Networking Basics Notes

Compiled by: Eman Elshimy

***Note:** The information presented in these notes is based on original content from Cisco's official learning resources. It has been paraphrased, summarized, and reorganized for educational and reference purposes.*

For the original content, refer to Cisco's Networking Basics Course.

This document has been compiled by: Eman Elshimy

Table of Contents

Introduction to the Network

1. Understanding Network Types

- The Internet is a global, decentralized collection of interconnected networks. No single owner.
- Local networks vary widely in size (2 to hundreds of thousands of devices).
    - SOHO (Small Office/Home Office) Networks: Connect a few local users, enabling shared resources (printers, documents) and often shared internet access.
    - Business Networks: Larger, supporting various organizational functions (sales, supply chains, communication) with centralized data. Also typically offer shared internet.
- Scale of networks:
    - Small home networks: a few computers connected.
    - Medium to large networks: corporations and schools, spanning multiple locations, thousands of devices.
    - Worldwide networks (The Internet): Links hundreds of millions of computers globally.
- IoT - Internet of Things:
    - Mobile devices: Smartphones, tablets, smartwatches, smart glasses (integrating communication, media, GPS, health tracking).
    - Connected home devices: Remotely monitored/configured items like security systems, smart appliances, smart TVs, gaming consoles.
    - Other connected devices which can be found outside the home, offering convenience or vital data. These include smart cars, RFID tags for tracking, environmental sensors, medical devices for vital sign monitoring.

2. Data Transmission Basics

- The Bit (Binary Digit) is the smallest unit of data (0 or 1) used by computers and networks.
    - Human input is converted to binary, and output is translated back.
    - ASCII: A common code representing characters using eight bits (ex: 'A' is 01000001).
    - Byte: A group of eight bits.
    - All digital information (text, graphics, audio, video) is represented in binary.
- Methods of data transmission (Signals over Media): Data is converted into various signal types for travel across physical or wireless links.
    - Electrical signals: Pulses over copper wires (common in homes/small businesses).
    - Optical signals: Light pulses over fiber-optic cables (used for longer distances, high reliability in larger networks).
    - Wireless signals: Infrared, microwave, or radio waves transmitted through the air (ex: Wi-Fi, often used in homes/small businesses).
- Types of personal data:
    - Volunteered data: Explicitly shared by individuals (ex: social media posts, direct inputs).
    - Observed data: Collected by monitoring actions (ex: GPS location from a phone).
    - Inferred data: Derived through analysis of volunteered and observed data (ex: credit scores, consumer preferences).

3. Bandwidth and Throughput

- Bandwidth represents the *maximum capacity* of a network medium to carry data.
    - Measured in bits per second (bps), often in Kilobits (Kbps), Megabits (Mbps), or Gigabits (Gbps).
    - Determined by physical properties of the media and current technology.
- Throughput is the *actual measured rate* of data transfer over a network medium during a specific time.
    - Throughput is almost always *less* than theoretical bandwidth due to factors like:
        - Data type and quantity.
        - Latency: The total time, including delays, for data to travel from source to destination.
    - Critical Rule: In a multi-segment network, the overall throughput is limited by the speed of the *slowest link* in the entire communication path.

Network Building Blocks

1. Clients and Servers

- Hosts is any device directly involved in network communication, capable of sending and receiving data. A host's role is defined by its software.
    - Servers: Hosts running specialized software to *provide* resources or information (ex: web pages, files, emails) to other hosts. Every online destination is supported by servers.
    - Clients: Hosts running software to *request* and display information from servers (ex: web browsers, email applications).
- Peer-to-Peer (P2P) Networks:
    - Concept: Computers act simultaneously as *both* clients and servers.
    - Setup can be as simple as 2 directly connected computers or involve multiple PCs via a switch.
    - Advantages: Easy to set up, less complex, lower cost (no dedicated servers needed), good for simple tasks like file sharing.
    - Disadvantages: No central control, generally less secure, not easily scalable. Performance can suffer if a device is heavily used as both client and server.
- P2P Applications: Software where each device involved acts as both a client and a server within the specific communication (ex: file-sharing apps). They often use a hybrid model: decentralized resource sharing but centralized indexing.
- Multiple Roles: A single server can serve many clients. A single computer can also run multiple server types (ex: file, web, email server) or multiple client types simultaneously.

2. Essential Network Components

- Network infrastructure is the underlying platform that provides a stable and reliable communication channel.
- Three main hardware categories:
    - End Devices (Hosts): User-facing devices that are the source or destination of network messages. Each host has a unique network address. Examples: Computers (workstations, laptops, servers), printers, phones, cameras, smartphones, tablets.
    - Intermediate Devices: Connect end devices and control the flow of data between them.
    - Network Media: The physical means by which signals are transmitted. Examples: Copper cables, fiber-optic cables, wireless frequencies (air).

3. Internet Service Provider (ISP) Connectivity

- ISP is the crucial link between a local network (home/small office) and the wider internet. ISPs themselves connect to form the "internet backbone" (high-speed fiber-optic networks).
- Common home/SOHO connection setup:
    - Most common and secure: A wireless integrated router. This device combines a switch (for wired connections), a wireless access point, IP addressing capabilities, and security features.
    - Direct modem-to-PC connection is generally insecure and discouraged.
- Primary high-speed SOHO options:
    - Cable Internet: Uses existing cable TV coaxial lines. Provides high-bandwidth, always-on connection. Requires a specialized cable modem.
    - DSL (Digital Subscriber Line): Uses existing telephone lines. High-bandwidth, always-on. Requires a special high-speed modem. Splits lines into voice, faster download, and slower upload channels. Performance depends on line quality and distance from the telephone company's central office.
- Other Connectivity Options:
    - Cellular: Internet via mobile phone networks. Convenient for mobility/remote areas but often has metered usage.
    - Satellite: Alternative for areas without cable/DSL. Requires dish with line of sight; generally good speeds but higher equipment/installation costs.
    - Dial-up Telephone: Very low bandwidth, uses any phone line and modem. Inexpensive but slow, only recommended as a last resort.
    - Direct Fiber-Optic Cables: Increasingly common in urban areas for very high bandwidth to homes/offices, supporting multiple services (internet, phone, TV).
- Choice Factors: Connectivity options depend on geographical location and available service providers.

