Gyanmanjari Innovative University

Syllabus
Gyanmanjari College of Computer Application
Semester-1 (MCA)

**Subject: Data Communication and Networks** – MCA2XX11503

**Type of course:** Minor Stream

**Prerequisite:** Basic knowledge of computers, networking concepts, and communication systems. Students should have a basic understanding of IP addresses, internet usage, and computer operations. Logical thinking and problem-solving skills are also helpful for understanding data communication and networking concepts effectively.

**Rationale:**

This course provides fundamental knowledge of Data Communication and Computer Networks (DCN). It covers data transmission, network models, communication media, network devices, IP addressing, routing, switching, and basic network security. Students learn how computers communicate, how data is transferred securely, and how networks operate in real-world environments. The course also introduces network configuration, troubleshooting, and monitoring techniques using networking tools and technologies.

**Teaching and Examination Scheme:**

| Teaching Scheme | | | Credits | Examination Marks | | Total Marks |
|---|---|---|---|---|---|---|
| CI | T | P | C | SEE | CCE | |
| 4 | 0 | 2 | 5 | 100 | 50 | 150 |

*Legends: CI-Classroom Instructions; T-Tutorial; P -Practical; C –Credit; SEE -Semester End Examination; MSE-Mid Semester Examination; V–Viva; CA-Continuous Assessment; ALA-Active Learning Activities.*

**Course Content:**

| Sr. No | Course content | Hrs | % Weightage |
|---|---|---|---|
| 1 | **Introduction to Data Communication and Networking** | 18 | 20% |

Components of Data Communication System, Characteristics of Effective Communication, Types of Computer Networks (LAN, MAN, WAN, PAN), Network Topologies, Transmission Modes (Simplex, Half Duplex, Full Duplex), Communication Media (Guided Media, Unguided Media), Networking Devices (Hub, Switch, Router, Modem, Repeater, Access Point), Internet, Intranet and Extranet, Overview of Modern Networking Applications.

**Practical :**

1. Identify Components of a Data Communication System.
2. Create a Small LAN Network using a device like phone,laptop,etc with wire or wirelessly .
3. Analyze delivery, accuracy, timeliness, and jitter using real-life networking examples.
4. Simulation of Network Topologies Using Cisco Packet Tracer Create ring and mesh topology in Packet Tracer.
5. Simulation of Network Topologies Using Cisco Packet Tracer Create Star and Bus topology in Packet Tracer.
6. Compare and Analyze Internet, Intranet, and Extranet .
7. Network Troubleshooting Basics Use ping, tracert/traceroute, and netstat commands.
8. Create network design for school, office, or college.Include topology, devices, media, and IP addressing.
9. Connect two devices using Bluetooth. Transfer files and analyze communication speed.
10. Prepare a network diagram and device inventory report for a lab setup.

| Sr no | Evaluation Method | SEE | CCE |
|---|---|---|---|
| 1 | **Understanding Network Topologies :** Students will practically create and compare Star and Bus network topologies using networking devices or simulation software, assign IP addresses, and test connectivity using ping commands. | 20 | |
| 2 | **Network Traffic analysis :** Students will use Wireshark and Nmap to capture and analyze live network traffic, identify devices, protocols, ports, and network activities. They will document their observations, | | 10 |

| | | | |
|---|---|---|---|
| | screenshots, and findings in a report and submit it on the GMIU web portal. | | |
| **Total** | | **20** | **10** |

## Examination Style:

**Understanding Network Topologies [20 marks]**

- Students will perform the practical examination using Cisco Packet Tracer. They must create two separate network topologies: Star Topology and Bus Topology (using the Hub/Coaxial Bus simulation available in Packet Tracer or an equivalent shared-medium representation). For each topology, students will connect 4 PCs, assign valid IPv4 addresses (e.g., 192.168.1.1–192.168.1.4 with subnet mask 255.255.255.0), and verify the IP configuration. After completing the network setup, students will test communication by executing the ping command between all connected devices using the Command Prompt in Packet Tracer and record the results. Students must demonstrate successful connectivity, explain the role of the central device in the Star topology and the shared communication medium in the Bus topology, and compare both topologies based on structure, data transmission, reliability, and fault tolerance. Evaluation will be based on correct network creation, accurate IP addressing, successful ping results, and the student's explanation of the differences between the two topologies .

