IMPORTANT NOTES FOR CompTIA N10-008 EXAM PREPARATION COMPILED BY JIWUEZE BRIGHT CHUKWUEBUKA (B.Sc. Computer Science (Hons), CompTIA N+ (Certified), CompTIA CySA+ (Certified), M.Sc. Cyber Security (Student)).

DISCLAIMER: The questions and answers you would see in this document are not the real compTIA exam questions, the contents of this document will prepare your mind to be comfortable with major networking concepts that would help you argue between options and choose the right answers when writing the N+ exam.

GENERAL KNOWLEDGE: The CompTIA N10-008 exam has 80 objective questions with 2 practical simulations, to be answered within 90mins.

FOR THE PRACTICAL SIMULATIONS

Be comfortable with how to configure and deploy wireless access points based on some guidelines they would provide for you.
Secondly, you also need to practically demonstrate how to use appropriate network devices and servers when installing a network in a specific environment. Knowledge of subnetting, different types of servers, their uses, and their port numbers, is an additional bonus for you.

FOR THE OBJECTIVE QUESTIONS

Be comfortable with the following networking concepts.

OSI MODEL

1. Which level of OSI MODEL provides network and interface services to the end user? APPLICATION LAYER
2. Which level of OSI MODEL does data encryption and decryption occur? PRESENTATION LAYER
3. Which layer of OSI MODEL initiates end-to-end connection between the sending server and the requesting or receiving server? THE SESSION LAYER
4. Which layer of OSI MODEL does data segmentation and transmission? TRANSPORT LAYER
5. Which layer of OSI MODEL handles routing of data, applying and checking logical addressing schemes to data going in and out of the network? NETWORK LAYER
6. Which layer of the OSI MODEL sets up links across physical networks, manages physical addressing, and packages bits into data frames? DATA-LINK LAYER
7. Which layer of OSI-Model comprises of the physical network equipment that transmits signals in 0s and 1s (Cables, power plugs, etc.)? PHYSICAL LAYER
8. TCP is a connection-based protocol while UDP is a connectionless-based protocol.

CABLES AND TRANSCEIVERS

9. The maximum length of a copper cable is 100m.
10. Copper cables are twisted to avoid CROSSTALK (UTP (Unshielded twisted pair)), also shielded to avoid INTERFERENCE (STP (Shielded twisted pair)).
11. The connectors and terminators used in coaxial cables are BNC, RG-6, RG-59, and F connectors.
12. We have two different and standardized ways of ordering individual wires into ethernet cables TIA/EIA 568 A and TIA/EIA 568 B, 568 A procedure is White Green, Green, White Orange, Blue, White Blue, Orange, White Brown, Brown. For 568 B, swap the Greens with the Oanges.
13. STRAIGHT THROUGH CABLE is a cable that have only 568 A or only 568 B at both ends while CROSS OVER CABLE is a cable that have 568 A at one end and 568 B at the other end.
14. Straight through cable are used to connecting similar network devices, example switch to switch, PC to PC, while cross over cables are used to connect different network devices like PC to switch.
15. MDIX (MEDIUM DEPENDENT INTERFACE CROSSOVER): this is a function which is enabled on a network device so it can accept cross over or straight through cabling without making distinction or exception.
16. The cable that we use when connecting a console to a switch or router for configuration is called ROLLEOVER or CONSOLE CABLE.
17. 10 BASE T, 100 BASE T, 1000 BASE T, 10 GBASE T, 40 GBASE T, are different types of ethernet standards in copper, NOTE: the first figure is the Speed, and the “T” means Twisted.
18. 100 BASE FX, 100 BASE SX, 1000 BASE SX, 100 BASE LX, 10 GBASE SR, 10 GBASE LR, are different types of ethernet standards in fiber, NOTE: only 100 BASE have FX in fiber. “S” means short distance while “L” means long distance. Generally, we bring in the concept of single and multi-modes cables, SINGLEMODE CABLES should be used over long distances (greater than 500 m), whereas MULTIMODE CABLES should be used over short distances (less than 500 m), for scenerio questions on best fiber optic for long or short distance connections, think of “L” and “S” in the standards or options given.
19. ST, FC, SC, LC, MT-RJ are different types of fiber optic connectors.
20. PLENUM RATED, RISER RATED, and PVC or NON-PLENUM RATED, are the 3 types of fire ratings in cable. PLENUM has the highest fire rating; it runs on top ceiling or below floor. RISER is in the middle, it runs between floors. PVC has no fire protection. **NOTE:** You would meet scenario questions that might test your knowledge on how, where, and when to use any of the 3.

21. A technique in fiber-optic transmission that uses multiple signal wavelengths to send data over the same medium is called WAVELENGTH DIVISION MULTIPLEXING (WDM)
22. BI-DIRECTIONAL WAVELENGHT DIVISION MULTIPLEXING (BWDM) converts multiple signals into one. COARSE WAVELENGTH DIVISION MULTIPLEXING(CWDM) provides 16 channels. DENSE WAVELENGTH DIVISION MULTIPLEXING(DWDM) provides 40 to 80 signal channels.
23. Transceiver types are Small Form-Factor Pluggable (SPF), Enhanced Small Form-Factor Pluggable (SPF+), Quad Small Form-Factor Pluggable (QSPF), Enhanced Quad Small Form Factor Pluggable (QSPF+). SFP data transfer rates range from 10 Mbps to 1000 Mbps (1 Gbps). SFP+ transceivers provide up to 10 Gbps rates, and for optimal speeds, QSFP/QSFP+ can reach up to 40 Gbps.

