

OSI model: Finally understand networking

Check GitHub for helpful DevOps tools:

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats information overload by adhering to the set of principles: simplify, prioritize, and execute.

 <https://github.com/MichaelRobotics>



Ask Personal AI Document assistant to learn interactively (FASTER)!

1


Download PDF

1

<https://github.com/MichaelRobotics/DevOpsTools/blob/main/OSImodel.pdf>

2

Go to website

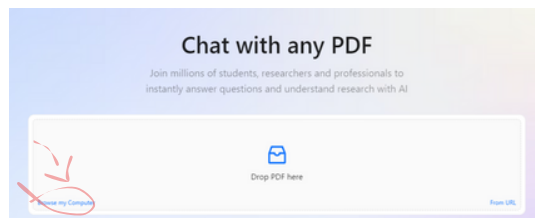
 | Click there to go to ChatPdf website

2

3

Browse file

3



4

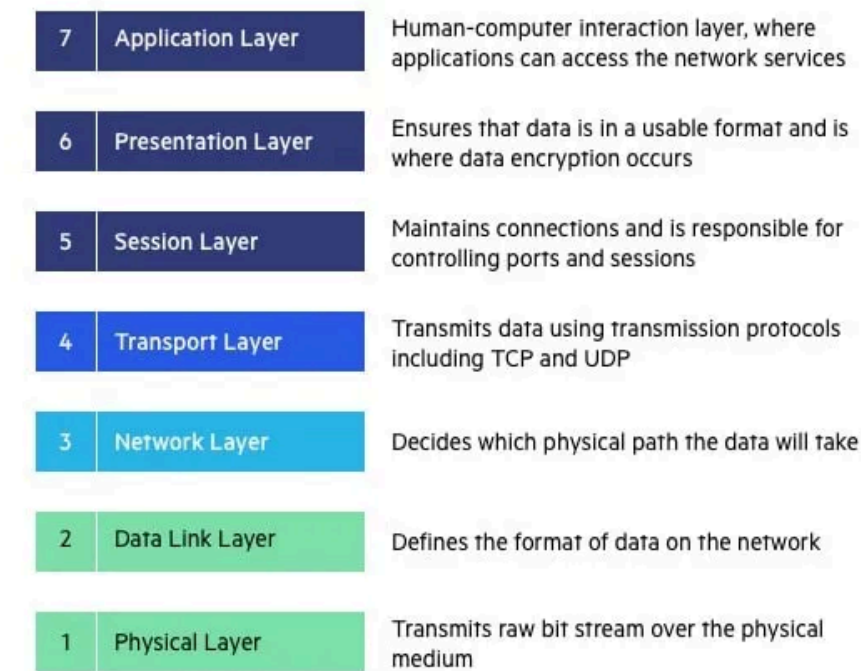
Chat with Document

Ask questions about document!

4

What is OSI?

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and standardize how different network protocols interact with each other to facilitate communication between devices over a network. It divides the process of communication into seven distinct layers, each with specific functions, ensuring that systems made by different manufacturers can communicate effectively



Why OSI model is used?

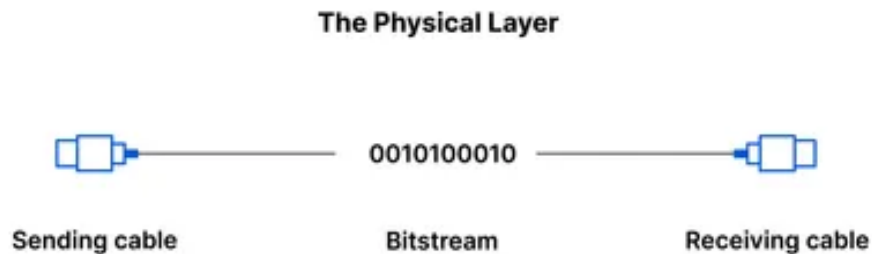
It simplifies complex networking through a layered, modular approach that aids in troubleshooting.

For example Engineers can fix hardware issues at the Physical Layer without affecting other layers. Switching from HTTP to HTTP/3 only changes the Application Layer. Security features like encryption and firewalls are added at different layers.

