Gyanmanjari
Innovative University

Syllabus
Gyanmanjari Institute of Technology Semester-4
(B.Tech.)

Subject: Computer Networks: Designing and Securing Modern Communication Systems – BET1CE14309

Type of course: Professional Core

Prerequisite: Basic understanding of computer programming, data structures and operating systems

Rationale:

This course provides a comprehensive introduction to Computer Networks, focusing on the principles, design, protocols, and security of modern communication systems. It covers fundamental topics such as network models, topologies, and switching techniques, while also exploring layered architectures (OSI and TCP/IP). Students will gain knowledge of transmission media, error detection and correction, flow control, addressing, routing, and congestion management. The course also emphasizes advanced topics such as IPv6, socket programming, peer-to-peer communication, and network security. By the end of the course, learners will understand both the theoretical foundations and practical aspects of computer networks, enabling them to analyze, configure, and secure communication systems in real-world applications.

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-Class Room Instructions; T – Tutorial; P - Practical; C – Credit; SEE - Semester End Evaluation; CCE-Continuous and Comprehensive Evaluation.

Course Content:

Sr. No	Course Content	Hrs	% Weightage
1	**Introduction & Network Models** ***Theory Topics:*** Basics of Computer Networks, Goals of Networking: Resource sharing, reliability, scalability, Types of Networks: LAN, MAN, WAN, Network Topologies: Bus, Star, Ring, Mesh, Hybrid, Switching Techniques: Circuit Switching, Packet Switching, Virtual Circuits, Layering Concepts, OSI Model, TCP/IP Model, OSI vs TCP/IP Comparison ***Practicals:*** 1. Understand networking devices like hubs, switches, routers, bridges, and access points to study working and functions. 2. Design and simulate Bus, Star, Ring, Mesh, and Hybrid topologies to understand structure and communication reliability. 3. Demonstrate and compare LAN, MAN, and WAN networks in Packet Tracer to understand scale and connectivity. 4. Create a small office network with HR and Sales departments for communication and resource sharing. 5. Simulate circuit-switched and packet-switched networks in Packet Tracer to observe data flow and efficiency. 6. Analyze OSI and TCP/IP models by mapping protocols and studying encapsulation and decapsulation. 7. Perform ARP analysis by generating ARP requests and replies to observe IP-to-MAC resolution. 8. Configure static routing to enable communication between networks and verify connectivity using ping commands. 9. Capture TCP traffic in Wireshark to study handshaking, acknowledgments, and reliable data transmission. 10. Capture DNS-based UDP communication to observe fast, connectionless data transfer without handshake. 11. Use ping and traceroute to analyze connectivity, delay, and hop by hop network path movement.	18	20%

GYANMANJARI INNOVATIVE UNIVERSITY
BHAVNAGAR

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Network Design and Layer Mapping Simulation:** Students will design a suitable network topology using simulation tools and explain data flow across OSI and TCP/IP layers.	20	
2	**Active Learning Assignment: Network Topology Design and Analysis using Cisco Packet Tracer:** Each student individually designs a network in Cisco Packet Tracer, configures devices, tests communication, analyzes performance, captures screenshots, prepares a detailed PDF report, and submits it on the GMIU Web portal.		10
	Total	20	10

Examination Style:

Network Design and Layer Mapping Simulation (20 Marks)

Students will use Cisco Packet Tracer to design an appropriate network topology (Bus, Star, Ring, or Mesh) based on a given scenario. They will map data flow across OSI and TCP/IP layers, analyze device roles and protocols, and provide screenshots with clear explanations of the topology design and layer-wise communication.

Network Topology Design and Analysis using Cisco Packet Tracer (10 Marks)

Students will design and simulate various topologies (Bus, Star, Ring, Mesh, Hybrid) in Cisco Packet Tracer using PCs, switches, and routers. They will configure IPs, test connectivity, analyze performance, redundancy, and scalability, and prepare a detailed report with screenshots and observations for submission on the GMIU portal.