DHCP

24. A client/server protocol that automatically provides hosts with their IP addresses and other related configurations such as the subnet mask and default gateway is DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP).
25. The range/pool of IP addresses a DHCP server can give is DHCP SCOPE
26. A range of IP addresses that cannot be given out by a DHCP server is EXCLUSION RANGE
27. Statically assigning IP address or reserving a particular IP address for a particular device or MAC address is IP RESERVATION
28. The DHCP communicates in this order DISCOVER – OFFER – REQUEST – ACKNOWLEDGEMENT (DORA)
29. IPAM (IP Address Management) keeps track of IP addresses, resolves the tools for addressing a system, and reserves IP addresses that are not supposed to be leased out.
30. Dynamically given out an IP address for a certain period is known as LEASE TIME.
31. Ipconfig /all to know if your host is getting IP address statically or dynamically, if DHCP is enabled, then IP address is given dynamically, else, if it is disabled, it means the host got it's IP statically.
32. A technology enabled to be sure that clients are receiving address only from the correct DHCP server, also, to protect network from man-in-the-middle attacks, is known as DHCP SNOOPING.

DOMAIN NAME SYSTEM(DNS)

33. Domain Name System (DNS) resolves fully Qualified domain names to their IP addresses, Address Record for IPV4 is "A record" while Adress record for IPV6 is "AAAA record", CNAME or Canonical Names are Alias or Nick names to domain names.
34. NSLookup, Dig, and Whois, are commands that provide information about a particurlar domain name, Forward lookup zone means "I have the domain name, tell me the IP

address". While Reversed lookup zone means "I have the IP address, tell me the domain name".

35. A server that responds to queries about the information of a particular domain is kwown as AUTHORITATIVE NAME SERVER.
36. When you visit a particular website very often, the local name server will keep record of that particular domain name, this the concept of DNS CACHING.
37. Description of DNS Service: example, www.mail.google.com, "com" is the top level domain, "." is the root, "google" is the domain, "mail" is the sub domain, "www" is the resource record.

CLOUD CONCEPT AND VIRTUALIZATION

38. A cloud computing environment dedicated only to a single individual or organization is known as PRIVATE CLOUD.
39. In a situation where a cloud service provider issues out a cloud environment to individuals and organizations for business purposes, such type is known as PUBLIC CLOUD.
40. A simple mixture of both public and private clouds is known as HYBRID CLOUD.
41. When organizations merge to share a cloud infrastructure or environment, this is known as COMMUNITY CLOUD.
42. The situation that allows users to connect to and make use of cloud-based apps over the Internet is called SOFTWARE AS A SERVICE (SAAS).
43. A type of cloud service that grant users flexibility, scalability, platform independent, to develop, deploy, run, and manage, apps is known as PLATFORM AS A SERVICE (PAAS)
44. A cloud service that allows you manage the infrastructure resources, including servers, virtual machines, networking resources, and storage, as an administrative user is known as INFRASTRUCTURE AS A SERVICE (IAAS)
45. A cloud computing service where a user can access virtual desktop through the internet is known as DESKTOP AS A SERVICE
46. The concept of SCALABILITY in cloud computing is the ability a cloud environment has to provide all IT infrastructures needed for a service without needing assistance from the local OS.
47. The concept of ELASTIC in cloud computing is the ability a cloud environment has to increase or decrease capacity for CPU, memory, and storage resources to adapt to the demands of a user or organization.
48. The concept of MULTITENANCY in cloud computing is the ability a cloud environment has to provide multiple customers same computing resources. cloud customers are not aware of each other, and their data are kept totally separate.

49. A technology that one can use to create virtual representations of networks, storage, servers, and other physical machines is known as VIRTUALIZATION.
50. Power saving, hardware conservation, and system recovery are ADVANTAGES of virtualization.
51. Computer, Hypervisor, Virtual machine, Virtua hard disks are COMPONENTS of virtualization.
52. A hypervisor is a software that sits in between the hardware and the virtual machine, we have type 1 hypervisor which is a bare metal, it boots up the system, we also have type 2 hypervisor which runs on top of the OS.
53. An architecture that describes how to design a virtual network and enables virtualization of network devices is known as NETWORK FUNCTION VIRTUALIZATION (NFV).
54. An approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with network devices and direct traffic on a network is SOFTWARE-DEFINED NETWORKING (SDN)
55. Layers of SDN: 1. FORWARD PLANE/LAYER is the hardware that takes the command and does the forwarding. 2. INFRASTRUCTURAL PLANE/LAYER is made up of the physical switches that forward the network traffic to their destinations. 3. CONTROL PLANE/LAYER is the place where the routing and network topology is defined. 4. APPLICATION PLANE/LAYER is the layer that has applications and services that make requests for network functions from the Control Plane. 5. MANAGEMENT PLANE/LAYER is the plane Responsible for monitoring, configuring, and maintaining network devices.
56. The concept of VIRTUAL PRIVATE NETWORK is creating a secured tunnel to use the public internet to connect to our private network remotely.
57. A cross platform and open-source connection tool that can be used to access a system remotely is known as TIGHT VIRTUAL NETWORK COMPUTING (TIGHT VNC):
58. A CLIENT-TO-SITE VPN connects a remote computer to a local network, while SITE-TOSITE VPN connects distance networks into a single network.
59. A dedicated network device that provides secure connections between remote users and a company network is a VPN CONCENTRATOR.
60. A feature that enables Linux virtualization and allows the use of host's keyboard and mouse to operate the virtualized machine or remote PC is known as KVM.
61. An intermediary device between the internet and the hosts that gets information from the internet and pass them to the hosts is known as PROXY SERVER, this server protects hosts from being hacked because it sits between hosts and the web pages they visit.
62. Classic Data Centers make use of three-tiered architecture, 1. Core layer. 2. Distributed layer. 3. Access/edge layer
63. East-West traffic moves within the server, North-South traffic is one that goes in and out of the server.

