OSI Layer Functions

The following table compares the functions performed at each OSI model layer.

Description	Protocols
Application Layer	
The Application layer integrates network functionality into the host operating system and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network. These services include: ● Interface--provides an interface for a service to operate. ● Communication--enables communication partner identification. ● File services--transferring, storing, and updating shared data. ● Print services--enabling network printers to be shared by multiple users. ● Message services--transferring data in many formats (text, audio, video) from one location to another or from one user to another. ● Application services--sharing application processing throughout the network and enabling specialized network servers to perform processing tasks. ● Database services--storing, retrieving, and coordinating database information throughout the network. Most Application layer protocols operate at multiple layers, down to the Session layers and even Transport layers. They are classified as Application layer protocols because they start at the Application layer (the Application layer is the highest layer where they operate).	● HTTP ● Telnet ● FTP ● TFTP ● SNMP
Presentation Layer	

The Presentation layer formats or presents data into a compatible form for receipt by the Application layer or the destination system. Specifically, the Presentation layer ensures: • Formatting and translation of data between systems. • Negotiation of data transfer syntax between systems by converting character sets to the correct format. • Compatibility with the host. • Encapsulation of data into message envelopes through encryption and compression. • Restoration of data through decryption and decompression.	• JPEG, BMP, TIFF, PICT • MPEG, WMV, AVI • ASCII, EBCDIC • MIDI, WAV
Session Layer	
The Session layer's primary function is managing the sessions in which data is transferred. Functions at this layer may include: • Keeps data streams separate (session identification). • Sets up, maintains, and tears down communication sessions. • Establishment and maintenance of communication sessions between the network hosts, ensuring that data is transported. • Management of multiple sessions (each client connection is called a *session*). A server can maintain thousands of sessions simultaneously. • Assignment of the session ID number to each session, which is then used by the Transport layer to properly route the messages. • Dialog control that specifies how the network devices coordinate with each other (simplex, half-duplex, and full-duplex). • Termination of communication sessions between network hosts after completion of the data transfer. • Coordination of requests and responses between different hosts using the same application.	• Network File System (NFS) • Apple Session Protocol (ASP) • Structured Query Language (SQL) • Remote procedure call (RPC) • X Window

Transport Layer

The Transport layer:

- Enables end-to-end flow control.
- Provides a transition between the upper and lower layers of the OSI model, making the upper and lower layers transparent from each other.
    - Upper layers format and process data without regard for delivery.
    - Lower layers prepare the data for delivery by fragmenting and attaching transport required information.
- Uses port (or socket) numbers to identify distinct applications running on the same system. This allows each host to provide multiple services.
- Receives large packets of information from higher layers and breaks them into smaller packets called segments. Segmentation is necessary to enable the data to meet network size and format restrictions.
- The receiving Transport layer uses packet sequence numbers to reassemble segments into the original message.
- Connection-oriented protocols perform error detection and correction and identify lost packets for retransmission. A connection-oriented protocol is a good choice when:
    - Reliable, error-free communications are more important than speed.
    - Larger chunks of data are being sent.
- Connectionless services assume an existing link between devices and allow transmission without extensive session establishment. Connectionless communications use no error checking, session establishment, or acknowledgements. Connectionless protocols allow quick, efficient communication at the risk of data errors and packet loss. Connectionless protocols are a good choice when:

TCP (connection-oriented)
UDP (connectionless)

Network Layer

The Network layer: • Defines logical addresses (host and network). • Uses path determination (identification and selection). • Routes packets. • Describes how data is routed across networks and to the destination. • Maintains addresses of neighboring routers. • Maintains a list of known networks. • Determines the next network point to which data should be sent. Routers use a routing protocol to take into account various factors, such as the number of hops in the path, link speed, and link reliability to select the optimal path for data. Packets forwarded from the Transport layer to the Network layer become datagrams, and network-specific (routing) information is added. Network layer protocols then ensure that the data arrives at the intended destinations.	• IP • AppleTalk
Data Link Layer	
The Data Link layer: • Converts bits into bytes and bytes into frames. • Uses MAC address (also called the burned in address or hardware address). • Defines the logical network topology. • Specifies media access methods. • Implements host-to-host flow control. • Uses parity and CRC.	LAN protocols: • 802.2 (LLC), 802.3 (Ethernet • 802.11 (Wireless) WAN protocols: • PPP • MLPPP • ISDN

