🔵 1. What Is Networking?

Networking is the process of connecting computers, mobile phones, routers, servers, and other devices so they can:

- Share data
- Access the internet
- Communicate with each other
- Transfer files
- Use online services

Every device connected to a network needs:

- An IP address (identity)
- A MAC address (hardware ID)
- A gateway (router)
- A DNS server (website to IP converter)

🔵 2. Network Components (Full Explanation)

2.1 IP Address (Internet Protocol Address)

An IP address is like the “home address” of a device on a network.

Types of IP:

🚀 Private IP (Inside home/college)

- Cannot access internet directly
- Example:
  - 192.168.0.5
  - 10.0.0.19

🌐 Public IP (Provided by ISP)

- Identifies you on the internet
- Example:
  - 103.54.98.22

IPv4 Example:

192.168.1.20

IPv6 Example:

2401:4900:cac4:a1b2:ef56:e5f0:6219:1118

2.2 MAC Address

MAC = Media Access Control

It is a 48-bit hardware address burned into your network card.

Example:

08:00:27:1F:B7:23

Purpose:

- Identifies device inside local network
- Used for ARP
- Helps switches deliver packets correctly

2.3 DNS (Domain Name System)

DNS converts:

Domain name → IP address

Why needed?

Because humans remember words, computers use numbers.

Example:

google.com → 142.251.43.238

Types of DNS Records:

- A record – IPv4
- AAAA record – IPv6
- CNAME – Alias
- MX – Mail server
- TXT – Verification records

When you enter google.com:

1. Browser → DNS Resolver
2. Resolver → Root Server
3. Root → TLD (.com)
4. TLD → Authoritative Server
5. IP returned to you

2.4 TCP vs UDP (FULL DETAIL)

🔵 TCP (Transmission Control Protocol)

- Connection-oriented
- Reliable
- Slow (handshake required)
- Ordered delivery
- Guaranteed delivery

Used in:

- HTTP
- HTTPS
- SSH
- FTP
- Email

🔴 UDP (User Datagram Protocol)

- Connectionless
- Fast
- Lightweight
- No guarantee
- No order

Used in:

- DNS
- Online games
- Video calls
- Streaming

🔵 3. HOW DATA TRAVELS IN A NETWORK (COMPLETE FLOW)

When you open google.com:

1. Browser checks cache
2. Sends DNS Query
3. DNS Server replies with IP
4. Browser starts TCP Handshake
5. Sends HTTP/HTTPS Request
6. Server sends Response
7. Data is shown in browser

Wireshark can see all of this.

🟢 4. INSTALLING WIRESHARK IN KALI LINUX

```
sudo apt update
sudo apt install wireshark -y
```

Enable capturing without root:

```
sudo usermod -aG wireshark $USER
```

Restart:

```
reboot
```

🟢 5. FIXING INTERNET (WHY IMPORTANT)

Your VM had:

❌ IPv6 issues

✔ IPv4 working after fix

Commands you used:

```
echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
echo "net.ipv6.conf.default.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
sudo sysctl -p
```

This ensures:

✔ DNS

✔ Browsing

✔ Packet capturing

✔ Ping

work correctly.

🟢 6. WIRESHARK COMPLETE PRACTICAL WORK (FULL DETAIL)

✔ Step 1 — Open Wireshark

```
wireshark
```

Select:

👉 eth0

👉 Start Capture

You will see packets like:

- ARP
- ICMP
- TLS
- TCP
- DNS

⭐ 7. TCP THREE-WAY HANDSHAKE — DETAILED

Filter:

```
tcp.flags.syn==1
```

Open Firefox → Go to:

http://example.com

You will see:

1. SYN (Client → Server)

Meaning:

“Hello server, I want to connect.”

2. SYN, ACK (Server → Client)

Meaning:

“Okay client, I accept.”
3. ACK (Client → Server)
Meaning:
“Connection confirmed.”
This makes TCP reliable, orderly, secure.

⭐ 8. DNS QUERY ANALYSIS — FULL DETAIL
Filter:
dns
Visit:
google.com
You will see:
Standard Query A google.com

- Asking for IPv4

Standard Query Response

- DNS server returns actual IP

This shows:
✔ DNS is working
✔ Domain resolution is successful

⭐ 9. HTTP PACKET ANALYSIS (FULL DETAIL)
Filter:
http
Visit:
http://example.com
You will see plain text:

- HTTP GET
- Host header
- Server header
- HTML response

Reason:
HTTP is NOT encrypted.
Anyone in the network can read your traffic.

⭐ 10. HTTPS PACKET ANALYSIS (FULL DETAIL)
Filter:
tls
Visit:
https://facebook.com
You will see:

- Client Hello
- Server Hello
- Certificate
- Encrypted Application Data

You CANNOT see:
❌ Password
❌ Message content
❌ Cookies

Because HTTPS uses TLS encryption.

⭐ 11. ARP PACKET ANALYSIS

ARP = Address Resolution Protocol

Converts:

IP → MAC

Example:

Who has 10.155.67.1? Tell 10.155.67.40

This shows:

- Your VM trying to find gateway
- Router replying with MAC address

⭐ 12. SAVE PCAP FILE

File → Save As → task3_capture.pcapng