COMPTIA NETWORK+ N10-007
MASTER CHEAT SHEET

TEST DETAILS

Required exam:	CompTIA Network+ N10-007
Number of questions:	Maximum of 90
Types of questions:	Multiple choice and performance-based
Length of test:	90 minutes
Recommended experience:	CompTIA A+ Certified, or equivalent
	Minimum of 9 months of experience in network support or administration; or academic training
Passing score:	720 (on a scale of 100—900)

EXAM OBJECTIVES (DOMAINS)

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%
Total	**100%**

1.0 NETWORKING CONCEPTS

1.1 EXPLAIN THE PURPOSES AND USES OF PORTS AND PROTOCOLS.

A) Protocols and ports:

   a. SMTP (Simple Mail Transfer Protocol) Port 25: A communications protocol that enables sending email from a client to a server or between servers.
   b. SFTP (Secure File Transfer Protocol) Port 22: A protocol available with the proprietary version of SSH that copies files between hosts securely. Like FTP, SFTP first establishes a connection with a host and then allows a remote user to browse directories, list files, and copy files. Unlike FTP, SFTP encrypts data before transmitting it.
   c. SNMP (Simple Network Management Protocol) Port 161: An Application-layer protocol used to exchange information between network device.
   d. SIP (Session Initiation Protocol) Port 5060 5061: A signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications.
   e. SMB (Server Message Block) Port 445: A protocol that works on the Application layer and is used to share files, serial ports, printers, and communications devices, including mail slots and named pipes, between computers.
   f. LDAP (Lightweight Directory Access Protocol) Port 389: A communications protocol that defines how a client can access information, perform operations, and share directory data on a server.
   g. LDAPS (Lightweight Directory Access Protocol Secure) Port 636: A client/server protocol used to access and manage directory information. It reads and edits directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.
   h. H.323 Port 1720: A VoIP standard that handles the initiation, setup, and delivery of VoIP sessions.

B) Protocol types:

   a. ICMP (Internet Control Message Protocol): A core protocol in the TCP/IP suite that notifies the sender that something has gone wrong in the transmission process and that packets were not delivered.

1.2 EXPLAIN DEVICES, APPLICATIONS, PROTOCOLS AND SERVICES AT THEIR APPROPRIATE OSI LAYERS.

Ways for remembering the OSI Model:
Please Do Not Teach Students Pointless Acronyms. (1) Physical - (2) Data Link - (3) Network - (4) Transport - (5) Session - (6) Presentation - (7) Application **All People Seem To Need Data Processing.**

(7) Application - (6) Presentation - (5) Session - (4) Transport - (3) Network - (2) Data - (1) Physical

A) Layer 1 – Physical: Defines hardware connections and turns binary into physical pulses (electrical or light). Cables operate at this layer.

B) Layer 2 – Data link: Identifies devices on the Physical layer. MAC addresses are part of this layer. Switches operate at this layer.

C) Layer 3 – Network: Moves packets between computers on different networks. Routers operate at this layer. IP operates at this layer.

D) Layer 4 – Transport: Breaks data down into manageable chunks with TCP, at this layer. UDP also operates at this layer.

E) Layer 5 – Session: Manages connections between machines. Sockets operate at this layer.

F) Layer 6 – Presentation: Can also manage data encryption, hides the differences among various types of computer systems.

G) Layer 7 – Application: Provides tools for programs to use to access the network (and the lower layers). HTTP, SSL/TLS, FTP, SMTP, DNS, DHCP, and IMAP are all examples of protocols that operate at this layer.

1.3 EXPLAIN THE CONCEPTS AND CHARACTERISTICS OF ROUTING AND SWITCHING.

A) Properties of network traffic:

  a. CSMA (Carrier Sense Multiple Access)/CD (Collision Detection): Rule that ends a sends a jam signal when a collision is detected and then transmits once it's done.

  b. CSMA (Carrier Sense Multiple Access)/CA (Collision Avoidance): Rule that checks to make sure a channel is clear before sending.

  c. Protocol data units: Bits (layer 1), frames (layer 2), packets (layer 3), and segments (layer 4).

  d. MTU (Maximum Transmission Unit): Defines the largest packet size that an interface will forward.

B) Segmentation and interface properties:

  a. Trunking (802.1q): A link between two switches that allows VLAN traffic to be carried.

  b. Tagging and untagging ports:

    i. Tagged ports: Accepts traffic for multiple VLANs

    ii. Untagged ports: Only accepts traffic for a single VLAN.

  c. Port mirroring: The practice 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.

  d. Switching loops/spanning tree:

    i. Switching loops: Occurs in computer networks when there is more than one Layer 2 path between two endpoints.

    ii. Spanning tree: A loop-free logical topology for Ethernet networks.

  e. PoE (Power over Ethernet) and PoE+ (802.3af, 802.3at): Technology that provides power and data transmission through a single network cable.

  f. DMZ (Demilitarized Zone): A small section of a private network that is located between two firewalls and made available for public access.

g. MAC address table: A table of forwarding information held by a Layer 2 switch, built dynamically by listening to incoming frames and used by the switch to match frames to make decisions about where to forward the frame.

h. ARP table: A database of records that maps MAC addresses to IP addresses. The ARP table is stored on a computer's hard disk where it is used by the ARP utility to supply the MAC addresses of network nodes, given their IP addresses.

C) Routing:

a. Distance-vector routing protocols: Routing decisions are based on how far away a destination network is and which exit interface is used to reach the destination.

i. RIP (Routing Information Protocol): A dynamic protocol that uses distance-vector routing algorithms to decipher which route to send data packets.

ii. EIGRP (Enhanced Interior Gateway Protocol): An improvement over IGRP that includes features that support VLSM and classful and classless subnet masks.

b. Link-state routing protocols: A complex type of routing protocol which floods the network with information in an attempt to build a database of routes to other segments.

i. OSPF (Open Shortest Path First): A routing protocol that makes up for some of the limitations of RIP and can coexist with RIP on a network.

c. Hybrid: Is a network routing protocol that combines Distance Vector Routing Protocol (DVRP) and Link State Routing Protocol (LSRP) features. Hybrid is used to determine optimal network destination routes and report network topology data modifications.

i. BGP (Border Gateway Protocol): Border Gateway Protocol is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems on the Internet.

d. Routing types:

i. Static: Packet forwarding rule where the route is manually configured based off the destination IP address.

ii. Dynamic: Packet forwarding rule where the route is automatically determined by the router based on the network conditions.

iii. Default: Packet forwarding rule when no specific rule is given for a destination address.

D) IPv6 concepts:

a. Addressing: Tunneling IPv6 traffic over an Ipv4 network.

b. Tunneling: IPv6 packets can be encapsulated inside IPv4 datagrams

c. Dual stack: When a device uses both IPv4 and IPv6 simultaneously.

d. Router advertisement: Is used for IPv6 auto-configuration and routing. When enabled, messages are sent by the router periodically and in response to solicitations. A host uses the information to learn the prefixes and parameters for the local network.

e. Neighbor discovery: Uses Internet Control Message Protocol (ICMP) messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring devices.

E) Performance concepts:
  a. Traffic shaping: Method of prioritizing network traffic to prevent the network from being bogged down.
  b. Diffserv: Is a simple technique that addresses QoS issues by prioritizing traffic.
  c. CoS (Class of service): Form of Quality of Service that operates at Layer 2.

F) NAT/PAT:
  a. NAT (Network Address Translation): Is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
  b. PAT (Port Address translation): Is an extension of NAT that permits multiple devices on a LAN to be mapped to a single public IP address to conserve IP addresses.

G) ACL (Access control list): Is a list of permissions associated with an object. Specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation.

H) Distributed switching: Is an architecture in which multiple processor-controlled switching units are distributed. There is often a hierarchy of switching elements, with a centralized host switch and with remote switches located close to concentrations of users.

I) Packet-switched vs. circuit-switched network:
  a. Packet-switched: Is a method of grouping data into packets that is then transmitted over a digital network. Packets are made of a header and a payload. One connection may have a higher priority and be allowed more bandwidth allocated.
  b. Circuit-switched network: Two network nodes establish a dedicated communications channel through the network before the nodes may communicate. Connected devices have the same priority and bandwidth.

J) Software-defined networking:

1.4 GIVEN A SCENARIO, CONFIGURE THE APPROPRIATE IP ADDRESSING COMPONENTS.

A) Private vs. public:
  a. Private: Private IPv4 addresses are not unique and can be used by an internal network. Private Address Blocks are 10.0.0.0/8 or 10.0.0.0 to 10.255.255.255, 172.16.0.0/12 or 172.16.0.0 to 172.31.255.255, 192.168.0.0/16 or 192.168.0.0 to 192.168.255.255.
  b. Public: Addresses which are globally routed between ISP routers but not all available IPv4 addresses can be used on the Internet.

B) Loopback and reserved: The IP address range 127.0. 0.0 – 127.255. 255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. Data sent on loopback is forwarded by the operating system to a virtual network interface within the operating system.

C) Virtual IP: A virtual interface means that there is no physical hardware on the device associated with it.

D) Subnetting:
  a. Classful:

        i. Classes A, B, C, D, and E:
            1. Class A: Ranges from 0.0.0.0/8 to 127.0.0.0/8, designed to support extremely large networks with more than 16 million host addresses.
            2. Class B: Ranges from 128.0.0.0/16 to 191.255.0.0, designed to support the needs of moderate to large size networks with up to approximately 65,000 host addresses.
            3. Class C: Ranges from 192.0.0.0/24 to 223.255.255.0/24, designed to support small networks with a maximum of 254 hosts.
            4. Class D: Multicast block consisting of 224.0.0.0 to 239.0.0.0.
            5. Class E: Class E experimental address block consisting of 240.0.0.0-255.0.0.0.
    b. Classless:
        i. VLSM (Variable Length Subnet Mask): Allows a network space to be divided into unequal parts.
        ii. CIDR (Classless Inter-Domain Routing) notation (IPv4 vs. IPv6): Is a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes.

E) Address assignments:
    a. DHCP (Dynamic Host Configuration Protocol): Centralizes management of IP addressing in a network by allowing a server to dynamically assign IP addresses to clients
    b. DHCPv6 (Dynamic Host Configuration Protocol Version 6): It is the IPv6 equivalent of the Dynamic Host Configuration Protocol.
    c. Static: IP addressing is the standard in small-to-large networks when configuring client computers.
    d. EUI64 (Extended Unique Identifier-64): The IEEE (Institute of Electrical and Electronics Engineers) standard defining 64-bit physical addresses. In the EUI-64 scheme, the OUI portion of an address is 24 bits in length. A 40-bit extension identifier makes up the rest of the physical address, for a total of 64 bits.
    e. IP reservations: A rule on the DHCP server called a DHCP reservation can tie the client's MAC address to a particular IP address.

1.5 COMPARE AND CONTRAST THE CHARACTERISTICS OF NETWORK TOPOLOGIES, TYPES AND TECHNOLOGIES.

A) Wired topologies:
    a. Logical vs. physical:
        i. Logical topology refers to the operating systems and protocols used on a network.
        ii. Physical: Refers to the hardware used to create a network (cables, routers, switches, and etc.).
    b. Star: All devices are connected to a central device like a hub or switch. Similar to the spokes on a wheel.

B) Wireless topologies:
   a. Ad hoc: Does not need pre-existing infrastructure to communicate with other devices. Devices communicate amongst themselves in this frequency.
   b. Infrastructure: All devices communicate through an access point. This is the most common wireless communication mode.

C) Technologies that facilitate the Internet of Things (IoT)
   a. Z-Wave: Is used with home automation networking: control lights, locks, and garage doors. Uses wireless mesh networking. Uses the 900 MHz ISM (Industrial, Scientific, and Medical) band. Has no conflicts with 802.11.
   b. Ant+: A proven ULP (Ultra-Low Power) wireless protocol that is responsible for sending information wirelessly from one device to another device, in a robust and flexible manner.
   c. RFID (Radio Frequency Identification): Uses electromagnetic fields to automatically identify and track tags attached to objects.

1.6 GIVEN A SCENARIO, IMPLEMENT THE APPROPRIATE WIRELESS TECHNOLOGIES AND CONFIGURATIONS.

A) 802.11 standards:
   a. a: Came out in October 1999. Issues with range and the signal being absorbed. Frequency is 5 GHz, Speeds up to 54 Mbps.
   b. b: Came out in October 1999. Longer range than 802.11a and less issues with absorption. Issues with frequency conflicts due to the common use of the frequency. Frequency is 2.4 GHz, Speeds up to 11 Mbps
   c. g: Came out in June 2003. Is considered an upgrade to 802.11b. Is backwards compatible with 802.11b. Frequency is 2.4 GHz, Speeds up to 54 Mbps
   d. n: Came out in June 2009. Is an upgrade to 802.11a, 802.11b, and 802.11g. Is the first to support MIMO (Multiple-Input Multiple-Output). Frequency is 2.4 GHz and/or 5 GHz, Speeds up to 600 Mbps
   e. ac: Came out in January 2014. Less issues with frequency conflicts due to 5 GHz being less common. Has greater speeds due to it having denser signaling modulation. Supports MIMO just like 802.11n. Uses Frequency is 5GHz, Speeds up to 7 Gbps.

B) Cellular:
   a. GSM (Global System for Mobile Communications): The Global System for Mobile Communications is a standard developed by the European Telecommunications Standards Institute to describe the protocols for second-generation digital cellular networks used by mobile devices.
   b. TDMA (Time-division multiple access): Is a channel access method for shared-medium networks. It allows several users to share the same frequency channel by dividing the signal into different time slots

    c. CDMA (Code Division Multiple Access): Is a channel access method used by various radio communication technologies.

C) Frequencies:
    a. 2.4 GHz: The 2.4 GHz band provides coverage at a longer range but transmits data at slower speeds.
    b. 5.0 GHz: The 5 GHz band provides less coverage but transmits data at faster speeds. The range is lower because higher frequencies cannot penetrate solid objects.

D) Speed and distance requirements: 2.4 GHz is better for longer distance and 5 GHz is better for shorter distances. Ensure the frequency being used is the correct one, that nothing is blocking the path, and that there is no interference to be able to send the data at an acceptable speed and distance.

E) Channel bandwidth: The rate at which data is exchanged, usually measured in bits per second (bps).

F) Channel bonding: A 802.11n feature that allows two adjacent 20-MHz channels to be combined to make a 40-MHz channel

G) MIMO/MU-MIMO:
    a. MIMO (Multiple-Input and Multiple-Output): Allows more than one antenna to be used on clients and access points, allowing devices to transmit and receive simultaneously.
    b. MU-MIMO (Multiuser MIMO): Allows multiple users to use the same channel.

H) Unidirectional/omnidirectional:
    a. Unidirectional: Unidirectional antennas transmit only in one general direction, allowing the full power of the transmission to be focused on a particular area.
    b. Omnidirectional: Most in home and office Wi-Fi antennas are omnidirectional. These antennas send and receive data in 360 degrees and as a result, the signal is available in the full circle.

I) Site surveys: Is the process of planning and designing a wireless network, for the purpose of providing a wireless solution that will deliver the required wireless coverage.

1.7 SUMMARIZE CLOUD CONCEPTS AND THEIR PURPOSES.

A) Types of services:
    a. SaaS: (Software as a Service): The customer uses software that is not locally stored, instead, all of that service is being provided in the cloud. Ex. Google docs or Gmail.
        i. Everything is managed by the provider.
    b. PaaS (Platform as a Service): Also known as software as a service.
        i. Managed by customer: Data, applications, and making sure apps run on the OS
        ii. Managed by Provider: Runtime, middleware, OS, virtualization, servers, storage, and networking.
    c. IaaS (Infrastructure as a Service): Also known as hardware as a service.
        i. Managed by customer: Software (applications, data, runtime, middleware, and operating system).

B) Cloud delivery models:
   a. Private: Deployed within the organization by the organization for the organization.
   b. Public: Cloud is deployed by the provider within their organization for other organizations to use.
   c. Hybrid: A combination of public and private into a single cloud service.

C) Connectivity methods:
   a. Internet: Is comparatively inexpensive and simple to use. There are issues with latency and security.
   b. Remote Access: These connections offer increased security by creating secure tunnels but are still subject to latency issues.
   c. Leased Line: This option reserves a predetermined bandwidth allocation between the customer and the cloud service provider.
   d. Dedicated Connection: This is the most expensive connection method. Provides a private fixed bandwidth point-to-point data connection. There's no concern of sharing bandwidth.
   e. Security implications/considerations: Consider the cloud provider's security and the security of the backups. Verify your stored data cannot be accessed by unauthorized parties. Ensure your cloud adheres to the Government's regulations.

D) Relationship between local and cloud resources: A customer's local network is easier to secure and offer the speed benefits of their network without the possibility of third-party access. Cloud storage offers greater scalability, user accessibility, and elasticity features when compared to local resources.

1.8 EXPLAIN THE FUNCTIONS OF NETWORK SERVICES.

A) DNS service:
   a. Record types:
      i. A, AAA: These records hold the name-to-address mapping (conversion) for a given host.
         1. A: Record for IPv4.
         2. AAA: Record for IPv6.
      ii. TXT (SPF, DKIM):
         1. TXT (Text): is used to provide freely formatted text to network administrators regarding any network related issues or comments.
         2. SPF (The Sender Provider Framework): validates the email servers allowed to send email.
         3. DKIM (DomainKeys Identified Mail): Is an encryption-based authentication method that validates the domain name of emails.
      iii. SRV (Service): Contains hostname and port details for hosts providing specific services.
      iv. MX (Mail Exchanger): Supports email traffic by identifying email servers.

        v. CNAME (Canonical Name): Contains the alias for a host's CNAME. This allows a hostname alias like myorganization to be recognized by its canonical name www.myorganization.com.
        vi. NS (Name Server): Specifies the authoritative name server for a domain. The NS record is used by name servers to locate each other. This record is used to delegate subdomains. An NS record is required for each primary and secondary name server in a domain.
        vii. PTR (Pointer): Is the opposite of an A record. It supports reverse lookups by providing the IP address-to-hostname information in a reverse lookup zone file (reverse zone). This format is essentially an A record with a reversed IP address listed first followed by the hostname. This differs from a forward lookup zone file (forward zone) in which the A record is used to find the host using the hostname.
    b. Internal vs. external DNS:
        i. Internal DNS: Serves the domain and is inaccessible from the Internet. Internal hosts requiring Internet communication or external resolution will have their requests forwarded from the internal DNS server to the external DNS server.
        ii. External DNS: Is placed in a DMZ and will only provide access to public services like a web server or VPN.
    c. Third-party/cloud-hosted DNS: Third-party or cloud-based DNS offers several advantages over traditional DNS services. In many cases, it can be more affordable to use cloud-based DNS as it is scalable, resilient, and secure. Administration is simplified. If you opt for a large cloud provider such as Google, you will reap the benefit of reduced latency due to the presence of multiple geographic locations which are available to resolve traffic quickly.
    d. Hierarchy:
        i. Root: The DNS root zone is the top-level DNS zone in the hierarchical namespace of the Domain Name System of the Internet.
        ii. Top-level domain: Servers are labeled as: .com, .org, .edu, etc. or by the country code (ccTLD) .us, .uk, or .jp.
        iii. Second-level Domain: are directly below their TLDs in this hierarchy. These are the domains assignable by domain registrars.
        iv. Third Level Domains: Are subdomains of SLDs.
    e. Forward vs. reverse zone:

B) DHCP service:
    a. MAC reservations: Since dynamic addressing does not work reliably for hosts that must be consistently available, such as a network printer, you can create a MAC reservation on your DHCP server to assign the same IP address to that particular device.
    b. Pools: A DHCP server can be configured to assign addresses from a predefined range. This is known as the DHCP scope or DHCP pool.

c. IP exclusions: Another way to guarantee that a host is consistently available is to statically assign an IP address to it. In order to prevent the address from being assigned in the DHCP environment, an IP exclusion can be configured on the DHCP server.

d. Scope options: When configuring a DHCP server, it is also necessary to provide additional information to the clients. In addition to the address, the client needs the default gateway address, a primary and secondary DNS server address, and the length of time the address is leased to the client. Known as lease time, this field is a variable time value that once expired, the IP address will be returned from the client back into the address pool for reissue.

e. Lease time: The amount of time that a client can hold an IP address. Default is 8 days.

f. TTL (Time to Live): Is a mechanism that limits the lifespan or lifetime of data in a computer or network.

g. DHCP relay/IP helper:

    i. DHCP Relay: Allows a single DHCP server to provide the necessary configurations in a network of multiple LANs with different subnets.

    ii. IP helper: The IP helper address provides support for the rebroadcasting or forwarding of UDP packets across a router.

C) NTP (Network Time Protocol): Is for clock synchronization between computer systems over packet-switched, variable-latency data networks. Oldest internet protocol still in use, introduced in 1985.

D) IPAM (IP Address Management): Tracks, plans, and manages IP addressing on networks.

2.0 INFRASTRUCTURE

2.1 GIVEN A SCENARIO, DEPLOY THE APPROPRIATE CABLING SOLUTION.

A) Media types:

- a. Copper:
  - i. UTP (Unshielded Twisted Pair): A type of copper twisted pair cabling that does not include shielding around its conductors.
  - ii. STP (Shielded Twisted Pair): A type of cable containing twisted-wire pairs that are not only individually insulated, but also surrounded by a shielding made of a metallic substance such as foil.
  - iii. Coaxial: Insulated copper wire; used to carry high-speed data traffic and television signals.
- b. Fiber: Type of cabling that uses light transmissions instead of electric pulses making threats such as EMI, crosstalk and attenuation non-issues. Well-suited for high-speed data communications and expensive too.
  - i. Single-mode: A type of fiber optic cable that uses a single direct beam of light, thus allowing for greater distance and increased transfer speeds.
  - ii. Multimode: A type of fiber optic cable that carries multiple beams of light through the cable, bouncing off the cable walls. This strategy actually weakens the signal, reducing the length and speed at which the data signal can travel.

B) Plenum vs. PVC:

- a. Plenum: Is made of Teflon or FEP which gives off much less poisonous gas than PVC when it burns. Also suffer from less attenuation than the PVC cabling.
- b. PVC (Polyvinyl Chloride): The jacket when burning or smoldering releases hydrochloric acid and dioxin which are both toxic.

C) Connector types:

- a. Copper:
  - i. RJ-45: An eight-position connector that uses all four pairs of wires. It is usually used for network connectivity.
  - ii. RJ-11: The standard connector used with unshielded twisted pair cabling (usually Cat 3 or Level 1) to connect analog telephones.
  - iii. BNC: A connector used with thin coaxial cable. Some BNC connectors are T-shaped and called T-connectors. One end of the T connects to the NIC, and the two other ends can connect to cables or end a bus formation with a terminator.
  - iv. DB-9: A type of connector with nine pins that's commonly used in serial communication that conforms to the RS-232 standard.
  - v. DB-25: A type of connector with 25 pins that's commonly used in serial communication that conforms to the RS-232 standard.
  - vi. F-type: A connector used with an RG-6 coaxial cable and is used for connections to a TV and has a single copper wire.
- b. Fiber:

i. LC (Lucent Connector): Used with fiber cables. It was developed by Lucent Technologies and is a miniaturized version of the SC connector. Is commonly found on MMF and SMF optic cables.

ii. ST (Straight Tip): A connector used with single-mode or multimode fiber-optic cable.

iii. SC (Standard Connector): A square connector with a floating ferrule that contains the fiber-optic cable.

1. APC (Angled Physical Connector): A connector that has an eight degree angle. Lower return loss, generally higher insertion loss than UPC.
2. UPC (Ultra Polished Connector): A connector with its end face polished flat. High return loss.
3. MTRJ (Mechanical Transfer Registered Jack): A type of connector popular for duplex multimode connections.

D) Transceivers:

a. SFP (Small Form Factor Pluggable): A transceiver commonly used to provide 1 Gbit/s fiber. Similar to a GBIC, but is smaller in size.

b. GBIC (Gigabit Interface): Converts electric currents to optical signals, and optical signals to currents. The GBIC is typically employed in fiber optic and Ethernet systems as an interface for high-speed networking.

c. SFP (Small Form-Factor Pluggable) +: Newer version of SFP, is the same size as SFP, supports data rates as high as 16 Gbit/s, and is commonly used with 10 Gigabit Ethernet.

d. QSFP (Quad Small Factor Pluggable): A compact hot-pluggable transceiver that is also used for data communication applications.

e. Characteristics of fiber transceivers:

i. Bidirectional: Can transmit and receive data through a single optical fiber.

ii. Duplex: Uses two fibers, one transmits data and the other receives it.

E) Termination points:

a. 66 block: A patch panel for analog voice. Left side is patched to the right. Replaced by 110 blocks but still seen in many installations. Is used primarily for telephone applications.

b. 110 block: A wire-to-wire patch panel that replaces the 66 block and is able to patch cat 5e and cat6 cables. Connecting block is on top. Wires are "punched" into the block top to bottom.

c. Patch panel: A wall-mounted panel of data receptors into which cross-connect patch cables from the punch-down block are inserted. Provides a connection point between network equipment such as switches and hubs.

d. Fiber distribution panel: A cabinet intended to provide space for termination, storage, and splicing fiber connections. Similar to a patch panel. Often includes a service loop which is extra fiber for future changes and serves as inexpensive insurance.

F) Copper cable standards:

a. Cat 3: Maximum speed is 10 Mbps, maximum distance is 100 meters, and certified frequency is 16 MHz.

b. Cat 5: Maximum speed is 100 Mbps, maximum distance is 100 meters, and certified frequency is 100 MHz.

c. Cat 5e: Maximum speed is 1 Gbps, maximum distance is 100 meters, and certified frequency is 250 MHz.

d. Cat 6: Maximum speed is 10 Gbps, maximum distance is 100 meters, and certified frequency is 500 MHz.

e. Cat 6a: Maximum speed is 10 Gbps, maximum distance is 100 meters, and certified frequency is 500 MHz.

f. Cat 7: Maximum speed is 10 Gbps, maximum distance is 100 meters, and certified frequency is 600 MHz.

g. RG-6: Uses F-type screw-on connectors. Used for television, satellite, and broadband cable connections.

h. RG-59: Typically used for short distance applications, such as carrying composite video between two nearby devices.

G) Copper termination standards:

a. TIA (Telecommunication Industries Association)/ EIA (Electronic Industries Alliance) 568a:

i. Green/White
ii. Green
iii. White/Orange
iv. Blue
v. White/Blue
vi. Orange
vii. Brown/White
viii. Brown

b. TIA/EIA 568b:

i. Orange/White
ii. Orange
iii. Green/White
iv. Blue
v. Blue/White
vi. Green
vii. Brown/ White
viii. Brown

c. Crossover: Cable that has two wires crossed (1 and 3, 2 and 6). Used to directly network two PCs without using a hub or switch.

d. Straight-through: A twisted pair patch cable in which the wire terminations in both connectors follow the same scheme.

H) Ethernet deployment standards:

a. 100BaseT: Ethernet cabling system designed to run at 100 Mbps on twisted pair cabling. It uses baseband signaling. Max length of 100 m. Uses Cat5 or better.

b. 1000BaseT: Ethernet cabling standard designed to run at 1000 Mbps on twisted pair cabling. It uses baseband signaling. Max length of 100 m. Uses Cat5 or better

c. 1000BaseLX: A Gigabit Ethernet standard using single-mode fiber cabling, with a 5-km maximum cable distance.

d. 1000BaseSX: A Gigabit Ethernet standard using multimode fiber cabling, with a 220- to 500-m maximum cable distance.

e. 10GBaseT: A 10 GbE standard designed to run on CAT 6a UTP cabling. Maximum cable length of 100 m.

2.2 GIVEN A SCENARIO, DETERMINE THE APPROPRIATE PLACEMENT OF NETWORKING DEVICES ON A NETWORK AND INSTALL/CONFIGURE THEM.

A) Firewall: Can be either software or hardware, firewalls control access to your network. Placed at networks entry/exit point. Can also control access between specific network segments within a network.

B) Router: Network device that joins two network segments. Receives packet, forwards the packet to the next hop on the route/destination. Layer 3 device.

C) Switch: Network device that forwards data only to the port that connects to the destination device. Layer 2/3 device.

D) Hub: Network device that directs data packets to all devices connected to it. Inefficient and can cause performance bottlenecks on busy networks.

E) Bridge: Network device that connects two networks. Replaced mostly by switches.

F) Modems: Network device that converts the digital signals generated by a computer into analog signals that can travel over conventional phone lines (and vice versa). Used to connect to ISP.

G) (WAP) Wireless access point: Network device that can operate as a bridge connecting a standard wired network to wireless device or as a router passing data transmissions from one access point to another. Layer 2 device. These are switches, DHCP servers, router and firewall.

H) Media converter: A device that enables networks or segments using different media to interconnect and exchange signals. Used mostly with fiber. Reasons to use: cost, disparate segments, and needing to run a particular medium in a setting. Examples include: single mode fiber to Ethernet, single mode to multimode fiber, multimode fiber to Ethernet, fiber to coaxial.

I) Wireless range extender: A device that amplifies wireless signal to make it stronger. Needs to be on the same channel as the AP for it to take the transmission and repeat it.

J) VoIP endpoint: Any final destination for a voice call (physical device, software, or server). Used with SIP.

2.3 EXPLAIN THE PURPOSES AND USE CASES FOR ADVANCED NETWORKING DEVICES.

A) Multilayer switch: Network device that examines the network data it receives, devices where the content is intended to go, and forwards it. Operates on layers 2 and 3. Known as content switch or load-balancing switch.

B) Wireless controller: A centralized appliance or software package that monitors, manages, and controls multiple wireless access points. Used with branch/remote office deployments for wireless authentication. On boot, the access point authenticates with this before it can start working as an access point.

C) Load balancer: Stand-alone network devices that perform load balancing as their primary function. This increases network performance, reliability, and availability. Increasing redundancy results in greater data availability.

D) IDS (Intrusion Detection System)/IPS (Intrusion Prevention System):

   a. IDS: A passive detection system that can detect the presence of an attack and then log that information. Alerts administrator to the potential threat.

   b. IPS: An active detection system that continually scans the network looking for inappropriate activity. Looks for known signature of attacks and automatically tries to prevent them

E) Proxy server: A server that sits between a client computer and the Internet and looks at the web page request the client sends. Provides caching which makes a copy of the web page contents and stores in cache for the next request. Increases network performance and response time, and reduces bandwidth needed to fulfill client requests

F) VPN concentrator: A device that aggregates hundreds or thousands of VPN connections. Increases remote access security, encrypt/decrypt data, regulate and monitor data transfer across the tunnel, control inbound and outbound traffic.

G) AAA (Authorization, authentication, and auditing) /RADIUS server: A protocol that enables a single server to become responsible for all remote-access AAA services. Client/server system

H) UTM (Unified Threat Management) appliance: Network device that functions as: a URL filter to monitor inbound traffic and restrict sites, spam filter to filter emails, router, switch, firewall, IPS/IDS, bandwidth shaper to prevent users/systems from hogging network, VPN endpoint, malware inspection to scan files for malware.

I) NGFW (Next Generation Firewall) /Layer 7 firewall: Network device that requires some advanced decodes. Every packet that passes through the network must be analyzed, categorized, and a security decision determined.

J) VoIP PBX (Private Branch Exchange): Device that connects to phone provider network and connects analog telephone lines to each desk. Aka the "phone switch".

K) VoIP gateway: The device that converts an analog telephone call (voice and signals) into data packets (and vice versa) for traversal over an IP-based network.

L) Content filter: Software that controls what users can peruse, mostly associated with websites. Allows for corporate control of outbound and inbound data. Can control traffic based on data within the content. Protects against viruses/malware.

2.4 EXPLAIN THE PURPOSES OF VIRTUALIZATION AND NETWORK STORAGE TECHNOLOGIES.

A) Virtual networking components:

   a. Virtual switch: A firewall that is implemented in software within a virtual machine in cases where it would be difficult, costly, or impossible to install a traditional physical firewall.

   b. Virtual firewall: A firewall that runs within a virtualized environment and monitors and controls traffic as it passes through virtual machines. The firewall can be a traditional firewall running within a guest virtual machine or a component of a hypervisor.

   c. Virtual NIC: Is the network connection for each virtual host. The virtual NIC connects to a virtual switch, which connects them to the virtual LAN, virtual Router or physical LAN.

   d. Virtual router: A router that is implemented in software within a virtual machine. The scalability of a virtual machine makes it easy to add capacity to the router when it is needed. Virtual routers are easily managed and are highly scalable without requiring the purchase of additional network hardware.

   e. Hypervisor: Software that enables a single computer to run multiple operating systems simultaneously.

B) Network storage types:

   a. NAS (Network Attached Storage): A specialized storage device or group of storage devices that provides centralized fault-tolerant data storage for a network. NAS depends on traditional network transmission methods such as Ethernet.

   b. SAN (Storage Area Network): A distinct network of storage devices that communicate directly with each other and with other networks. A SAN uses a proprietary network transmission method such as Fibre Channel rather than a traditional network transmission method such as Ethernet.

C) Connection type:

   a. FCoE (Fibre Channel over Ethernet): A technology that encapsulates Fibre Channel frames over Ethernet networks allowing FC to use 10 Gigabit Ethernet networks (or higher) while preserving the Fibre Channel protocol.

   b. Fibre Channel: A high-speed storage network protocol that can transmit up to 16 gigabits per second.

   c. iSCSI (Internet Small Computer Systems Interface): Send SCSI commands over an IP network.

   d. InfiniBand: High-performance networking protocol that is used as a SAN connectivity type. Designed to be extremely low-latency, high throughput, and lossless connection.

   e. A high speed serial connection or bus used to interconnect processors and peripheral devices. Speeds such as 100Gbit/s and 200 Gbit/s are common. Designed to be scalable and alternative to FC.

D) Jumbo frame: A single non-standard Ethernet frame that allows for larger maximum payload size. Increases transfer efficiency due to having to send fewer packets to a switch/node.

2.5 COMPARE AND CONTRAST WAN TECHNOLOGIES.

A) Service type:

   a. ISDN (Integrated Services Digital Network): A broadband telephone line that can carry data at about five times the speed of regular telephone lines. Two channels (telephone numbers) share a single pair of wires. ISDN has been replaced by DSL.

   b. T1/T3: North America, copper

      i. T1: Is a communications transmission service that uses 2 twisted pair copper wires to transmit and receive data or voice traffic. A leased-line connection capable of carrying data at 1,544,000 Mbps.

      ii. T3: A T3 line is composed of 28 bundled T1-level circuits. Each T1 circuit operates at 1.544 Mbps, for a total connection speed of 44.736 Mbps.

   c. E1/E3: European, copper

      i. E1: A connection that carries 32 channels at 64 Kbps for a total of 2.048 Mbps. E1 lines can be interconnected with T1 lines for international use.

      ii. E3: Line that carries 16 E1 lines (512 channels), for a total bandwidth of 34.368 Mbps.

   d. OC-3 – OC-192: Fiber optics

      i. OC-3: A popular throughput rate for SONET services, providing a maximum 155.52 Mbps.

      ii. OC-192: A popular throughput rate for SONET services, providing a maximum 10 Gbps.

   e. DSL (Digital Subscriber Line): A broadband Internet connection method that transmits digital signals over existing phone lines.

   f. Metropolitan Ethernet: The use of Carrier Ethernet technology in metropolitan area networks (MANs).

   g. Cable broadband: Technology used for cable Internet and cable TV. It operates at a higher speed than DSL.

   h. Dial-up: Internet access that connects using a telephone line and a MODEM.

   i. PRI (Primary Rate Interface): A type of ISDN that uses 23 bearer channels and one 64-Kbps data channel, represented by the notation 23B+D.

B) Transmission mediums:

   a. Satellite: Satellite communication relies on line of sight transmission and is subject to physical obstructions like thick storm clouds. It also has higher latency than other WAN technologies since the signal is transmitted thousands of miles to the satellite then thousands of miles back down.

   b. Copper: Is a popular handoff from the provider when the network equipment is within 100 meters or less from the provider's termination point. The various services that copper is used with include leased lines, broadband cable, DSL, and dialup.

   c. Fiber: A cable that transmits data at close to the speed of light along glass or plastic fibers.

d. Wireless: A form of computer networking or other communication that uses radio signals and microwaves to transmit data

C) Characteristics of service:

a. MPLS (Multiprotocol Label Switching): A network technology defined by a set of IETF specifications that enable Layer 3 devices, such as routers, to establish and manage network traffic.

b. ATM (Asynchronous Transfer Mode): A cell-switching network technology designed for the high-speed transfer of voice, video, and data in LANs, WANs, and telephone networks.

c. Frame relay: A WAN protocol that operates at the Physical and Data Link layers of the OSI model.

d. PPPoE (Point-to-Point Protocol over Ethernet): A protocol used to connect multiple network users on an Ethernet local area network to a remote site through a common device.

e. PPP (Point-to-Point Protocol): A protocol that works on the Data Link layer of the TCP/IP protocol suite, PPP is used to send IP datagrams over serial point-to-point links. PPP can be used in synchronous and asynchronous connections and can dynamically configure and test remote network connections.

f. DMVPN ((Dynamic Multipoint Virtual Private Network): Is a protocol that dynamically builds Internet Protocol Security (IPsec) VPN connections between branch offices.

g. SIP trunk (Session Initiation Protocol): Is a trunk purchased from a SIP provider for connecting VoIP PBXs calls. The SIP trunk is an IP version of a leased line for a PBX, since it allows for connectivity to the PSTN for VoIP.