MAC, IPV4, & IPV6

64. A layer 2 unique 48-bits identifier given to a device NIC (Network Interface Card) in a network is called “MAC ADDRESS” 94-65-9C-3B-8A-E5 (windows), 94:65:9C:3B:8A:E5 (Linux), 9465.9C3B.8AE5 (Switches).
65. The first part of the MAC address is an organizationally unique identifier (OUI). The second part is vendor’s assigned address (Device identifier)
66. IPV4 is a 32 bits layer 3 address that makes it possible for our device to connect to the internet, it ranges from 0.0.0.0 - 255.255.255.255.
67. 127.0.0.0 is a loopback address for IPV4, 169.254.X.X. is a link local IPV4, others include 10.X.X.X, 172.16.X.X -172.31.X.X, 192.168.X.X, are all private IPs and cannot be seen on the internet.
68. Class A IPs are 1.0.0.0-126.255.255.255 /8, and subnet mask of 255.0.0.0, Number of Hosts per Network: 16,777,214. Class B IPs are 128.0.0.0-191.255.255.255 /16, and subnet mask of 255.255.0.0, Number of Hosts per Network: 65,534. Class C IPs are 192.0.0.0-223.255.255.255 /24, and subnet mask of 255.255.255.0, Number of Hosts per Network: 254. Class D IPs are 224.0.0.0-239.255.255.255 /32, and subnet mask of 255.255.255.255, Number of Hosts per Network: multicasting.
69. APIPA (AUTOMATIC PRIVATE IP ADDRESSING) is an automatic private IP address given to a system in a network when the DHCP server is down, note that this IP address can only be used locally, not on the internet e.g. 169.254.X.X
70. IPV6 has 128- bits addresses, they are 8 groups of 4 hexadecimals values separated with 7 columns, they only make use of NEIGHBOUR DISCOVERY PROTOCOL (NDP).
71. The address starting with Fe80 is a link local IPV6, ::1 or 0:0:0:0:0:0:0:1 are IPV6 loopback addresses
72. The concept of DUAL STACK is simply running IPV4 and IPV6 simultaneously.
73. A feature that enables a host in a network to automatically get a temporary IPV6 is known as STATELESS ADRESS AUTO CONFIGURATION (SLAAC).
74. Building a VPN between a system and the IPV6 network on the internet is known as TUNNELLING, and encapsulating IPV6 packets into IPV4 is known as 6 TO 4.
75. ICMP V6 helps hosts on a network to use their link local to start neighbour solicitation and neighbour advertisement.
76. IP HEADER is the information at the beginning of an IP packet. It contains information such as the IP version, the packet's length, the source, and the destination. IPV4 header format is 20 to 60 bytes in length. It contains information needed for routing and delivery.
77. VIRTUAL IPs (VIP) uses a single IP for multiple applications running on a server, or multiple servers running on a network to cluster all traffic together.

78. A way to map multiple private addresses inside a local network to a public IP address before transferring information onto the internet is known as NETWORK ADDRESS TRANSLATION (NAT)
79. A feature that permits multiple ports on a LAN to be mapped to a single public IP address to conserve IP addresses is known as PORT ADDRESS TRANSLATION (PAT).

ROUTING TECHNOLOGIES AND BANDWIDTH

80. The basic unit of exchange between entities that communicates using a specified network protocol is known as PROTOCOL DATA UNIT (PDU).
81. A form of routing that occurs when a router uses a manually configured routing entry to route traffic is known as STATIC ROUTING.
82. A form of routing that uses an algorithm to update routing table by computing multiple possible routes and determining the best path for traffic to travel through the network is known as DYNAMIC ROUTING PROTOCOL, it is divided into two, DISTANCE VECTOR and LINK STATE PROTOCOLS.
83. VIRTUAL ROUTER REDUNDANCY PROTOCOL (VRRP) is a computer networking protocol that provides for automatic assignment of available IP routers to participating hosts.
84. A type of routing protocol used for exchanging routing table information between routers within an autonomous system in a LAN is known as INTERIOR GATEWAY PROTOCOL (IGP), they are EIGRP, OSPF, RIP.
85. A feature that allows the exterior gateway of an autonomous system to share routing information with exterior gateways on other autonomous systems is known as EXTERIOR GATEWAY PROTOCOL (EGP), example is Boarder Gateway protocol (BGP).
86. EIGRP and RIP uses Distance Vector protocols, EIGRP is a more advanced distance vector and it account for speed, while RIP account for hop counts, the maximum number of a RIP is 15 hops.
87. OPEN SHORTEST PATH FIRST (OSPF) uses link state routing protocols.
88. The TRUSTWORTHINESS of a particular route is the administrative distance, the lesser the number of administrative distance, the more trustworthy it is.

SOURCE	ADMINISTRATIVE DISTANCE
Local interface/Directly connected	0
Static route	1
BGP	20
EIGRP	90
OSPF	110
RIP	120
Unknown	255

89. An error that occurs when the routers forward packets such that the same single packet ends up back at the same router repeatedly in the network is commonly known as ROUTING LOOP.
90. one mechanism to avoid routing loop is TIME-TO-LIVE, it is the amount of time or “hops” that a packet is meant to exist inside a network before being discarded by a router.
91. A dead link marked by a router in other that packet would not be routed to it is known as POISON ROUTE
92. SPLIT HORIZON is principle that helps in preventing routing loop, “never send routing information back to the direction from which it was sent”.
93. Controlling the amount of data that flows into a traffic to increase network performance is known as TRAFFIC SHAPING
94. Two approaches to bandwidth management are CLASS OF SERVICE (COS) and QUALITY OF SERVICE (QOS).
95. CLASS OF SERVICE operates at layer 2, it manages traffic in a network by grouping them into similar types, gives them names, and treats each class with its own level of network service and priority, this follows 802.1P standard.
96. QUALITY OF SERVICE operates at layer 3, it is a traffic shaping mechanism that prioritizes a service based on the labels made by class of service.
97. The method of distributing network traffic equally across a pool of resources or servers that support an application to increase performance is known as LOAD BALANCING.
98. GIANTS or JUMBO FRAMES are packets that exceed the Maximum Transmission Unit (MTU) which is 1500.
99. RUNTS are packets that is below the Maximum Transmission Unit (MTU)

