PAPER ENGLISH AND COMMUNICATION SKILL

“Network and Communication Systems”

UIN IMAM BONJOL
PADANG

Supporting lecturer:

Renggi Vrika, M.Pd

By:

Beryl Cholif Arrahman Meuraxa	2117020030
Rabbiatul Rafiah Salamah	2117020035
Atika Reizky Marini	2117020082

INFORMATION SYSTEMS STUDY PROGRAM

FACULTY OF SCIENCE AND TECHNOLOGY

IMAM BONJOL STATE ISLAMIC UNIVERSITY

PADANG

2024

Foreword

The author would like to express his praise and gratitude to Allah Almighty for His grace and blessings so that the author could complete the paper entitled "Network and Communication Systems". The aim of writing this paper is to fulfill an assignment for the English For Reading And Communication Skills course.

The author is fully aware that the completion of this paper cannot be separated from the support, encouragement and guidance, as well as prayers from various parties. Therefore, the author would like to express his deepest gratitude to Mrs. Renggi Vrika, M. Pd as a lecturer in the English For Reading And Communication Skills course. who have provided time, energy, thoughts and support in the form of direction and guidance so that this paper can be completed well. Parents who always provide prayers and motivation, as well as very meaningful support, encourage the author to do his best. The author hopes that Allah SWT will give abundant rewards for the goodness that has been given to the author.

The author feels that there are still many shortcomings in writing this paper. Therefore, the author really hopes for criticism and suggestions from readers to improve this paper.

Padang, 7 May 2024

Group 8

Table of Contents

Chapter I Introduction

A. Background

In the continuously evolving digital era, networks and communication systems play a central role in facilitating interactions among individuals, devices, and organizations worldwide. With the increasing adoption of Information and Communication Technology (ICT), networks have become the backbone of digital infrastructure connecting people, devices, and data across various parts of the world. In this introduction, we will explore the importance of networks and communication systems in the context of the modern world.

Computer networks enable the exchange of information among individuals, organizations, and machines worldwide quickly and efficiently. Through networks, we can send messages, transfer data, access resources, and collaborate in real-time, overcoming geographical and time barriers. In the business world, reliable networks enable companies to optimize business processes, enhance productivity, and achieve competitive advantages.

Meanwhile, communication systems form the foundation for various technological applications, ranging from mobile phones to the internet. Effective communication allows for rapid and accurate information exchange, facilitating cooperation and coordination among individuals and groups. In the social context, communication systems play a crucial role in expanding social networks, promoting awareness, and facilitating positive social change.

B. Problem Formulation

1. What are the fundamentals of computer networks?
2. What are the types of networks?
3. What is communication protocol?
4. What are the latest communication technologies?
5. What is network security?

C. Objectives

1. To understand the fundamentals of computer networks
2. To identify the types of networks
3. To understand communication protocols
4. To explore the latest communication technologies
5. To comprehend network security

Chapter II Discussion

A. Fundamentals of Computer Networks

1. Definition and Basic Concepts of Computer Networks

A computer network is a collection of hardware and software that are interconnected, enabling data communication between users, devices, and applications. The main purpose of computer networks is to enable resource sharing, such as printers, files, and internet connections, as well as facilitate communication between connected users[1].

The basic concepts of computer networks include:

- Node: Each individual device in the network, such as a computer, printer, or router, is referred to as a node.
- Link: The physical or wireless connection between two nodes in the network is called a link. These links can be copper cables, optical fibers, or wireless signals.
- Topology: The physical or logical arrangement of nodes and links in the network is called topology. Examples of topologies include star topology, mesh topology, and bus topology.
- Protocol: Rules and procedures that govern communication between nodes in the network are called protocols. Protocols determine message formats, transmission methods, and error detection and correction mechanisms.

2. OSI (Open Systems Interconnection) Model and Its Role in Networking

The OSI model is a standard framework used to understand and design computer networks. This model consists of seven layers, each having specific functions in the communication process. These layers are:

a. Physical Layer: Responsible for transferring bits between devices and handling the physical aspects of data transmission, such as cables and electrical signals.

b. Data Link Layer: Handles the delivery of data frames between two connected nodes in the network. It is also responsible for detecting and correcting errors that occur at the physical level.

c. Network Layer: Manages data routing through the network from source to destination. This involves addressing, routing, and delivering data packets between networks.

d. Transport Layer: Provides mechanisms for reliable data delivery between applications on communicating nodes. It includes segmentation, data delivery, and error recovery.

e. Session Layer: Responsible for managing and maintaining communication sessions between applications on communicating nodes. This involves opening, managing, and closing communication sessions.

f. Presentation Layer: Handles encryption, compression, and data formatting to ensure compatibility between different systems.
g. Application Layer: Provides an interface for user applications and supports services used for resource and information sharing.

The OSI model aids in a systematic understanding of how data is transferred across networks and enables seamless interconnection between different devices and protocols. Thus, this model serves as an important foundation in the design, development, and troubleshooting of computer networks[2].

B. Types of Networks

1. LAN (Local Area Network)

Definition: LAN is a computer network that covers a limited geographical area, such as a building, campus, or specific room. Typically, LAN connects devices such as computers, printers, and servers within an organization.

Advantages:

- High Speed: Due to its short distance, LAN often has high data transfer speeds.
- Low Cost: Installation and maintenance costs of LAN are usually lower compared to larger networks.
- Easy to Manage: Due to its small size, LAN is easier to manage and monitor.

Examples of Usage:

- Office: For sharing files, printers, and computing resources.
- Home: To connect devices such as computers, laptops, printers, and smart devices.

2. WAN (Wide Area Network)

Characteristics: WAN is a computer network that covers a wide geographical area, often spanning countries, continents, or even the entire globe. WAN uses various technologies to connect distant locations, such as fiber optics, copper cables, and satellite signals.

Differences from LAN:

- Scale: WAN is much larger than LAN and covers a wide area.
- Speed: Due to long distances and complexity, WAN tends to have slower data transfer speeds than LAN.
- Cost: The construction and maintenance costs of WAN are usually higher compared to LAN.

Examples of Famous WANs:

- Internet: It is the largest WAN connecting millions of computers worldwide.
- Corporate Networks: Many multinational companies use WAN to connect their offices in different countries.

3. WLAN (Wireless Local Area Network)

   WLAN uses wireless technology, such as Wi-Fi, to connect devices in a limited geographical area without physical cables.

   Advantages:

   - Flexibility: Users can move freely without being restricted by physical cables.
   - -Scalability: It is easy to add or remove devices in the network without requiring new cable installations.
   - -Easy Access: Users can connect to the network by using devices that support Wi-Fi.

   Disadvantages:

   - Vulnerable to Interference: WLAN signals can be affected by interference such as walls, electronic devices, or other interferences.
   - Security: WLAN is vulnerable to security attacks such as sniffing and identity theft if not properly configured.

4. MAN (Metropolitan Area Network)

   MAN is a computer network that covers a larger geographical area than LAN but smaller than WAN. Usually, MAN covers a city or a specific metropolitan area.

   When is it Used:

   - City Government: To provide services such as public transportation, traffic monitoring, and city security.
   - Corporations: Some large companies use MAN to connect their offices across the city or metropolitan area.

By understanding the characteristics, advantages, and disadvantages of these various types of networks, organizations can choose the network infrastructure that suits their needs, whether for local environments or broader scopes[3].

C. Communication Protocols

1. TCP/IP (Transmission Control Protocol/Internet Protocol)

   Introduction: TCP/IP is a set of communication protocols used to govern data communication on the internet and other computer networks. This protocol consists of two main parts: TCP (Transmission Control Protocol) and IP (Internet Protocol)[4].

Functions:

- TCP: Provides a reliable connection between two devices by ensuring the delivery of data in sequence, without duplication, and without corruption.
- IP: Responsible for transmitting data packets between nodes in the network by determining the destination address and finding the best route for delivery.

