# OSI Model

by :mohamed salah

# Introduction

*OSI (**O**pen **S**ystems **I**nterconnection)*

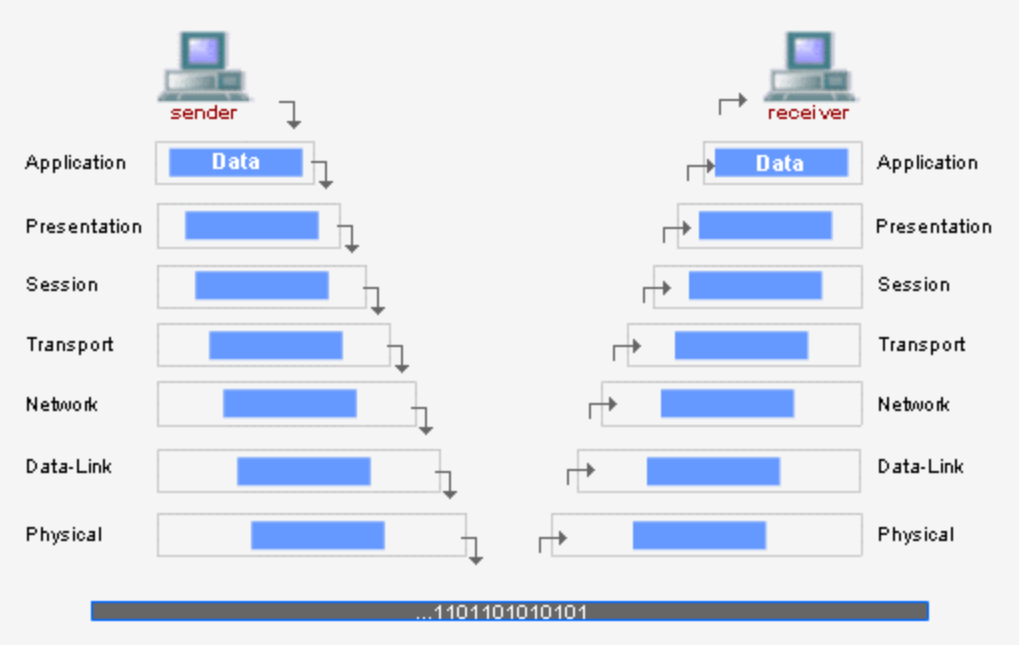
OSI model is a standardized model created by ISO and it was the first standard model for network communications adopted by all computer and telecommunication companies since the early 1980s .

The purpose of the OSI model is interconnection between systems as it's split into seven different layers  Physical, Data Link, Network, Transport, Session, Presentation, and Application .

each layer in the OSI model has its functions and the methods to communicate in a flow between above and below layers as appropriate .

A method to memorize the 7 layers is as follows :  All People Seem To Need Data Processing
(Application, Presentation, Session, Transport, Network, Data Link, Physical)

As you notice the flow of the communication starts from top to bottom of the layers specially when it to user interaction , as user interacts with the 7th layer ( Application ) and then the flow goes to the bottom layer which deals with the physical aspect /security and hardware as shown in the image below :




---

# The Seven layers :

7-Application Layer: Interfaces directly with user applications (browsers, email) Example : user opening a browser and accessing https://www.google.com it works exclusively with programs or applications that the user interacts with and when the user provides data its transferred down to the next layer.

6-Presentation Layer: Translates data formats (encryption, compression) , basically receives data from the application that the user interacted with but its not in a languages or format that is understood by the application layer , it translates data into a formal that into a standardized format and handles all the encryption and compression of said data .

5-Session Layer: Manages sessions (start, control, end of communication) once the data is transferred into the correct format the session layers sets up the connection with the other computers across the network , if there is any error in the data received it will return it back to the past layer until the proper format is delivered and it will not go further to the next layer , when the connection is successful the data is passed down to the next layer in the list which is the transport layer.

4-Transport Layer: Ensures reliable data delivery (TCP, UDP). this layer is serves several functions in the network and its main purpose is to choose the protocol in which data will be transmitted further depending on the need and requirements , the two most common protocols are TCP ( transmission control protocol ) and UDP ( User datagram protocol ) , this layer maintains a connection and makes sure al the packets are in the right place .

Example : TCP is mainly used for situations where there is need for speed , transferring data or loading webpages .

UDP : is preferred when speed is more important over accuracy and that shows itself in the form of video streaming .

3-Network Layer: Handles addressing and routing (IP addresses, routers) the network layer is responsible for locating the destination of requests as the internet is a huge network and there is need request information for a webpage, its this layer that takes the IP address for the page and routes to the best route , the most common form of addressing is the IPV4 format , E.g ( 192.168.1.1 ) which is the common ip address for a personal router .

2-Data Link Layer: Ensures error-free data transfer between directly connected devices , the data layer focuses on the physical addressing part of the data transmission I.e ( MAC ADDRESS ) which every unique internet card has its own ( fingerprint MAC address ) that is easily identifiable based on the manufacturer of said network card ( NIC ) , the data layer then makes sure that the data is presented in a suitable format for transmission of data , it also servers a the function of checking for corruptions in the data transmitted , although layer two is responsible for error detection (Checksum ) the data link layer servers a similar function .

1-Physical Layer: Deals with physical connections (cables, signals, etc.) the physical layer basically deals with all the hardware and wiring of the computer , it also servers the job of converting the data binary data transferred over the network into signals to be transmitted through the network and vice versa .

# Importance of the OSI Model

- Makes it easier to design and build networks.
- Allows special focus on each layer's specific role (physical, data transfer, routing, etc.).
- Even though networks today use the TCP/IP model, OSI is still used for learning and understanding networking concepts.
- Helps SOC analysts understand how attacks move through different layers.
- Helps detect anomalies at each layer

# Conclusion

The OSI Model is a vital tool for understanding how networks work and how cyber threats move through them. In a SOC environment, it helps analysts pinpoint vulnerabilities, detect attacks, and respond effectively by breaking down complex communication into clear, manageable layers. Even as technology evolves, the OSI Model remains a foundation for both networking and cybersecurity.

---