iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 Issue: I Month of publication: January 2024

DOI: https://doi.org/10.22214/ijraset.2024.57862

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

Computer Network

Drashti Gudhka
Computer Engineering, K J Somaiya Polytechnic, Mumbai

Abstract: This paper presents a comprehensive overview of computer networking, covering fundamental concepts and modern advancements. It explores core networking principles, including models, architectures, and essential layers. Emphasising contemporary trends, it delves into topics like network security (Zero Trust Architecture, AI/ML), Software-Defined Networking (SDN), IoT security challenges, 5G and Mobile Edge Computing (MEC), network performance optimisation, Big Data analytics, and eco-friendly networking strategies. Aimed at students, researchers, and professionals, this overview serves as a valuable resource for understanding both foundational principles and cutting-edge developments in networking.
Keywords: Computer Networking, Network Models, SDN, IoT Security, 5G, Network Performance, Big Data, Eco-friendly Networking.

I. INTRODUCTION

Computer networking forms the bedrock of global communication and information exchange in our digitally connected world. This paper comprehensively explores networking, spanning fundamental principles and contemporary advancements.

Beginning with an overview of core networking concepts, including models, architectures, and essential layers, this paper navigates through the evolving landscape of modern networking. From heightened cybersecurity concerns to the emergence of innovative technologies like

Software-defined networking (SDN), IoT integration, 5G networks, and sustainability-driven solutions, this exploration serves as a guide for students, researchers, and practitioners seeking insights into the dynamic realm of computer networking.

A. Fundamentals of Computer Networking

1) Definition, Need, and Applications

Computer networks refer to interconnected systems enabling data sharing and communication between devices. They facilitate resource sharing, efficient communication, and remote access.

The need for computer networks arises from the demand to share resources, facilitate rapid data transfer, enhance communication, and ensure reliability through redundancy.

Applications include business collaboration, communication tools (email, video conferencing), education platforms, entertainment (online gaming, streaming), research collaboration, and infrastructure management in smart cities and IoT setups.

2) Classification Of Networks

- *LAN (Local Area Network):* Covers a small geographical area like an office, building, or campus. Usually, they are privately owned and offer high data transfer rates.
- *MAN (Metropolitan Area Network):* Spans a city or a large campus, connecting multiple LANs.
- *WAN (Wide Area Network):* Encompasses a broad geographical area, often connecting multiple cities or countries. The internet is the largest WAN, providing global connectivity.

3) Network Architecture: Client-Server, Peer-to-Peer

- *Client-Server:* Follows a centralised model where servers provide resources or services to clients (devices) upon request. It's common in business environments.

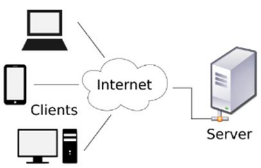

Fig.1 Client-Server Architecture

- *Peer-to-Peer:* Distributed architecture where devices act as both clients and servers, sharing resources and services directly without a central server. Often used in file-sharing networks.

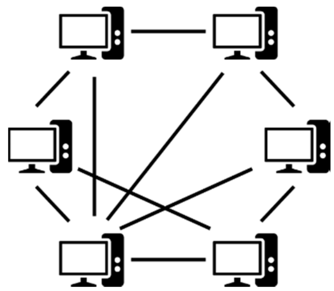

Fig. 2 Peer-to-Peer Architecture

4) Network Devices

- *Repeater:* Extends the range of a network by amplifying or regenerating signals.

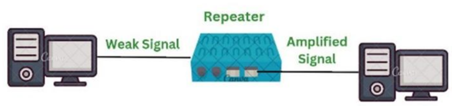

Fig. 3 Repeater

- *Bridge:* Connects two LAN segments and filters traffic based on MAC addresses.
- *Hub:* Passively broadcasts data to all connected devices in a network.

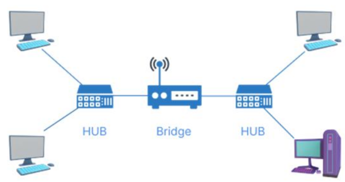

Fig. 4 Hub

- *Router:* Directs data packets between networks, determining the best path based on IP addresses.

