**Exam Code: MB0-001**

GRATIS EXAM
*Free Practice Exams*

http://www.gratisexam.com/

**Exam Code: MB0-001**

**Exam Name: CompTIA Mobility+ Certification Exam**

ExamSheets
DISCOVER CERTIFICATION EXAM ANSWERS

**QUESTION 1**
Which of the following would be used to enforce a policy requiring two-factor authentication on certain mobile devices?

A.  Username and password
B.  Facial recognition and PIN
C.  Pattern unlock and password
D.  Fingerprint and retina scan

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 2**
An employee reports a network connectivity issue to the helpdesk. Which of the following steps should be taken before escalating the issue?

A.  Identify and document the issue, questioning the obvious
B.  Attempt to resolve the network issue by rebooting a server
C.  Ask the user to remote their machine and wait 15 minutes before calling back
D.  Document resolution outcomes and lessons learned

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 3**
Which of the following can be applied to a mobile device to support a corporate mandate which does not allow Internet gambling activities?

A.  Network IDS
B.  Host IDS
C.  Software antivirus

D. Content filtering

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 4**
An end-user has notified the helpdesk that a tablet was left in a taxi-cab. Which of the following is the order of response?

A. Wipe device, track device, escalate
B. Wipe device, confirm end-user identity, escalate
C. Confirm end-user identity, determine policy response, report incident

D. Confirm end-user identity, unlock device, track device

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 5**
The IT department has been contacted by Joe, an end-user, reporting he is unable to login to his smart phone. Which of the following would cause this issue?

A. The certificate for the Wi-Fi has expired
B. Passwords must be changed after a certain amount of days
C. Updates are required to the OS
D. The device is not connected to the Internet

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 6**
Which of the following is used so that mobile devices can continue to communicate with a mobile device management service if multiple front-end servers are configured?

A. Cellular tower
B. Network load-balancer
C. Traffic shaper
D. Proxy server

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 7**
Which of the following secure protocols is used for Microsoft Exchange ActiveSync communications traffic?

A. HTTPS
B. MAPI
C. SMTP
D. SFTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 8**
Which of the following must be used to successfully deploy an in-house developed application?

A. LDAP server
B. Application certificate store
C. Content management solution
D. Enterprise application store

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 9**
Joe, a user, has noticed that his corporate-owned device has been stolen. Which of the following actions should Joe take FIRST?

A. Report the incident
B. Revoke the device certificate
C. Monitor device activity
D. Capture logs

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 10**
Ann, a user, called to report an issue related to authenticating to her mobile device. After resolving the issue, which of the following is the FINAL task that should be completed by the mobility administrator according to troubleshooting best practices?

A. Establish a theory of probable cause
B. Verify full system functionality
C. Document findings, actions, and outcomes
D. Implement preventative measures

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

## QUESTION 11
A technician receives a trouble ticket that Joe, a wireless customer, cannot access his email. As part of the troubleshooting process, the technician gathered information and identified the symptoms. Which of the following is the NEXT logical step in troubleshooting?

A. Test the theory
B. Document findings and outcomes
C. Establish a theory to determine the cause
D. Implement the solution

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

## QUESTION 12
Which of the following can be used to secure data at rest? (Select TWO).

A. VPN
B. AES
C. SSL
D. 3DES
E. IPsec

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 13**
Which of the following is a best practice for configuring mobile network access control?

A. Device password
B. Certificate authentication
C. IPsec VPN
D. ActiveSync

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 14**
A company wants to deploy a wireless network for their employees and guests. Employee and guest networks should be separated for security and privacy. Which of the following can be implemented to meet these requirements? (Select TWO).

A. TCP
B. UDP
C. APN
D. SSID
E. VLAN

**Correct Answer:** DE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 15**
Guests are allowed to use the company wireless network for Internet access only by connecting to the guest SSID through a captive portal for authentication.
Guests reported that they connected to the Internet without captive portal authentication. Which of the following would BEST explain this problem?

A. Directory services authentication failure
B. DHCP failure
C. DNS failure

D. Rogue access point

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 16**
Which of the following describes dynamically switching from one cellular tower to the next without dropping connectivity in cellular and WiFi networks?

A. Bouncing
B. Roaming
C. Failover
D. 3-way handshake

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 17**
Joe, a network technician, has been using the company smart phone to fulfill his job role. Joe must return the company smart phone at the end of his shift. Upon retrieving the smart phone at the start of his shift, the phone is not sending text nor making phone calls. Other coworkers were not experiencing these issues. Which of the following is the MOST likely problem?

A. Joe is encountering a jamming attack.
B. The smart phone is out of reach from the cellular tower.
C. The smart phone's network mode setting was changed from automatic to manual.
D. The smart phone battery option is conflicting with the network mode options.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 18**
The chief executive officer (CEO) is reporting extreme latency issues with three new wireless access points. The CEO and the financial department stream stock quotes all day through their tablets. The total number of wireless users in the building is 280. Which of the following is the MOST probable cause?

