The OSI Reference Model

What is the OSI Reference Model?

OSI Model stands for the *Open System Interconnection model*. **OSI Model** defines how **data is transferred** from one computer to another computer regardless of the operating system or vendor of the hardware.

In a very basic scenario, two computers connected with a LAN and transfer data using the Network Interface Card (NIC or Network Adapter). This forms a computer network, however, if both systems use different operating systems, for example, one system runs on Windows and the other one runs on macOS then how can data be exchanged between these two different systems? Here comes the role of an OSI model which is a seven-layered model that defines how data can be exchanged between different systems.

OSI model was introduced by the International Organisation for standardization (ISO) in 1984. There are seven layers in an OSI model.

Data	Application Network services to Application	7
Data	Presentation Data Formatting and Encryption	6
Data	Session Interhost Communication	5
Segments (TCP) Datagrams (UDP)	Transport End-to-End Connections and Reliability	4
Packets	Network Routing and IP (Logical Addressing)	3
Frames	Data Link MAC and LLC (Physical Addressing)	2
Bits	Physical Media, Signal and Binary Transmission	1

The OSI Network Layers

As the complexity of computer hardware and software increases, the problem of successfully communicating between these systems becomes more difficult. Dividing these difficult problems into "sub-tasks" allows them to be readily understood and solved more easily. Using this layered approach means that a vendor can work on the design and debugging for a particular layer without affecting any of the others.

Each layer performs a different group of tasks required for network communication. Although not all network systems implement layers using this structure, they all implement each task in some way. The OSI model is not a standard or a specification; it serves as a **functional guideline** for designing network protocols, software, and appliances and for troubleshooting networks.

The OSI's seven layers are divided into two groups. The top three layers (**upper layers**) define the rules of how the applications working within host machines communicate with each other as well as with end-users. The bottom four layers (**lower layers**) define how the actual data is transmitted from end to end.

Advantages of OSI Reference Model

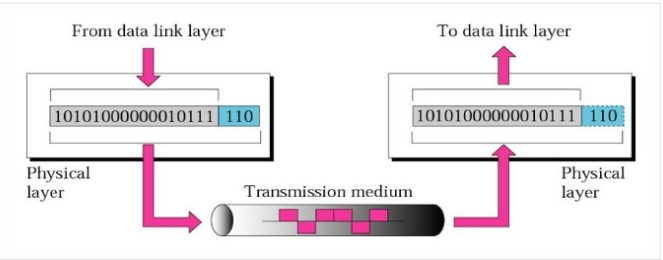
The OSI model is hierarchical. Understand that the central purpose of the OSI, and all networking models, is to allow different vendors' networks to interoperate smoothly. This short-list depicts some of the most important advantages we gain by using the OSI layered model:

- The OSI model divides network communication processes into smaller and simpler components, thus aiding component development, design, and troubleshooting.
- It allows multiple-vendor development through the standardization of network components.
- It encourages industry standardization by defining the specific functions that occur at each layer of the model.
- It allows various types of network hardware and software to communicate.
- It prevents changes in one layer from affecting other layers, facilitating development and making application programming much easier.

Physical Layer

The physical layer of the OSI model (layer 1) is responsible for the transmission and receipt of bits from one node to another node. It specifies the following:

- Physical network topology - mechanical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
- The process of transmitting and receiving signals from the network medium including modulation schemes and timing/synchronization.



Transmission at Physical Layer

Devices operating at the physical layer include:

- **Transceiver** - the part of a network interface that sends and receives signals over the network media.
- **Media Converter** - converts one media signaling type to another.
- **Repeater** - amplifies the signal to extend the maximum allowable distance for a media type.
- **Hub** - a multiport repeater, deployed as the central point of connection for nodes wired in a star topology.
- **Modem** - a device that converts between digital and analog signal transmissions.

