**GUIDELINES FOR THE PRACTICE EXAM**

* Practice exams should be taken without using any notes
* Try to complete the 90 questions in under 90 minutes
* Aim to achieve a score of 85% or higher on this exam

1. Patches have just need released by a third-party vendor to resolve a major vulnerability. There are over 100 critical devices that need to be updated. What action should be taken to ensure the patch is installed with minimal downtime?
2. Test the patch in a lab environment and then install it in the production network during the next scheduled maintenance
3. Download and install all patches in the production network during the next scheduled maintenance period
4. Configure end points to automatically download and install the patches
5. Deploy the patch in a lab environment and immediately install it in the production environment
6. A network administrator has set up a firewall and entered only three rules allowing traffic on ports 21, 110, and 25 to secure the network. Now, users are reporting they cannot access web pages using their URLs. What can the technician do to correct this?
7. Add a rule to the end allowing port 80 and 53
8. Add a rule to the end allowing port 143 and 22
9. Add a rule to the end allowing port 137 and 66
10. Add a rule to the end allowing port 445 and 173
11. 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 doesn't need anything faster than 55 Mbps of connection speed. What could the technician do to resolve this issue quickly?
12. Rewire both ends to have the wire on pin 6 remapped to pin 3. Force the duplex and speed to 100Mbps full duplex.
13. Rewire both ends to have the wire on pin 6 remapped to pin 3. Force the duplex and speed to 1000Mbps full duplex.
14. Rewire both ends to have the wire on pin 7 remapped to pin 3. Force the duplex and speed to 100Mbps full duplex.
15. Rewire both ends to have the wire on pin 7 remapped to pin 3. Force the duplex and speed to 1000Mbps full duplex.
16. A host has been assigned the address 169.254.0.1. This is an example of what kind of IPv4 address?
17. APIPA
18. MAC
19. Static
20. Public
21. 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?
22. 802.11n
23. 802.11ac
24. 802.11b
25. 802.11g
26. Mark is setting up a DHCP server on a LAN segment. What option should he NOT configure in the DHCP scope, in order to allow hosts on that LAN segment using dynamic IP addresses, to be able to access the Internet and internal company servers?
27. Default gateway
28. Reservations
29. DNS servers
30. Subnet mask
31. What connection type is used to terminate DS3 connections in a telecommunications facility?
32. 66 block
33. BNC
34. F-connector
35. RJ-11
36. A company-wide audit revealed employees are using company laptops and desktops for personal gain. As a result, the company has incorporated the phrase ‚ÄúCompany-owned IT assets are to be used to perform authorized company business only‚Äô in what document?
37. MSA
38. MOU
39. SLA
40. AUP
41. 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. What solution would be BEST to achieve this?
42. TACACS+ device and RADIUS server
43. TACACS and proxy server
44. RADIUS server and access point
45. RADIUS server and network controller
46. What should be considered when determine the coverage for a new implementation of 802.11n WLAN?
47. Humidity
48. Temperature
49. Heatmap
50. Building material
51. Policies, procedures, and end-user training are effective ways to mitigate:
52. Zero-day attacks
53. Attempted DDoS attacks
54. Man-in-the-middle attacks
55. Social engineering attempts
56. A SQL server needs several terabytes of disk space available to do an uncompressed backup of a database. What device would be the MOST cost efficient to use for this backup?
57. iSCSI scan
58. FCoE SAN
59. NAS
60. USB flash drive
61. Andy is a network technician who is preparing to configure a network. He has installed a firewall to allow for an internal DMZ and external network. No hosts on the internal network should be directly accessible by their IP address from the internet, but they should be able to reach remote networks after receiving a proper IP address. What addressing solution would work for this network?
62. Teredo tunneling
63. Private
64. APIPA
65. Classless
66. A company is selecting a fire suppression system for their new datacenter and wants to minimize the IT system recovery period in the event of a fire. What is the best choice for their new fire suppression system?
67. Portable extinguishers
68. Wet Pipe
69. Clean Gas
70. Dry Pipe
71. An administrator notices an unused cable behind a cabinet that is terminated with a DB-9 connector. What protocol was MOST likely used on this cable?
72. RS-232
73. 802.3
74. ATM
75. Tonken Ring
76. A VLAN with a gateway offers no security without the addition of:
77. An ACL
78. 802.1w
79. A RADIUS server
80. 802.1d
81. An F-connector is used on which cable type?
82. CAT3
83. Single mode fiber
84. CAT5
85. RG6
86. A network technician is troubleshooting connectivity problems between switches but suspects the ports are not properly labeled. What option will help to quickly identify the switches connected to each port?
