous AP configured as shown in the exhibit.

If authentication fails for the client, what is the cause of this problem?

```
show:
aaa new-model
!
aaa group server radius eap_methods
 server 192.168.1.22 auth-port 1645 acct-port 1646
aaa authentication login default local
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
!
dot11 ssid test
  authentication open eap eap_methods
  authentication network-eap eap_methods

interface Dot11Radio0
 encryption mode wep mandatory
 !
 ssid test

interface BVI1
 ip address 192.168.1.113 255.255.255.0

radius-server host 192.168.1.22 auth-port 1645 acct-port 1646 key <blah>

show debug:
labap 1131 ip 113#sho debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
dot11 authenticator:
  state machine debugging is on
  process debugging is on
Radius protocol debugging is on
Radius packet protocol debugging is on

*Apr  6 21:05:39.668: AAA/BIND(00000016): Bind i/f
*Apr  6 21:05:39.668: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start
*Apr  6 21:05:39.669: dot11_auth_dot1x_send_id_req_to_client: Sending identity request to 000c.8591.6d84
*Apr  6 21:05:39.669: dot11_auth_dot1x_send_id_req_to_client: Client 000c.8591.6d84 timer started for 30 seconds
*Apr  6 21:05:39.676: dot11_auth_parse_client_pak: Received EAPOL packet from 000c.8591.6d84
*Apr  6 21:05:39.677: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,EAP_START) for
000c.8591.6d84
*Apr  6 21:05:39.677: dot11_auth_dot1x_send_id_req_to_client: Sending identity request to 000c.8591.6d84
*Apr  6 21:05:39.677: dot11_auth_dot1x_send_id_req_to_client: Client 000c.8591.6d84 timer started for 30 seconds
*Apr  6 21:05:39.677: dot11_auth_parse_client_pak: Received EAPOL packet from 000c.8591.6d84
*Apr  6 21:05:39.678: dot11_auth_parse_client_pak: id is not matching req-id: 1 resp-id: 2, waiting for response
*Apr  6 21:05:39.681: dot11_auth_parse_client_pak: Received EAPOL packet from 000c.8591.6d84
*Apr  6 21:05:39.681: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for
000c.8591.6d84
*Apr  6 21:05:39.681: dot11_auth_dot1x_send_response_to_server: Sending client 000c.8591.6d84 data to server
*Apr  6 21:05:39.681: AAA/AUTHEN/PPP (00000016): Pick method list 'Permanent Local'
*Apr  6 21:05:39.682: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds
*Apr  6 21:05:39.682: dot11_auth_dot1x_parse_aaa_resp: Received server response: FAIL
*Apr  6 21:05:39.682: dot11_auth_dot1x_parse_aaa_resp: found eap pak in server response
*Apr  6 21:05:39.682: Client 000c.8591.6d84 failed: EAP reason 0
*Apr  6 21:05:39.682: dot11_auth_dot1x_parse_aaa_resp: Failed client 000c.8591.6d84 with aaa_req status_detail 0
*Apr  6 21:05:39.682: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_FAIL) for
000c.8591.6d84
*Apr  6 21:05:39.683: dot11_auth_dot1x_send_response_to_client: Forwarding server message to client
000c.8591.6d84
*Apr  6 21:05:39.683: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 seconds
*Apr  6 21:05:39.683: dot11_auth_dot1x_send_client_fail: Authentication failed for 000c.8591.6d84
```

A.The RADIUS server timeout: This timeout is too short; the access point will wait for the RADIUS server, then the timer will expire and authentication will fail.

B.The RADIUS server at 192.168.1.22: There is either a RADIUS key mismatch or user

credentials are not matching on the RADIUS Server.

C.The client supplicant: This client is providing the wrong EAP-ID in its EAP Identity response.

D.The AP: The AP is misconfigured, because the authentication is set to use the local database on the AP.

E.The AP: The AP is misconfigured, because WEP uses static keys and is not compatible with LEAP.

Correct Answers: D

20: When a wireless client performs a Layer 2 roam between two WLCs with management IP addresses on different IP subnets but dynamic interfaces in the same VLAN, which two actions happen? (Choose two.)

A.The new WLC exchanges mobility messages with the original WLC and the client database entry is moved to the new WLC.

B.The original WLC marks the client with an "Anchor" entry in its own client database.

C.The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new WLC.

D.The client database entry is maintained on both the original and new WLCs.

E.The client database entry is removed from the original WLC once it has been entered into the new WLC.

F.All traffic to the client from the LAN is sent through an IP tunnel via Ethernet from the original WLC to the new WLC.

Correct Answers: A E