Week-1  
Assignment

Celebal Summer Internship 2025



#### By [Tushar Tak](mailto:tushartak.work@gmail.com) Jun 8, 2025

## Table of content

* Introduction
* Working of OSI Model
* Working of TCP/IP Model
* TCP & UDP Protocols
* Working of HTTP, HTTPS, and ICMP Protocols
* Conclusion
* References

## 

## Introduction

In modern-day computing, the exchange of data across diverse devices and networks is fundamental. To ensure smooth and structured communication between systems, networking models and protocols were developed. These models define how data travels from one point to another, ensuring consistency, interoperability, and security across platforms.

This document explores key networking frameworks such as the OSI Model and TCP/IP Model, along with widely used protocols including TCP, UDP, HTTP, HTTPS, and ICMP. The purpose of this R&D document is to gain a thorough conceptual understanding of these networking fundamentals, and to relate them to practical use cases during internship tasks.

Why These Models and Protocols Are Used:

* To define and manage end-to-end communication between applications and devices.
* To ensure reliable data transmission using protocols like TCP.
* To support real-time and fast communication where reliability is less critical using UDP (e.g., video streaming, gaming).
* To enable secure and encrypted communication over the internet through HTTPS.
* To allow systems to perform diagnostics and error reporting using ICMP (e.g., ping, traceroute).

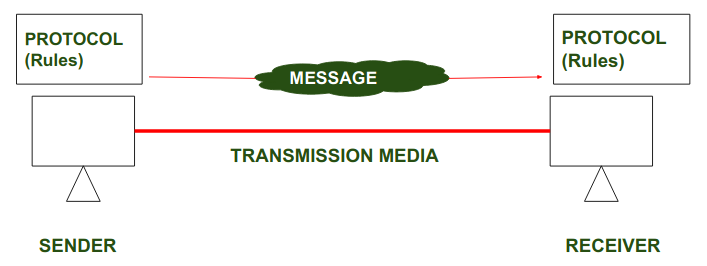


Figure 1: Data Transmission

## Working of OSI Model

* The Open Systems Interconnection (OSI) Model is a standard framework that helps us understand how communication happens between different devices over a network. It was developed by the International Organization for Standardization (ISO) and is still widely used today, especially for learning, troubleshooting, and designing network systems.
* The OSI model breaks down the complex process of network communication into seven distinct layers. Each layer has a specific role and interacts with the layers directly above and below it. This layered approach makes it easier to understand how data moves from one computer to another and helps in isolating problems when something goes wrong in a network.
* To better understand how the OSI model works, let’s walk through each of its seven layers:

1. **Application Layer:** This is the topmost layer, closest to the end-user. It allows users to interact with the network using protocols like HTTP, SMTP, and FTP. Web browsers, email clients, and file-sharing tools operate here.
2. **Presentation Layer :** This layer focuses on data formatting, encryption, and compression. It ensures that the data sent by the application layer of one system can be read and interpreted by the application layer of another.
3. **Session Layer :** It manages sessions between applications. This includes establishing, maintaining, and ending connections. It also helps with things like authentication and reconnection in case of session drops.
4. **Transport Layer :** This layer ensures reliable or fast delivery of data between systems. Protocols like TCP (reliable, connection-based) and UDP (faster, connectionless) operate here.
5. **Network Layer :** The Network Layer handles routing and addressing. It decides how data packets should be forwarded across different networks using IP addresses. Routers work at this layer.
6. **Data Link Layer :** This layer is responsible for node-to-node data transfer, error detection, and handling MAC addresses. Technologies like Ethernet and Wi-Fi operate at this layer. It ensures that data frames are sent and received properly.
7. **Physical Layer :** This is the lowest layer. It deals with the actual hardware transmission of raw binary data (0s and 1s) over cables, fiber optics, or wireless signals. It defines things like voltage levels, pin layouts, and physical connectors.