**Network Traffic Analysis [10 marks]**

- Students will complete this activity as an **individual take-home assignment** using **Wireshark** and **Nmap** installed on their personal computer/laptop. Students must first use **Nmap** to scan their home network and identify the active devices connected to the network, recording the IP addresses, host names (if available), and scan results. They will then use **Wireshark** to capture live network traffic for **5–10 minutes** while performing normal internet activities such as browsing websites, watching a YouTube video, or using online applications. Students are required to identify and analyze at least **five different network protocols** (e.g., TCP, UDP, HTTP/HTTPS, DNS, ICMP), examine the corresponding source and destination IP addresses, MAC addresses, protocol types, and port numbers, and briefly explain the purpose of each protocol observed. The final submission must be a **PDF report** containing the objective, software used, methodology, Nmap scan results, Wireshark capture screenshots, protocol analysis,

| | | | |
|---|---|---|---|
| | observations, conclusion, and references (if any). The completed report must be uploaded to the **GMIU Web Portal** . | | |
| 2 | **Network Models, IP Addressing and Internet Protocols**<br>OSI Reference Model, Functions of OSI Layers, TCP/IP Reference Model, Comparison between OSI and TCP/IP Models, Encapsulation and Decapsulation, IPv4 and IPv6 Addressing, IP Address Classes, Subnetting and Supernetting, MAC Address and ARP, DNS and DHCP Concepts, Introduction to NAT.<br>**Practical:**<br>11. Identify and explain functions of all seven OSI layers using real-world examples.<br>12. Mapping OSI Layers with Networking Devices and Protocols.<br>13. Observe packet formation and data flow using Packet Tracer or Wireshark.<br>14. Capture and analyze Ethernet frames, IP packets, and TCP/UDP segments using Wire Shark .<br>15. Identification of IPv4 Address Use ipconfig or ifconfig command to identify IPv4 address, subnet mask, and default gateway.<br>16. Configure static IPv4 addresses on computers and test connectivity.<br>17. Combine multiple networks into a single larger network using supernetting concepts.<br>18. Find MAC address of network interfaces using system commands.<br>19. Study of ARP Protocol Use arp -a command to view ARP table<br>a. Observe IP-to-MAC address mapping.<br>20. Create a small office or college network using proper IP addressing, subnetting, DHCP, DNS, and NAT concepts.<br>21. Trace how data travels from sender to receiver using OSI and TCP/IP models. | 17 | 20% |

| Sr No | Evaluation Method | SEE | CCE |
|---|---|---|---|
| 1 | **Understanding Network Model & IP Addressing :** Students will study OSI/TCP-IP models, IP addressing, subnetting, and key networking protocols through theory, practical exercises, and simulations, and document their findings in a report. | **20** | |
| 2 | **Case Study on Network Communication Device:** | | **10** |

| | | | | | |
|---|---|---|---|---|---|
| | | Students will study and analyze a network communication device, its features, working principles, connectivity, and applications, and submit a detailed technical report on the GMIU Portal. | | | |
| | | **Total** | **20** | **10** | |

**Examination Style :**

**Understanding Network Model & IP Addressing . [20 marks]**

- Students will use **Cisco Packet Tracer** to create a simple network, assign **static IP addresses**, and configure the devices. They will perform **IP addressing and subnetting**, verify connectivity using the **ping** command, and identify the **OSI/TCP-IP layers** and protocols involved in communication. Finally, students will submit a **practical report** containing the network topology, IP addressing details, subnetting calculations, connectivity results, and a brief conclusion. Evaluation will be based on correct configuration, successful communication, and the accuracy of the report .