ETHERNET SWITCHING AND WIRELESS ACCESS POINT FEATURES

100. IEE 802. 3 is the standard for ethernet. The major difference between PoE (IEEE 802.3af standard) and PoE+ (802.3at) is the amount of power delivered. PoE can provide 15.4 watts over Cat5 cables, while PoE+ can provide up to 30W over Cat5 cables. Note that POE is an abbreviation for Power Over Ethernet.
101. CARRIER SENSE MULTIPLE ACCESS/COLLISION DETECTION (CSMA/CD) is used in WIRED network to regulate how communication must take place in a network. CARRIER SENSE MULTIPLE ACCESS/COLLISION AVOIDANCE (CSMA/CA) is used for WIRELESS network.
102. A HALF-DUPLEX transmission is said to be a one-way communication between sender and receiver. FULL-DUPLEX, on the other hand, enables two-way communication at the same time.

103. DUPLEX MISMATCH is when the two communicating network devices have duplex settings that are not the same.
104. ADDRESS RESOLUTION PROTOCOL (ARP) matches MAC address with the host's IP address, we use ARP when we have the IP address, but we need to know the MAC address, RARP is the reverse of ARP, we use it when we have the MAC address but looking for the IP address.
105. A network configuration in which a physical path is obtained and dedicated to a single connection between two endpoints in the network is known as CIRCUIT SWITCHING.
106. Grouping data into packets that can be transmitted over a digital network is known as PACKET SWITCHING
107. Frames are created and destroyed inside a NETWORK INTERFACE CARD (NIC).
108. Device on network send and receive data in discrete chunks called FRAMES.
109. A point-to-point interface in a network where data packets can collide with one another when being sent on a shared medium is the COLLISION DOMAIN.
110. A logical division of a computer network, in which all points in the network can reach each other by broadcast at the data link layer is known as BROADCAST DOMAIN.
111. A network configuration, that opens a port in the LAN to be accessed using external network from a location outside the network is known as PORT FORWARDING:
112. A network configuration, that allows request going out from a particular port to come back through a different port is known as PORT TRIGERRING:
113. A layer 2 technology that splits one broadcast domain into two or more broadcast domains is known as the VLAN.
114. Different broadcast domains can relate to virtual routers using INTERVLAN ROUTING. Also note that for different VLANs to communicate, there should be the presence of a layer 3 device.
115. The communication lines or links designed to carry multiple signals simultaneously to provide network access between two points is known as TRUNKING or NETWORK TRUNK.
116. VLAN TRUNKING allows layer 2 switches to forwards frames from different VLANs over a single line called trunk.
117. A connection on a switch that transmits data to and from a specific VLAN is known as ACCESS PORT.
118. A type of connection on a switch that is used to connect a guest virtual machine that is VLAN aware is known as TRUNK PORT, generally, TRUNK PORTS are used to connect intermediary devices.

119. 802.1Q is a standard that supports trunking
120. VLAN 1 is the DEFAULT or the NATIVE VLAN, by default, every device is connected to this VLAN. It is important to note that all packets that are not going to configured VLANs are automatically going to the NATIVE VLAN.
121. Combining different ports together to increase bandwidth is known as PORT BONDING or PORT AGGREGETION. In PC, when different network interfaces are combined, it known as NIC TEAMING.
122. Two protocols under port aggregation are LINK AGGREGATION CONTROL PROTOCOL (LACP) and PORT AGGREGATION PROTOCOL (PAgP), LACP is open source while PAgP is used only on CISCO devices.
123. A technique used on a network switch to send a copy of network packets seen on one switch port to a network monitoring connection on another switch port is known as PORT MIRROING. This technique enables administrators to track switch performance via a protocol analyzer on the port that receives the mirrored data.
124. A protocol enabled by default to avoid broadcast storm is known SPANNING TREE PROTOCOL (STP).
125. The standard for STP is 802.1d, for Rapid STP is 802.1w.
126. In STP, all ports that cannot be turned off, especially the ones linked to the root switch is known as DESIGNATED PORTS.
127. In STP, all ports connected to the root switch are known as ROOT PORTS.
128. Turned off ports design to take over for the root port if that path fails is known as ALTERNATIVE or BLOCKED PORTS.
129. In STP, a technology that memorizes the address of the root switch so other switches cannot take over its position is known as the ROOT GUARD.
130. BPDU GUARD is a security feature. It helps to prevent attacks on a network by blocking Bridge Protocol Data Units (BPDUs) that are sent from unauthorized devices.
131. To implement security in VLANs , it is very important to always change default VLANs.
132. IEE 802.11 is a standard that supports wireless network, it uses radio signals to communicate among devices.
133. ACCESS POINTS (AP) can be Uni-directional (One direction), Bi-directional (two directions), Omni-directional (many directions).
134. Different types of wireless standards are, 802.11b uses 2.4GHZ and 11mbps. 802.11a uses 5.0GHZ and 54mbps. 802.11g uses 2.4GHZ and 54 mbps. 802.11n uses 2.4GHZ /5.0GHZ and 600mbps. 802.11ac uses 5.0GHZ and 1.3Gbps. 802.11ax uses 2.4GHZ/5.0GHZ and 10Gbps.

135. 802.11n is Wi-Fi 4 standard, 802.11ac is Wi-Fi 5 standard, 802.11ax is Wi-Fi 6 standard.

136. 2.4GHZ can travel distance and penetrate through walls more than 5.0GHZ.

137. When configuring 2.4GHZ frequency for different WAPs, use channels 1, 6, and 11, to avoid overlapping, also note that in scenarios where neighboring buildings are using the same channel with your newly configured WAP, it might lead to INTEFERENCE.