87. Configure TACACs+ on each network device
88. Enable a discovery protocol on the network devices.
89. Configure each uplink to send LACP discovery units.
90. Enable a packet sniffer on each network device’s uplink port.

1. A network’s design includes gateways connecting an assembly-line network. The assembly-line network users specialized cabling and interfaces to allow the assembly-line robots to communicate with one another. The IP is connecting the technician workstation with what type of network?
2. CSU/DSU
3. SCADA/ICS
4. IS-IS
5. LAN
6. There has been an increased amount of successful social engineering attacks at a corporate office. What would reduce this attack in the near future?
7. Helpdesk training
8. Appropriate use policy
9. User awareness training
10. Personal Identifiable Information
11. A technician is called to investigate a connectivity issue to a remote office that is connected by fiber optic cable. Using a light meter, it is determined that the Db loss is excessive. The installation has been working for several years. The switch was recently moved to the other side of the room and new patch cable installed. What is most likely the reason for this problem?
12. Distance limitations
13. Wavelength mismatch
14. Bend radius limitation
15. Dirty connectors
16. A project manager is tasked with the planning of a new network installation. The customer requires that everything discussed in the meetings will be installed and configured when a network engineer arrives onsite. What should the project manager provide the customer?
17. Acceptable Use Policy
18. Service Level Agreement
19. Statement of Work
20. Security Policy
21. During a high availability test of a system, a fiber interruption did not reroute traffic. This is an indication of what routing concept?
22. Static
23. Dynamic
24. Hybrid
25. Routing loops
26. A technician needs to limit the amount of broadcast traffic on a network and allow different segments to communicate with each other. What would satisfy these requirements?
27. Add a router and enable OSFP
28. Add a layer 3 switch and create a VLAN
29. Add a bridge between two switches
30. Add a firewall and implement proper ACL
31. 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.
32. VTP
33. Driver update
34. ESD
35. Halon particles
36. An offsite backup company involved in an investigation is not recycling outdated tapes. This is MOST likely due to:
37. the process of Discovery
38. a chain of custody breach
39. a data transport request
40. the notice of a legal hold
41. What infrastructure implementation is used to connect various circuits between remote locations?
42. WAN
43. PAN
44. WLAN
45. LAN
46. An employee of a highly secure company needs to use facial recognition in addition to username/password to successfully establish a VPN. What BEST describes this methodology?
47. PKI
48. Federated identity
49. Two-factor authentication
50. Biometric authentication
51. What would provide the highest level of physical security for the client is they are concerned with theft of equipment from the datacenter?
52. Cipher lock
53. Proximity reader
54. Magnetic key swipe
55. Man trap
56. Exploiting a weakness in a user's wireless headset to compromise the mobile device is known as what?
57. Multiplexing
58. Zero-day attack
59. Smurfing
60. Bluejacking
61. OFDM, QAM and QPSK are all examples of what wireless technology?
62. Frequency
63. Modulation
64. RF interference
65. Spectrum
66. A company has implemented the capability to send all log files to a central location by utilizing an encrypted channel. The log files are sent to this location in order to be reviewed. A recent exploit has caused the company's encryption to become unsecure. What would be required to resolve the exploit?
67. Utilize a FTP service
68. Install recommended updates
69. Send all log files through SMTP
70. Configure the firewall to block port 22
71. What would be used in an IP-based video conferencing deployment?
72. RS-232
73. 56k modem
74. Bluetooth
75. Codec
76. A user is receiving certificate errors in other languages in their web browser when trying to access the company's main intranet site. What is MOST likely the cause?
77. DoS
78. Reflective DNS
79. Man-in-the-middle
80. ARP poisoning
81. A network technician has been tasked with connecting three 802.11a clients to an 802.11g access point that is configured for WEP and is within a (9m) line of sight from the client. The clients are unable to associate with the access point. What is MOST likely cause of this issue?
82. Interference
83. Wrong frequency
84. Signal loss
85. Wrong encryption
86. What is used to define how much bandwidth can be used by various protocols on the network?
87. Traffic shaping
88. High availability
89. Load balancing
90. Fault tolerance
91. How does a DHCP reservation work?
92. By leasing a set of reserved IP addresses according to their category
93. By letting the network switches assign IP addresses from a reserved pool
94. By assigning options to the computers on the network by priority
95. By matching a MAC address to an IP address within the DHCP scope
96. A network administrator is comparing several different wireless technologies. To calculate the effective maximum file transfer rate instead of the theoretical, what should be measured?
