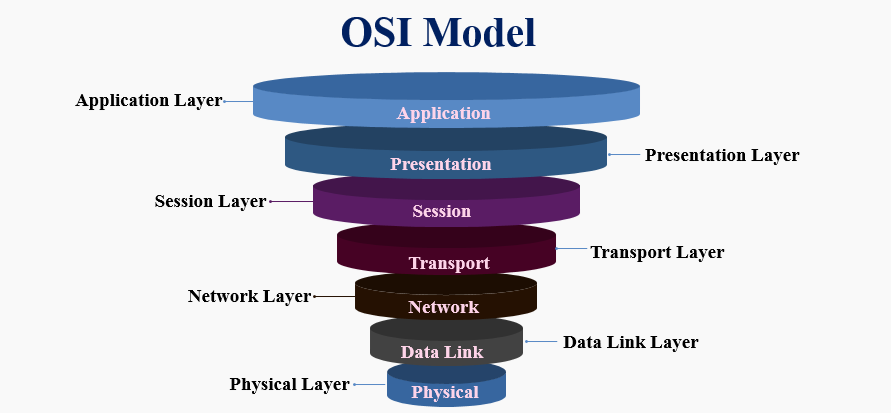
Module code: athe 5.1 Cyber secuity

Name: FATIMA EJAZ BARRI

Email: [mishalfatimaeb@gmail.com](mailto:mishalfatimaeb@gmail.com)

Topic: Given by tutor by Shahid Mustafa

# What is OSI model? Explain functionality of all the layers?

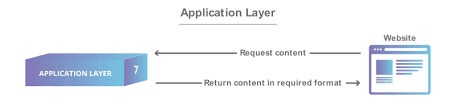
A networking model offers a generic means to separate computer networking functions into multiple layers. Each of these layers relies on the layers below it to provide supporting capabilities and performs support to the layers above it. Such a model of layered functionality is also called a “protocol stack” or “protocol suite”. Protocols, or rules, can do their work in either hardware or software or, as with most protocol stacks, in a combination of the two. The nature of these stacks is that the lower layers do their work in hardware or firmware (software that runs on specific hardware chips) while the higher layers work in software.

# Functions of the OSI layers

* Application layer
* Presentation layer
* Session layer
* Transport layer
* Network layer
* Data link layer
* Physical layer

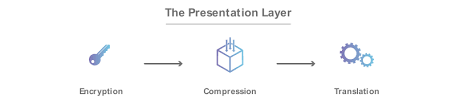
**Application layer:**

This layer personalizes data according to the user by using many tools. It is the only layer that uses the data from user to its advantage. This layer is used to make communication easier and is used my many social websites and apps.



**Presentation Layer:**

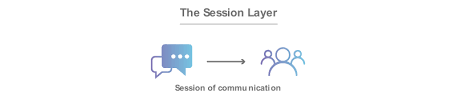
The presentation layer encrypts data to be sent across the network, and decrypts it so that it can be accessed by the application layer on the receiving end.



**Session Layer:**

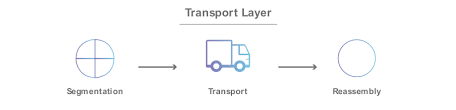
The session layer, provides various services, including tracking the number of bytes that each end of the session has acknowledged receiving from the other end of the session. This session layer allows applications functioning on devices to establish, manage, and terminate a dialog through a network. Session layer functionality includes:

* + Virtual connection between application entities
  + Synchronization of data flow
  + Creation of dialog units
  + Connection parameter negotiations
  + Acknowledgements of data received during a session
  + Retransmission of data if it is not received by a device



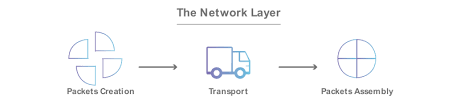
**Transport Layer:**

This layer is responsible for the communication between two devices and it breaks down the information into big chunks to pass it on to the next layer. The second device that receives information arranges the segments into data so it can be easily interpreted by the next layer. This layer also controls flow and error in the network. Flow control entails that the layer makes sure that the difference in connection does not affect the data transmission while error control makes sure that the data received is useful and complete.



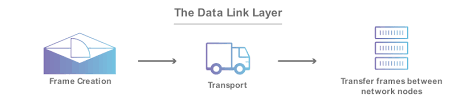
**Network Layer:**

The network layer establishes the route between the sender and receiver across switching points, which are typically routers. The most ubiquitous example of this layer is the IP protocol in TCP/IP. IPX, SNA and AppleTalk are other examples of routable protocols, which mean that they include a network address and a station address in their addressing system. This layer is also the switching function of the dial-up telephone system. If all stations are contained within a single network segment, then the routing capability in this layer is not required.



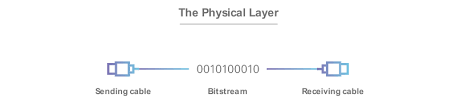
**Data Link Layer:**

Data-link layer helps in the transfer of information between devices which are in the same network. It breaks down information transferred from the network layer into smaller pieces and then transfers them on. It controls the errors and flow of the network but the ones that are inside the network its working in.



**Physical Layer:**

The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements. Electrical, mechanical, functional, and procedural specifications are provided for sending a bit stream on a computer network.



# Difference between IPv4 and mac address?

# Internet protocol version (IPv4)

IPv4 uses 32-bit (four-byte) addresses, which limits the address space to 2^32 addresses. Due to this limitation and phenomenal increase in devices accessing internet IPv6 was developed in the 1990s. IPv4 addresses may be represented in any notation expressing a 32-bit integer value. They are most often written in the dot-decimal notation, which consists of four octets of the address expressed individually in decimal numbers and separated by periods.

# MAC address

The MAC address is a hardware address, which means it is unique to the network card installed on your PC. No two devices on a local network should ever have the same MAC address. In the unlikely event this occurs, the two devices will have major communication problems. During the manufacturing process, the vendor "burns" a specific MAC address into each network card's ROM. When the serial numbers have all been used, they start from the beginning, as it's very unlikely anyone would buy two network cards from the same vendor, and they will contain the same MAC address. So, to sum all that up, you should remember that an IP address is a logical address which is configured via the operating system, while the MAC address is a hardware address, burnt into the network card's ROM during the manufacturing process.

