New Category: Networking Fundamentals	**New Category: Networking Fundamentals**
OSI Model	Physical Data link Network Transport Session Presentation Application
Ethernet header	The header added to data frames in Ethernet networks, containing source and destination MAC addresses and other control information.

Internet Protocol (IP) header	The header added to IP packets containing source and destination IP addresses and other control information.
Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) headers	Headers added to TCP/UDP segments containing port numbers and other control information.
TCP flags	These are control bits within the TCP header that determine the status of a TCP connection or specific communication options.

Payload	It refers to the actual data being transmitted within a packet or frame. The payload does not include the headers or control information.
Maximum transmission unit (MTU)	MTU is the largest size of a packet or frame that can be transmitted over a network without being fragmented into smaller units.
Mesh	A network topology where every device is connected to every other device, providing redundancy and multiple paths for data transmission.

Star/hub-and-spoke	A network topology where all devices are connected to a central hub or switch, which manages the data flow between them.
Bus	A network topology where all devices are connected to a single communication line, and data is transmitted in both directions.
Ring	A network topology where devices are connected in a circular fashion, and data travels in a unidirectional loop.

Hybrid	A combination of two or more network topologies, allowing for more flexible and scalable network designs.
Peer-to-peer	A network model where devices can communicate directly with each other without relying on a central server.
Client-server	A network model where clients (devices) request services or resources from a central server that fulfills these requests.

Local area network (LAN)	A network that covers a small geographic area, typically within a single building or campus.
Metropolitan area network (MAN)	A network that spans a larger area than a LAN, usually covering a city or metropolitan area.
Wide area network (WAN)	A network that extends over a large geographical area, connecting LANs and MANs over long distances.

Wireless local area network (WLAN)	A LAN that uses wireless communication to connect devices.
Personal area network (PAN)	A network designed for communication between personal devices in close proximity, such as Bluetooth connections.
Campus area network (CAN)	A network that interconnects LANs within a specific geographical area, like a university campus.

Storage area network (SAN)	A specialized network that provides access to shared storage devices, enabling high-speed data storage and retrieval.
Software-defined wide area network (SDWAN)	A network architecture that uses software-defined techniques to manage and optimize WAN connections.
Multiprotocol label switching (MPLS)	A routing technique that uses labels to direct data packets along predefined paths, improving network performance and efficienc.

Multipoint generic routing encapsulation (mGRE)	A tunneling protocol used to enable communication between multiple endpoints over an IP network.
Demarcation point	The physical point where a service provider's network ends and the customer's network begins, typically located at the customer premises.
Smartjack	A device used at the demarcation point to monitor and diagnose the connection between the service provider and the customer's network.

vSwitch	A virtual switch used in virtualized environments to manage network traffic between virtual machines (VMs) on the same host.
Virtual network interface card (vNIC)	A software-based network interface used by virtual machines to communicate with the network.
Network function virtualization (NFV)	The process of virtualizing network services that were traditionally performed by dedicated hardware devices.

Hypervisor	Software that enables the virtualization of physical hardware, allowing multiple operating systems and applications to run on the same physical server.
Satellite	A communication technology that uses orbiting satellites to transmit and receive signals for various applications, such as internet connectivity, broadcasting, and remote communication.
Digital subscriber line (DSL)	A technology that provides high-speed internet access over traditional copper telephone lines, offering faster speeds than dial-up connections.

Cable	A type of broadband internet connection that utilizes coaxial cables to transmit data, commonly provided by cable television companies.
Leased line	A dedicated point-to-point connection between two locations, leased from a telecommunications provider, offering high reliability and performance.
Metro-optical	Optical fiber networks designed for metropolitan areas, providing high-speed data transmission over short distances.

Twisted pair	A type of cabling in which pairs of wires are twisted together to reduce interference and crosstalk, commonly used in Ethernet connections.
Cat 5, Cat 5e, Cat 6, Cat 6a, Cat 7, Cat 8	Categories of twisted-pair Ethernet cables, each providing different data transmission speeds and capabilities.
Coaxial/RG-6	Coaxial cables, often referred to as RG-6, used for television and internet connections.

Twinaxial	A type of cabling that consists of two coaxial cables with a shared shield, commonly used in high-speed data transmission.
Termination standards	Guidelines and specifications for terminating cables in a consistent and standardized manner to ensure proper connectivity.
TIA/EIA-568A, TIA/EIA-568B	Two wiring schemes used for terminating twisted-pair cables, defining the order of wire connections.

Single-mode	A type of optical fiber that allows a single mode of light to propagate, enabling long-distance communication with high bandwidth.
Multimode	A type of optical fiber that supports multiple modes of light, suitable for shorter distances with lower bandwidth requirements.
Local connector (LC), Straight tip (ST), Subscriber connector (SC), Mechanical transfer (MT), Registered jack (RJ), Angled physical contact (APC), Ultra-physical contact (UPC)	Various types of fiber optic connectors used for terminating and connecting optical fibers.

RJ11 - RJ45	Standardized connectors used for telecommunication, with RJ11 commonly used for telephone connections and RJ45 for Ethernet connections.
F-type connector	A coaxial connector used for cable television and internet connections.
Transceivers/media converters	Devices used to convert signals between different types of media or interfaces, such as fiber optic to Ethernet.

Transceiver type	Specific models and specifications of transceivers used in networking equipment.
Small form-factor pluggable (SFP), Enhanced form-factor pluggable (SFP+), Quad small form-factor pluggable (QSFP), Enhanced quad small form-factor pluggable (QSFP+)	Types of transceiver modules used in high-speed data transmission.
Patch panel/patch bay	A device used to terminate and organize multiple network cables, facilitating easy connectivity and management.

Fiber distribution panel	A panel used for organizing and distributing fiber optic connections in data centers or telecommunication rooms.
66 Punchdown block, 110 Punchdown block, Krone Punchdown block, Bix Punchdown block	Different types of punchdown blocks used for terminating twisted-pair cables.
10BASE-T Ethernet Standard, 100BASE-TX Ethernet Standard, 1000BASE-T Ethernet Standard, 10GBASE-T Ethernet Standard, 40GBASE-T Ethernet Standard	Different Ethernet standards specifying data transmission speeds over twisted-pair cables.

100BASE-FX Fiber Standard, 100BASE-SX Fiber Standard, 1000BASE-SX Fiber Standard, 1000BASE-LX Fiber Standard, 10GBASE-SR Fiber Standard, 10GBASE-LR Fiber Standard	Different Ethernet standards specifying data transmission speeds over fiber optic cables.
Coarse wavelength division multiplexing (CWDM), Dense wavelength division multiplexing (DWDM), Bidirectional wavelength division multiplexing (WDM)	Technologies used in optical networking to combine multiple signals onto a single fiber.
Dense wavelength division multiplexing (DWDM)	A technology used in optical networks to combine multiple data streams at different wavelengths onto a single optical fiber, increasing the capacity and efficiency of the network.

Bidirectional wavelength division multiplexing (WDM)	A variant of WDM that allows for bidirectional transmission over a single optical fiber by using different wavelengths for upstream and downstream data.
RFC1918	A set of reserved IP address ranges specified in Request for Comments (RFC) 1918, which are used for private networks and should not be routed on the public internet.
Network address translation (NAT)	A technique that allows multiple devices on a private network to share a single public IP address for internet communication.

Port address translation (PAT)	A form of NAT that maps multiple private IP addresses to a single public IP address using different port numbers.
Automatic Private IP Addressing (APIPA)	A feature in some operating systems that automatically assigns a unique IP address to a device on a local network in the absence of a DHCP server.
Extended unique identifier (EUI-64)	A method for generating IPv6 interface identifiers based on the MAC address of a network interface.

Multicast	A method of data transmission where a single packet is sent to multiple recipients simultaneously.
Unicast	A method of data transmission where a packet is sent from a source to a single destination.
Anycast	A method of data transmission where a packet is sent to the nearest available destination from a group of potential recipients.