Wireless and Mobile Network Connectivity

1. Smartphone Wireless Connections

- Smartphones use various wireless technologies beyond just cellular:
    - GPS (Global Positioning System): Uses satellite signals to pinpoint location (accurate within 10 meters).
    - Wi-Fi: Connects smartphones to local wireless networks and the internet. Requires being within range of an access point. Can be privately owned or public hotspots.
    - Bluetooth: Low-power, short-range technology (replaces wires for accessories). Used for devices like speakers, headphones, smartwatches. Transmits data and voice, forming small local networks. Supports multiple simultaneous device connections.
    - NFC (Near Field Communication): Enables data exchange over very short distances (centimetres). Uses electromagnetic fields. Commonly used for contactless payments.

2. Mobile Device Connectivity Management

- Mobile devices offer flexibility for work, learning, and communication.
- Wi-Fi connectivity benefits: Does not use cellular data allowance. Conserves battery (Wi-Fi radios use less power than cellular).

- Wi-Fi security precautions: Never send sensitive data (passwords) unencrypted. Use a VPN (Virtual Private Network) for sensitive data, especially on public Wi-Fi. Enable security on home Wi-Fi (ex: strong passwords). Use WPA2 or higher encryption for robust Wi-Fi security.
- Wi-Fi settings & configuration: Mobile OS (Android, iOS) allow Wi-Fi configuration. Devices typically auto-connect to known networks.
    - Manual Configuration: Needed if SSID (network name) is hidden or auto-connect is off. Requires entering SSID and passphrase.
- Cellular data settings: Cellular plans have data limits and costs. Users often prefer Wi-Fi to save cellular data.
    - Prioritization: Mobile devices automatically prioritize Wi-Fi if available; otherwise, they use cellular data (if enabled). Transitions are usually seamless.
    - *General On/Off:* Accessed via "Mobile Networks" or "Cellular Data" toggles in device settings.
- Simple connectivity with bluetooth:
    - Benefits: Wireless, automatic, very low power consumption.
    - Can connect up to eight devices simultaneously.
    - Common uses: Hands-free headsets, wireless keyboards/mice, car audio control, mobile speakers, tethering (sharing mobile internet with other devices via Bluetooth, Wi-Fi, or USB).
    - Bluetooth pairing:
        - Process to establish a connection between two Bluetooth devices for resource sharing.
        - Both devices must have Bluetooth enabled.
        - One device searches, the other must be in "discoverable" (visible) mode.
        - Authentication: Often requires a PIN or passcode.
        - Once paired, the PIN is stored for automatic future reconnections.
    - General pairing steps: Enable discoverable mode on one device, search from the other, select device, enter PIN (if required). Specific steps vary by device/OS.

Home Network Essentials

1. Home Network Fundamentals

- A typical home network connects various devices (computers, smartphones, smart TVs, printers, security cameras) to an integrated router, which then connects to an Internet Service Provider (ISP).
- Router components:
    - Ethernet/LAN Ports: Connect wired devices (like PCs, smart TVs) to the router's internal switch, putting them on the same local network.
    - Internet Port (WAN Port): The single port connecting the router to the ISP's modem (and thus, the internet). It's the only port on a different network by default.
    - Many home routers also include a built-in wireless access point and sometimes an integrated modem.

2. Network Technologies in the Home

- Wireless frequencies (LAN):
    - 2.4 GHz Band: Used by Bluetooth (low-speed, short-range, peripherals) and some Wi-Fi (IEEE 802.11) standards (ex: 802.11b/g/n).

    - 5 GHz Band: Used by newer Wi-Fi (IEEE 802.11) standards (ex: 802.11a/n/ac/ad) for higher speeds and range than Bluetooth.
- Wired network technologies: Best for applications needing dedicated bandwidth.
    - Ethernet protocol: Most common wired LAN protocol.
    - Wiring media examples:
        - Category 5e Cable (Cat 5e): Common for LAN, uses twisted pairs to reduce interference.
        - Coaxial Cable: Used for cable internet, has an inner wire surrounded by insulation and a shield.
        - Fiber-Optic Cable: High-bandwidth, long-distance transmission using light over glass/plastic strands.
    - Powerline: Technology to extend wired network connectivity over existing electrical outlets within a home.

3. Wireless Standards & Router Settings

- Standard organizations:
    - IEEE (Institute of Electrical and Electronics Engineers): Develops technical wireless standards (ex: IEEE 802.11 for WLANs, defining frequency, data rates).
    - Wi-Fi alliance: Certifies wireless devices for interoperability (indicated by the "Wi-Fi logo").
- Key wireless router settings:
    - Network mode selects the supported 802.11 standard (ex: 802.11n, 802.11ac, or Mixed Mode).
    - Mixed mode allows older devices to connect but might slow down newer ones.
    - Network Name (SSID - Service Set Identifier): The name of your wireless network (case-sensitive, up to 32 characters). All devices must use the same SSID to connect.
    - Standard channel: Usually "Auto" allows the router to select the best channel.
    - SSID broadcast: Determines if the network name is visible. Disabling it is NOT a sufficient security measure. Always use strong encryption like WPA2/WPA3.

Network Communication Principles

1. Communication Protocols

- These are agreed-upon rules that govern conversations and ensure successful message delivery and understanding between devices.
- Key agreements for network communication:
    - Message Format: Specific structure for different message types.
    - Message Size: Rules for data segment sizes; large messages are often broken down.
    - Timing: Controls transmission speed, when a host can send, and amount of data per transmission.
    - Encoding: Conversion of messages into transmittable patterns (ex: electrical impulses) and decoding by the receiver.
    - Encapsulation: Adding header information (source/destination addresses) to data segments for proper delivery.
    - Message Pattern: Defines communication flow (ex: request/response requiring acknowledgment, or simple streaming without confirmation).

2. Communication Standards

- Essential for managing network complexity and ensuring consistent, reliable service delivery across diverse devices and technologies. A standard provides a consistent "how-to."
- Involves a process of discussion, problem-solving, and testing.
    - Request for Comments (RFC) Documents: Records each stage of a new standard's development.
    - Internet Engineering Task Force (IETF): Organization that publishes and manages RFCs for internet standards.
    - Other Supporting Organizations: IEEE, ICANN, ITU-T.

3. Network Communication Models

- Layered Models: Conceptual frameworks that simplify understanding of how different protocols work together.
    - Benefits: Aids protocol design, fosters vendor competition, allows independent technology changes per layer, provides a common language for network functions.
- The TCP/IP Model (Internet Model):
    - Defines four functional categories, reflecting the TCP/IP protocol suite structure.
    - Layers (Top to Bottom):
        - Application Layer: Interacts with user applications, handles data representation, and dialogue control (ex: HTTP, FTP, DNS).
        - Transport Layer: Manages end-to-end communication between different devices across networks, including reliability and flow control (ex: TCP, UDP).
        - Internet Layer: Determines the best path for data packets through the network (ex: IP).
        - Network Access Layer: Controls hardware devices and media for network access (combines physical and data link functions).
- The OSI (Open Systems Interconnection) Reference Model:
    - A widely recognized, more theoretical internetwork reference model (developed by ISO).
    - Layers (7 - Top to 1 - Bottom):
        - 7. Application: Protocols for direct user application communication.
        - 6. Presentation: Ensures common data representation between applications.
        - 5. Session: Manages and synchronizes dialogue between applications.
        - 4. Transport: Segments, transfers, and reassembles data between end devices.
        - 3. Network: Handles logical addressing and routing of packets between identified end devices.
        - 2. Data Link: Manages physical addressing and data frame exchange over common media (ex: Ethernet, Wi-Fi MAC addresses).
        - 1. Physical: Describes mechanical and electrical means for physical connection activation/maintenance/deactivation for raw data bit transmission.
- Comparison of OSI and TCP/IP Models:
    - Similarities/Direct Mappings:
        - TCP/IP Transport Layer ↔ OSI Layer 4 (Transport) - both handle reliable data delivery.
        - TCP/IP Internet Layer ↔ OSI Layer 3 (Network) - both manage addressing and routing.
    - Differences/Layer Combinations:
        - TCP/IP Network Access Layer combines OSI Data Link (L2) and Physical (L1).

        - TCP/IP Application Layer combines OSI Session (L5), Presentation (L6), and Application (L7).
    - Usage: Both models are used for discussing protocols. OSI is often preferred for more detailed discussions of lower layers (Data Link and Physical) due to its granular separation.

Network Media Types

1. Twisted-Pair Cable

- Consists of insulated copper wires grouped into pairs, which are then twisted together. Each pair typically has a solid-colored wire and a matching striped wire for identification.
- The twisting of wire pairs is crucial for reducing electrical interference (crosstalk and electromagnetic interference), which helps maintain signal quality and integrity.
- Primary use: The most common type of cabling for Ethernet-based Local Area Networks (LANs).
- Example: Category 5e (Cat 5e) is a widely used type, typically containing four twisted pairs.

2. Coaxial Cable

- Features a central, rigid copper conductor. This conductor is surrounded by an insulating layer, which is then covered by a braided metal shield (for noise reduction) and finally an outer protective jacket.
- Designed to carry high-frequency or broadband electrical signals.
- Common Applications:
    - Used extensively by cable television providers for delivering both internet and TV services.
    - Connects components in satellite communication systems.

3. Fiber-Optic Cable

- Made from very thin strands of glass or plastic, comparable in diameter to a human hair.
- Transmits digital information using pulses of light, not electricity.
- Key advantage: Immune to electrical interference because it transmits light signals.
- Capable of transmitting digital data at exceptionally high speeds over very long distances.
- Offers extremely high bandwidth, enabling the transmission of vast amounts of data simultaneously.
- Beyond networking, it's used in medical imaging, treatment, and mechanical engineering inspection.
- Common networking uses:
    - Network backbones (high-capacity connections between major network segments)
    - Large enterprise networks
    - Large data centres
    - Primary medium for long-distance and high-capacity links used by telephone companies

Encapsulation and Ethernet Framing

1. Ethernet Frame Components

- Ethernet is the most common technology used for Local Area Networks (LANs).
- Network Interface Card (NIC): Hardware that allows a device to connect to an Ethernet LAN.