**Case Study on Network Communication Device [10 marks]**

- Students will select **one network communication device** (e.g., Router, Switch, Hub, Modem, Access Point, or Firewall) and prepare a **technical case study report** at home. The report should include the device's **features, working principle, connectivity, advantages, limitations, and real-world applications**, supported with diagrams or images where appropriate. Students must upload the completed report in **PDF format** on the **GMIU Portal** before the submission deadline

| | | | |
|---|---|---|---|
| 3 | **Data Transmission and Network Protocols**<br>Analog and Digital Signals, Data Transmission Concepts, Transmission Impairments, Switching Techniques (Circuit Switching, Packet Switching, and Message Switching), Multiplexing Techniques, Error Detection and Correction, Flow Control and Error Control, TCP and UDP Protocols, Application Layer Protocols (HTTP/HTTPS, FTP, SMTP, and POP3), and Wireless Communication Basics.<br>**Practical:**<br>22. Create and observe Analog and Digital Signals by generating different signal waveforms and comparing their characteristics such as amplitude, frequency, and transmission behavior using Falstad Circuit Simulator or Multisim. | 19 | 20% |

| | | | |
|---|---|---|---|
| | 23. Design a simple data communication network and demonstrate Simplex, Half-Duplex, and Full-Duplex transmission between devices. Analyze the direction of data flow using Cisco Packet Tracer.<br>24. Simulate a communication channel to study the effect of transmission impairments such as attenuation, distortion, and noise on data transmission. Observe how these impairments affect signal quality using NetSim or an Online Communication Simulator.<br>25. Create three different network topologies to demonstrate Circuit Switching, Packet Switching, and Message Switching. Compare their working principles, delay, and resource utilization using Cisco Packet Tracer.<br>26. Configure a Circuit Switching communication scenario between two end devices and observe connection establishment, dedicated path creation, and data transmission using Cisco Packet Tracer.<br>27. Implement a Packet Switching network by connecting multiple devices and transmitting data packets. Analyze packet routing, packet delivery, and path selection using Cisco Packet Tracer.<br>28. Study Message Switching by simulating the Store-and-Forward technique and observing how complete messages are stored and forwarded between intermediate nodes using NetSim or Cisco Packet Tracer.<br>29. Demonstrate Multiplexing Techniques by simulating Frequency Division Multiplexing (FDM), Time Division Multiplexing (TDM), and Wavelength Division Multiplexing (WDM). Compare how multiple signals share a single communication channel using Cisco Packet Tracer and an Online Multiplexing Simulator.<br>30. Develop a Python program to implement Error Detection and Correction techniques such as Parity Check, Checksum, and Cyclic Redundancy Check (CRC). Verify whether transmitted data contains errors using Python IDLE or Visual Studio Code.<br>31. Simulate Flow Control and Error Control mechanisms by implementing Stop-and-Wait ARQ and Sliding Window protocols. Observe frame transmission, acknowledgements, retransmission, and data reliability using Cisco Packet Tracer or NetSim.<br>32. Configure TCP and UDP communication between client and server devices and compare their reliability, connection establishment, packet delivery, and transmission speed using Cisco Packet Tracer and Wireshark.<br>33. Configure HTTP and HTTPS services on a web server and access the web pages from client systems. Observe the communication | | |

process and analyze protocol packets using Cisco Packet Tracer and Wireshark.

34. Configure FTP, SMTP, and POP3 services in a client-server environment. Perform file transfer, send an email, and retrieve emails while analyzing protocol communication using Cisco Packet Tracer and Wireshark.
35. Configure a Wireless Local Area Network (WLAN) by setting up a wireless router, assigning SSID and security settings, connecting wireless devices, and verifying wireless communication using Cisco Packet Tracer.

| Sr no | Evaluation Method | SEE | CCE |
|---|---|---|---|
| 1 | **Network Flow Evaluation :** Students will perform data communication methods, switching techniques, protocols, and error-control mechanisms, and analyze how reliable data transfer is achieved in computer networks through practical demonstrations and reporting. | 20 | |
| 2 | **Smart Campus Network Design Challenge :** Students will design and present a secure and efficient campus/office network using appropriate devices, topology, IP addressing, and security measures, along with a detailed network diagram and report. | | 10 |
| | **Total** | 20 | 10 |

