…TCP/IP vs. OSI: What's the Difference Between the Two Models?

Sheldon

Updated on Sep 29, 2021   👁 229.0k

When we are talking about layer 2 switches and layer 3 Ethernet switch, we are actually referring to the layers of a generic protocol model—Open Source Interconnect (OSI) model. It is commonly used in describing network communications. The data communications between different networks are not possible if there are no common rules for transmitting and receiving the packets of data. These rules are known as protocols, among which the Transmission Control Protocol (TCP)/Internet Protocol (IP) is one of the most widely used. The TCP/IP model is popularly used in network description and is older than OSI model. They both have many layers, what's the difference between them?

OSI Reference Model Layers

OSI model is a conceptual model that characterizes and standardizes how different software and hardware components involved in a network communication should divide labor and interact with one another. It has seven layers.
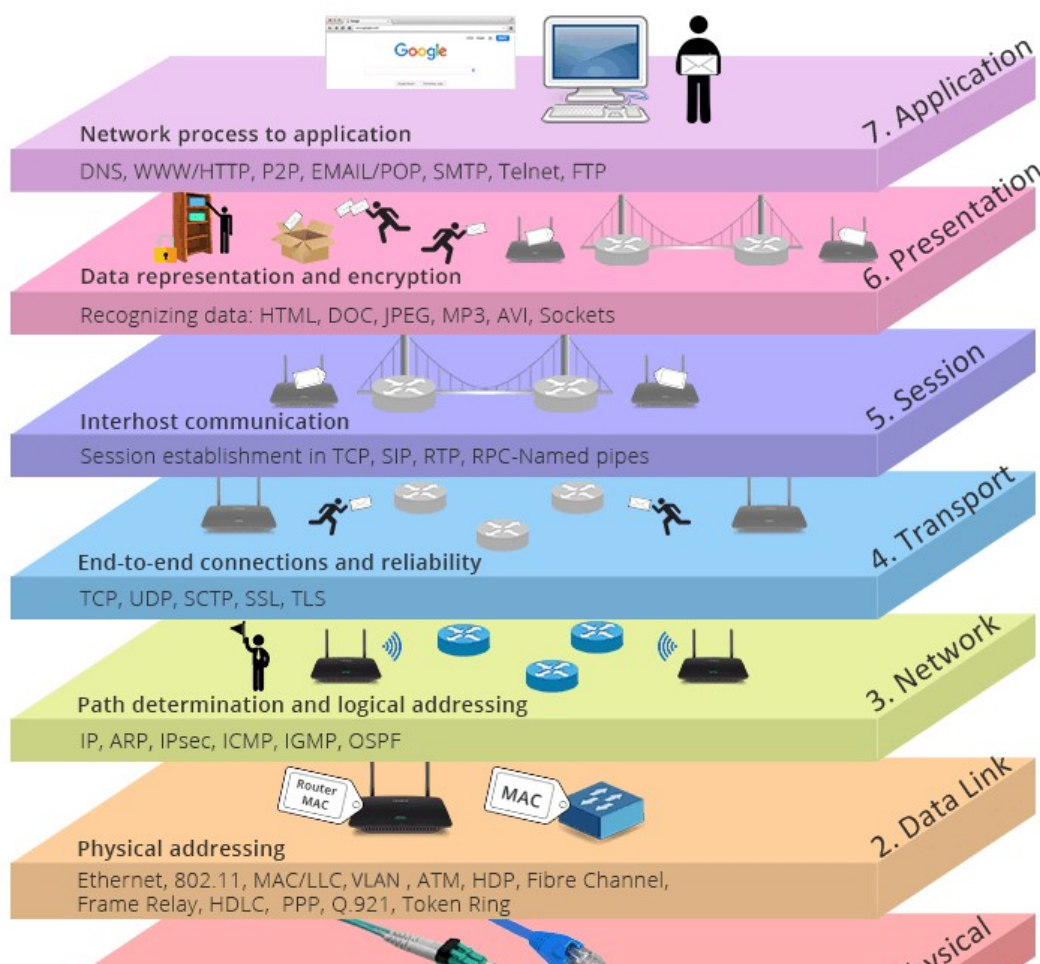
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Figure 1: seven layers of the OSI model.

Layer 7: Application Layer

The application layer of OSI model interacts directly with software applications to provide communication functions as required, and it is the closest to end users. Functions of application layer typically include verifying the availability of communication partners and resources to support any data transfer. This layer also defines protocols for end applications, such as domain name system (DNS), file transfer protocol (FTP), hypertext transfer protocol (HTTP), Internet massage access protocol (IMAP), post office protocol (POP), simple mail transfer protocol (SMTP), Simple Network Management Protocol (SNMP), and Telnet (a terminal emulation).