Broadcast	A method of data transmission where a packet is sent to all devices on a network.
Link local	A type of IP address used for communication within a single network segment, typically not routed on the internet.
Loopback	A virtual network interface that allows a device to send data to itself.

Default gateway	The IP address of the router that devices use to access other networks or the internet.
Classless (variable-length subnet mask)	A subnetting method that allows the division of IP address space into smaller, variable-sized subnets.
Classful Subnet - A - B - C - D – E	The original addressing scheme of IP addresses, divided into different classes based on the size of the network.

Classless Inter-Domain Routing (CIDR) notation	A method of representing IP addresses and their associated subnet masks in a compact form.
Tunneling	Encapsulating one protocol within another for transmission over a network.
Dual stack	A networking configuration that allows a device to support both IPv4 and IPv6 protocols simultaneously.

Shorthand notation	A compact representation of an IPv6 address, omitting leading zeros and using "::" to represent groups of zeros.
Router advertisement	Messages sent by routers to inform devices of their presence and provide network configuration information.
Stateless address autoconfiguration (SLAAC)	A method in IPv6 where devices automatically configure their IP addresses without the need for a DHCP server.

Virtual IP (VIP)	An IP address that is not associated with a specific physical network interface but is instead mapped to multiple real IP addresses.
Subinterfaces	Virtual network interfaces created on a physical interface, allowing a single physical interface to be logically divided into multiple segments.
File Transfer Protocol (FTP)	A standard network protocol used to transfer files from one host to another over a TCP-based network, such as the internet.

Secure Shell (SSH)	A cryptographic network protocol used for secure remote login and encrypted data communication over an unsecured network.
Secure File Transfer Protocol (SFTP)	A secure extension of FTP that allows for secure file transfers over SSH.
Telnet	A network protocol used to provide remote access to a command-line interface on a remote host.

Simple Mail Transfer Protocol (SMTP)	A protocol used for sending and receiving email messages between email servers.
Domain Name System (DNS)	A system that translates domain names (e.g., www.example.com) into IP addresses, enabling users to access websites using easy-to-remember names.
Dynamic Host Configuration Protocol (DHCP)	A network protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network.

Trivial File Transfer Protocol (TFTP)	A simplified version of FTP, commonly used for basic file transfer tasks.
Hypertext Transfer Protocol (HTTP)	The protocol used for communication between web browsers and web servers, enabling the retrieval of web pages and resources.
Post Office Protocol v3 (POP3)	A protocol used for retrieving email messages from a mail server to a local email client.

Network Time Protocol (NTP)	A protocol used to synchronize the clocks of devices on a network to a reference time source.
Internet Message Access Protocol (IMAP)	A protocol used for accessing and managing email messages on a remote mail server.
Simple Network Management Protocol (SNMP)	A protocol used to manage and monitor network devices and their performance.

Lightweight Directory Access Protocol (LDAP)	A protocol used to access and manage directory information services, commonly used for user authentication and authorization.
Hypertext Transfer Protocol Secure (HTTPS) [Secure Sockets Layer (SSL)]	A secure version of HTTP that encrypts data transmitted between a web browser and web server.
HTTPS [Transport Layer Security (TLS)]	Another name for HTTPS, indicating the use of TLS for securing web communications.

Server Message Block (SMB)	A network file-sharing protocol used for sharing files, printers, and other resources between devices on a network.
Syslog	A standard protocol used for sending log messages from network devices to a centralized log server for monitoring and troubleshooting.
SMTP TLS	The use of TLS to encrypt email communication between email servers.

Lightweight Directory Access Protocol (over SSL) (LDAPS)	LDAP communication secured with SSL/TLS encryption.
IMAP over SSL	IMAP communication secured with SSL/TLS encryption.
POP3 over SSL	POP3 communication secured with SSL/TLS encryption.

Structured Query Language (SQL) Server	A relational database management system that uses SQL for managing and querying databases.
SQLnet	Oracle's networking protocol used for client-server communication in Oracle databases.
MySQL	An open-source relational database management system that uses SQL for managing databases.

Remote Desktop Protocol (RDP)	A protocol that allows remote access to a desktop environment on a remote server.
Session Initiation Protocol (SIP)	A signaling protocol used for initiating, maintaining, and terminating multimedia communication sessions, such as VoIP calls.
Internet Control Message Protocol (ICMP)	A network protocol used for diagnostics and error reporting in IP networks.

TCP	Transmission Control Protocol, a connection-oriented protocol that ensures reliable data delivery.
UDP	User Datagram Protocol, a connectionless protocol that provides faster but less reliable data delivery.
Generic Routing Encapsulation (GRE)	A tunneling protocol used to encapsulate packets within IP packets for transmission over a network.

Internet Protocol Security (IPSec)	A suite of protocols used to secure communication over IP networks through encryption and authentication.
Authentication Header (AH)/Encapsulating Security Payload (ESP)	Protocols used in IPSec to provide authentication, data integrity, and encryption.
Connectionless vs. connection-oriented	Refers to the communication behavior of protocols; connectionless protocols like UDP do not establish a connection before sending data, while connection-oriented protocols like TCP establish a connection before

DHCP relay	A device that forwards DHCP messages between devices in different network segments.
IP helper/UDP forwarding	A feature that allows routers to forward specific types of UDP traffic, like DHCP requests, to a designated IP address.
DNS A Address Record	A DNS record that maps a domain name to an IPv4 address.

DNS AAAA Address Record	A DNS record that maps a domain name to an IPv6 address.
DNS Canonical name (CNAME Record)	A DNS record that provides an alias or canonical name for a domain.
DNS Mail exchange (MX Record)	A DNS record that specifies the mail server responsible for receiving email messages for a domain.

DNS Start of authority (SOA Record)	A DNS record that indicates the primary DNS server for a domain and its various properties.
DNS Pointer (PTR Record)	A DNS record used for reverse DNS lookups, mapping an IP address to a domain name.
DNS Text (TXT Record)	A DNS record that holds arbitrary text information for a domain.

DNS Service (SRV Record)	A DNS record used to define the location of specific network services within a domain.
DNS Name server (NS Record)	A DNS record that identifies the authoritative name servers for a domain.
Global hierarchy	The hierarchical structure of DNS servers responsible for different top-level domains.

Root DNS servers	The highest level of DNS servers that store information about the root zone and direct queries to the appropriate top-level domain servers.
Internal vs. external DNS	Refers to DNS servers used for resolving names within an organization (internal) and those used for resolving public domain names (external).
Zone transfers	The process of transferring DNS data from one DNS server to another to keep zone information synchronized.

Authoritative name servers	DNS servers that hold the definitive DNS information for a specific domain.
Time to live (TTL)	The time duration for which DNS information is considered valid before it needs to be refreshed.
DNS caching	The practice of temporarily storing DNS records in a cache to reduce response times and network traffic.

Reverse DNS/reverse lookup/forward lookup	The process of looking up a domain name based on its IP address (reverse DNS) or looking up an IP address based on its domain name (forward lookup).
Recursive lookup/iterative lookup	The process of resolving a domain name by recursively querying DNS servers until the authoritative name server is found (recursive lookup) or querying each DNS server in sequence until the answer is obtained (iterative lookup).
NTP Stratum	A hierarchical level of NTP servers indicating their proximity to a reliable time source.

NTP Clients	Devices that synchronize their clocks with NTP servers.
NTP Servers	Devices that provide accurate time information to NTP clients.
Datacenter Core Layer	The central layer of a datacenter network responsible for high-speed data transfer between core devices.

Datacenter Distribution / Aggregation Layer	The layer that aggregates connections from access layer switches and connects to the core layer in a datacenter network.
Datacenter Access / Edge Layer	The layer that connects end-user devices and servers to the distribution layer in a datacenter network.
Software Defined Networking Application Layer	The layer in an SDN architecture that hosts applications and services for network management.