97. Throughput
98. Latency
99. Goodput
100. Bandwidth

1. A network engineer is designing a wireless network that uses multiple access point for complete coverage. What channel selection would result in the LEAST amount of interference between each access point?
2. Adjacent access point should be assigned channels 1, 6, and 11 with a 20MHz channel width.
3. Adjacent access points should be assigned channels 2,6, and 10 with a 20MHz channel width.
4. Adjacent access points should be assigned channels 7 and 11 with a 40MHz channel width.
5. Adjacent access points should be assigned channels 8 and 11 with a 40MHz channel width
6. Sarah connects a pair of switches using redundant links. When she checks the status of the links, one of them is not active, even when she changes ports. What MOST likely disabled the redundant connection to the other switch?
7. Spanning tree
8. IGRP routing
9. SSID mismatch
10. Port Mirroring
11. A network administrator is following the best practices to implement firewalls, patch management and policies on his network. What should be performed to verify that the security controls in place?
12. Penetration testing
13. AAA authentication testing
14. Disaster recovery testing
15. Single point of failure testing
16. An administrator is told they need to set up a space in the break room where employees can relax. So, the administrator sets up several televisions with interconnected video game systems in the break room. What type of network did the administrator setup?
17. CAN
18. MAN
19. WAN
20. LAN
21. 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. What cloud delivery models and technologies is the technician using?
22. SaaS
23. Public
24. Community
25. PaaS
26. When installing a network cable with multiple strands, a network technician pulled the cable past a sharp edge and exposes the copper conductor on several of the wire strands. These exposed wires come into contact with each other forming an electrical connection. What condition is created?
27. Short
28. Twisted Pair
29. Electrostatic discharge
30. Crosstalk
31. A technician needs to ensure wireless coverage in the green space near the center of the college campus. The antenna is being installed in the middle of the field on a pole. What type of antenna should be installed to ensure maximum coverage?
32. Omnidirectional
33. Yagi
34. Unidirectional
35. Directional
36. A network technician replaced a faulty Ethernet cable. The technician replaced one side of the patch in the incorrect part of the patch panel. Within a few minutes, the technician was informed that users were experiencing slow or no Internet connectivity all over the building. A broadcast storm has begun. After removing the replacement cable, what should the technician do next?
37. Replace the cable during the next maintenance window
38. Review labeling and logical network diagram documentation
39. Attempt to isolate the storm to the domain by rebooting the switch
40. Re-terminate all of the other Ethernet cables on the switch to isolate the issue
41. Company policies require that all network infrastructure devices send system level information to a centralized server. What should be implemented to ensure the network administrator can review device error information from one central location?
42. TACACS+ server
43. Single sign-on
44. SYSLOG server
45. Wi-Fi analyzer
46. A network administrator receives a call asking for assistance with connecting to the network. The person on the phone asks for the IP address, subnet class, and VLAN required to access the network. What type of attack might this be?
47. Social engineering
48. Spoofing
49. Zero-day attack
50. VLAN hopping
51. A technician wants to implement a network for testing remote devices before allowing them to connect to the corporate network. What could the technician implement to meet this requirement?
52. High availability
53. MAN network
54. Quarantine
55. Honeynet
56. Jason is the network manager and is leading a project to deploy a SAN. He is working with the vendor's support technician to properly set up and configure the SAN on the network. To begin SAN I/O optimization, what should Jason need to provide to the vendor support technician?
57. Network diagrams
58. Baseline documents
59. Asset management document
60. Access to the data center
61. A user reports slow computer performance. A technician troubleshooting the issue uses a performance monitoring tool and receives the following results:
62. Hard drive
63. Memory
64. Processor
65. NIC

1. What encryption type MOST likely is used for securing a client-to-server VPN connection?
2. TKIP
3. Kerberos
4. ISAKMP
5. AES
6. A network technician has received reports of an Internet-based application that has stopped functioning. Employees reported that after updating the Internet browsers, the application began to fail. Many users rolled back the update, but this did not correct the issue. What should the company do to reduce this type of action from causing network problems?
7. Implement a disaster recovery plan with a hot site to allow users to continue working
8. Segment the network and create a test lab for all updates before deployment
9. Verify the update hashes match those on the vendor’s website.
10. Coordinate the Internet Server update to coincide with the users’ updates
11. 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. What is MOST likely the cause of this issue?
12. Device saturation
13. Antenna type
14. Bandwidth saturation
15. Interference
16. Johnny installed an SFTP server behind a load-balancing router. He opened port 21 but was unable to establish a connection. What port should he have opened?