Layer 6: Presentation Layer

The presentation layer checks the data to ensure it is compatible with the communications resources. It translates the data into the form that the application level and lower levels accept. Any needed data formatting or code conversion is also handled by the sixth layer, such as converting an Extended Binary Coded Decimal Interchange Code (EBCDIC) coded text file to an American Standard Code for Information Interchange (ASCII) coded text file. It functions for data compression and encryption as well. For example, video calls will be compressed during the transmission so that it can be transmitted faster, and the data will be recovered at the receiving side. For the data that has high security requirements, such as a text message containing your password, it will be encrypted at this layer.

Layer 5: Session Layer

The session layer controls the dialogues (connections) between computers. It establishes, manages, maintains and ultimately terminates the connections between the local and remote application. Layer 5 software also handles authentication and authorization functions. It verifies the data is delivered as well. The session layer is commonly implemented explicitly in application environments that use remote procedure calls.

Layer 4: Transport Layer

The transport layer provides the functions and means of transferring data sequences from a source to a destination host via one or more networks, while maintaining the quality of service (QoS) functions and ensure the complete delivery of the data. The integrity of the data can be guaranteed via error correction and similar functions. It can also provide explicit flow control function. Though not strictly conforming to the OSI model, the TCP and User Datagram Protocols (UDP) are essential protocols in layer 4.

Layer 3: Network Layer

The network layer handles packet routing via logical addressing and switching functions. A network is a medium to which many nodes can be connected. Every node has an address. When a node needs to transfer message to other nodes, it can merely provide the content of the massage and the address of the destination node, then the network will find the way to deliver the message to the destination node, possibly routing through other nodes. If the message is too long, the network may split it into several segments at one node, sending them separately and reassembling the fragments at another node.

Layer 2: Data Link Layer

The data link layer provides node-to-node transfer—a link between two directly connected nodes. It handles packaging and unpacking the data in frames. It defines the protocol to establish and terminate a connection between two physically connected devices, such as Point-to-Point Protocol (PPP). The data link layer is generally divided into two sublayers—media access control (MAC) layer and logical link control (LLC) layer. MAC layer is responsible for controlling how devices in a network gain access to a media and permission to transmit data. LLC layer is responsible for identifying and encapsulating network layer protocols, and controls error checking and frame synchronization.

Layer 1: Physical Layer

The physical layer defines the electrical and physical specifications of the data connection. For example, the layout of pins of the connector, the operation voltages of an electrical cable, optical fiber cable specifications, and the frequency for wireless devices. It is responsible for transmission and reception of unstructured raw data in a physical medium. Bit rate control is done at the physical layer. It is the layer of low-level networking equipment and is never concerned with protocols or other higher-layer items.

TCP/IP Model Layers

TCP/IP model is also a layered reference model, but it is a four-layer model. Another name for it is Internet protocol suite. It is commonly known as TCP/IP because the foundational protocols are TCP and IP, but not only these two protocols are used in this model.

Application Layer

The application layer of TCP/IP model provides applications the ability to access to services of the other layers, and defines the protocols that applications use to exchange data. Most widely-known application layer protocols include HTTP, FTP, SMTP, Telnet, DNS, SNMP and Routing Information Protocol (RIP).

Transport Layer

The transport layer, also known as the host-to-host transport layer, is responsible for providing the application layer with session and datagram communication services. The core protocols of this layer are TCP and UDP. TCP provides a one-to-one, connection-oriented, reliable communications service. It is responsible for sequencing and acknowledgment of packets sent, and recovery of packets lost in

transmission. UDP provides one-to-one or one-to-many, connectionless, unreliable communications service. UDP is used typically when the amount of data to be transferred is small (such as that data would fit into a single packet).

Internet Layer

The Internet layer is responsible for host addressing, packaging, and routing functions. The core protocols of the Internet protocol layer are IP, Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) and Internet Group Management Protocol (IGMP). The IP is a routable protocol responsible for IP addressing, routing, and the fragmentation and reassembly of packets. The ARP is responsible for the discovering the network access layer address such as a hardware address associated with a given Internet layer access. The ICMP is responsible for providing diagnostic functions and reporting errors due to the unsuccessful delivery of IP packets. The IGMP is responsible for the management of IP multicast groups. In this layer, the IP adds header to the packets, which is known as IP address. Now there's both IPv4 (32-bit) address and IP Ipv6 (128-bit) address.
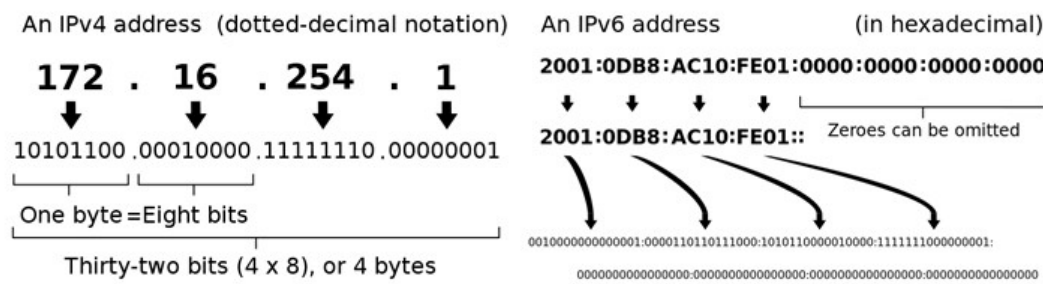