OSI: Layer 1

Layer 1: Physical Layer

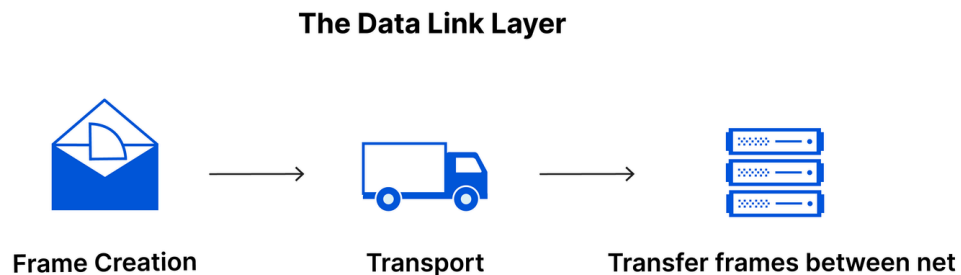
The Physical Layer is the first and lowest layer of the OSI model. Its primary responsibility is to handle the physical aspects of network communication.



The Physical Layer is responsible for defining the hardware technologies, such as cables, connectors, and other components used to transmit data over a network. It manages the encoding of data into physical signals (electrical, optical, or radio), ensuring proper transmission, reception, and synchronization of bits across the medium. Additionally, it defines signal characteristics and the physical network design, including the topology of the network (e.g., star, ring, bus, or mesh).

OSI: Layer 2

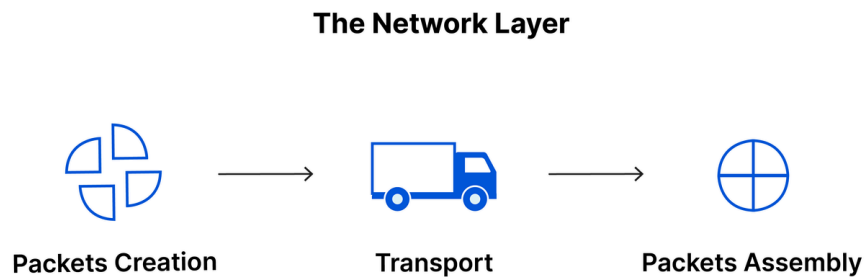
Layer 2 of the OSI model is the Data Link Layer. It sits above the Physical Layer (Layer 1) and is responsible for creating a reliable link between two directly connected nodes on a network.



The Data Link Layer organizes raw bits from the Physical Layer into frames, which include the payload and control information such as addresses and error-checking data. It uses MAC addresses to uniquely identify devices on the same network segment, ensuring that frames are delivered to the correct destination, and employs mechanisms like CRC for error detection and correction. Additionally, it regulates data flow to prevent overwhelming receivers and manages access to the physical medium to prevent collisions using protocols like CSMA/CD.

OSI: Layer 3

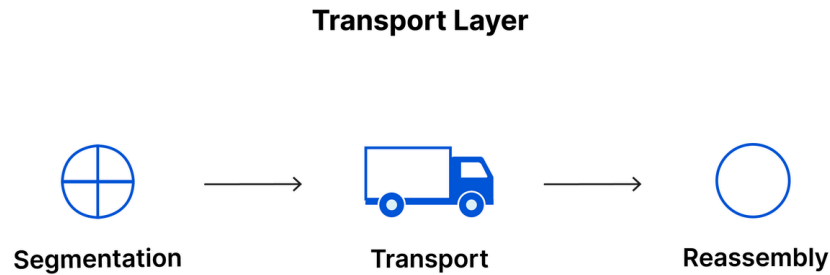
Layer 3 of the OSI model is the Network Layer. This layer is responsible for determining how data is routed and delivered across networks, often involving multiple hops between different devices and networks.



The Network Layer uses logical IP addresses to identify devices across different networks, enabling data to be routed over complex paths. It is responsible for finding the best path for data through routers, which forward packets based on destination IP addresses using routing protocols like OSPF and BGP. Additionally, the Network Layer handles packet forwarding, fragmentation and reassembly, error reporting through protocols like ICMP, and congestion control to ensure efficient data transmission.

OSI: Layer 4

Layer 4 of the OSI model is the Transport Layer. This layer is responsible for providing end-to-end communication services for applications, ensuring that data is delivered reliably and accurately between devices.

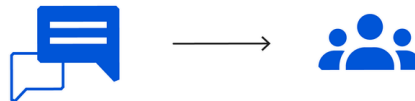


The Transport Layer divides large data into smaller segments for transmission and reassembles them at the destination, ensuring efficient data handling. It manages connections between devices either in a connection-oriented mode (using TCP for reliable, ordered delivery) or a connectionless mode (using UDP for faster, less reliable transmission). Additionally, the Transport Layer controls data flow to prevent congestion, handles error detection and recovery (in TCP), ensures data ordering, and multiplexes/demultiplexes data streams using port numbers to support multiple applications.