2	**Physical & Data Link Layer** ***Theory Topics:*** Transmission Media: Wired (coaxial, twisted pair, fiber) & Wireless (Wi-Fi, Bluetooth, Satellite), Bandwidth, Latency, Throughput, Encoding & Modulation (conceptual) , Multiplexing Techniques: TDM, FDM, WDM , Framing & Error Detection: Parity, CRC, Checksum , Error Correction Codes (conceptual) , Flow Control: Stop-and-Wait, Sliding Window (Go-Back-N, Selective Repeat) , Multiple Access Protocols: ALOHA, CSMA, CSMA/CD, CSMA/CA , Ethernet (IEEE 802.3), Token Ring, Wireless LAN (802.11 basics) , Switching Devices: Hub, Bridge, Layer-2 Switches, Point-to-Point Protocol (PPP) ***Practicals:*** 12. Wired Transmission Media Demonstration identifies and compares coaxial, twisted pair, and fiber cables. 13. Wireless Transmission Technologies Demonstration analyzes Wi-Fi, Bluetooth, and satellite communication behavior. 14. Bandwidth, Latency, Throughput Measurement calculates speed, delay, and data transfer performance. 15. Framing and Error Detection Practical applies parity and checksum to detect data errors. 16. CRC Error Detection Practical generates CRC values to verify data integrity. 17. Stop-and-Wait Flow Control Practical shows acknowledgment-based packet transmission and retransmission. 18. Sliding Window Flow Control Practical demonstrates Go-Back-N and Selective Repeat retransmissions. 19. ALOHA and Slotted ALOHA Practical observes random access collisions and network efficiency. 20. CSMA, CSMA/CD, CSMA/CA Practical analyzes wired collision detection and wireless collision avoidance. 21. Ethernet LAN Implementation Practical builds IEEE 802.3 LAN and studies MAC frame flow. 22. Wireless LAN Implementation Practical configures IEEE 802.11 Wi-Fi communication with CSMA/CA.	18	20%

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Transmission Media Design Challenge:** Students design a simulated network connecting labs, choosing media, setting bandwidth, and ensuring reliable data flow.	20	
2	**Active Learning Assignment: Ethernet Cabling and Connectivity Testing using RJ45 Connectors:** Students create a straight-through and cross-over cable using RJ45 connectors and test connectivity and need to prepare a report on given activity and upload it on the GMIU Web Portal.		10
	Total	20	10

Examination Style:

Transmission Media Design Challenge: (20 Marks)
Students create a simulated network linking multiple labs, choosing suitable transmission media, estimating needed bandwidth, and explaining how the system maintains data accuracy and smooth communication through appropriate error handling and flow management techniques.

Ethernet Cabling and Connectivity Testing using RJ45 Connectors: (10 Marks)
Students will create straight-through and cross-over UTP cables using T568A and T568B standards with RJ45 connectors. They will test connectivity using a LAN tester or network devices, understand physical layer concepts, and prepare a report with photos, screenshots, and test results for submission on the GMIU Web Portal.

3	**Network Layer** ***Theory Topics:*** IPv4 Addressing: Classes, Subnetting, CIDR , IPv6 Basics , Routing Principles: Shortest Path (Dijkstra, Bellman-Ford), Distance Vector, Link State, Flooding, Hierarchical Routing , Routing Protocols (concepts only): RIP, OSPF, BGP, IP Packet Format and Fragmentation, ARP, ICMP, DHCP, NAT ***Practicals:*** 23. Subnetting and finding network & broadcast addresses. 24. Configure IPv4 and IPv6 addresses on nodes. 25. Study of routing algorithms (Distance Vector and Link State) using simulation tools. 26. Demonstrate DHCP and NAT configuration. 27. Router Configuration: Configure static routing and RIP between 3 routers in Packet Tracer. 28. Study and demonstration of ARP (Address Resolution Protocol) using simulation tools. 29. Demonstrate ICMP operations using Ping and Traceroute commands. 30. Study of IP packet fragmentation and reassembly. 31. Configure and verify OSPF routing protocol in a simple network. 32. Study and configuration of Distance Vector routing using RIP protocol. 33. Demonstrate Static and Dynamic NAT configuration using router.	18	20%

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Subnetting and Inter-Network Communication using RIP/OSPF Protocols:** Students create a simulated network that includes subnetting for a given IP range, IP allocation for departments, and routing through RIP or OSPF in Cisco Packet Tracer, showing how communication works across interconnected networks.	20	
2	**Active Learning Assignment: Pathfinder – Dynamic & Static Routing in Action:** Students will individually use Cisco Packet Tracer to simulate and analyze routing algorithms such as Static Routing, RIP, OSPF, and EIGRP. They will observe how different routing techniques impact network performance, efficiency, and fault tolerance. The final simulation-based analysis report in PDF format will be uploaded to the GMIU Web Portal.		10
	Total	20	10

Examination Style:

Subnetting and Inter-Network Communication using RIP/OSPF Protocols: (20 Marks)
Students will perform subnetting to divide a network into smaller subnets, assign IPs and gateways, and configure routers using RIP or OSPF in Cisco Packet Tracer. They will test connectivity using ping and traceroute, justify their addressing scheme and routing choice, and submit a detailed report with configurations and observations for evaluation.

Pathfinder – Dynamic & Static Routing in Action: (10 Marks)
Students will configure static and dynamic routing (RIP, OSPF, EIGRP) in Cisco Packet Tracer to study data transfer, path selection, and fault tolerance. They will analyze performance, convergence, and routing behavior, compare both methods, and prepare a detailed PDF report with configurations, results, and observations for submission on the GMIU portal.