Figure 2: IPv4 address and IPv6 address examples.

Network Access Layer

Network access layer (or link layer) is responsible for placing the TCP/IP packets on the network medium and receiving TCP/IP packets off the network medium. TCP/IP is designed to be independent of the network access method, frame format, and medium. In other word, it is independent from any specific network technology. In this way, TCP/IP can be used to connect different network types, such as Ethernet, Token Ring, X.25, Frame Relay, and Asynchronous Transfer Mode (ATM).

How Is Data Processed During the Transmission?

In a layered system, devices of a layer exchange data in different format, which is known as protocol data unit (PDU). The table below shows the PDUs in different layers.

Table: protocol data unit (PDU) being processed in different layers.

Model Type	OSI Layers	Protocol Data Unit (PDU)	TCP/IP
Host Layers	Application Layer	Data	Applicati

	Presentation Layer		Session
	Session Layer		Applicati
	Transport Layer	Segment (TCP) / Datagram (UDP)	Transpor
	Network Layer	Packet	Internet
Media Layers	Data Link Layer	Frame	Network
	Physical Layer	Bit	

For example, when a user requests to browse a website on the computer, the remote server software firstly gives the requested data to the application layer, where it is processed from layer to layer down with each layer performing its designated functions. The data is then transmitted over the physical layer of the network until the destination server or another device receives it. At this point the data is passed up through the layers again, each layer performing its assigned operations until the data is used by the receiving software.
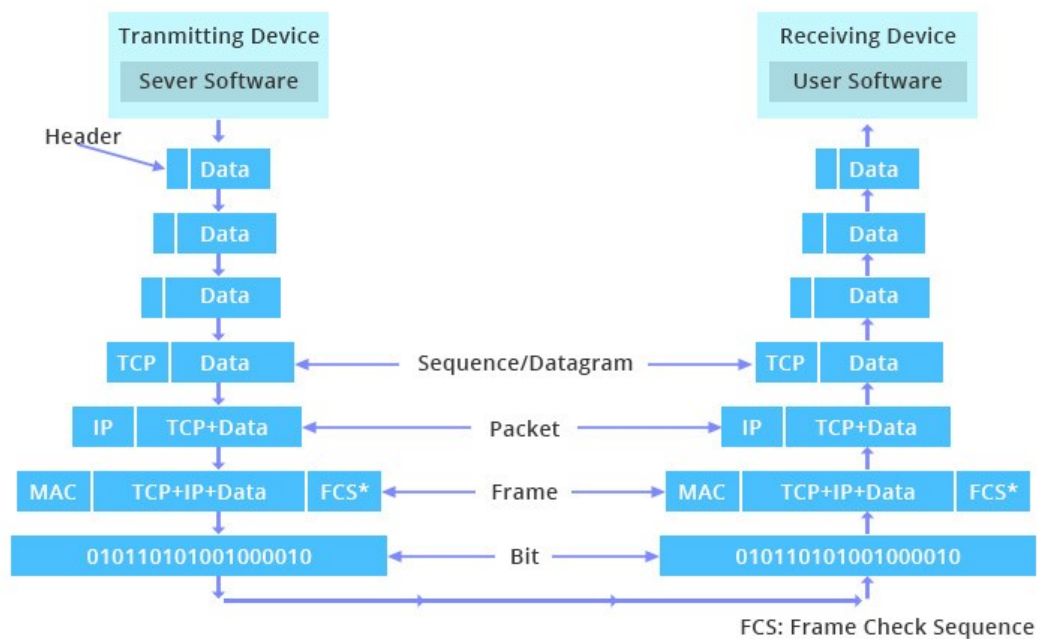

Figure 3: data flows down from upper layers to lower layers, each layer add header/footer to the PDU.

During the transmission, each layer adds a header, or footer, or both to the PDU coming from the upper layer, which directs and identifies the packet. This process is called encapsulation. The header (and footer) and the data together form the PDU for the next layer. The process continues until reaching the lowest-level layer (physical layer or network access layer), from which the data is transmitted to the receiving device. The receiving device reverses the process, de-encapsulating the data at each layer with the header and footer information directing the operations. Then the application finally uses the data. The process is continued until all data is transmitted and received.