## Examination Style :

**Network Flow Evaluation [20 marks]**

- Students will perform the following tasks using Cisco Packet Tracer and Wireshark: Create a network consisting of 4 PCs, 1 Switch, and 1 Router, assign valid IP addresses to all devices, and verify connectivity using the ping command. Configure and test HTTP (TCP) and TFTP (UDP) services by accessing the server from client PCs and compare the communication process. Demonstrate packet switching by sending data between multiple devices through the router and observe the path followed by

| | | | |
|---|---|---|---|
| | packets using the Simulation Mode in Cisco Packet Tracer. Start Wireshark, capture the network traffic, and identify the TCP three-way handshake, UDP packets, source and destination IP addresses, sequence numbers, acknowledgements, and retransmitted packets (if any). Finally, submit the Packet Tracer (.pkt) file, Wireshark capture (.pcap) file, and a one-page report containing screenshots, observations of packet flow, comparison of TCP and UDP communication, and an explanation of reliable data transfer mechanisms.<br>**Smart Campus Network Design Challenge [10 marks]**<br>• Students will work in groups to design a complete computer network for a University Campus or an IT Company Office. They must create a network layout by selecting suitable networking devices, topology, transmission media, and IP addressing methods based on organizational requirements.<br>Students must include the following components in their design:<br>• Minimum **20 PCs/Laptops**<br>• **2 Switches**<br>• **1 Router**<br>• **1 Wireless Access Point**<br>• **1 Server**<br>• **1 Firewall**<br>• **Printer and CCTV connections**<br>• **Cat6 UTP Cable** for wired communication<br>• **Star Topology** for internal network connection<br>Students will draw the complete network diagram using tools like Cisco Packet Tracer or on chart paper. They must explain:<br>• Device selection and functions<br>• Topology used and reason for selection<br>• IP addressing scheme<br>• Internet and wireless connectivity setup<br>• Security implementation using firewall<br>• Communication flow between departments/users | | |

| | | | |
|---|---|---|---|
| | Students will finally present their network design and justify how it supports reliable, secure, and efficient communication for the organization and create a report which includes network design , device lists. | | |
| 4 | **Routing, Switching and Wireless Networks**<br>Routing Fundamentals,Routing Tables,Static Routing,Dynamic Routing Basics,Introduction to Routing Protocols,Switching Concepts,VLAN Concepts,Wireless LAN Fundamentals ,Wi-Fi Standards and Architecture,Mobile Communication Basics,Network Configuration Commands,Basic Network Troubleshooting.<br>**Practical :**<br>36. To study routing fundamentals and configure basic routing between networks using Cisco Packet Tracer.<br>37. To create, analyze, and verify routing tables in a simulated network environment using Cisco Packet Tracer.<br>38. To configure and test static routing for communication between multiple networks using Cisco Packet Tracer.<br>39. To study and implement dynamic routing concepts using routing protocols in Cisco Packet Tracer.<br>40. To configure and analyze basic routing protocols for network communication using Cisco Packet Tracer.<br>41. To study switching concepts and configure switching operations in a local area network using Cisco Packet Tracer.<br>42. To create and configure Virtual Local Area Networks (VLANs) for network segmentation using Cisco Packet Tracer.<br>43. To configure inter-VLAN communication and verify connectivity between VLANs using Cisco Packet Tracer.<br>44. To study Wireless LAN fundamentals and configure wireless communication using Cisco Packet Tracer.<br>45. To study Wi-Fi standards, wireless network architecture, and wireless security configuration using Cisco Packet Tracer and Wireshark.<br>46. To study basic mobile communication concepts and analyze wireless network traffic using Wireshark.<br>47. To perform network configuration using basic networking commands such as ping, tracert, ipconfig, ifconfig, and netstat using Cisco Packet Tracer and operating system command line tools.<br>48. To capture and analyze routing, switching, and wireless network packets using Wireshark. | 18 | 20% |

