Naan Mudhalvan – Polytechnic – Even Semester 2024-25
4th Semester – Course Curriculum

ABOUT THE COURSE

COURSE NAME:	Network Essentials
TOTAL DURATION:	60 HRS
MODE OF DELIVERY	PHYSICAL CLASSROOM TRAINING AT RESPECTIVE COLLEGES
TRAINER TO STUDENT RATIO:	1:60
TOTAL MARKS:	70 (External) + 30 (Internal) **(Final Assessment shall be done by TNSDC)**

TABLE 1	
OVERALL COURSE OBJECTIVE:	● Analyse the foundational principles of networking and data communication ● Configure and secure networks using essential protocols and hardware ● Utilise practical experience with tools for network monitoring and troubleshooting ● Provide network security fundamentals, including firewalls and encryption ● Develop the skills to deploy and maintain small to medium-sized networks
LEARNING OUTCOME:	● Apply the fundamental networking concepts, protocols, and architectures, highlighting their roles in network communication ● Configure and manage IP addresses, subnetting, and basic routing to establish and optimize network connectivity ● Install and troubleshoot network devices such as switches, routers, and access points to ensure seamless network operation ● Utilize packet analysis tools to diagnose network traffic issues and maintain network performance ● Implement basic cybersecurity measures to secure network communication and protect data from unauthorized access or attacks.

TABLE 2: MODULE-WISE COURSE CONTENT AND OUTCOME				
SL. NO	**MODULE NAME**	**MODULE CONTENT**	**MODULE LEARNING OUTCOME**	**DURATION (HRS)**
1	**Introduction to Networking Basics**	Overview of Networking Concepts - Types of networks (LAN, WAN, MAN) and their applications - Key networking architecture: OSI and TCP/IP models - Core concepts such as bandwidth, latency, throughput, and data encapsulation - Importance of network topology and design in communication systems	• Simulate various network topologies • Analyze data encapsulation and communication processes • Implement basic network configurations using simulation tools	15 hrs
2	**IP Addressing and Subnetting**	Overview of Addressing Techniques - Structure and importance of IPv4 and IPv6 addressing - Subnetting techniques for efficient network segmentation - Dynamic addressing with DHCP and its role in network management	• Apply IP addressing techniques for resource optimization • Configure DHCP to manage IP address allocation • Design and implement subnetworks for efficient network segmentation	15 hrs
3	**Networking Protocols and Devices**	Overview of Protocols and Devices - Common network protocols: TCP/IP, HTTP/HTTPS, DNS, and FTP - Role and configuration of network devices: routers, switches, and access points - Building and managing small-scale networks with basic routing and switching	• Configure and manage routers and switches for seamless communication • Analyze and troubleshoot protocols using network monitoring tools	15 hrs

4	**Network Security Fundamentals**	Overview of Security Practices - Importance of firewalls, VPNs, and encryption techniques - Identifying vulnerabilities and securing communication systems - Implementing basic security measures for protecting network data	• Apply security measures like firewalls and VPNs to protect networks • Identify and mitigate potential network vulnerabilities • Secure remote access through encrypted communication channels	15 hrs
5	**Network Troubleshooting and Optimization**	Overview of Troubleshooting Techniques - Identifying common network issues like IP conflicts, latency, and DNS failures - Tools for diagnosing and resolving network problems: Ping, Traceroute, and Netstat - Optimizing network performance for scalability and reliability	• Diagnose and resolve common network problems efficiently • Optimize network performance through monitoring and traffic management • Ensure consistent and reliable communication within the network	15 hrs

TABLE 3: OVERALL COURSE LEARNING OUTCOME ASSESSMENT CRITERIA AND USECASES

LEARNING OUTCOME	ASSESSMENT CRITERIA	PERFORMANCE CRITERIA	USECASES
Designing and Implementing a Secure Network Architecture	Analyze existing network architecture and identify vulnerabilities.	Develops a secure network plan that addresses vulnerabilities, scalability, and performance.	**Use Case 1:** Analyze the existing network and design a secure architecture with flowcharts and diagrams, integrating firewalls and VPNs to ensure data protection.
Optimizing Network Performance for Business Growth	Review network performance and identify inefficiencies.	Optimizes network parameters to enhance bandwidth, reduce latency, and improve throughput.	**Use Case 2:** Use diagnostic tools like Wireshark and Ping to analyze network traffic, resolve congestion, and apply IP addressing strategies for optimal performance.
Troubleshooting and Resolving Network Issues	Use network diagnostic tools to identify and	Resolves network issues efficiently using diagnostic tools and	**Use Case 3:** Identify and resolve network issues such as DNS failures or IP conflicts using tools like

	resolve issues.	appropriate configurations.	Traceroute and ipconfig, and test post-resolution stability.
Configuring and Securing Remote Access for Employees	Assess existing remote access solutions for security gaps.	Configures secure remote access solutions that ensure privacy and ease of use.	**Use Case 4:** Set up a secure VPN and multi-factor authentication (MFA) for remote access to company networks, ensuring high security.
Integrating Emerging Technologies into Existing Networks	Research and evaluate technologies like IoT and cloud for integration.	Seamlessly integrates new technologies into the network infrastructure without compromising security.	**Use Case 5:** Implement IoT and cloud services into the network by creating an integration plan and testing system performance.
Enhancing Network Security Posture	Review and enhance network security protocols.	Implements best practices like firewalls, encryption, and IDS to fortify security.	**Use Case 6:** Strengthen network security by configuring firewalls, intrusion detection systems (IDS), and access control to prevent external threats.
Managing Network Traffic for Optimal Performance	Analyze and optimize network traffic.	Optimizes bandwidth allocation and traffic management to prioritize critical services.	**Use Case 7:** Use tools like NetFlow and Wireshark to monitor traffic, implement QoS for critical services, and ensure minimal congestion.
Setting Up and Managing Network Monitoring Tools	Configure network monitoring systems to track performance.	Provides proactive issue resolution with custom alerts and real-time monitoring.	**Use Case 8:** Set up monitoring tools like SolarWinds or Nagios, configure alerts, and monitor network devices to maintain operational integrity.
Configuring and Managing Wi-Fi Networks	Design and configure a secure and reliable wireless network.	Provides strong Wi-Fi coverage with secure access and high performance.	**Use Case 9:** Design a Wi-Fi network with optimized coverage and security protocols, and monitor ongoing performance using Wi-Fi analyzers.
Designing a Disaster Recovery Plan for Network Infrastructure	Review critical systems for disaster recovery needs.	Implements a disaster recovery plan that ensures minimal downtime and data loss.	**Use Case 10:** Create and test a disaster recovery plan that includes offsite backups and redundant systems to protect critical network infrastructure.

Automating Network Management Tasks	Automate repetitive network tasks using scripts or tools.	Develops automation processes that improve efficiency and reduce human error.	**Use Case 11:** Implement automation for network configuration and monitoring using tools like Ansible, and evaluate the impact on operational efficiency.
Implementing Zero Trust Security Architecture	Implement Zero Trust principles to enhance access control.	Ensures that all users, devices, and applications are continuously verified.	**Use Case 12:** Set up a Zero Trust security framework with multi-factor authentication and micro-segmentation to secure the network against internal and external threats.
Supporting Hybrid Cloud Networking	Configure secure connections between cloud and on-premises environments.	Seamlessly integrates cloud and on-premises systems while optimizing performance.	**Use Case 13:** Implement VPNs and optimize bandwidth for a hybrid cloud infrastructure, ensuring secure and reliable data transfer between local and cloud systems.
Implementing Redundant Network Infrastructure	Design and configure redundant network systems.	Ensures network resilience with minimal downtime during failovers.	**Use Case 14:** Set up redundant network paths and test failover mechanisms to guarantee continuous service during outages or failures.
Securing IoT Devices in a Network	Secure IoT devices and segment them from critical systems.	Protects the network from potential vulnerabilities posed by IoT devices.	**Use Case 15:** Isolate IoT devices using VLANs, configure firewalls for access control, and monitor traffic for anomalies to secure the network.
Establishing Network Policies for Bring Your Own Device (BYOD)	Define security policies for personal devices.	Implements policies and security measures for safe BYOD access.	**Use Case 16:** Set up a separate network for BYOD, enforce security protocols, and test compatibility with different personal devices to ensure network security.
Optimizing Video Conferencing Traffic	Analyze and optimize bandwidth for video conferencing services.	Prioritizes video conferencing traffic to ensure optimal performance.	**Use Case 17:** Implement QoS to prioritize video conferencing traffic, ensuring quality during peak network usage.
Conducting Penetration Testing on	Use penetration testing tools to identify	Identifies and remediates vulnerabilities by	**Use Case 18:** Use tools like Metasploit to conduct penetration tests, identify weak spots, and address

Network Infrastructure	vulnerabilities.	simulating real-world attacks.	vulnerabilities to strengthen network security.
Creating a Centralized Logging System	Set up centralized logging and monitoring systems.	Provides real-time event tracking and analysis for network performance and security.	**Use Case 19:** Implement a centralized logging system with tools like Splunk, analyze logs, and set alerts for critical events to improve security.
Migrating to IPv6	Plan and execute the transition to IPv6 addressing.	Ensures a smooth transition with minimal disruption to network operations.	**Use Case 20:** Migrate the network to IPv6 by configuring devices for dual-stack operation, testing connectivity, and addressing performance issues post-migration.

TABLE 4: LIST OF FINAL PROJECTS (20 PROJECTS THAT COMPREHENSIVELY COVER ALL THE LEARNING OUTCOME)

SL.NO	FINAL PROJECT
1	Designing and Securing a Network Architecture for Scalability and Performance
2	Optimizing Network Performance to Drive Business Growth
3	Troubleshooting Network Connectivity Issues Using Diagnostic Tools
4	Configuring and Securing Remote Access for Safe Employee Connectivity
5	Integrating Emerging Technologies (IoT and Cloud) into an Existing Network
6	Enhancing Network Security to Safeguard Against Threats
7	Managing and Optimizing Network Traffic for Improved Efficiency
8	Configuring Network Monitoring Tools for Real-Time Issue Resolution
9	Designing and Managing a Reliable Wi-Fi Network for Enterprise Use
10	Developing a Disaster Recovery Plan for Network Resilience
11	Automating Network Management Tasks for Increased Efficiency
12	Establishing a Zero Trust Security Framework for Network Protection
13	Building a Secure Hybrid Cloud Network Infrastructure
14	Designing Redundant Network Paths to Ensure Business Continuity
15	Securing IoT Devices Across the Network
16	Creating Network Policies for Secure BYOD Management
17	Optimizing Network Performance for Video Conferencing Applications
18	Conducting Penetration Testing to Identify Network Vulnerabilities
19	Setting Up a Centralized Logging System for Network Monitoring
20	Migrating Network Infrastructure to IPv6 for Future-Proof Connectivity

TABLE 5: COURSE ASSESSMENT RUBRICS (TOTAL MARKS: 70)				
ASSESSMENT CRITERIA	**DESCRIBE THE CRITERIA OF THE BELOW CATEGORY PERFORMANCE**			**TOTAL MARKS**
	FAIR	**GOOD**	**EXCELLENT**	
Practical Skills	Basic configuration and implementation with significant errors in network setup and security.	Basic configuration and implementation with significant errors in network setup and security.	Basic configuration and implementation with significant errors in network setup and security.	20
Technical Knowledge	Limited understanding of networking concepts such as IP addressing, routing, or security protocols.	Limited understanding of networking concepts such as IP addressing, routing, or security protocols.	Limited understanding of networking concepts such as IP addressing, routing, or security protocols.	10
Project Execution	Minimal completion of tasks, lacking depth or innovation in network design, troubleshooting, or optimization.	Minimal completion of tasks, lacking depth or innovation in network design, troubleshooting, or optimization.	Minimal completion of tasks, lacking depth or innovation in network design, troubleshooting, or optimization.	30
Communication and Reporting	Lacks clarity and detail in reporting, with minimal analysis and visualization of the network setup and issues.	Lacks clarity and detail in reporting, with minimal analysis and visualization of the network setup and issues.	Lacks clarity and detail in reporting, with minimal analysis and visualization of the network setup and issues.	10