Transceiver

Media Converter

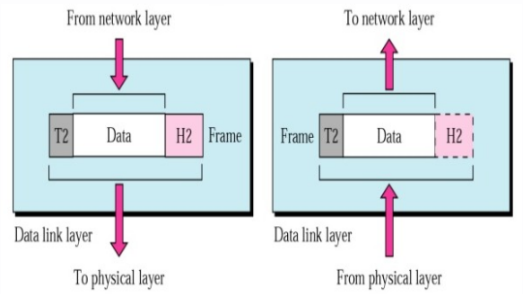
Repeater

Hub

Modem

Data Link Layer

The data link layer (layer 2) is responsible for transferring data between nodes on the same network segment. The data link layer splits the message into pieces, each called a *data frame*, and adds a customized header. This header contains a source and destination hardware (MAC) address and error checking values. Other information includes the frame length and network layer protocol identifier.



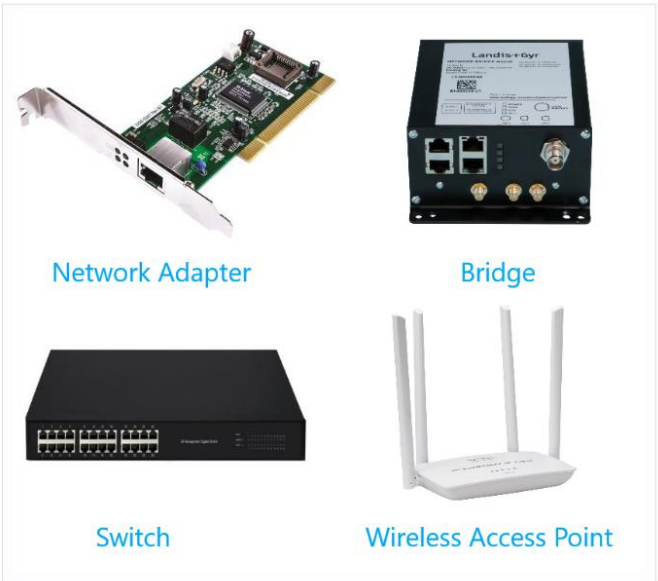
A network frame

Some network products use multiple different frame types. For example, Ethernet specifies four frame types. The basic structure remains the same but each frame type contains a slightly different header structure. Devices must communicate using the same frame type.

The last part of the frame usually contains some sort of error checking. Protocols at almost every layer perform a consistency check to verify that data has been transferred correctly. The data link layer is only capable of very basic error checking, such as identifying truncated or corrupted frames. There is no function to acknowledge or retransmit damaged frames. That function is handled at higher layers of the OSI model.

Connectivity devices found at the data link layer include:

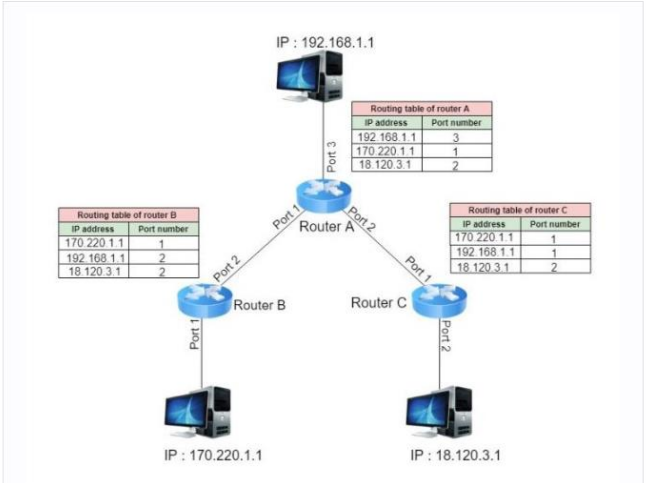
- **Network adapter (or Network Interface Card [NIC])** - joins a host computer to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
- **Bridge** - joins two network segments while minimizing the performance reduction of having more nodes on the same network.
- **Basic switch** - a multiport bridge that creates links between nodes more efficiently.
- **Wireless Access Point (AP)** - allows nodes with wireless network cards to communicate and joins wireless networks to wired ones.



