

N10-006 - Quiz K – Answers Provided

Periodically you will face a question where you do not agree with the answer. That purposely happens because the wrong answer has been purposely inserted. When you find that situation raise the issue in the course discussion board under the discussion area relating to this Quiz.

1. A network technician has configured a point-to-point interface on a router, however, once the fiber optic cables have been run, the interface will not come up. The technician has cleaned the fiber connectors and used an optical power meter to confirm that light is passing in both directions without excessive loss. Which of the following is the MOST likely cause?

A. Distance limitation

*B. Wavelength mismatch

C. cross-talk

D. EMI

E. Macro bend

2. A network administrator wants to deploy a wireless network in a location that has too much RF interference at 2.4 GHz. Which of the following standards requires the use of 5 GHz band wireless transmissions? (Select TWO)

*A. 802.11a

*B. 802.11ac

C. 802.11b

D. 802.11g

E. 802.11n

3. Upon arrival at work, an administrator is informed that network users cannot access the file server. The administrator logs onto the server and sees the updates were automatically installed and the network connection shows limited and no availability. Which of the following needs to be rolled back?

A. The browser on the server

*B. The server's NIC drivers

C. The server's IP address

D. The antivirus updates

4. A network engineer is conducting an assessment for a customer that wants to implement an 802.11n wireless network. Before the engineer can estimate the number of WAPs needed, it is important to reference which of the following?

A. Network diagram

*B. Site survey

C. Network topology

D. PoE requirements

5. A company is implementing enhanced user authentication for system administrators accessing the company's confidential servers. Which of the following would be the BEST example of two-factor authentication?

A. ID badge and keys

*B. Password and key fob

C. fingerprint scanner and retina scan

D. Username and password

6. A company that was previously running on a wired network is performing office-wide upgrades. A department with older desktop PC's that do not have wireless capabilities must be migrated to the new network, ensuring that all computers are operating on a single network. Assuming CAT5e cables are available, which of the following network devices should a network technician use to connect all the devices to the wireless network?

A. Wireless bridge

B. VPN concentrator

C. Default WAP

*D. Wireless router

7. Which of the following integrity security mechanisms ensures that a sent message has been received intact, by the intended receiver?

*A. IPSEC

B. SHA

C. DES

D. CRC

8. A technician installs a new piece of hardware and now needs to add the device to the network management tool database. However, when adding the device to the tool using SNMP credentials, the tool cannot successfully interpret the results. Which of the following would need to be added to the network management tool to allow it to interpret the new device and control it using SNMP?

- A. TRAP
- B. GET
- *C. MIB
- D. WALK

9. Which of the following communication technologies is used by video conferencing systems to synchronize video streams, and reduce bandwidth, sent by a central location to subscribed devices?

- A. Anycast
- B. Unicast
- C. CoS
- D. QoS
- *E. Multicast

10. Which of the following is a UC application?

- *A. Softphone
- B. Intranet
- C. Proxy
- D. Facsimile

11. A company is installing several APs for a new wireless system that requires users to authenticate to the domain. The network technician would like to authenticate to a central point. Which of the following would work BEST to achieve these results?

- A. A TACACS+ device and a RADIUS server
- B. A TACACS and a proxy server
- *C. A RADIUSserver and an access point
- D. A RADIUS server and a network controller

12. A network technician is replacing security devices that protect the DMZ for a client. The client has an application that allows external users to access the application remotely. After replacing the devices, the external users are unable to connect remotely to the application. Which of the following is MOST likely misconfigured?

A. Content filter

*B. Firewall

C. DNS

D. DHCP

13. A technician is dispatched to investigate sporadic network outages. After looking at the event logs of the network equipment, the technician finds that all of the equipment is restarting at the same time every day. Which of the following can the technician deploy to this issue?

A. Grounding bar

B. Rack monitoring

*C. UPS

D. Air flow management

E. Surge protector

14. A network technician needs to protect IP based servers in the network DMZ from being discovered by an intruder utilizing a ping sweep. Which of the following should the technician do to protect the network from ping sweeps?

A. Block echo replies inbound to the DMZ

B. Disable UDP on the servers

*C. Block ICMP at the firewall

D. Disable TCP/IP on the server

15. Which of the following 802.11g antennas broadcast an RF signal in a specific direction with a narrow path?

A. Omni-direction

*B. Unidirectional

C. Patch

D. Yagi

16. A network administrator notices that the border router is having high network capacity loads during non-working hours which is causing web services outages. Which of the following is the MOST likely cause?

A. Evil twin

B. Session hijacking

*C. Distributed DoS

D. ARP cache poisoning

17. A client is receiving certificate errors in other languages when trying to access the company's main intranet site. Which of the following is MOST likely the cause?

A. DoS

B. Reflective DNS

*C. Man-in-the-middle

D. ARP poisoning

18. A technician add memory to a router, but that memory is never recognized by the router. The router is then powered down, and the technician relocates all of the memory to different modules. On startup, the router does not boot and displays memory errors. Which of the following is MOST likely the cause?

A. VTP

*B. Driver update

C. ESD

D. Halon particles

19. An additional network segment is urgently needed for QA testing on the external network. A software release could be impacted if this change is not immediate. The request come directly from management, and there is no time to go through the emergency change control process. Given this scenario, which of the following is the BEST course of action for the network administrator to take?

A. Wait until the maintenance window, and make the requested change

B. First document the potential impacts and procedures related to the change

C. Send out a notification to the company about the change

*D. Make the change, noting the requester, and document all network changes

20. A technician who is working with a junior member of the team is called away for another issue. The junior technician orders an SC 80/125 fiber cable instead of an ST 80/125. Which of the following will MOST likely be an issue with the new cable?

A. Wavelength mismatch

B. Distance limitations

*C. Connector mismatch

D. Attenuation/Db loss: