www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 13 Issue 08 August 2024, Page No. 26358-26372
ISSN: 2319-7242 DOI: 10.18535/ijecs/v13i08.4842

Comparative Study Between the OSI Model and the TCP/IP Model: Architecture and Protocols in Computer Networking Systems

Zainab Hassan Muhamad [1]., Dhafer Abdulameer Abdulmonim [2].

[1,] Department of Computer Science, Gifted Student School, Gifted Guardianship Committee, Ministry of Education, Najaf, Iraq.

[2] Department of Computer Science, Open Educational College, Ministry of Education, Najaf, Iraq

Abstract

In the world of computing and networking, it is critical to understand the theoretical framework that underlies data communication to ensure the best performance and compatibility between various systems. Both the Open Systems Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models offer a comprehensive perspective on how the entire communication operation is separated into various layers, with each layer assigned particular roles and functions. This paper compares the OSI and TCP/IP models in terms of the functionalities and responsibilities of the various layers in each model, with an emphasis on how these layers work together to ensure effective and robust network communications. The paper covers encapsulating and decapsulating processes, managing sessions, and ensuring reliable data transmission. The TCP/IP model focuses on practical application with four main layers, while the OSI model has seven detailed layers that provide a theoretical and structured approach. The goal of both models is reliable and standardized communication, which in turn promotes interoperability in a variety of network environments.

Key Words: OSI Model, TCP/IP Model, protocols, Encapsulation, Decapsulation, Session Management, and Ensuring Reliability.

1. Introduction

Computer networks consist of multiple computers that can communicate with one another and share network devices (printers, for example) that can be accessed from any computer connected to the network [1]. The availability of an appropriate protocol to enable communication from one computer to another is a critical requirement for networking [2]. A protocol is a set of standards and guidelines that enable computers to communicate with each other on a network. These protocols specify how networked devices communicate with each other. Protocols are also a set of standards and guidelines that all network devices must follow. For both the sending and receiving of data, the exchange of packets is often used by protocols [3]. Network protocols include techniques for network devices to specify and communicate with each other, and formatting rules that define how data is packaged in sending and receiving messages. Some protocols also provide support for message discovery and data aggregation, which are intended to provide high reliability and performance for network communications. In addition, they are layered [4].

The OSI reference model and the TCP/IP model are two reference models that are essential for understanding and evolving complex network systems and are considered critical foundations in the development of computer networks [5]. An Open System Interconnection Model, commonly known as the OSI Model, ratified in 1984, is like an interface between two entities, i.e., one transmitting and the other receiving. The OSI model was essentially developed to reduce the complexity of networking, to make networking easier to learn, and to make networking easy to understand and analyze [6]. Because it does not explicitly define the services and protocols that each layer should use, the OSI model is not a true network architecture. Rather, it describes what the layers are required to do. It is an ISO standard for world-wide web Communications that establishes a networking framework for the deployment of protocols in seven layers. The OSI model specifies a network framework for implementing protocols in seven layers. The flow of data is from one layer to the other as control passes from the application layer in one station to the lowest layer, through the communications channel to the next station, and up to the highest layer [7]. On the other hand, Transmission Control Protocol/Internet Protocol (TCP/IP) is a model that was specifically designed to provide a high- reliability, end-to-end packet stream through an un-reliable Internet network. TCP/IP specifies how specific computers connect to the Internet and how to transport data between them [8]. When multiple computer networks are connected, TCP/IP enables to create a virtual network. TCP/IP is concerned with end-to-end data transmission and provides the specifications for how data is to be transmitted, accessed, encapsulated in packets, routed, and finally delivered. It includes four layers: application, transport, Internet, and link. The Internet Engineering Task Force (IETF) developed and maintains its technical standards. The concept of a stack of protocols underlies both the OSI and TCP/IP reference models. The layers' functionality is almost similar [9].

In the scope of computer networks, the OSI and TCP/IP models are critical fundamentals in the design of complex interconnection systems, since the function of the individual layers in each of these models is to provide an end-to-end, network-independent communication capability for processes that need to communicate with each other. Both models have been around for many years. However, they remain relevant and necessary for understanding the basic principles of network communications [10]. The OSI model consists of seven layers. Each layer plays a specific role in the network communication process. This model helps to understand the basic concepts of network communication, from the physical layer, which determines the flow of data bits, to the application layer, which interfaces with user applications [11]. The TCP/IP model, on the other hand, has only four layers. However, it is effective in controlling end-to-end interconnects and data delivery between the network's devices. In addition, this protocol conforms to ISO and OSI standards, enabling seamless communication between different platforms around the world [12]. Although both models have the common goal of enabling an effective and reliable connection between different systems, there are significant variations in the layered architecture, management of data, security issue, and performance efficiency. The differences in design concepts and architectures between the OSI seven-layer model versus the TCP/IP four-layer model. These differences lead to many issues as to how these architectures impact the overall performance of the network. In particular, security and fault management mechanisms diverge between the two models, requiring a rigorous analysis to identify which model provides better assurance and higher performance in a variety of network environments. From this perspective, the research problem focuses on the performing a comparative study detailed between the OSI and TCP/IP models regarding layer architecture and layer interaction and its impact on network performance.

In general, this paper aims to provide a deeper understanding of comparative aspects that will help in selecting the most appropriate model for use in specific networks, thus improving overall network design and performance. Specifically, it aims to achieve the following objectives:

i. To review the historical background and evolution of both the OSI model and the TCP/IP model.
ii. To analyze the architecture and layers of the both models.
iii. To compare both models based on the functionalities, the responsibilities and the interaction of the different layers.
iv. To compare both models based on Encapsulation, Decapsulation, Session Management, and Ensuring Reliability of data communication.

The rest of this paper is organized in the following manner: Section 2 reviews the background and evolution of the OSI and TCP/IP models, with key concepts related to both models. Section 3 provides an analysis of the architecture and the layers of the two models. Section 4 provides a detailed comparison and highlights the similarities and differences between the TCP/IP and OSI Reference Models, and Section 5 presents the conclusions of this paper.

Background

OSI Model's Evolution History

The International Standard Organization (ISO), founded in 1947, is a multi-national organization that deals with worldwide consensus on international standards. In 1983, ISO proposed a model called OSI that covers all aspects of network connectivity. OSI model aims to allow open communication among different systems without needing to change underlying hardware and software logic. OSI is not a protocol; it is a model for understanding and designing flexible, robust, interoperable network architecture [13]. In 1977, ISO decided to create a new subcommittee (SC16) for OSI, recognizing the special and urgent need for standards for heterogeneous information networks. The universal need to interconnect systems from different vendors quickly became apparent, and ISO decided to create SC16 to develop the standards needed for OSI. The term "open" was selected to reflect the fact that compliance with these standards would result in the use of the same systems all over the world [14]. SC 16 held its first meeting in March 1978, and initial discussions indicated that consensus had been quickly achieved on a layered architecture that could meet most OSI requirements and could later expand to meet new needs. SC16 decided that its highest priority should be to develop a standard architectural model, a framework for developing standard protocols. Technical Committee on Data Processing (TC97) recommended the formal launch of a number of projects to develop a first set of standard OSI protocols. In late 1979, these recommendations were formally adopted by TC97 as the basis for the subsequent development of Open Systems Interconnection standards under ISO [15]. The CCITT Rapporteur Group on Public Data Network Services has also approved the OSI Reference Model. The Consultative Committee for International Telephony and Telegraphy (CCITT) is a branch of the International Telegraph Union (ITU), which has established many essential standards for data communications, and it provides standards for telecommunications. CCITT, known today as (ITU-T) for the Telecommunication Standardization Sector of the International Telecommunications Union, is the principal international body for the facilitation of common standards for telecommunications devices and systems [16].

The OSI model was intended to help designers and developers establish standards for interoperable networks. It was designed to be a replacement for all earlier computer communication standards. However, the OSI model is no longer considered to be such a replacement. Instead, it has become a tool to describe and define the communication of a diverse set of network systems [17]. OSI relies on a widely-accepted structure known as layers. In this approach, communication functions are divided into a series of vertically oriented layers. Each level serves an associated set of functions and uses and enriches the services of the level immediately below. It is designed to achieve these objectives: Provides network designers, managers, vendors, and users with a standardized tool for describing network functions. And, its analysis of a complex communications networks more standardized, understandable, and manageable. In addition, it supplies logical interfaces between network functions [18]. The seven-layer OSI reference model described in the following sections resulted from modeling the above goals.

TCP/IP Model's Evolution History

In 1969, the Department of Defense conducted a network study (ARPANET) that led to the introduction of the Internet. ARPANET has been successful since the beginning of that year. ARPANET's original design provided easy access to remote computers, allowing scientists to share data and explore and debate various topics. The first of many rules for entities operating a growing network is cooperation in international networking [19]. In the 1980s, Transmission Control Protocol/Internet Protocol is abbreviated as (TCP/IP). It was created by Bob Kent and Winton Joseph, who were the main members of the TCP/IP team. TCP/IP is the common language for all Internet-connected computers. ARPANET, a loose network, which is now called Internet [20]. In the 1980s, the computer industry experienced such a surge. The Internet allowed companies to communicate with their customers and business partners by combining low-cost desktops with powerful servers. Another critical requirement for the network design was the continuation of ongoing conversations. This means that even if one of the devices or communication lines in between suddenly stops working, the

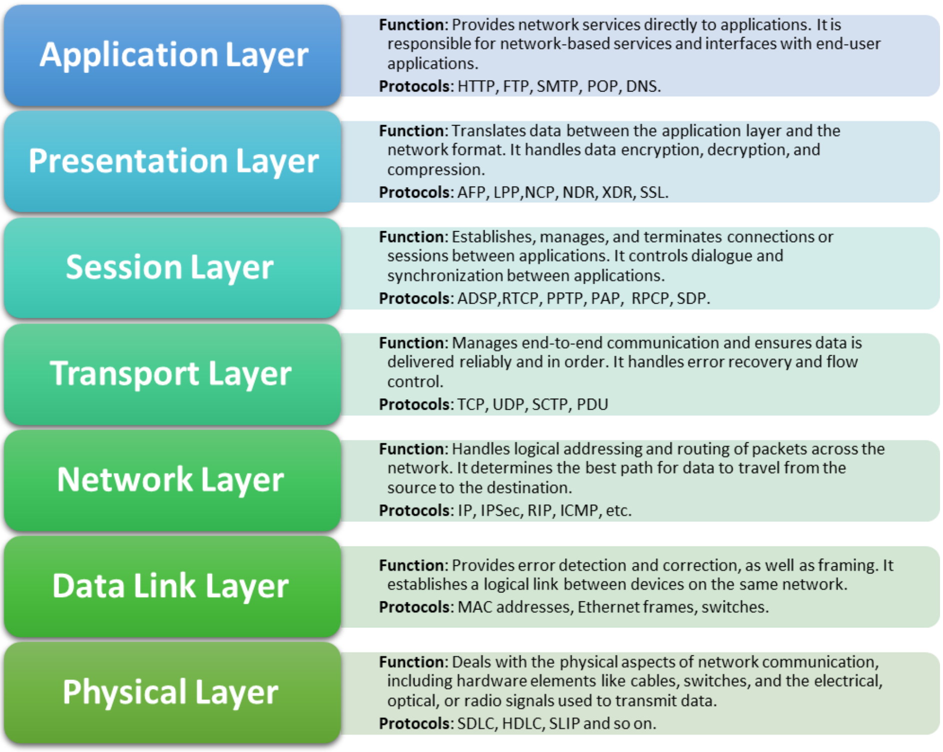
Department of Defense (DOD) required that the links remain up as long as the source and destination devices are operational [21]. A versatile layout is required for applications ranging from document exchange to live voice over IP. IP and TCP are highly dependent on each other. IP is the direction of travel for data packets, while TCP is the guarantee of their secure transmission [22].

