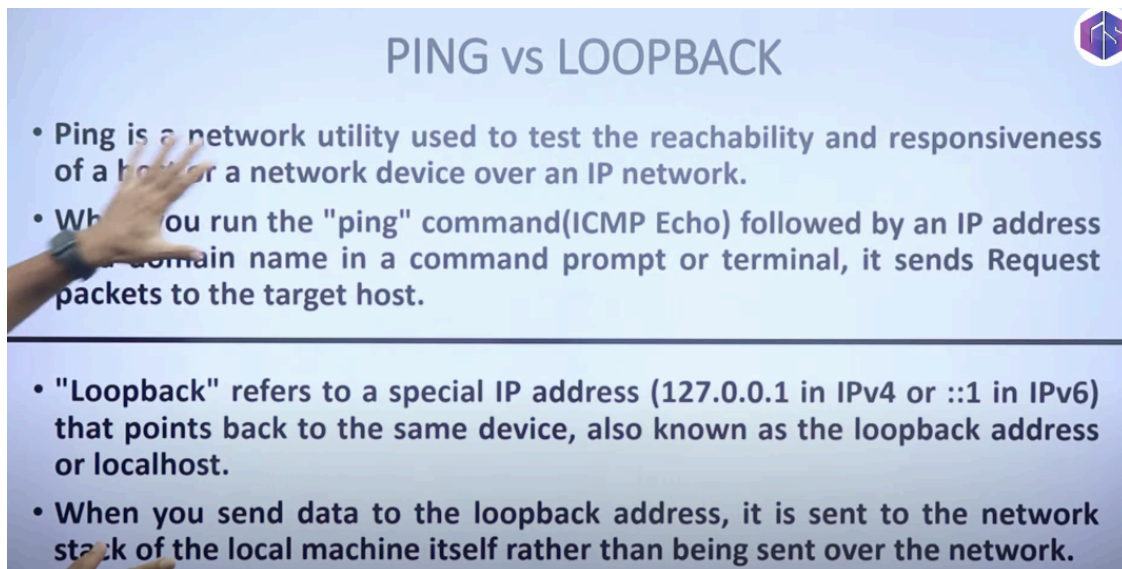# 2Terminologies

September 9, 2025

[ ]:

0.0.1 Modulation: done by moderm

nowadays router have built in moderm

encoding digital data onto an analog carrier signal for transmission over a communication channel.

This is done to enable the transmission of digital information over various physical mediums like copper wires, optical fibers, or wireless radio waves, which typically support analog signals.

Hub broadcast the signal, repeater with multiple ports

Switch applies logic

Bridge
Connecting two LAN netwoks

Router

Amplifies the signal

stores the packet so that it can retransmit it

1. Routers can also act as firewalls blocking or permitting traffic based on criteria like source/destination IP addresses, ports, and protocols.

Routers often provide management interfaces (web interfaces or command-line interfaces) that allow network administrators to configure and monitor the router's settings, including security policies and routing tables.

Some routers have built-in VPN capabilities, allowing remote users to securely connect to the network over the internet.

Load Balancing: In some cases, routers can distribute network traffic across multiple internet connections or routes to balance the load and ensure optimal network performance.

1 Network Address Translation,

which allows multiple devices on a LAN to share a single public IP address. NAT assigns a unique local IP address to each device on the LAN

2 ARP

ARP (Address Resolution Protocol) is a network protocol used in computer networks to map an IP address to a corresponding MAC address (Media Access Control address). It operates at the Link Layer (Layer 2) of the OSI model and is essential for communication within a local network (LAN).

3 DHCP

, simplifying network setup.

DHCP simplifies the process of configuring devices on a network by dynamically providing them with the necessary network settings, such as

Dynamic Host Configuration Protocol ?

It is a network protocol

Many routers include DHCP servers,

which

1. automatically assign IP addresses
2. manage IP addresses

1. other network configuration parameters to devices
    1. subnet masks,
    2. default gateways,
    3. DNS (Domain Name System) server addresses

4 Topologies

PING vs LOOPBACK

- Ping is a network utility used to test the reachability and responsiveness of a host or a network device over an IP network.
- When you run the "ping" command(ICMP Echo) followed by an IP address or domain name in a command prompt or terminal, it sends Request packets to the target host.

- "Loopback" refers to a special IP address (127.0.0.1 in IPv4 or ::1 in IPv6) that points back to the same device, also known as the loopback address or localhost.
- When you send data to the loopback address, it is sent to the network stack of the local machine itself rather than being sent over the network.

wastage of resources
SPOF

③ Mesh Topology

PING vs LOOPBACK

- Ping is a network utility used to test the reachability and responsiveness of a host or a network device over an IP network.

- When you run the "ping" command(ICMP Echo) followed by an IP address or domain name in a command prompt or terminal, it sends Request packets to the target host.

- "Loopback" refers to a special IP address (127.0.0.1 in IPv4 or ::1 in IPv6) that points back to the same device, also known as the loopback address or localhost.

- When you send data to the loopback address, it is sent to the network stack of the local machine itself rather than being sent over the network.