- MAC Address (Media Access Control Address): A unique, physical address permanently embedded in each Ethernet NIC.
- Ethernet frame is the basic unit of data transmitted over an Ethernet network. It includes both the source and destination MAC addresses as key fields.

2. Encapsulation: The Packaging of Data

- Encapsulation is the process of embedding one message format (the data) inside another (the frame).
- Ensures messages are correctly formatted, addressed, and can be understood and processed by the receiving device. Incorrectly formatted messages are typically discarded.
- De-encapsulation is the reverse process where the recipient removes the data from its outer frame.
- Frame functionality: A frame serves as a container, holding essential information like the address of the intended destination host and the address of the source host.
- Frame characteristics: The specific format and content of a frame are determined by the type of message being sent and the communication medium/channel used for transmission.
- Network example - Internet Protocol (IP):
    - IP acts like another "envelope" layer.
    - An IP packet (ex: IPv4 or IPv6) contains source and destination IP addresses.
    - IP's primary role is to deliver the message from its origin to its final destination across multiple networks.

IPv4 Addressing & Network Segmentation

1. Purpose and Format of IPv4 Addresses

- An IPv4 address is essential for a host to connect to the internet and most local networks.
- It's a logical network address that uniquely identifies a host.
- Must be unique within the local network for local communication and unique globally for internet communication.
- Assigned to a network interface connection (ex: NIC on a workstation, server, printer, IP phone). Routers also have IPv4 addresses on their interfaces.
- Every internet packet contains both a source and destination IPv4 address for routing.
- IPv4 Format (Octets and Dotted-Decimal):
    - 32 bits long. Grouped into four 8-bit bytes (octets).
    - Each octet is converted to its decimal value, separated by dots (ex: 209.165.200.1).

2. IPv4 Address Structure

- Two logical parts:
    - Network portion: Identifies the specific network the host belongs to.
    - Host portion: Uniquely identifies a device within that network.
- Subnet mask: A 32-bit value (in dotted-decimal format) that works with the IPv4 address to determine which bits are for the network and which are for the host.
    - 1s in the subnet mask indicate the network portion.
    - 0s in the subnet mask indicate the host portion.
    - *Ex:* 255.255.255.0 for 192.168.1.100 means the first three octets are network, the last is host.

- Special IPv4 addresses within a network:
  - Network address: All host bits are 0. Represents the entire network; cannot be assigned to a host. *Ex:* 192.168.1.0 for /24.
  - Broadcast address: All host bits are 1. Packets sent here reach all hosts on that local network segment; cannot be assigned to a host. *Ex:* 192.168.1.255 for /24.
  - Host addresses: All valid addresses between the network and broadcast addresses that *can* be assigned to devices. *Ex:* 192.168.1.1 to 192.168.1.254 for /24.
- Classless Inter-Domain Routing (CIDR) notation: A shorthand for the subnet mask, indicating the number of network bits with a prefix length (ex: /24).

3. Important Info

- Always remember an IPv4 address has a network and host portion, defined by the subnet mask.
- Network and Broadcast addresses are special and cannot be assigned to individual devices.
- CIDR significance: /XX notation simplifies indicating the network portion's length.
- Connectivity rule: For direct communication on the *same local network*, hosts *must* share the same network address (same network portion of IP and subnet mask).

IPv4 Communication Types & Network Segmentation

1. IPv4 Communication Types

- IPv4 Unicast (One-to-One):
  - Definition: Packet sent from a single source to a single, specific destination.
  - Use: Most common traffic (web Browse, file transfer).
  - Addressing: Destination IP is the unique address of the target device.
- IPv4 Broadcast (One-to-All):
  - Definition: Packet sent from one source to *all* other hosts on the same local network segment (broadcast domain).
  - Addressing: Uses a special broadcast IP address.
  - Routing: Routers *do not* forward broadcast packets to other networks.
  - Common Uses: DHCP (for IP address discovery), ARP (for MAC address resolution). *Example:* A host sends a DHCP Discover broadcast to find a DHCP server.
- IPv4 Multicast (One-to-Many):
  - Definition: Packet sent from a source to a *selected group* of subscribed destination hosts (a multicast group).
  - Membership: Devices must explicitly join a multicast group to receive its traffic.
  - Addressing: Identified by a unique IPv4 multicast destination address.
  - Common Uses: Streaming media, video conferencing, some routing protocols (ex: OSPF uses 224.0.0.5 for router communication).

2. Types of IPv4 Addresses (Categories)

- Public IPv4 Addresses:
  - Globally routable on the internet.
  - Required for direct internet accessibility.

    - IPv4 exhaustion led to private addresses and IPv6.
- Private IPv4 addresses:
    - Not routable on the internet (internet routers drop them).
    - Reserved for use within private networks (home, internal organization networks).
    - Common ranges:
        - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
        - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
        - 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)
    - Network Address Translation (NAT) allows multiple private IPs to share a single public IP for internet access.
- Loopback address (127.0.0.1):
    - Refers to the device itself.
    - Used for testing a device's own TCP/IP configuration or troubleshooting software without sending traffic onto the physical network. *Ex:* ping 127.0.0.1.
- Link-Local Address (APIPA - Automatic Private IP Addressing):
    - Range: 169.254.0.0 - 169.254.255.255 (169.254.0.0/16).
    - Automatically assigned by OS (ex: Windows) when a device can't get an IP from DHCP.
    - Only allows communication with other devices on the *same local segment* that also have APIPA addresses. Not routable.
    - Troubleshooting: Indicates a DHCP or network connectivity problem.
- TEST-NET Addresses (192.0.2.0/24):
    - Reserved for documentation, examples, and testing.
    - Should *not* be used on public or production private networks.