TCP/IP is a set of standards that govern how computers and other electronic equipment communicate. TCP is the protocol that is in control of the division of data into packets before it is sent over a network and the reassembly of the packets once they have reached their destination. IP manages intermachine communication. It addresses, sends and receives packets online. TCP ensures the accurate transfer of data packets between applications across a network, such as the Internet. It can be found at the transport layer [23]. The TCP/IP protocol operates on two separate layers. Transmission Control Protocol, an upper layer, is responsible for breaking up a communication or document into smaller fragments for transmission over the World Wide Web, and then reassembling it into the original communication when it is received. The Internet Protocol is responsible for ensuring that packets are sent to the correct destination, a lower layer protocol [24]. Each gateway machine on the network uses this location to determine where to send the message. Some of the communication packets may take different routes, but all of them are reassembled at the final destination. Another important goal was that the network should withstand the loss of subnetwork hardware without disrupting existing conversations [25]. That is, they wanted to keep the connections intact as long as the source and destination computers worked, even if one of the computers or the lines between them suddenly stopped working. From file transfer to real-time voice, an architecture with diverse requirements was needed. Understanding how IP and TCP relate to each other is essential. There is a unique role for each protocol: While TCP provides reliable transport, IP provides the path for the packets. The four-layer model of TCP/IP that is described in the following sections is the result of modeling the above goals.

Architectures and protocols

Seven-Layer OSI Model

OSI is a seven-tier model that summarizes complex network phenomenology. The inner workings of a communication system can be defined and standardized by breaking it down into abstraction layers. The various communication functions are organized into the seven logical layers of the model. Every layer is providing and receiving services from the levels on top of it [26]. The following principles underlie the seven-layer structure: In a network protocol, each layer serves a specific purpose to ensure that efficient and organized communication takes place. An additional layer should be introduced when a new level of abstraction is required. To maintain consistency and interoperability, international protocols should clearly define the role of each layer. Maintaining the integrity and functionality of each layer requires minimizing data leakage across its boundaries. In addition, layers should be sufficient to avoid the combination of unrelated tasks that would decrease their effectiveness, but are not so numerous that the design is confusing. This model is designed to simplify the learning process of networking and to make network problems less difficult to troubleshoot [27]. Figure 1 describes the layers of the OSI model. According to [28] each layer related to the OSI model architecture is briefly described in the following:



Application Layer

Function: Provides network services directly to applications. It is responsible for network-based services and interfaces with end-user applications.
Protocols: HTTP, FTP, SMTP, POP, DNS.

Presentation Layer

Function: Translates data between the application layer and the network format. It handles data encryption, decryption, and compression.
Protocols: AFP, LPP,NCP, NDR, XDR, SSL.

Session Layer

Function: Establishes, manages, and terminates connections or sessions between applications. It controls dialogue and synchronization between applications.
Protocols: ADSP,RTCP, PPTP, PAP, RPCP, SDP.

Transport Layer

Function: Manages end-to-end communication and ensures data is delivered reliably and in order. It handles error recovery and flow control.
Protocols: TCP, UDP, SCTP, PDU

Network Layer

Function: Handles logical addressing and routing of packets across the network. It determines the best path for data to travel from the source to the destination.
Protocols: IP, IPSec, RIP, ICMP, etc.

Data Link Layer

Function: Provides error detection and correction, as well as framing. It establishes a logical link between devices on the same network.
Protocols: MAC addresses, Ethernet frames, switches.

Physical Layer

Function: Deals with the physical aspects of network communication, including hardware elements like cables, switches, and the electrical, optical, or radio signals used to transmit data.
Protocols: SDLC, HDLC, SLIP and so on.

Figure 1. OSI Model Architecture.

Layer 1: Physical Layer

Physical layer functions include converting signals into bits that can be used by other layers, and modulating signals so that multiple users can share the same connection. In addition, the physical layer determines how a physical device can send and receive information; for example, the cables used to connect the various computers, or the radio signals used in wireless communications. A physical layer protocol is a set of rules that govern how computers communicate with each other on a network, including Fiber, Integrated Services Digital Networks, Ethernet, Universal Serial Bus (USB), Bluetooth, etc.

Layer 2: Data Link Layer

The primary function of this layer is to provide a method for breaking up network information into frames and transmitting them over the physical layer. Some error detection and correction is also performed at this layer. The validity and integrity of the transmission from node to node is the responsibility of the data link layer. It divides into frames the bits to be transmitted. It provides the hardware means to send and receive data on a carrier, including the definition of cables, cards, and physical aspects. Sending and receiving bits on the connection medium is the responsibility of the physical layer. This layer is concerned with the electrical and mechanical properties of the signals and signaling methods, not with the meaning of the bits. There are various protocols in the data link layer, which are the Synchronous Data Link Protocol (SDLC), the High-Level Data Link Protocol (HDLC), the Serial Line Interface Protocol (SLIP) and so on.