PING vs LOOPBACK

- Ping is a network utility used to test the reachability and responsiveness of a host or a network device over an IP network.
- When you run the "ping" command(ICMP Echo) followed by an IP address or domain name in a command prompt or terminal, it sends Request packets to the target host.
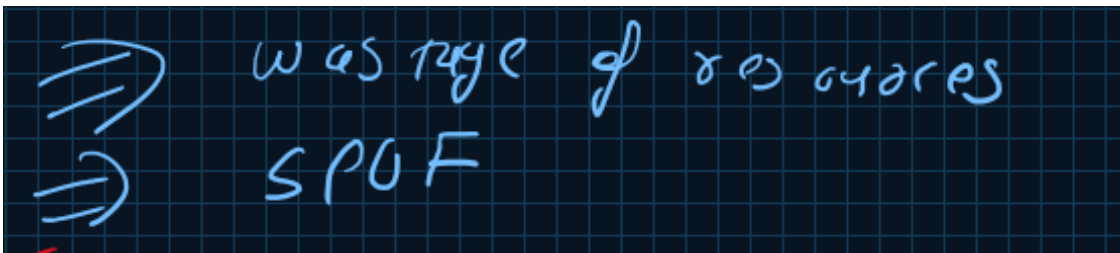

- "Loopback" refers to a special IP address (127.0.0.1 in IPv4 or ::1 in IPv6) that points back to the same device, also known as the loopback address or localhost.
- When you send data to the loopback address, it is sent to the network stack of the local machine itself rather than being sent over the network.
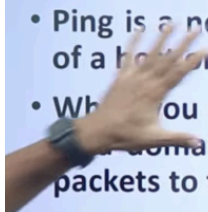
PING vs LOOPBACK

- **Ping is a network utility used to test the reachability and responsiveness of a host or a network device over an IP network.**
- **When you run the "ping" command(ICMP Echo) followed by an IP address or domain name in a command prompt or terminal, it sends Request packets to the target host.**

- **"Loopback" refers to a special IP address (127.0.0.1 in IPv4 or ::1 in IPv6) that points back to the same device, also known as the loopback address or localhost.**
- **When you send data to the loopback address, it is sent to the network stack of the local machine itself rather than being sent over the network.**
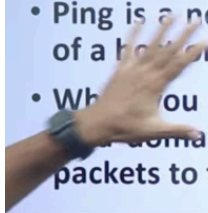
Queue op/vs/op processing

PING vs LOOPBACK

- Ping is a network utility used to test the reachability and responsiveness of a host or a network device over an IP network.
- When you run the "ping" command(ICMP Echo) followed by an IP address or domain name in a command prompt or terminal, it sends Request packets to the target host.

- "Loopback" refers to a special IP address (127.0.0.1 in IPv4 or ::1 in IPv6) that points back to the same device, also known as the loopback address or localhost.
- When you send data to the loopback address, it is sent to the network stack of the local machine itself rather than being sent over the network.

⇒ wastage of resources

⇒ SPOF

5 three way handshake

The three-way handshake is a process used in the Transmission Control Protocol (TCP) to establish a reliable connection between a client and a server before data transfer begins.

Visual Representation Client sends SYN → Request to start communication. Server sends SYN-ACK → Confirms receipt of SYN and sends its own SYN. Client sends ACK → Acknowledges the server's SYN-ACK.

Step 1: SYN (Synchronize)

The client sends a synchronization (SYN) packet to the server to initiate a connection. This packet includes a randomly generated sequence number, which the server will acknowledge. Purpose: To indicate the client's intent to start communication and synchronize sequence numbers. Client → Server: SYN
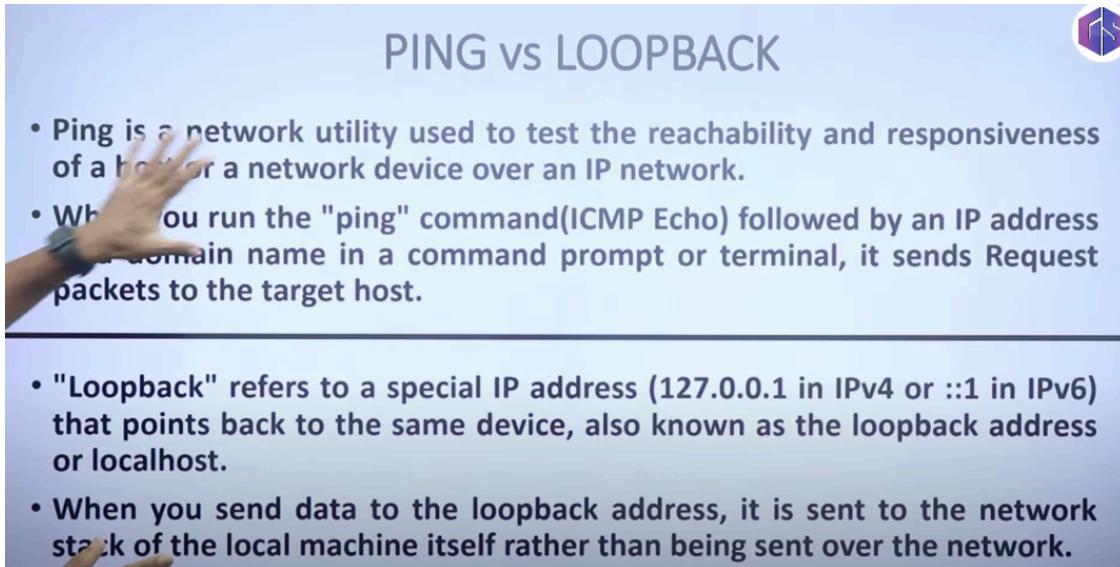
Step 2: SYN-ACK (Synchronize-Acknowledge)

The server responds with a SYN-ACK packet. This packet acknowledges the client's SYN packet by sending an acknowledgment number (which is the client's sequence number + 1) and includes its own sequence number for synchronization. Purpose: To confirm the server's readiness and establish its sequence number. Server → Client: SYN-ACK

Step 3: ACK (Acknowledge)

The client responds with an acknowledgment (ACK) packet. This packet acknowledges the server's SYN-ACK packet by sending an acknowledgment number (server's sequence number + 1). Purpose: To confirm the connection is established. Client → Server: ACK