A. The wireless access points are not utilizing a wireless network controller.
B. The wireless access points are experiencing a high level of interference because of newly installed cubicles.
C. The wireless access points are not broadcasting.
D. The wireless access points areover utilized.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 19**
Which of the following are considered security protocols? (Select THREE).

A. TLS
B. GCM
C. POP3
D. SSL
E. IMAP
F. 3DES
G. SMTP

**Correct Answer:** ADF
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 20**
Which of the following is the BEST way to renew an expired remote employee's device certificates?

A. Email the certificates to the personal email account so the employee can import them
B. Remote into the device and update the certificates with administrative rights
C. Ask the employee to perform a device level wipe and reactivate the device on MDM
D. Have the employee delete all policies and reactivate the device on MDM

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 21**
Which of the following protocols ensures reliable communication?

A. TCP
B. UDP
C. MAC
D. IP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 22**
Which of the following protocols is used to configure devices and to gather information for reporting?

A. POP3
B. PoE
C. SNMP
D. MIB

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 23**
Which of the following methods would MOST likely prevent a laptop from being booted without the correct key or password?

A. File level encryption

B. Full-disk encryption

C. Folder level encryption

D. Removable media encryption

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 24**
A device that maliciously transmits on the same frequency as another device, which would prevent normal wireless communication, is an example of:

A. Spoofing

B. Sandboxing

C. Jamming

D. Rooting

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 25**
An antenna that propagates its signal in 360 degrees is called which of the following?

A. Semi-directional

B. Parabolic

C. Directional

D. Omni-directional

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 26**
Which of the following phenomenon results in decreased signal levels due to passing through a solid structure?

A. Reflection

B. Absorption

C. Attenuation

D. Refraction

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 27**
Joe, a help desk technician, is receiving multiple calls that WiFi is not working in a new area of the building. Joe determines that the coverage should be adequate. Which of the following would be the recommended escalation procedure?

A. Log analysis

B. Spectrum analysis

C. Protocol analyzer

D. Penetration testing

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 28**
It takes a user 20 seconds or more to send mail from a remote location, and experiences intermittent slowness during web browsing. The technician determines that the network signal is adequate. There is a large meeting in the conference room adjacent to the user. Which of the following conditions is MOST likely occurring?

A. Email congestion
B. Bandwidth optimization
C. Content filtering
D. Network latency

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 29**
A user traveling overseas is in a place where there is access to WiFi. The user can receive email and talk using VoIP, but cannot place or receive phone calls. Which of the following is the MOST likely cause of this issue?

A. The phone will need a new SIM card
B. Incompatible cellular technology
C. ICCID needs to be changed
D. IMEI needs to be changed

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 30**
The proper order to configure a mobile device for use with an MDM system is:

A. install client, sign in to server, accept certificates, install profiles.

B. install profiles, install client, accept certificates, sign in to server.

C. sign in to server, install profiles, install client, accept certificates.

D. sign in to server, install profiles, accept certificates, install client.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 31**
The correct sequence for deploying a new security profile in an MDM server is:

A. deploy to test group, observe results, create policy, deploy profile.

B. create policy, deploy to test group, observe results, deploy profile.

C. observe results, deploy profile, create policy, deploy to test group.

D. deploy profile, observe results, create policy, deploy to test group.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 32**
Which of the following technologies isolates the internal network from the outside world?

A. Email server

B. Rogue access point

C. DNS server

D. DMZ

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 33**
Ann, an employee, works remotely most of the time, only visiting the office for quarterly meetings. During one of these visits, a wireless technician picks up a new network that seems to be broadcasting from Ann's laptop. Which of the following types of networks has the technician encountered?

A. WLAN
B. Point-to-point
C. VPN
D. Ad-hoc

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 34**
A wireless administrator has been tasked with ensuring all WAPs backup their configurations on a daily basis at a 24/7 operations center. This backup cannot take place over the wireless network without interrupting operations. Which of the following should be implemented to meet these requirements?

A. QoS
B. Traffic shaping
C. Backhauling traffic
D. Off-hours backups

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 35**
A corporation provides their board members with tablets, preloaded with materials containing sensitive information, at each board meeting. Prior to one of the quarterly meetings, the operating system for the tablet is updated to include mandatory cloud storage of all information on the devices. Which of the following actions can be taken to maintain usability for these tablets while reducing the risk of leaking sensitive information to an outside party?

A. Revoke tablet certificates from trusted sources and cloud sites
B. Block communication from the tablets to the cloud storage provider
C. Remove communication from the tablets to external networks
D. Harden the tablets to only allow connections from trusted sources

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 36**
An insurance company has employees responding to a regional disaster through use of mobile printers and tablet devices. Which of the following options should be allowed on mobile devices to ensure the employees are able to route through a number of impassable road ways in order to aid customers as quickly as possible?

