Indian Institute of Technology Kharagpur
School of Information Technology
IT 30037 : Introduction to Internet

1. **Introduction:** Complexity of Data communication networks, Need for layered/modular architecture, Circuit/Packet/Message switching, Layering concept, OSI reference model, TCP/IP model. *(Barteskas and Gallager, Tanenbaum, Fourouzan)*

2. **Physical layer:** Fundamentals of signals, Concepts of analog and digital signals, Bandwidth, Data rate Vs Bandwidth, Transmission losses, Channel capacity, Digital transmission (Encoding techniques), Analog transmission (brief about ASK/FSK/PSK/QAM), A/D conversion, Transmission media (brief), Multiplexing (TDM/FDM). *(Fourouzan 4ed, William Stasllings)*

3. **Data link layer:** Framing (flag-based), Parity check codes, ARQs (stop-and-wait, go-back-n and selective-repeat). *(Tanenbaum 4ed: Chapter 3)*

4. **Medium access control layer:** ALOHA, CSMA, Collision free, limited contension, CSMA/CA and Ethernet. *(Tanenbaum 4ed: Chapter 4)*

5. **Network layer:** Connection less Vs connection oriented services, Routing protocols: shortest path, flooding, distance vector and link state routing. IPv4 header, Fragmentation and IP addressing. *(Tanenbaum 4ed: Chapter 5)*

6. **Transport layer:** Transport service premitives, Elements of transport protocols (addressing, connection establishment, connection release, flow control and buffering, multiplexing and crash recovery), UDP, TCP (intorduction to TCP, TCP service model, TCP protocol, TCP segment header, TCP connection establishment, release and management, TCP transmission policy, TCP congestion control and TCP timer management. *(Tanenbaum 4ed: Chapter 6)*

7. **Application layer:** Client-server model, concurrent and iterative servers, *(Fourouzan 3ed)* DNS, TELNET, FTP E-mail and WWW. *(Fourouzan 4ed: Chapter 26 and 27)*

8. **Network security:** Basic network attacks, Basics of cryptography: principles of symmetric (private) key and asymmetric (public) key cryptography, substitution and transposition ciphers, Symmetric key cryptosystems: DES and AES, Public key cryptosystems: RSA, Diffie-Hellman cryptosystem, Man-in-middle attack. Security services: Message confidentiality, Message integrity, Message authentication, Digital signature, Entity authentication and Key management (symmetirc key and public key distribution), Security in the Internet: IPSec, SSL/TLS, PGP, VPN and Firewalls *(Fourouzan (4ed) : Chapters 30, 31 and 32)*