17. Port 20
18. Port 22
19. Port 162
20. Port 443
21. What network device uses ACLs to prevent unauthorized access into company systems?
22. IDS
23. Firewall
24. Content filter
25. Load balancer
26. When two or more links need to pass traffic as if they were one physical link, what could be used to satisfy the requirement?
27. Port mirroring
28. 802.1w
29. LACP
30. VTP
31. A system administrator wants to verify external IP addresses are unable to collect software versioning from servers on the network. What should the system administrator do to confirm the network is protected?
32. Analyze packet captures
33. Utilize netstat to locate active connections
34. Use nmap to query known ports
35. Review the ID3 logs on the network
36. A technician needs to set up uplink ports for multiple switches to communicate with one another. ALL VLANs should be transferred from the designed server switch. What should be set on the uplink ports if VLAN 1 is not the management VLAN?
37. STP
38. Port mirroring
39. Port security
40. 802.1x
41. In what type of attack does the potential intruder trick a user into providing sensitive information?
42. Social engineering
43. Bluesnarfing
44. Man-in-the-middle
45. Evil Twin
46. What network infrastructure implementations would be used to support files being transferred between Bluetooth-enabled smartphones?
47. PAN
48. LAN
49. WLAN
50. MAN
51. What cloud infrastructure designs includes on-premise servers utilizing a centralized syslog server that is hosted at a third-party organization for review of the logs?
52. Hybrid
53. Public
54. Community
55. Private
56. An area to which access is controlled by retina scan is protected by what type of security measure?
57. Two-factor authentication
58. Biometric
59. Cipher locks
60. Optical reader
61. What BEST describes the process of documenting everyone who has physical access or possession of evidence?
62. Legal hold
63. Chain of custody
64. Secure copy protocol
65. Financial responsibility
66. A network technician wants to create a network where consultants can access the Internet without disrupting the office’s intranet. What type of network should be created?
67. Guest network
68. VLAN network
69. Security network
70. DMZ network
71. A network technician needs to set up two public facing web servers. The technician wants to ensure that an intruder cannot access the intranet even if those web servers have been compromised. What security technique should be utilized?
72. Place them behind honeypots
73. Place them in a separate subnet
74. Place them between two identical firewalls
75. Place them in the demilitarized zone
76. After a company rolls out software updates, a lab researcher is no longer able to use lab equipment connected to her PC. The technician contacts the vendor and determines there is an incompatibility with the latest IO drivers. What should the technician perform to get the researcher back to work as quickly as possible?
77. Roll back the drivers to the previous version
78. Reset Ann's equipment configuration from a backup
79. Downgrade the PC to a working patch level
80. Restore Ann's PC to the last known good configuration
81. A network technician must create a wireless link between two buildings in an office park utilizing the 802.11ac standard. The antenna chosen must have a small physical footprint and minimal weight as it will be mounted on the outside of the building. What kind of antenna should they choose?
82. Yagi
83. Omni-directional
84. Parabolic
85. Patch
86. A company is experiencing accessibility issues reaching services on a cloud-based system. What monitoring tools should be used to locate possible outages?
87. Network analyzer
88. Packet analyzer
89. Protocol analyzer
90. Network sniffer
91. A network technician has been asked to make the connections necessary to add video transported via fiber optics to the LAN within a building. What is the MOST common connector that will be used on the switch to connect the media converter?
92. FDDI
93. Fiber coupler
94. MT-RJ
95. ST
96. The Chief Information Officer (CIO) wants to improve the security of the company's data. What management control should be implemented to ensure employees are using encryption to transmit any sensitive information over the network?
97. Policies
98. VPN
99. HTTPS
100. Standards
101. What describes a design where traffic is shared between multiple network servers to provide greater throughput and reliability?
102. Load balancing
103. MPLS trunking
104. VLAN tagging
105. Multiplexing
106. What type of equipment should be used for telecommunications equipment and have an open design?
107. 2/4 post racks
108. Rail racks
109. Vertical frame
110. Ladder racks
111. What protocol is used to send email from one server to another server?
112. RTP
113. SNMP
114. POP
115. SMTP
116. A network technician has installed and configured a new wireless router. The clients and hosts can ping each other. The WAN is a 10Gbp/s cable connection. The wired clients have fast connections, but the wireless clients are slow to ping and browse the Internet. What could cause the slow wireless clients?