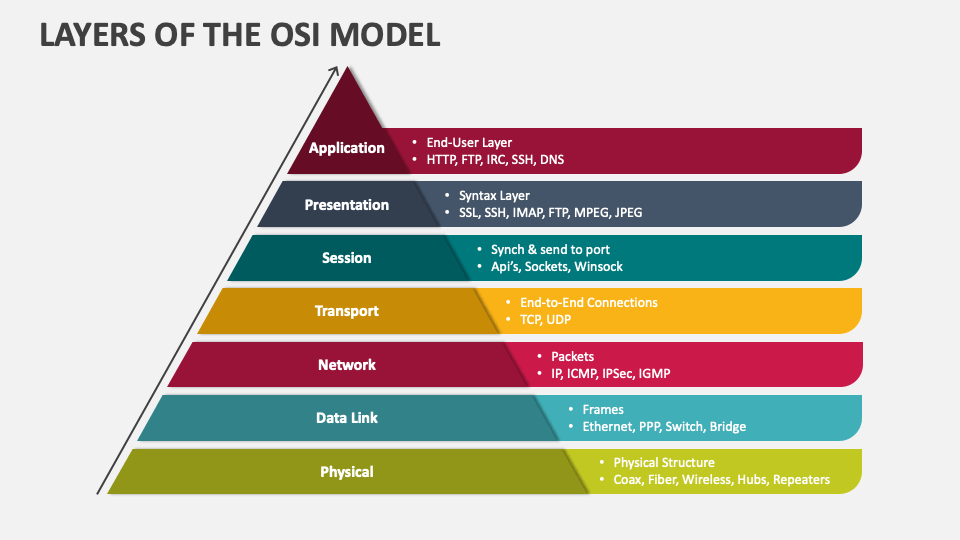


Figure 2: Layers of OSI Model

* Why the OSI Model is Important:
  + It standardizes communication between different hardware and software systems.
  + It helps developers and engineers troubleshoot issues by focusing on a specific layer.
  + It gives a clear structure to network architecture, making it easier to design and maintain.
  + It provides a common language for people working in networking to describe how systems connect and exchange data.

## Working of TCP/IP Model

* The TCP/IP model - Transmission Control Protocol/Internet Protocol is a widely adopted suite of communication protocols that serves as the foundation of modern internet communication. Unlike the OSI model, which is more theoretical, TCP/IP is a practical model that defines how data should be packaged, addressed, transmitted, routed, and received across networks.
* It consists of 4 layers, each handling specific aspects of network communication. Together, these layers support everything from basic data transfer to application-level interactions.
* The Four Layers of the TCP/IP Model :

1. **Application Layer :** The topmost layer interacts directly with the user. It supports various protocols like HTTP, FTP, SMTP, and others to enable email, file transfer, web browsing, and more. This is where applications gain access to the network.
2. **Transport Layer :** This layer ensures reliable or fast delivery of data between applications on different devices. It uses TCP for reliable, connection-oriented transmission and UDP for faster, connectionless communication. It also handles port addressing and segmentation of data.
3. **Internet Layer :** The Internet Layer is responsible for routing and addressing. It uses the IP protocol to assign logical addresses (IP addresses) and determine the best path for data to travel across multiple interconnected networks.
4. **Network Access Layer :** This is the lowest layer in the TCP/IP model. It handles the physical and data link functions, including the actual transmission of raw data over a physical medium (like Ethernet or Wi-Fi). It also manages addressing (such as MAC addresses) and ensures data can travel from one device to another within the same network.

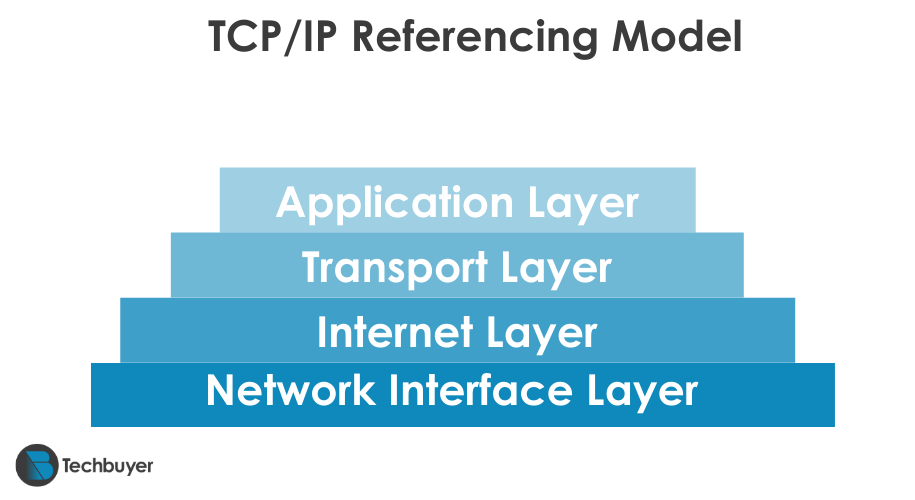


Figure 3: Layers of TCP/IP Model

* Key Characteristics of TCP/IP:
  + End-to-End Communication: Ensures data is reliably sent and received between devices across networks.
  + Layered Architecture: Organized into four layers, each handling specific networking functions.
  + Protocol-Based: Uses core protocols like TCP, UDP, IP, and ICMP for efficient data transfer.
  + Hardware Independent: Works seamlessly across different devices and operating systems.

## TCP & UDP Protocols

* Introduction to TCP (Transmission Control Protocol)
* The **Transmission Control Protocol (TCP)** is a core protocol of the Internet Protocol suite. It operates at the transport layer of the TCP/IP model and is designed to provide reliable, ordered, and error-checked delivery of data between systems on a network. TCP is connection-oriented, meaning it establishes a secure and synchronized connection before data transfer begins.

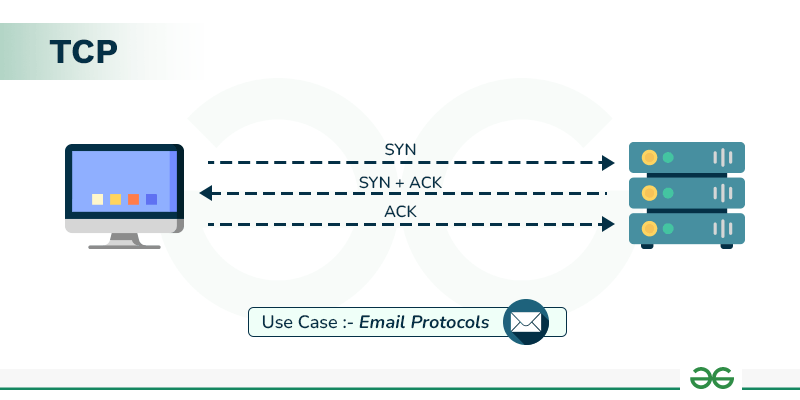


Figure 4: TCP Protocol

* Introduction to UDP (User Datagram Protocol)
* The **User Datagram Protocol (UDP)** is a lightweight, connectionless transport layer protocol. Unlike TCP, UDP does not establish a connection before sending data, nor does it guarantee delivery, order, or error checking. However, this simplicity makes it much faster and more efficient in real-time communication scenarios.

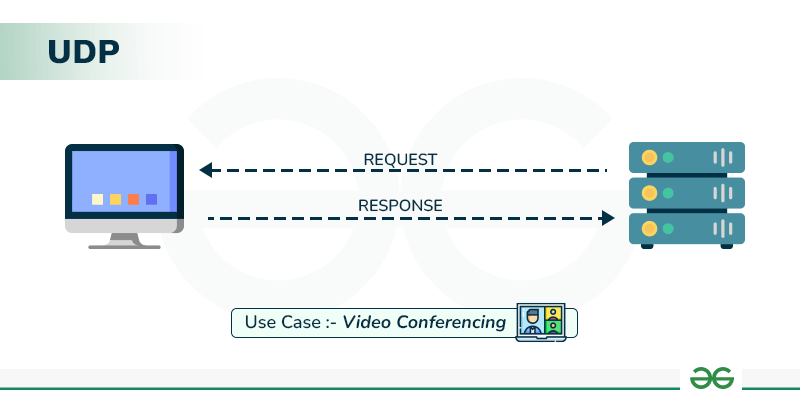


Figure 5: UDP Protocol

* **TCP vs UDP -**

| Features | TCP | UDP |
| --- | --- | --- |
| Connection | Connection-oriented (3-way handshake) | Connectionless |
| Reliability | Reliable – ensures delivery, order, and error correction | Unreliable – no guarantee of delivery or order |
| Data Ordering | Guarantees data is received in order | No ordering of packets |
| Use Cases | Web browsing, file transfers, emails, remote login (SSH, FTP, HTTP) | Video streaming, VoIP, gaming, DNS lookups |
| Error Checking | Yes, with retransmission of lost or corrupt packets | Basic error checking, no retransmission |

## Working of HTTP, HTTPS, and ICMP Protocols

* HTTP (Hypertext Transfer Protocol)
* **HTTP** is the foundational protocol used by the World Wide Web to enable communication between web browsers and servers. It operates at the application layer of the TCP/IP model and is used to request and transfer data such as HTML files, images, videos, and documents.
* Each HTTP request is independent. The server does not retain any information about previous interactions. HTTP uses human-readable commands like - Get, Post, Put, and Delete.
* HTTP typically communicates over port 80.

