***ISO Model***

1. **Application layer:**

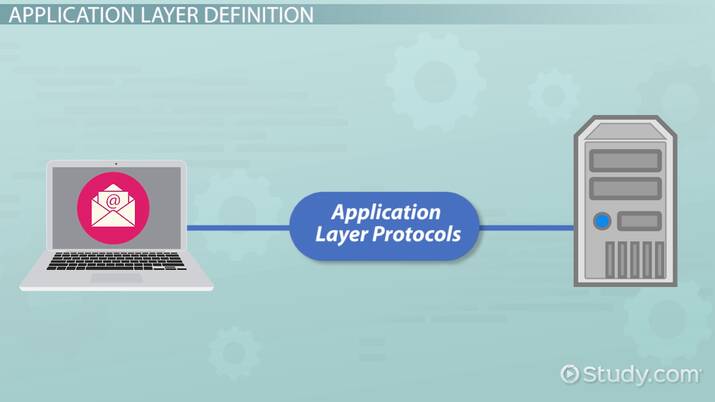
It fetches the data from the application and provides email services.

The Application layer is implemented by the network applications.

These applications produce the data to be transferred over the network.

The application services access the network and display the received information to the user.

This application provides distributed database sources and access to global information about various objects and services.

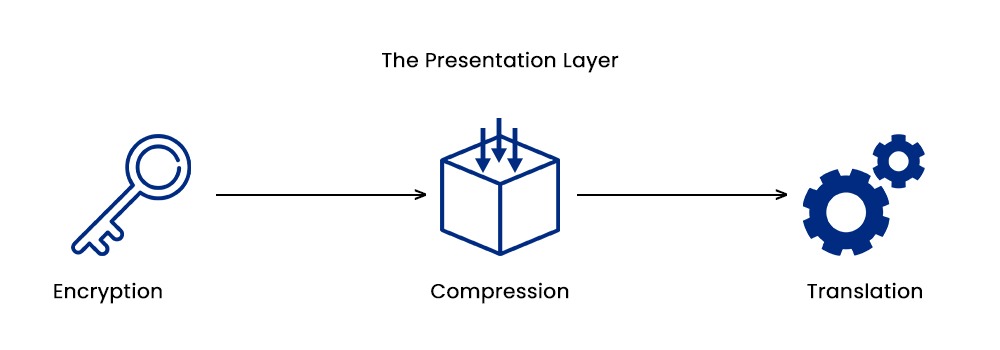


1. **Presentation Layer:**

The presentation layer is also called the Translation layer.

The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

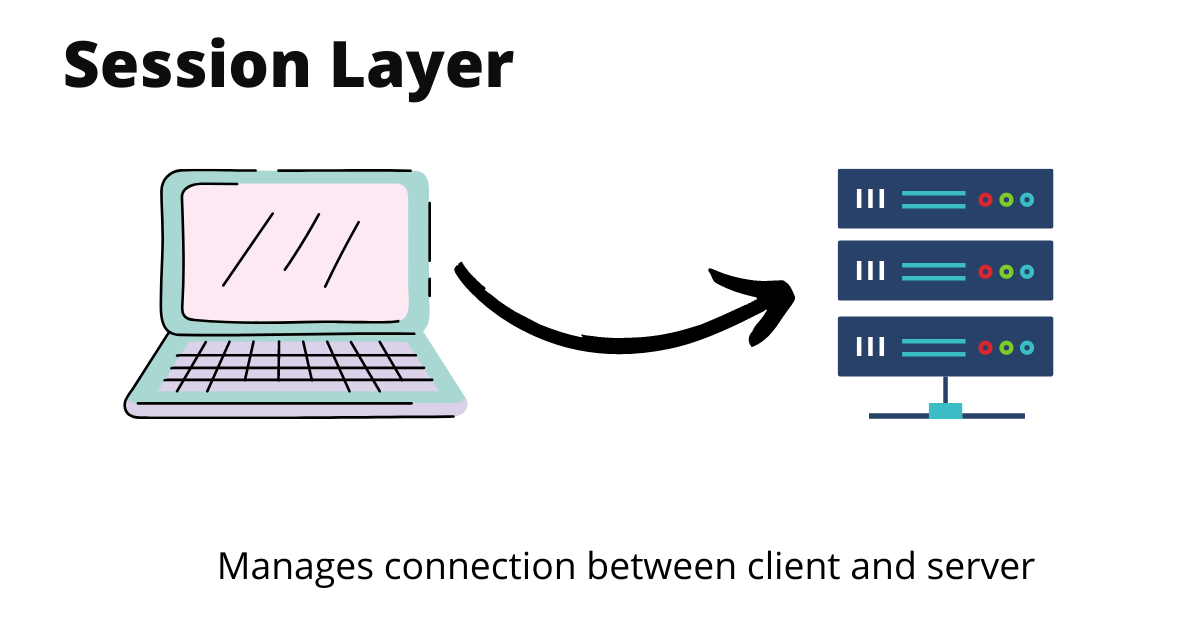
Mail application prepares for data transmission like encrypting data and formatting it for transmission.