117. An access point experiencing RFI from fluorescent light bulbs
118. A router is on the incorrect LAN
119. A cable connection does not support wireless
120. A high signal-to-noise ratio on the wireless network
121. What port(s) does SIP use?
122. 443
123. 1720
124. 2427/27/27
125. 5060/5061
126. What tool would a network technician use to troubleshoot a span of single-mode fiber cable?
127. Punchdown tool
128. Spectrum analyzer
129. Ethernet tester
130. OTDR
131. A technician is troubleshooting a PC that is having intermittent connectivity issues. The technician notices that the STP cables pairs are not completely twisted near the connector. What might be the issue?
132. Cross-talk
133. 568A/568B mismatch
134. Tx/Rx reverse
135. Split Pairs
136. A technician troubleshooting an area that is having difficulty connecting to a WAP. After identifying the symptoms, what should the technician do NEXT?
137. Document findings
138. Resolve the issue
139. Establish the probable cause
140. Implement a solution
141. What is a network topology in which all nodes have point to point connections to all other nodes known as?
142. Mesh
143. Ring
144. Bus
145. Star
146. Michael is a system administrator that is troubleshooting an issue with remotely accessing a new server on the local area network. He is using an LMHOST file and the file contains the hostname and IP address of the new server. The server that he cannot remote to is located on the same LAN as another server that he can successfully remote to. What output from the command line would BEST resolve the issue?
147. C:\windows\system32>ipconfig /flushdns
148. C:\windows\system32>ipconfig /registerdns
149. C:\windows\system32>nslookup
150. C:\windows\system32>nbtstat -a
151. A company has a new offering to provide access to their product from a central location rather than clients internally hosting the product on the client network. The product contains sensitive corporate information that should not be accessible from one client to another. What is this an example of?
152. Public SaaS
153. Private SaaS
154. Hybrid IaaS
155. Community IaaS
156. Various hypervisor guests are configured to use different VLANs in the same virtualization environment through what device?
157. Virtual router
158. Virtual firewall
159. NIC teaming
160. Virtual switch
161. When troubleshooting a T1 connection, the service provider’s technical support representative instructs a network technician to place a special device into the CSU/DSU. Using this device, the provider is able to verify that communications are reaching the CSU/DSU? What was used by the network technician?
162. Cable analyzer
163. Toner probe
164. OTDR
165. Loopback plug
166. A company has decided to upgrade its legacy phone system to VoIP. The new phones will download the configurations from a TFTP server each time they boot up. What firewall port must be opened to ensure the phones can communicate with the server?
167. 20
168. 53
169. 69
170. 161
171. What attack utilizes a wireless access point which has been made to look as if it belongs to the network in order to eavesdrop on the wireless traffic?
172. Evil twin
173. Rogue access point
174. WEP attack
175. War driving
176. An increased amount of web traffic to an e-commerce server is observed by a network administrator, but without an increase in the number of financial transactions. What kind of attack might the company be experiencing?
177. Bluejacking
178. ARP cache poisoning
179. Phishing
180. DoS
181. A small office has an Internet connection that drops out about two times per week. It often takes until the next day for the vendor to come out and fix the issue. What should the office implement to reduce this downtime?
182. EULA
183. SLA
184. SOW
185. MOU
186. What can be issued from the command line to find the layer 3 hops to a remote destination?
187. traceroute
188. nslookup
189. ping
190. netstat
191. What physical device provides the BEST security to a datacenter?
192. Cipher lock
193. Thumbprint reader
194. Video monitoring
195. Mantrap

ANSWERS TO PRACTICE EXAM #1

As you check the answers to your Practice Exams #1, it is important to understand why each answer is correct. As you go over your practice exam results, ensure you pay close attention to the questions you missed and understand the explanation provided for their correct answers.

1. D - Patches should always be tested first. Once successfully tested, then deployment to the production environment can be accomplished.
2. A - Port 80 is used for HTTP traffic. It listens to the web client and port 53 is needed to reach the DNS servers to determine the IP address for a given URL or domain name.
3. D - Ethernet uses pins 1-2-3-6 so you’ll choose to use pin 7 since it’s not normally what UTP depends on. Choosing the 1000Mpbs full duplex also still uses the full extent of the cable depending on what’s being sent and received.
4. A - APIPA stands for Automatic Private IP Addressing and is a feature of Windows operating systems. When a client computer is configured to use automatic addressing (DHCP), APIPA assigns a class B IP address from 169.254.0.0 to 169.254.255.255 to the client when a DHCP server is unavailable.
5. B - 802.11ac wireless transmission channel uses the 5Ghz band. While 802.11n can operate in the 5 GHz band, it also operates in the 2.4 GHz band. Only 802.11ac and 802.11a operate exclusively in the 5 GHz band.