Data Link Layer devices

Network Layer

The network layer (layer 3) is responsible for moving data around a network of networks, known as an internetwork or internet. While the data link layer moves data using hardware addresses within a single network segment, the network layer moves information around an internetwork using a logical network and host IDs.



Network Layer

The network layer transfers information between networks by examining the destination network layer address or logical network address and routing the packet through the internetwork using intermediate systems (routers). The packet moves, hop by hop, through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to move the packet to the target node. This process requires each logically separate network to have a unique network address.

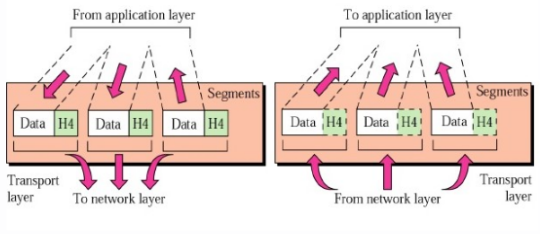
The main appliance working at layer 3 is the router. Other devices include Layer 3 switches (combining the function of switches and routers) and basic firewalls.

Transport Layer

The first three layers of the OSI model are primarily concerned with moving frames and datagrams between nodes and networks. At the transport layer (also known as the end-to-end or host-to-host layer) the content of the packets starts to become significant.

Any given host on a network will be communicating with many other hosts using many different types of networking data. One of the critical functions of the transport layer is to identify each type of network application by assigning it a port number. For example, data from the HTTP web browsing application can be identified as port 80 while data from an email server can be identified as port 25.

At the transport layer, on the sending host, data from the upper layers are packaged as a series of segments and each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. The host could be transmitting multiple HTTP and email segments at the same time.



Transport Layer

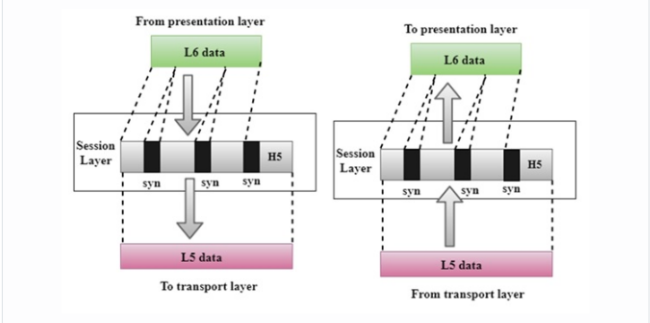
At the network and data link layers, the port number is not significant - it becomes part of the data payload and is "invisible" to routers and switches working at the network and data link layers. At the receiving host, each segment is extracted from its frame and then identified by its port number and passed up to the relevant handler at the upper session and application layers.

The transport layer is also responsible for ensuring reliable data delivery so that packets arrive error-free and without loss. The transport layer can overcome any lack of reliability in the lower level protocols. This reliability is achieved using **acknowledgment** messages that inform the sender the data was successfully received. The kinds of problems that may occur during the delivery of the data are non-delivery and delivery in a damaged state. In the first case, the lack of acknowledgment results in the retransmission of the data and, in the second case, a **Negative Acknowledgement (NACK)** forces retransmission.

Devices working at the transport layer (or above) include multilayer switches and security appliances such as more advanced firewalls and Intrusion Detection Systems (IDS).

Session Layer

Most application protocols require the exchange of multiple messages between the client and the server. This exchange of such a sequence of messages is called a **session** or **dialog**. The session layer (layer 5) represents the dialog control functions that administer the process of establishing the dialog, managing data transfer, and then ending (or "tearing down") the session.



Sessions can work in three modes:

- **One-way/simplex** - only one system is allowed to send messages; the other receives only.
- **Two-Way Alternate (TWA)/half-duplex** - the hosts establish some system for taking turns to send messages, such as exchanging a token.
- **Two-Way Simultaneous (TWS)/duplex** - either host can send messages at any time.

The session layer can also provide a synchronization service for long transactions in which checkpoints are inserted into the data stream (dialog separation). If a problem occurs, only the data transferred after the last checkpoint is re-sent.

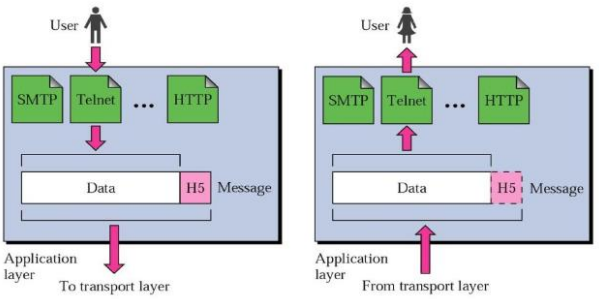
In summary, this layer primarily manages applications' data by separating from each other application. For instance, multiple web browser sessions at the same time on your desktop are handled by the help of session layer.

Presentation Layer

The presentation layer (layer 6) transforms data between the format required for the network and the format required for the application. For example, the presentation layer is used for character set conversion. The communicating computers may use different character coding systems (such as American Standard Code for Information Interchange [ASCII] and Unicode); the peer presentation layers agree to translate the data into one of the formats or they will both translate the data into a third format. The presentation layer can also be conceived as supporting data compression and encryption (scrambling a message so that it can only be read in conjunction with a valid "key"). However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack.

Application Layer

The application layer (layer 7) is at the top. An application layer protocol doesn't encapsulate any other protocols or provide services to any protocol. An application layer protocol provides an interface for software applications on network hosts that have established a communication channel using the lower-level protocols to exchange data. For example, one of the most utilized services provided by the application layer is file transfer. Different file systems may use entirely different file naming conventions and data syntax and the application layer must overcome these differences. More widely, upper-layer protocols provide most of the services that make a network useful, rather than just functional, including network printing, electronic mail and communications, directory lookup, and database services.

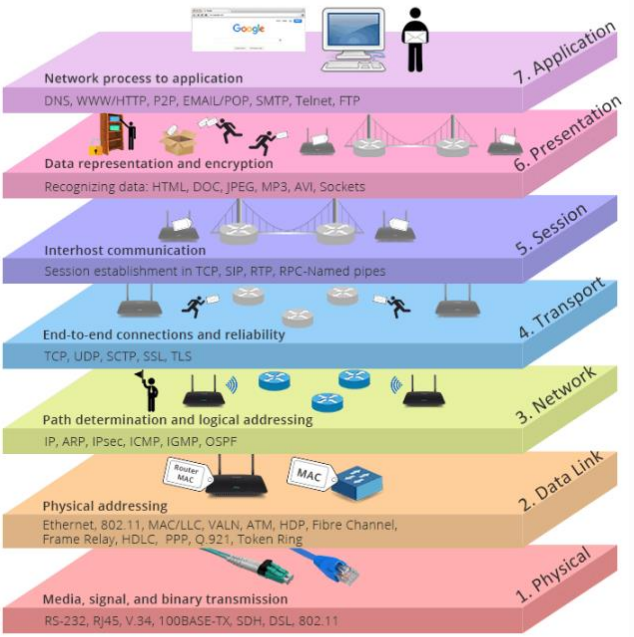


Application Layer

It is important to distinguish between network application protocols and the software application code (programs and shared programming libraries) that run on computers. Software programs and operating systems make use of the Application Programming Interface (API) to call functions of the relevant part of the network stack. Examples of APIs include:

- Network card drivers could use the Network Driver Interface Specification (NDIS) API to implement functions at the data link layer.
- The Sockets / WinSock APIs implement transport and session layer functions.
- High-level APIs implement functions for services such as file transfer, email, web browsing, or name resolution.

Summary



The OSI Reference Model