

## N10-006 - Quiz S – 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 technician is looking at an issue with a computer connecting to the network. The technician determines wire 3 of a UTP Ethernet cable run has a break in it. This computer was previously connected to the switch at 1Gbps throughput. This PC is a kiosk and does not need anything more than 50-60Mbps connection speed. Which of the following can the technician do to resolve the issue quickly?

A. Rewire both ends to have the wire on pin 6 remapped to pin 3. Force the duplex and speed to 100Mbps full duplex.

B. Rewire both ends to have the wire on pin 6 remapped to pin 3. Force the duplex and speed to 1000Mbps full duplex.

C. Rewire both ends to have the wire on pin 7 remapped to pin 3. Force the duplex and speed to 100Mbps full duplex.

\*D. Rewire both ends to have the wire on pin 7 remapped to pin 3. Force the duplex and speed to 1000Mbps full duplex.

2. Which of the following physical devices provides the BEST security to a datacenter?

A. Cipher lock

B. Thumbprint reader

C. Video monitoring

\*D. Mantrap

E. Key pad

3. A network administrator need to install a border device on the network that will help ensure FTP commands are not being sent in traffic communicating on port 25. Which of the following devices will allow for deep packet inspection?

A. Layer 7 firewall

\*B. Web proxy

C. Layer 3 switch

D. Protocol analyzer

4. An employee of a highly secure company needs to use facial recognition in addition to username/password to successfully establish a VPN. Which of the following describes this methodology?

- \*A. PKI
- B. Federated identity
- C. Two-factor authentication
- D. Biometric authentication
- E. AAA

5. An outside technician notices that a SOHO employee who is logged into the company VPN has an unexpected source IP address. Which of the following is the employee MOST likely using?

- \*A. Proxy server
- B. Least-cost routing
- C. IPv6
- D. VPN concentrator

6. A system administrator wants to verify external IP addresses are unable to collect software versioning from servers on the network. Which of the following should system administrator do to confirm the network is protected?

- \*A. Analyze packet captures.
- B. Utilize netstat to locate active connections.
- C. Use nmap to query known ports.
- D. Review the ID3 logs on the network.

7. A network technician is connecting three temporary office trailers with a point-to-multipoint microwave radio solution in a wooded area. The microwave radios are up and the network technician can ping devices in all office trailers, however, connectivity is sporadic. Which of the following is MOST likely the cause of this issue?

- A. Latency
- B. Throttling
- \*C. Interference
- D. Split horizon

8. A client has combined the voice-data circuit from a provider and is getting the maximum download and upload speeds of 2.0Mbps. Which of the following services is being used?

\*A. ADSL

B. T1

C. E1

D. VDSL

9. Joe, a network administrator, has installed an SFTP server behind a load-balancing router. He opened port 21 but was unable to establish a connection. Which of the following ports should he have opened?

A. Port 20

\*B. Port 22

C. Port 162

D. Port 443

10. A technician is installing a network firewall and would like to block all WAN to LAN traffic that is using ports other than the default ports for Internet and email connectivity. Which of the following rules should the technician verify FIRST?

A. All outbound traffic is blocked

B. All inbound traffic is blocked

C. A DMZ has been created

\*D. An implicit deny is enabled

11. Which of the following network infrastructure implementations would be used to connect two remote sales back to the main campus for all data and voice traffic?

A. Crossover cable

\*B. Multimode fiber

C. Satellite

D. MPLS

12. A disgruntled employee executes a man-in-the-middle attack on the company network. Layer 2 traffic destined for the gateway is redirected to the employee's computer. This type of attack is an example of:

- \*A. ARP cache poisoning
- B. IP spoofing
- C. amplified DNS attack
- D. evil twin

13. A home user reports to a network technician that the Internet is slow. The network administrator discovers that multiple unknown devices are connected to the access point. Which of the following is the MOST likely cause?

- A. An evil twin has been implemented.
- \*B. A successful WPS attack has occurred.
- C. The user is experiencing ARP poisoning.
- D. The user is connected to a botnet.

14. A user reports slow performance. A technician troubleshooting the issue uses a performance monitoring tool and receives the following results:

Avg. % Processor Time = 15%

Avg. Pages/Second = 5

Avg. Disk Queue Length = 1

Based on these results, which of the following is causing a bottleneck?

- A. Hard drive
- \*B. Memory
- C. NIC
- D. Processor

15. A network technician has received a report that workstations are unable to gain access to the network. During the troubleshooting process, the technician discovers that the switch connecting these workstations has failed. Which of the following will be the QUICKEST option configure a new switch?

A. Baseline

\*B. Image

C. Archive

D. Syslog

16. A technician is testing a new web-based tool capable of generating automatic teller machine (ATM) cash and service availability reports. The web-based tool was developed by a consortium of financial institutions. Which of the following cloud delivery models and technologies are being utilized? (Select two.)

A. SaaS

B. Public

\*C. Community

D. PaaS

\*E. Private

F. IaaS

17. Workers in a company branch office are required to click on an initial web page and agree to have web surfing mentioned. This is an example of:

A. an end-user license agreement

B. an SLA

\*C. an AUP

D. an MOU

18. A network administrator wants to implement a centralized monitoring solution that utilizes push alerts sent from the client to a server. Which of the following types of monitoring should be put in place?

\*A. SNMP

B. SMTP

C. NIDS

D. SMS

19. After upgrading a fiber link from 1Gbps, a network technician ran a speed test of the link. The test shows the link is not operating at full speed and connectivity is intermittent. The two buildings are 1.476ft (450m) apart and are connected using CM4 fiber and 10G SR SFPs. The fiber runs through the electrical and boiler rooms of each building. Which of the following is the MOST likely reason for the connectivity issue?

- \*A. The wrong SFPs are being used
- B. There is interference from the electrical room.
- C. CM1 fiber should be used instead
- D. There is heat from the boiler room

20. Several users at an adjacent office building report connectivity issues after a new building was built in between the two offices. The network technician has determined the adjacent office building is connected to the main office building via an 802.11ac bridge. The network technician logs into the AP and confirms the SSID, encryption and channels are all correct. Which of the following is MOST likely the cause of this issue?

- A. Device saturation
- B. Antenna type
- C. Bandwidth saturation
- \*D. Interference