The Logical Link Control (LLC) layer provides an interface between the MAC layer and upper-layer protocols. LLC protocols are defined by the IEEE 802.2 committee. The LLC sub-layer is responsible for:

- Maintaining orderly delivery of frames through sequencing.
- Controlling the flow or rate of transmissions using:
    - Acknowledgments
    - Buffering
    - Windowing
- Ensuring error-free reception of messages by retransmitting.
- Converting data into an acceptable form for the upper layers.
- Removing framing information from the packet and forwarding the message to the Network layer.
- Providing a way for upper layers of the OSI model to use any MAC layer protocol.
- Defining Service Access Points (SAPs) by tracking and managing different protocols.

The Media Access Control (MAC) layer defines specifications for controlling access to the media. The MAC sub-layer is responsible for:

- Adding frame start and stop information to the packet.
- Adding Cyclical Redundancy Check (CRC) for error checking.
- Converting frames into bits to be sent across the network.
- Identifying network devices and network topologies in preparation for media transmission.
- Defining an address (such as the MAC address) for each physical device on the network.
- Controlling access to the transmission medium.

Physical Layer

The Physical layer: • Moves bits across the media. • Defines cables, connectors, and pin positions. • Specifies electrical signals (voltage, bit synchronization). • Defines the physical topology (network layout). • Sets standards for sending and receiving electrical signals between devices. It describes how digital data (bits) are converted to electric pulses, radio waves, or pulses of lights. Devices that operate at the physical layer send and receive a stream of bits.	• EIA/TIA 232 (serial signaling) • V.35 (modem signaling) • Cat6 • RJ45

OSI Networking Model

Open Systems Interconnection model, or OSI model

7 - Application
6 - Presentation
5 - Session
4 - Transport
3 - Network
2 - Data Link
1 - Physical

APSTNDP

“All People Seem To Need Data Processing”

Presentation

The Presentation layer's primary purpose is to format data. The data you see on screen isn't how data on computer systems is stored and sent. The data is converted into a binary format. For example, the capital letter A is going to be encapsulated into a binary format of 1s and 0s.

Session

The session layer is used for session management, or to keep track of different connections that a particular system might maintain. For example, on a file server, you may have several hundred

users all logged in, accessing that server at the same time. The server has to keep track of requests coming in and out. It needs to know exactly who it's working for at the moment. That's called session management.