Software Defined Networking Control Layer	The layer in an SDN architecture that controls the behavior of network devices and routes traffic.
Software Defined Networking Infrastructure Layer	The layer in an SDN architecture that includes the physical network devices.
Software Defined Networking Management Plane	The plane in an SDN architecture that provides management and monitoring capabilities for the SDN controller and network devices.

Spine and Leaf Datacenter Architecture	A datacenter network design that uses a spine of high-speed switches interconnected with leaf switches, providing a scalable and efficient fabric for datacenter traffic.
Software Defined Network	A network architecture that separates the control plane from the data plane, enabling centralized control and programmability of network devices.
Top-of-rack switching	A network design where each rack of servers connects directly to a switch at the top of the rack.

Network backbone	The central high-speed network that connects multiple networks and serves as the primary route for data traffic.
East to West Network Traffic	Data traffic flowing horizontally between servers or devices within a datacenter.
North to South Network Traffic	Data traffic flowing vertically between different layers of the network, such as from end-user devices to servers in a datacenter.

Branch Office Datacenter	A datacenter located in a branch office, typically serving local needs.
On-Premises Datacenter	A datacenter located within an organization's physical premises and managed internally.
Colocation Datacenter	A datacenter facility where multiple organizations can rent space for their servers and network equipment.

Storage Area Networks	Specialized networks dedicated to providing high-speed access to shared storage resources.
Connection types	Different ways of connecting devices and networks, such as Ethernet, Fibre Channel, and iSCSI.
Fibre Channel over Ethernet (FCoE)	A protocol that encapsulates Fibre Channel frames over Ethernet networks, allowing convergence of storage and data networks.

Fibre Channel	A high-speed network technology used for connecting servers and storage devices in a storage area network (SAN).
Internet Small Computer Systems Interface (iSCSI)	A protocol that allows SCSI commands to be transmitted over IP networks, enabling remote storage access.
Public	A type of cloud computing service provided by third-party providers and accessible over the internet.

Private	A type of cloud computing service dedicated to a single organization and hosted on-premises or by a third-party provider.
Hybrid	A cloud computing environment that combines both public and private clouds, allowing data and applications to move between them.
Community	A type of cloud computing service shared by multiple organizations with shared interests or requirements.

Software as a service (SaaS)	A cloud computing service model where software applications are delivered over the internet.
Infrastructure as a service (IaaS)	A cloud computing service model that provides virtualized computing resources over the internet.
Platform as a service (PaaS)	A cloud computing service model that provides a platform for developing, running, and managing applications over the internet.

Desktop as a service (DaaS)	A cloud computing service model that delivers virtual desktops over the internet.
Infrastructure as Code	The practice of managing and provisioning infrastructure using code and automation tools.
Automation/orchestration	The use of automated tools to manage and control IT processes and workflows.

Virtual private network (VPN)	A secure connection that allows remote users to access a private network over a public network, typically the internet.
Private-direct connection to cloud provider	A dedicated, private network connection between an organization's on-premises network and a cloud provider's datacenter.
Multitenancy	A cloud computing architecture where multiple users or organizations share the same computing resources.

Elasticity	The ability of a cloud service to scale resources up or down dynamically based on demand.
Scalability	The ability of a system to handle increasing workloads by adding resources or nodes.
Security implications	The potential security risks and considerations associated with implementing certain technologies or practices in a network or system.

New Category: Network Implementations	**New Category: Network Implementations**
Layer 2 switch	A network switch that operates at the data link layer (Layer 2) of the OSI model. It uses MAC addresses to forward data between devices within a local network.
Layer 3 capable switch	A network switch that can perform routing functions in addition to its switching capabilities. It operates at both Layer 2 and Layer 3 of the OSI model, allowing it to make forwarding decisions based on IP addresses as

Router	A network device that connects different networks and directs traffic between them based on IP addresses. Routers determine the optimal path for data to travel from the source to the destination across the
Hub	An older network device that operates at the physical layer (Layer 1) of the OSI model. It is a simple device that receives data from one device and broadcasts it to all other devices connected to it. Hubs are inefficient and have
Access point	A device that enables wireless devices to connect to a wired network. It acts as a bridge between wireless clients and the wired infrastructure, allowing devices to access network resources and the internet

Bridge	A device that connects two or more network segments and forwards traffic between them based on MAC addresses. It operates at the data link layer (Layer 2) and can be used to extend network coverage or segment traffic.
Wireless LAN controller	A device used to manage multiple access points in a wireless network. It centralizes configuration, security, and management tasks for all connected access points.
Load balancer	A device or software that distributes network traffic across multiple servers or resources to ensure efficient utilization and prevent overloading on a single resource.

Proxy server	An intermediary server that acts on behalf of clients to request resources from other servers. It enhances security, performance, and privacy by providing an additional layer of separation between clients and servers.
Cable modem	A device that modulates and demodulates digital data to allow internet access over cable television lines.
DSL modem	A device that connects to a digital subscriber line (DSL) service to provide internet access over telephone lines.

Repeater	A device used to extend the range of a network by amplifying and retransmitting signals between network segments.
Voice gateway	A device that converts voice traffic between traditional telephony systems and IP-based networks, allowing VoIP communication.
Media converter	A device that converts network signals between different media types, such as copper to fiber optic.

Intrusion prevention system (IPS)	A security device or software that monitors network traffic for malicious activity and takes proactive measures to prevent security breaches.
Intrusion detection system (IDS) device	A security device or software that monitors network traffic for signs of suspicious or unauthorized activity and generates alerts for further investigation.
Firewall	A network security device or software that filters and controls incoming and outgoing network traffic based on predefined security rules.

VPN headend	The main endpoint of a Virtual Private Network (VPN) where encrypted tunnels are established and network traffic is secured between remote locations and the central network.
Voice over Internet Protocol (VoIP) phone	A phone that uses internet protocols to transmit voice communication over an IP network, such as the internet or a private network.
Printer	A peripheral device that produces physical copies of digital documents and images.

Physical access control devices	Devices used to control and restrict access to physical locations, such as card readers, biometric scanners, and electronic locks.
Cameras	Devices used to capture images or videos for surveillance, security, or other purposes.
Heating, ventilation, and air conditioning (HVAC) sensors	Sensors used to monitor and control environmental conditions in buildings for heating, cooling, and air quality.

Internet of Things (IoT)	A network of interconnected devices and objects that can collect, exchange, and act upon data through embedded sensors and communication technologies.
Industrial control systems/ supervisory control and data acquisition (SCADA)	Systems used to control and monitor industrial processes and critical infrastructure, such as power plants and manufacturing facilities.
Dynamic routing	A routing technique where routers use protocols to dynamically exchange information and adapt to changes in network topology.

Routing Internet Protocol (RIP)	A distance vector routing protocol used to determine the best path for data packets in smaller networks.
Open Shortest Path First (OSPF)	A link-state routing protocol used to determine the best path for data packets in larger networks.
Enhanced Interior Gateway Routing Protocol (EIGRP)	A hybrid routing protocol that combines features of both distance vector and link-state protocols.

Border Gateway Protocol (BGP)	A routing protocol used to exchange routing information between different autonomous systems on the internet.
Link state	A type of routing protocol where routers exchange information about their directly connected links to build a detailed network map.
Distance vector	A type of routing protocol where routers exchange information about the distance and direction to destination networks.

Hybrid routing	A type of routing protocol that combines features of both link-state and distance vector protocols.
Static routing	A routing technique where network administrators manually configure the routing table with fixed paths for data packets.
Default route	A preconfigured route used by a router when it doesn't have a specific route for a destination network.