6. B - In order to effectively access the internet, the DHCP must provide a default gateway, DNS server, and subnet mask to each client.
7. B - Bayonet Neill-Concelman Connector (BNC connector) is a type of coaxial RF (Radio frequency) electrical connector that is used in place of coaxial connectors. A DS3 (Digital Signal 3) is also known as a T3 line with a maximum bandwidth of 44.736 Mbit/s. DS3 uses 75 ohm coaxial cable and BNC connectors.
8. D - Acceptable Use Policy dictates what things an employee can or cannot do on company issued IT equipment.
9. C - A Remote Authentication Dial-in User Service (RADIUS) server provides AAA management for users connecting to a wired or wireless network, which includes the ability to authenticate users. As servers inherently are not built with wireless access capabilities, an access point would have to be included in the setup for the RADIUS to work correctly with wireless clients.
10. D - Some building materials are more dense than others, the denser the object, the more you will have a degradation of signal. For optimal signal, a LoS (Line of sight) of 25 feet or less is advised, as well.
11. D - Social engineering attempts occur when someone uses something like: phishing (they are attempting to receive your personal information and look legitimate), pretexting (basically they give you a scenario and expect you to react quickly), tailgating (following too closely into a door they aren’t allowed in) and many other situations. Educating your users on the dangers posed by social engineering could prevent them from becoming a victim of a phishing attack as well as many other attacks.
12. C - A NAS is a Network Attached Storage device; typically a bunch of cheap hard disks, usually arranged in a Raid and consisting of either SAS (serial attached SCSI) or Sata disks just like the ones in most desktops.
13. B - A private IP address is an IP address that is reserved for internal use behind a router or other Network Address Translation (NAT) device, apart from the public. Private IP addresses provide an entirely separate set of addresses that still allow access on a network but without taking up a public IP address space.
14. C - Using a clean gas fire suppression system in datacenters are the best, since it minimizes the IT system recovery costs and prevents damage to the equipment. The clean gas extinguishes the fire faster and is more common in datacenter environments.
15. A - RS-232 is a standard for serial communication transmission of data. It formally defines the signals connecting between a DTE (data terminal equipment) such as a computer terminal, and a DCE (data circuit-terminating equipment or data communication equipment).
16. A - VLANs can be protected with an ACL. Without a properly configured ACL, there is not additional security provided by a VLAN.
17. D - An F connector is a coaxial RF connector commonly used for cable television with a RG6 cable. RG6 is a type of coaxial cable used to transmit audio and video signals to devices such as television sets.
18. B - By enabling a discovery protocol on the network devices, the technician will be able to get detail information such as the IP addresses, system version and the type of device information from supporting devices directly connected to the discovery protocol therefore providing information about the specific routers.
19. B - SCADA/ICS is used in industrial control systems, such as assembly-line work.
20. C - Users are the biggest vulnerabilities in a network, therefore providing good user awareness training is crucial to obtaining good network security.
21. D - With Fiber Optic Connectors become dirty, the loss of signal can cause severe problems and performance issues. The technician will need to use appropriate cleaning cloths to clean the dirty connectors and restore the service.
22. C - A Statement of work (SOW) is a document that outlines all work that is to be performed, deliverables and timelines to be agreed upon.
23. A - Static routes must be configured and rerouted manually during an issue. Dynamic and Hybrid would reroute automatically.
24. B - By adding a layer 3 switch to improve network routing performance and reducing broadcast traffic, a VLAN provides LAN segmentation within a network.
25. C - The most likely cause is that the memory chips are bad, because they have suffered from electrostatic discharge (ESD) during the installation and movement of the chips.
26. D - A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.
27. A - WAN because to connect various circuits between remote locations. A Wide Area is required. And Local can only be within a limited small area and PAN even smaller areas.
28. C - This would classify best as two-factor authentication, since it requires "something you are" (face) and "something you know" (username/password) for successful authentication to occur.
29. D - A man trap will ensure that only a single authorized person can get in or out of the building at time. It provides the highest level of physical security of the choices given.
30. D - Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers or sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another.
31. B - Common types of modulation include Orthogonal frequency-division multiplexing (OFDM), Quadrature Amplitude Modulation (QAM), and Quadrature Phase-shift keying (PSK).
32. B - If the encryption is unsecure then we must look for encryption software updates or patches. If they are available we must install them.
33. D - The term "codec" is a concatenation of "encoder" and "decoder”. In video conferencing, a codec is software (or can be hardware) that compresses (encodes) raw video data before it is transmitted over the network.