Layer 3: Network Layer

This layer is related to finish the Network Packet transmitting between the hosts. For each packet sent from the source to the destination, the primary uses the services of the data link layer. If the subnets simultaneously receive an excessive number of packets, it may form subnet congestion because of the need to avoid this from happening. The network layer transmits communications across a network. It controls how the subnet works. Among other things, the network layer is responsible for logical addressing. Media Access Control (MAC) addressing are physical addresses that are assigned to each network device. To obtain access to any device connected to a network, it must be assigned a unique address. MAC addresses are derived from logical addresses by the network layer protocol. The network layer is also responsible for routing, or determining the best path through the network. A router functionality is in the network layer and is responsible for transmitting the packet to its final destination. The common protocols used by routers are Internet Protocol (IP), Internet Protocol Secure (IPSec), Routing Information Protocol (RIP), Internet Control Message Protocol (ICMP), etc. Within network layer, the Protocol Data Unit (PDU) is called the packet. Packets encapsulate the data to be transmitted with header and footer data.

Layer 4: Transport Layer

It ensures end-to-end data transfer and makes logical connections between sending and receiving hosts. Key features include flow monitoring, sequencing, error detection and restoration. The transport layer guarantees that messages are transferred correctly, in proper order, and without loss or duplication. It relieves higher-layer protocols of any concern about transferring data between them and their peers. The type of service a transport protocol can receive from the network layer determines its size and complexity. If the network layer is reliable and has a virtual circuit capability, then a minimal transport layer is required. The transport protocol should include extensive error detection and recovery if the network layer is unreliable and/or supports only data grams. Often, the transport protocol breaks large messages into smaller packets that can travel efficiently across the network. This ensures that all packets contained in an individual transmission are received without losing any data. The most important protocols in this layer are the Transmission Control Protocol (TCP), the User Datagram Protocol (UDP), and the Stream Control Transmission Protocol (SCTP). The Protocol Data Unit (PDU) at Layer four is known as a data segment. Segmentation is the process of dividing raw data into smaller pieces. Once the raw data is packaged from the higher application layers it is segmented at the transport layer before being passed to the Network Layer.

Layer 5: Session Layer

This layer is responsible for the establishment, management and then termination of sessions between two computers. It is used to control data flow when two computers are connected to each other. Dialog control, token management and synchronization are the main services provided. Session control refers to the organization of a data communication session between two computers through three modes namely simplex, halfduplex and fullduplex. Token control means that during a session between two computers, when a critical operation is to be performed, they pass tokens and the one holding the token will perform the operation. Synchronization is used for functions such as checkpoint insertion to manage the timing signal between sessions. Session Layer uses some protocols that are required for secure and accurate communication that exists between two end user applications like AppleTalk Data Stream Protocol (ADSP), Real-time Transport Control Protocol (RTCP), Point-to-Point Tunneling Protocol (PPTP), Password Authentication Protocol (PAP), Remote Procedure Call Protocol (RPCP) and Sockets Direct Protocol (SDP).

Layer 6: Presentation Layer

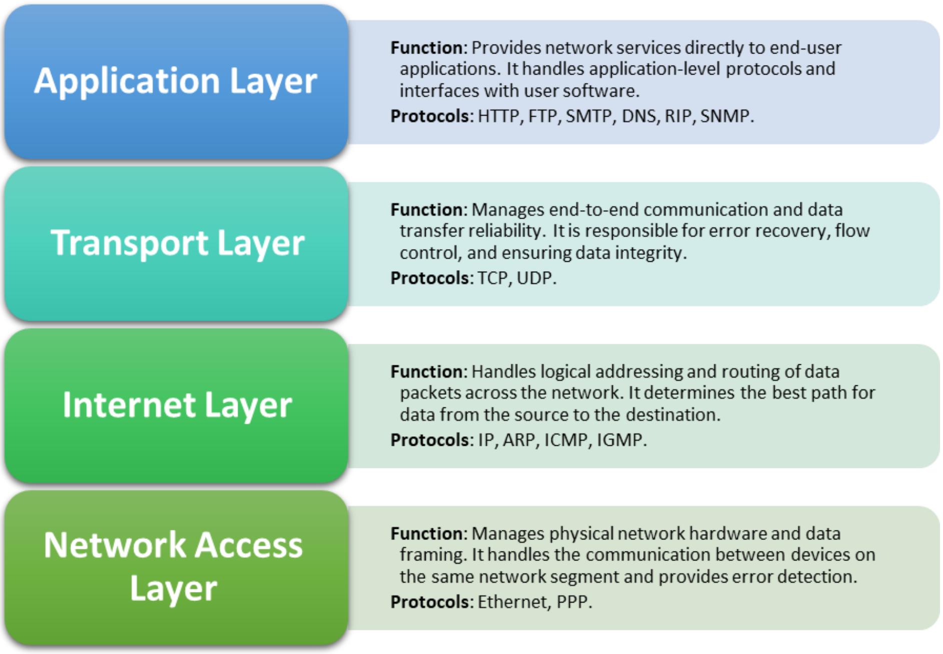
The format of the data transmitted during network communication is the responsibility of the presentation layer. It deals with the syntax and semantics of transmitted information. It translates data into a generic format to be transmitted. It converts data from the generic form into a format that the receiving application can understand for incoming messages. Different computers represent data differently. The presentation layer enables communication between computers that have different representations of data. Common communications services such as encryption, text compression, and reformatting are provided by the presentation layer. Other aspects of information presentation are also handled by the presentation layer. The number of bits to be transmitted can be reduced by data compression. For privacy and authentication, cryptography is often required. Generally, the main work of the presentation layer is to represent data, encrypt for security, and convert computer code to network formatted code. In order to perform translations or other specified functions, the presentation layer must use certain protocols, which are Apple Filing Protocol (AFP), Lightweight Presentation Protocol (LPP), NetWare Core Protocol (NCP), Network Data Representation (NDR), External Data Representation (XDR), and Secure Socket Layer (SSL).