D) Termination:

a. Demarcation point (Demarc): The point of division between a telecommunications service carrier's network and a building's internal network.

b. CSU (Channel Service Unit) /DSU (Data Service Unit): A combination of two WAN connectivity devices on a Frame Relay network that work together to connect a digital WAN line with a customer's LAN.

c. Smart jack: A termination for T-carrier wire pairs that is located at the customer demark and which functions as a connection protection and monitoring point.

3.0 NETWORK OPERATIONS

3.1 GIVEN A SCENARIO, USE APPROPRIATE DOCUMENTATION AND DIAGRAMS TO MANAGE THE NETWORK.

A) Diagram symbols: Pictures depicting routers, switches, firewalls, etc. in a network diagram. In diagrams, routers are typically depicted as circles and switches are depicted as triangles.

B) Standard operating procedures/work instructions: This document shows who can/cannot access server rooms, network policy and procedures such as network firewalls, passwords, physical security, protocols, mobile device use, and etc.

C) Logical vs. physical diagrams:

   a. Logical: A diagram that shows how data flows in a network.

   b. Physical: A diagram that shows how a network is physically connected showing information such as: cabling info, servers, network devices, WAN, user info, and etc.

D) Rack diagrams: Diagram that shows where cables go to and their purpose on a rack.

E) Change management documentation: A set of documents that defines procedures for changes to the network.

F) Wiring and port locations: Diagram that shows where wires/ports are set on a network. The more general this is written, the less updating is required when changes occur.

G) IDF (Intermediate Distribution Frame)/MDF (Main Distribution Frame) documentation: Termination point within local telephone exchange where equipment and local loopbacks are connected by jumper wires. Must document all free-standing or wall-mounted rack and the cables running between them and the end users so technicians can easily refer to it.

H) Labeling: The process of labeling items/devices. Should have standard rules that are enforced at all levels in the organization.

I) Network configuration and performance baselines: Document that shows how a network should normally operate: typical network usage, speeds, and etc.

J) Inventory management: Process of tagging and recording all assets.

3.2 COMPARE AND CONTRAST BUSINESS CONTINUITY AND DISASTER RECOVERY CONCEPTS.

A) Availability concepts:

   a. Fault tolerance: The ability for a system to respond to unexpected failures or system crashes as the backup system immediately and automatically takes over with no loss of service.

   b. High availability: When a system is continuously operational at all times.

   c. Load balancing: Distributing a computing or networking workload across multiple systems to avoid congestion and slow performance.

   d. NIC (Network Interface Controller) teaming: A type of link aggregation in which two or more NICs work in tandem to handle traffic to and from a single node.

   e. Port aggregation: Is a mechanism for aggregating ports together for increasing bandwidth between switches

f. Clustering: Provides failover, load balancing, and high availability for the services running on the cluster.
g. Power management: The ability to place computers and devices in low-power states when they are not being used.
h. Battery backups/UPS (Uninterruptible Power Supply): A device that provides backup power when the electrical power fails or drops to an unacceptable voltage level.
i. Power generators: Supply power during a power outage. Power generators consist of three major components: fuel, an engine, and a generator. The engine burns the fuel to turn the generator and create power. The three common sources of fuel are natural gas, gasoline, and diesel. Diesel fuel generators are the most common type of generator supplying data centers around the world.
j. Dual power supplies: Power generators and battery UPSs are a requirement to operate during a power outage.
k. Redundant circuits: Redundant Circuit Pair means two identical power circuits installed in the same cabinet or rack, neither of which is a part of another pair of circuits in the same cabinet or rack.

B) Recovery:

a. Cold sites: A "recovery" cold site is essentially data center space, with power, and network connectivity that is available when needed. In the event of a disaster, teams can move and install a business's hardware at the cold site in order to get the systems back up and running.
b. Warm sites: A "preventative" warm site allows a business to pre-install hardware and pre-configure their bandwidth needs. In the event of a disaster, the business can then load their software and restore their business systems.
c. Hot sites: A "proactive" hot site allows a business to keep servers and a live backup site up and running in the event of a disaster. The production environment is replicated in a data center, allowing for immediate access in the event of a disaster at the primary site.
d. Backups: Procedures that store company data files in a safe place, such as online or on a flash drive.
e. Full: A backup that copies all data to the archive medium.
f. Differential: A type of partial backup that involves copying all changes made since the last full backup. Thus, each new differential backup file contains the cumulative effects of all activity since the last full backup.
g. Incremental: A type of partial backup that involves copying only the data items that have changed since the last partial backup. This produces a set of incremental backup files, each containing the results of one day's transactions
h. Snapshots: Technology that is very flexible, allowing making different types of momentary copies of volumes or file systems

C) MTTR (Mean Time To Repair): The average length of time required to perform a repair on the device

D) MTBF (Mean Time Between Failures): A measure of the average time between failures in a system - the higher the amount, the more reliable the thing is.

E) SLA requirements (Service Level Agreement): A legally binding contract or part of a contract that defines, in plain language and in measurable terms, the aspects of a service provided to a customer. Specific details might include contract duration, guaranteed uptime, problem management, performance benchmarks, and termination options.

3.3 EXPLAIN COMMON SCANNING, MONITORING AND PATCHING PROCESSES AND SUMMARIZE THEIR EXPECTED OUTPUTS.

A) Processes:

   a. Log reviewing: Process for looking at event logs to find intrusions and diagnosing current system problems. You need a lot of memory space to store logs, use data rollup when necessary.

   b. Port scanning: Using a program to remotely determine which ports on a system are open.

   c. Vulnerability scanning: The act of scanning for weaknesses and susceptibilities in the network and on individual systems.

   d. Patch management: The process of regularly applying patches and updates to software.

      i. Rollback: Undo any changes made to a system if the update that was recently installed negatively affects it.

   e. Reviewing baselines: Concept of understanding what normal operation of your network looks like over time.

   f. Packet/traffic analysis: Concept of gathering information from packets and traffic patterns on the network. Use this to identify unknown traffic or verify packet filtering and security controls.

B) Event management:

   a. Notifications: Getting alerted to an event occurring by sending an alert via SMS text or Email to the administrator.

   b. Alerts: Set alerts for when important events occur that need immediate addressing.

   c. SIEM (Security Information and Event Management): Provide notifications and real-time analysis of security alerts and can help you head off problems quickly.

C) SNMP (Simple Network Messaging Protocol) monitors: Is any kind of software that manages workstations and devices on a network.

   a. MIB (Management Information Base): A database used in network management that contains a device's definitions of managed objects and their data.

D) Metrics:

   a. Error rate: The amount of packets per second that error out.

   b. Utilization: Is how much bandwidth of a port is being used.

   c. Packet drops: The amount of packets dropped per second

   d. Bandwidth/throughput: The amount of data that can be transferred in a given time period.

3.4 GIVEN A SCENARIO, USE REMOTE ACCESS METHODS.

A) VPN (Virtual Private Network): A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network
   a. IPSec (Internet Protocol Security): A Layer 3 protocol that defines encryption, authentication, and key management for TCP/IP transmissions. IPSec is an enhancement to IPv4 and is native to IPv6. IPSec is unique among authentication methods in that it adds security information to the header of all IP packets.
   b. SSL/TLS/DTLS:
      i. SSL (Secure Socket Layer): Protocol for web browsers and servers that allows for the authentication, encryption and decryption of data sent over the Internet.
      ii. TLS (Transport Layer Security): Replaced SSL. It is a security protocol that uses certificates and public key cryptography for mutual authentication and data encryption over a TCP/IP connection.
      iii. DTLS (Datagram Transport Layer Security): Is based on the TLS protocol and provides the same security TLS provides. DTLS is mainly used for UDP encryption of segments and datagrams.
   c. Site-to-site: This VPN type connects one entire network site to another; such as a headquarters location to a branch office.
   d. Client-to-site: Connections are used to connect an individual device, such as a laptop or mobile phone, to the company network.

B) RDP (Remote Desktop Protocol): Allows the user to access a remote system as if they were sitting in front of it in the remote location.

C) SSH (Secure Shell): Protocol used for encrypted console communication. An SSH connection is secure at both ends of the connection.

D) VNC (Virtual Network Computing): An open source system that enables a remote workstation to manipulate and receive screen updates from a host.

E) Telnet: An unsecure protocol used for console communication.

F) HTTPS/management URL: Protocol used for secure web pages for when users must enter personal information like credit cards, passwords, and etc.

G) Remote file access:
   a. FTP/FTPS:
      i. FTP (File Transport Protocol): Transfers files between systems with authentication but no built in encryption.
      ii. FTPS (File Transport Protocol Security): Is an extension to FTP that adds support for the TLS.
   b. SFTP (SSH File Transfer Protocol): Provides file system functionality over SSH. Used for resuming interrupted transfers, directory listing, and remote file removal.
   c. TFTP (Trivial File Transfer Protocol): Has no authentication. May be used to download configurations for devices such as VoIP phones.