Protocol Structure:

- TCP: Involves connection establishment, data transfer, flow control, and error recovery.
- IP: Involves determining packet delivery routes, packet fragmentation and reassembly, and address processing.

2. UDP (User Datagram Protocol) vs. TCP (Transmission Control Protocol)
   Comparison:
   - UDP:
     a. Lightweight and fast connectionless protocol.
     b. No error correction or data retransmission mechanisms.
     c. Suitable for applications that require fast data transfer, such as streaming video or online gaming.
   - TCP:
     a. Reliable and dependable connection-oriented protocol.
     b. Provides error correction, data retransmission, and flow control mechanisms.
     c. Suitable for applications that require guaranteed and ordered data delivery, such as file transfers and web browsing.

   Utilization:

   - UDP: Used for applications that require fast and real-time data transfer, where speed is more important than reliability, such as in video streaming and online gaming.
   - TCP: Used for applications that require reliable and guaranteed data delivery, where data integrity is more important than speed, such as in file transfers, web browsing, and email.

3. HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure)
   Definition:

- HTTP: A communication protocol used to transfer hypertext data (web documents) over the internet.
- HTTPS: A secure version of HTTP that uses SSL/TLS encryption to protect data transferred between the client and server.

Differences:

- HTTP: Sends data openly over the network, vulnerable to hacker attacks and data theft.
- HTTPS: Secures communication with encryption, ensuring the confidentiality, integrity, and authenticity of transferred data.

Importance in Web Browsing:

- HTTP: Used to access web content in a standard manner but may leave users vulnerable to hacker attacks exploiting vulnerabilities in open communication.
- HTTPS: Important to maintain user privacy and data security while browsing the web, especially in terms of logins, online payments, and exchange of sensitive information.

D. Cutting-Edge Communication Technologies

1. 5G

5G is the latest generation in the evolution of cellular telecommunication technology promising significantly higher speeds and connections than its predecessors. It encompasses various technologies such as MIMO (Multiple Input Multiple Output), beamforming, and millimeter wave frequencies[5].

Impact:

5G has the potential to revolutionize how we communicate, work, and interact with the world around us. With much higher speeds, better connectivity, and faster response times, 5G can drive innovation in various fields including medical technology, transportation, industry, and entertainment.

Some potential applications of 5G include:

- Advanced and widespread Internet of Things (IoT).
- Autonomous vehicles and connected cars.
- Low-latency streaming and gaming services.
- Telemedicine and remote healthcare.
- Industry 4.0 and smart manufacturing.
- Smart cities and connected urban infrastructure.

2. Internet of Things (IoT)

IoT refers to a network of connected physical devices that can communicate with each other over the internet. It encompasses everything from smart home devices like lights and door locks to industrial sensors deployed in factories and urban infrastructure.

Implementing IoT involves the use of sensors, hardware, software, and network infrastructure to collect, transfer, and analyze data from various sources. This enables better monitoring and control of environments, processes, and systems.

Some challenges in implementing IoT include:

- Security and data privacy vulnerabilities to cyber-attacks.
- Standardization and interoperability between various platforms and devices.
- Management and analysis of large and complex data.
- Availability of network infrastructure required to support rapid IoT growth.

3. Cloud Computing

Cloud computing is a computing service model that enables easy, flexible, and on-demand access to computing resources such as servers, data storage, and applications over the internet. Cloud services are typically provided by cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform.

Some advantages of cloud computing include:

- Scalability: Ability to scale computing resources according to demand.
- Cost efficiency: Pay-per-use model reduces upfront investment costs in IT infrastructure.
- Accessibility: Easy access from anywhere with an internet connection.
- Flexibility: Ability to access various services and applications without physical limitations.

There are several cloud service models, including:

- Infrastructure as a Service (IaaS): Provides access to basic computing infrastructure such as virtual servers, storage, and networking.
- Platform as a Service (PaaS): Provides development and testing environments for building, testing, and deploying applications.
- Software as a Service (SaaS): Provides hosted software applications accessed over the internet, such as productivity apps and management software.

