Week 3 Revision notes

Week 3 - Internet Protocol (IPv4) and IPv4 Addressing

1. Introduction to Internet Protocol (IP)

- **Roles of the Network Layer**:
  - Defines and verifies **IP addresses** for devices.
  - Routes packets across different networks.
  - Uses **ARP (Address Resolution Protocol)** to convert IP addresses to MAC addresses.
  - Efficiently delivers packets without guarantees of reliability (handled by upper layers).

2. IP Versions: IPv4 and IPv6

- **IPv4**:
  - Introduced in 1977, supports approximately 4.3 billion addresses.
- **IPv6**:
  - Introduced to address IPv4 address limitations.
  - Allows for a vastly larger address space.

3. IP Header Fields

- **Version**: Indicates whether it's an IPv4 or IPv6 packet.
- **Header Length**: Size of the IP header.
- **Differentiated Services (DiffServ)**: Specifies the priority of the packet.
- **Total Length**: Total size of the packet, including header and data.
- **Time to Live (TTL)**: Sets a limit on the number of hops a packet can take before being discarded.
- **Protocol**: Specifies the type of transport protocol (TCP or UDP).
- **Source and Destination Addresses**: IP addresses of the sender and receiver.

4. IP Fragmentation

- **Purpose**: Splits large packets to meet the Maximum Transmission Unit (MTU) of each network.
- **Fragmentation Fields**:
  - **Identification**: Unique ID for reassembling fragments.
  - **Flags**:
    - **D** (Don't Fragment): Prevents fragmentation if set.
    - **M** (More Fragments): Indicates more fragments follow.
  - **Fragment Offset**: Helps reassemble fragments in the correct order.
- **Fragmentation Issues**:
  - Increases processing time due to reassembly.
  - If one fragment is lost, the entire datagram must be resent.

5. Core Components of Internet Connections

- **Addressing**:
  - Managed by the **Internet Assigned Numbers Authority (IANA)**.
  - IANA delegates to **Regional Internet Registries (RIRs)**, which assign IP addresses to local organizations.
- **Naming**:
  - **Domain Names** provide human-friendly addresses, which map to IP addresses.
- **Routing**:
  - Routes packets through multiple networks to reach the final destination.

6. IPv4 Addressing Basics

- **Structure**:
  - **32-bit addresses** represented in **dotted decimal notation** (e.g., `192.168.1.1`).
  - Divided into two main parts:
    - **Network ID**: Identifies the network.
    - **Host ID**: Identifies the specific device on the network.
- **Binary and Decimal Conversion**:
  - **Decimal to Binary**: Break down each decimal value in the IP address into an 8-bit binary equivalent.
  - **Binary to Decimal**: Add values based on bit positions to convert binary to decimal.

7. IPv4 Address Classes

- **Classful Addressing** (obsolete, but foundational):
  - **Class A**:
    - First octet (0-127), large networks, supports many hosts.
  - **Class B**:
    - First octet (128-191), medium-sized networks.
  - **Class C**:
    - First octet (192-223), small networks, limited hosts.
  - **Class D**:
    - Reserved for **multicasting**.
  - **Class E**:
    - Reserved for **experimental use**.
- **Special Addresses**:
  - **Loopback Address (127.0.0.1)**: Tests local machine's network stack.
  - **Private IP Ranges**: Used within private networks, not routable on the internet.
    - **Class A**: `10.0.0.0 – 10.255.255.255`
    - **Class B**: `172.16.0.0 – 172.31.255.255`
    - **Class C**: `192.168.0.0 – 192.168.255.255`

8. Subnet Mask and Network Masking

- **Subnet Mask**:
  - Separates the **network ID** and **host ID**.
  - Examples:
    - **Class A**: `255.0.0.0`
    - **Class B**: `255.255.0.0`
    - **Class C**: `255.255.255.0`
  - **Slash Notation**: Specifies the number of bits used for the network, e.g., `192.168.1.0/24`.
- **Network Masking**:
  - Routers use masking to determine if packets belong to their network or another.
  - **Logical ANDing**: Combines the IP address with the subnet mask to identify network portions.

9. Troubleshooting with IPv4 Addresses

- **Ping and Connectivity Tests**:
  - Use **ping 127.0.0.1** to verify local TCP/IP stack.
  - Ping remote addresses to test connectivity and identify network issues.

- **Common Scenarios**:
  - Check if hosts on different subnets can communicate by ensuring correct routing and subnet configurations.