49. To perform basic network troubleshooting, connectivity testing, and network scanning using Wireshark and Nmap

| Sr no | Evaluation Method | SEE | CCE |
|---|---|---|---|
| 1 | **Packet Tracer Network Design :** Students will design and configure a small office network in Cisco Packet Tracer, implement VLANs, test connectivity, and troubleshoot networking issues to gain practical experience in network design and management. | 20 | |
| 2 | **Network Command Explorer:** Students will explore and analyze common networking commands, documenting their syntax, purpose, and practical applications in a structured report for submission on the GMIU web portal. | | 10 |
| | **Total** | 20 | 10 |

## Examination Style:

**Packet Tracer Network Design :[20 Marks]**

- Students will create a small office network topology in Cisco Packet Tracer by adding and connecting PCs, switches, and routers using suitable cables. They will design the network by creating and configuring VLANs (Virtual Local Area Networks) on switches to separate different departments and control network communication. Students will assign IP addresses, subnet masks, default gateways, and router settings to enable communication between devices and VLANs using inter-VLAN routing. They will verify connectivity using commands like ping, ipconfig, show vlan brief, and configuration commands, observe data transmission using Simulation Mode, and troubleshoot issues related to VLAN configuration, IP addressing, routing, and device connections. The final submission will include the configured Cisco Packet Tracer (.pkt) file and a brief explanation of the implemented network design.

**Network Command Explorer: [10 Marks]**

- Students will explore and study commonly used networking commands and prepare a detailed document based on their findings. They will collect different types of network commands such as

| | | | |
|---|---|---|---|
| | connectivity commands (ping, tracert), IP configuration commands (ipconfig, ifconfig), DNS commands (nslookup), and troubleshooting commands (netstat, arp). For each command, students must write its syntax, purpose, and practical application in real-world networking scenarios. They should explain how these commands help in checking network connectivity, identifying network issues, analyzing communication between devices, and monitoring network activities. After completing the study, students will organize their findings into a properly formatted document and submit the final report through the GMIU Web Portal. | | |
| 5 | **Network Security and Emerging Networking Technologies**<br>Introduction to Network Security.Threats and Vulnerabilities.Firewall Concepts.Antivirus and Security Tools.VPN Concepts.Basics of Cryptography.Types of Network Attacks(Phishing.Spoofing.Denial of Service (DoS)).Cloud Networking Basics.IoT Networking Concepts.Software Defined Networking (SDN).Virtualization in Networking .Network Monitoring and Management.<br>**Practical:**<br>50. Introduction to Network Security Understanding basic methods used to secure computer networks and data communication.<br>51. Threats and Vulnerabilities Identifying common security threats and weaknesses present in networks.<br>52. Firewall Concepts Studying how firewalls filter and control incoming and outgoing traffic.<br>53. Antivirus and Security Tools Learning the use of antivirus software and basic network security tools.<br>54. VPN Concepts Understanding secure remote communication using Virtual Private Networks.<br>55. Basics of Cryptography Studying encryption and decryption techniques used for data protection.<br>56. Understanding fake emails and websites used to steal user information.<br>57. Spoofing Attack Study Learning how attackers use fake identities or IP addresses in networks.<br>58. Understanding networking concepts used in cloud computing environments.<br>59. Studying communication methods used by smart and connected devices.<br>60. Software Defined Networking (SDN)Learning software-based approaches for managing network operations. | 18 | 20% |

61. Virtualization in Networking Understanding creation and use of virtual network resources and devices.
62. Learning tools used to monitor network traffic and performance.
63. Understanding methods used to manage and maintain computer networks.
64. Security Configuration Practice Performing basic configuration of network and system security settings.

