Chapter 1:

Internet, Intranet and Extranet

- **Internet**: A global network that connects millions of private, public, academic, business, and government networks. It's open to anyone and allows access to a vast range of information and services worldwide.
- Generally, less secure; relies on individual users and organizations to implement security measures.

  Examples: Websites, email, and social media platforms.
- **Intranet**: A private network accessible only to an organisation's members, employees, or others with authorization. It uses internet technologies (like web pages and browsers) but is restricted to internal use for sharing company information.
- More secure; controlled access and internal security measures.

  Examples: Internal websites, company portals, and HR systems.
- **Extranet**: An extension of an intranet that allows controlled access to outsiders, such as partners, vendors, or clients. It's used for collaboration and information sharing between the organisation and external stakeholders.
- Secure but requires careful management of external access.

Key Differences:

- **Scope**: Internet is global; Intranet is internal; Extranet is semi-private (internal + authorized external users).
- **Access**: The Internet is public; the Intranet is restricted to a specific organisation; the Extranet is limited to external collaborators with permission.

Network types

- **LAN (Local Area Network)**: A network that covers a small geographic area, like a home, office, or building. Devices within a LAN are connected and can share resources.
  Example: Computers in an office connected via Ethernet.
- **PAN (Personal Area Network)**: A network for personal devices within a short range, typically within a few meters. It connects devices like phones, tablets, and laptops.
  Example: Bluetooth connection between a smartphone and a wireless headset.
- **CAN (Campus Area Network)**: A network that spans multiple buildings within a campus, like a university or corporate campus. It connects various LANs within the campus.
  Example: A university's network connecting different departments and buildings.
- **MAN (Metropolitan Area Network)**: A network that covers a city or large campus. It's larger than a LAN but smaller than a WAN and connects various LANs within a metropolitan area.
  Example: Citywide Wi-Fi network.
- **WAN (Wide Area Network)**: A network that spans a large geographic area, such as a country or continent. WANs connect multiple LANs and MANs and are used by businesses and governments.
  Example: The internet is the largest WAN, connecting networks worldwide.

Key Differences:

- **Size/Scope**:
  - **LAN**: Small (building or office).
  - **PAN**: Very small (personal space).
  - **CAN**: Medium (campus or group of buildings).
  - **MAN**: Large (city or region).
  - **WAN**: Very large (across cities, countries, or globally).
- **Use Case**:
  - **LAN**: Local resource sharing.
  - **PAN**: Personal device connections.
  - **CAN**: Organizational network across buildings.
  - **MAN**: Citywide services.

- **WAN**: Long-distance networking.

TCP/OSI Model

OSI Model (Open Systems Interconnection Model)

The OSI model is a conceptual framework used to understand and implement network communications between different systems. It divides the communication process into seven layers, each with specific functions.

1. **Layer 7: Application**
   Provides network services directly to user applications (e.g., web browsers, email).
   Example: HTTP, FTP, SMTP.
2. **Layer 6: Presentation**
   Translates data between the application layer and the network (e.g., encryption, compression).
   Example: SSL/TLS, JPEG, MPEG.
3. **Layer 5: Session**
   Manages and controls the connections (sessions) between computers.
   Example: RPC (Remote Procedure Call), NetBIOS.
4. **Layer 4: Transport**
   Ensures end-to-end communication, reliability, and error recovery.
   Example: TCP, UDP.
5. **Layer 3: Network**
   Routes data between devices across different networks.
   Example: IP, ICMP.
6. **Layer 2: Data Link**
   Handles error detection and correction in the physical transmission of data. It includes sub-layers: MAC (Media Access Control) and LLC (Logical Link Control).
   Example: Ethernet, Wi-Fi.
7. **Layer 1: Physical**
   Concerned with the transmission of raw bits over a physical medium (e.g., cables, radio waves).
   Examples: USB, Ethernet cables, fibre optics.

TCP/IP Model (Transmission Control Protocol/Internet Protocol Model)

The TCP/IP model, also known as the Internet protocol suite, is a more practical model and the basis for the Internet. It has fewer layers than the OSI model and is more focused on the protocols used in real-world networking.

