TCP AND UDP MASTER CLASS

Transport Layer (Layer 4) Ke Asan Notes | Prepared by Syed Ghous

1. Transport Layer Ka Asal Kam Kya Hai?

Sochein jab data Layer 3 (Network Layer) se IP address dhoond kar aap ke computer tak pohnch jata hai, to computer ko kaisy pata chalta hai k yeh data kis app ka hai? Kya yeh WhatsApp ka message hai, Chrome ka page hai, ya Valorant game ka data hai?

Yeh kaam **Transport Layer** ka hai! Yeh **Ports** ka istemal karti hai taky data ko sahi application tak pohnchaye. Aur is layer par data chalane ke do sab se bade tareeqay (Protocols) hain: **TCP** aur **UDP**.

TCP: The Responsible Brother (Zimmadar)

Real Life Example (Aam Misaal):

Sochein aap ne darzi (tailor) ko kapray siwaye aur us ne aap ko **Registered Courier** (TCS/Post) ke zariye bhejay. Courier wala aap ke ghar aaye ga, aap ka darwaza khatkhatae ga, aap ka naam poochay ga, aur jab aap hath se **Sign** karein gy, tabhi parsal aap ke hawale karein ga. Agar rasty mein koi cheez ghum ho jaye, to company ki zimmadari hoti hai k naya parsal bhejay.

Internet Par Kaam: TCP data bhejne se pehle doosry computer ke sath pakki dosti (Connection) banata hai jise **3-Way Handshake** kehty hain. Yeh ek ek tukda pohnchne par check karta hai k sab sahi pohncha ya nahi.

UDP: The Fast Speed Brother (Tez Raftar)

Real Life Example (Aam Misaal):

Sochein aap subha ke waqt apny ghar ke bahar khray hain aur **Akhbar wala (News Agent)** cycle par aata hai. Woh rukta nahi hai, balkeh chalti cycle se akhbar aap ke sehan (courtyard) mein phankta hai aur aage nikal jata hai. Ab akhbar sahi gira, mitti mein gira, ya chat par chala gaya, usay koi parwah nahi! Uska kaam bas tezi se akhbar pheknna tha.

Internet Par Kaam: UDP koi dosti ya connection nahi banata. Yeh bas data ko boht hi tezi se agay phekta rehta hai. Isay is baat se koi matlab nahi hota k saamne wala computer so raha hai ya jag raha hai.

2. TCP vs UDP: Bilkul Khul Kar Difference Table

Aap ki website ke readers ke liye yeh amne-samne ka mukabla dekhna boht zaroori hai:

Feature / Khoobi	TCP (Transmission Control Protocol)	UDP (User Datagram Protocol)
Connection Status	Connection-Oriented (Pehle dosti karta hai, phir data bhejta hai).	Connectionless (Bina dosti kiye direct data phekta hai).
Guaranteed Delivery?	**Haan!** Agar data rasty mein ghum ho jaye, to dobara bhejta hai.	**Nahi!** Agar data rasty mein ghum ho gaya to bas ghum ho gaya.
Speed / Raftar	Slow (Kyunki check-and-balance boht zyada hota hai).	Boht Tez (Kyunki koi checking ya rona dhona nahi hota).
Header Size (Wazan)	Bada Size (20 Bytes) — Kyunki boht saari extra maloomat hoti hain.	Chhota Size (8 Bytes) — Bilkul halka phulka hota hai.
Best For (Istemal)	Websites (HTTPS), Emails (SMTP), File Transfer (FTP).	Online Gaming (Valorant, PUBG), Live Streaming, Video Calls.

3. Cybersecurity Point of View (Hacker Kaise Khelta Hai?)

Hacker in dono protocols ke kaam karne ke tareeqay ko un ki kamzori bana dete hain:

🚨 TCP Ka Attack: SYN Flood (DDoS Attack)

TCP ki aadat hai k woh pehle dosti karta hai (SYN Packet se). Hacker iska faida uthata hai aur computer ko lakhoon fake dosti ki requests bheta hai. Masoom server rasta khol kar kehta hai "Aao dosti karein", lekin hacker aage se gayab ho jata hai. Server ka dimagh ghoom jata hai aur woh hang ho jata hai.

🛡️ Syed Ghous Ki Expert Security Defense Tip:

"Apni website ya server ko in attacks se bachane ke liye hamesha **Rate Limiting** aur **SYN Cookies** on rakhein. Is se fuzool aur had se zyada aany waly fake connections pehle hi block ho jaty hain aur aap ka network hamesha mahfooz rehta hai!"