1. **Session Layer:**

This layer builds the connection between sender and receiver on the internet. And also ensures security.

This layer allows the communication between two systems via half duplex or full duplex.



1. **Transport Layer:**

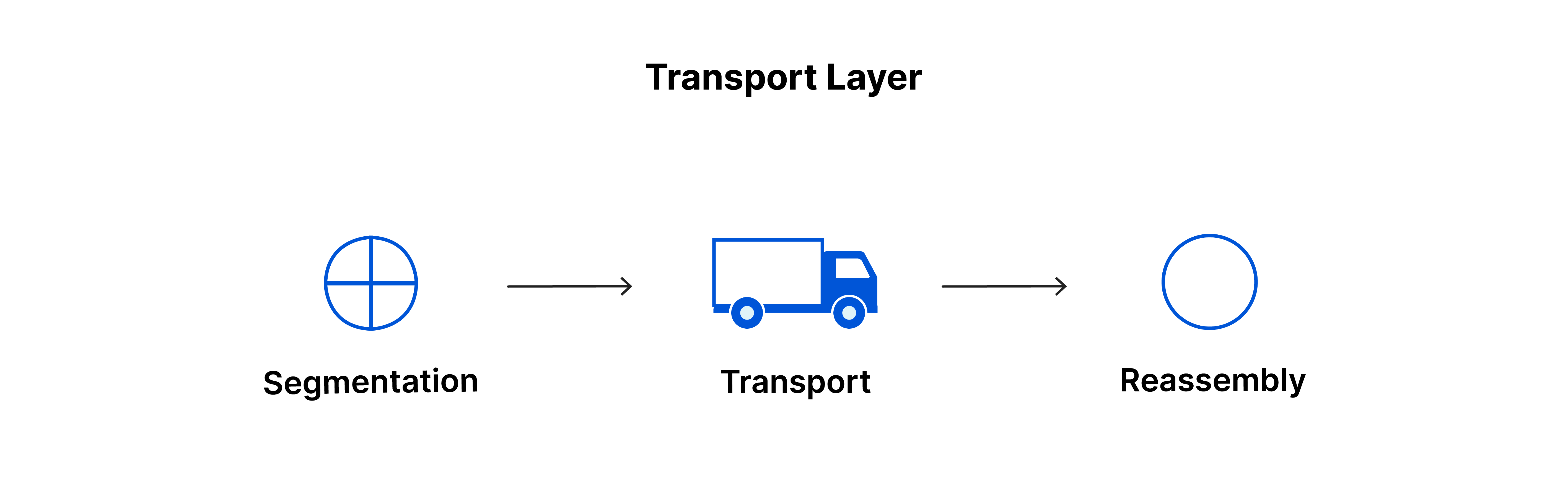
It provides services to the application layer and takes services from the network layer.

The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

The transport layer receives the formatted data from the upper layers and performs Segmentation. The transport layer implements the flow and error control to ensure proper data transmission.

It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Transport Layer reads the port number from its header and forwards the Data that it has received to the respective application.



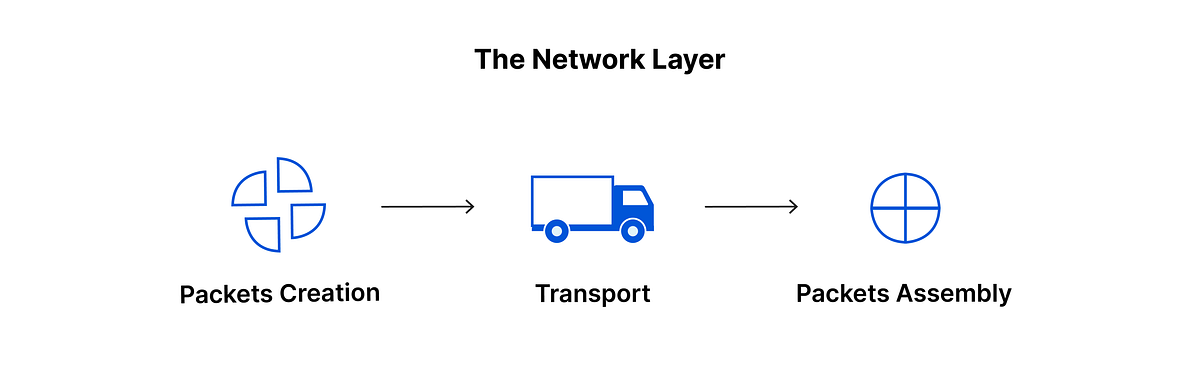
1. **Network Layer:**

The network layer works for the transmission of data from one host to the other located in different networks.

It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.