34. C - A man in the middle attack is a general term for when a perpetrator positions himself in a conversation between a user and an application either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is occurring.
35. B - 802.11a operates in the 5GHz band while 802.11g operates in the 2.4GHz band. 802.11a clients cannot communicate to a 802.11b or 802.11g access point.
36. A - Traffic shaping, also known as packet shaping, Quality of Service (QoS) or bandwidth management, is the manipulation and prioritization of network traffic to reduce the impact of heavy users or machines from affecting other users.
37. D - The client requests an IP address by sending a message on the network to the DHCP server. This DHCP server will assign an IP from its DHCP scope to the client and reserve it based on the clients MAC address.
38. A - Throughput is the measurement of the maximum amount of data being able to be sent over a transmission path.
39. A - Because the overlapping signals are from access points that come from unrelated non-overlapping channels so as a result, the Access Points are least likely to interfere with each other. For Wireless B and G networks, you should always use channels 1, 6, and 11.
40. A - The purpose of spanning tree is to verify no loops exist in the network. If something isn’t working it’s possibly because the switch detects that there’s a loop in the redundant connections.
41. A - Penetration testing (also called pen testing) is the practice of testing a computer system, network, or web application in order to find vulnerabilities that an attacker could exploit. It can be used to ensure all security controls are properly configured and in place.
42. A - Since this gaming network is within one room, it is considered a LAN. All the other answers require a larger geographical area.
43. C - A community or private delivery mode would work best. The community delivery mode sends out based on joint interests and limited enrollment. The private option is owned by the organization and they act as the provider and consumer equally.
44. A - A short in electrical terms is an abbreviation for a short circuit. This generally means that there is an unintended connection between two points allowing current to flow where it should not. In your particular case, it means that a cable is damaged and that two or more of the conductors are connected together causing the cable to fail.
45. A - Omnidirectional antennas send the signal out equally in all directions, therefore it will provide the best coverage since it is located in the center of the field.
46. B - The technician will be able to see the domain architecture the, strength of user connections and the relationships in those connections therefore making it easy to reassign the patches. It is likely that something has been mislabeled, and his connection of that ethernet cable caused a loop.
47. C - Syslog is a protocol designed to send log entries generated by a device or process called a facility across an IP network to a message collector, called a syslog server. A syslog message consists of an error code and the severity of the error. A syslog server would enable the network administrator to view device error information from a central location.
48. A - Social engineering is a type of attack on a network using confidence and gullibility of users to gain access. It is the only type of attack on a network that is directed towards the human element. The human interaction with the network administrator makes the other three answers incorrect.
49. C - Quarantine is where devices that do not meet the standards for the regular network can be placed. In this area, they can be checked before connecting to the main network.
50. A - A network diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. This information will be important when deploying a Storage Area Network (SAN).
51. A - Based on the results, the hard drive (disk queue) is causing the bottleneck, since the average processor is not over 50%, the pages/second (memory) is not heavily burdened, nor do we have any information on the NIC.
52. C - ISAKMP is used in IPSec, which is commonly used in client-to-server VPN connections.
53. B - Segmented networks would ensure every system isn’t updated at the same time, they would be updated in groups. The test lab would ensure proper functionality prior to deployment or would allow you to work through the technical difficulties prior to deployment.
54. D - The most likely reason is interference from the new building being placed between the signal path. By process of elimination: Device saturation is too many devices with too few sources, antenna type restricts the direction for the data to travel and the bandwidth saturation occurs if too many devices are on one WAN link.
55. B- FTP works off of 20/21 but it is known to be unsecured. Port 22 is SSH which can be added to secure telnet. Port 443 is HTTPS and port 162 is SNMP.
56. B - A firewall is a network security device which is designed to prevent systems or traffic from unauthorized access. An ACL is a list that shows which traffic or devices should be allowed into or denied from accessing the network.
57. C - The Link Aggregation Control Protocol (LACP) enables you to assign multiple physical links to a logical interface that will appears as a single link to a route processor.
58. A - Captured packets show you the information that was travelling through certain files, etc. Packet sniffers detail the information they’ve received so working through those would show if the external network shows or details software versions.
59. A - Setting STP on the uplink ports will ensure that loops are not created.
60. A - Social engineering is the art of convincing people to reveal confidential information to the intruder.
61. A - A personal area network (PAN) refers to the interconnection of information technology devices or gadgets within the environment of an individual user (typically within 10 meters).
