NIRMA UNIVERSITY

Institute:	**Institute of Technology, School of Technology**
Name of Programme:	**BTech CSE**
Course Code:	4CS207ME25
Course Title:	**Network Administration and Security**
Course Type:	**Department Elective-IV**
Year of Introduction:	**2025-26**

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLO):

At the end of the course, the students will be able to –

1. demonstrate the principles and practices of network administration (BL2)
2. solve network infrastructure issues (BL3)
3. design and implement network infrastructure (BL6)
4. plan, secure, and optimize network infrastructure. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Network Administration:** Understanding the role of network administrators, Overview of networking components and protocols	05
Unit-II	**Network Planning and Design:** Network topologies and architecture, IP addressing and subnetting, Designing LANs and WANs	08
Unit-III	**Network Device Configuration:** Configuring routers and switches, setting up firewalls and security appliances, Managing DHCP and DNS	08
Unit-IV	**Network Security:** Introduction to network security principles, Implementing access control lists (ACLs) and firewalls, Network encryption, and VPNs	08
Unit-V	**Troubleshooting and Diagnostics:** Identifying and resolving common network issues, Network monitoring tools and techniques	08
Unit-VI	**Network Optimization:** Bandwidth Management and QoS, Load balancing and redundancy	08

Self-Study:

The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study contents

Suggested Readings/ References:

1. Jill West and Tamara Dean, *Network+ Guide to Networks*, Cengage Learning
2. Todd Lammle, Sybex, *CCNA Routing and Switching Complete Study Guide*, Wiley
3. Craig Hunt, *TCP/IP Network Administration*, O'Reilly.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Set up a basic LAN network with a router and a few switches. Configure IP addresses, subnets and test connectivity.	02
2	Configure a router with multiple interfaces, set up static routes, and test routing between different networks.	02
3	Configure a Layer 2 switch with VLANs, and assign ports to different VLANs. Test inter-VLAN routing.	02
4	Implement access control lists (ACLs) on a router to restrict traffic. Set up a basic firewall on a network segment.	04
5	Configure a DHCP server to assign IP addresses dynamically. Set up a DNS server for name resolution.	02
6	Use network monitoring tools (e.g., Wireshark, SNMP) to capture and analyze network traffic. Identify network issues.	04
7	Troubleshoot common network problems, such as connectivity issues and slow network performance, and identify the root causes.	04
8	Configure a Virtual Private Network (VPN) to connect remote users securely to the network. Test VPN connectivity.	04
9	Set up a load balancer to distribute network traffic across multiple servers. Test the load balancing configuration.	04
10	Create network documentation for the entire network setup, including diagrams, configuration files, and best practices documentation.	02