Administrative distance	A metric used in routers to determine the preference of one routing protocol over another when multiple protocols provide paths to the same destination.
Exterior vs. interior	Exterior routing protocols are used to exchange routing information between autonomous systems, while interior routing protocols are used within a single autonomous system.
Time to live	A field in IP packets that limits the time a packet can remain in the network before being discarded to prevent infinite loops.

Traffic shaping	The process of controlling the rate of data transmission to manage and prioritize network traffic.
Quality of Service (QoS)	A set of techniques used to manage and prioritize network traffic to ensure optimal performance for specific applications or users.
Data virtual local area network (VLAN)	A logically segmented network created by grouping devices together based on their functional roles, regardless of their physical location.

Voice VLAN	A VLAN specifically dedicated to carrying voice traffic in a VoIP network.
Port configurations	Settings and parameters applied to network switch ports to define their behavior and features.
Port tagging/802.1Q	A protocol that allows multiple VLANs to share a single physical switch port.

Port aggregation	Combining multiple physical ports to increase bandwidth and provide redundancy.
Link Aggregation Control Protocol (LACP)	A protocol used to negotiate and manage port aggregation between devices.
Duplex	A mode of communication that allows data to flow bidirectionally between network devices simultaneously.

Speed	The data transfer rate supported by a network interface or link.
Flow control	Techniques used to manage data transmission to prevent congestion and ensure smooth communication.
Port mirroring	The process of duplicating network traffic from one port to another for monitoring and analysis purposes.

Port security	A feature that restricts access to switch ports based on MAC addresses to prevent unauthorized network access.
Jumbo frames	Larger-than-standard Ethernet frames that increase data transmission efficiency for specific applications.
Auto-medium-dependent interface crossover (MDI-X)	A feature that automatically detects and configures the correct cable type (straight-through or crossover) for network connections.

Media access control (MAC) address tables	Tables in network switches that store MAC addresses and their associated switch ports.
Power over Ethernet (PoE)/Power over Ethernet plus (PoE+)	Technologies that deliver power to network devices over Ethernet cables, eliminating the need for separate power cables.
Spanning Tree Protocol	A network protocol that prevents loops in Ethernet networks and ensures redundant paths are managed effectively.

Carrier-sense multiple access with collision detection (CSMA/CD)	A protocol used in Ethernet networks to manage access to the shared network medium and detect collisions.
Address Resolution Protocol (ARP)	A protocol used to map IP addresses to MAC addresses in local networks.
Neighbor Discovery Protocol	A protocol used in IPv6 networks to discover and manage neighboring devices.

802.11a Standard	A Wi-Fi standard that operates in the 5 GHz frequency band, providing higher data rates but shorter range compared to 802.11b/g.
802.11b Standard	A Wi-Fi standard that operates in the 2.4 GHz frequency band, offering lower data rates but better range than 802.11a.
802.11g Standard	A Wi-Fi standard that operates in the 2.4 GHz frequency band, offering higher data rates than 802.11b while maintaining backward compatibility.

802.11n Standard	A Wi-Fi standard that operates in both 2.4 GHz and 5 GHz frequency bands, providing improved data rates and better range compared to older standards.
802.11ac Standard	A Wi-Fi standard that operates in the 5 GHz frequency band, offering higher data rates and better performance than 802.11n.
802.11ax Standard	A Wi-Fi standard, also known as Wi-Fi 6, designed to handle high-density environments and offer improved efficiency and performance compared to previous standards.

Channel Bonding	A technique used in Wi-Fi to combine multiple channels for increased data throughput.
Service Set Identifier (SSID)	A unique identifier for a wireless network.
Basic service set	A single access point and the wireless devices connected to it.

Extended service set	A group of interconnected basic service sets to extend the coverage area of a wireless network.
Independent basic service set (Ad-hoc)	A wireless network configuration where devices communicate directly with each other without the need for an access point.
Roaming	The ability of a wireless client to maintain connectivity as it moves between different access points in a wireless network.

Omni Antenna	A type of antenna that radiates signals in all directions, providing 360-degree coverage.
Directional Antenna	A type of antenna that focuses signals in a specific direction, providing higher gain and longer range.
WiFi Protected Access (WPA)/WPA2 Personal (AES/TKIP)	Security protocols used to encrypt and secure wireless network communications.

WPA/WPA2 Enterprise (AES/TKIP)	An enterprise-level security mode for Wi-Fi networks that uses an authentication server, providing higher security than WPA/WPA2 Personal.
Code-division multiple access (CDMA)	A cellular communication technology that allows multiple users to share the same frequency by assigning unique codes to each user.
Global System for Mobile Communications (GSM)	A cellular communication standard used for digital mobile networks.

Long-Term Evolution (LTE)	A high-speed wireless communication standard used for 4G cellular networks.
3G, 4G, 5G	Generations of cellular network technology, with each generation providing improved data speeds and capabilities.
New Category: Network Operations	**New Category: Network Operations**

Temperature	The measure of the degree of hotness or coldness of a substance or environment.
Central Processing Unit (CPU) Usage	The percentage of time the CPU spends executing non-idle tasks, indicating how much processing power is being utilized.
Memory	Also known as RAM (Random Access Memory), it is a volatile data storage component in a computer that stores data and instructions for the CPU to access quickly.

Network Metrics	Quantitative measures used to assess the performance, efficiency, and health of a computer network.
Bandwidth	The maximum data transfer rate or capacity of a network communication channel, usually measured in bits per second (bps).
Latency	The time delay experienced in data transmission between the sender and the receiver in a network.

Jitter	The variation in the delay of received data packets in a network, which can cause irregularities and disruptions in the data stream.
SNMP Traps	Asynchronous notifications sent from a managed device (like a network router or switch) to a management station, indicating a significant event or condition.
SNMP Object Identifiers (OIDs)	Unique identifiers used in Simple Network Management Protocol (SNMP) to represent managed objects (parameters) in a device.

SNMP Management Information Bases (MIBs)	A collection of hierarchical data structures that define the parameters and entities managed by SNMP in a device.
Log Reviews	The process of examining logs (records of events or activities) to identify anomalies, security breaches, or system issues.
Traffic Logs	Logs that record information about network traffic, including the source, destination, and type of data being transmitted.

Audit Logs	Logs that track and record events related to system activities, user actions, and security-related events for auditing purposes.
Syslog	A standard protocol used for forwarding log messages in IP networks.
Logging Levels/Severity Levels	A system of categorizing log messages based on their importance and criticality, typically ranked from lowest to highest severity.

Link State (Up/Down)	The status of a network link, indicating whether it is operational (up) or not functioning (down).
Speed/Duplex	The data transfer rate and communication mode (e.g., full duplex or half duplex) of a network interface.
Send/Receive Traffic	The data transmitted and received by a network interface.

Cyclic Redundancy Checks (CRCs)	Error-checking mechanisms used to detect errors in data during transmission.
Protocol Packet and Byte Counts	The number of packets and bytes sent or received for a specific network protocol.
CRC Errors	The number of packets or frames that failed the CRC check and were discarded due to data corruption.

Giants	Packets or frames that exceed the maximum allowable size in a network.
Runts	Packets or frames that are smaller than the minimum allowable size in a network.
Encapsulation Errors	Errors that occur when a packet is improperly encapsulated within another data unit during data transmission.

Humidity	The measure of moisture or water vapor present in the air or environment.
Electrical	Relating to or involving electricity.
Flooding	In networking, it refers to the excessive transmission of data, leading to network congestion and performance issues.

Baselines	Reference points or benchmarks used for comparison to assess changes, anomalies, or performance improvements in a system or network.
NetFlow Data	Information collected by Cisco's NetFlow technology, providing visibility into network traffic and usage patterns.
Uptime/Downtime	The period a system or service is operational (uptime) or unavailable (downtime).

Change Management	The process of controlling and managing changes to a system or network in a structured and coordinated manner.
Incident Response Plan	A documented strategy outlining actions to be taken in response to cybersecurity incidents or emergencies.
Disaster Recovery Plan	A comprehensive plan that outlines the procedures to recover IT infrastructure and operations after a significant disruptive event.

