OSI Reference Model

The OSI stand for **Open System Interconnection**

It was first introduced in the late 1970s by the ISO (**International d Organization for Standardization**).

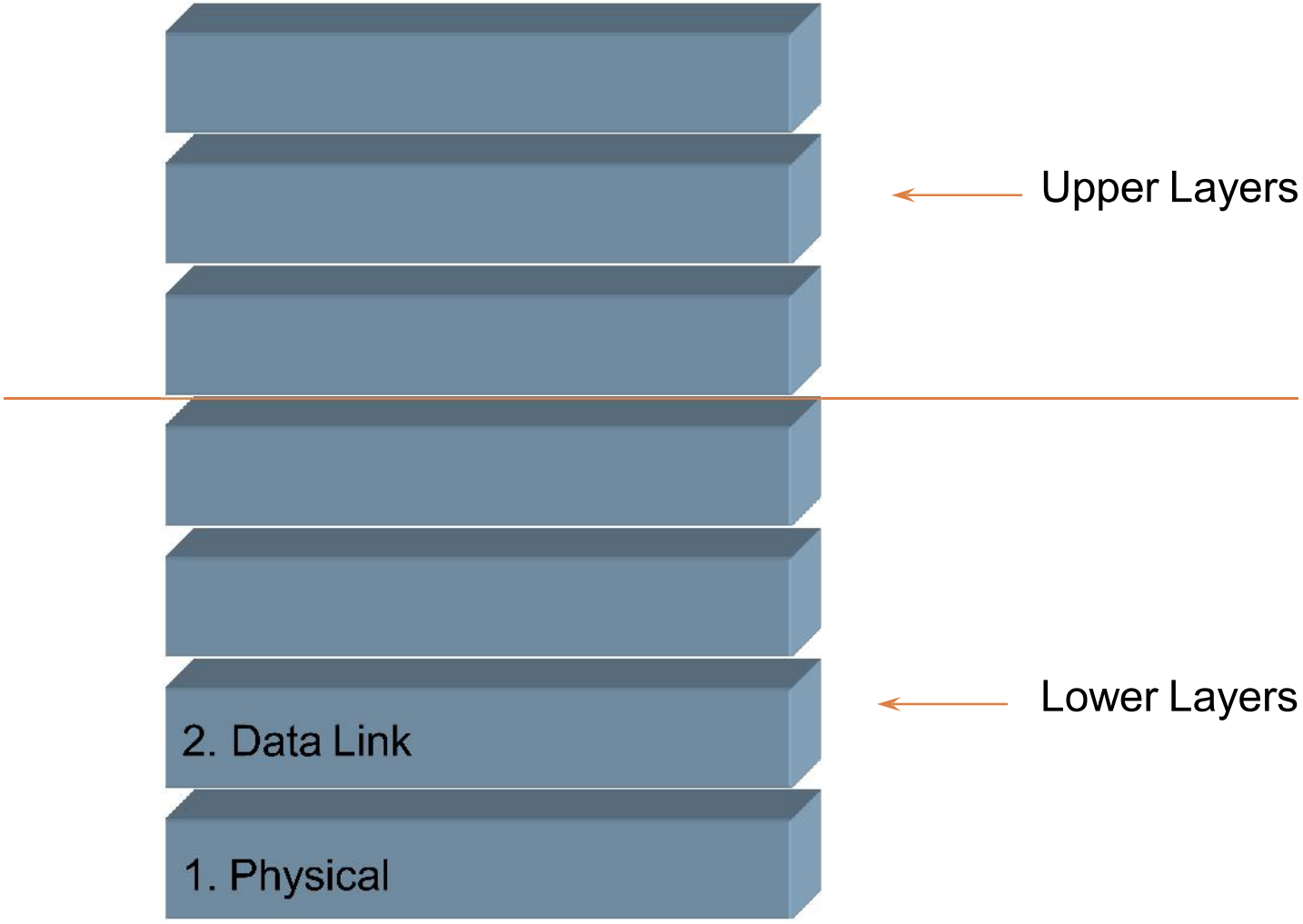
An OSI is a set of protocols that allow any two different system to communicate regardless of their underlying architecture.