62. A - Since the admin network is hidden behind firewalls (surrounding the DMZ), SSH connections from the admin network are inherently secure and therefore should be allowed to communicate with the other three networks.
63. B - Retina scans are considered a biometric control, facial recognition would be as well.
64. B - Chain of custody refers to documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence.
65. A - Guest network allow anyone to have access to the internet without having the rights to disrupt the intranet. This network should be logically isolated from the corporate intranet of the office.
66. D - A demilitarized zone (DMZ) is a sub-network inside a network and acts as a semi-trusted zone. It is used for servers that need to be public facing, such as web, mail, ftp, and VOIP servers, and doesn’t provide trust between the DMZ and the intranet.
67. A - By rolling back the drivers Ann would be able to use her lab equipment again. To roll back a driver in Windows means to return the driver to the version that was last installed for the device.
68. D - A patch antenna is a type of radio antenna with a low profile, which can be mounted on a flat surface. A patch antenna is typically mounted to a wall or a mast and provides coverage in a limited angle pattern. A yagi antenna could also be used, but if the distance is smaller than about 300 feet between the buildings, using a Patch antenna would be sufficient. For longer distances, a Yagi would be utilized.
69. A - A network analyzer is a useful tool, helping you do things like track traffic and malicious usage on the network. A software tool like Wireshark is a network analyzer and protocol analyzer.
70. D - Straight Tip (ST) fiber connections are the most common ones used in fiber optic connections in LAN networking applications, therefore this is most likely the correct answer.
71. A - Policies are plans that describe the goal of an established procedure (Acceptable use, Physical Security or VPN access), while the standards are the mechanisms implemented to achieve the goal. VPN and HTTPS are examples of standards.
72. A - Load Balancing is a technique used to spread work across multiple computers, network links or other devices.
73. A - The 2/4 post racks are open framed which are most common with telecommunication equipment. These are where servers and network equipment are mounted inside the IDF and MDF.
74. D - Simple Mail Transfer Protocol (SMTP) is a well-known application that uses port 25 for sending email from one server to another server.
75. A - If interference in the wireless spectrum is occurring, more retransmissions will be needed (and thereby slowing speeds experienced). All the other answers will not cause a slow down of only the wireless network. And a high signal to noise ratio is a good thing on wireless networks.
76. D - SIP works with other protocols over 5060/5061. 443 is HTTPS, 2427 deals with TCP/UDP (wireshark) and ports 5004/5005 is RTP (real time transport).
77. D - The other answers are used with copper cables (like CAT5). An optical time-domain reflectometer (OTDR) is an optoelectronic instrument used to characterize an optical fiber. An OTDR is the optical equivalent of an electronic time domain reflectometer.
78. A - Cross-talk can occur if the twisted pairs are not twisted sufficiently. The cable should be trimmed down and reterminated to prevent this issue.
79. C - Establishing a probable cause is the second step in the troubleshooting process which allows for the technician to list reasons from top to bottom beginning with the simplest and most obvious issues to the most complex.
80. A - A mesh network is a network topology in which each node relays data for the network.
81. B - Since he is using a local LMHOST file, it is bypassing the DNS of the machine and flushing the DNS will not solve the problem. In this case, registering the dns entries will fix the issue.
82. B - SaaS stands for Software as a Service. This is a cloud model whereby a service provider provides a software service and makes the service available to customers over the Internet. Examples of SaaS include Microsoft Office 365, Microsoft Exchange Online, and Google Docs.
83. D - Virtual switches can act like real switches, but are configured in the Hyper-V environment.
84. D - A loopback plug, also known as a loopback adaptor or a loopback cable is a device used to test ports (such as serial, parallel USB and network ports) to identify network and network interface card (NIC) issues. Loopback plug equipment facilitates the testing of simple networking issues and is available at very low costs.
85. C - TFTP uses port 69 to communicate.
86. A - An Evil Twin is meant to mimic a legitimate hotspot provided by a nearby business, such as a coffee shop that provides free Wi-Fi access to its patrons.
87. D - A DoS attack or Denial-of-Service attack works by overloading a server with multiple requests (more than it can handle) thus eventually knocking the server offline.
88. B - A service level agreement (SLA) is a contract between a service provider (either internal or external) and the end user that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. If the customer requires faster response times, it should be in the SLA.
89. A - Traceroute will determine every hop between the host and the destination using ICMP.
90. D - A mantrap allows you to enter one door and wait for it to close before entering another door. Video monitoring is a passive security feature while the thumbprint reader can be tricked. A cipher lock is a good option, but it will not prevent piggybacking into the data center.