Business Continuity Plan	A strategic plan that ensures essential business functions can continue during and after a major disaster or crisis.
System Life Cycle	The stages through which a system or application progresses, from planning and development to retirement.
Standard Operating Procedures	Detailed step-by-step instructions for routine tasks and processes to ensure consistency and efficiency.

Password Policy	A set of rules and guidelines for creating and managing passwords securely.
Acceptable Use Policy	A policy that outlines acceptable and unacceptable behaviors or actions when using an organization's IT resources.
Bring Your Own Device (BYOD) Policy	A policy that governs the use of personal devices in the workplace.

Remote Access Policy	Guidelines and restrictions related to accessing an organization's network or resources from remote locations.
Onboarding and Offboarding Policy	Policies and procedures for the integration and departure of employees within an organization.
Security Policy	A set of guidelines and rules to protect an organization's information and assets.

Data Loss Prevention	Strategies and technologies to prevent sensitive data from being lost, leaked, or accessed by unauthorized users.
Physical Network Diagram	A visual representation of a network's physical layout, including devices and connections.
Floor Plan	A diagram that shows the layout of a building's floors and spaces.

Rack Diagram	A diagram illustrating the arrangement of network devices and equipment in a server rack.
Intermediate Distribution Frame (IDF)/Main Distribution Frame (MDF) Documentation	Documentation related to network distribution points.
Logical Network Diagram	A visual representation of a network's logical structure, including subnets, protocols, and routing.

Wiring Diagram	A graphical representation of network cabling and connections.
Site Survey Report	A document outlining observations and findings from a site survey to plan network deployments.
Audit and Assessment Report	A report detailing the results of an audit or assessment of a system's security and compliance.

Baseline Configurations	Established and documented standard configurations for systems or network devices.
Non-Disclosure Agreement (NDA)	A legally binding contract that prohibits the sharing of confidential or proprietary information.
Service-Level Agreement (SLA)	A contract or agreement that defines the level of service a provider will deliver to a customer.

Memorandum of Understanding (MOU)	A formal document outlining the terms and understanding between parties involved in a partnership or collaboration.
Change Control Documentation	Documentation that tracks and manages changes to systems or networks.
Load Balancing	The distribution of network traffic across multiple servers or paths to optimize resource utilization and avoid overloading.

Multipathing	Using multiple physical paths or connections for data transmission to improve redundancy and performance.
Network Interface Card (NIC) Teaming	Combining multiple NICs to work as a single virtual interface for enhanced throughput and fault tolerance.
Redundant Hardware/Clusters	Having duplicate hardware or systems in place to provide backup in case of failures.

Switches	Networking devices that connect multiple devices in a local area network (LAN) and forward data packets to their destinations.
Routers	Devices that connect different networks and facilitate data traffic between them.
Firewalls	Security devices that control and monitor incoming and outgoing network traffic based on predefined security rules.

Uninterruptible Power Supply (UPS)	A device that provides emergency power to connected equipment during power outages.
Power Distribution Units (PDUs)	Devices that distribute electrical power to multiple devices or equipment.
Generator	A device that converts mechanical energy into electrical energy to provide backup power during prolonged outages.

HVAC	Heating, Ventilation, and Air Conditioning systems used to control temperature and air quality in data centers and network facilities.
Fire Suppression	Systems or methods to detect and extinguish fires in data centers or critical infrastructure.
Cold Site	A disaster recovery site that provides the necessary infrastructure, but no active equipment until a disaster occurs.

Warm Site	A disaster recovery site that provides partial infrastructure and some pre-configured equipment in case of a disaster.
Hot Site	A fully operational and redundant disaster recovery site ready to take over immediately after a disaster.
Cloud Site	A disaster recovery solution hosted on cloud platforms with data and services replicated off-site.

Active-Active vs. Active-Passive	Configurations in which both systems are actively running (active-active) or one system is on standby (active-passive).
Multiple Internet Service Providers (ISPs)/Diverse Paths	Having multiple ISP connections or network paths for redundancy and fault tolerance.
Virtual Router Redundancy Protocol (VRRP)/First Hop Redundancy Protocol (FHRP)	Protocols that provide network redundancy by allowing multiple routers to work together as a single virtual router.

Mean Time to Repair (MTTR)	The average time required to repair a failed system or component.
Mean Time Between Failure (MTBF)	The average time between failures for a system or component.
Recovery Time Objective (RTO)	The maximum acceptable downtime or duration for restoring a system after a disaster.

Recovery Point Objective (RPO)	The maximum amount of data loss that an organization can tolerate in the event of a disaster.
State Backup	Backing up the current state or data of a system or application.
Configuration Backup	Backing up the configuration settings of network devices or systems for recovery or replication purposes.

New Category: Network Security	**New Category: Network Security**
Confidentiality, Integrity, Availability (CIA)	Confidentiality ensures that data is only accessible to authorized individuals and remains protected from unauthorized access. Integrity ensures that data remains unaltered and maintains its accuracy and
Internal Threats	Internal threats refer to security risks that originate from within an organization. These threats can be posed by employees, contractors, or anyone with privileged access to the organization's systems.

External Threats	External threats refer to security risks that come from outside an organization. These threats can be from hackers, cybercriminals, or any malicious entities attempting to breach an organization's security.
Common Vulnerabilities and Exposures (CVE) - Zero-day	- CVE: Common Vulnerabilities and Exposures (CVE) is a list of publicly known information security vulnerabilities and exposures. - Zero-day: A zero-day vulnerability is a security flaw
Cybersecurity Exploits	Cybersecurity exploits are techniques or methods used to take advantage of vulnerabilities in a computer system or network, potentially allowing unauthorized access or malicious actions.

Least Privilege	Least privilege is a principle in cybersecurity that grants users the minimum level of access necessary to perform their tasks and nothing more. This reduces the risk of accidental or intentional misuse of privileges.
Role-based Access	Role-based access control (RBAC) is a method of managing user permissions based on their roles within an organization. Users are assigned specific roles, and access privileges are associated with those roles.
Zero Trust	Zero Trust is a security model that assumes no implicit trust for any user, device, or network component, regardless of its location. It requires verification and validation of every access request before granting

Network Segmentation Enforcement	Network segmentation enforcement involves dividing a network into smaller segments and enforcing security measures to restrict communication between segments, increasing security and reducing the impact of
Screened Subnet (DMZ)	A screened subnet, previously known as a demilitarized zone (DMZ), is a network segment that acts as a buffer between an internal trusted network and an external untrusted network, providing additional
Separation of Duties	Separation of duties is a security principle that ensures critical tasks are divided among multiple individuals to prevent any single person from having complete control over sensitive operations.

Network Access Control	Network Access Control (NAC) is a security technology that enforces policies to control access to a network, ensuring that only authorized and compliant devices are allowed access.
Honeypot	A honeypot is a decoy system or network designed to attract attackers and gather information about their tactics and techniques to improve security measures.
Multifactor Authentication	Multifactor authentication (MFA) is a security method that requires users to provide multiple forms of identification (e.g., password, biometrics, OTP) before granting access to a system or service.

Terminal Access Controller Access Control System Plus (TACACS+)	TACACS+ is a network authentication protocol that provides centralized access control for network devices.
Single Sign-On (SSO)	Single Sign-On is an authentication method that allows users to access multiple applications or systems with a single set of credentials.
Remote Authentication Dial-in User Service (RADIUS)	RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting for remote access users.

LDAP (Lightweight Directory Access Protocol)	LDAP is a protocol used to access and manage directory information, such as user authentication and authorization data.
Kerberos	Kerberos is a network authentication protocol used to securely authenticate users and devices over a non-secure network.
Local Authentication	Local authentication refers to the process of authenticating users directly against a local database on a system or device.