138. Different types of antennas are Omni Anthena, Dipole, Patch Antenna, Directional/Yagi antenna. Omni is the highest, its radiation is spherical, dipole have two antennas that cuts across each other, patch antennas can be installed on exterior walls, its radiation pattern is exactly like half of a sphere, directional antennas are extremely directional and parabolic.

139. A piece of hardware or software that sits on a server and allows us control over our wireless devices simultaneously is known as WIRELESS CONTROLLER.

140. Joining multiple antennas together to increase speed is known as MIMO (Multiple-In Multiple-Out).

141. A SERVICE SET IDENTIFIER (SSID) is a sequence of characters that uniquely names a Wi-Fi network. An SSID is sometimes referred to as a network name, note that when there are multiple access points, it is known as EXTENDED SERVICE SET IDENTIFIER (ESSID).

142. Turn on SSID broadcast or BEACON FRAME, if you want users to see your network SSID, otherwise, turn it off.

143. Before installing wireless network, first study the floor plan, to avoid interference, reflection, refraction, absorption, and attenuation. Also pay great attention to bandwidth and use channels with the least amount of congestion.

144. Increase the power level of the access point in other to increase the distance the signal can travel (Scenario based question like, as a network administrator, employees in an office 20m away from the access point are complaining of low or no wireless signal, what would you do?)

145. ICMP (INTERNET CONTROL MESSAGE PROTOCOL) is an error-reporting protocol that network devices such as routers use to generate errors with data transmission to the source IP address when network problems prevent delivery of IP packets.

146. IGMP (INTERNET GROUP MANAGEMENT PROTOCOL) is a protocol that allows several devices to share one IP address so they can all receive same data.

147. NTP (NETWORK TIME PROTOCOL) is a network protocol used for clock synchronization between computer sytems connected to the network.

148. IOT (INTERNET OF THINGS) are home devices connected to the internet and can be control via the internet.

149. To harden IOT devices, place them on separate SSID and VLAN, use long PSK that contains different characters, set up routine queries for firmware updates from manufacturers, use username ACL to control who have access to the device.

NETWORK AVALIABILITY AND TROUBLESHOOTING

150. Note that we have 525,600mins in a year, so for 99.999% uptime in a year, the network is expected to have approximately 5mins down time, for 99.99% uptime, the network is supposed to have 52mins or approximately 1hr down time, for 99.9% uptime, the network is supposed to have 525mins downtime within the year.
151. A protocol that computer systems use to send event data logs to a central location for storage is known as SYSLOG.
152. Syslog severity levels are 0. Emergency 1. Alert 2. Critical 3. error 4. warning 5. notice 6. information 7. debug. Always note that in a scenario where you enable any level of log, it will also capture other levels under but will not capture the ones above the level you enabled.
153. An internet standard protocol that enable network administrators to monitor and manage network devices connected over an IP is known as SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP), Port 161 and 162.
154. AGENT is software built into the devices from factory that enables them to do SNMP. MANAGED DEVICES are devices that have SNMP. SNMP MANAGER is a system that can talk to managed devices to perform a specific function or functions.
155. The interface an SNMP manager uses to communicate with managed devices is known as NETWORK MANAGEMENT STATION.
156. AN SNMP COMMUNITY is an organization of managed devices, note that SNMP v3 has encryption advantage over other versions.
157. OBJECT IDENTIFIER (OID) is an individual ID given to each managed device on the managed network for monitoring and tracking.
158. GET, TRAP, and WALK, are commands to query devices on our managed network, The Get request queries for a value of the parameter from the managed device, SNMP TRAPS are used to monitor network devices in real time and detect critical events and errors, SNMP WALK command allows users to extract useful information without entering the unique commands for each OID or node.
159. An ASYMMETRIC ROUTING has multiple routes for incoming and outgoing network traffic, traffic takes a different route when entering or exiting the network. A SYMMETRIC ROUTING has a single route for incoming and outgoing network traffic.

160. JITTER is when there is a time delay in sending data packets over your network connection, which is often caused by network congestion, and sometimes route changes.

161. A network DELAY is the amount of time required for one packet to go from a transmitter (source) to a receiver (destination).

162. A network LATENCY is the amount of time required for one packet to go from a transmitter to a receiver, and then back to the transmitter.

163. ATTENUATION is the loss of signal strength in networking cables or connections.

164. INTERFERENCE is When the wireless communication signals are disrupted or weakened by the presence of other wireless signals.

165. TX/RX REVERSE occurs when a cross over cable is used with two devices that should be using a straight through cable.

166. When broadcast packets are sent by switches through every port, it can cause SWITCHING LOOP, this can be eliminated using Spanning Tree Protocol.

167. ROGUE DHCP server assigns malicious default IP and gateway information that can redirect legitimate devices to an unauthorized default gateway, eg. When your dynamic IP address is different from your subnet mask, it could be a cause of rogue DHCP.

168. When hosts are connecting to the internet with different encryption protocol, it is known as ENCRYPTION PROTOCOL MISMATCH

169. Other network issues that you would see as scenario-based questions in the exam are, Duplicate MAC address, Duplicate IP address, Incorrect Subnet Mask, Incorrect IP address, Incorrect DNS, certificate issues, DHCP scope exhaustion, broadcast storm, channel overlap, wrong SSID, insufficient wireless coverage. Please research more on these network issues, be comfortable with their causes and effect, and what to do as network administrator to fix them.

170. RSSI (RECEIVED SIGNAL STRENGTH INDICATOR) is a more common name for the Signal value, meaning, it is the strength that the device is getting a specific signal, also measurement of the power present in a received radio signal.

Original FM RSSI	6-level FM RSSI	Wi-Fi RSSI
40 to 45	-50	Excellent
30 to 39	-60	Very good
20 to 29	-70	Good
10 to 19	-80	Low
1 to 9	-90	Very low
0	0	No signal

FM RSSI level conversion

171. A webpage that the user of a public network is required to view and interact with for authentication before they can access the network is known as CAPTIVE PORTAL.

