Switch

A switch is a networking device that operates at the data link layer (Layer 2) of the OSI (Open Systems Interconnection) model. It is a critical component of modern Local Area Networks (LANs), enabling devices to connect, communicate, and share resources within a network. Here's an overview of switches:

Purpose of Switches:

- **Packet Forwarding:** Switches forward data packets between devices on a network.
- **Efficient Communication:** They improve network efficiency by reducing collisions and providing dedicated bandwidth to connected devices.
- **Segmentation:** Switches divide a network into segments, improving performance and security.

How Switches Work:

- **MAC Address Learning:**
  - When a switch receives a data packet, it examines the destination MAC address.
  - The switch checks its MAC address table (also known as a MAC address forwarding table) to determine the port to which the destination device is connected.
  - If the MAC address is not found in the table, the switch broadcasts the packet to all ports except the one it was received on (flooding).
  - When the destination device responds, the switch learns the MAC address and associates it with the corresponding port in its table.

speed of switch is measured in PPS (Packets Per Seconds) collision are still possible in switch

UTP (Unshielded Twisted Pair) and STP (Shielded Twisted Pair)

UTP (Unshielded Twisted Pair) and STP (Shielded Twisted Pair) are two common types of copper cabling used in networking to transmit data between devices. They are both made up of twisted pairs of copper wires, but they differ in their construction and shielding. Here's an overview of UTP and STP:

1. **UTP (Unshielded Twisted Pair):**

- **Construction:**
  - UTP cables consist of twisted pairs of copper wires without any additional shielding.
  - Each pair of wires is twisted together to reduce electromagnetic interference (EMI) and crosstalk.
- **Advantages:**
  - Cost-Effective: UTP cables are generally more affordable than STP cables.
  - Flexible and Easy to Install: UTP cables are flexible and easy to work with, making installation simpler.
  - Suitable for Most Environments: Ideal for general networking applications in typical office environments.

2. **STP (Shielded Twisted Pair):**

- **Construction:**
  - STP cables have an additional shielding layer, usually made of metal foil or braided metal around each pair of twisted wires.

    - This shielding helps to reduce electromagnetic interference (EMI) and crosstalk, providing better signal quality.
- **Advantages:**
    - Enhanced Protection: STP cables offer better protection against external interference, making them suitable for environments with high levels of electromagnetic interference.
    - Improved Signal Integrity: The shielding minimizes signal loss and ensures more reliable data transmission.
    - Suitable for Noisy Environments: Ideal for industrial settings, data centers, and areas with heavy electrical equipment.

half duplex- walkytalk simplex - FM Radio Full duplex - Phone call

> Algorithm used is CSMA/CD to avoid collision

Switching in Computer Networking

Switching is a fundamental process in computer networking that involves the forwarding of data packets between devices within a Local Area Network (LAN). It occurs at the data link layer (Layer 2) of the OSI (Open Systems Interconnection) model and plays a crucial role in establishing direct communication paths between network devices. Here's an overview of switching:

Types of Switches:

- **Unmanaged Switches:**
    - Basic switches with plug-and-play functionality.
    - No configuration required, making them easy to set up.
- **Managed Switches:**
    - Configurable switches with advanced features.
    - Allow network administrators to monitor, manage, and configure settings such as VLANs, QoS, and port mirroring.

Drawbacks of Switchig

- As you go connect more connection the number of delays are increasing
- As you grow more number fo switches there will be more delay.
- Proxy servers
- Email servers
- File servers
- Name Advertisement
- User Password by domain controller
- In typing recieves broadcast halt period generated and letter typed stored in keyboard buffer
- once broadcast flooded it gets injuries to network
- switches can not control broadcast because broadcast goes every corner in network and consume the processing power of machines.