H) Out-of-band management:
   a. Modem: Connect a modem and dial-in to manage the device when the network is not available or if the device is not accessible from the network.
   b. Console router: Gives out-of-band access for multiple devices when the network is not available or if the device is not accessible from the network.

3.5 IDENTIFY POLICIES AND BEST PRACTICES.

A) Privileged user agreement: A signed agreement to only use privileged access only for assigned job duties.

B) Password policy: A collection of settings to control password characteristics such as length, complexity, how often it should be changed.

C) On-boarding/off-boarding procedures:
   a. On-boarding: Procedure for new hires in organization. IT agreements need to be signed, create accounts and associate users with proper groups, rights/access files, and departs, and provide required IT software.
   b. Off-boarding: Procedure for out-going employees in an organization. Should be preplanned on how to handle the hardware, data. Account information is usually deactivated, not always deleted.

D) Licensing restrictions: Policy that only grants licenses to authorized users. Make sure licenses are always available and not expired.

E) International export controls: U.S. laws and regulations that restrict the release of critical technologies and information to foreign nationals, within and outside of the United States, for reasons of foreign policy and to ensure national security.

F) Data loss prevention: Policies that dictate how an organization handles personally identifiable data such as medical records. Details how the sensitive data is: transferred and encrypted.

G) Remote access policies: Policies that define how to manage data and process of communication outside of the network. Sets specific technical requirements such as encrypted connection, confidential credentials, use of network, and hardware and software requirements.

H) Incident response policies: Policies on how to respond to security attacks. Shows how an incident is defined, how the incident is organized, and who responds to the incident.

I) BYOD (Bring Your Own Device): The practice of allowing users to use their own personal devices to connect to an organizational network. Difficult to secure.

J) AUP (Acceptable Use Policy): A Set of rules and guidelines that are set up to regulate Internet use as well as what employees can perform on company equipment.

K) NDA (Non-Disclosure Agreement): A signed agreement between a company and an agency in which the agency promises they will not disclose or share confidential information.

L) System life cycle:
   a. Asset disposal: Some information must not be destroyed, consider offsite storage. Wipe devices completely to prevent dumpster diving, or physically destroy it.

M) Safety procedures and policies: Policies on equipment safety, personal safety, handling of toxic waste, local government regulations, and environmental regulations.

4.0 NETWORK SECURITY

4.1 SUMMARIZE THE PURPOSES OF PHYSICAL SECURITY DEVICES.

A) Detection:

   a. Motion detection: Determining an object's change in position in relation to its surroundings.
   b. Video surveillance: The use of video cameras to monitor activities of individuals, such as employees or individuals in public locations, for work-related or crime-prevention purposes.
   c. Asset tracking tags: A record of every asset.
   d. Tamper detection: A common form of Tamper detection is a sticker which when broken, indicates the opening of a device enclosure. This is not the only tamper detection that may be encountered. More sophisticated tamper detectors are mounted inside the device and can trigger alarms, lights, and cameras.

B) Prevention:

   a. Badges: Are used to provide proof of access to others. Proper processes and procedures must be in place for a successful implementation of this prevention tactic.
   b. Biometrics: The identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice, or handwriting
   c. Smart cards: Plastic cards, similar in appearance to a credit card, with a computer chip embedded in it
   d. Key fob: A small device containing a microchip used to generate unique passwords for logging on to a computer or a network.
   e. Locks: Use of locks on doors and equipment. This might mean the installation of a tumbler-style lock for the switching closet or an elaborate electronic combination lock.

4.2 EXPLAIN AUTHENTICATION AND ACCESS CONTROLS.

A) Authorization, authentication and accounting:

   a. RADIUS (Remote Authentication Dial-In User Service): A protocol that enables a single server to become responsible for all remote-access authentication, authorization, and auditing (or accounting) services. Functions as a client/server system.
   b. TACACS+ (Terminal Access Controller Access-Control System Plus): A security protocol designed to provide centralized validation of users who are attempting to gain access to a router or NAS. Uses TCP on port 49 by default.
   c. Kerberos: A non-proprietary protocol and is used for cross-platform authentication. This is also the main authentication protocol used with windows servers. This protocol used SSO and symmetric cryptography. Security tokens are called tickets.
   d. Single sign-on: A gateway service that permits users to log in once with a single user ID and password to gain access to multiple software applications.
   e. Local authentication: Authentication done locally by the OS using values stored in it.

f. LDAP (Lightweight Directory Access Protocol): A communications protocol that defines how a client can access information, perform operations, and share directory data on a server.
g. Certificates: A key component of PKI. A form of electronic credentials that validates users, computers, or devices on the network. A digitally signed statement that associates the credentials of a public key to the identity of the person, device, or service that holds the corresponding key.
h. Auditing and logging: The process of monitoring occurrences and keeping a log of what has occurred on a system. This helps prevent unauthorized access, provides a record for admins to analyze and make security changes, and provides solid evidence in case of improper misconduct.

B) Multifactor authentication:

a. Something you know: Certain knowledge only known to the user, such as a password.
b. Something you have: Some physical object in the possession of the user.
c. Something you are: Some physical characteristic of the user, also known as biometrics.
d. Somewhere you are: Some connection to a specific computing network or using a GPS signal to identify the location.
e. Something you do: Proves identities by observing actions, such as gestures or touches.

C) Access control:

a. 802.1x: The standard that defines port based security for wireless networks access control. Allows APs and switches to not do the authentication but instead rely on the authentication server to do the work.
b. NAC (Network Access Control): A method to restrict access to the network based on identity or posture. Posture assessment any evaluation of a systems security based on settings and applications found.
c. Port security: Disabling unused application/service ports to reduce the number of threat vectors.
d. MAC filtering: A list of MAC addresses and configured to allow or deny access to certain systems based on the list.
e. Captive portal: Forces clients using a web browser to complete a task before being able to access the network.
f. Technical solution that forces clients using web browsers to complete a specific process before it allows them access to the network.
g. Access control lists: Allow or disallow traffic based on tuples.

4.3 GIVEN A SCENARIO, SECURE A BASIC WIRELESS NETWORK.

A) WPA (Wi-Fi Protected Access): A security protocol developed by the Wi-Fi Alliance in 2003 for use in securing wireless networks; designed to replace the WEP protocol. Still uses WEP's insecure RC4 stream cipher but provides extra security through TKIP.

B) WPA2: Security protocol developed by the Wi-Fi Alliance in 2004 for use in securing wireless networks; designed to replace the WEP and WPA protocols. Uses the AES standard instead of the RC4 stream cipher

C) TKIP-RC4: The extra layer of security that Wi-Fi Protected Access (WPA) adds on top of Wired Equivalent Privacy (WEP).

D) CCMP-AES: A 128-bit block cipher used in the IEEE 802.11i standard.

E) Authentication and authorization:

   a. EAP (Extensible Authentication Protocol): An extension to the PPP protocol suite that provides the framework for authenticating clients and servers. It does not perform encryption or authentication on its own, but rather works with other encryption and authentication schemes to verify the credentials of clients and servers.

   b. PEAP (Protected Extensible Authentication Protocol): Uses a password function based on MS-CHAPv2 with the addition of an encrypted TLS tunnel.

   c. EAP-FAST (EAP - Fast Authentication via Secure Tunneling): EAP Flexible authenticator via secure tunneling. Cisco's replacement for LEAP. Combo of MS-CHAP and RADIUS

   d. EAP-TLS (EAP-Transport Layer Security): EAP with Transport Layer Security. Use of a RADIUS server as well as mutual authentication, requiring certificates on both the server and every client.

   e. Shared or open:

      i. Shared: An optional Wired Encryption Privacy (WEP) authentication that uses challenge text for authentication.

      ii. Open: simple authentication request containing the station ID and an authentication response containing success or failure data. Any client can send its station ID in an attempt to associate with the AP. In effect, no authentication is actually done.

   f. Preshared key: An authentication protocol that uses a passphrase to generate the encryption key and must be created and entered into both the access point and all wireless devices prior to the devices communicating.

   g. MAC filtering: Prevents an access point from authenticating any device whose MAC address is not listed by the network administrator.

F) Geofencing: The use of GPS or RFID technology to create a virtual geographic boundary, enabling software to trigger a response when a mobile device enters or leaves a particular area.

4.4 SUMMARIZE COMMON NETWORKING ATTACKS.

A) DoS: Impact system availability by flooding the target system with traffic or requests or by exploiting a system or software flaw.
   a. Reflective: Uses an amplification network to increase the severity of the attack. Packets are sent to the amplification network addressed as coming from the target. The amplification network response back to the target system.
   b. Amplified: An attack instigated using small, simple requests that trigger very large responses from the target.
   c. Distributed: Multiple PCs attack a victim simultaneously and a series of computers scan target computers to find weaknesses and then compromise the most vulnerable systems.

B) Social engineering: An attack that exploits human nature by convincing someone to reveal information or perform an activity.

C) Insider threat: Someone who is inside the company who has intricate knowledge of the company and how its network works. They can pinpoint a specific vulnerability and may even have access to multiple parts of the network.

D) Logic bomb: Designed to execute only under predefined conditions and lies dormant until the predefined condition is met.

E) Rogue access point: An unauthorized WAP (Wireless Access Point) or Wireless Router that allows for attackers to bypass many of the network security configurations and opens the network and its users to attacks.