OSI: Layer 5

Layer 5 of the OSI model is the Session Layer. This layer is responsible for managing and controlling the interactions between applications on different devices. It establishes, maintains, and terminates connections (sessions) between applications, ensuring that they can communicate effectively.

The Session Layer

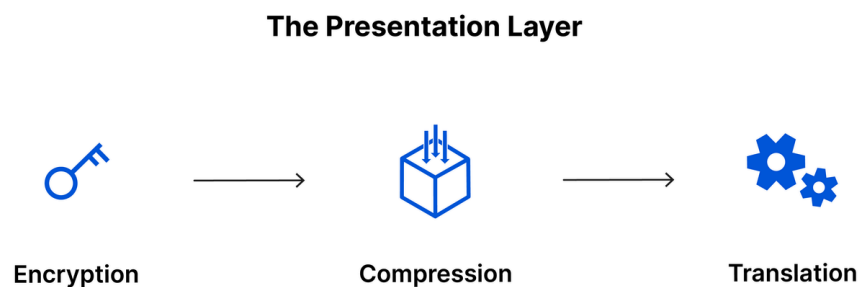


Session of communication

The Session Layer is responsible for establishing, maintaining, and terminating communication sessions between applications, ensuring both sides remain synchronized throughout the interaction. It manages the data exchange process by setting checkpoints, allowing sessions to resume from specific points if interrupted, and controlling the mode of communication, whether full-duplex or half-duplex. Additionally, the Session Layer provides synchronization mechanisms and protocols like NetBIOS and RPC to facilitate orderly and reliable inter-process communication between applications across a network.

OSI: Layer 6

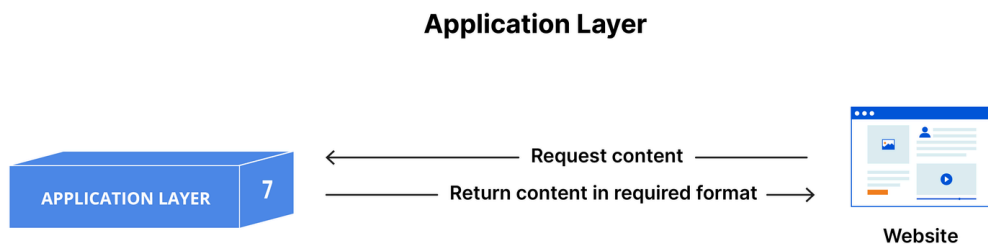
Layer 6 of the OSI model is the Presentation Layer. This layer is responsible for translating, encrypting, and compressing data to ensure that it can be properly understood by the receiving application. It acts as a translator between the application layer (Layer 7) and the lower layers of the OSI model.



The Presentation Layer translates and formats data from the application layer into a suitable format for transmission, including tasks like converting character sets and handling data encryption and compression. It ensures that data is properly formatted and compatible with the receiving application, and can perform protocol conversion to facilitate communication between different systems. This layer also manages syntax and semantics, making sure data is correctly interpreted and securely transmitted, with technologies such as MIME and SSL/TLS supporting these functions.

OSI: Layer 7

Layer 7 of the OSI model is the Application Layer. This is the topmost layer and is closest to the end user. It interacts directly with software applications to provide network services and enable communication between different applications over a network.