802.1X	802.1X is an IEEE standard for port-based network access control, providing authentication for devices connecting to a LAN or WLAN.
Extensible Authentication Protocol (EAP)	EAP is a framework that allows multiple authentication methods to be used within a single authentication process.
Security Risk Assessments	Security risk assessments involve identifying and evaluating potential security risks and vulnerabilities within an organization's systems, processes, and infrastructure.

Threat Assessment	Threat assessment involves identifying and evaluating potential threats that may target an organization's assets and resources.
Vulnerability Assessment	Vulnerability assessment involves identifying and evaluating weaknesses and vulnerabilities within an organization's systems and infrastructure.
Penetration Testing	Penetration testing, or ethical hacking, involves actively simulating cyberattacks to identify and exploit vulnerabilities in a controlled and secure manner.

Posture Assessment	Posture assessment involves evaluating an organization's overall security posture, considering its readiness to defend against cyber threats.
Business Risk Assessments	Business risk assessments involve evaluating risks that could impact an organization's ability to achieve its business objectives.
Process Assessment	Process assessment involves evaluating and analyzing an organization's security processes and practices for effectiveness and efficiency.

Vendor Assessment	Vendor assessment involves evaluating the security practices and risks associated with third-party vendors that provide products or services to an organization.
Security Information and Event Management (SIEM)	SIEM is a cybersecurity system that collects and analyzes security event data from various sources to provide real-time monitoring and threat detection.
Denial-of-Service (DoS)	Denial-of-Service is an attack that disrupts the normal functioning of a computer system or network, making it unavailable to legitimate users.

Distributed Denial-of-Service (DDoS)	DDoS is an attack that involves multiple compromised systems (a botnet) to flood a target system with traffic, overwhelming its resources and causing a denial of service.
Botnet/Command and Control	A botnet is a network of compromised computers controlled by a central command and control server, often used for malicious activities.
On-path Attack (Man-in-the-Middle Attack)	An on-path attack, previously known as a man-in-the-middle attack, involves intercepting and possibly altering communication between two parties without their knowledge.

DNS Poisoning	DNS poisoning is an attack that alters the DNS records of a domain, redirecting users to malicious websites or intercepting their traffic.
VLAN Hopping	VLAN hopping is a technique used to gain unauthorized access to traffic on different Virtual LANs (VLANs) by exploiting vulnerabilities in network switches.
ARP Spoofing	ARP spoofing is a technique where an attacker sends falsified Address Resolution Protocol (ARP) messages to link their MAC address with the IP address of a legitimate host, intercepting traffic meant for the target.

Rogue DHCP	A rogue DHCP server is an unauthorized DHCP server that assigns IP addresses to devices on a network, potentially causing connectivity issues and security risks.
Rogue Access Point (AP)	A rogue access point is an unauthorized wireless access point connected to a network, providing an entry point for attackers or causing interference.
Evil Twin	An evil twin is a fake wireless network set up by an attacker to mimic a legitimate network, tricking users into connecting and capturing their sensitive information.

Ransomware	Ransomware is malicious software that encrypts a victim's data, demanding a ransom payment to decrypt the data and restore access.
Password Attacks	Password attacks are attempts to gain unauthorized access to a system by guessing or cracking passwords. - Brute-Force: Trying all possible combinations until the correct password is
Malware	Malware is malicious software designed to harm or gain unauthorized access to computer systems. It includes viruses, worms, Trojans, and other harmful programs.

Social Engineering	Social engineering is the use of psychological manipulation to trick individuals into divulging sensitive information or performing actions that compromise security.
Phishing	Phishing is a social engineering attack that involves sending fraudulent emails or messages to deceive recipients into revealing sensitive information or clicking on malicious links.
Tailgating	Tailgating is a physical security breach where an unauthorized person follows an authorized individual into a secured area without proper authentication.

Piggybacking	Piggybacking is a physical security breach where an unauthorized person gains access to a secured area by using someone else's legitimate access.
Secure SNMP	Secure SNMP (Simple Network Management Protocol) involves using encryption and authentication to protect SNMP communication.
Router Advertisement (RA) Guard	RA Guard is a feature that protects against rogue router advertisements on IPv6 networks, preventing attackers from hijacking network traffic.

Port Security	Port security is a feature that restricts access to a network switch port based on MAC addresses, preventing unauthorized devices from connecting.
Dynamic ARP Inspection	Dynamic ARP Inspection (DAI) is a security feature that validates ARP packets to prevent ARP spoofing attacks.
Control Plane Policing	Control Plane Policing (CoPP) is a mechanism to protect a network device's control plane from excessive traffic and potential attacks.

Private VLANs	Private VLANs allow you to segment a VLAN into sub-VLANs, isolating devices within the same VLAN from each other.
Disable Unneeded Switchports	Disabling unused switchports reduces potential attack surfaces and unauthorized access points.
Disable Unneeded Network Services	Disabling unnecessary network services reduces potential security vulnerabilities.

Change Default Passwords	Changing default passwords on network devices and systems is essential to prevent unauthorized access.
Password Complexity/Length	Enforcing strong password policies with complexity and length requirements improves security.
Enable DHCP Snooping	DHCP snooping is a security feature that ensures only authorized DHCP servers can assign IP addresses to devices on a network.

Change Default VLAN	Changing the default VLAN on network switches reduces the risk of unauthorized access and VLAN hopping attacks.
Patch and Firmware Management	Regularly applying security patches and firmware updates helps protect against known vulnerabilities.
Access Control List (ACL)	An ACL is a list of rules that controls traffic flow and filters packets based on specified criteria.

Firewall Rules - Explicit Deny - Implicit Deny	Explicit deny and implicit deny are firewall rules that specify whether to allow or block traffic based on defined criteria. Explicit deny blocks specific traffic, while implicit deny denies all traffic that hasn't been explicitly allowed.
MAC Filtering	MAC filtering involves allowing or denying access to a network based on the Media Access Control (MAC) address of a device.
Antenna Placement	Proper antenna placement can improve wireless network coverage and security by minimizing signal leakage.

Power Levels	Adjusting wireless access point power levels can control the signal range and reduce the risk of unauthorized access.
Wireless Client Isolation	Wireless client isolation prevents communication between devices connected to the same wireless network, enhancing security.
Guest Network Isolation	Guest network isolation separates guest traffic from the main network, preventing unauthorized access to sensitive resources.

Preshared Keys (PSKs)	PSKs are shared encryption keys used in WPA and WPA2 security protocols to secure wireless network communication.
EAP (Extensible Authentication Protocol)	EAP is an authentication framework used in wireless networks and other security protocols.
Geofencing	Geofencing is a feature that allows defining virtual boundaries, triggering actions when devices enter or leave specific geographic areas.

Captive Portal	A captive portal is a web page that requires users to authenticate or agree to terms before accessing a public network.
IoT Access Considerations	IoT access considerations involve managing and securing access to Internet of Things (IoT) devices to prevent unauthorized access and attacks.
IoT Detection Methods	IoT detection methods involve using specialized tools and techniques to identify and monitor IoT devices on a network.

Employee Training as a Prevention Method	Educating employees about cybersecurity risks and best practices can significantly reduce the likelihood of security breaches.
Access Control Hardware as a Prevention Method	Access control hardware, such as card readers and biometric scanners, can enhance physical security.
Badge Readers as a Prevention Method	Badge readers are devices that grant access based on employee identification cards or badges.

Biometrics as a Prevention Method	Biometric authentication uses unique physical characteristics (fingerprint, iris, etc.) for access control.
Locking Racks as a Prevention Method	Locking racks provide physical security for network equipment and servers.
Locking Cabinets as a Prevention Method	Locking cabinets secure sensitive equipment and prevent unauthorized access.

