

Exam : **351-050**

Title : CCIE Wireless Beta Written Exam

Version : Demo

www.Pass4itSure.com

1. Which two options are correct according to debug output presented in the following exhibit? (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
line4474 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(0)]
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)
```

- A. The wireless client uses a static IP address, so "0.0.0.0 START (0)" can be found in the logs.
- B. The wireless client has been successfully authenticated. Reauthentication is set to occur on an extremely aggressive schedule (every five seconds).
- C. 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.
- D. Since the AP receives a probe request from the wireless client, the Access Point Function state for the machine changes from "Idle" to "Probe."

Answer: C,D

2. Which two statements correctly describe RTS/CTS? (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. Since the introduction of EDCA (WMM and 802.11e), the RTS/CTS sequence has been rendered unnecessary.
- C. 802.11d replaced the RTS/CTS sequence with CTS to Self.
- 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.

Answer: A,D

3. The following message can be seen 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. Which action should you take?

- A. Check the logs for rogues in the area, then turn on rogue mitigation.
- B. Seek out the source of the noise with a spectrum analyzer.
- C. Manually increase the power of the AP to overcome the interference.
- D. Increase the interference threshold from the default 10%.

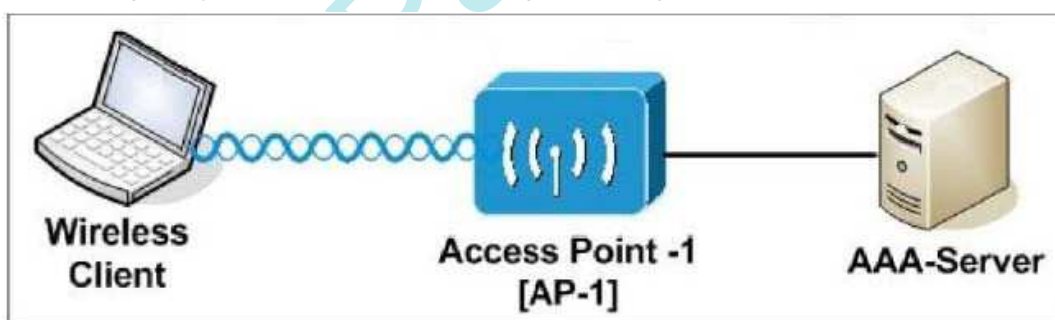
Answer: B

4. Study the following situations carefully, then answer my question. Wireless client (CB21) configured for SSID "CCIE-2"; IP address "dhcp". Configure standalone autonomous AP with three SSIDs and three data VLANs plus the native VLAN. AAA server IP ranges:

VLAN-2: 10.20.1.1.100-10.20.1.1.128 VLAN-3: 10.30.1.1.100-10.30.1.1.128

VLAN-4: 10.40.1.1.100-10.40.1.1.128

The user wants to get an IP address from VLAN-2 which is mapped to the SSID CCIE-2 the client is associating. Why does this wireless client get a wrong IP address?



- A. LEAP authentication fails due to wrong password or unknown username, therefore the wireless client is mapped to the default VLAN.
- B. The RADIUS server is not reachable from the AP, therefore the wireless client is mapped to the default VLAN.
- C. LEAP needs "network-eap" <eap_methods> on the SSID. You must not configure "open eap" <eap_methods.>
- D. The RADIUS server assigned VLAN-4 during authentication/authorization process.

Answer: D

5. It is suggested that you prime or stage your lightweight access points in a convenient location, rather than after they have been installed in locations that may be difficult to reach. Which three items can be configured by using the controller CLI, controller GUI, or Cisco WCS while priming a lightweight AP prior to deployment? (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 the access-point-specific LED blink sequence
- D. To configure the access-point-specific 802.11a, 802.11b, and 802.11g network settings

Answer: A,B,D

6. How to describe the radiation pattern of patch and Yagi antennas when viewed from the side (Hplane)?

- A. The patch patterns are egg-shaped, the Yagi patterns are conical
- B. The patch patterns are doughnut-shaped, the Yagi patterns are conical
- C. The patch patterns are conical, the Yagi patterns are doughnut-shaped
- D. The patch patterns are conical, the Yagi patterns are egg-shaped

Answer: A

7. Which description concerning wireless voice traffic is correct?

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

Answer: A

8. Observe the following statements, which limitation applies to the use of the Cisco WLAN Solution Management over Wireless feature?

- A. Read-write access is not available; only read-only access is supported.
- B. Controllers must be managed using only secure protocols (that is, SSH and HTTPS), not nonsecure protocols (that is, HTTP and Telnet).
- C. Uploads and downloads from the controller are not allowed.
- D. Wireless clients can manage other controllers however not the same controller and AP to which the client is associated.

Answer: C

9. Observe the following options carefully, which functionality, as defined by IEEE 802.11e, does WMM certify as part of the tests for QoS done by the WiFi Alliance?

- A. EDCA
- B. HCCA
- C. Direct Link Setup
- D. S-APSD

Answer: A

10. Lightweight Access Point Protocol or LWAPP is the name of a protocol that can control multiple Wi-Fi wireless access points at once. How does the Cisco WCS know what has happened in an LWAPP system when an AP's interface goes down and then comes up again?

- A. The Cisco WCS polls the APs and when the AP is unreachable, reports "Max retransmissions reached on AP <name>".
- B. 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.
- C. 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.
- D. The Cisco WLC sends a trap to the Cisco WCS when it detects that an AP is down.

Answer: D

11. You work as a network engineer. If the WLAN interfaces configured on the different controllers are on different IP subnets (Layer 3 inter-controller roaming), can you tell me what will happen when a client roams from one controller (controller A) to a new controller (controller B)?

- A. 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.
- 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 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.