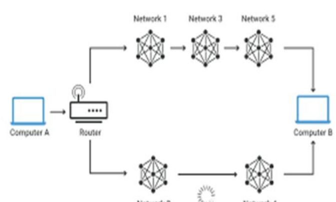

Fig. 5 Router

- *Gateway:* Connects disparate networks, translating protocols if necessary.

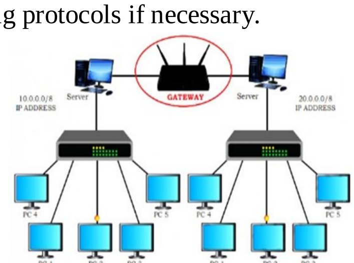

Fig. 6 Gateway

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

- *Switch:* Directs data within a network based on MAC addresses, increasing efficiency.

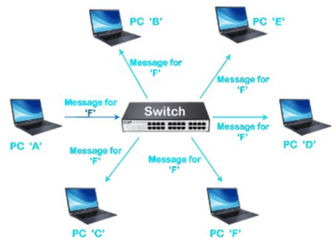

Fig. 7 Switch

- *Modem:* Converts digital data to analogue signals for transmission over communication lines.

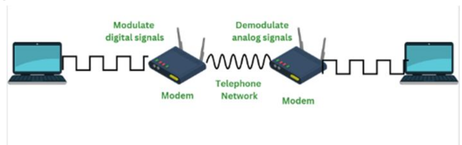

Fig. 8 Modem

5) *Network Topologies*

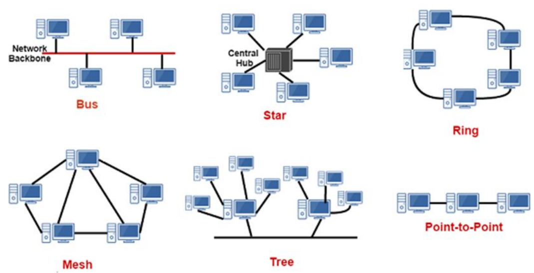

Fig. 9 Network Topologies

- *Bus:* Devices connected linearly along a single cable, sharing the same communication line.
- *Star:* Devices connected to a central hub/switch, communicating through it.
- *Ring:* Devices connected circularly, and data flows in one direction.
- *Mesh:* Every device is connected to every other device, offering redundancy.
- *Tree:* Hierarchical arrangement connecting multiple star topologies.
- *Hybrid:* Combination of two or more topologies for flexibility and scalability.

B. Network Models and Emerging Technologies

1) ISO/OSI Reference Model and TCP/IP Model Features and functions of each layer

ISO/OSI Reference Model

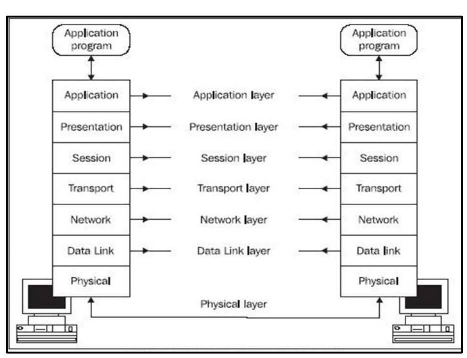

Fig. 10 ISO/OSI Reference Model

- Description: Developed by the International Organization for Standardization (ISO), this model defines a framework for network communications. It comprises seven distinct layers, each responsible for specific functions.
- Layers: Physical, Data Link, Network, Transport, Session, Presentation, Application.
- Functions:
  - *Physical:* Concerned with hardware transmission, cables, connectors, and signals.
  - *Data Link:* Manages data framing and error control within a local network.
  - *Network:* Handles routing and addressing, establishing logical paths between devices.
  - *Transport:* Ensures reliable data delivery between devices.
  - *Session:* Manages sessions between applications, and handles dialog control.
  - *Presentation:* Deals with data representation, encryption, and decryption.
  - *Application:* Provides user interface and network services to applications.