Layer 7: Application Layer

It is layer in which users communicate with computers. This layer is used for transferring files, sending email, accessing remote computers, and performing network management activities. Communication partners are identified, quality of service is assessed, user authentication and privacy are considered, and data grammar constraints are recognized. At this level, everything is adapted to a specific software. Hyper Text Transfer Protocol (HTTP) is widely used because it is the foundation of the World Wide Web. A browser accesses a web page by sending the server the title of the desired page via HTTP. The server then delivers the page. File sharing, email, and network bulletin boards all use different application protocols. A few examples of application layer protocols are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Domain Name System (DNS).

Four-layer TCP/IP model

The TCP/IP protocols correspond to a four layers architecture model known as the Defense Advanced Research Projects Agency (DARPA). The DARPA model is modeled after the government organization that originally created TCP/IP. The four layers of the TCP/IP model include Application, Transport, Internet, and Network Interface. TCP/IP has two different layers; an upper layer, is responsible for breaking a communication or document into smaller fragments for transmission over the World Wide Web, and then reconstructing them into the original communication upon receipt. The Internet Protocol is responsible for ensuring that packets are sent to the correct destination, a lower layer protocol. Each gateway machine on the network uses this location to determine where to send the message. Some of the packets may take an alternate route. However, they are all recreated at the final endpoint. Each layer in the DARPA model corresponds to one or more layers in the OSI model [29]. Figure 2 shows the layered configuration of the TCP/IP model. According to [30] each layer included in the TCP/IP model architecture is briefly described in the following:



Application Layer

Function: Provides network services directly to end-user applications. It handles application-level protocols and interfaces with user software.
Protocols: HTTP, FTP, SMTP, DNS, RIP, SNMP.

Transport Layer

Function: Manages end-to-end communication and data transfer reliability. It is responsible for error recovery, flow control, and ensuring data integrity.
Protocols: TCP, UDP.

Internet Layer

Function: Handles logical addressing and routing of data packets across the network. It determines the best path for data from the source to the destination.
Protocols: IP, ARP, ICMP, IGMP.

Network Access Layer

Function: Manages physical network hardware and data framing. It handles the communication between devices on the same network segment and provides error detection.
Protocols: Ethernet, PPP.

Figure 2. TCP/IP Model Architecture.

Layer 1: Network Access Layer

The Network Access Layer is the top layer in the TCP/IP model. It explains how bits are represented visually or electrically by hardware devices that directly interface with a network physical medium, such as coaxial cable, fiber optics, or twisted-pair copper wire. This layer is responsible for managing the transmission and reception of TCP/IP packets over the network medium. TCP/IP has been designed to work with any frame structure and any media, regardless of the type of network access. TCP/IP allows many different networking structures to interoperate. TCP/IP's capability to adapt to individual network technologies is primarily due to its independence from any specific network technology. The data link and physical layers of the OSI model are consolidated into a single component known as the Network Access Layer. It is important to keep in the knowledge that the Internet layer does not employ any request or acknowledgement services that might be available at the data link layer. It is considered that the Network Access Layer is unpredictable, and it is the responsibility of the Transport Layer to provide reliable transmissions by creating sessions and properly ordering and validating packets. The protocol of the packet is identified by the network access layer. This layer also provides error prevention and framing. Point-to-Point Protocol (PPP) framing and Ethernet IEEE 802.2 framing are two examples of protocols at this layer.

Layer 2: Internet Layer

Addressing, packaging, and routing functions are handled by the Internet layer. The Internet layer in tcp/ip model corresponds to the network layer of OSI model. A connectionless Internetwork layer is necessary for the proper function of a packet-switched network. The highest layer is the Internet layer; its purpose is to enable hosts to send and receive packets. The data packets that arrive at final destination may not be in the same order as they were sent. The upper layers are concerned with re-arranging the packets so that the application layer of the network can properly obtain and handle them. The most important protocols of this layer are: The Internet Protocol (IP) is a routable protocol responsible for IP addressing, routing, and packet fragmentation and reassembly. The Address Resolution Protocol (ARP) is used to translate an Internet layer address into a Network Interface Layer address, such as a physical address. The Internet Control Message Protocol (ICMP) is also used to provide the capability to perform diagnostics and report errors caused by failed delivery of IP packets. And the Internet Group Management Protocol (IGMP) is used to manage IP multi-cast networks.

Layer 3: Transport Layer

The transport layer, which handles communications between hosts, whether the hosts are the same or separate, and whether they are on the local network or on remote networks that are separated by routers. Providing session and datagram communication services to the application layer is the responsibility of the transport layer. Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the main protocols of the transport layer. TCP enables a one-to-one, connection oriented, and reliable communication service. In addition, it is responsible for establishing a TCP connection, ordering and acknowledging sent packets, and recovering packets dropped during transmission. UDP provides a connectionless, unreliable communication service and one-to-one or one-to-many. It is used in situations where the amount of data transferred is small, the overhead of connecting to TCP is undesirable, or the applications or upper-layer protocols do not guarantee reliable delivery. It includes the functions of the OSI Transport Layer, and some of the functions of the OSI Session Layer.

Layer 4: Application Layer

The application layer allows applications to access the other layer services. It determines the protocols that applications use to transfer data. Numerous application layer protocols are available. The most common application layer protocols are Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), and Telnet, a terminal emulation protocol used to remotely log on to network hosts. In addition, there are many of application layer protocols that are used to enable the usage and manage TCP/IP networks, such as Domain Name System (DNS), Routing Information Protocol (RIP), and Simple Network Management Protocol (SNMP). Windows Sockets and NetBIOS are examples of application layer interfaces for TCP/IP applications. Under Windows 2000, Windows Sockets provides a standard application programming interface (API). NetBIOS is an industry-standard interface. It provides access to protocol features such as session, datagram, and name resolving.