- D. Controller B will update its client database and all client ingress and egress traffic will transition to the new controller.

Answer: B

12. You work as a network technician at Company.com, read this subject carefully, then answer the question. The existing Cisco Unified Wireless Controller is running v5.0 code for both the controllers and the Cisco WCS. A controller has been configured with an appropriate rogue rule condition to report discovered APs to the Cisco WCS. What default alarm level is used to display all rogue APs in the Alarm Summary?

- A. Major
- B. Critical
- C. Flash
- D. Minor

Answer: D

13. 802.11i is a forthcoming specification that will clear up a number of security problems in 802.11. For the following items, which 802.11i key can provide data origin authenticity during the four-way handshake and the group key handshake messages?

- A. Key Caching Key
- B. Key Encryption Key
- C. Groupwise Master Key

D. Key Confirmation Key

Answer: D

14. For the following commands, which one can determine the health of a RADIUS server on an autonomous AP?

- A. show radius statistics
- B. debug radius-server
- C. show radius table {server_ip} D.
- show radius-server {server_ip}

Answer: A

15. In order to be able to communicate with the WDS master, what must be configured on the APs while setting up a WLAN for Wireless Domain Services?

- A. Username and password valid on the AAA server
- B. Multicast group for the WDS
- C. Ip address of the master WDS and any backup master WDS
- D. Pre-shared key which matches that of the master WDS

Answer: A

16. Cisco Client Management Frame Protection is running on a mobility group with two controllers. For the following options, which two MFP requirements protect the network?

(Choose two.)

- A. Requires the use of a nonbroadcast SSID
- B. Requires CCXv5
- C. Implements the validation of wireless management frames
- D. Forces clients to authenticate, using a secure EAP method only

Answer: B,C

17. Refer to the following options, which two are long-term solutions to hidden node problems? (Choose two.)

- A. Enable CTS to Self
- B. Change the RF situation by increasing the power on client work stations (None-AP-STA)
- C. Increase the radio speed to at least 24 Mb/s
- D. Change the RF situation by adding additional access points

Answer: B,D

18. A user complains about problems authenticating via wireless. Which two of the Cisco WLC debug commands below would solve this problem? (Choose two.)

- A. debug mac { addr MAC}
- B. debug client authentication enable
- C. debug dot1x events enable
- D. debug client events enable

Answer: A,C

19. Can you tell me what the LWAPP data and control port numbers are?

- A. TCP 16666 and 16667
- B. UDP 16666 and 16667
- C. TCP 12124 and 12134
- D. UDP 12222 and 12223

Answer: D

20. The central office is currently using a combination of 4400 and 2100 series WLAN controllers running v4.2 and a variety of LWAPP-enabled access points servicing both 2.4 GHz and 5 GHz. The WLAN deployment has been extended to each remote office by implementing a 526 WLAN controller running v4.1 and several 521 access points. Wireless client deployment uses EAP-TLS authentication by use of a centralized RADIUS server plus 802.11n for performance. After the first remote office deployment, remote office users complain that they are not connecting via 802.11n. Which will most likely cause this problem?

- A. The 521 AP does not support 5 GHz, which prohibits 802.11n.
- B. The 521 AP and 526 WLAN controllers do not support AES, which prohibits 802.11n.
- C. The 526 WLAN controller does not support external authentication via RADIUS, prohibiting authentication.
- D. The 526 WLAN controller does not support 802.11n with either v4.1 or v4.2.

Answer: D

21. A VoWLAN user reports bad voice quality. Which three items most likely cause this problem? (Choose three.)

- A. Round trip delay is greater than 150 ms
- B. Packet loss is greater than 1%
- C. Jitter is greater than 30 ms
- D. One-way delay is greater than 150 ms

Answer: B,C,D

22. Which is the objective of a radome?

- A. To reduce the mechanical load from wind
- B. To indicate which way the antenna is pointing
- C. To increase the gain of an antenna
- D. To mitigate interference

Answer: A

23. Do you know at what distance the curve of the earth factors into the antenna elevation calculation?

- A. Greater than 6 miles (~10 km)
- B. 60% of the Fresnel zone
- C. Greater than 26 miles (~42 km)
- D. The width of the Fresnel zone, which varies depending on the distance by which the bridges are separated

Answer: A

24. How do the characteristics that are available on the Cisco WCS for Linux version differ from those of

the Cisco WCS for Windows version?

- A. Cisco WCS for Linux is required for deployments.
- B. Assuming that there are no differences in hardware, a Cisco WCS for Linux can support up to 750 wireless LAN controllers. A Cisco WCS for Windows can support up to 250 wireless LAN controllers.
- C. Cisco WCS for Windows includes support for Cisco Spectrum Expert clients. Cisco WCS for Linux does not support Cisco Spectrum Expert clients.
- D. There are no differences in features between the Linux and Windows versions of Cisco WCS.

Answer: D

25. You are a network technician. According to the following exhibit, a client configured for LEAP authentication, a RADIUS server configured for LEAP, and an autonomous AP configured as displayed. If authentication fails for the client, which is the most likely cause of this problem?

www.Pass4itSure.com