A. Location services
B. PAN
C. Geo-fencing
D. Self-service portals

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 37**
Joe, an employee, from a company with a BYOD policy synchronizes his mobile device information to his home computer on a weekly basis. After connecting to Joe's corporate network for the first time, all of his stored files are no longer recognized by his home computer. Which of the following policies is MOST likely causing this issue to occur?

A. Encryption of all device information
B. Remote wipe
C. Application and OS patching on the mobile device
D. OS patching on the home computer

**Correct Answer:** A

**QUESTION 38**
Which of the following can be used to ensure login credentials are secured when in transit from a mobile device's browser to a web server? (Select THREE).

A. 3DES
B. DES
C. MD5
D. HTTPS
E. SSL
F. TLS
G. AES

**Correct Answer:** DEF

**QUESTION 39**
Joe, an employee, contacts the database administrator about an issue with a local database on his hard drive. Which of the following questions would be MOST helpful in determining the next step in troubleshooting?

A. What is the state of the database service?
B. What is the error message being received?
C. Is there a connection to the Internet?
D. What is the password being used to access the database?

**Correct Answer:** B

**QUESTION 40**
An outside firm has been hired to conduct a penetration test on a company. The firm informs the company of what tools may be used, when the test will be completed, and the IP addresses they will be attacking from. The IPS is setup to ignore all alerts geared around the tools during this timeframe. Which of the following is at risk of occurring in this scenario?

A. Content filter misconfiguration
B. False negative
C. Authentication failure
D. False positive

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 41**
A large organization, with multiple remote locations, is looking for a way to securely provision company-owned mobile devices. Which of the following would be BEST to use for MDM enrollments?

A. LDAP
B. IMEI
C. SCEP
D. ICCID

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 42**
Corporate users have been assigned locked-down mobile devices where the ability to add, remove, or update the software and operating system has been disabled. Which of the following can be used to approve centralized device updates?

A. Problem management
B. Incident management
C. Change management
D. Asset management

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 43**
Ann, a user, wants to configure the email client on her newly purchased mobile device. Ann wants to ensure that the phone email client and the email server stay synchronized at all times, and that offline changes to the read status of an email will be synchronized once the phone is online. Which of the following should she configure?

A. IMAP
B. SSMTP
C. POP
D. SMTP

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 44**

An administrator wants to configure two-factor authentication on all enterprise-owned mobile devices. Which of the following should the administrator configure?

A. Username and password
B. Face recognition and PIN
C. Face recognition and thumbprint
D. Pattern lock and PIN

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 45**
Which of the following should a mobile administrator deploy to prevent sensitive company information from being transmitted to an employee's personal email account?

A. Transmission encryption
B. DLP system
C. Content filter
D. Mobile antivirus

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 46**
Two children have been given new phones by their parents with the GPS tracking feature enabled. Both phones are powered on and have connectivity. Which of the following is the MOST likely cause of why the parents are unable to track their children's location?

A. The children's phones did not come with a removable SD card.
B. The GPS on the parent's phone is not enabled.
C. The location service is not working properly.
D. The phone is only connected to three satellites.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 47**
An administrator has installed a network based security appliance. The security appliance was placed between the email server and the company's Internet gateway. Employees are now reporting issues with email synchronization. Which of the following is the MOST likely reason for the issue?

A.  The SSL certificate on all employees' mobile devices has expired.
B.  The employees are reporting what is known to be a false positive.
C.  A required port is being blocked by the newly installed network device.
D.  The email server must be reconfigured to account for the security appliance.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 48**
Which of the following is a characteristic of 802.11a?

A.  802.11a uses dual band.
B.  802.11a is unable to stream video.
C.  802.11a uses 5 GHz.
D.  802.11a uses 2.4 GHz.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 49**

Which of the following is a BEST practice when selecting corporate cellular hardware devices?

A. Choose based on frequency hopping capabilities
B. Choose the AP from one vendor and terminals from others
C. Choose devices from the same wireless carrier
D. Choose devices based on user preference

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 50**
When mobile users roam from one point of a building to another, their connection drops and they have to reinitiate pending downloads. The administrator determines that the signal is weak in certain areas of the building. Which of the following is the BEST way of addressing this issue?

A. Identify areas as known dead zones for wireless connectivity
B. Increase the signal strength in the mobile device
C. Use a different SSID while roaming the building
D. Strengthen AP signal and AP device placement

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 51**
An administrator is tasked with implementing disk encryption for information stored on a mobile device with at least 128-bits of strength. Which of the following should be applied to meet this requirement?

A. AES
B. SSL
C. SHA-1
D. DES

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 52**
Joe, a corporate MDM administrator, needs to implement device encryption. Which of the following would provide the BEST encryption?

A.  Data in transit encryption
B.  Block level device encryption
C.  Folder level device encryption
D.  Whole device encryption

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 53**
Which of the following should MOST likely be used at corporate headquarters to secure transmission between a mobile device and a wireless access point?

A.  VPN
B.  SSL
C.  WPA2
D.  TLS

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 54**

Which of the following is MOST likely to be used by default for WPA2?