TCP/IP Model

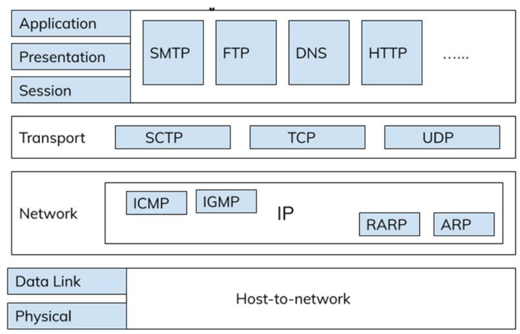

Fig. 11 TCP/IP Model

- *Description:* The Transmission Control Protocol/Internet Protocol (TCP/IP) model is the foundation of the Internet. It's a four-layered architecture.
- *Layers:* Network Interface (or Link), Internet, Transport, Application.
- *Functions*
  - Network Interface: Equivalent to both Physical and Data Link layers of the OSI model.
  - Internet: Manages IP addressing, packet routing, and basic internetworking functions.
  - Transport: Houses protocols like TCP and UDP for data delivery.
  - Application: Represents various application protocols for user interaction (HTTP, FTP, SMTP, etc.).

2) Differences between ISO/OSI and TCP/IP Mode
- *Layer Structure:* OSI has seven distinct layers, while TCP/IP combines layers for greater simplicity (four-layered).
- *Developers:* OSI was developed by ISO, while TCP/IP was developed by ARPANET and later standardized by DARPA.
- *Functionality:* Though both models facilitate communication, their layer functionality and terminologies differ.
- *Usage:* The OSI model is a conceptual model, while TCP/IP is more practical and is directly used in the internet's functioning.

3) Blockchain in Networking
- *Description:* Blockchain is a decentralized, distributed ledger technology, initially developed for cryptocurrencies like Bitcoin. In networking, it offers secure, immutable data storage and transactional transparency.
- *Applications*
  - *Secure Transactions:* Ensuring secure and tamper-proof data transfer.
  - *Decentralized Networks:* Facilitating peer-to-peer networking without centralized authorities.
  - *Smart Contracts:* Automating and securing contract execution within networks.
- *Benefits:* Improved security, transparency, and trust among network participants.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

4) *Edge Computing in Networks*

- *Description:* Edge computing brings computation and data storage closer to the data source (devices or sensors) rather than relying solely on centralized cloud servers.
- *Functions*
  - *Reduced Latency:* Processing data closer to the source reduces latency and improves response times.
  - *Bandwidth Optimization:* Minimizes data transfer to central servers, optimizing bandwidth usage.
  - *Real-time Processing:* Enables real-time analytics and decision-making.

- *Applications*
  - *IoT:* Enhancing IoT device performance and responsiveness.
  - *Industrial Automation:* Enabling faster decision-making in manufacturing processes.
  - *Autonomous Vehicles:* Processing data for immediate decisions locally.

C. *Physical & Data Link Layers*

1) *Physical Layer*

a) *Functions of the Physical Layer*

- Hardware Transmission: Manages the actual transmission of raw data bits over a physical medium.
- Physical Interface: Defines the electrical, mechanical, and procedural specifications for activating, maintaining, and deactivating physical connections.

b) *Types of Media: Guided and Unguided*

- *Guided Media:* Transmission occurs through physical cables or wires.
- *Twisted Pair:* Commonly used for telephone lines and Ethernet networks.

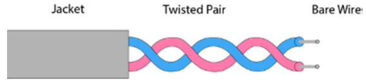

Fig. 12 Twisted Pair

- *Coaxial Cable:* Suitable for TV distribution and broadband internet.

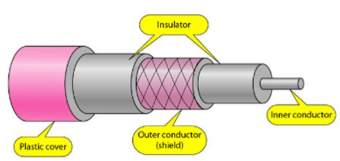

Fig. 13 Coaxial Cable

- *Optical Fiber:* Offers high-speed transmission via light pulses.

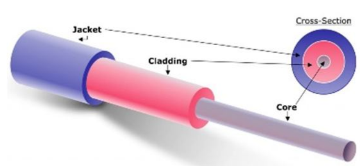

Fig. 14 Optical Fibre

- *Unguided Media:* Transmission occurs wirelessly.
- *Radio Waves:* Used in wireless networking.
- *Infrared:* Utilized in short-range communication.
- *Microwave and Lightwave Transmission:* Employed in satellite communication and high-speed networks.

c) Switching Basics

- Circuit Switching: *Establishes a dedicated communication path between nodes for the entire duration of the conversation (e.g.,* traditional phone systems).
- *Packet Switching:* Breaks data into packets that travel independently to the destination and are reassembled upon arrival (e.g., internet traffic).
- *Message Switching:* Complete messages are routed from node to node, stored temporarily at each node, and forwarded when the next node is free.