```

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 authentication exec default local
aaa accounting network acct_methods start-stop grouprad_acct
!
dot11 ssid test
 authentication open eap eap_methods
 authentication network-eap eap_methods

interface Dot11Radio0
 encryption mode wepmandabry
!
ssid test

interface BV11
 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 1131ip 113#show debug
General OS:
 AAA Authentication debugging is on
 AAA Authentication 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 dot1_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 EAP OL packet from 000c.8591.6d84
*Apr 6 21:05:39.677: dot11_auth_run_rfm: 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 EAP OL packet from 000c.8591.6d84
*Apr 6 21:05:39.678: dot11_auth_parse_client_pak: id is not matching req-id: lresp-id:2,waiting for response
*Apr 6 21:05:39.681: dot11_auth_parse_client_pak: id Received EAPOL packet from 000c.8591.6d84
*Apr 6 21:05:39.681: dot11_auth_dot1x_run_rfm: 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 'Permanant Local'
*Apr 6 21:05:39.682: dot11_auth_dot1x_send_response_to_server: Stated 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: EAPreason 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_rfm: Executing (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 client supplicant: This client is providing the wrong EAP-ID in its EAP Identity response.
- B. 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.
- C. 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.
- D. The AP: The AP is misconfigured, because the authentication is set to use the local database on the AP.

Answer: D

26. Which two actions will happen when a wireless client deploys a Layer 2 roam between two WLCs with

management IP addresses on different IP subnets but dynamic interfaces in the same VLAN? (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 client database entry is maintained on both the original and new WLCs.
- C. The original WLC marks the client with an "Anchor" entry in its own client database.
- D. The client database entry is removed from the original WLC once it has been entered into the new WLC.

Answer: A,D

27. What is the reason that using a tool like Cisco Spectrum Expert is important?

- A. It maps the RF area to a floor plan.
- B. It allows you to detect multipath.
- C. It allows you to see the radiating environment at Layer 1.
- D. It decodes WLAN IPS attacks

Answer: C

28. In the AP Layer 3 controller discovery process, after the LWAPP Discovery Request is broadcast on a local subnet, which action will AP take next?

- A. Send an LWAPP response to the master controller if known.
- B. Send an LWAPP discovery request to controllers learned via OTAP if operational.
- C. Wait 5 seconds and resend a Discovery Request to the local subnet.
- D. Determine whether the controller responses are the primary controller.

Answer: B

29. Which three options are true when an H-REAP AP is in the "authentication down/local switching" state for a given WLAN? (Choose three.)

- A. New WebAuth sessions are permitted.
- B. The AP continues to send beacon probes and responses to keep current clients connected.
- C. 802.11 roaming events incur a full 802.1X re-authentication.
- D. Any new clients trying to authenticate are rejected.

Answer: B,C,D

30. Tom works as a network administrator for a company. He is asked to manually configure the Tx power on an 802.11b access point to a power level of 1 (100 mW) after implementing a Cisco 7921G wireless IP phone within a Cisco Unified Wireless Network. Which problem is the user likely to experience when the phone associates to the AP?

- A. One-way audio
- B. Loss of connectivity to Cisco Unified Communications Manager
- C. Audio delay or jitter or both
- D. The phone displays a "network busy" status message

Answer: A

Trying 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 **69,000** Satisfied Customers Worldwide
- ★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

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

To update a previously submitted ticket:



Submit A 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.



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.



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.

Guarantee & Policy | Privacy & Policy | Terms & Conditions

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

All trademarks are the property of their respective owners.

Copyright © 2004-2014, All Rights Reserved.