Results and Discussions

In the realm of networking and communications, it is essential to clearly understand the framework that provides the basis for data exchange in order to ensure optimal functionality and reliability between different systems. Both the OSI (Open Systems Interconnection) and TCP/IP (Transmission Control Protocol/Internet Protocol) models offer a comprehensive perspective on how the entire communication operation is divided into different layers, with each layer having unique responsibilities and functionalities. The OSI model, consists of seven layers, each of which handles a different aspect of the communication in the network, starting with the physical layer, which is concerned with the physical media used to transmit data, and ending with the application layer, which is concerned with the software applications. On the other hand, the TCP/IP model is more convenient and popular, consisting of four layers that simplifies the communication process and combines some of the functionalities of the OSI layers.

In this section, the comparison between OSI Model and TCP/IP model is offered that aims to analyze the functionalities and the roles of the various layers in both of the models, with emphasis on the interaction of these layers with each other to ensure an efficiency and reliability of the network connection as shown in Table 1. The comparison focuses on the manner in which each model manages processes such as Encapsulation, Decapsulation, Session Management, and Ensuring Reliability of data communication, in order to identify the differences and similarities between the models, as shown in Table 2. From this perspective, determining which model is most suitable for specific network requirements and demonstrating how engineers and administrators can utilize these architectures to achieve the highest levels of performance and reliability in their networks. In addition, this comparison will allow us to highlight the key similarities and differences between these two fundamental network models, as shown in Table 3.

Table1. Comparison of OSI and TCP/IP models based on functions, roles, and interactions of layers in both models.

OSI Model				**TCP/IP Model**			
Layers	**Function**	**Role**	**Interaction**	**Layers**	**Function**	**Role**	**Interaction**
Physical Layer **(Layer 1)**	Addresses the physical connectivity between devices, and defines the hardware components used in the network, such as cables, switches, and other physical features.	Transfers raw bitstreams via a physical medium.	Receives frames to be converted into electrical, radio, or optical signals and interfaces directly with the data link layer above.	**Network Access Layer** **(Layer 1)**	Manages the physical and logical connections of the network, encompassing the physical layer and the data link layer of the OSI model.	Manages the addressing of hardware and the access control of media.	Interfacing with the higher layers of the Internet, transmitting frames over the physical network.
Data Link Layer **(Layer 2)**	Provides reliable data transmission between two devices. It handles detecting and correcting errors from the physical layer.	Manages data frames between nodes.	Ensures the integrity of frames transmitted by the physical layer and forwards frames to the network layer above.				

Network Layer **(Layer 3)**	Determines how data packets travel from source to destination, managing logical addressing and routing.	Forwards, addresses, and routes packets on the basis of logical addressing.	Provides end-to-end packet delivery across multiple network segments and interfaces with the transport layer above.	**Internet Layer** **(Layer 2)**	Provides logical addressing and routing for data packages.	Equivalent to the OSI networking layer, manages logical addressing and routing through protocols such as IP.	Interfaces with the Transport layer at the top to forward packets to their final destinations.
Transport Layer **(Layer 4)**	Manages end-to-end communication, error recovery, and flow control to ensure reliable data transfer between end systems.	Establishment, maintenance, and termination of connections between hosts.	Cooperates with lower network layer to divide and merge data for end-to-end communication, and with higher session layer to manage sessions.	**Transport Layer** **(Layer 3)**	Similar to the OSI transport layer, ensures reliable data transfer between host systems.	Manages protocols such as TCP and UDP for end-to-end communication, error recovery, and flow control.	Interfaces with the Internet layer at the bottom for packet transfer and with the application layer at the top to manage the session.
Session Layer **(Layer 5)**	Manages sessions or connectivity, controlling the interaction between host applications.	Creates, administers, and terminates sessions between applications.	Provides interfaces to the presentation layer at the top and the transport layer at the bottom to manage sessions.	**Application Layer** **(Layer 4)**	Combines the functions of the OSI application, presentation, and session layers to provide services directly to end-user applications.	Interacts directly with user applications by managing protocols such as HTTP, FTP, SMTP, and DNS.	Provides network services to applications by interfacing with the underlying transport layer.
Presentation Layer **(Layer 6)**	Handles the encryption, decryption, compression, and translation of data between the application layer and the network.	Assures the data is in a proper format and correctly represented to the application layer.	Interacts for data format translation with the application layer above and the session layer below.				
Application Layer **(Layer 7)**	Offers network services directly to user applications, such as	Interfacing directly to user applications, providing network services.	Provides network services to applications by interacting with the underlying				

	emailing, transferring files, and browsing the Web.		presentation layer.				

Table2. Comparison between OSI model and TCP/IP model based on encapsulation, decapsulation, session management and ensuring reliability of data communication in both models.

Aspect	**OSI Model**		**TCP/IP Model**	
Encapsulation	**Physical Layer (Layer 1)**	Does not append headers to data. It is responsible for sending raw bits over the physical medium.	**Network Access (Layer 1)**	Similar to the OSI Data Link Layer, it handles encapsulation at the frame level. It adds a frame header to the data, which includes information for physical addressing and error detection.
	Data Link Layer (Layer 2)	Adds a frame header to the data. This header contains MAC addresses and error checking information.		
	Network Layer (Layer 3)	Adds a packet header that contains IP addresses and routing information to the packet.	**Internet Layer (Layer 2)**	Similar to the OSI network layer, it adds an IP header to the data. This header contains information for logical addressing and routing information.
	Transport Layer (Layer 4)	Adds a segment header. This header contains information about flow control, sequencing, and error detection.	**Transport Layer (Layer 3)**	Similar to the OSI transport layer, adds a transport header (segment or datagram header). This header contains information used to manage the flow, detect errors, and ensure data integrity.
	Upper Layers (Layers 5-7)	Instead of adding headings, process the data directly. However, session-related information can be managed at the session layer (layer 5).	**Application Layer (Layer 4)**	Handles the data directly rather than adding encapsulation headers. This layer is concerned with data formats, encryption, and application specific functions.
Decapsulation	**Physical Layer (Layer 1)**	Converts signals back to bits without decapsulation.	**Network Access (Layer 1)**	Removes the frame header and handles the data prior to transfer to the Internet layer.
	Data Link Layer (Layer 2)	Removes the frame header and performs data processing before passing the data to the network layer.		
	Network Layer (Layer 3)	Removes the packet header, obtains routing information, and passes the data to the transport layer.	**Internet Layer (Layer 2)**	Removes the IP header, retrieves routing information, and routes the data to the transport layer.
	Transport Layer (Layer 4)	Removes the segment header, validates for errors, and recombines the data before it passes to the Session Layer.	**Transport Layer (Layer 3)**	Removes the transport header, validates for errors, reconstructs the data, and routes it to the application layer.
	Upper Layers	Manage the data based on the routing information	**Application Layer**	Handles the data directly, interprets it based on specific