A. AES
B. TKIP
C. WEP
D. 3DES

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 55**
During the e-discovery process, a litigation hold has been placed on information stored in several areas, including the mobile device of the Chief Financial Officer (CFO). Which of the following steps should be taken to prove the data integrity of information on this device during the investigation?

A. Review logging on the device and connecting MDM server
B. Isolate the device and apply chain of custody controls
C. Encrypt information stored internally on the device
D. Hash information stored on the device

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 56**
An administrator has been informed that one of the systems on the corporate network has been compromised. Which of the following steps should the administrator take NEXT to initiate proper incident response?

A. Take screen shots and copy logs from the affected machine, storing these in a secured environment.
B. Use MD5 on the system and backup the current image if the system is virtual.
C. Isolate the device and perform a device wipe.
D. Alert the incident response team and await further instruction on procedures.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 57**
Which of the following involves a key exchange which introduces the vulnerability of a man-in-the- middle attack?

A. SSL
B. RSA
C. Kerberos
D. PKI

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 58**
An administrator noticed a number of mobile devices are downloading applications from

unauthorized mobile application stores. Which of the following has MOST likely occurred?

A. Jamming
B. Jailbreaking
C. Out-of-date virus definitions
D. Keylogging

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 59**
An administrator has been tasked with correlating system logs to identify brute force attacks. Which of the following would allow for this as well as a centralized location to review system logs?

A. NIDS
B. SIEM
C. NIPS
D. DLP

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 60**
Which of the following devices can be used to block a list of known malicious IP addresses at the furthest edge of a corporate network?

A. Network firewall
B. Software firewall
C. NIDS
D. HIPS

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 61**
Ann, an attacker, has spoofed a mobile device serial number so she can connect to the MDM environment. Which of the following would an administrator check to uncover this attack?

A. Review the SIEM logs on a corporate network to determine authentication issues
B. Review certificate revocations by the MDM
C. Review connection attempts to the network from that phone's serial number
D. Review recent connection locations, looking for an abnormal location

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 62**
Ann, an end-user reports, that she cannot access popular web pages unless she enters the IPv4 address of the site. Which of the following ports is MOST likely blocked for the device?

A. 25
B. 53
C. 80
D. 443

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 63**
Which of the following allows devices to access an organization's WiFi network before ensuring that they conform to policy?

A. Captive portal
B. SCEP portal
C. TKIP portal
D. Administrative portal

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 64**
Which of the following is a capability of geo-fencing?

A. Enable SDLC on device
B. Disable corporate firewall
C. Enable POE-injector of device
D. Disable camera on device

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 65**
Which of the following technologies allows secure communication with a previously unverified entity?

A. VPN
B. IMAP
C. TKIP
D. PKI

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 66**
Which of the following helps ensure that a correct channel is configured for an access point?

A. Geo-fencing analysis
B. Directory analysis
C. Firewall analysis
D. Spectrum analysis

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 67**
Which of the following technologies allows a network administrator to force traffic to be cached by
a network device?

A. Proxies

B. Certificates
C. Roaming
D. Biometrics

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 68**
In the troubleshooting process, which of the following steps help identify the problem? (Select TWO).

A. Provide additional training
B. Capture logs
C. Implement preventative measures
D. Document the findings and outcomes
E. Identify symptoms

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 69**
While troubleshooting a problem reported by an end-user, which of the following steps comes between establishing a plan of action and implementing the plan of action?

A. Gather information
B. Verify full system functionality
C. Question the user
D. Identify potential effects

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 70**
Which of the following is the MOST important consideration for in-house application development?

A. Attenuation
B. Platform
C. Topology
D. Firmware

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 71**
A user is able to view unauthorized websites using a secure MDM browser on a device. Which of the following is BEST used for troubleshooting the issue?

A. Group membership
B. Firewall port configuration
C. Certificate authentication
D. Firmware version

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 72**
Corporate policy stipulates user accounts only be granted to employees; however, many departments within the organization use private consultants to assist with various projects. Which of the following allows consultants network access without compromising security? (Select TWO).

A. Provide open wireless access.
B. Provide wireless guest network access.
C. Provide an internal user account.
D. Provide VPN access.
E. Provide a CAT5 cable.

**Correct Answer:** BD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 73**
A well-known security organization has released an alert regarding an exploit that could affect a popular mobile device. Which of the following steps should the mobile device administrator take NEXT?

A. Force all users to change their pass codes.
B. Alert the user community.
C. Update firewall configuration.

D. Monitor the device logs.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 74**
Disabling which of the following jeopardizes device performance if enrolled in an MDM? (Select TWO).

A. APNS
B. SSMTP
C. RDP
D. ICMP
E. GCM

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 75**
An administrator can control network access to enterprise resources using which of the following?

A. AES encryption
B. SNMP
C. DNS
D. PKI

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 76**
Joe, a user, normally has access to internal network resources while in the office. Suddenly, his mobile device is not able to access any of the resources. Which of the following is the FIRST item to check in the troubleshooting process?

