Core-X **Computer Network**

Course Objectives:

- To understand data communication and network concepts.
- To learn about different communication standards
- To understand different network protocols

Learning Outcomes:

Upon completion of this course, students will be able to:

- Understand concepts on data communication and the use of communication devices
- Learn about analog and digital signals and basic components of data communication
- Learn about errors during data communication & access control mechanisms
- Learn various network protocols and network security issues

Unit-I:

Introduction to Data Communications and Network Models: Protocols and Standards, Layers in OSI Models, Analog and Digital Signals, Transmission Modes, Transmission Impairment, Data Rate Limits, Performance, Digital Transmission, Network Devices & Drivers: Router, Modem, Repeater, Hub, Switch, Bridge (fundamental concepts only).

Unit-II:

Signal Conversion: Digital-to-Digital Conversion, Analog-to-Digital Conversion, Digital-to-analog Conversion, Analog-to-Analog Conversion. Transmission Media: Guided Media, Unguided Media, Switching Techniques: Packet Switching, Circuit Switching, Datagram Networks, Virtual-Circuit Networks, and Structure of a Switch.

Unit-III:

Error Detection and Correction: Checksum, CRC, Data Link Control: Framing, Flow and Error Control, Noiseless Channels, Noisy channels, (Stop and Wait ARQ, Sliding Window Protocol, Go Back N, Selective Repeat) HDLC, Point-to-Point Protocol. Access Control: TDM, CSMA/CD, and Channelization (FDMA, TDMA, and CDMA).

Unit-IV:

Network Layer: Logical Addressing, IPv4 Addresses, IPv6 Addresses, Virtual-Circuit Networks: Frame Relay and ATM, Transport Layer: Process-Process Delivery: UDP, TCP. Application layers: DNS, SMTP, POP, FTP, HTTP, Basics of WiFi (Fundamental concepts only), Network Security: Authentication, Basics of Public Key and Private Key, Digital Signatures and Certificates (Fundamental concepts only).

Text Book:

- ✓ *Data Communications and Networking, Fourth Edition by Behrouza A. Forouzan, TMH.*

Reference Book:

- ✓ *Computer Networks, A. S. Tanenbaum, 4th edition, Pearson Education*.

Core X- Lab: Computer Network

1. Use the ***ipconfig*** (Windows) or ***ifconfig*** (Linux/Mac) command to display the current network configuration.
    i. Identify and document the IP address, subnet mask, and default gateway of the system.
    ii. Change the IP address of the system using ***netsh*** (Windows) or ***ifconfig*** (Linux/Mac). Verify the change using the same command.
    iii. Experiment by configuring static IP, dynamic IP.
2. Use the ***ping*** command
    i. to check connectivity between Systems in your Lab.
    ii. to a remote server (e.g., google.com).
    iii. Analyze the round-trip time and packet loss.
3. Use the ***tracert*** (Windows) or ***traceroute*** (Linux/Mac) command to trace the path to a remote server. Document the intermediate hops and their IP addresses.
4. Use the ***netstat*** command to display active connections, listening ports, and network statistics.
    i. Document and explain the various parameters and their significance.
    ii. Use ***netstat -r*** or ***route*** to display the routing table of your system. Identify the default gateway and other routes.
5. Use the ***arp -a*** command to display the ARP table of your system.
    i. Identify the MAC addresses corresponding to different IP addresses.
    ii. Clear the ARP cache using ***arp -d*** and verify the cache is cleared. Re-populate the ARP table by pinging different hosts on the network and verify the entries.
6. Use the ***nslookup*** command to query the DNS records of a domain (e.g., google.com).
    i. Identify and document the IP addresses associated with the domain.
    ii. Use the ***dig*** command (Linux/Mac) for a more detailed DNS query and compare the output with ***nslookup***
7. Use the ***nmcli*** command (Linux) or ***netsh wlan show networks*** (On Windows) to scan for available Wi-Fi networks and connect to a specified network. Document the steps and verify the connection.
8. Use the ***tcpdump*** command (Linux) or ***Wireshark*** to capture network packets.
    i. Capture and analyze traffic for a specific protocol (e.g., HTTP) and identify key details like source and destination IPs, ports, and packet content.
    ii. Filter captured packets to display only traffic to/from a specific IP address or port using ***tcpdump*** for Wireshark filters.
9. Use the ***nmap*** command to perform a network scan of your local network.
    i. Identify active hosts, open ports, and running services.
    ii. Perform a more detailed scan with service/version detection using ***nmap -sV*** and analyze the results.
10. Use the ***iptables*** command (Linux) to set up basic firewall rules. On Windows, use ***netsh advfirewall.***Block all incoming traffic except for SSH and HTTP, and verify the rules are working.

11. Use the ***route*** command to add a static route to a specific network.
    i. Verify the route using ***route -n*** (Linux) or ***route print*** (Windows).
    ii. Set up IP forwarding on a Linux system using ***sysctl*** to enable packet forwarding. Test the configuration by pinging through the system acting as a router.