NAME: TANKISO MASOEBE

DATA COM WEEK 9

1. **Scenario Analysis**

In a VoIP (Voice over Internet Protocol) system, the OSI model plays a vital role in ensuring smooth voice communication across networks. When a user initiates a voice call, the **Application layer (Layer 7)** handles the VoIP application, such as Zoom or Skype. The **Presentation layer (Layer 6)** encodes and compresses audio data, while the **Session layer (Layer 5)** manages call setup, control, and termination. The **Transport layer (Layer 4)** ensures data delivery using UDP for real-time voice transmission. The **Network layer (Layer 3)** routes the voice packets across different networks using IP addresses. The **Data Link layer (Layer 2)** provides error detection and frame synchronization over local area networks. Finally, the **Physical layer (Layer 1)** transmits the digital voice signals as electrical or optical pulses through cables or wireless media. Together, these layers enable reliable and efficient real-time voice communication over the internet.

2. **Concept Research**

The Transport layer, the fourth layer of the OSI model, is responsible for reliable data transfer between devices over a network. It ensures that data is delivered accurately, completely, and in the correct sequence. This layer manages end-to-end communication, flow control, segmentation, error detection, and retransmission of lost packets. Two main protocols operate at this layer: **Transmission Control Protocol (TCP)** and **User Datagram Protocol (UDP)**. TCP provides reliable, connection-oriented communication by establishing a session before data transfer and confirming successful delivery. In contrast, UDP offers faster, connectionless communication without guaranteeing delivery, commonly used for real-time applications like video streaming and VoIP. The Transport layer also assigns port numbers to applications, allowing multiple network processes to operate simultaneously. Overall, it acts as a bridge between the application and network layers, ensuring efficient and controlled data communication between systems on a network.

3.Tool Practice

Using Wireshark to analyze network packets provided a clear understanding of how data travels across layers in the OSI model. By capturing live traffic, I observed packet details such as source and destination IPs, protocols, and port numbers. I identified TCP and UDP packets, seeing how TCP ensures reliability through acknowledgments and sequence numbers. The color-coded display made it easy to differentiate between protocols like HTTP, DNS, and ARP. This exercise helped me connect theoretical OSI concepts to real-world network behavior. Overall, Wireshark proved to be a powerful tool for troubleshooting and studying network communication in detail

Application Practice

When troubleshooting a network issue using the OSI model, it's effective to start from either the **Physical layer (bottom-up)** or **Application layer (top-down)**, depending on the problem. Begin at the **Physical layer** by checking cables, connectors, and device power. Next, verify the **Data Link layer** for network card status and MAC address configuration. At the **Network layer**, ensure IP addresses, gateways, and routing tables are correct. Move to the **Transport layer** to test connectivity with tools like *ping* or *netstat* and check for port blocking. Then, inspect the **Session layer** to confirm that sessions are properly established. At the **Presentation layer**, verify data format compatibility and encryption settings. Finally, check the **Application layer** by testing user applications or services such as email or web browsers. Document each step and result to identify where communication fails. This structured approach isolates problems quickly and ensures effective troubleshooting