Data Link

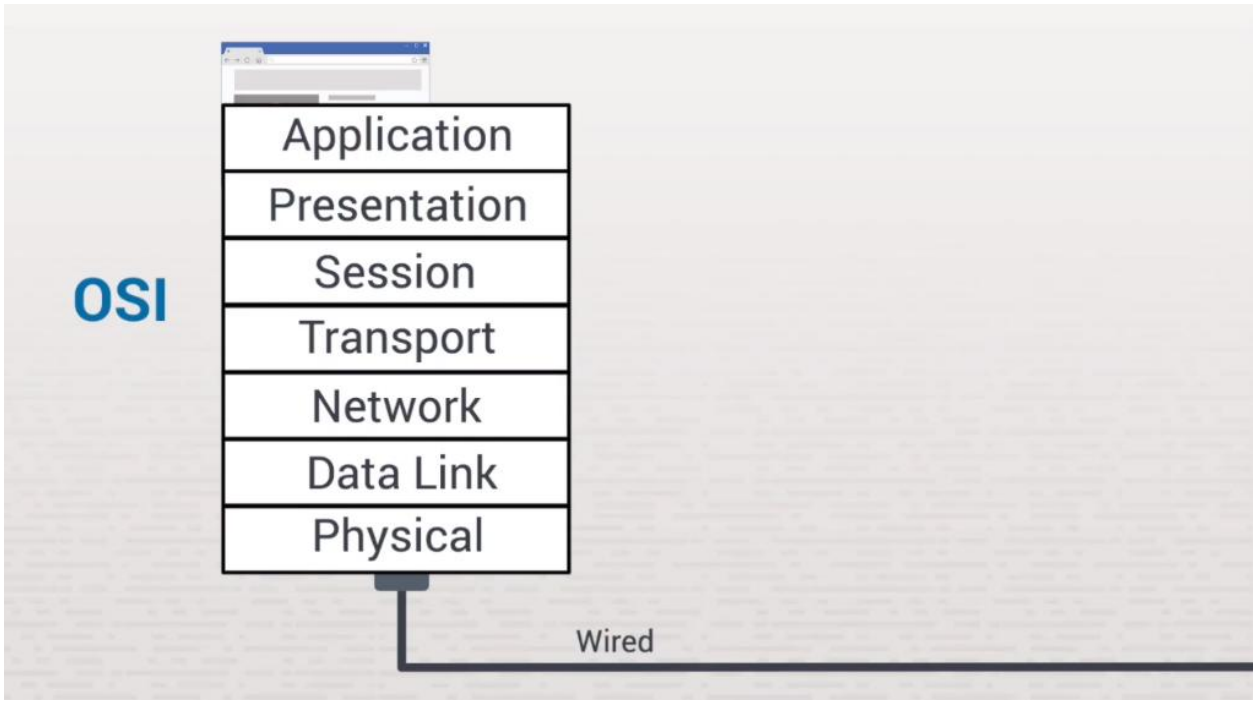
The Data Link layer is responsible for physical addressing. It can also be called MAC addressing, which stands for Media Access Control addressing. Every network system has a MAC address that identifies the network connection (or the physical card or port) that it connects to.

If you have an Ethernet port in your workstation, it has a burnt-in MAC address. It's a 6-byte address that's specific to that card throughout the whole network. It's burnt into the card from the factory it came from. You can see that every system on the network has both a logical address (an IP address) and a physical address (a MAC address) burnt into its network card. All these addresses are used by network devices to figure out how to move data to and from that device around the network.

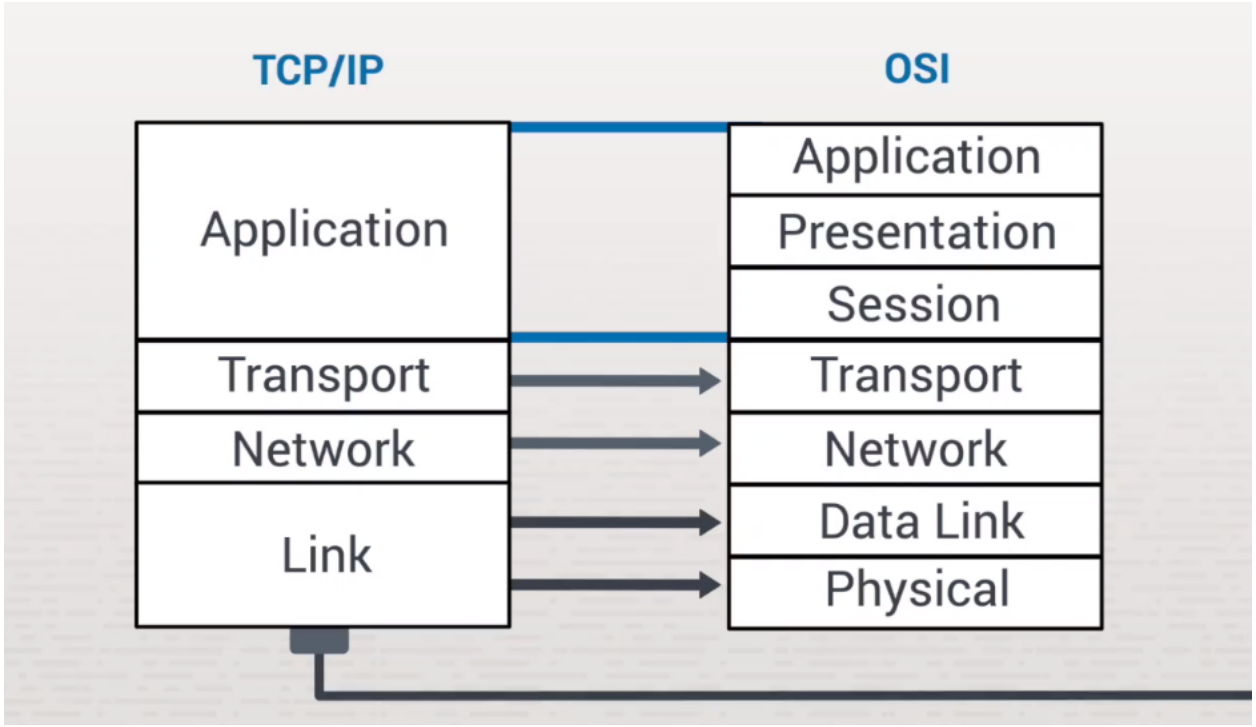
Once the Data Link layer has added its information to the data, it creates what's called a frame. As data continues to be encapsulated from layer to layer, packets become frames. Frames have to be physically transmitted as electrical signals on wired systems or as radio frequencies for wireless connections.