The sender & receiver’s IP addresses are placed in the header by the network layer.

The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.



1. **Data Link Layer:**

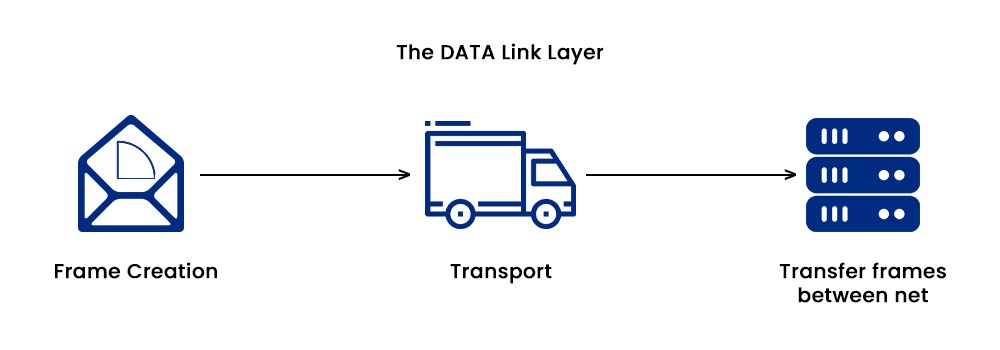
The data link layer is responsible for the node-to-node delivery of the message.

The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer.

When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

**The Data Link Layer is divided into two sublayers:**

* Logical Link Control (LLC)
* Media Access Control (MAC)



1. **Physical Layer:**

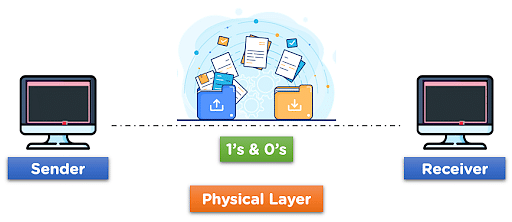
The lowest layer of the OSI reference model is the physical layer.

It is responsible for the actual physical connection between the devices.

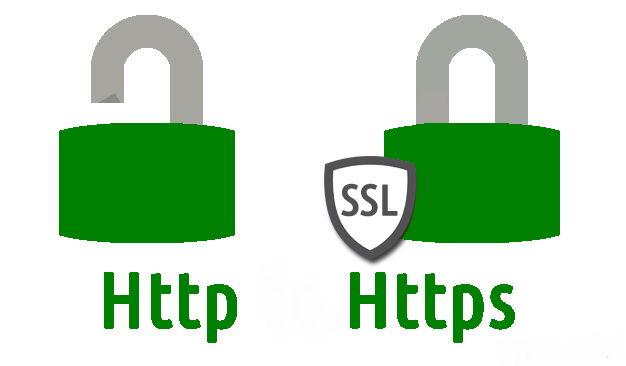
The physical layer contains information in the form ofbits.

It is responsible for transmitting individual bits from one node to the next.

When receiving data, this layer will get the signal received and convert it into 0s and 1s, and send them to the Data Link layer, which will put the frame back together.



***HTTP & HTTPS***



**HTTP(Hypertext Transfer Protocol):**

* HyperText Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web.
* Due to its simplicity, HTTP has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using HTTP isn’t as secure as we would like it to be.
* In fact, hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data.
* The web server delivers the desired data to the user in the form of web pages when the user initiates an HTTP request through their browser. Above the TCP layer lies an application layer protocol called HTTP. It has given web browsers and servers certain standard principles that they can use to talk to one another.
* Because each transaction on the HTTP protocol is carried out independently of the others and without reference to the history, the connection between the web browser and the server ends after the transaction is finished. This makes HTTP a stateless protocol.

**HTTPS(Hypertext Transfer Protocol Secure):**

* Hypertext Transfer Protocol Secure (HTTPS) is an extended version of the Hypertext Transfer Protocol (HTTP). It is used for secure communication.
* In HTTPS, the communication protocol is encrypted using Transport Layer Security.
* HTTPS stands for Hypertext Transfer Protocol Secure.
* While HTTP guarantees data security, the HTTP protocol does not provide data security.
* As a result, HTTPS can be defined as a secure variant of the HTTP protocol. Data can be transferred using this protocol in an encrypted format.
* In most cases, the HTTPS protocol must be used while entering bank account information.
* The HTTPS protocol is mostly utilised in situations when entering login credentials is necessary. Modern browsers like Chrome distinguish between the HTTP and HTTPS protocols based on distinct markings.
* HTTPS employs an encryption mechanism called Secure Sockets Layer (SSL), also known as Transport Layer Security, to enable encryption.

***Note:***

* HTTPS is just HTTP with verification and encryption. The use of TLS (SSL) by HTTPS to encrypt and digitally sign standard HTTP requests and answers is the only distinction between the two protocols.
* The default port number of HTTP is 80 and the default port number of HTTPS is 443.