	(Layers 5-7)	provided by the low-level layers, without addition or removal of headers.	**(Layer 4)**	application protocols and data standards.
Session Management	**Session Layer (Layer 5)**	Manages sessions or connecting between applications. It is used to establish, maintain, and terminate sessions and to control the interaction between systems.	**Application Layer (Layer 4)**	Provides session management in the application protocols directly. Session management is built into protocols such as HTTP, FTP, and others; there is no separate session layer.
Ensuring Reliability of Data Transfer	**Transport Layer (Layer 4)**	Through protocols such as TCP, provides mechanisms for reliable data transfer. It manages data delivery by providing error detection, error recovery, and flow control.	**Transport Layer (Layer 3)**	Provides reliability mechanisms similar to the OSI model. TCP provides mechanisms for reliable data transfer, including error detection, error correction, and flow control. UDP is an alternative that does not provide reliability guarantees.

Table3. Comparison between OSI model and TCP/IP model based on similarities and differences between models.

	Aspect	**OSI Model**	**TCP/IP Model**
Differences	**Layers Number**	Seven	Four
	Evolution	ISO (theoretical framework)	DARPA (practical implementation)
	Protocol dependencies	Protocol independent	Protocol dependent
	Design Flexibility	Robust and clearly defined	Dynamic and adaptive
	Implementation issues	Rarely implemented fully	Widely implemented
	Error management	Multi-tiered	Transport layer mainly
	Session / Presentation	Separating Layers	Application layer combined
	Interaction between layers	Rigorous	More flexible
Similarities	**Multi-Layer Architecture**	Both used a layered-based approach to simplify designing and debugging networks.	
	Functionality	Both support a conceptual model to simplify the understanding, designing, and deployment of network protocols.	
	Architecture Modularity	Both support the modularity that enables the flexibility and ease of development.	
	End-to-End Connectivity	Both ensure end-to-end reliable communication, supporting data integrity and distribution over various networks.	
	Standard Unification	Both help enable standardization of network protocols, which facilitates cross-vendor compatibility and integration.	
	Hierarchical Architecture	Both are hierarchically designed, with functions organized in a logically sequential manner.	
	Error handling and error recovery	Both integrate error handling and recovery to enable reliable data transfer.	
	Encapsulation	Both utilize the technique of encapsulation to package data with routing information to ensure proper processing and distribution over the network.	

	Abstract presentation	Both facilitate conceptual understanding and implementation by providing an abstract representation of network functions.
	Supporting Multiple Protocols	Both promote flexibility and adaptability in network design by allowing multiple protocols to operate within their respective layers.

Conclusion

This paper provides a comparative study of the OSI and TCP/IP models in terms of the functions and roles of each layer, emphasizing both their similarities and differences, and highlighting their unique contributions to ensure efficient and reliable network communications. By analyzing the encapsulation, decapsulation, session management, and data reliability issues, significant insight can be gathered into each model's approach to achieving these objectives as follows:

Encapsulation and Decapsulation Issue

OSI Model: Across its seven layers, the OSI model provides a highly detailed process of encapsulation and decapsulation. It provides a robust and structured approach that enables accurate troubleshooting and distinct functionality separation by adding specific headers to each layer.

TCP/IP Model: Encapsulation and decapsulation are also used in the TCP/IP model, but in a more streamlined manner, with its four-layer structure. This approach is more lightweight. However, it is more efficient for practical deployment and is more consistent with real-world network requirements.

Session Management Issue

OSI model: The OSI model involves a specific session layer that controls establishing, maintaining, and terminating sessions. This layer ensures a systematic approach to session management by ensuring that sessions are properly coordinated and synchronized.

TCP/IP Model: Session management responsibilities are typically handled within the application layer in the TCP/IP model. This integration allows for simplification of the model, but requires applications to manage sessions in an organized manner.

Ensuring Data Reliability Issue

OSI Model: The OSI model provides error detection, correction, and flow control through its transport layer. Data is transferred accurately and efficiently through this comprehensive approach.

TCP/IP Model: Similarly, to ensure reliable data transmission, the TCP/IP model relies on the transport layer. TCP is highly reliable for data communications because it provides error checking, retransmission of lost packets, and proper sequencing.

Similarities and differences Issue

Similarities: The goal of both models is to ensure the standardization of network and communication processes, the promotion of interworking, and the assurance of reliable data transfer. They use a multi-layer approach to encapsulate and decapsulate data, to manage sessions, and to ensure data reliability, although the concrete design and architecture differ.

Differences: Complexity and application are the primary differences. The OSI model provides a theoretical and detailed conceptual framework that is useful for educational purposes and accurate network analysis, with its seven distinct layers. The TCP/IP model, the backbone of modern Internet communications, focuses on practical and real-world applicability with its four-layer approach.

