TCP / IP & Packet Flow by Morphine

TCP / IP is the practical model used in real networks, while OSI is theoretical.

It has 4 Layers :

TCP / IP Layer	OSI Equivalent	Key Concepts
Application	Application, Presentation, Session	HTTP, HTTPS, DNS, FTP, SSH
Transport	Transport	TCP / UDP, Ports
Internet	Network	IP, Routing, ICMP
Network Access	Data Link, Physical	MAC, Ethernet, ARP, WiFi

1. Application Layer (Browser Apps, Web, Email)

Includes all high-level protocols :

- HTTP / HTTPS
- DNS
- SMTP
- FFTP / SFTP
- SSH
- DHCP
- Telnet (old)

Cyber Security focus :

- SQL Injection
- XSS (HTTP)
- DNS Spoofing
- SMTP spoofing
- Man-in-the-middle

- API Hacking

---

2. Transport Layer (TCP / UDP)

Handles port numbers and end-to-end connections.

TCP

Reliable, Connection-based.

1. SYN
2. SYN-ACK
3. ACK

UDP

Fast, connectionless (gaming, video).

Cybersecurity Focus :

- SYN Flood attack
- UDP Flood
- Port scanning (Nmap)
- Banner grabbing
- TCP reset attack

---

3. Internet Layer (IP + Routing)

Moves packets between networks.

Includes :

- IP

- ICMP
- ARP (Between Layer 2/3)
- Routing (Finding path)
- NAP / PAT

Cybersecurity Focus :

- IP spoofing
- ICMP tunnel attacks
- ARP spoofing
- DoS attacks
- Router hijacking

---

4. Network Access Layer (LAN - Level)

Deals with MAC address + Frames.

Includes :

- Ethernet
- WiFi
- MAC Addressing
- Frames
- ARP
- Switches

Cybersecurity Focus :

- ARP Poisoning
- MAC Flooding
- VLAN hopping

- Evil twin WiFi attacks