Routers in Computer Networking

Routers are essential networking devices that operate at the network layer (Layer 3) of the OSI (Open Systems Interconnection) model. They are responsible for forwarding data packets between different networks,

directing traffic based on IP addresses, and determining the optimal path for data transmission. Here's an overview of routers:

Purpose of Routers:

- **Interconnecting Networks:** Routers connect multiple networks together, such as LANs, WANs, and the Internet.
- **Packet Forwarding:** They forward data packets between networks based on IP addresses, using routing tables to determine the best path.
- **Network Address Translation (NAT):** Routers perform NAT, translating private IP addresses to public IP addresses for communication over the Internet.
- **Security:** Routers can act as a firewall by filtering and controlling incoming and outgoing traffic.

How Routers Work:

- **Routing Table:**
    - Routers maintain a routing table, which contains information about network paths, IP addresses, and next-hop destinations.
    - When a router receives a data packet, it checks the destination IP address against its routing table to determine the best path.
    - If the router has a direct connection to the destination network, it forwards the packet directly.
    - If not, it forwards the packet to the next-hop router along the path to the destination.
- **Packet Forwarding:**
    - Routers use protocols such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol) to exchange routing information and build their routing tables.
    - They analyze the IP header of incoming packets to determine the destination IP address and make forwarding decisions.
- **Network Segmentation:**
    - Routers create logical network segments, known as subnets, by dividing larger networks into smaller, more manageable parts.
    - Each subnet can have its own IP address range, allowing for efficient use of IP addresses and improved network organization.

Functions of Routers:

- **Primary function of router** To restrict the broadcast
- to connectes with WAN link
- router bifurgate the all unnessary broadcast and allows only necessary broadcast to respective network
- If router not present, all machines connected to network not pick up or not run.
- **Efficient Data Routing:** Routers determine the best path for data packets to reach their destination, optimizing network performance.
- **Network Segmentation:** Routers create logical segments, improving network organization and security.

- **Interconnection of Networks:** Enable connectivity between LANs, WANs, and the Internet, facilitating global communication.
- **Security:** Routers provide firewall features, NAT, and VPN capabilities to protect networks from unauthorized access and attacks.

Redundancy and High Availability:

- **Redundant Paths:** Multiple routers or links are used to provide backup paths in case of primary path failures.
- **Load Balancing:** Distributes traffic across multiple paths to optimize network performance and utilization.

IP Address and Classes

IP addresses are unique numerical identifiers assigned to devices in a network to facilitate communication. They are divided into classes, which determine the range and format of IP addresses within a network. Here's an overview of IP address classes:

1. **IP Address Format:**

- An IP address is a 32-bit binary number, typically represented in decimal format for human readability.
- It is divided into four octets (8 bits each) separated by periods (e.g., 192.168.1.1).
- Each octet can have a value from 0 to 255, representing a total of 256 possible values.

2. **Classes of IP Addresses:**

- IP addresses are categorized into five classes: A, B, C, D, and E.
- Classes A, B, and C are commonly used for addressing hosts, while Class D is reserved for multicast addresses, and Class E is reserved for experimental purposes.

3. **Classful IP Addressing:**

- Classful addressing refers to the original scheme for allocating IP addresses, where the first few bits of an IP address indicate the class.
- The class determines the range of IP addresses available for network, subnet, and host portions.

4. **IP Address Classes:**

- **Class A (1.0.0.0 to 126.255.255.255):**
    - First octet: 0xxxxxxx
    - Network portion: 8 bits (1.0.0.0 to 126.0.0.0)
    - Host portion: 24 bits (0.0.0.0 to 255.255.255.255)
    - Supports up to 126 networks with 16 million hosts each.
    - Reserved for large organizations with many hosts per network.
- **Class B (128.0.0.0 to 191.255.255.255):**
    - First octet: 10xxxxxx
    - Network portion: 16 bits (128.0.0.0 to 191.255.0.0)

    - Host portion: 16 bits (0.0.0.0 to 255.255.255.255)
    - Supports up to 16,384 networks with 65,534 hosts each.
    - Used for medium-sized networks with moderate numbers of hosts.