3. Network Segmentation

- Dividing a large network into smaller, isolated sub-networks to improve performance and security.
- Broadcast Domain: A network segment where all devices receive all broadcast traffic.
- Broadcast domains issue: Too many broadcasts consume bandwidth and slow down network/device performance.
- Routers act as boundaries for broadcast domains; they *do not* forward broadcast packets between different networks. This is key to segmentation.
- Advantages of segmentation:
    - Performance improvement: Reduces broadcast traffic in each segment, leading to better overall network speed.
    - Security enhancement: Isolates network segments, limiting the spread of breaches and allowing granular control over traffic flow and access rights.
- Subnetting:
    - This is the logical division of a larger network into smaller sub-networks (subnets).
    - Achieved by "borrowing" bits from the host portion of an IP address to create more network bits.
    - Benefits include efficient IP address usage, reduced broadcast traffic, improved security, and easier network management.

IPv6 Addressing and Transition

1. Why IPv6? (IPv4 Issues)

- Primary reason: The exhaustion of available IPv4 addresses.
- IPv6 design: The successor to IPv4, offering a vastly larger 128-bit address space (trillions of addresses).
- Includes improvements over IPv4, like better address resolution and autoconfiguration through ICMPv6.

2. IPv6 Transition Mechanisms

- Methods enabling IPv4 and IPv6 networks/devices to coexist and communicate.
- Dual Stack:
    - Concept: A device (or network) runs both IPv4 and IPv6 protocols simultaneously.
    - Ideal scenario: Considered "native IPv6" when a customer network has a direct IPv6 connection to its ISP, allowing direct IPv6 internet access.
    - Benefit: Devices can use the available protocol for communication, ensuring seamless coexistence.
- Tunneling:
    - Concept: Encapsulating an IPv6 packet inside an IPv4 packet to travel across an IPv4-only network.
    - Use case: Allows "IPv6 islands" to communicate over existing IPv4 infrastructure.
- Translation (NAT64):
    - Concept: Similar to IPv4 NAT, it translates IPv6 packets to IPv4 and vice-versa.
    - Enables communication between IPv6-only and IPv4-only devices.
    - While tunneling and translation are crucial for transition, the ultimate goal is native end-to-end IPv6 communication.

Dynamic Addressing with DHCP

1. Static IPv4 Assignment:

- Method: Manual configuration of IP address, subnet mask, default gateway, and DNS server(s) by a network administrator.
- Required Info: IP address, subnet mask, default gateway (router's IP), DNS server(s).
- Typical use: Reserved for network infrastructure devices that need fixed addresses (servers, printers, routers, switches).
- Disadvantages: Time-consuming for many hosts, prone to errors (ex: duplicate IPs).

2. Dynamic IPv4 Assignment:

- Method: Most client devices (PCs, smartphones) obtain their IP configuration automatically.
- Protocol: Dynamic Host Configuration Protocol (DHCP) is used for automatic IP address leasing and parameter assignment. When a device connects, it requests an IP from a DHCP server, which leases an address from its pool.

- Advantages: Reduces administrative effort, prevents IP conflicts, simplifies network management (especially in large or dynamic environments).

Network Gateways

1. Router Roles: Gateways and Boundaries

- Routers as gateways: Routers enable communication *between* different networks.
    - Each router interface connects to a unique network and has an IP address identifying that network.
    - All devices within a network must know their router's IP address (the default gateway) to send traffic outside their local network.
    - The default gateway can be set manually (static) or automatically by DHCP.
    - Wireless routers often act as DHCP servers, automatically providing their own internal IP as the default gateway to connected devices, enabling internet access.
- Routers as network boundaries: A wireless router functions as a DHCP server for all connected local devices (both wired and wireless), which are considered part of the "internal" or "inside" network.
    - Most DHCP servers assign private IPv4 addresses to internal devices. These IPs are not routable on the internet, meaning they can't be directly accessed from outside, which enhances security.
    - The router's internal interface usually takes the first available host IP in the private network range (ex: 192.168.1.1).
    - The router's external (internet-facing) interface typically obtains a public, internet-routable IP address from the ISP (often via DHCP client mode).
    - This setup positions the wireless router as the demarcation point between the private local network and the public internet.

2. Network Address Translation (NAT) Overview

- NAT is vital for allowing devices with private IP addresses to communicate on the public internet.
- When inspecting a wireless router's configuration, you'll see the internal network uses private IP addresses (ex: 192.168.x.x, 10.x.x.x, 172.16-31.x.x).
- Since private addresses cannot traverse the internet, NAT must translate them to the router's single public IP address when traffic goes out, and vice-versa for incoming traffic.
- In network simulations, you can observe a packet's source IP address change from a private internal IP to the router's public external IP as it crosses the router to access an internet server.

Address Resolution Protocol (ARP)

1. MAC and IP Addresses: The Resolution Process

- Address Resolution: The core process by which a device determines the MAC (physical) address of another device when it only knows its IP (logical) address.
- Two Key Addresses per Device (on Ethernet):
    - MAC Address: A unique hardware identifier. Used for direct communication between network interfaces on the *same local network segment*.