1. **Application Layer**
   Combines the OSI model's Application, Presentation, and Session layers. Provides protocols for applications to communicate over the network.
   Example: HTTP, FTP, DNS, SMTP.
2. **Transport Layer**
   Similar to the OSI Transport layer, it provides reliable communication, flow control, and error checking.
   Example: TCP, UDP.
3. **Internet Layer**
   Corresponds to the OSI Network layer and handles the logical addressing and routing of data packets.
   Example: IP, ICMP, ARP.
4. **Network Access (Link) Layer**
   Combines the OSI model's Data Link and Physical layers. Manages physical data transmission and handles hardware addressing.
   Example: Ethernet, Wi-Fi.

Key Differences

- **Number of Layers**: OSI has 7 layers, while TCP/IP has 4 layers.
- **Design Focus**: OSI is more theoretical and idealized, often used for teaching and conceptual understanding. TCP/IP is more practical and is the foundation of the internet.
- **Layer Grouping**: In TCP/IP, the Application layer combines several OSI layers (Application, Presentation, Session), and the Network Access layer combines the Data Link and Physical layers.

Routers and switches

- **Importance of Routers:**

Routers are essential devices in networking that connect multiple networks and direct data packets between them. They play a crucial role in ensuring efficient and secure data transmission across the internet and within local networks.

- **Routing Table:**

A routing table is a data table stored in a router or a networked computer that lists the routes to particular network destinations.

It is used by the router to determine the best path for forwarding packets.

- **Network Destination**

This shows either the network address, a specific IP address, or the broadcast address. It indicates where the data packet is intended to go.

- **Netmask**

Another term for the subnet mask, which helps in determining the network portion of an IP address.

- **Gateway**

If the network is outside of your subnet, this is the default gateway to which the data is sent. It acts as an access point to another network.

- **Interface**

This lists the IP address of the local interface (that is, the one on the device) from which the data will be sent. It specifies the outgoing interface for the packet.

- **Metric**

This is the metric value attributed to that route/interface. It helps in determining the best route among multiple routes to the same destination.

Understanding Static and Default Routes

Static Routes

Manually configured routes that do not change unless updated by an administrator.

Advantages: Simple to configure and understand, provides control over routing decisions.

Limitations: Not flexible, requires manual updates if network changes.

Example Configuration: ip route 192.168.1.0 255.255.255.0 10.0.0.1

Default Routes

A route is used when no specific path is found in the routing table.

Purpose: Provides a gateway of last resort for packets with unknown destinations.

Example Configuration: ip route 0.0.0.0 0.0.0.0 10.0.0.1

Routing protocols

RIP (Routing Information Protocol)

- **Type**: Distance-vector routing protocol.
- **Function**: Uses hop count as a metric to determine the best path to a destination. Each router sends its entire routing table to its neighbours at regular intervals.
- **Limitations**: Maximum hop count of 15, making it suitable only for smaller networks.
- **Example Use**: Small, simple networks where ease of setup is prioritized over efficiency.

OSPF (Open Shortest Path First)

- **Type**: Link-state routing protocol.
- **Function**: Calculates the shortest path to each network using the Dijkstra algorithm, based on the link cost (like bandwidth or delay). Routers share link state information only when changes occur, making it more efficient.
- **Advantages**: Supports larger, more complex networks and provides fast convergence and scalability.
- **Example Use**: Large enterprise networks where efficiency and fast convergence are critical.

BGP (Border Gateway Protocol)

- **Type**: Path-vector routing protocol.
- **Function**: Manages the routing of data between autonomous systems (AS) on the internet. Use policies and attributes to select the best paths, rather than just the shortest ones.
- **Advantages**: Handles large, complex networks (like the internet) and allows for policy-based routing.
- **Example Use**: Internet Service Providers (ISPs) and large networks that connect to multiple external networks (like other ISPs or companies).

Network Address Translation

NAT is a technique used in networking to map private IP addresses used within a local network to a public IP address that can be used on the internet. It allows multiple devices on a private network to share a single public IP address

How NAT Works:

- **Private IP Addresses**: Devices in a local network have private IP addresses (e.g., 192.168.1.x). These addresses are not routable on the internet.
- **Public IP Address**: When a device from the private network needs to communicate with the internet, NAT translates its private IP address to a public IP address.
- **Translation Table**: NAT maintains a translation table that maps private IP addresses and ports to the corresponding public IP addresses and ports. This allows responses from the internet to be sent back to the correct device on the private network.

