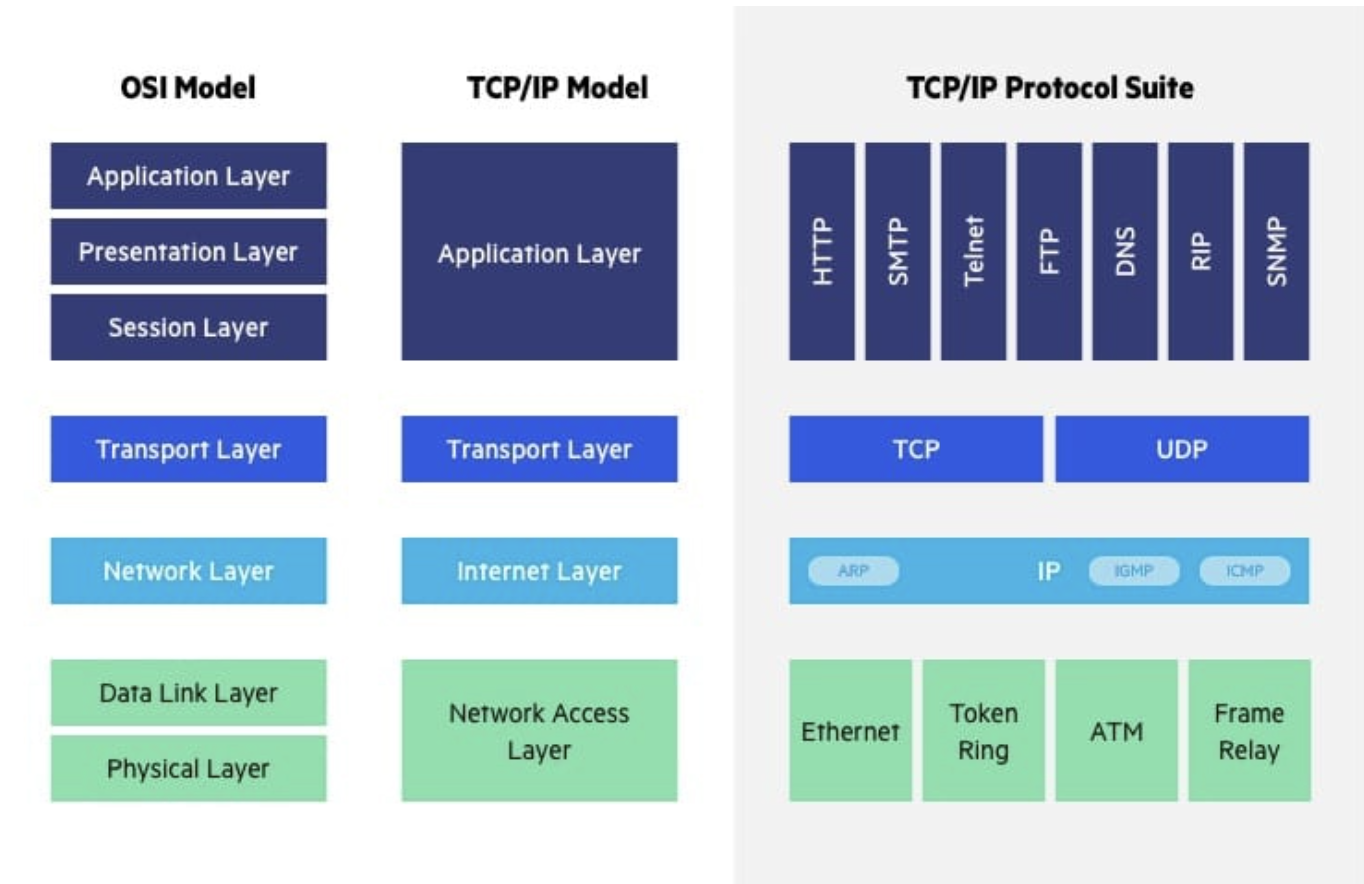
OSI model helps in troubleshooting, ease of software vendors for consistency.

1. **Application layer** is in user level. (HTTP, FTP, SMTP)
2. **Presentation layer** helps in encryption, compression of data for transmission.
3. **Session layer** creates communication and if required checkpoints for resume purpose in case of any interruptions.
4. **Transport layer** breaks data into segments (in sending end) and reassemble it (in receiving end). Ex: TCP, UDP
5. **Network layer Ex**: IP
6. Breaking up and assembling segments into smaller network packets and vice versa.
7. Routing packets across best path in physical layer
8. **Data link layer** creates and deletes a connection b/w two nodes. (Packets->frames):
9. Logical link control (Network protocols, error checking, sync the frames)
10. Media access control (MAC address connect devices)
11. **Physical Layer** helps in physical connection b/w nodes.

****

**What is TLS:**

SSL->TLS

Help from data breaches and other attacks:

Components:

1. Encryption
2. Authentication
3. Integrity

TLS certificate should be present on the server.

1. Initiated using TLS handshake. (Client and server).
2. Cipher suites is decided. -> set of algos which decides which encryption key or session key to use.
3. Authentication is established using TLS certificate. Public keys are used to decipher. (Public key cryptography).
4. Generation of session key and handshake is complete.

Some space and time are utilized which can affect the performance to a little extent.

Public key cryptography