Access Control Vestibule (Mantrap)	An access control vestibule, previously known as a mantrap, is a small area with two doors designed to prevent unauthorized access.
Smart Lockers as a Prevention Method	Smart lockers provide secure storage for personal belongings and prevent theft.
Asset Disposal	Asset disposal involves securely disposing of hardware and devices to ensure data protection.

Factory Reset/Wipe Configuration	Performing a factory reset or wiping the configuration of a device removes all data and settings.
Sanitize Devices for Disposal	Sanitizing devices involves securely erasing data to prevent data leakage when disposing of hardware.
Site-to-Site VPN	Site-to-Site VPN connects two or more remote networks over the internet, creating a secure private network.

Client-to-Site VPN	Client-to-Site VPN allows remote users to securely access a corporate network over the internet.
Clientless VPN	Clientless VPN allows users to access a private network through a web browser without installing a VPN client.
Split Tunnel vs. Full Tunnel	In split tunneling, only specific traffic goes through the VPN, while full tunneling directs all traffic through the VPN.

Remote Desktop Connection	Remote desktop connection allows users to access and control a remote computer over a network.
Remote Desktop Gateway	A remote desktop gateway allows users to connect to remote desktops securely.
SSH (Secure Shell)	SSH is a secure network protocol used for secure remote access and data communication.

Virtual Network Computing (VNC)	VNC is a remote desktop sharing protocol that allows remote access and control of a computer.
Virtual Desktop	A virtual desktop is a virtualized environment hosted on a server, accessible remotely by users.
Authentication and Authorization Considerations	Authentication and authorization considerations involve managing user access to resources based on their identity and permissions.

In-Band vs. Out-of-Band Management	In-band management uses the same network infrastructure for management traffic, while out-of-band management uses a separate dedicated network.
Compare and Contrast Remote Access Methods and Security Implications	Remote access methods differ in their security features and potential vulnerabilities, and it is essential to choose the appropriate method based on security requirements.
New Category: Network Troubleshooting	**New Category: Network Troubleshooting**

Identify the problem	The first step in troubleshooting, where the issue or challenge is recognized or noticed.
Gather information	Collect relevant data and details about the problem to aid in the troubleshooting process.
Question users	Interact with users or affected parties to gain insights into the nature and circumstances of the problem.

Identify symptoms	Recognize the observable signs or indications that point to the existence of the problem.
Determine if anything has changed	Investigate if any recent modifications or alterations have been made to the system or network, as they might be related to the problem.
Duplicate the problem, if possible	Try to recreate the issue in a controlled environment to understand its behavior better and test potential solutions.

Approach multiple problems individually	Handle and address each problem independently to avoid confusion and ensure effective troubleshooting.
Establish a theory of probable cause	Formulate a hypothesis about the possible reason or root cause of the problem based on gathered information.
Question the obvious	Challenge assumptions and consider alternative explanations beyond the apparent cause of the issue.

Consider multiple approaches	Think about different methods to tackle the problem and explore various solutions.
Top-to-bottom/bottom-to-top OSI model	Refers to troubleshooting techniques that involve examining the layers of the OSI (Open Systems Interconnection) model either from the top layer (application layer) down to the bottom (physical layer) or vice versa.
Divide and conquer	A problem-solving strategy that involves breaking down a complex issue into smaller, more manageable parts for easier resolution.

Test the theory to determine the cause	Validate the theory of probable cause by conducting tests and experiments.
If the theory is confirmed, determine the next steps to resolve the problem	If the hypothesis is proven correct, plan the appropriate course of action to fix the issue.
If the theory is not confirmed, reestablish a new theory or escalate	If the initial hypothesis is incorrect, revise the theory or seek additional help from higher-level support.

Establish a plan of action to resolve the problem and identify potential effects	Create a detailed plan outlining the steps to address the issue and consider any potential consequences.
Implement the solution or escalate as necessary	Carry out the planned solution or involve higher-level support if required.
Verify full system functionality and, if applicable, implement preventive measures	Ensure that the problem is resolved and consider preventive measures to avoid similar issues in the future.

Document findings, actions, outcomes, and lessons learned	Keep comprehensive records of the troubleshooting process, including the problem, actions taken, and the final outcome for future reference and learning.
Specifications and limitations	Understand the specifications and constraints of the systems or components involved in troubleshooting.
Throughput	The rate at which data is successfully transmitted through a network or system.

Speed	Refers to the data transmission rate, usually measured in bits per second (bps) or a multiple (e.g., Mbps or Gbps).
Distance	The physical span between two network devices or points.
Cable considerations	Factors to be taken into account when selecting or using network cables.

Shielded and unshielded	Types of cables designed with or without shielding to protect against electromagnetic interference.
Plenum and riser-rated	Cable types suitable for different installation environments (e.g., plenum-rated cables are used in airspaces like drop ceilings, while riser-rated cables are suitable for vertical runs between floors).
Cable application	Identifying the appropriate use or purpose of specific cable types.

Rollover cable/console cable	A special type of serial cable used for connecting to the console port of networking equipment.
Crossover cable	A network cable used to directly connect two similar devices (e.g., two computers or two switches) without using a network hub or switch.
Power over Ethernet (PoE)	A technology that allows network devices to receive power and data over a single Ethernet cable.

Attenuation	The reduction of signal strength or power as it travels through a medium, such as a cable or an optical fiber. Attenuation is usually measured in decibels (dB) and occurs due to absorption, scattering, or other losses.
Interference	In networking and wireless communications, interference refers to the disruption or distortion of signals caused by other signals or electromagnetic radiation in the environment. Interference can lead to data errors,
Decibel (dB) loss	A unit of measurement used to express the reduction in signal strength or power. It is commonly used in networking and telecommunications to indicate signal loss or attenuation in cables, connectors, or other

Incorrect pinout	Pinout refers to the arrangement of pins or connectors on a device or cable. Incorrect pinout implies that the connections do not match the expected configuration, which can lead to communication issues or
Bad ports	Refers to malfunctioning or damaged network ports on devices such as routers, switches, or network interface cards (NICs), causing connectivity problems.
Open/short	In the context of cabling or electrical circuits, "open" refers to a break or discontinuity in the circuit, while "short" refers to an unintended connection between two points. Both can cause network connectivity

Light-emitting diode (LED) status indicators	LEDs on networking devices that provide visual indications about the device's status, network activity, link status, or errors.
Incorrect transceivers	Transceivers are devices used to convert signals between different media types, such as electrical signals to optical signals in fiber optics. Incorrect transceivers may not be compatible with the
Duplexing issues	Refers to problems related to the method of communication used for data transmission between devices, such as half-duplex and full-duplex. Duplexing issues can lead to collisions and performance problems.

Transmit and receive (TX/RX) reversed	This occurs when the transmit and receive connections are switched or reversed, causing data to be transmitted in the wrong direction.
Dirty optical cables	Optical cables with contaminants or dirt on their connectors can cause signal degradation and affect the quality of optical communication.
Cable crimper	A tool used to attach connectors to the ends of network cables, ensuring a secure and reliable connection.

Punchdown tool	A tool used to terminate and connect individual wires to a punchdown block, patch panel, or keystone jack.
Tone generator	A tool used to generate a tone signal on a specific wire in a cable, helping to identify and trace the cable's path.
Loopback adapter	A hardware or software component used to redirect transmitted data back to the sender, allowing testing of network connections and interfaces.

Optical time-domain reflectometer (OTDR)	A device used to test and characterize optical fibers by measuring the light reflections and losses along the fiber.
Multimeter	An electronic measuring instrument used to measure various electrical quantities, such as voltage, current, and resistance.
Cable tester	A tool used to verify the integrity and correctness of network cables, checking for open circuits, shorts, or incorrect pinouts.

Wire map	A graphical representation of how the wires in a network cable are connected to the connector pins.
Tap	In networking, a tap is a passive device used to capture network traffic for analysis without interrupting the flow of data.
Fusion splicers	Devices used to join or fuse optical fibers together to create a continuous and low-loss connection.