Types of NAT:

1. **Static NAT**: A one-to-one mapping between a private IP address and a public IP address. This is often used for servers that need to be accessible from the internet.
2. **Dynamic NAT**: Maps a private IP address to any available public IP address from a pool. This is used when there are more private IP addresses than available public IP addresses.
3. **PAT (Port Address Translation)**: Also known as "NAT overload," it allows multiple devices to share a single public IP address by assigning different ports to each session. This is the most common type of NAT used in home routers.

Advantages of NAT:

- **Conserves IP Addresses**: By allowing multiple devices to share a single public IP address, NAT helps conserve the limited number of available IPv4 addresses.
- **Security**: NAT can hide the internal structure of a network from external users, adding a layer of security.

Quality of service

Quality of Service (QoS) is a set of techniques used in networking to manage and prioritize network traffic, ensuring that critical or time-sensitive data (such as voice, video, and online gaming) receives the necessary bandwidth and low latency.

This is essential in networks where bandwidth is limited, and multiple applications or users are competing for resources.

Key Concepts in QoS:

- **Traffic Shaping**
  Controls the flow of data to ensure a smooth and consistent transmission.
- **Prioritization**
  Assign priority levels to different types of traffic (e.g., VoIP, video streaming).
- **Bandwidth Management**
  Allocates bandwidth to ensure that high-priority applications receive the necessary resources

How to Implement QoS:

- Determine which traffic needs prioritization.
- Create policies for traffic treatment.
- Use mechanisms to classify packets.
- Apply QoS markings based on classification.
- Enable QoS on network devices.
- Control traffic flow to prevent congestion.
- Regularly check and optimize QoS settings.
- Test QoS setups before deploying.

Switches

- **Switches in LANs:**

Switches are devices used to forward traffic within a local network, segmenting it into smaller, more manageable, and efficient areas.

- **Collision Reduction:**

Switches reduce collisions by creating separate collision domains for each port, leading to more efficient network performance.

- **Zero Collisions:**

In modern switched networks, properly configured switch ports are connected to individual devices, resulting in zero collisions. However, incorrect configurations or connecting hubs can still cause collisions.

- **VLANs for Further Segmentation:**

Virtual LANs (VLANs) can be used for additional network segmentation beyond the basic switch setup.

- **Forwarding Frames:**

Switches forward frames within the network to ensure efficient communication between devices

Frame forwarding

- **Store-and-Forward Switching:**

When a switch receives a frame, it stores the frame data in buffers until the full frame has been received. This method involves receiving the entire frame, computing the CRC (Cyclic Redundancy Check), and then forwarding it.

- **Cut-Through Switching:**

In this method, the switch starts forwarding the frame as soon as it reads the destination MAC address. It does not wait for the entire frame to arrive before forwarding it.

- **Destination MAC Address Lookup:**

Switches determine the correct port for forwarding by looking at the destination MAC address of the incoming frame. This information is typically stored in a Content Addressable Memory (CAM) table.

- **Efficient Communication:**

By using these frame forwarding methods, switches ensure that data packets are delivered accurately and swiftly within the network, contributing to efficient communication between devices.

What is the Root bridge?

The main switch in a network controls the flow of data and prevents loops by creating a tree-like structure for communication.

How the Spanning Tree Protocol (STP) works:

- **Root Bridge Election**

The network chooses one main switch called the Root Bridge based on the lowest ID**.**

- **Designated Ports**

Each switch picks the best path to the Root Bridge, marking those ports as Designated Ports for forwarding.

- **Blocking Ports**

Other ports are Blocked to prevent loops in the network.

- **Loop-Free Setup**

STP ensures there are no loops by identifying and blocking redundant paths.

- **Communication (BPDU- Bridge Protocol Data Unit)**

Switches exchange messages to share network details and make decisions.

- **Cost Calculation**

Each path's cost is determined based on link speed to find the best route.

- **Port States**

Ports go through stages like Blocking, Listening, Learning, and Forwarding to manage network traffic.

- **Adapting to Changes**

STP adjusts to network changes by updating port states to maintain a stable network.

VLANs (Virtual Local Area Networks)

VLANs are used to logically divide a single physical network into multiple isolated virtual networks.

Devices within the same VLAN can communicate as if they are connected to the same physical network, even if they are physically located in different parts of the network.