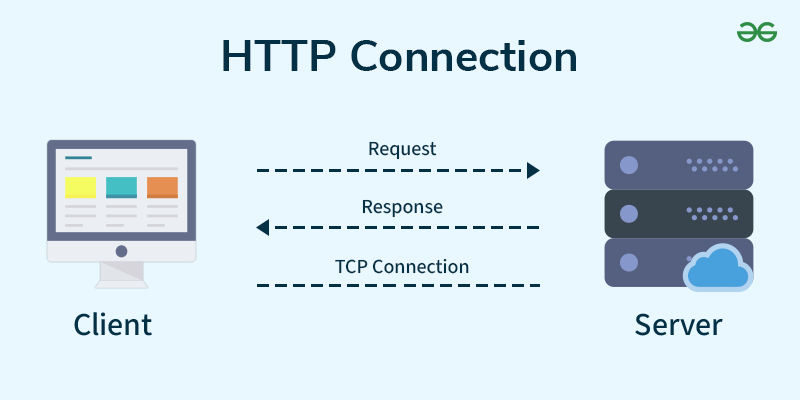


Figure 6: HTTP Protocol

* HTTPS (Hypertext Transfer Protocol Secure)
* **HTTPS** is the secure version of HTTP, providing encrypted communication over a network. It uses TLS (Transport Layer Security) or SSL (Secure Sockets Layer) to encrypt data transmitted between the client and server.
* Data is encrypted to prevent interception and ensure privacy. It uses digital certificates (SSL/TLS) to verify the identity of the server.
* HTTPS uses port 443 for secure communications.

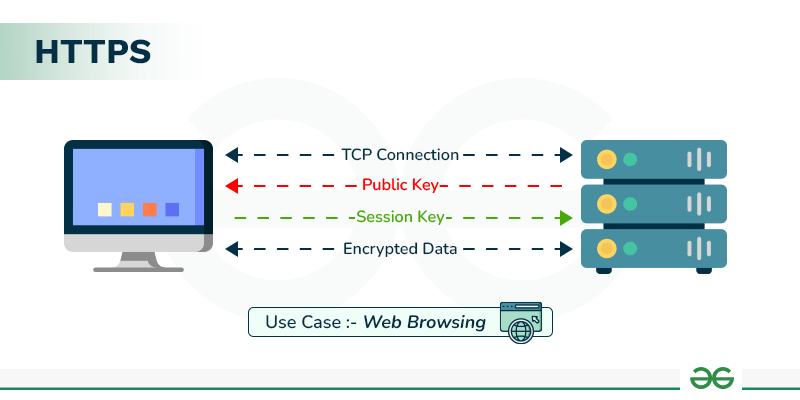


Figure 7: HTTPS Protocol

* ICMP (Internet Control Message Protocol)
* **ICMP** is a network-layer protocol used for diagnostics and error reporting in network communication. Unlike HTTP/HTTPS, it is not used to transmit data but rather to report problems or check network status.
* Used to notify a source device about issues in packet delivery (e.g., destination unreachable). Forms the basis of tools like Ping and Traceroute which test network connectivity and path information.
* ICMP does not use TCP or UDP, and does not require ports since it's not designed for data exchange.

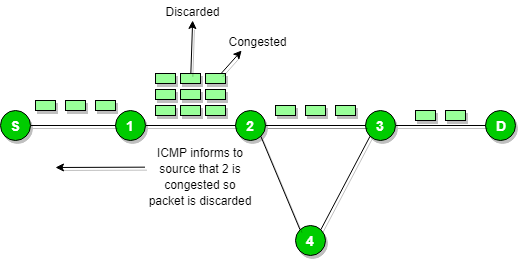


Figure 8: ICMP Protocol

## 

## Conclusion

* This R&D document explored the OSI and TCP/IP models along with key protocols like TCP, UDP, HTTP, HTTPS, and ICMP—each essential for understanding how devices communicate over a network.
* These concepts are particularly valuable for my internship in **Cloud Infrastructure & Security**. They help in configuring secure cloud environments, managing virtual networks, and troubleshooting issues effectively. Protocols like HTTPS ensure encrypted communication, while tools based on ICMP aid in network diagnostics.
* Overall, this knowledge strengthens my ability to contribute to real-world cloud infrastructure projects with a focus on **reliability, performance, and security**.

## 

## References

* Book: "Computer Networking: A Top-Down Approach"
* *By James F. Kurose and Keith W. Ross, 7th Edition, Pearson Education*
* GeeksforGeeks - OSI Model in Computer Network
* [*https://www.geeksforgeeks.org/layers-of-osi-model*](https://www.geeksforgeeks.org/layers-of-osi-model)
* Tech Buyer’s Guide - OSI vs TCP/IP Models
* [*https://www.techbuyer.com/uk/blog/osi-vs-tcp-ip*](https://www.techbuyer.com/uk/blog/osi-vs-tcp-ip)
* Book: "Data Communications and Networking"
* *By Behrouz A. Forouzan, 5th Edition, McGraw-Hill Education*

## Done by-

* Name - Tushar Tak
* Intern ID - CT\_CSI\_CI\_4391
* Contact Mail - [tushartak.work@gmail.com](mailto:tushartak.work@gmail.com)