    - IP Address: A logical identifier used for host identification and routing packets *across different networks*.
- Key Distinction: ARP performs this resolution for IPv4. For IPv6, a similar function is handled by ICMPv6 Neighbor Discovery (ND).
- Communication within the Same Local Network:
    - When a source sends a packet to a destination *on the same local network*:
        - The Ethernet frame's destination MAC address will be the actual MAC address of the target device.
        - The IP packet's source and destination IP addresses remain the original sender's and receiver's IPs.
    - *Example:* PC1 (IP 192.168.10.10, MAC aa-aa) sending to PC2 (IP 192.168.10.11, MAC 55-55) on the same network. The Ethernet frame's destination MAC is 55-55.
- Communication to a Remote Network:
    - When the destination IP address is on a *different (remote) network*:
        - The Ethernet frame's destination MAC address will be the MAC address of the local router's interface (the default gateway).
    - Router's Forwarding Process:
        - A router receives an Ethernet frame, removes its Layer 2 (Ethernet) information.
        - It then examines the Layer 3 (IP) destination address to determine the next best path.
        - The router then re-encapsulates the IP packet into a *new* Layer 2 frame, using the data link technology of the *outgoing* interface.
        - Crucial Point (Exam): Layer 2 (MAC) addresses change at *every router hop* to reflect the next device in the path. Layer 3 (IP) addresses remain constant from the original source to the final destination.

2. Broadcast Management and the ARP Process Detail

- Broadcast domains:
    - A broadcast domain is the area of a network where all devices can receive broadcast messages.
    - All devices on the same Layer 2 network segment are in the same broadcast domain.
    - Routers act as boundaries for broadcast domains. By default, they do not forward broadcasts to other networks. This "broadcast containment" improves network efficiency and security.
    - Switches forward broadcasts out all ports within the same VLAN (except the incoming port).
- The ARP Process (Address Resolution Protocol): Essential for IPv4 Ethernet devices to find the MAC address of a *local* device given its IPv4 address.
    - How it Works (ARP Request):
        - A source device checks its ARP table (cache) for the destination's MAC.
        - If not found, it sends an ARP request.
        - An ARP request is a Layer 2 broadcast (destination MAC FF-FF-FF-FF-FF-FF) containing the target IP address.
        - All devices on the local segment receive this request.
    - How it Works (ARP Reply):
        - Only the device whose IP matches the target IP in the request sends an ARP reply.
        - The ARP reply is a Layer 2 unicast message (sent directly to the source), containing the target's MAC address.
    - ARP Table (Cache):

        - Hosts and routers maintain an ARP table to store dynamically learned IP-to-MAC mappings.
        - Entries are temporary (typically a few minutes) and expire if not used.
        - Entries can also be added statically.
        - Commands (Windows): arp -a to view, arp -d to delete an entry.
    - Benefit: The ARP cache reduces the number of broadcast messages, improving network efficiency.

Inter-Network Routing

1. The Routing Table

- Routers are essential for moving IP packets between different networks. They rely on their routing table to make intelligent forwarding decisions.
- Packet forwarding steps by a router:
    - Incoming packet processing: A router first confirms the incoming Ethernet frame's destination MAC address matches its own. It then removes the Layer 2 (Ethernet) header/trailer to access the Layer 3 (IP) packet.
    - Destination IP check: The router examines the destination IP address in the IP packet header.
    - Route lookup: It consults its routing table to find the most efficient path to the destination network.
    - Outgoing packet preparation: Once a path is identified, the router re-encapsulates the IP packet into a *new* Layer 2 frame, specifically formatted for the technology of the *outgoing* interface (ex: Ethernet).
    - Forwarding to next hop: The new Layer 2 frame includes the MAC address of the next device in the path (another router or the final destination host) as its destination MAC.
- During this entire process, the Layer 3 (IP) source and destination addresses remain unchanged. Only the Layer 2 (MAC) addresses are modified at each router hop as the packet traverses different network segments.

2. Types of Router Paths (Routing Table Entries)

- The routing table is a database within a router that stores information about how to reach various networks. There are three primary types of route entries:
    - Directly connected networks:
        - These are networks that are physically connected to one of the router's active interfaces.
        - The router automatically adds these entries to its table when an interface is configured and becomes operational.
    - Remote networks:
        - Networks that are not directly attached to the router.
        - Routers learn about these in two ways:
            - Static routes: Manually entered by a network administrator. These are fixed paths.
            - Dynamic routes: Learned automatically by routers that exchange information using dynamic routing protocols (ex: OSPF, EIGRP, RIP).

    - Default route (gateway of last resort):
        - A special "fallback" route used when a router receives a packet for a destination network that is *not explicitly listed* in its routing table.
        - It acts as a "catch-all," directing traffic to a specific next-hop router (often the one providing internet access).
        - A router will utilize a default route if it has no more specific route for the packet's destination network.
- On a Windows computer, you can inspect the routing table using command-line tools:
    - netstat -r: Displays active network connections and the routing table.
    - route print: Specifically shows the IP routing table.

3. Local Area Networks (LANs)

- A LAN refers to a local network, or a collection of interconnected local networks, all operating under the same administrative control.
- Historically, LANs were small, single-location networks. Today, they can span multiple buildings and encompass hundreds of devices, as long as they remain under one central administration.
- Key characteristics:
    - Operate under single administrative control.
    - Typically use Ethernet or wireless (Wi-Fi) protocols.
    - Support high data rates.
- Intranet: A common term for a private LAN that belongs to an organization, accessible only by authorized members (employees, etc.).