| Sr no | Evaluation Method | SEE | CCE |
|---|---|---|---|
| 1 | **Cyber Shield: Exploring and Preventing Network Attacks:** Students will analyze different network attacks, their impact on computer networks, and recommend security measures such as cryptography, VPNs, firewalls, and system updates to prevent them. | **20** | |
| 2 | **Firewall Technologies and Security Analysis** Study and compare different firewall technologies, analyze their security features and real-world applications, determine suitable use cases for various environments, and submit the findings in a single document on the GMIU Web Portal. | | **10** |
| | **Total** | **20** | **10** |

## Examination Style :

**Cyber Shield: Exploring and Preventing Network Attacks: [20 Marks]**

- In this activity, students will identify different types of network attacks, study how they are performed, and analyze their impact on computer networks, such as data loss, unauthorized access, and service disruption. They will research effective prevention methods, including cryptography, VPNs, firewalls, system updates, and security improvements. Finally, students will prepare a structured report summarizing their findings, analysis, and recommended security measures.

**Firewall Technologies and Security Analysis: [10 Marks]**

- In this activity, students will study different types of firewalls, including Packet Filtering, Stateful Inspection, Proxy, Next-Generation

| | | | |
|---|---|---|---|
| | (NGFW), and Software/Hardware Firewalls. They will analyze their working principles, security features, advantages, limitations, and applications. Students will prepare diagrams, comparison tables, and recommend suitable firewall solutions for different networking scenarios. Finally, they will compile their findings and recommendations into a report and upload it on the GMIU Web Portal. | | |

**Continuous Assessment:**

**Suggested Specification table :**

| Distribution of Theory Marks **(Revised Bloom's Taxonomy)** | | | | | | |
|---|---|---|---|---|---|---|
| Level | Remembrance (R) | Understanding (U) | Application (A) | Analyze (N) | Evaluate (E) | Create (C) |
| Weightage | 25% | 30% | 15% | 15% | 5% | 10% |

**Note:** This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

**Course Outcome:**

| After learning the course the students should be able to: | |
|---|---|
| **CO1** | Understand the basic concepts, components, and types of computer networks along with different network topologies, transmission modes, communication media, and networking devices used in real-world networking environments. |
| **CO2** | Apply the knowledge of OSI and TCP/IP reference models and implement IPv4/IPv6 addressing, subnetting, and network protocols such as ARP, DNS, DHCP, and NAT to analyze and configure basic network communication systems. |
| **CO3** | Analyzing and applying data transmission techniques, switching methods, and multiplexing along with error detection and flow control mechanisms using application layer protocols like HTTP, FTP, SMTP, TCP, and UDP in wired and wireless networks. |
| **CO4** | Diagnose routing and switching concepts to configure static and dynamic routing, implement VLANs for network segmentation, and understand wireless LAN communication and basic network troubleshooting using standard networking commands. |
| **CO5** | Recognize various types of network attacks and vulnerabilities along with basic knowledge of security measures such as firewalls, VPNs, and cryptography, and emerging technologies like Cloud Networking, IoT, SDN, and network virtualization |

**Instructional Method:**

The course delivery method will depend upon the requirement of content and the needs of students. The teacher, in addition to conventional teaching methods by black board, may also use any tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc. From the content 10% topics are suggested for flipped mode instruction.

Students will use supplementary resources such as online videos, NPTEL/SWAYAM videos, e-courses, Virtual Laboratory.

The internal evaluation will be done on the basis of Active Learning Assignment.

Practical/Viva examination will be conducted at the end of semester for evaluation of performance of students in the laboratory.

## Reference Books:

[1]. Data communications and networking - Fifth Edition - 2013 - Behrouz A. Fourouzan - McGraw-Hill Companies,Inc,New York

[2]. Computer Networks - Fifth Edition - 2014 - Andrew S. Tanenbaum and David J. Wetherall - Dorling Kindersley (india) Pvt.Ltd

[3]. Computer Networks A Top-Down Approach - 2012 - Behrouz A. Fourouzan and Firoz Mosharraf - McGraw-Hill Companies,Inc,New York

[4]. Data communications and networking - Edition Detail: (I) : Dr. Rajni Bhalla - Published By : Lovely Professional University