172. A method of detecting accidental changes/errors in data transmission is known as Cyclic Redundancy Check (CRC).

173. Link state, speed duplex factor, sending received traffic, giant & runts, and cyclic redundancy check (CRC) errors, are tools that show interface statistics and status. Be comfortable with these terms to be able to know when there are interface errors, because you would see it as scenario base question in exam.

174. Reduction of power for a long time is known as BROWN OUT, reduction of power for a short time is known as POWER SAG, where there is entirely no power is known as BLACK OUT.

175. RECOVERY TIME OBJECTIVE (RTO) is an acceptable amount of downtime to restore normal operation, while RECOVERY POINT OBJECTIVE (RPO) is an acceptable amount of data an organization can tolerate losing due to disaster.

176. MEAN TIME TO FAIL (MTTF) is the space between the time of repair to the time of failure. MEAN TIME TO RECOVER (MTTR) is the space between the time of failure to the time of repair. MEAN TIME BETWEEN FAILURES (MTBF) is the time from a failure to repair and then till the time it fails again.

177. WIRE CRIMPERS AND CABLE CRIMPERS are tools that are used to crimp connectors onto the ends of wire and/or cable.

178. PUNCH DOWN TOOL is used to connect or terminate wires into punch down patch panels and punch down keystone jacks, PLEASE KNOW THE SPECIFIC TYPE OF BLOCK BEFORE CHOOSING THE CORRECT PUNCH DOWN TOOL.

179. TONE GENERATOR produces sounds artificially, by converting electrical signals into sounds that enable technicians to identify, locate and test cables.

180. TDR and OTDR are used to determine the location and magnitude of cable faults, breaks, splices, terminations, they are also used to certify the integrity of cables.

181. FUSION SPLICER uses electric arc to melt two optical fibers and join their two ends together to form a single long fiber.

182. WIRE STRIPPER is used to remove the sheath STP cables.

183. CABLE CERTIFIER are Certification testers that provide “Pass” or “Fail” information for a cable network infrastructure in accordance with the industry standards.

184. A MULTIMETER is an electronic tool used to measure metrics, eg. voltage, amps and resistance across circuits.

185. Please be comfortable with the following network troubleshooting commands. Ping, ipconfig(windows), ifconfig(Linux), tracert(windows), traceroute (Linux), Nslookup, dig, whois, netstat, nbtstat, Nmap, route, iptables, telnet, SSH. Be comfortable with how and when to use them, options to use them with, verify options associated with each command by typing eg. “netstat –help" both in Linux and Windows CMD, you will see the options associated with it, same to other commands listed.

186. NOTE that “netstat –r” will give you same output as “route print”. Telnet and SSH are for remote connections but SSH is secured and encrypted to use than telnet. “ipconfig /release | ipconfig /renew” to solve issue of duplicate ip address.

187. PACKET SNIFFER is used to check packet and traffic flow within the network.

188. A network protocol analyzer or packet capture is a tool used to monitor data traffic and analyze captured signals as they travel across communication channels. Examples are, WIRESHARK which is a packet capture tool that has GUI, TCPDUMP is a packet capture tool with command line used in Linux, NETFLOW is a packet capture tool that is used for CISCO product.

189. NETWORK TROUBLESHOOTING THEORY: 1. Identify the problem. 2. Establish a theory of probability cause. 3. Test the theory. 4. Establish a plan of action to resolve the problem. 5. Implement and test the solution. 6. Verify system functionality. 7. Document the issue. **NOTE:** Be sure to understand the concept of this theory before going in for the exam, because you must see it as a scenario-based question in the exam, which will demand you to explain what is needed at each step of the theory.

BACKUP PLANS AND DISASTER RECORVERY

190. The service of gathering, preserving and presenting evidence stored in computer to be used in court is known as FORENCIS

191. The process of an organization to organize data in response to a pending legal issue is known as LEGAL HOLD.
192. An approved written document, that helps an organization before, during, and after a confirmed or suspected security incident or malicious software attack is known as INCIDENT RESPONSE PLAN.
193. THE INCIDENT RESPOSE CYCLE is as follows, prepare – identify – contain – eradicate – recover – lesson learnt.
194. A DISASTER RECOVERY PLAN (DRP) is a structured, documented approach, that describes how an organization can quickly resume work after an unplanned incident eg. Fire, natural disaster, etc.
195. A BUSINESS CONTINUITY PLAN (BCP) is a detailed strategy and set of systems for ensuring an organization's ability to prevent or rapidly recover from a significant disruption to its operations.
196. CONTINGENCY PLANNING means preparing an organization to be ready to respond effectively in the event of an emergency.
197. A DIFFERENTIAL BACKUP is a data backup that copies all the files that have changed since the last full backup was performed.
198. INCREAMENTAL BACKUP is the backup of changes made from the last backup, it is used when the amount of data that must be protected is too voluminous to do a full backup of that data every day.
199. LOCAL BACKUP, OFFSITE BACKUP, and CLOUD BACKUP, are different types of media for backup.
200. LOCAL BACKUP, or ON-PREMISES BACKUP, refers to the whole process of backing up systems, applications, and data to a local device, such as tape, disk, hard disk, flash drive, CD, external hard drive or other media that is located on-site, close to the data source.
201. An OFFSITE BACKUP is a copy of a business production system data stored in a different geographical location from the main production area.
202. CLOUD BACKUP or online backup or remote backup is the process of backing up data to cloud-based servers, which are owned and managed by a cloud base service provider.
203. COLD SITE, WARM SITE, HOT SITE, and CLOUD SITE, are different types of backups sites
204. A COLD SITE is a backup facility with little or no hardware equipment installed. it is essentially an office space with basic utilities such as power, cooling system, air conditioning, and communication equipment, etc. it is the most cost-effective option among others.