F) Evil twin: Has same SSID (Service Set Identifier) as a proper access point (AP). Once a user connects to it, all wireless traffic goes through it instead of the real AP.

G) War-driving: Driving around with a mobile device looking for open WAPs with which to communicate and looking for weak implementations that can be cracked. Warchalking marks a physical signal to notify others that the vulnerability is there.

H) Phishing: Sending a false email pretending to be legitimate to steal valuable information from the user.

I) Ransomware: Ransomware: Denies access to a computer system or data until a ransom is paid. Can be spread through a phishing email or unknowingly infected website.

J) DNS poisoning: Is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.

K) ARP poisoning: The act of falsifying the IP-to-MAC address resolution system employed by TCP/IP.

L) Spoofing: The real source of a transmission file or email is concealed or replaced with a fake source.

M) Deauthentication: An attack where an intruder sends a frame to the AP with a spoofed address to make it look like it came from the victim that disconnects the user from the network. This increases the chance of the user using another AP, a rogue one.

N) Brute force: A password-cracking program that tries every possible combination of characters through A to Z.

O) VLAN hopping: Attacking the host of a VLAN to gain access to the resources on other VLANs that are not supposed to be accessible.

P) Man-in-the-middle: The attacker alters the communication between two parties who believe they are directly communicating.

Q) Exploits vs. vulnerabilities:

  a. Exploits: Taking advantage of a vulnerability in order to gain control of a system or modify data.

  b. Vulnerabilities: Weaknesses in a system that sometimes are not even ever discovered.

4.5 GIVEN A SCENARIO, IMPLEMENT NETWORK DEVICE HARDENING.

A) Changing default credentials: Many routers come with a default "admin" account with "password" as the value.

B) Avoiding common passwords: Use complex passwords and different ones for each device. People typically use common words and phrases as their passwords. Add numbers and special characters to strengthen your passwords.

C) Upgrading firmware: This type of software needs to be updated due to security issues, bugs. Devices like BIOS on the motherboard, expansion boards, switches, routers and wireless access points. Test upgrade first before rolling them out to verify their compatibility with your machines to avoid problems.

D) Patching and updates: Same as securing firmware to secure issues but with software including OSs.

E) File hashing: Method used to verify integrity, confirming that the sent files are unaltered. Represents data as a short string of text. This is unique to a particular data structure. Different if the data changes.

F) Disabling unnecessary services: Close services and ports that are not in use as to not be exploited.

G) Using secure protocols: Protocols that help encrypt your information, examples like SSH, SSL, TLS, and etc.

H) Generating new keys: Use this when installing a used switch. Should be done regularly like password management.

I) Disabling unused ports:

  a. IP ports: Disable unused ports, if open could be a door for attackers to walk through.

  b. Device ports (physical and virtual): Use NAC to authenticate before you can communicate with the network when devices are plugged into the network.

4.6 EXPLAIN COMMON MITIGATION TECHNIQUES AND THEIR PURPOSES.

A) Signature management: Digital signatures are used to verify publishers and file integrity. PKI (Public Key Infrastructure) enables you to issue certificates to internal developers/contractors and enables any employee to verify the origin and integrity of downloaded applications.

B) Device hardening: No system is secure with the default configurations. You need some guidelines to keep everything safe. Hardening guides are specific to the software or platform.

Get feedback from the manufacturer or Internet interest group. Other general-purpose guides are available online

C) Change native VLAN: By default, native VLAN is set to port 1. The native VLAN is the only VLAN that is not tagged in a trunk.

D) Switch port protection:

   a. Spanning tree: Protocol that is used to help solve certain problems with switches. Enables bridges/switch interfaces to be assigned a value that is then used to control the learning process.

   b. Flood guard: Used to look for and prevent malicious traffic from bringing the switch to a halt (ex. DoS, DDoS). Can be purchased as a standalone device or as part of another.

   c. BPDU (Bridge Protocol Data Unit) guard: This prevents looping on a switch. Protects the spanning tree domain from external influence when moving a nontrunking port into an error state when a BPDU is received on that port. The guard shuts down interfaces that receive BPDUs instead of putting them into the spanning tree blocking state.

      i. BPDU (Bridge Protocol Data Unit): Are frames that contain information about the spanning tree protocol.

   d. Root guard: Similar to BPDU guards in that it is also used to prevent malicious exploitation of BPDU packets. Used to prevent another switch from becoming the BPDU superior. Needed when you connect a network that you manage to one that you do not.

   e. DHCP snooping: The capability for a switch to look at packets and drop DHCP traffic that it determines to be unacceptable based on the defined rules. Prevents rogue DHCP servers from offering IP addresses to DHCP clients.

E) Network segmentation:

   a. DMZ (Demilitarized Zone): Part of a network where you place servers that must be accessible by sources both outside and inside your network. Gives firewall configuration an extra level of flexibility, protection, and complexity.

   b. VLAN: Use this method to isolate busy load systems or certain protocols for better network performance.

F) Privileged user account: Monitor all types of this account as well as apply more protection to them than to any other accounts. Limit elevated permission uses only when needed.

G) File integrity monitoring: Using checksums and file integrity systems to monitor your files and make certain the ones you are backing up are unchanged and complete.

H) Role separation: Reduces risk of fraud and to prevent other losses in an organization such as embezzlement or collusion. Not one user is able to do everything.

I) Restricting access via ACLs: Method used to control who can access resources, if permission is not granted then it is set automatically as denied.

J) Honeypot/honeynet:

   a. Honeypot: A trap that allows intruders in the network but does not allow access to sensitive data.

   b. Honeynet: An entire network setup to monitor attacks from outsiders. Traffic monitored in/out. Helps isolate attacks and manage security risks.

K) Penetration testing: Finding flaws in a systems security, using the same attacks as hackers.

5.0 NETWORK TROUBLESHOOTING AND TOOLS

5.1 EXPLAIN THE NETWORK TROUBLESHOOTING METHODOLOGY.

A) Identify the problem: Effective troubleshooting begins with a clear problem definition.
   a. Gather information.
   b. Duplicate the problem, if possible.
   c. Question users.
   d. Identify symptoms.
   e. Determine if anything has changed.
   f. Approach multiple problems individually.

B) Establish a theory of probable cause: This is the point in the troubleshooting process where your experience and intuition can be extremely helpful because you are now going to brainstorm a list of possible causes.
   a. Question the obvious.
   b. Consider multiple approaches.
      i. Top-to-bottom/bottom-to-top.
      ii. OSI model.
      iii. Divide and conquer.

C) Test the theory to determine the cause: Before taking action on what you consider to be the most likely cause of a problem, do a sanity check on your theory.
   a. Once the theory is confirmed, determine the next steps to resolve the problem.
   b. If the theory is not confirmed, reestablish a new theory or escalate.

D) Establish a plan of action to resolve the problem and identify potential effects: You may determine that you could fix the problem right away, but doing so might require excessive network down-time. Down-time costs organizations money and is usually unacceptable.

E) Implement the solution or escalate as necessary: Once done, don't automatically assume that the system will work properly. You should implement a series of tests to verify full system functionality.

F) Verify full system functionality and, if applicable, implement preventive measures.

G) Document findings, actions, and outcomes.

5.2 GIVEN A SCENARIO, USE THE APPROPRIATE TOOL.

A) Hardware tools:

   a. Crimper: Used to attach a connector (for example, an RJ-45 connector) to the end of an unshielded twisted-pair (UTP) cable.
   b. Cable tester: Verifies if a cable to transmit a signal and if the wire mapping is correct.
   c. Punchdown tool: A specialized tool for connecting UTP wires to a 66 or 110-block.
   d. OTDR (Optical Time Domain Reflectometer): Detects the location of a fault in a fiber cable by sending light down the fiber-optic cable and measuring the time required for the light to bounce back from the cable fault.
   e. Light meter: Used to measure the amount of loss of light within a fiber connection.
   f. Tone generator: An electronic device that sends an electrical signal through one set of UTP cables. Used to locate a particular cable.
   g. Loopback adapter: Used to test the send and receive capability of a NIC card.
   h. Multimeter: A measuring instrument for current, voltage, and resistance.
   i. Spectrum analyzer: A tool used to locate and document wireless connections in an area. Used to diagnose network issues for 2.4 GHz and 5 GHz connections.

B) Software tools:

   a. Packet sniffer: Software or hardware used to collect data travelling over a network.
   b. Port scanner: Software to search a system for any port vulnerabilities.
   c. Protocol analyzer: Hardware or software that captures packets to decode and analyze their contents.
   d. Wi-Fi analyzer: Tool for checking/diagnosing issues on a wireless network.
   e. Bandwidth speed tester: Method of measuring traffic flow on a network.
   f. Command line:
      i. ping: Simple command used to see if a device is reachable.
      ii. tracert, traceroute: Used to trace all of the routers between two end-points to troubleshoot.
      iii. nslookup: A utility that is used to test and troubleshoot DNS.
      iv. ipconfig: Command used to display a computer's IP settings.
      v. ifconfig: Mac/Linux equivalent of ipconfig.
      vi. iptables: Allow a system administrator to alter the Linux kernel firewall.
      vii. netstat: Prints out all running IP processes running on a system.
      viii. tcpdump: Command-line method of analyzing packet traffic.
      ix. pathping: Combination of tracert and ping.
      x. nmap: Tool for checking ports on a system. You may use it to check for port vulnerabilities.
      xi. route: Allows you to modify a machine's routing table
      xii. arp: Displays the table of IP addresses and the Mac addresses.
      xiii. dig: Mac/Linux equivalent of nslookup.