[5].Data Communication & Computer Network- 2020 - V.S BAGAD , VIRAT V. GIRI , I.O DHOTRE , SACHIN S. MAHULKAR - Technical Publication

## Suggested Assessment Guidelines :

### Module 1: Introduction to Data Communication and Networking

| Program Implementation Task (20 Marks) : | | |
|---|---|---|
| **Criteria** | **Description** | **Marks** |
| Topology Identification | Correct identification and creation of Star and Bus Topologies using networking devices or simulation software. | 5 |
| Network Configuration & Communication | Ability to assign IP addresses correctly and test communication between devices using the ping command | 5 |
| Topology Analysis | Correct comparison of data flow, performance, cable usage, cost, advantages, disadvantages, and real-world applications of both topologies | 5 |
| Practical Observation & Report Presentation | Accuracy of practical observations, explanation quality, teamwork, and proper presentation of the final report | 5 |
| **Total** | | **20** |

### Module 2: Understanding Network Model & IP Addressing .

| Program Implementation Task (20 Marks) : | | |
|---|---|---|
| **Criteria** | **Description** | **Marks** |
| Understanding of Network Models | Demonstrates clear understanding of OSI and TCP/IP models, their layers, functions, and diagram representation. | 5 |
| IP Addressing & Calculation Skills | Performs IPv4/IPv6 addressing, IP classification, subnetting, and supernetting calculations accurately. | 5 |
| Knowledge of Network Communication Concepts | Explains and applies concepts of MAC Address, ARP, DNS, DHCP, and NAT using theory and simulation tools | 5 |
| Observation, Interpretation & Documentation | Presents accurate observations, proper analysis, neat diagrams, calculations, and well-organized report submission. | 5 |
| **Total** | | **20** |

### Module 3: Network Flow Evaluation

| Program Implementation Task (20 Marks) : | | |
|---|---|---|
| **Criteria** | **Description** | **Marks** |
| Communication Process Understanding | Explains the process of data communication, transmission modes, and switching methods with suitable examples | 5 |

| | | |
|---|---|---|
| Protocol & Error Handling Knowledge | Demonstrates understanding of networking protocols and error detection/control techniques used in communication networks | 5 |
| Simulation & Practical Performance | Effectively performs practical demonstrations or simulations to study network communication and protocol operations | 5 |
| Observation, Comparison & Report Preparation | Accurately presents observations, diagrams, comparison tables, findings, and final report in a proper format | 5 |
| **Total** | | **20** |

**Module 4 : Packet Tracer Network Design**

| **Program Implementation Task (20 Marks) :** | | |
|---|---|---|
| **Criteria** | **Description** | **Marks** |
| Network Topology Design | Creates a proper office network topology using PCs, switches, routers, and appropriate cable connections in Cisco Packet Tracer | 5 |
| Network Topology Design | Correctly configures VLANs, IP addresses, subnet masks, and basic router/switch settings for network communication | 5 |
| Connectivity Testing & Command Usage | Effectively uses networking commands such as ping and ipconfig to test and verify communication between devices | 5 |
| Troubleshooting & Practical Analysis | Identifies and resolves network issues related to VLANs, IP configuration, or connections, and presents proper observations and findings | 5 |
| **Total** | | **20** |

**Module 5 : Cyber Shield: Exploring and Preventing Network Attacks**

| **Program Implementation Task (20 Marks) :** | | |
|---|---|---|
| **Criteria** | **Description** | **Marks** |
| Identification of Network Attacks | Correctly identifies different types of network attacks and explains their impact on computer networks | 5 |
| Security Solution Analysis | Demonstrates understanding of security mechanisms such as cryptography, VPNs, and firewalls for network protection | 5 |
| Prevention & Risk Reduction Strategies | Suggests effective preventive measures, system improvements, and security practices to minimize network threats | 5 |
| Research, Analysis & Report Presentation | Presents clear findings, proper analysis, organized documentation, and a well-structured final report | 5 |
| **Total** | | **20** |