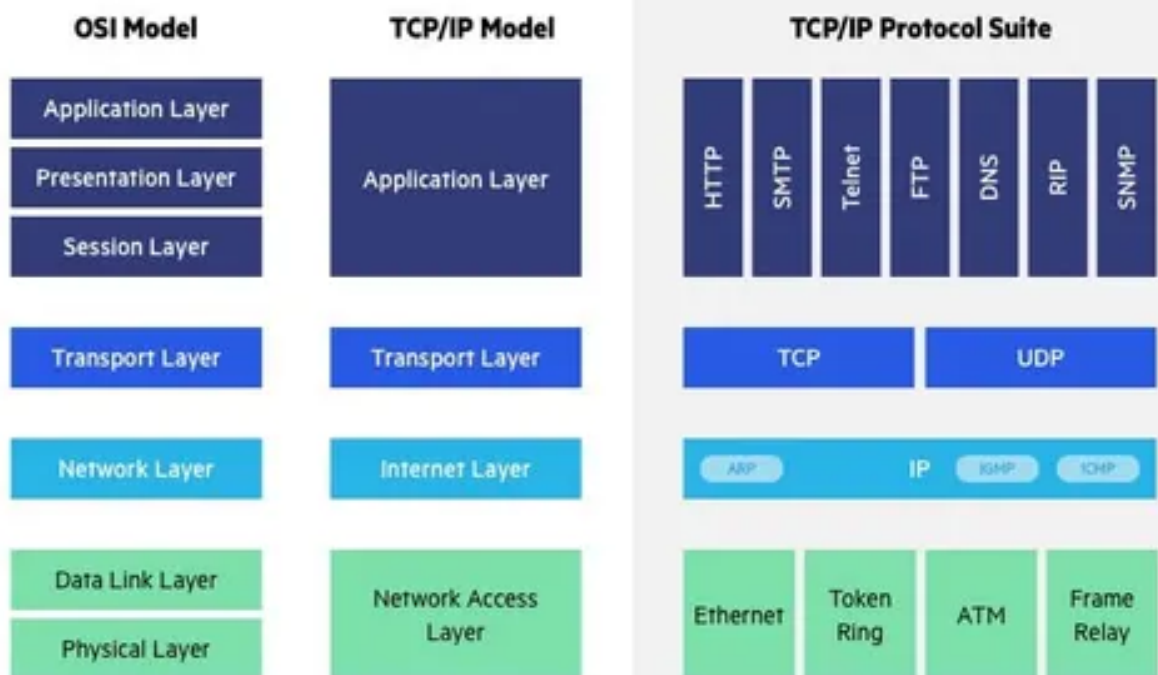


The Application Layer provides network services directly to end-user applications, supporting protocols like HTTP, FTP, SMTP, and DNS to enable tasks such as web browsing, file transfer, and email communication. It handles data representation and formatting, ensuring compatibility and proper interpretation between different systems, while also offering network services like authentication, authorization, and encryption. Although it does not provide user interfaces, it interacts with applications that do, facilitating end-to-end communication and managing data exchange, error handling, and recovery.

OSI vs TCP / IP

. Practical vs Theoretical Implementation

- OSI Model:
 - Use: Primarily a theoretical model used for understanding and designing network protocols and for educational purposes.
 - Implementation: Not directly implemented in its entirety but serves as a guideline for designing and analyzing network systems.
- TCP/IP Model:
 - Use: Directly implemented and used in real-world networking, including the Internet and most modern networks.
 - Implementation: Based on actual protocols used in networking, making it more pragmatic and aligned with real-world technologies.



OSI in DevOps

Load Balancers

- Layer 4 load balancers manage traffic based on IP addresses, ports, and transport protocols (TCP or UDP).
- Layer 7 load balancers manage traffic based on application-level details like HTTP headers, cookies, URLs, and request body content.

Infrastructure

- Understanding Layer 1 (Physical) and Layer 2 (Data Link) helps in designing efficient and secure virtual networks and subnets in cloud platforms like AWS, Azure, and GCP.
- Layer 3 (Network) knowledge of IP addressing and routing is crucial for configuring routing, load balancers, VPNs, and firewalls, as well as troubleshooting connectivity issues.

Security

- Securing data in transit involves Transport Layer 4 encryption (e.g., TLS/SSL) and proper configuration of firewall rules and secure communication protocols like HTTPS.
- On Layer 7, Secure application deployment requires managing access control, authentication, and authorization protocols like OAuth, SSL/TLS, and API keys.

Learn more about networking

Check HTB, they have great content

HTB - Your Cyber Performance Center

We provide a human-first platform creating and maintaining high performing cybersecurity individuals and organizations.

 <https://www.hackthebox.com/>



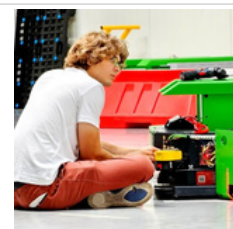
Share, comment, DM and check GitHub for scripts & playbooks created to automate process.

Check my GitHub

Michael Robotics

Hi, I'm Michal. I'm a Robotics Engineer and DevOps enthusiast. My mission is to create skill-learning platform that combats skill information overload by adhering to the set of principles: simplify, prioritize, and execute.

 <https://github.com/MichaelRobotics>



PS.

If you need a playbook or bash script to install KVM on a specific Linux distribution, feel free to ask me in the comments or send a direct message!