VLANs improve network security, efficiency, and management by segregating traffic and controlling communication between different groups of devices

Switch Security

- Switches increase network efficiency by reducing collision domains and forwarding data only to specific interfaces.
- Security measures include password-protecting console connections to prevent unauthorized access.
- To prevent physical tampering, unused switch ports should be disabled, and port security can be implemented to control MAC addresses on ports.
- MAC Flooding can overwhelm a switch, causing it to fail to open and broadcast frames to all ports; port security helps prevent this by authenticating new MAC addresses.

Wired Networks

A **wired network** uses physical cables (such as Ethernet) to connect devices, like computers, printers, and servers, to a network. These cables transmit data through electrical signals, providing a stable and high-speed connection.

Features of Wired Networks:

- **Reliability**: Wired connections are generally more stable and less prone to interference than wireless connections.
- **Speed**: Wired networks typically offer faster data transfer rates compared to wireless networks, especially over long distances.
- **Security**: Wired networks are considered more secure since they require physical access to the network, reducing the risk of unauthorized access.
- **Installation**: Requires running cables, which can be time-consuming and costly, especially in large or complex environments.

Example:

An office LAN where computers are connected to a central switch via Ethernet cables.

Wireless Networks

A **wireless network** uses radio waves to connect devices, eliminating the need for physical cables. Devices such as laptops, smartphones, and tablets can connect to the network via Wi-Fi, Bluetooth, or other wireless technologies.

Features of Wireless Networks:

- **Flexibility**: Wireless networks offer greater mobility, allowing devices to connect from anywhere within the coverage area without the need for cables.
- **Ease of Installation**: Setting up a wireless network is generally easier and faster since no physical cables are needed.
- **Range and Interference**: Wireless networks can be affected by physical obstacles (walls, furniture) and interference from other wireless devices, potentially reducing signal strength and speed.
- **Security**: Wireless networks are more vulnerable to unauthorized access and attacks, so encryption and strong security measures (like WPA3 for Wi-Fi) are essential.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

CSMA/CA is a network protocol used in wireless communication to prevent data collisions and ensure that devices on the same network can communicate efficiently. It's commonly used in Wi-Fi networks (IEEE 802.11).

How CSMA/CA Works:

1. **Carrier Sense (CS)**: Before a device (like a laptop or smartphone) sends data, it listens to the communication channel (wireless medium) to check if it is idle or busy.
    - If the channel is **idle** (no other device is transmitting), the device can proceed to the next step.
    - If the channel is **busy** (another device is transmitting), the device waits for a random period (known as the backoff period) before trying again.
2. **Collision Avoidance (CA)**: Unlike CSMA/CD (Collision Detection) used in wired networks, where collisions are detected after they occur, CSMA/CA tries to **avoid collisions before they happen**.
    - After sensing the channel is idle, the device sends a small control packet called a **Request to Send (RTS)** to the receiver.
    - The receiver, upon receiving the RTS, responds with a **Clear to Send (CTS)** packet, indicating that the sender can transmit data.
    - Once the sender receives the CTS, it sends the actual data.

    - This exchange of RTS and CTS reduces the chance of collisions by informing other devices in the network that the channel will be occupied, so they should wait before transmitting.

3. **Data Transmission**: After the RTS/CTS handshake, the data packet is transmitted. Once the data is received, the receiver sends an acknowledgement (ACK) to confirm successful transmission. If the ACK is not received, the sender assumes a collision occurred and retransmits the data after a backoff period.

Why CSMA/CA is Important:

- **Collision Prevention**: Wireless networks are prone to collisions because multiple devices share the same medium, but CSMA/CA minimizes the chances of collisions, ensuring smoother communication.
- **Efficiency**: By avoiding collisions, CSMA/CA reduces the need for retransmissions, saving time and bandwidth.

Radio Waves, Frequency, and Modulation

What are Radio waves?

Radio waves are a type of electromagnetic wave used for wireless communication. They travel through the air and can carry information over long distances.

What is Frequency?

Frequency refers to the number of oscillations or cycles a wave completes in one second, measured in Hertz (Hz). Higher frequencies correspond to shorter wavelengths and vice versa.

What is Frequency?

Modulation is the process of varying a carrier wave to encode information. There are two main types of modulation used in radio communication:

- Amplitude Modulation (AM)
- Frequency Modulation (FM)