A. Whether the device is connected to the WiFi network
B. Whether the device is connected to the cellular network
C. Whether a VPN misconfiguration exists on the device
D. Whether a port misconfiguration exists on the device

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 77**
A user in a hotel is unable to see the hotel captive WiFi portal. Which of the following is the MOST likely explanation?

A. Encryption problem
B. VPN is active
C. APN issues
D. Location services problem

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 78**
When configuring user groups that use separate applications managed by the MDM solution, it is important that each group has its own:

A. Policy
B. AUP
C. APNS

D. High availability

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 79**
Which of the following is a best practice for protecting mobile devices that use RDP to access highly sensitive information? (Select TWO).

A. Block network connectivity

B. Block internal storage

C. Block personal backup

D. Block firewall traffic

E. Block SD storage

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 80**
Which of the following provides recourse in the event a third party application vendor causes application or network outages because of updates?

A. SLA

B. Sandboxing

C. EULA

D. Network segmentation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 81**
Which of the following strategies helps mitigate risk of data loss in a BYOD solution?

A. Firewalling
B. Content filtering
C. Antivirus implementation
D. Containerization

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 82**
Ann, a user, is in another country using her device, but when using the browser to find local restaurants she is seeing the search engine site for her home country. Which of the following is the MOST likely cause?

A. Roaming is disabled
B. Browser cache is full
C. VPN is active
D. GPS is disabled

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 83**
A user on a mobile device is unable to access a video-sharing website. Other network connectivity is working normally. Which of the following actions should the administrator perform to troubleshoot the situation? (Select TWO).

A. Check MAC address
B. Check APNS
C. Check user group

D. Check WiFi settings

E. Check MDM policy

**Correct Answer:** CE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 84**
Which of the following ports is used as alternate SMTP?

A. 25

B. 443

C. 587

D. 2175

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 85**
An administrator receives a call from Ann, a user, after wiping her device. The server does not allow Ann to re-enroll the device, while other users are able to enroll their devices successfully. The administrator confirms that Ann's account is not the problem. Which of the following can cause this?

A. Group policy is misconfigured

B. Ann has locked out her directory account

C. The password was entered incorrectly in the self service portal

D. Policy limits one device per person

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 86**
Which of the following is an example of a faraday cage?

A.  Location that blocks API policies
B.  Secured enterprise datacenter
C.  Location that blocks RF signals
D.  Area that secures unauthorized individuals from accessing the datacenter

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 87**
Which of the following can be either broadcasted or hidden?

A.  GPRS
B.  PAN
C.  SSID
D.  WiMAX

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 88**
Which of the following services can be used to improve streaming traffic across networks?

A.  UDP
B.  DoS
C.  SMTP
D.  QoS

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 89**
Which of the following devices can handle a full data backup from a device? (Select TWO).

A. SD card
B. SIM card
C. RF device
D. USB drive
E. RFID

**Correct Answer:** AD
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 90**
A replicated network at another location is used as part of which of the following?

A. Network backhauling
B. RAID 1
C. Incident response
D. Disaster recovery

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 91**
Which of the following is the correct sequence for promoting changes from development to production?

A. Quality Assurance, Development, Production
B. Development, Documentation, Production
C. Development, Quality Assurance, Production
D. Document, Development, Quality Assurance, Production

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 92**
BYOD is a concept that combines which of the following aspects of mobility?

A. Usability and security
B. Security and recovery
C. Security and performance
D. Usability and carrier agreements

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 93**
Which of the following BEST facilitates OTA on-boarding?

A. De-provisioning
B. Change management
C. Device certificate
D. Reset device
E. Device wipe

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 94**
Joe, an end-user, reports that his smart phone has been lost. Which of the following should a helpdesk staff member perform FIRST?

A. Call the phone number associated with the device.
B. Follow the approved response to the incident.
C. Lock or disable all of Joe's network accounts.
D. Initiate a remote wipe of Joe's device.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 95**
Ann, a user, reports that her touch screen enabled device is activating various icons and randomly calling people. Which of the following is the MOST likely cause of the issue?

A. Incomplete backup
B. The screen is dirty
C. Sync issues
D. RF interference

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 96**
Joe, a user, is unable to use the mapping features on his GPS enabled mobile device. The device is not able to show his exact point on the map included. Which of the following is the MOST likely cause?

A. Location services are disabled
B. Syncing has been disabled
C. Cellular latency is high
D. No cellular signal is available

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 97**
An organization needs to configure and deploy dozens of new mobile devices at a central location for use at various off-site locations. Which of the following deployment methods should the organization implement?

A. Image and deploy
B. Server push of applications
C. Mandatory Access Control
D. Remote control of devices

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 98**
Which of the following is the BEST practice to maintain awareness of new technologies?

A. Checking vendor websites and the Internet for updates after encountering issues
B. Attending a primary industry trade show annually
C. Periodically checking vendor websites for updated news and software releases
D. Registering for email updates from appropriate vendors, OEMs, and related companies

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 99**
Given a WiFi deployment using the 2.4GHz band, which of the following channels are the BEST for multiple mobile channel access deployment?