5.3 GIVEN A SCENARIO, TROUBLESHOOT COMMON WIRED CONNECTIVITY AND PERFORMANCE ISSUES.

A) Attenuation: Loss of power in a signal as it travels from the sending device to the receiving device.

B) Latency: Is the measurement of time for data traveling from the source host to the destination host. Latency for network connections is measured in millionths of a second, called milliseconds.

C) Jitter: A delay in completing a transmission of all the frames in a message; caused by excessive machines on a network.

D) Crosstalk: Occurs when a signal travels no on one wire or cable infringes on the signal traveling over an adjacent wire or cable.

E) EMI (Electromagnetic Interference): A type of interference that may be caused by motors, power lines, televisions, copiers, fluorescent lights, or other sources of electrical activity.

F) Open/short:

   a. Open: One end of the cable doesn't connect. Diagnose cable, if bad then replace.

   b. Short: One or more of the wires in a cable connect to another wire in the cable. If bad then replace.

G) Incorrect pin-out: The twisted pair wires are not all correctly aligned on both ends of the cable. Use a cable tester to verify that that was the issue with the cable.

H) Incorrect cable type: The Ethernet cabling used to connect to the network are all rated according to the specification they support. It is important to look at the cable sheath for the specification it supports. A Cat5 cable on a Cat 6 network will not perform as expected.

I) Bad port: When diagnosing a connection issue, always check the network adapter for the connection LED status indicators, technicians can use a loopback plug to diagnose a bad port or failed adapter. It is possible that the port has bent pins creating intermittent connections or no connection at all.

J) Transceiver mismatch: Is not common with Ethernet transceivers because most transceivers auto-negotiate speed and duplex. Most 10 Gbps transceivers are not backward compatible with lower data rates, and some 1 Gbps transceivers are not compatible with lower data rates as well.

K) TX/RX reverse: Is when Transmit and the Receive pairs of a cable are inverted so the TX sides are connected to each other and the RX sides are connected to each other (as opposed to the correct way of connecting TX to RX).

L) Duplex/speed mismatch: When two devices connected by Ethernet do not properly negotiate their connection.

   a. Duplex: Duplex mismatch occurs when the two communicating Ethernet devices end up with duplex settings that are not the same, either because of manual settings or the auto-negotiation process. Two devices with a duplex mismatch will communicate.

   b. Speed: the two devices with a speed mismatch will communicate

M) Damaged cables: Cables that are run through walls or overhead are not usually subject to damage. However, you will find some cabling run under a floor mat or rug. This subjects the cable to foot traffic that can eventually damage the cable. Some cables can be pinched between the desk and a wall which will cause damage over time.

N) Bent pins: Over time these can wear down from use. The connectors get bent over time. Try plugging into another device to see if it is still an issue

O) Bottlenecks: Often occur when network traffic or a process slows down at a specific point. The specific point will not have the same capacity as the network traffic or process and is restricted in some way.

P) VLAN mismatch: A switch will be configured to support one preconfigured default VLAN containing all switch ports which cannot be renamed or deleted and additional native VLAN(s) that should be renamed for security. When configuring native VLANS remember that both ends must match the VLAN assignment or a VLAN mismatch will occur.

Q) Network connection LED status indicators:

5.4 GIVEN A SCENARIO, TROUBLESHOOT COMMON WIRELESS CONNECTIVITY AND PERFORMANCE ISSUES.

A) Reflection: Is when a wireless signal bounces off an object and weakens the signal. To prevent this, remove any metal materials that could be causing it.

B) Refraction: Is when a signal passes through an object and exists at a different angle. The presence of glass or water (especially during weather) can cause this.

C) Absorption: Is when a signal passes through an object and loses some of the signal as it passes through. Things like walls and ceilings can absorb the signal.

D) Latency: The delay between the transmission of a signal and its recipient.

E) Jitter: Variations of latency over a given time.

F) Attenuation: Is the loss of signal from an access point to a receiving device. You can fix this by boosting the signal strength on the access point or by moving closer to the AP.

G) Incorrect antenna type: Omnidirectional antennas are best used on ceilings to service a single building. Directional antennas are best used to connect to buildings together

H) Interference: Is when something else is trying to use the same frequency. Examples of devices that can cause interference: cordless phones, microwave ovens, and fluorescent lights.

I) Incorrect antenna placement: Antennas too close will cause overlapping, too far apart will cause slow throughput.

J) Channel overlap: Is when multiple channels share the frequency band causing interference and performance degradation for devices operating on channels that are too close to each other.

K) Overcapacity: With wireless networks there's only so much capacity available. Only so many devices can be communicating over these very narrow frequency ranges that we have for wireless networks. If you have too many devices on the same wireless network, the network performance will begin to degrade.

L) Distance limitations: If the distance limitations for a given network media are exceeded, transmissions over that media are degraded to the point where the receiving device is unable to properly interpret the transmission.

M) Frequency mismatch: Devices must match the access point. Verify the client is communicating over the correct channel. This is normally done automatically and may cause issues if done manually.

N) Wrong SSID (Security Set Identifier): When configuring a wireless client, you must be sure that you are accessing the correct SSID. The SSID will not be visible unless it is broadcasted.

O) Wrong passphrase: Once you have the correct configuration you can attempt to connect. Your next challenge is using the correct Password/passphrase for authentication. A wrong passphrase will be denied.

P) Security type mismatch: Wireless signals are transmitted openly making them subject to interception. The signals are encrypted to secure communications. Early encryption types like WEP and WPA are insecure and your network should use at least WPA2. If the client security is set to something other than that of the access point it will not connect to the network.

Q) Power levels: If the power level is too low, mobile devices further away may not receive a signal. On some access points, radio power can be increased to expand the coverage area. In situations where your signals reach outside the intended area, you can decrease the radio power.

R) Signal-to-noise ratio: Devices in your networking environment produce EMI. The aggregate of this EMI is the noise floor. If your signal is too close to the noise floor you risk corrupted data and the retransmissions created by this corruption.

5.5 GIVEN A SCENARIO, TROUBLESHOOT COMMON NETWORK SERVICE ISSUES.

A) Names not resolving: When you have an issue where a statically configured client cannot access the internet try to ping a publicly available resource like google.com by its IP address 8.8.8.8. If you can connect to the server with the IP address try its URL (www.whatyouaretrying.com). If the resource cannot be located by its domain name, you should check the static DNS settings for misconfiguration.

B) Incorrect gateway: Your gateway directly affects internet connectivity. Using the incorrect gateway will limit your connections to the local network.

C) Incorrect netmask: A computer's netmask identifies the number of bits of its IP address that are assigned to the network and those bits assigned to the host. An incorrect configuration will result in limited connectivity or no connectivity at all.

D) Duplicate IP addresses: No two devices can have the same IP address on public or private networks. Address duplication is prevented by using DHCP. When an address is static it is possible to assign the same IP configuration to two devices.

E) Duplicate MAC addresses: The hardware address of your interface is assigned by the manufacturer and is unique. Duplicate MAC addresses will not communicate on a LAN. This address can be changed and possibly misconfigured manually through software.

F) Expired IP address: Your device using DHCP negotiates a lease for an IP address from the DHCP server. The lease time is set by the administrator. The lease times should be tailored to your usage. The lease lengths should be long enough to support your usage without causing an exhausted DHCP scope.

G) Rogue DHCP server: Unusual internet/internetwork traffic should be reported immediately. This misdirection can be attributed to a rogue DHCP server. The rogue server can provide compromised DHCP settings and can use these settings to further compromise your network.

H) Untrusted SSL certificate: SSL certificates must be maintained and accurate. An SSL certificate can become untrusted in several ways. It can expire. It could be using an incorrect date or time. It can also be revoked for a mismatch between the server name on the certificate and the actual server. These issues can be significantly reduced by not allowing self-signed certificates (certificates signed by the user).

I) Incorrect time: Device time synchronization is supported by the NTP protocol on your network. NTP servers can be on your local network or the internet. In the absence of a reliable NTP server, the device's internal clock is used. The internal clock is powered by the CMOS battery which could be the source of the problem.

J) Exhausted DHCP scope: Is when a DHCP scope has run out of addresses to lease. If possible add more IP addresses to the address pool. IPAM (IP Address Management) will help monitor and report IP address shortages.

K) Blocked TCP/UDP ports: Cause necessary applications to not work or slow down. Could be caused by a Firewall or ACL configuration. Confirm the issue with a packet capture. If you receive no response to requests, run a TCP- or UDP-based traceroute tool to see how far the packets go.

L) Incorrect host-based firewall settings: Cause necessary applications to not work or not be accessible. Based on the application in use and not necessarily the protocol and port. Check the host-based firewall settings.

M) Incorrect ACL settings: Causes only certain IP addresses accessible or all IP addresses to be blocked. Confirm with packet captures and TCP/UDP traceroutes to identify the point of no return.

N) Unresponsive service: Is when there is no response to an application request. Ensure that it is the correct application, port, and protocol (TCP/UDP). When there is an unresponsive service, an administrator who can respond/resolve may need to be contacted.

O) Hardware failure: To properly diagnose a hardware failure, follow the best practices for troubleshooting. Once a failed device is identified it should be replaced. All critical devices should have failover capabilities or a compatible and preconfigured hardware replacement.