**TCP/IP vs OSI Model:**

There are two network models that are very much used nowadays. One is the OSI model, and the other is the TCP/IP model. TCP/IP vs. OSI is a persistent topic in the networking field, so let’s see how both models really differ.

**OSI Model**

OSI (Open System Interconnection) model was created by the International Organization for Standardization (ISO), an international standard-setting body. It was designed to be a reference model for describing the functions of a communication system.

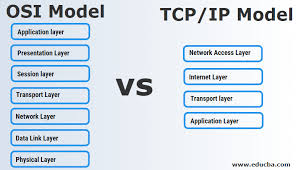
The OSI model provides a framework for creating and implementing networking standards and devices and describes how network applications on different computers can communicate through the network media.

**TCP/IP Model**

The TCP/IP model was created in the 1970s by the Defense Advance Research Project Agency (DARPA) as an open, vendor-neutral, public networking model. Like the OSI model, it describes general guidelines for designing and implementing computer protocols. It consists of four layers: Network Access, Internet, Transport, and Application.

**Differences between TCP/IP vs OSI model**

There are other differences between these two models besides the obvious difference in the number of layers. OSI model prescribes the steps needed to transfer data over a network, and it is very specific in it, defining which protocol is used at each layer and how. The TCP/IP model is not that specific. It can be said that the OSI model prescribes and TCP/IP model describes.



**Comparison TCP/IP vs OSI model**

The TCP/IP and OSI models are two prominent network models used in the field of networking. The OSI model, developed by the International Organization for Standardization (ISO), serves as a reference model for describing communication systems' functions. It consists of seven layers, each detailing specific network functions and protocols. Conversely, the TCP/IP model, established by the Defense Advanced Research Projects Agency (DARPA), is a simpler, four-layer model focusing on practical guidelines for network protocol design and implementation.

**OSI** **Model**:

**Physical** **Layer**: Handles raw data transmission over physical media and defines hardware specifications.

**Data** **Link** **Layer**: Encapsulates data into frames, manages access to the physical medium, and performs error detection.

**Network** **Layer**: Manages device addressing, routing, and path determination across networks.

**Transport** **Layer**: Segments data, establishes connections, and provides reliability mechanisms like flow control.

**Session** **Layer**: Manages session establishment, maintenance, and termination between systems.

**Presentation** **Layer**: Defines data formats, compression, and encryption techniques.

**Application** **Layer**: Provides interfaces for user applications to access network services.

**TCP/IP** **Model**:

**Network** **Access** **Layer**: Specifies protocols and hardware for data delivery across physical networks.

**Internet** **Layer**: Handles logical packet transmission over the network and includes protocols like IP.

**Transport** **Layer**: Manages transmission service levels, ensures data reliability, and includes protocols like TCP and UDP.

**Application** **Layer**: Facilitates node-to-node application communication and provides services to application software.

**Local Area Network (LAN)**

The term local area network (LAN) is commonly used to describe a network of devices in a limited area (a house, office, building, etc.). This type of network is usually capable of achieving high data transfer rate (up to 10 Gbps!) at low cost. Examples of this type of network are a small office network inside a single building or your home network. are commonly associated with the Physical layer, laying the groundwork for communication across diverse network infrastructures.

**TCP/IP Suite of Protocols**

**ARP (Address Resolution Protocol):** Associates IP addresses with MAC addresses, facilitating communication within a network by resolving hardware addresses.

**IP** (**Internet** **Protocol**): Governs packet delivery based on IP addresses, enabling data transmission from source to destination hosts across networks.

**ICMP** (**Internet** **Control** **Message** **Protocol**): Detects and reports network errors, commonly utilized in tools like ping to diagnose network connectivity issues.

**TCP** (**Transmission** **Control** **Protocol**): A connection-oriented protocol ensuring reliable data transfer between computers by establishing and maintaining connections.

**UDP** (**User** **Datagram** **Protocol**): A connectionless protocol facilitating data transfer without prior session establishment, though without guaranteeing delivery.

**FTP** (**File** **Transfer** **Protocol**): Enables the transfer of files between hosts, commonly used for sharing files over networks securely.

**Telnet** (**Telecommunications** **Network**): Allows remote access to computers, enabling users to issue commands and perform tasks on distant systems.

**DNS** (**Domain** **Name** **System**): Facilitates host name to IP address resolution, essential for translating human-readable domain names into IP addresses.

**HTTP** (**Hypertext** **Transfer** **Protocol**): Primarily used for transferring files, including text, images, sound, video, and multimedia content, over the World Wide Web.

**(KARAN TOLAMBIYA)**

**15-05-2024**