The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and inter-operable.

It consists of seven separate but related layers, each of which defines a part of the process of moving information across network.

The Layered Approach to Communication

Division of Layers



OSI Reference Model

- Upper Layer (Application Layer):
  - This part consist three top layer as: Application layer, Presentation layer, Session layer.
  - These layers provide the application services required for the exchange of information.
- Lower Layer (Data Transport):
  - These layer consist remaining four layers as: Physical layer, Data link, Network layer, Transport layer.
  - These layers handle the data transport issues.
  - In other word these layers provides the end-to-end service necessary for the transfer of data between two system.

Physical Layer

- The data units on this layer are called bits.
- Responsible for physical connection between devices
- Movements of individual bits from one node to next
- Repeaters & Hub are used in physical layer.
- Functions:
  - Converts bits into signals
  - Bit Synchronization
  - Manage physical connection
  - Bit rate control
  - Line configuration
  - Physical topology
  - Transmission mode
  - Multiplexing
  - Switching

Date Link Layer (DLL)

- The data unit on this layer is called frame (Group of bits)
- This layer divided into two sub layers:
  - Media Access Control (MAC)
    - The MAC sub-layer controls how a computer on the network gains access to link resources and grant permission to transmit it.
  - Logical Link Control (LLC)
    - The LLC layer controls frame synchronization flow control and error checking.
- DLL taks:
  - Framing
  - Physical Addressing
  - Error Control
- Bridge used in DLL.

Network Layer

- The unit of data at network layer is called packet or Data-gram.
- Network layer is responsible for providing logical address known as IP address. Router works on this layer. Main functions of this layer are following:-
- Define IP address
- Find routes based on IP address to reach its destination
- Connect different data link type together like as Token Ring, Serial, FDDI, Ethernet etc.
- Router used in network layer.
- Functions:
  - Logical Addressing
  - Routing

IP address

- IP address a 32 bit long software address which made from two components:
- **Network component: -** Defines network segment of device.
- **Host component :-** Defines the specific device on a particular network segment
- Subnet mask is used to distinguish between network component and host component.
- IP addresses are divided in five classes.
  - Class **A** addresses range from **1-126**.
  - Class **B** addresses range from **128-191**.
  - Class **C** addresses range from **192-223**.
  - Class **D** addresses range from **224-239**.
  - Class **E** addresses range from **240-254**.
- **Following addresses have special purpose: -**
- **0 [*Zero*]** is reserved and represents all IP addresses;
- **127** is a reserved address and it is used for testing, like a loop back on an interface:
- **255** is a reserved address and it is used for broadcasting purposes.

Transport Layer

- Provides reliable end-to-end delivery of the transmission.
- Connection-less service uses UDP protocol; Connection-oriented service uses TCP protocol.
- For a reliable connection, sequence numbers and acknowledgments (ACKs) are used.
- Reliable connection controls flow through the uses of windowing or acknowledgements.
- In this layer data unit called segment.
- Gateway devices used in transport layer.

- **Functions:**
  - **Segmentation and Reassembly**
  - **Connection Management**
  - **Reliable and Unreliable data delivery**
  - **Flow Control**
  - **Connection Multiplexing**

Segmentation

- Segmentation is the process of breaking large data file into smaller files that can be accommodate/supported by network.
- To understand this process think about a 700 MB movie that you want to download from internet. You have 2MBPS internet connection. How will you download a 700MB movie on 2MBPS internet connection?

ANSWER:

- In this case segmentation process is used.
- On server, transport layer breaks 700MB movie in smaller size of segments (less than your internet connection speed). Assume that 700Mb movie is divided in 700 segments. Each segment has file size of 1Mb that your PC can easily download at current connection speed. Now your PC will download 700 small files instead of one large file. So next time when you see download progress bar in browser, think it about segment receiver progress bar. Once your browser receives all segments from server, it will pop up a message indicating download is completed. Transport layer at your PC will merge all segments back in a single 700Mb movie file. End user will never know how a 700Mb movie makes its way through the 2Mbps connection line.

Reliability

- Reliability means guaranteed data delivery.