A. 1, 2, 3
B. 1, 6, 11
C. 3, 5, 7
D. 36, 40, 44

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 100**
Given an enterprise WLAN deployment, which of the following access point types is BEST to use?

A.  SOHO
B.  Point-to-point
C.  Point-to-multipoint
D.  Lightweight

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 101**
A wireless network administrator finds that many users are unable to achieve a link-speed of more than 130Mbps. Which of the following is the MOST likely cause?

A.  802.11b is enabled on the network
B.  Switches are set to half-duplex
C.  NAC is enabled
D.  The device supports only 2.4GHz

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 102**
A company has locations worldwide and needs to push promotional videos, a total of 10GB in size, to mobile devices in each region. Which of the following is the BEST content distribution method to minimize impact on company network?

A.  OTA
B.  VPN
C.  Centralized distribution
D.  Decentralized distribution

**Correct Answer:** D
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 103**
Which of the following ports are used by APNS? (Select TWO).

A. 2175
B. 2195
C. 2196
D. 3389
E. 8080

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 104**
A company replicates their MDM system to a geographically separate backup site. Which of the following is the BEST option to restore normal operations as soon as possible, in the event the
main site goes down?

A. Cold site
B. Hot site
C. Intermediate site
D. Warm site

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 105**

Which of the following is the BEST configuration for mission critical applications such as email that require load-balancing?

A. Active/Active
B. Active/Passive
C. Active
D. Passive/Passive

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 106**
A company does not wish to provide the WiFi network password to their employees. Which of the following is the BEST option to allow employees to connect to the company's WiFi if devices are managed by MDM?

A. Have an administrator configure each employee's mobile device
B. Push encrypted WiFi profile to mobile devices
C. Give MAC-based access to mobile devices
D. Give IMEI-based access to mobile devices

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 107**
Which of the following is the BEST practice to create groups within MDM server?

A. Manually create groups
B. Use VLANS
C. Use ACL
D. Use directory services

**Correct Answer:** D

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 108**
Which of the following application development methods delivers the BEST performance?

A. Hybrid
B. Native
C. Java
D. Web app

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 109**
Which of the following is the BEST model to deploy managed in-house applications?

A. Cloud storage service
B. Company web server
C. Enterprise application store
D. Email attachments

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 110**
An MDM console works with which of the following layers of the OSI model?

A. Application
B. Session
C. Transport
D. Presentation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 111**
Joe, an employee, is unable to unlock his mobile device and has forgotten the device password. Which of the following is the BEST way to resolve this issue?

A. Replace the certificate
B. Reset the password
C. Perform a soft reset of the device
D. Perform a hard reset of the device

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 112**
Which of the following is the definition of jailbreak?

A. Locking down a device and disabling all applications
B. Bypassing OEM OS security controls
C. Wiping personal data and returning the device to factory settings
D. Theft of a device and use by an unauthorized user

**Correct Answer:** B
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 113**
Ann, a user, can no longer receive corporate email on her mobile device, but she has Internet access and can receive her web-based personal email. Which of the following is the MOST likely cause?

A.  The device is having latency issues.
B.  The mail client needs to be reinstalled.
C.  The device is roaming.
D.  The email server is down.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 114**
A user's mobile phone will not keep a charge. Which of the following troubleshooting steps should a technician take to assist the user? (Select TWO).

A.  Check device backlight
B.  Check the connector
C.  Check operating system
D.  Check cellular data
E.  Check the power supply

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 115**
Which of the following technologies is considered PAN?

A. HSPA+

B. Bluetooth

C. Edge

D. IR

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 116**
Access points function at which of the following layers of the OSI model?

A. 2

B. 3

C. 4

D. 7

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

Topic 3, Volume C

**QUESTION 117**
Roaming between APs takes place in which of the following layers of the OSI model?

A. Data Link

B. Transport

C. Session

D. Presentation

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 118**
Joe, a user, reports that he does not have connectivity in WLAN. Which of the following is the FIRST approach a mobile technician should take for troubleshooting?

A. Use ICMP echo through ping
B. Check if DNS is providing name resolution
C. Use packet sniffer to investigate
D. Check if DHCP server is functioning

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 119**
Which of the following protocols is preferred for VoIP communication?

A. MAC
B. UDP
C. TCP
D. NAT

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 120**

Joe, a user, has problems connecting to the wireless network when he changes locations. Joe has a good signal and enters his credentials correctly, but cannot connect to the wireless network in the new location. Which of the following is the BEST course of action?

A. Check if the mobile device can be powered on in any location of the building
B. Check if Joe's password is still valid in the new location
C. Check whether new location blocks Joe's MAC address
D. Check if Joe is provided with the right IP address at the new location

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 121**
Which of the following is the BEST approach when installing 802.11 access points in a building to ensure that everyone will get a signal to attach to the WLAN?