In summary, the OSI and TCP/IP models, although structurally different, both play a critical role in the development and implementation of network communications. The OSI model affords a comprehensive and methodical framework that is essential for understanding the theoretical concepts of networking and for troubleshooting unique networking problems. In contrast, the TCP/IP model provides a more rational and practically oriented approach that facilitates the deployment and development of Internet services. In addition, network engineers can obtain a coordinated approach to developing robust, efficient, and reliable communications systems by leveraging the strengths of both models. Both models are based on the same layered architecture. This approach highlights the importance of standardization and modularity in ensuring interoperability in diverse network environments.

References

1. Sadiku, M. N., & Akujuobi, C. M. (2022). Fundamentals of Computer Networks (pp. 1-192). Springer.
2. Al-Masri, E., Kalyanam, K. R., Batts, J., Kim, J., Singh, S., Vo, T., & Yan, C. (2020). Investigating messaging protocols for the Internet of Things (IoT). IEEE Access, 8, 94880-94911.
3. Suresh, P. (2016). Survey on seven layered architecture of OSI model. International Journal of research in computer applications and robotics, 4(8), 1-10.
4. Latif, Z., Sharif, K., Li, F., Karim, M. M., Biswas, S., & Wang, Y. (2020). A comprehensive survey of interface protocols for software defined networks. Journal of Network and Computer Applications, 156, 102563.
5. Alade, A. A., Ajayi, O. B., Okolie, S. O., & Alao, D. O. (2017). A survey of Computer Network Communication Protocols and Reference Models. American Journal of Engineering Research, 6(11), 174.
6. Russell, A. L., Pelkey, J. L., & Robbins, L. (2022). The business of internetworking: Standards, start-ups, and network effects. Business History Review, 96(1), 109-144.
7. Solomon, M. G., & Kim, D. (2021). Fundamentals of communications and networking. Jones & Bartlett Learning.
8. Rico, D., & Merino, P. (2020). A survey of end-to-end solutions for reliable low-latency communications in 5G networks. IEEE Access, 8, 192808-192834.
9. Pawar, A. B., Jawale, M. A., William, P., & Sonawane, B. S. (2022). Efficacy of tcp/ip over atm architecture using network slicing in 5g environment. In Smart Data Intelligence: Proceedings of ICSMDI 2022 (pp. 79-93). Singapore: Springer Nature Singapore.
10. Murkomen, T. (2024). Performance, privacy, and security issues of TCP/IP at the application layer: A comprehensive survey. GSC Advanced Research and Reviews, 18(3), 234-264.
11. Fraihat, A. (2021). Computer networking layers based on the OSI model. Test Eng. Manag, 83, 6485-6495.
12. Rahouma, K. H., Abdul-Karim, M. S., & Nasr, K. S. (2020). TCP/IP network layers and their protocols (A Survey). In Internet of Things—Applications and Future: Proceedings of ITAF 2019 (pp. 287-323). Springer Singapore.
13. Fraccaroli, E., & Quaglia, D. (2020). Engineering IoT Networks. Intelligent Internet of Things: From Device to Fog and Cloud, 97-171.
14. Jasud, P. V. (2017). The OSI Model: Overview on the Seven Layers of Computer Networks. International Journal for Innovative Research in Science & Technology, 4(3), 116-124.
15. Houldsworth, J., Taylor, M. A., & Caves, K. (2014). Open System LANs and Their Global Interconnection: Electronics and Communications Reference Series. Butterworth-Heinemann.
16. Day, J. (2015). The clamor outside as INWG debated: Economic war comes to networking. IEEE Annals of the History of Computing, 38(3), 58-77.
17. Sadiku, M. N., & Akujuobi, C. M. (2022). Network Models. In Fundamentals of Computer Networks (pp. 19-36). Cham: Springer International Publishing.

18. Bora, G., Bora, S., Singh, S., & Arsalan, S. M. (2014). OSI reference model: An overview. International Journal of Computer Trends and Technology (IJCTT), 7(4), 214-218.

19. Rajaraman, V. (2022). A Concise History of the Internet—I. Resonance, 27(11), 1841-1856.

20. Aljubayri, M. (2022). Enhancements to the Multipath Transmission Control Protocol for Internet of Things Wireless Networks (Doctoral dissertation, King's College London).

21. Davidson, J. (2012). An introduction to TCP/IP. Springer Science & Business Media.

22. Faisal, A., & Zulkernine, M. (2021). A secure architecture for TCP/UDP-based cloud communications. International Journal of Information Security, 20(2), 161-179.

23. Nath, P. B., & Uddin, M. M. (2015). Tcp-ip model in data communication and networking. American Journal of Engineering Research, 4(10), 102-107.

24. Abed, G. A., Ismail, M., & Kasmiran, J. (2011). Architecture And Functional Structure Of Transmission Control Protocol Over Various Networks Applications. Journal Of Theoretical And Applied Information Technology, 34.

25. Aykurt, K., Zerwas, J., Blenk, A., & Kellerer, W. (2023). When TCP Meets Reconfigurations: A Comprehensive Measurement Study. IEEE Transactions on Network and Service Management.

26. Kumar, S., Dalal, S., & Dixit, V. (2014). The osi model: overview on the seven layers of computer networks. International Journal of Computer Science and Information Technology Research, 2(3), 461-466.

27. Poo, G. S., & Ang, W. (1990). OSI protocol choices for LAN environments. Computer Communications, 13(1), 17-26.

28. Barr, Roland. "Computer System Architecture." Bibliotex, Canada (2022).

29. Hunt, C. (2002). TCP/IP network administration (Vol. 2). " O'Reilly Media, Inc.".

30. Loshin, P. (2003). TCP/IP clearly explained. Elsevier.