4. Network Segment Design - Single vs. Multiple Segments

- How hosts are placed on a network (single or multiple segments) depends on desired network outcomes.
- All hosts in one local segment (single broadcast domain): All devices reside on a single local network, sharing one broadcast domain. Hosts use ARP to discover each other.
    - Advantages: Simpler network design, lower cost. Devices are easily "seen" by others. More direct and potentially faster data transfer. Easier device access.
    - Disadvantages: Larger broadcast domain leads to more broadcast traffic, potentially slowing network performance as it grows. Harder to implement Quality of Service (QoS). More challenging to enforce granular security.
- Hosts on remote segments (multiple broadcast domains): Dividing hosts across multiple networks, connected by a router (a "distribution layer device"). This creates separate broadcast domains.
    - Advantages: More suitable for larger, complex networks. Splits broadcast domains, reducing overall traffic impact on individual segments. Can improve performance within each segment. Increases invisibility of machines across different segments (improves security). Better network organization. Enhanced security control.
    - Disadvantages: Requires routing, adding complexity. Routers can introduce latency (delay) when traffic crosses segments. Higher complexity and cost (due to router requirement).

Transport Layer Port Numbers & netstat

1. Port Numbers - Identifying Services

- When data is sent using TCP or UDP, port numbers are used to identify specific services or applications at the destination and to keep track of individual conversations.
- Every message (segment) sent by a host contains both a source port and a destination port.
- How it works: Applications like HTTP, SMTP, and DNS use specific destination port numbers.
    - For example:
        - HTTP (web traffic) commonly uses Port 80 (TCP).
        - SMTP (email sending) commonly uses Port 25 (TCP).
        - DNS (domain name resolution) commonly uses Port 53 (UDP) for client requests (and TCP for server-to-server communication).
- Some applications can use both TCP and UDP depending on the specific function.

2. Socket Pairs

- Encapsulation: Source and destination port numbers are placed in the Transport Layer segment, which is then encapsulated within an IP packet (containing source and destination IP addresses).
- A socket is the combination of an IP address and a port number.
    - *Example Client Socket:* 192.168.1.5:1099 (IP:Port)
    - *Example Server Socket:* 192.168.1.7:80 (IP:Port)
- Socket pair: The combination of the source socket and the destination socket.
    - *Example Socket Pair:* 192.168.1.5:1099, 192.168.1.7:80
- Sockets allow:
    - Multiple applications/processes on a client to maintain distinct connections.
    - Multiple connections to a single server process to be uniquely distinguished.
- The source port acts as a return address for the client application. The Transport Layer uses this to direct responses back to the correct application on the client.

3. The netstat Command

- netstat is a crucial network utility used to view active TCP connections and other network statistics on a host. It helps identify unexplained connections which could be security risks. Output information:
    - Protocol (Proto): ex: TCP
    - Local address and port: Local Address (your computer's IP:Port)
    - Foreign address and port: Foreign Address (remote computer's IP:Port)
    - Connection state: State (ex: ESTABLISHED, LISTEN, TIME_WAIT)
- Example output:

```
Proto  Local Address          Foreign Address        State
TCP    192.168.1.124:3126     192.168.0.2:netbios-ssn   ESTABLISHED
TCP    192.168.1.124:3158     207.138.126.152:http      ESTABLISHED
```

- By default, netstat tries to convert IP addresses to domain names and port numbers to well-known application names (ex: http for port 80).
- -n Option: Use netstat -n to display IP addresses and port numbers in their numerical form only, without name resolution.

Application Layer Services

1. Client-Server Interaction

- Everyday internet services rely on complex interactions between clients (requesting devices/software) and servers (providing information/services). This interaction is enabled by agreed-upon standards and protocols.
- A server is a host running software that delivers information or services to other network hosts. Examples include web, email, and file servers.
- Client software, such as web browsers (ex: Chrome, Firefox) or email clients (ex: Microsoft Outlook), allows users to access server services. A single computer can run various client software simultaneously.
    - Email server: Manages and stores emails for user mailboxes, accessed by clients like Outlook.
    - Web server: Hosts web pages accessed by client browsers.
    - File server: Centralized storage for corporate and user files, accessed by client software like File Explorer.

2. Uniform Resource Identifiers (URIs)

- A URI is a character string that identifies a specific network resource, including web resources and RESTful APIs.
- Specializations of URI:
    - Uniform Resource Name (URN): Identifies the resource's name or namespace, without specifying its network location or how to access it.
    - Uniform Resource Locator (URL): Defines the network location of a resource. URLs typically use protocols like HTTP, HTTPS, FTP, or SFTP. For example, https://www.example.com is a URL.
- Parts of a URL:
    - Protocol/Scheme: ex: HTTPS, FTP, SFTP, mailto, NNTP.
    - Hostname: ex: www.example.com.
    - Path and file name: ex: /author/book.html.
    - Fragment: ex: #page155.

3. Key Network Application Services

- Many common internet services rely on protocols from the TCP/IP suite for reliable client-server communication.
- Common protocols and services:
    - Domain Name System (DNS): Translates human-readable internet names (like www.example.com) into IP addresses.
    - Secure Shell (SSH): Provides secure remote access to servers and networking devices.
    - Simple Mail Transfer Protocol (SMTP): Used by email clients to send messages to local email servers, and between email servers to deliver mail.
    - Post Office Protocol (POP): Used by email clients to retrieve emails and attachments from a server. By default, messages are downloaded and removed from the server.
    - Internet Message Access Protocol (IMAP): Used by email clients to retrieve emails, but unlike POP, it keeps messages on the server unless explicitly deleted by the user.

- Dynamic Host Configuration Protocol (DHCP): Automatically configures network devices with IP addressing information for communication.
- Hypertext Transfer Protocol (HTTP): Used by web browsers to request and retrieve web pages and their associated files from the World Wide Web.
- File Transfer Protocol (FTP): Facilitates interactive file transfers between systems.