E. Network Security

1. Network Security Threats

- Malware : Malware, short for malicious software, refers to any software designed to cause harm to a computer, server, or network. This includes viruses, worms, Trojans, ransomware, spyware, and adware. Malware can compromise network security by stealing sensitive information, disrupting operations, or gaining unauthorized access to systems.

- DoS (Denial of Service) Attacks: DoS attacks aim to make a network or system unavailable to its intended users by flooding it with excessive traffic or overloading its resources. This prevents legitimate users from accessing services or resources, causing disruptions and downtime. Distributed Denial of Service (DDoS) attacks involve multiple compromised devices targeting a single system, amplifying the impact of the attack.
- Other Threats: Other network security threats include phishing attacks, social engineering, man-in-the-middle attacks, insider threats, and zero-day exploits. These threats exploit vulnerabilities in network infrastructure, software, or human behavior to gain unauthorized access, steal data, or disrupt operations.

2. Security Solutions
    - Encryption: Encryption is the process of encoding information in such a way that only authorized parties can access it. It scrambles data into an unreadable format using encryption algorithms and requires a decryption key to convert it back into its original form. Encryption protects data confidentiality and integrity, ensuring that sensitive information remains secure during transmission and storage.
    - Firewalls: Firewalls are network security devices that monitor and control incoming and outgoing traffic based on predetermined security rules. They act as barriers between internal networks and external networks (such as the internet), filtering out potentially harmful traffic and preventing unauthorized access to network resources. Firewalls can be hardware-based or software-based and are essential for enforcing network security policies and protecting against various threats.
    - Anti-Malware Software: Anti-malware software, also known as antivirus or anti-malware programs, detects, prevents, and removes malicious software from computers and networks. These programs scan files, emails, websites, and other digital assets for known malware signatures or suspicious behavior patterns. By regularly updating malware definitions and scanning systems for threats, anti-malware software helps mitigate the risk of malware infections and protects network devices from compromise.

Implementing a combination of encryption, firewalls, anti-malware software, and other security measures is crucial for safeguarding network infrastructure and data against a wide range of security threats. Additionally, maintaining regular security updates, conducting security audits, and educating users about security best practices are essential components of a comprehensive network security strategy[6].

Chapter 3 Conclusion

A. Conclusion

Computer networks enable the exchange of information among individuals, organizations, and machines worldwide quickly and efficiently. A computer network is a collection of hardware and software that are interconnected, enabling data communication between users, devices, and applications. The main purpose of computer networks is to enable resource sharing, such as printers, files, and internet connections, as well as facilitate communication between connected users.

Network Types, such as LAN (Local Area Network), WAN (Wide Area Network), WLAN (Wireless Local Area Network), MAN (Metropolitan Area Network). Communication Protocol consist of TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol) vs. TCP (Transmission Control Protocol), HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure). As for cutting edge communication technologies which consist of 5G, Internet of Things (IoT), and Cloud Computing. Computer networks also have network security

References

[1] S. Pujowati and B. B. Harianto, *Pengenalan Dasar Jaringan Komputer*. Penerbit Pustaka Rumah C1nta, 2021.

[2] A. Wimatra, P. Sunardi, and R. Saputro, “Dasar–dasar komputer,” *Medan Civ.*, 2008.

[3] E. V. Haryanto, *Jaringan Komputer*. Penerbit Andi, 2012.

[4] D. N. H. Apriawan, “Protokol Jaringan Komputer,” *Ilmu Komput.*, 2013.

[5] I. P. Hadi, M. Wahjudianata, and I. I. Indrayani, “Komunikasi massa,” *KOMUNIKASI MASSA*. CV. Penerbit Qiara Media, 2020.

[6] T. Karygiannis and L. Owens, *Wireless Network Security:*. US Department of Commerce, Technology Administration, National Institute of …, 2002.