The Significance of TCP/IP and OSI to Troubleshooting

With the knowledge of division of layers, we can diagnose where the problem lies when a connection

fails. The principle is to check from the lowest level, rather than from the highest level. Because each layer serves for the layer higher than it, and it will be easier to deal with lower-layer problems. For example, if your computer cannot connect the Internet, the first thing you should do is checking if the network cable is plugged your computer, or if the wireless access point (WAP) is connected to the switch, or if the pins of the RJ45 connectors are in good condition.

TCP/IP Model vs. OSI Model

The TCP/IP model is older than the OSI model. The following figure shows corresponding relationship of their layers.
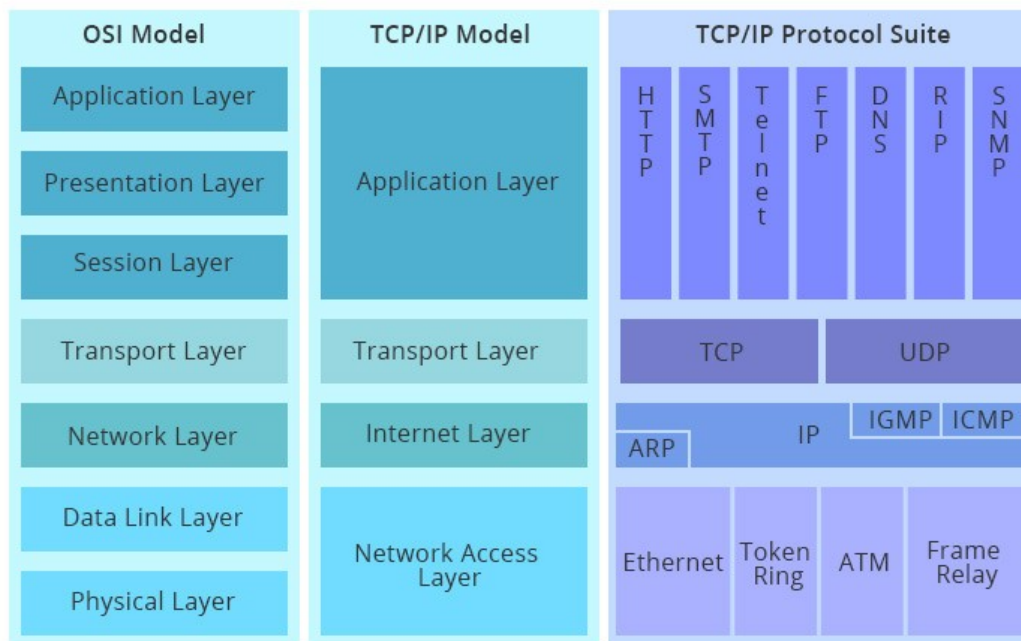

Figure 4: OSI model vs. TCP/IP model, and TCP/IP protocl suite.

Comparing the layers of the TCP/IP model and the OSI model, the application layer of the TCP/IP model is similar to the OSI layers 5, 6, 7 combined, but TCP/IP model does not have a separate presentation layer or session layer. The transport layer of TCP/IP encompasses the responsibilities of the OSI transport layer and some of the responsibilities of the OSI session layer. The network access layer of the TCP/IP model encompasses the data link and physical layers of the OSI model. Note that the Internet layer of TCP/IP does not take advantage of sequencing and acknowledgment services that might be present in the data link layer of OSI model. The responsibility is of the transport layer in TCP/IP model.

Considering the meanings of the two reference models, the OSI model is just a conceptual model. It is mainly used for describing, discussing, and understanding individual network functions. However, TCP/IP is firstly designed to solve a specific set of problems, not to function as a generation description for all network communications as OSI model. OSI model is generic, protocol independent, yet most protocols and systems adhere to it, while TCP/IP model is based on standard protocols which the Internet has developed. Another thing should be noted in OSI model is that not all layers are used in simpler applications. While the layers 1, 2, 3 are mandatory for any data communication, the application may use some unique interface layer to the application instead of the

usual upper layers in the model.

Summary

The TCP/IP model and OSI model are both conceptual models used for description of all network communications, while TCP/IP itself is also an important protocol used in all Internet operations. Generally, when we talk about layer 2, layer 3 or layer 7 in which a network device works, we are referring to the OSI model. The TCP/IP model is used for both modelling current Internet architecture and providing a set of rules that are followed by all forms of transmission over the network.

Related Articles:
Comparison Between Store-and-Forward Switching and Cut-Through Switching
Managed vs Unmanaged Switch: Which One Can Satisfy Your Real Need?