205. A WARM SITE is a backup facility that has network connectivity and the necessary hardware equipment already pre-installed, but it cannot perform on the same level as the production center because they are not equipped in the same way.
206. A HOT SITE is equipped with all the necessary hardware, software, and network connectivity, which allows you to perform near real-time backup or replication of critical data. It is just an exact replica of the data center, this type of back up site is very difficult to maintain.
207. A CLOUD SITE means virtualizing your computing technologies and storing them on the internet via cloud.
208. For ASSET or STORAGE DEVICES disposal, perform a complete or full factory wipe on the devices before disposal, and do not dispose documents that contain sensitive information at the public dumps to avoid attacks that might come through social engineering.

NETWORK DIAGRAM AND DOCUMENTATION

209. NETWORK BASELINES are ideal performance metrics obtained by measuring your network for a particular period, it helps administrators find the normal operating level of network devices.
210. A PHYSICAL NETWORK DIAGRAM depicts the network topology with the physical aspects like ports, cables, racks, and more when new devices are added or removed, always refer to this diagram.
211. A LOGICAL NETWORK DIAGRAM, on the other hand, shows the invisible elements and connections flowing through the physical objects on the network.
212. Different types of topologies are, 1. BUS TOPOLOGY where all hosts are connected by a single trunk cable. 2. STAR TOPOLOGY which is also known as hub and spoke, network topology in which each network component is physically connected to a central node such as a router, hub or switch. 3. STAR BUS TOPOLOGY which is a hybrid topology. 4. MESH TOPOLOGY which is a network setup where each computer and network device is interconnected with one another, it is the highest fault tolerance of all the topologies. 5. RING TOPOLOGY, here, various devices are connected forming a “ring” within which the frames circulate continuously in one direction.
213. WIRING DIAGRAM: when there is wire or cable issues, addition and removal, refer to wiring diagram, it is a diagram that shows how circuits work logically and electrically.
214. A RACK DIAGRAM is a visual representation of the organization of IT equipment within a server rack, always refer to this documentation when there is exchange of switches and routers.
215. TELECOMMUNICATION CLOSET/EQUIPMENT ROOM, WORK AREA, AND

HORIZONTAL CABLING, are 3 basic components of structured cabling.

216. EQUIPMENT RACK is 19 inches and the spaces between each rack is measured in UNIT(U), a unit is 1.75 inches.

217. MDF (MAIN DISTRIBUTION FRAME) AND IDF (INDEPENDENT DISTRIBUTION FRAME). An MDF is the main computer room for servers, hubs, routers, DSL's, etc. to reside. An IDF is a remote room or closet connected to the MDF, in which you can expect to find hubs and patch panels.

218. SLA (SERVICE LEVEL AGREEMENT) Is a document that outlines a commitment. between a service provider and a client, including details of the service, the scope, the standards the provider must adhere to, equipments, and the metrics to measure the performance.

219. A MEMORANDUM OF UNDERSTANDING (MOU) is a starting point of negotiations between clients and service providers to signal the intent of doing business or coming to an agreement. It simplifies a legal contract by establishing the key objectives and goals.

220. A MULTI-SOURCE AGREEMENT is an agreement among multiple manufacturers to make products which are compatible across vendors.

221. A STATEMENT OF WORK (SOW) is a document that provides a description of a given project's requirements. It defines the scope of work being provided, project deliverables, timelines, work location, and payment terms and conditions.

222. When employees use their own personal devices to connect to the organization's network and access what they need to do their jobs, this is the concept of BYOD (BRING YOUR OWN DEVICE).

223. ONBOARDING refers to the processes in which new hires or external devices are integrated into the organization. OFFBOARDING is the reverse of Onboarding.

224. MOBILE DEVICE MANAGER (MDM) allows the company to connect to the device (BYOD) in a centralized location in other to monitor the device.

225. BYOD Challenges: 1. Personal vs Company use. 2. Personal data vs Company data. 3. MDM must be able to manage the device.

226. AN ACCEPTABLE USE POLICY(AUP) is an agreement between two or more parties that outlines the appropriate use of access to a corporate network or the internet. This document describes what users may and may not do when accessing this network or when making use of the company’s equipments.

227. REMOTE ACCESS POLICY is a security policy governing network and computer use in the office to remote users connecting to the network.

228. A PASSWORD POLICY defines the password strength rules that are used to determine whether a new password is valid. Be comfortable with the best types of passwords to use because you must see it as a scenario questions in exam,

best passwords are one's with numbers, alphabet (upper and lower case) and at least 8 character long, don't choose password that can be seen in the dictionary or can be easily memorize by hackers, don't use any of your names as password.

229. NONE DISCLOSURE AGREEMENT (NDA) is an agreement an employee or service provider in organization signs not to give away company secrets to the outside world.
230. LICENSE RESTRICTION is any type of rule that talks about how you handle licensing for any product especially eg. usage, transfer, renewal
231. CHANGE MANAGEMENT is the process of guiding organizational change to realization, from the earliest stages of conception and preparation, through implementation and, finally, to resolution.
232. TYPE OF CHANGE, CONFIGURATION PROCEDURE, ROLLBACK PROCESS, POTENTIAL IMPACT, AND NOTIFICATIONS, all these are contained in change request.
233. STRATEGIC CHANGE is a massive change that will affect the business infrastructure itself, eg. relocation of the business to another location.