- **Class C (192.0.0.0 to 223.255.255.255):**

    - First octet: 110xxxxx
    - Network portion: 24 bits (192.0.0.0 to 223.255.255.0)
    - Host portion: 8 bits (0.0.0.0 to 255.255.255.255)
    - Supports up to 2 million networks with 254 hosts each.
    - Commonly used for small networks, such as home or office networks.

- **Class D (224.0.0.0 to 239.255.255.255):**

    - First octet: 1110xxxx
    - Reserved for multicast addresses, used for sending data to multiple recipients simultaneously.
    - Not assigned to individual hosts but to groups of hosts interested in receiving multicast traffic.

- **Class E (240.0.0.0 to 255.255.255.255):**

    - First octet: 1111xxxx
    - Reserved for experimental purposes and not used for general addressing.
    - Not available for public use, reserved for research and development.

5. **Subnetting and CIDR:**

- Subnetting allows further division of IP networks into smaller sub-networks for efficient address utilization.
- Classless Inter-Domain Routing (CIDR) is a method that allows more flexible allocation of IP addresses by using variable-length subnet masks (VLSM).

6. **Private IP Addresses:**

- Reserved IP address ranges for private networks to use internally without requiring public IP addresses.
- Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
- Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
- Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

7. **Public IP Addresses:**

- Public IP addresses are assigned by Internet Assigned Numbers Authority (IANA) for use on the Internet.
- These addresses are globally unique and routable on the public Internet.

Loopback Addresses in IP Networking

Loopback addresses are a special type of IP address that allows a device to send packets to itself. They are commonly used for testing network interfaces, troubleshooting, and internal network operations. In IP networking, the loopback address range is reserved and defined within the IPv4 and IPv6 standards.

Loopback Address Range:

- In IPv4, the loopback address range is defined as '127.0.0.0' to '127.255.255.255'.
    - The most commonly used loopback address is '127.0.0.1', which is also known as "localhost."
- In IPv6, the loopback address is represented as '::1'.

Purpose of Loopback Addresses:

- **Testing and Troubleshooting:** Loopback addresses are used to test the functionality of a network interface without needing external connectivity.
- **Software Development:** Developers use loopback addresses to test and debug applications that communicate over the network.
- **Internal Communication:** Applications and services on a device can use loopback addresses to communicate internally without needing an external network.

Subnetting in IP Networking

Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks, known as subnets. It is a fundamental concept in IP networking that allows for efficient use of IP addresses, improved network performance, and logical segmentation of networks.

Key Concepts:

- **Subnet Mask:** A subnet mask is a 32-bit number that defines the network portion and the host portion of an IP address.
    - It is represented in dotted-decimal notation, such as '255.255.255.0' for IPv4.
    - The subnet mask uses "1" bits to represent the network portion and "0" bits to represent the host portion.
- **Network Address:** The network address is the first address in a subnet, representing the network itself.
    - For example, in the subnet '192.168.1.0/24', the network address is '192.168.1.0'.
- **Broadcast Address:** The broadcast address is the last address in a subnet, used to send a packet to all devices in the subnet.
    - For example, in the subnet '192.168.1.0/24', the broadcast address is '192.168.1.255'.
- **Host Range:** The host range includes all the addresses between the network and broadcast addresses, excluding those reserved for the network and broadcast themselves.
    - For the subnet '192.168.1.0/24', the host range is '192.168.1.1' to '192.168.1.254'.

Benefits of Subnetting:

- **Optimized IP Addressing:** Subnetting allows for efficient use of IP addresses by creating smaller, more manageable address blocks.
- **Reduced Broadcast Domain:** Smaller subnets reduce broadcast traffic, improving network performance and efficiency.
- **Enhanced Security:** Subnets provide a level of security by isolating traffic within specific network segments.

- **Simplified Network Management:** Network administrators can manage and troubleshoot smaller subnets more easily.