4. Domain Name System (DNS) Operations

- DNS servers are critical for resolving domain names into IP addresses, which is essential for devices to connect to internet resources.
- Configuration:
  - DNS server addresses are included when manually configuring network connectivity for a device.
  - In home networks, DHCP (Dynamic Host Configuration Protocol) on the router typically handles this. The ISP provides the DNS server address to the router, which then uses DHCP to send this configuration to connected devices.
- nslookup command is used to manually query DNS servers and discover the IP addresses associated with any domain name.

5. Web Communication: HTTP and HTTPS

- HTTP (Hypertext Transfer Protocol): When a web client has a web server's IP address, it uses HTTP on port 80 to request web services. The server then responds by sending the requested web page back to the client.
- HTML (HyperText Markup Language): Web page content is encoded using markup languages, primarily HTML, which instructs the browser on how to format the page, including graphics and fonts.
- HTTPS (HTTP Secure): HTTP is inherently insecure as data is sent as plaintext, making it vulnerable to interception. For secure communication, HTTP is combined with secure transport protocols, forming HTTPS. HTTPS requests are sent to port 443 and use https in the site address.

6. File Transfer Protocol (FTP)

- FTP is a widely used service for transferring files between computers. An FTP client can access an FTP server to perform various file management tasks, including uploading, downloading, deleting, and renaming files.
- Dual port usage: FTP utilizes two separate ports for client-server communication:
  - Control Connection (Port 21 TCP): Used to send commands and manage the FTP session.
  - Data Connection (Port 20 TCP): Used for the actual transfer of data files once the session is established.
- FTP client software is often built into operating systems and web browsers. Dedicated GUI-based FTP clients also offer advanced features.

7. Remote Terminal Access: Telnet vs. SSH

- Telnet: Developed in early 1970s, Telnet is one of the oldest application layer protocols used to emulate text-based terminals over a network, allowing remote access to command-line interfaces (CLIs).
  - Port: Telnet servers listen for client requests on TCP port 23.

    - Telnet is not considered a secure protocol because all data, including login credentials, is transmitted in plaintext, making it vulnerable to interception and easy understanding.
- Secure Shell (SSH): SSH is the preferred and secure alternative to Telnet for remote access.
    - SSH provides secure remote login and other network services through stronger authentication and encryption of session data, protecting it from interception.

8. Email and Messaging Services

- Email is a popular client-server application where email servers store mail for users, and email clients are used to access and read messages. Email addresses follow the user@company.domain format.
- Email Protocols:
    - SMTP (Simple Mail Transfer Protocol):
        - Used by email clients to send messages to their local email server.
        - Also used between email servers to transfer messages to destination servers.
        - SMTP requests are sent to port 25.
    - POP3 (Post Office Protocol version 3):
        - Clients connect to POP3 servers (on port 110) to download messages.
        - By default, messages are typically removed from the server after being downloaded by the client.
    - IMAP4 (Internet Message Access Protocol version 4):
        - Clients connect to IMAP4 servers (on port 143) to retrieve messages.
        - Unlike POP, IMAP keeps messages on the server unless the user explicitly deletes them, allowing multiple clients to access the same mailbox.
- Text messaging: Enables real-time communication over the internet, also known as instant messages, direct messages, or chat messages.
    - Often accessed via web-based clients integrated into social media sites or standalone applications like WhatsApp, Microsoft Teams, or Cisco Webex Teams.
    - These services support not only text but also document, video, music, and audio file transfers.
- Internet Phone Calls (VoIP): Uses Voice over IP (VoIP) technology to convert analog voice signals into digital data, which is then encapsulated into IP packets for transmission over the network.
    - Allows calls to other users of the same service or, via a gateway, to the Public Switched Telephone Network (PSTN) for landlines and cell phones (which may incur charges).
    - Protocols and ports vary depending on the specific VoIP software used.

Network Testing Utilities

The ipconfig command is a crucial tool for viewing and managing a host's IP configuration, essential for network troubleshooting.

- ipconfig (Basic): Displays fundamental IP configuration details.
    - Output: Shows the IP address, subnet mask, and default gateway for active network adapters (ex: Wi-Fi, Ethernet). Example output:

```
Wireless LAN adapter Wi-Fi:
  IPv4 Address. . . . . . . . . . . : 10.10.10.130
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 10.10.10.1
```

- ipconfig /all: Provides comprehensive IP configuration information, aiding deeper troubleshooting.
    - Additional output includes:
        - MAC address (Physical Address) for each adapter.
        - DHCP Enabled status (Yes/No).
        - DHCP Server IP address (if DHCP is enabled).
        - DNS Servers' IP addresses.
        - IP lease information (Obtained and Expires times).
        - Host Name, Node Type, etc.
    - Troubleshooting aid: Vital for diagnosing connectivity issues (ex: incorrect IP, missing DNS server info, or DHCP problems). A host needs proper IP settings and DNS server locations to communicate effectively.
- ipconfig /release and ipconfig /renew (DHCP Lease Management)
    - Applied when IP addressing is obtained dynamically via DHCP.
    - ipconfig /release: Releases the current IP address and configuration back to the DHCP server.
        - The host will no longer have an IPv4 address.
        - Effect: Disconnects the host from its current IP configuration.
    - ipconfig /renew: Requests a new IP address and configuration from the DHCP server.
        - Useful for fixing faulty or outdated IP configuration information. A successful renewal can restore network connectivity.
    - Post-Release/Renew Troubleshooting:
        - If renew fails, check physical network connectivity (ex: adapter's link light).
        - If physical connection is good, the issue might be with the DHCP server or network path to it.