4	**Transport & Application Layer** ***Theory Topics:*** Transport Layer Services, Connection-Oriented vs Connectionless Protocols, UDP: Features and Header, TCP: Features, Header, Flow Control, Congestion Control (AIMD, Slow Start, Fast Retransmit, Fast Recovery), TCP Connection Establishment (3-way handshake) and Termination, Basics of Socket Programming, Application Layer Protocols: DNS, FTP, HTTP, SMTP, POP3, IMAP, Basics of Email System, Peer-to-Peer Applications ***Practicals:*** 34. Simulate TCP 3-way handshake using a packet analyzer (Wireshark). 35. Compare TCP and UDP communication using basic socket programming. 36. Configure a DNS server and perform client query resolution. 37. Demonstrate Email transmission using SMTP, POP3, and IMAP protocols. 38. Capture and analyze HTTP request and response packets using packet analyzer. 39. Study TCP flow control mechanism using sliding window concept. 40. Demonstrate TCP congestion control mechanisms (Slow Start and AIMD) using simulation or packet analysis. 41. Study TCP connection termination using four-way handshake. 42. Demonstrate FTP file transfer between client and server. 43. Simulate peer-to-peer (P2P) communication between nodes. 44. Study UDP header fields and analyze UDP packets using packet analyzer. 45. Analyze TCP header fields to understand reliability sequencing and acknowledgment mechanisms behavior.	18	20%

Evaluation Method:

Sr. No.	Evaluation Methods	SEE	CCE
1	**Network Protocol Analysis in E-Commerce Systems:** Students observe e-commerce data exchange, study TCP connection behavior, note congestion handling, and explore essential protocols using Packet Tracer or Wireshark.	20	
2	**TCP Connection Establishment and Analysis using Wireshark:** Students will use Wireshark to capture and analyze TCP 3-way handshake packets, identify SYN, SYN-ACK, and ACK segments, and understand how reliable connections are established and terminated in TCP communication. The Final report in PDF format will be uploaded to the GMIU Web Portal.		10
	Total	20	10

Examination Style:

Network Protocol Analysis in E-Commerce Systems: (20 Marks)

Students use Packet Tracer or Wireshark to observe how an e-commerce system handles data exchange, examine the TCP connection process, understand how congestion is controlled during communication, and explore essential protocols that support secure and efficient online transactions.

TCP Connection Establishment and Analysis using Wireshark: (10 Marks)

Students will use Wireshark to capture and analyze TCP three-way handshake packets, identify SYN, SYN-ACK, and ACK segments, and understand how reliable connections are established and terminated in TCP communication. After completing the analysis, students must compile their captured results and findings in PDF format and upload the file on the GMIU Portal for evaluation.

5	**Network Security** ***Theory Topics:*** Fundamentals of Network Security, Firewalls & Intrusion Detection Systems, Symmetric & Asymmetric Encryption (concepts), Authentication & Digital Signatures, Secure Protocols: SSL/TLS, HTTPS, Email Security (conceptual overview) ***Practicals:*** 46. Configure a basic firewall using software tools. 47. Demonstrate encryption and decryption using simple symmetric and asymmetric algorithms. 48. Study SSL/TLS handshaking process using Wireshark. 49. Implement a basic user authentication system using software. 50. Capture and analyze SSL/TLS handshake messages between client and secure server using Wireshark. 51. Demonstrate digital signature creation and verification using software tools. 52. Study HTTPS communication by capturing and analyzing secure web traffic. 53. Demonstrate email security concepts using encrypted email transmission simulation. 54. Study intrusion detection system (IDS) alerts using network security simulation tools. 55. Demonstrate authentication mechanism using username and password verification. 56. Analyze firewall rule ordering effects on packet filtering and network access control.	18	20%

Evaluation Method:

Sr. No.		SEE	CCE
1	**Network Security Configuration and SSL/TLS Analysis using Wireshark:** Students observe firewall behavior, study encryption and decryption, and examine SSL/TLS connection steps using Wireshark to understand secure communication processes.	20	
2	**Firewall Configuration and Traffic Monitoring Lab:** Students will configure a firewall to control network traffic using ACLs, analyze packets with Wireshark, and verify rule effectiveness. They will understand how firewalls enhance network security, document configurations, include screenshots, and submit a detailed report on the GMIU Web Portal.		10
	Total	20	10

Examination Style:

Network Security Configuration and SSL/TLS Analysis using Wireshark: (20 Marks)
Students use Wireshark and security tools to observe how a firewall handles traffic, explore basic encryption and decryption processes, examine each stage of the SSL/TLS connection, and understand how secure communication maintains confidentiality, integrity, and authentication across network interactions.

Firewall Configuration and Traffic Monitoring Lab: (10 Marks)
Students will configure a firewall using simulation tools or system settings to control network traffic with access control lists (ACLs). They will monitor packets using Wireshark to verify rule effectiveness and understand firewall protection against unauthorized access. Students will compile configurations, screenshots, and observations into a detailed report and upload it to the GMIU portal.

Suggested Specification Table:

Distribution of Marks (Revised Bloom's Taxonomy)						
Level	Remembrance (R)	Understanding (U)	Application (A)	Analyze (N)	Evaluate (E)	Create (C)
Weightage %	10%	15%	20%	15%	20%	20%

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 the above table.

Course Outcome:

After learning the course, the students should be able to:	
CO1	Explain fundamental concepts of computer networks, goals, network models, topologies, and switching techniques.
CO2	Demonstrate understanding of physical and data link layer concepts including transmission media, error detection, flow control, and multiple access protocols.
CO3	Apply addressing, routing algorithms, and protocols in the network layer for efficient data delivery.
CO4	Compare and implement transport layer mechanisms such as TCP/UDP, congestion control, and socket programming basics.
CO5	Evaluate application layer protocols (DNS, HTTP, FTP, Email) and apply security mechanisms (encryption, firewalls, SSL/TLS) to secure communication systems.

Instructional Method:

The course delivery method will depend upon the requirement of content and 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 the 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] Computer Networking: A Top-Down Approach, James F. Kurose, Keith W. Ross, Pearson.

[2] Data Communications and Networking, Behrouz A. Forouzan, McGraw-Hill.

[3] Computer Networks, Andrew S. Tanenbaum, David J. Wetherall, Pearson.

[4] Computer Communications and Networking, Atul Kahate, McGraw-Hill.

[5] Internetworking with TCP/IP, Douglas E. Comer, Pearson.

Suggested Assessment Guidelines:

MODULE 1 – Introduction & Network Models

SEE : Network Design and Layer Mapping Simulation (20 Marks)

Criteria	Description	Marks
Topology Design	Correct network topology creation with proper device selection and logical layout.	5
LayerMapping Accuracy	Accurate OSI–TCP/IP layer mapping, clear explanation of each protocol's layer role.	5
Device Configuration	Proper configuration of IP addressing, routing, connectivity testing (ping, tracert).	5
Documentation & Screenshots	Clear presentation of results, screenshots, and structured explanation.	5
Total		20

MODULE 2 – Physical & Data Link Layer

SEE: Transmission Media Design Challenge: (20 Marks)

Criteria	Description	Marks
Topology Design	Correct network topology creation with proper device selection and logical layout.	5
Layer Mapping Accuracy	Accurate OSI–TCP/IP layer mapping, clear explanation of each protocol's layer role.	5
Device Configuration	Proper configuration of IP addressing, routing, connectivity testing (ping, tracert).	5
Documentation & Presentation	Clear presentation of results, screenshots, and structured explanation.	5
Total		20

MODULE 3 – Network Layer

SEE : Subnetting and Inter-Network Communication using RIP/OSPF Protocols: (20 Marks)

Criteria	Description	Marks
Subnetting Accuracy	Correctly calculated subnets, IP ranges, valid masks, and proper address allocation.	5
Routing Configuration	Accurate RIP/OSPF setup with proper network statements and stable routing tables.	5
Communication Verification	Successful connectivity testing using ping, tracert, and route checks across all subnets.	5
Analysis & Interpretation	Clear explanation of routing behavior, screenshots, and well-structured presentation.	5
Total		20

MODULE 4 – Transport & Application Layer

SEE: Network Protocol Analysis in E-Commerce Systems: (20 Marks)

Criteria	Description	Marks
TCP Behavior Analysis	Accurate observation of TCP handshake, flow control, congestion handling, and connection behavior.	5
Protocol Interpretation	Correct interpretation of HTTP/HTTPS, DNS, SMTP, or other application-layer protocol patterns.	5
Packet Observation Accuracy	Proper packet capture, identifying flags, ports, sequence numbers, and end-to-end communication.	5
Documentation , Explanation &Viva	Clear, structured explanation with screenshots and justified analysis of protocol behavior.	5
Total		20

MODULE 5 – Network Security

SEE: Network Security Configuration and SSL/TLS Analysis using Wireshark: (20 Marks)

Criteria	Description	Marks
Firewall Configuration	Correct setup of security rules, ACLs, and filtering policies with proper justification.	5
Encryption & TLS Analysis	Accurate examination of SSL/TLS handshake, certificate details, and encryption mechanisms.	5
Security Packet Observation	Proper capture and identification of secure packet fields, flags, alerts, and communication behavior.	5
Documentation & Explanation	Clear screenshots, structured report, and well-explained security analysis and findings.	5
Total		20