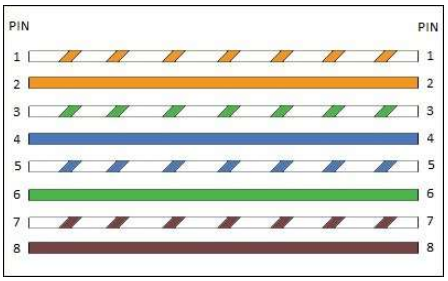
Experiment 1

AIM – To study cross over, straight through, router, switch, firewall.

THEORY –

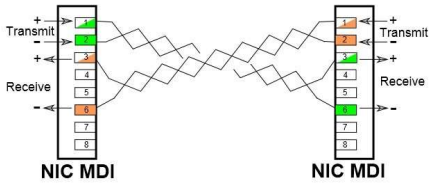
1. Straight-Through Cable:

- Straight-through cables have the same wiring configuration on both ends.
- They are commonly used to connect different types of devices, such as a computer to a switch or router.
- Connect a PC to a router, a switch to a hub, or a computer to a network printer.
- The color-coated wires are in the same order on both ends of the cable .
- Transmit (TX) pins on one end connect to receive (RX) pins on the other end, allowing data to flow from sender to receiver without crossing over3.
- This cable type has identical wiring on both ends (pin 1 on one end of the cable is connected to pin 1 at the other end of the cable, pin 2 is connected to pin 2 etc.)



2. Crossover Cable:

- Crossover cables have their transmit and receive pairs crossed over.
- They are used to directly connect similar devices, bypassing the need for a switch or hub.
- Connect two computers directly, or link two switches together.

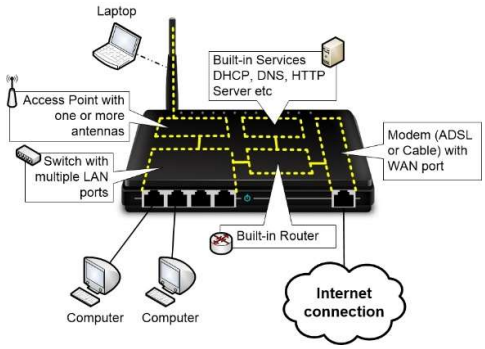


- The color-coated wires are different on each end of the cable14.
- The TX pin on one end connects to the RX pin on the other end, enabling direct communication between devices
- With the crossover cable, the wire pairs are swapped, which means that different pins are connected together – pin 1 on one end of the cable is connected to pin 3 on the other end, pin 2 on one end is connected to pin 6 on the other end

3. Router
    - A router is a crucial networking device that connects two or more IP networks or subnetworks.
    - It forwards data packets between networks based on their intended IP addresses. Think of them as air traffic controllers guiding packets to their destinations efficiently.
    - It allows multiple devices to share a single Internet connection.
    - They manage traffic between local area networks (LANs) and wide area networks (WANs). LANs are restricted to specific geographic areas, while WANs cover larger regions, often requiring multiple routers and switches.
    - A router uses an internal routing table—a list of paths to various network destinations. When a packet arrives, the router examines its header to determine the destination IP

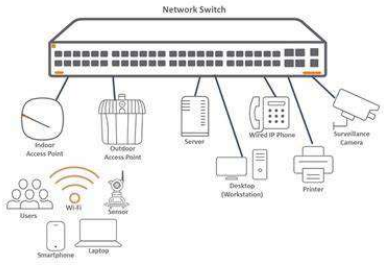
address. It then consults the routing table to find the most efficient path and forwards the packet accordingly.

- While routers handle network traffic, modems connect networks to the Internet. Modems convert signals from an Internet service provider (ISP) into digital signals interpretable by connected devices1.



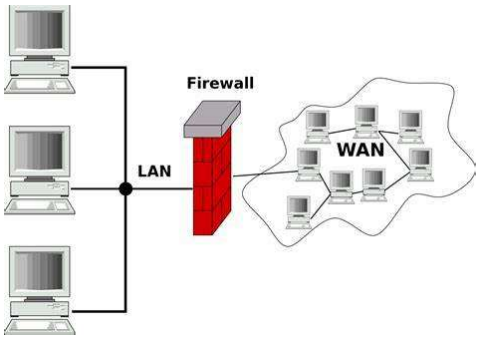
4. Switches

- Switches connect devices within a LAN, allowing them to communicate directly. They operate at the data link layer (Layer 2) of the OSI model.
- They learn MAC addresses by observing traffic. They build a MAC address table, which helps them forward packets efficiently to the correct destination.
- Each switch port creates a separate broadcast domain. Unlike hubs, switches don't flood broadcast traffic to all ports.
- Switches can segment a network into virtual LANs (VLANs) for better organization and security.
- Switches offer different port speeds (e.g., 1 Gbps, 10 Gbps) and support full-duplex communication.



5. Firewalls:

- Firewalls filter incoming and outgoing traffic based on predefined rules. They block unauthorized access and protect against threats.
- Modern firewalls use stateful inspection to track the state of connections. They allow or deny traffic based on context (e.g., established connections).
- Some firewalls inspect application-layer data (e.g., HTTP requests) to enforce security policies.
- Firewalls create security zones (e.g., DMZ, internal network) and control traffic flow between them.
- Advanced firewalls include intrusion prevention systems (IPS) to detect and prevent



RESULT –

Successfully studied the intermediary devices such as switch, router, firewalls, wires etc.