NETWORK SECURITY

234. VULNERABILITY is a weakness in hardware, software, or procedures. THREAT is anything that can attack a vulnerability. EXPLOITS are what hackers use vulnerability to do.
235. A ZERO-DAY VULNERABILITY is an undiscovered flaw in a network, application, or operating system. A ZERO-DAY THREAT is an unknown vulnerability in the system. A ZERO-DAY EXPLOIT is a cyber-attack targeting a vulnerability which is unknown to the vendors, administrators and security personnels.
236. PENETRATION TESTING means thinking like an attacker to test or evaluate how strong or weak a system could be.
237. HONEYPOTS and HONEYNETS are used to lure hackers and attackers to test for vulnerabilities, it happens at the perimeter part of the network. Understand that honeynet is a network of honeypots, that is the difference between both.
238. COMMON VULNERABILITIES ENUMERATION/EXPOSURE (CVE) is an organized database of known vulnerabilities and exposures.
239. SCREENED SUBNET also known as DMZ, it is in between the internal and external network, it has a perimeter network that separates the internal network from the external network.
240. MULTI-FACTOR AUTHENTICATION is a multi-step account login process that requires users to enter more information than just a password. Information like, something you have, something you know, something you are, somewhere you are, and something you do.

241. SINGLE SIGN ON is a federated service, it enables users to log in to multiple applications and websites with one set of credentials.
242. KERBEROS is a protocol for authenticating service requests between trusted hosts across the internet, it is a protocol that talks about certificate.
243. 802.1X is a protocol for port security
244. Apply port security and close unused ports to prevent unwanted devices to plug in through the ports and gain access to the network.
245. Apply network segmentation using VLANs (layer 2) and SUBNETTING (Layer 3), to prevent unwanted users from assessing some important aspect of the organization's network, e.g. Segment customers network from employees own, it is also important to keep administrative network in a separate VLAN or subnet.
246. GPs LOCATION and GEO-IP are the technologies to ensure that a user who logged in to a network is physically in the same building as the network.
247. Getting insurance to manage a particular risk is known as RISK TRANSFER or TRANSFER OF RISK.
248. STICKY is when you want a port to dynamically detect the MAC address allocated to it.
249. HASHING is the process of transforming any given key or a string of characters into another value. The result of a hash is always fix in size, and it changes if there is a change in the plain text, MD5 and SHA1 are hashing algorithms, SHA 1024 is stronger.
250. ENCRYPTION is the process of protecting information or data by using mathematical functions to scramble it in such a way that only the parties who have the key to unscramble it can access it. Decryption is the process of converting a cypher text back to its original plain text. SYMMETRIC ENCRYPTION uses one key to encrypt and decrypt while ASSYMETRIC ENCRYPTION uses two keys (public and private) to encrypt and decrypt.
251. A FIREWALL is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies, it protects the internal network from the public internet. An IDS (INTRUSION DETECTION SYSTEM is designed to only provide an alert about a potential incident, while an IPS (INTRUSION PREVENTION SYSTEM), on the other hand, takes action to block the attempted intrusion or otherwise remediate the incident. Firewalls do STATEFUL AND STATELESS FIREWALLING. STATEFUL FIREWALLING is looking at data coming in and going out of the internet, filters traffic base on IP address and port number. STATELESS FIREWALLING Filters base on conversations.
252. IMPLICIT DENIAL is a firewall rule that states that if a packet does not meet the 3 access roles, it will automatically drop.

253. Be comfortable with the basic understanding of firewall configurations, understand how to restrict access via ACL (Access Control List), when and how to apply it, the 3 types of access control, MANDATORY ACCESS CONTROL (MAC), DISCRETIONARY ACCESS CONTROL (DAC), ROLE-BASE ACCESS CONTROL (RBAC).

254. MAC address filtering is a security mechanism that allows you to block traffic coming from certain known machines or devices.

255. Home office or SOHO uses WPA2 or WPA3 PERSONAL for encryption, understand that the higher the version, the more stronger it is, for enterprise, WPA2 or WPA3 ENTERPRISE , or it can be connected to an authentication server, e.g. RADIUS which is an open source authentication server that used ports 1812 and 1813, it is a UDP protocol and provides AUTHENTICATION, AUTHORIZATION, and ACCOUNTING (AAA) for enterprises. TACACS+ is a CISCO authentication server that used port 49, it is a TCP protocol and provides AUTHENTICATION, AUTHORIZATION, and ACCOUNTING (AAA) for enterprises. **NOTE:** Be comfortable with the major difference between RADIUS and TACACS+.

256. The best and most current encryption standard for access points is WPA3/AES.

257. The two aspects of PHYSICAL SECURITY are DETECTION METHOD and PREVENTION METHOD. DETECTION METHOD includes use of cameras, motion detections, assess tags, tamper detection. PREVENTION METHOD includes, employee training, access control hardware, badge readers, locking racks, locking cabinets, access control vestibule, and smart locker. NOTE: Read meaning into scenario questions that talk about physical security to understand if they are talking about DETECTION METHOD or PREVENTION METHOD.

258. SCRIPT KIDDIE is when a person that is new into the hacking world decides to try and impress his friends by attempting to hack into an FBI database.

259. NON REPUDATION is the process of verifying with a high degree of confidence that the sender is who the receiver thinks he or she is, it is used to verify data integrity.

260. Be comfortable with the following types of ATTACKS; Man in the middle also known as onpath attack, DOS (Denial of Service), DDOS (Distributed Denial of Service), Social engineering, Phishing, Eaves dropping, Shoulder surfing, Tailgating/piggybacking. Understand any scenario question linking to any of them, be comfortable with their causes, effects, and mitigation strategies.

CONCLUSION

Note that the real exam questions may not appear as you are seeing them here, compTIA questions are mostly scenario based, so be comfortable with the terms explained in this document, research more on the network terminologies in other to understand more, so you would be able to read meaning into a real compTIA scenario question, hopefully, you would do perfectly well. I wish you success in your exams.

REFERENCES

- Google search www.google.come
- Jarrel Revera's Network+ class https://www.youtube.com/playlist?list=PLPDtyxMzZVjAL9BK6dNTHZvuIYR49kwA9
- https://en.wikipedia.org
- Station X CompTIA N10-008 preparatory tutorial.