A. Configure the adjacent access points in adjacent channel order
B. Configure the adjacent access points to use the same channel
C. Configure the adjacent access points to use channels that do not interfere with each other
D. Configure all the access points in the same floor on the same channel but different floors in different channels

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 122**
Which of the following is the BEST approach when configuring server-based management in

A. Mobile devices need their own server and should be configured as their own server-client.
B. Mobile devices can be configured just like any other device in the network based on requirement.
C. Mobile devices should be treated different than other device as they need more IP addresses.
D. Mobile devices should be configured on their own on the server regardless of the requirement.

**Correct Answer:** B

**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 123**
Which of the following is correct while designing/implementing mobility?

A.  More wavelength is required in order to cover all the users in crowded areas
B.  More mobile controllers and antennas are required in the crowded areas
C.  More users require more applications to be loaded in the crowded areas
D.  More frequencies are required in the crowded areas, one antenna is adequate

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 124**
Joe, a mobile user, claims he is unable to connect to resources on the WiFi network. Joe has a good signal and an IP address assigned to his device. Which of the following is the BEST troubleshooting technique that the administrator can take?

A.  Verify that Joe is able to connect to the cellular network.
B.  Verify that Joe is logged on to the network.
C.  Check the IP address to ensure it is in the correct range.
D.  Check the MAC address of the device.

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 125**
Which of the following is a WiFi topology that occurs when Ann, an end-user, configures her laptop to be a WiFi access point to which another device connects?

A. Gateway

B. Bluetooth

C. DMZ

D. Ad-hoc

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 126**
Which of the following technologies allows multiple network devices to have the same public source IPv4 address when communicating with other devices on the Internet?

A. DHCP

B. DNS

C. NAT

D. MAC address

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 127**
If an application stores data on corporate servers, which of the following is a technique to ensure that data is available even if someone accidentally deletes it?

A. Ensure that each server uses RAID 5

B. Perform regular backups of the servers

C. Install load balancers in front of multiple servers

D. Require VPN to access the corporate servers

**Correct Answer:** B

**QUESTION 128**
Which of the following technologies allows multiple devices to use a single source of authentication for access to services?

A.  Proxy services
B.  Trusted platform module
C.  Directory services
D.  VPN concentrator

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 129**
Which of the following is MOST likely to benefit from an MDM solution to support multiple platforms?

A.  BYOD
B.  Enterprise application store
C.  Self-service portal
D.  Onsite support kiosk

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 130**
Which of the following conditions are required for an administrator to be able to use an MDM solution to remote wipe a lost device? (Select TWO).

A. The device has network connectivity.
B. The device is locked.
C. The device's PIN is longer than 8 characters.
D. The device has an active VPN connection.
E. The device is enrolled with the MDM.

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 131**
Which of the following is the BEST technique to segregate corporate data from personal data on end-user devices?

A. Use an application that requires multifactor authentication
B. Use an application to sandbox device content
C. Require a specific version of TPM
D. Force all traffic over a corporate VPN

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 132**
For a device that has corporate data segregated from personal data, if the device is destroyed and replaced, which of the following must be available to ensure the BEST end-user experience on the replacement device? (Select TWO).

A.  Backup of corporate data
B.  Backup of full-disk encryption key
C.  Device PIN
D.  Backup of MDM enrollment certificate
E.  Backup of personal data

**Correct Answer:** AE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 133**
An application is installed through the enterprise MDM application store. An upgrade is issued and a single device does not receive the upgrade as expected.
Which of the following is the MOST likely cause?

A.  The user does not have a certificate installed.
B.  The user is assigned to the incorrect directory services group.
C.  The application store is unavailable or has experienced a temporary outage.
D.  The application was not signed.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**

Explanation:

**QUESTION 134**
An email password prompt appears on a device after a specific interval. Which of the following is the MOST likely cause?

A.  The email server was recently upgraded and mailbox configurations changed.
B.  The user's mailbox has exceeded the corporate size limits.
C.  The device battery level is low, requiring charging in order to sync password information.
D.  A password was reset according to corporate security policy guidelines.

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 135**
When addressing BYOD local backups, it is best practice to do which of the following?

A. Restore the device to factory settings
B. Allow personal backups at regular intervals
C. Encrypt and password protect backups
D. Save the backup to another source

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 136**
A potential security breach has occurred that requires a device policy change to mitigate the risk. The default policy sync interval is four hours. Which of the following should occur immediately?

A. Mobile administrator should manually push the changed policy to affected devices.
B. Mobile administrator should allow the policy change to occur at the regularly scheduled interval.
C. Mobile administrator should send a company-wide email alert.
D. Mobile administrator should quarantine any affected devices.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 137**
Which of the following is required to leverage Kerberos for authentication to internal resources from an external mobile device?

A. MDM
B. Firewall
C. SHA
D. Gateway

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 138**
If Android devices are synching email successfully, but iOS devices are not, which of the following is the MOST likely scenario?