2) Data Link Layer

a) Framing Techniques and Error Detection/Correction Codes

- *Framing:* Divides data into frames for transmission, adding start and stop bits, headers, and trailers for identification and error checking.
  - *Character Count:* Uses a character count to mark the end of a frame.
  - *Character Stuffing:* Adds an escape character to the data to differentiate it from control characters.
  - *Bit Stuffing:* Inserts extra bits into the data to signify the end of a frame.

- *Error Detection/Correction Codes:* Implemented to identify and correct errors in transmitted data.
  - *Cyclic Redundancy Check (CRC):* Uses polynomial division to detect errors.
  - *Hamming Code:* Adds redundant bits to the data to detect and correct errors.

b) Protocols at this Layer

- *Simple Stop-and-Wait Protocol:* Basic protocol where the sender waits for an acknowledgement after sending each frame.
- *Sliding Window Protocols*
  - One-Bit Sliding Window Protocol: Uses a single bit to manage the flow of data.
  - Go-Back-N Protocol: Allows multiple frames to be sent without waiting for acknowledgements.
  - Selective Repeat Protocol: Enables retransmission of only lost or damaged frames.

D. Medium Access Layer (MAC)

1) CSMA Protocols and Variations

CSMA (Carrier Sense Multiple Access): A protocol used to regulate data transmission in shared media networks.

- *CSMA/CD (Collision Detection):* Commonly used in Ethernet networks. Stations listen to the network before transmitting; if a collision is detected, stations follow a backoff algorithm before reattempting transmission.
- *CSMA/CA (Collision Avoidance):* Utilized in wireless networks like Wi-Fi. Stations contend for the medium by using a 'ready to send' (RTS) and 'clear to send' (CTS) mechanism to prevent collisions.
- *Persistent and Non-Persistent CSMA:* Variations where stations either persistently listen before transmitting or wait for random time slots before retrying transmission.

2) Collision-Free Protocols

- *Bit-Map Protocol:* Utilized in LANs to prevent collisions by designating slots for specific stations.
- *Binary Countdown:* Stations contend for the medium by decrementing a counter until it reaches zero, allowing transmission.

3) IEEE Standards: 802.4 (Token Bus), 802.5 (Token Ring)

- *802.4 (Token Bus):* Defines a LAN access method using a token-passing scheme over a bus topology, ensuring fair access to the medium.
- *802.5 (Token Ring):* Utilizes a token-passing mechanism in a ring topology where a token circulates, granting permission for stations to transmit data.

4) Bluetooth: Architecture and Applications

- *Architecture:* Bluetooth is a wireless technology designed for short-range communication between devices.

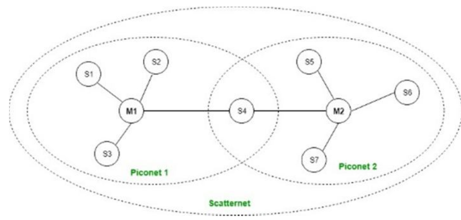

Fig. 15 Bluetooth Architecture

- *Piconet:* Basic unit of a Bluetooth network, comprising one master device and up to seven slave devices connected in a star topology.
- *Scatternet:* Network formed when multiple piconets are interconnected.

- *Applications*
- *Wireless Personal Area Networks (WPANs):* Bluetooth enables connections between devices such as smartphones, laptops, headsets, and IoT devices.
- *Hands-Free Systems:* Bluetooth is widely used in car systems for hands-free calling.
- *Wireless Audio Devices:* Headphones, speakers, and other audio devices often utilize Bluetooth for connectivity.

E. Network and Transport Layers

1) Network Layer

a) Functions of the Network Layer

- *Routing:* Determines the best path for data packets between source and destination across interconnected networks.
- *Logical Addressing:* Assigns logical addresses (IP addresses) to devices for identification and addressing purposes.
- *Packet Forwarding:* Directs packets based on logical addressing information (IP addresses).

b) IP Addressing: Classful and Classless, Subnetting, Masking

- *Classful IP Addressing:* Divides IP addresses into five classes (A, B, C, D, E) based on the leading bits of the address.
- *Classless IP Addressing (CIDR):* Uses variable-length subnet masks (VLSM) and super-netting to efficiently allocate IP addresses.
- *Subnetting:* Divides a network into smaller subnetworks for better management and efficiency.
- *Masking:* Applies a subnet mask to an IP address to determine the network and host portions.

c) Overview of IPv4 and IPv6, their Differences and Features

- *IPv4:* 32-bit address, in decimal format (e.g., 192.168.1.1). Limited address space (4.3 billion addresses).
- *IPv6:* 128-bit address, in hexadecimal format (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Offers a significantly larger address space.
- *Differences:* IPv6 offers enhanced security, better support for mobile networks, and improved efficiency compared to IPv4.

d) Routing Protocols, ARP, RARP, ICMP

- *Routing Protocols:* Algorithms used by routers to determine the best path for packet forwarding. Examples include OSPF, RIP, and BGP.
- *ARP (Address Resolution Protocol):* Resolves IP addresses to MAC addresses within a local network.
- *RARP (Reverse Address Resolution Protocol):* Maps MAC addresses to IP addresses, primarily in diskless workstations.
- *ICMP (Internet Control Message Protocol):* Manages error reporting and diagnostic functions, including ping and traceroute.

2) Transport Layer

a) Functions of the Transport Layer

- *Segmentation and Reassembly:* Divides data into smaller segments for transmission and reassembles them at the receiving end.

- *End-to-End Communication:* Ensures reliable and orderly data delivery between end systems.
- *Flow Control and Error Checking:* Manages data flow and implements error detection mechanisms.

b) TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)

- *TCP:* Offers reliable, connection-oriented, and error-checked delivery of data.
  - *Features:* Connection establishment, reliable data delivery, flow control, and error detection through sequence numbers and acknowledgements.
  - *Header Format:* Contains source and destination port numbers, sequence numbers, acknowledgement numbers, and control flags.

- *UDP:* Provides unreliable, connectionless, and faster transmission.
  - *Features:* Minimal overhead, no connection establishment or error recovery.
  - *Header Format:* Contains source and destination port numbers and a checksum for error detection.

F. Session and Application Layers

1) Session layer

a) Functions of the Session Layer

- *Dialog Control:* Establishes, maintains, and terminates sessions between applications.
- *Synchronization:* Allows checkpoints during data exchange to enable recovery if the session is disrupted.
- *Token Management:* Manages token passing in token-based networks.

b) Protocols at the Session Layer

- *RPC (Remote Procedure Call):* Allows a program to execute code on another computer or server over a network.
- *NetBIOS (Network Basic Input/Output System):* Provides communication services between applications on separate computers.

2) Application Layer

a) Functions of the Application Layer:

- *Data Representation and Encryption:* Converts data formats and encrypts/decrypts data for secure transmission.
- *Resource Sharing:* Facilitates file access, printing, and other resource sharing within a network.
- *User Interface and Network Services:* Provides user interfaces and network services for applications to access the network.

b) Protocols at the Application Layer

- *SNMP (Simple Network Management Protocol)*
  - *Function:* Manages and monitors network devices and their functions.
  - *Use:* Allows network administrators to manage network performance, detect and solve network problems, and plan for network growth.
- *POP3 (Post Office Protocol version 3)*
  - *Function:* Retrieves emails from a server and downloads them to a local email client.
  - *Use:* Commonly used for downloading emails and managing mailboxes.
- *IMAP4 (Internet Message Access Protocol version 4)*
  - *Function:* Retrieves emails from a server and allows manipulation without downloading.
  - *Use:* Suitable for managing emails across multiple devices without downloading them.
- *SMTP (Simple Mail Transfer Protocol)*
  - *Function:* Sends emails between servers.
  - *Use:* Responsible for the transmission of emails over the internet.
- *E-MAIL Protocol (Extended MAIL Protocol)*
  - *Function:* Provides a framework for managing and exchanging emails.
  - *Use:* Supports various operations like message submission, retrieval, and deletion.

G. Advanced Networking Topics

1) *Network Security*
a) *Zero Trust Architecture*
- *Definition:* Security framework where no one is trusted by default, and every device, user, or application must be verified before gaining access.
- *Implementation:* Relies on continuous verification and strict access controls, using identity verification, encryption, and micro-segmentation.

b) *AI/ML in Security*
- *Application:* Utilized for threat detection, anomaly detection, pattern recognition, and behavioural analysis to enhance cybersecurity.
- *Use Cases:* Predictive analysis, malware detection, and user behaviour analysis for identifying suspicious activities.

2) *Software-Defined Networking (SDN)*
a) *Cloud Networks*
- *Integration with SDN:* Utilizes SDN principles to create agile, scalable, and programmable cloud networks.
- *Benefits:* Offers centralized control, automation, and flexibility in managing cloud resources.

b) *Intent-Based Networking*
- *Definition:* A network architecture that allows administrators to define network behaviour and policies in simple, high-level terms.
- *Advantages:* Improves automation, reduces errors, and aligns network operations with business intent.

3) *Internet of Things (IoT) Security*
a) *Challenges:* Unique security challenges due to the massive number of connected devices, diverse communication protocols, and varying security capabilities.
b) *Solutions:* Encryption, authentication, secure device provisioning, and continuous monitoring to mitigate vulnerabilities.

4) *Edge Computing in IoT*
a) *Definition:* Processing data near the data source (IoT devices) rather than relying solely on centralized cloud servers.
b) *Benefits:* Reduced latency, bandwidth optimization, real-time processing, and improved scalability.

5) *Wireless and Mobile Networks*
a) *5G Networks*
- *Features:* High data speeds, low latency, increased device connectivity, and support for IoT.
- *Use Cases:* Enhanced mobile broadband, mission-critical communications, and massive IoT deployments.

b) *Mobile Edge Computing (MEC)*
- *Definition:* Brings cloud computing closer to the mobile user by placing servers at the edge of the mobile network.
- *Advantages:* Low latency, improved performance, and real-time data processing for mobile applications.

6) *Network Performance Optimization*
a) *QoS in Multimedia Networks*
- *Quality of Service (QoS):* Ensures high-quality transmission of multimedia data by prioritizing bandwidth and minimizing latency.
- *Use Cases:* Video conferencing, streaming, online gaming.

b) *Traffic Analysis*
- *Purpose:* Studies patterns, behaviours, and data flow within networks to optimize traffic management and resource allocation.

7) *Big Data in Networking*
a) *Network Data Analytics*
- *Utilization:* Analyzes large volumes of network data to derive insights, detect anomalies, and improve network performance.

b) *Data-driven Network Management*
- *Approach:* Uses data analytics to optimize network operations, predict failures, and enhance security.

8) *Green Networking*
a) *Energy-Efficient Networks*
- *Focus:* Reducing power consumption by optimizing hardware, protocols, and network configurations.

b) *Eco-Friendly Network Design*
- *Objective:* Reducing the carbon footprint through efficient network infrastructure and design.

II. CONCLUSIONS

In conclusion, computer networking stands as the backbone of modern global communication, embodying a dynamic amalgamation of foundational principles and cutting-edge innovations. From the essential frameworks and architectures to the emergence of groundbreaking technologies, this exploration elucidates the intricate tapestry of connectivity that defines our digital landscape. As networks evolve, embracing transformative paradigms such as Software-defined Networking (SDN), IoT integration, and sustainability-driven solutions becomes pivotal, shaping a future where networks are not just efficient but also adaptable and secure

III. ACKNOWLEDGEMENT

We express sincere gratitude to the dedicated minds and collaborative efforts shaping the realm of computer networking. Our appreciation extends to the researchers, educators, and practitioners whose contributions drive the evolution of networking technologies. Special thanks to the trailblazers, whose vision and innovation pave the way for transformative advancements, enabling us to navigate the ever-expanding horizons of networked connectivity

REFERENCES

Books
[1] "Computer Networking: A Top-Down Approach" by James F. Kurose and Keith W. Ross
[2] "Computer Networks" by Andrew S. Tanenbaum and David J. Wetherall
[3] "TCP/IP Illustrated, Volume 1: The Protocols" by W. Richard Stevens
[4] "Blockchain Basics: A Non-Technical Introduction in 25 Steps" by Daniel Drescher
[5] "Edge Computing: A Primer" by Hsinchun Chen and George F. Luger
[6] "5G NR: The Next Generation Wireless Access Technology" by Erik Dahlman, Stefan Parkvall, and Johan Skold

Websites
[1] Cisco Networking Academy - Networking Basics
[2] NetworkWorld - Networking & Security Section
[3] IEEE Xplore Digital Library
[4] Cloudflare Blog
[5] The Linux Foundation