Physical

By the time it gets to the Physical layer, data is simply referred to as bits. The purpose of the bottom layer is to physically transmit these bits, which exist as information passed on to the frame. So it transmits everything that was converted into 1s and 0s onto a wired system or wireless network. The packets are encapsulated within frames and sent to the network as bits of data.



OSI Comparison to TCP/IP



Comparing osi model to TCP/IP
Note: TCP/IP is industry standard

OSI Model Facts

The OSI model classifies and organizes the tasks that hosts perform to prepare data for transport across the network. You should be familiar with the OSI model because it is the most widely used method for understanding and talking about network communications. However, remember that it is only a theoretical model that defines standards for programmers and network administrators. It is not a model of actual physical layers.

The OSI model is useful when discussing networking concepts. It is useful because the OSI Model:

- Provides a common language or reference point between network professionals.
- Divides networking tasks into logical layers for easier comprehension.
- Allows specialization of features at different levels.
- Aids in troubleshooting.
- Promotes standards and interoperability between networks and devices.
- Provides modularity in networking features. Developers can change features without changing the entire approach.

Remember the following limitations of the OSI model:

- OSI layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the OSI layers.
- Different protocols within the stack perform different functions that help send or receive the overall message.
- A particular protocol implementation may not represent every OSI layer, or may spread across multiple layers.

Network Applications

Not a complete list, but the popular ones.

Application	Function	TCP/IP Protocol	Port
HTTP	Browse web content	TCP	80
HTTPS	Secure web traffic	TCP	443
SMTP	Send email	TCP	25
POP3	Send email	TCP	110
FTP	Transfer file content	TCP	20, 21
TFTP	Transfer file content	UDP	69
Telnet	Connect remote devices	TCP	23
SSH	Connect remote devices	TCP	22
SNMP	Gather information and manage devices	UDP	161
DNS	Translate between host addresses and IP addresses	TCP, UDP	53
DHCP	Deliver IP configurations	UDP	67, 68

TCP/IP Protocol Suite Facts

The TCP/IP protocol suite was developed to work independently of the Physical layer implementation. You can use a wide variety of architectures with the TCP/IP protocol suite. The following table lists several protocols in the TCP/IP protocol suite:

Protocol	Description	OSI Model Layer(s)	TCP/IP Model Layer

File Transfer Protocol (FTP)	FTP provides a generic method of transferring files. It can include file security through user names and passwords. It allows file transfer between dissimilar computer systems.	Application, Presentation, Session	Application/Process
Trivial File Transfer Protocol (TFTP)	TFTP is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and uses UDP instead of TCP as the transport protocol.	Application, Presentation, Session	Application/Process
Hypertext Transfer Protocol (HTTP)	HTTP is used by web browsers and web servers to exchange files, such as web pages, through the World Wide Web and intranets. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send web documents but is also used as the protocol for communication between agents using different TCP/IP protocols.	Application, Presentation, Session	Application/Process
Simple Mail Transfer Protocol (SMTP)	SMTP is used to route electronic mail through the internetwork. E-mail applications provide the interface to communicate with SMTP or mail servers.	Application, Presentation, Session	Application/Process

Simple Network Management Protocol (SNMP)	SNMP is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.	Application, Presentation, Session	Application/Process
Remote Terminal Emulation (Telnet)	Telnet allows an attached computer to act as a dumb terminal, with data processing taking place on the TCP/IP host computer. It is still widely used to provide connectivity between dissimilar systems.	Application, Presentation, Session	Application/Process
Network File System (NFS)	NFS was initially developed by Sun Microsystems. It consists of several protocols that enable users on various platforms to seamlessly access files from remote file systems.	Application, Presentation, Session	Application/Process
Voice over Internet Protocol (VoIP)	VoIP is a protocol optimized for the transmission of voice through the internet or other packet switched networks. Voice over IP protocols carry telephony signals as digital audio encapsulated in a data packet stream over IP.	Application, Presentation, Session	Application/Process
Domain Name System (DNS)	DNS is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name www.testout.com would be	Application, Presentation, Session	Application/Process

	identified with a specific IP address.		
Transmission Control Protocol (TCP)	TCP provides connection-oriented services and performs segment sequencing and service addressing. It also performs important error-checking functions.	Transport	Host-to-Host (Transport)
User Datagram Protocol (UDP)	UDP is considered a host-to-host protocol like TCP but is not connection-oriented. Because of less overhead, UDP transfers data faster but is not as reliable.	Transport	Host-to-Host (Transport)
Internet Protocol (IP)	IP is the main TCP/IP protocol. It is a connectionless protocol that makes routing path decisions based on the information it receives from ARP. It also handles logical addressing issues through the use of IP addresses.	Network	Internet
Internet Control Message Protocol (ICMP)	ICMP works closely with IP in providing error and control information that helps move data packets through the internetwork.	Network	Internet
Internet Group Membership Protocol (IGMP)	IGMP is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or	Network	Internet

	across networks (connected with a router).		
Address Resolution Protocol (ARP)	ARP is used to get the MAC address of a host from a known IP address. ARP is used within a subnet to get the MAC address of a device on the same subnet as the requesting device.	Network	Internet
Reverse Address Resolution Protocol (RARP) and Bootstrap Protocol (BOOTP)	Both BOOTP and RARP are used to discover the IP address of a device with a known MAC address. BOOTP is an enhancement to RARP and is more commonly implemented than RARP. As its name implies, BOOTP is used by computers as they boot to receive an IP address from a BOOTP server. The BOOTP address request packet sent by the host is answered by the server.	Network	Internet
Dynamic Host Configuration Protocol (DHCP)	DHCP simplifies address administration. DHCP servers maintain a list of available and assigned addresses and communicate configuration information to requesting hosts. DHCP has the following two components: ● A protocol for delivering IP configuration parameters from a DHCP server to a host.	Network	Internet

	• A protocol specifying how IP addresses are assigned.		
Open Shortest Path First (OSPF)	OSPF is a route discovery protocol that uses the link-state method. It is more efficient than RIP in updating routing tables, especially on large networks.	Network	Internet
Routing Information Protocol (RIP)	RIP is a route discovery protocol that uses the distance-vector method. If the network is large and complex, OSPF should be used instead of RIP.	Network	Internet