A. Firewall port blocking 25
B. Firewall port blocking 2195-2196
C. Firewall port blocking 5223-5225
D. Firewall port blocking 5228

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 139**
A solution which tracks and organizes the usage and cost of voice and data is referred to as:

A. TEM.
B. MaaS.
C. SaaS.
D. B2B.

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 140**
An MDM client was recently installed on a device. The user has reported decreased battery life. Which of the following can be edited to increase battery life?

A. OS version
B. Email push settings
C. Password requirements
D. Speaker settings

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 141**
A user's device has not checked-in with MDM for a long period of time. Which of the following would be the MOST likely cause?

A. VPN is turned off
B. Email account was removed
C. PIN was changed
D. MDM profile was removed

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 142**
Ann, a user, is unable to login to the network from her mobile device. Which of the following is the FIRST step a help desk administrator should take to resolve this

issue?

A. Wipe Ann's device
B. Lock Ann's device
C. Verify password was entered correctly
D. Reset Ann's password

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 143**
Which of the following is the BEST way to mitigate risk associated with a BYOD deployment?

A. Content filtering
B. Virtualization
C. Containerization
D. WPA2

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 144**
Ann, a user, has removed or turned off the MDM solution on her device triggering an alert to the network administrator. The network administrator should respond by performing which of the following?

A. Lock the device
B. Wipe the device
C. Quarantine the device
D. Initiate company policy

**Correct Answer:** D

**QUESTION 145**
If a user's device is compromised, it is best practice to FIRST:

A. Wipe the device.
B. Capture the logs.
C. Lock the device.
D. Document the incident.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 146**
Which of the following is the BEST way to ensure users de-provisioned from directory services are also de-provisioned from the MDM solution?

A. Remove user certificate
B. LDAP to MDM
C. SCEP sync with MDM
D. Re-enroll in MDM

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 147**
Which of the following would help mitigate threats inherent in legacy operating systems?

A. Using a telecommunications carrier
B. Using a device hardware provider
C. Using an OS vendor
D. Using an MDM

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 148**
Ann, a user, reports there is a power outage and she is unable to access the Internet or the company network. Which of the following would MOST likely cause this issue?

A. Certificate expiration
B. VPN failure
C. WiFi is unavailable
D. Device battery is low

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 149**
It is possible to switch between which of the following technologies?

A. GPRS and GSM
B. LTE and TDMA
C. EDGE and CSD
D. GSM and WiMAX

**Correct Answer:** A
**Section: (none)**

**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 150**
Which of the following are considered part of a site coverage map? (Select TWO).

A. Capacity survey
B. Wireless survey
C. Cellular site survey
D. Traffic routing
E. Traffic shaping

**Correct Answer:** BC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 151**
VPN transmitting data over secure connections is an example of which of the following layers of the OSI model?

A. Layer 1
B. Layer 4
C. Layer 6
D. Layer 7

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 152**
HTTP is run over which of the following ports? (Select TWO).

A. 25
B. 80
C. 110
D. 443
E. 8080

**Correct Answer:** BE
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 153**
Joe, a user, is receiving errors from an application service indicating a token has been redeemed and is not available. Which of the following should the administrator check to determine the issue?

A. Directory service settings
B. MDM application store configuration
C. DMZ server connections
D. Private application store

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 154**
When an application is assigned to a group profile:

A. it is assigned to all administrative users by default.
B. it is assigned to all users in the group.

C. it is removed from all users in the group.

D. it is assigned to all other groups.

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 155**
An administrator receives a call from an executive who had been traveling. The executive informed the administrator that upon returning the service provider bill is much larger than expected. Which of the following MOST likely occurred?

A. Traffic shaping

B. Roaming

C. Latency

D. Content filtering

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 156**
Which of the following is the entry point between external resources and internal servers?

A. VPN concentrator

B. Gateway

C. Access point

D. Switch

**Correct Answer:** B
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 157**
Which of the following will help in restoring data in the event of loss of the mobile device?

A. Backup of all data to an internal SIM

B. Installing a third-party geo-tracking application

C. Backup of all data to a third-party server

D. Encryption of all internal data on the device

**Correct Answer:** C
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 158**
Which of the following is considered a best practice when maintaining awareness of new technologies?

A. Applying all firmware patches released by vendors

B. Continually testing the effects of all new risks and threats

C. Subscribing to operating system vendor sources only

D. Subscribing to multiple sources related to the technology in question

**Correct Answer:** D
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 159**
In WiFi, loss of signal strength over distance is a result of which of the following?

A. Attenuation
B. Refraction
C. Reflection
D. Absorption

**Correct Answer:** A
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation:

**QUESTION 160**
Ann, an administrator, is at a tradeshow and wishes to exchange contact information with a vendor. Which of the following can she use? (Select TWO).

A. IR
B. DMZ
C. NFC
D. DNS
E. CSD

**Correct Answer:** AC
**Section: (none)**
**Explanation**

**Explanation/Reference:**
Explanation: