This document provides a concise overview of key concepts for the CompTIA Network+ exam, covering various aspects of networking. Here's a structured explanation of each topic:

Media and Topologies

- **Network Types:**

  - **Peer-to-peer networks:** Suitable for small networks (e.g., home, small offices). Devices share resources directly.
  - **Client/server networks (Server-centric):** Feature clients requesting data from servers. Servers provide centralized administration, data storage, and security.

- **Network Topologies (Physical arrangement of devices):**

  - **Bus:**
    Devices connected via a single cable (trunk/backbone).
    - **Failure points:** Loose terminators or cable breaks disrupt the entire segment.

  - **Star:**
    All devices connect to a central device.
    - **Failure point:** The central device is a single point of failure.

  - **Ring:**
    Devices form a complete loop.
    - **Failure point:** Breaking the loop disrupts the entire network.

  - **Mesh:**
    Every device is individually connected to every other device.
    - **Benefit:** Provides maximum reliability and redundancy.

  - **Wireless:** Uses a Wireless Access Point (WAP) as a centralized device.

- **IEEE Standards:**

  - **802.2 (LLC):** Defines specifications for the Logical Link Control sublayer.
  - **802.3 (CSMA/CD):** Ethernet standard using Carrier-Sense Multiple Access with Collision Detection. Most popular today.
  - **802.5 (Token Ring):** Defines Token Ring networking.
  - **802.11:** Defines standards for wireless LAN communication.

- **Media Characteristics:**

- **EMI (Electromagnetic Interference):**
  Caused by monitors, lighting, etc.
  - **Copper-based media:** Prone to EMI.
  - **Fiber-optic cable:** Resistant to EMI.
- **Crosstalk:** Interference between signals from different cables or wires within the same cable.
- **Attenuation:** Weakening of data signals as they travel through media.

- **Transmission Modes:**

  - **Half-duplex:** Devices can transmit and receive, but only one at a time.
  - **Full-duplex:** Devices can transmit and receive simultaneously. (e.g., a 100Mbps NIC in full-duplex can achieve 200Mbps).

Cables and Connectors

- **Coaxial Cable:**

  - **Thin Coax:**

    - Diameter: 0.25 inches.
    - Max length: 185 meters (approx. 600 feet).

  - **Thick Coax:**

    - Max length: 500 meters.
    - Uses a "tap" to connect to the backbone.
    - **AUI (Attachment Unit Interface):** 15-pin port often associated with thick coax (10Base5) for transceiver connection.

- **Fiber Optic Connectors:**

  - **SC:** Push-on connectors.
  - **ST:** Twist-type connectors.

- **UTP Cable Connectors:**

  - **RJ-45:** Used with Unshielded Twisted Pair cable.

10BASEX, 100BASEX, and 1000BASEX Standards

- **10Base2 (Thinnet/Thin Ethernet):**
    - **Standard:** 802.3 specification.
    - **Cable:** Thin coaxial cable (RG-58).
    - **Speed:** 10 Mbps maximum.
    - **Connectors:** BNC barrel and BNC T connectors.
    - **Termination:** 50-ohm terminators at each end to absorb signals and prevent reflection.
    - **Segment Limit:** 185 meters (approx. 600 feet).

Network Devices

- **Multistation Access Units (MSAUs):** Used to create Token Ring networks.
- **Cables:**
    - **Straight-through cable:** Connects systems to switches/hubs using MDI-X ports.
    - **Crossover cable:** Crosses wires 1 and 3, and 2 and 6 (used for direct device-to-device connections, like PC to PC or switch to switch).
- **Bridges:** Divide networks to reduce traffic on each segment.
- **MAC Address:**
    - A unique 6-byte (48-bit) hardware address assigned to a Network Interface Card (NIC).
    - **Format:** XX:XX:XX:XX:XX:XX
    - **First 3 bytes:** Manufacturer identifier (e.g., 00:D0:59).
    - **Last 3 bytes:** Unique Universal LAN MAC address assigned by the manufacturer.
- **Routing Information Protocol (RIP):** A distance-vector routing protocol supporting TCP and IPX.

OSI Model

The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes the functions of a telecommunication or computing system in terms of abstraction layers.

- **Encapsulation/Decapsulation:** As data moves down the stack (to be sent), headers are added at each layer (encapsulation). As data moves up the stack (upon receipt), headers are removed (decapsulation).

- **Layer Descriptions:**

- **Application Layer (Layer 7):** Provides network access for applications and end-user functions. Handles displaying information and preparing outgoing data.
- **Presentation Layer (Layer 6):** Translates data between the Application Layer and the Session Layer. Handles data formatting, encryption/decryption, and compression/decompression.
- **Session Layer (Layer 5):** Manages communication sessions between applications on different devices. Handles error detection and notification.
- **Transport Layer (Layer 4):** Establishes, maintains, and breaks connections. Manages data ordering, priorities, error checking, and retransmissions. (Protocols like TCP and UDP operate here).
- **Network Layer (Layer 3):** Handles logical addressing (IP addresses) and routing of data across networks. Discovers destination systems.
- **Data-link Layer (Layer 2):**
  - **Sublayers:** LLC (Logical Link Control) and MAC (Media Access Control).
  - **Functions:** Performs error detection/handling for transmitted signals, defines media access methods, and defines hardware addressing (MAC addresses).
- **Physical Layer (Layer 1):** Defines the physical structure of the network. Specifies voltage/signal rates, physical connection methods, and physical topology.

- **Device Mapping to OSI Layers:**

  - **Hub:** Physical (Layer 1)
  - **Switch:** Data-link (Layer 2)
  - **Bridge:** Data-link (Layer 2)
  - **Router:** Network (Layer 3)
  - **NIC (Network Interface Card):** Data-link (Layer 2)

Protocols

- **IP Addressing Classes:**

  - **Class A:** Network portion uses the first octet. Range: 1-126. Default Subnet Mask: 255.0.0.0.
  - **Class B:** Network portion uses the first two octets. Range: 128-191. Default Subnet Mask: 255.255.0.0.
  - **Class C:** Network portion uses the first three octets. Range: 192-223. Default Subnet Mask: 255.255.255.0.
  - **Loopback Address:** Network ID 127 is reserved for local loopback (ping 127.0.0.1).

- **Protocol Categories by OSI Layer:**

- **Application Protocols:** Map to Application, Presentation, and Session layers. Examples: FTP, TFTP, SNMP.
- **Transport Protocols:** Map to the Transport Layer. Responsible for data transport. Examples: TCP, UDP.
- **Network Protocols:** Responsible for addressing and routing. Examples: IP, IPX.

- **Specific Protocols and Services:**

  - **NetBEUI:** Protocol used on Windows networks; uses names as addresses; **not routable**.
  - **IPX/SPX:** Associated with NetWare networks; **routable**.
  - **TCP/IP:** Used by all major operating systems; **routable**.
  - **Firewall:** Controls traffic between networks, providing services like NAT, proxy, and packet filtering.
  - **Proxy Server:** Centralizes and controls Internet access.
  - **DHCP/BOOTP:** Automatically assigns IP addressing information.
  - **DNS (Domain Name System):** Resolves hostnames to IP addresses.
  - **WINS (Windows Internet Name Service):** Resolves NetBIOS names to IP addresses.
  - **NAT/ICS (Network Address Translation/Internet Connection Sharing):** Translates private network addresses to public network addresses.
  - **SNMP (Simple Network Management Protocol):** Provides network management for TCP/IP networks.

Network Support (Troubleshooting Tools and Concepts)

- **Command-Line Utilities:**

  - ping 127.0.0.1: Tests if the TCP/IP suite is installed and functioning locally.
  - tracert (or traceroute): Shows the path (routers) to a destination and the time taken, useful for identifying bottlenecks.
  - arp: Resolves IP addresses to MAC addresses (operates at the Network Layer).
  - netstat: Displays active TCP/IP connections (inbound/outbound).
  - nbtstat: Displays NetBIOS over TCP/IP protocol and statistical information.
  - ipconfig
    (Windows): Shows IP configuration.
    - ipconfig /all: Displays detailed IP configuration.
    - ipconfig /renew: Refreshes DNS information.

  - ifconfig (Linux): Equivalent to ipconfig.
  - winipcfg (Windows 9x/Me): Equivalent to ipconfig.
  - nslookup: Troubleshoots DNS problems.

- **Connectivity Issues:**

  - When using ipconfig to diagnose client connectivity, check if the **default gateway** is

  correctly set.
  - In non-DHCP networks, watch for **duplicate IP addresses** causing login issues.

- **Permissions:** If a user cannot access files others can, check **file permissions**.

Media Tools and LEDs

- **Tools:**

  - **Wire Crimper:** Attaches connectors to cables.
  - **Media Tester (Cable Tester):** Tests cable functionality.
  - **Optical Cable Tester:** Tests optical media.
  - **Hardware Loopback:** Tests outgoing signals from a device (e.g., NIC).

- **NIC LEDs:**

  - **Constantly lit LED:** May indicate a "chattering" network card (constantly transmitting).

Protocols (Reiteration and Additional Points)

- **TCP/IP:** Routable, used by major OSs.
- **IPX/SPX:** Routable, associated with NetWare.
- **NetBEUI:** Not routable, used on Windows networks.

Remote Access and Security Protocols

- **Remote Access Services (RAS):**

  - **Underlying Protocols:** PPP (Point-to-Point Protocol) and SLIP (Serial Line Internet Protocol).
  - **SLIP:** Lacks error checking and packet addressing; only for serial communications.
  - **PPP:** Offers security enhancements over SLIP, including encryption of usernames/passwords during authentication.

- **Application Access Protocols:**

  - **ICA (Independent Computing Architecture):** Allows clients to run server applications, transferring only the user interface, keystrokes, and mouse movements.

- **Security Protocols:**

  - **IPSec (Internet Protocol Security):** Encrypts data during communication. Operates at the Network Layer (Layer 3) and secures higher-layer protocols.
  - **SSL (Secure Sockets Layer):**
    Security protocol for the internet.
    - Secure websites use https://.
    - HTTPS connections typically use **port 443**.

  - **Kerberos:** Uses "tickets" as security tokens for authentication.

RAID (Redundant Array of Independent Disks)

- **RAID 0 (Striping):**

  - No fault tolerance.
  - Improves I/O performance.
  - Requires minimum of two disks.

- **RAID 1 (Mirroring):**

  - Provides fault tolerance.
  - Requires two disks.
  - **Disk Duplexing:** Uses separate disk controllers for each disk, adding redundancy.

- **RAID 5 (Striping with Distributed Parity):**

  - Requires minimum of three disks.
  - Uses one disk's capacity for parity calculations across all disks.

Backups

- **Full Backup:** Backs up all data. Does not use or clear the archive bit.
- **Incremental Backup:** Backs up data changed since the last full or incremental backup. Uses and clears the archive bit.
- **Differential Backup:** Backs up data changed since the last full backup. Uses the archive bit but does not clear it.

VLANs and NAS

- **VLANs (Virtual Local Area Networks):** Used to segment networks logically, often for organizational or security reasons.
- **NAS (Network Attached Storage):** Devices connected directly to the network for offloading data storage. Use SMB and NFS protocols.

Client Connectivity

- **NetWare Logon:** May require username, password, tree, and context.
- **Unix/Linux File Sharing:** Uses the NFS (Network File System) protocol.

Security: Physical, Logical, Passwords, and Firewalls

- **Strong Passwords:** Typically involve a combination of eight or more case-sensitive characters, including letters, numbers, and special characters.
- **Windows Permissions:** Include Full Control, Modify, Read & Execute, List Folder Contents, Read, Write.