Spectrum analyzers	Instruments used to analyze and visualize the frequency spectrum of signals, helping to identify interference and signal quality issues.
Snips/cutters	Tools used for cutting and trimming cables during installation or maintenance.
Cable stripper	A tool used to remove the outer sheath from network cables, exposing the individual wires for termination.

Fiber light meter	A device used to measure the amount of light transmitted through an optical fiber, providing information about the link's power and quality.
WiFi analyzer	Software or hardware tools used to analyze and optimize wireless networks, identifying signal strength, channel utilization, and interference.
Protocol analyzer/packet capture	Tools used to capture, analyze, and decode network traffic for troubleshooting and performance monitoring.

Bandwidth speed tester	Tools used to measure the speed and performance of internet connections or local networks.
Port scanner	A tool used to identify open ports on network devices and assess potential security vulnerabilities.
iperf	A network testing tool used to measure network performance by generating data streams between two endpoints.

NetFlow analyzers	Tools used to analyze and monitor network traffic, providing insights into bandwidth usage, applications, and sources of traffic.
Trivial File Transfer Protocol (TFTP) server	A simple file transfer protocol often used for network device configurations and firmware upgrades.
Terminal emulator	Software that allows a computer to emulate a terminal, enabling remote access to network devices through a command-line interface.

IP scanner	A tool used to scan a range of IP addresses to identify active devices on a network.
Command line tools	A set of utilities that can be executed from the command line or terminal to perform various network-related tasks.
ping	A command used to test network connectivity by sending ICMP echo requests to a target host and receiving echo replies.

ipconfig/ifconfig/ip	Commands used to view and configure network interfaces and IP addresses on Windows, Linux, and other operating systems.
nslookup/dig	Commands used to query DNS (Domain Name System) servers to retrieve domain name information and IP addresses.
traceroute/tracert	Commands used to trace the route packets take from the source to the destination, helping to identify network latency and routing issues.

arp	A command used to view and manage the Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses.
netstat	A command used to display network statistics and active network connections on a system.
hostname	A command used to view or set the hostname of a computer on a network.

route	A command used to view and manage the IP routing table on a device.
telnet	A command-line tool used for remote access to network devices using the Telnet protocol.
tcpdump	A command-line packet capture utility used to capture and analyze network traffic.

nmap	A powerful network scanning tool used for network discovery and security auditing.
show interface	A command used to display detailed information about a network interface on networking devices.
show config	A command used to display the current configuration of networking devices.

show route	A command used to display the routing table and routes on networking devices.
Device configuration review	The process of examining and verifying the configuration settings of networking devices to ensure they are correctly set up and optimized.
Routing tables	Data structures used by routers to determine the best path for forwarding packets to their destinations.

Interface status	The operational state of a network interface, indicating whether it is up or down.
VLAN assignment	Assigning network devices or ports to specific Virtual Local Area Networks (VLANs) for network segmentation.
Network performance baselines	Reference points used to assess and measure the normal performance of a network, helping to identify deviations and potential issues.

Collisions	In Ethernet networks, collisions occur when two devices attempt to transmit data simultaneously, causing data loss and reduced network performance.
Broadcast storm	A network situation where excessive broadcast or multicast packets flood the network, consuming bandwidth and causing congestion.
Duplicate MAC address	A situation where two devices on a network have the same Media Access Control (MAC) address, leading to communication issues.

Duplicate IP address	A situation where two devices on a network have the same IP address, leading to network conflicts and communication problems.
Multicast flooding	A situation where multicast packets are unnecessarily forwarded to all network ports, causing increased network traffic.
Asymmetrical routing	A network routing scenario where data packets take different paths to reach the source and destination, potentially leading to issues with packet delivery.

Switching loops	Network loops caused by misconfigured switches or redundant connections, leading to broadcast storms and network instability.
Routing loops	A situation in network routing where packets are forwarded endlessly between routers, unable to reach their destination.
Rogue DHCP server	An unauthorized DHCP (Dynamic Host Configuration Protocol) server that assigns IP addresses to devices on a network, causing network connectivity problems.

DHCP scope exhaustion	When a DHCP server runs out of available IP addresses to assign to devices, preventing new devices from obtaining IP configurations.
IP setting issues	Problems related to incorrect or misconfigured IP settings on devices, including gateway, subnet mask, IP address, and DNS.
Incorrect gateway	Setting the wrong gateway IP address on a device, causing connectivity issues outside the local network.

Incorrect subnet mask	Configuring an incorrect subnet mask on a device, leading to communication problems with devices on different subnets.
Incorrect IP address	Assigning an IP address to a device that conflicts with another device on the network.
Incorrect DNS	Using incorrect DNS server settings, leading to name resolution and internet connectivity issues.

Missing route	When a device lacks the necessary routing information to reach a particular destination, leading to packet drops and communication problems.
Low optical link budget	In optical communication, a situation where the total optical power budget is insufficient to maintain a reliable link.
Certificate issues	Problems related to SSL/TLS certificates, causing security warnings and potential communication failures.

Hardware failure	When networking equipment or components fail to function properly, resulting in network disruptions.
Host-based/network-based firewall settings	Issues with firewall configurations that may block or allow network traffic inappropriately.
Blocked services, ports, or addresses	When specific services, ports, or IP addresses are intentionally or unintentionally blocked, preventing communication.

Incorrect VLAN	Misconfiguration of Virtual LAN (VLAN) settings, leading to communication issues between devices on different VLANs.
DNS issues	Problems with the Domain Name System (DNS), affecting name resolution and internet access.
NTP issues	Problems with Network Time Protocol (NTP) synchronization, causing time-related issues on the network.

BYOD challenges	Issues related to the integration and security of personal devices brought into a corporate network (Bring Your Own Device).
Licensed feature issues	Challenges related to the licensing and availability of specific features on networking devices.
Network performance issues	Various problems that impact the overall performance and efficiency of a network.

Throughput	The amount of data that can be transmitted over a network in a given period, usually measured in bits per second (bps) or megabits per second (Mbps).
Speed	Refers to the data transmission rate of a network connection, typically measured in Mbps or Gbps.
Distance	The physical span or length over which a network connection or wireless signal can be effectively maintained.

Received signal strength indication (RSSI) signal strength	A measurement of the strength of a received wireless signal, indicating the signal's power level.
Effective isotropic radiated power (EIRP)/power settings	The amount of power radiated from an antenna in a specific direction, accounting for antenna gain and cable loss.
Antennas	A device used to transmit or receive radio frequency (RF) signals in a wireless communication system.

Channel utilization	The amount of time a wireless channel is occupied by active transmissions or interference, affecting network performance.
AP association time	The time it takes for a wireless client to establish a connection with an access point (AP) when joining a wireless network.
Site survey	A process of analyzing a location to determine the optimal placement of wireless access points and identify potential sources of interference.

Channel overlap	A situation where neighboring wireless channels interfere with each other due to overlapping frequencies.
Antenna cable attenuation/signal loss	Loss of signal strength that occurs as a wireless signal travels through the antenna cable.
RF attenuation/signal loss	Signal loss in radio frequency (RF) transmission due to various factors, such as distance and obstacles.

Wrong SSID	When wireless clients attempt to connect to an incorrect or unauthorized network SSID (Service Set Identifier).
Incorrect passphrase	Entering an incorrect pre-shared key or passphrase when attempting to join a secured wireless network.
Encryption protocol mismatch	Incompatibility between the encryption protocols used by the wireless access point and the client device.

Insufficient wireless coverage	Areas in a wireless network with weak or no signal coverage, resulting in limited or no connectivity.
Captive portal issues	Problems related to the captive portal authentication used in public Wi-Fi networks.
Client disassociation issues	Problems with wireless clients disconnecting from the network, often due to signal issues or client settings.