- To insure delivery of each single segment, connection oriented method is used.
- In this approach before sending any segments three way handshake process is done.

Three way handshake process

Three way handshake process

1) PC1 sends a SYN signal to PC2 indicating that it wants to establish a reliable session.
2) P2 replies with ACK/SYN signal where ACK is the acknowledgment of PC1's SYN
   signal and SYN indicates that PC2 is ready to establish a reliable session.
3) PC1 replies with ACK signal indicating that is has received SYN signal and session is now fully established.

Once connection is established data transmission will be initiated. To provide maximum reliability it includes following functions:-

- Detect lost packets and resend them
- Detect packets that arrived out of order and reorder them
- Recognize duplicate packets and drop extra packets
- Avoid congestion by implementing flow control

Flow control

- The transport layer implements two flow control methods:
- Ready/not ready signals
- Windowing

Ready / not ready signals method

- In this method sender sends data according to its buffer size. Receiver receives data in its buffer. When receivers buffer get filled, it send a not ready signal to sender, so sender can stop transmitting more segments. Receivers send ready signal when it becomes ready to receive next segments. This method has two problems.
- First, the receiver may respond to the sender with a not ready signal only when its buffer fills up. While this message is on its way to the sender, the sender is still sending segments to the receiver, which the receiver will have to drop because its buffer space is full.
- The second problem with the uses of this method is that once the receiver is ready to receive more segments, it must first send a ready signal to the sender, which must be received before sender can send more segments.

Windowing

- In windowing a window size is defined between sender and receiver. Sender host will wait for an acknowledgement signal after sending the segments equal to the window size. If any packet lost in the way, receiver will respond with acknowledgement for lost packet. Sender will send lost packet again. Window size is automatically set during the three step handshake process. It can be adjust anytime throughout the lifetime of connection.

Connection Multiplexing/Application Mapping

- Connection multiplexing feature allows multiple applications to connect at a time.
- For example a server performs a number of functions like email, FTP,DNS, Web service, file service, data service etc.

- Suppose server has a single IP address, how will it perform all these different functions for all the hosts that want to connect with it?

ANSWER:

To make this possible transport layer assigns a unique set of numbers for each connection. These numbers are called port or socket numbers. These port numbers allow multiple applications to send and receive data simultaneously.

- **Port numbers are divided into following ranges by the IANA**
- 0–1023 [Well-Known]—For common TCP/IP functions and applications
- 1024–49151[Registered]—For applications built by companies
- 49152–65535 [Dynamic/Private]—For dynamic connections or unregistered applications

Common TCP and UDP Port Numbers

TCP	UDP
FTP – 20,21	DNS-53
Telnet-23	DHCP-67,68
SMTP-25	TFTP-69
DNS-53	NTP-123
HTTP-80	SNMP-161
POP-110	
HTTPS-443	

Session Layer

- Session layer deals with connections.
- It establishes, manages, and terminates sessions between two communicating nodes.
- This layer provides its services to the presentation layer.
- Session layer also synchronizes dialogue between the presentation layers of the two hosts and manages their data exchange.
- For example, web servers may have many users communicating with server at a given time. Therefore, keeping track of which user communicates on which path is important and session layer handle this responsibility accurately.
- The session layer responsible for following:
  - Dialog Controller
  - Synchronization
  - Translation

Presentation Layer

- Presentation layer prepares the data.
- It takes data from application layer and marks it with formatting code such as .doc, .jpg, .txt, .avi etc.
- These file extensions make it easy to realize that particular file is formatted with particular type of application.
- With formatting presentation layer also deals with compression and encapsulation.
- It compresses (on sending computer) and decompresses (on receiving computer) the data file.

Tasks:

- Data Translation/ Formatting
- Compression/Decompression
- Encryption/Decryption

Application Layer

- This layer provides platform to send and receive data over the network. All network applications and utilities that communicate with network fall in this layer. For examples:
  - **Browsers :-** Mozilla Firefox, Internet Explorer, Google Chrome etc
  - **Email clients: -** Outlook Express, Mozilla Thunderbird etc.
  - **FTP clients :-** Filezilla, sFTP,vsFTP
- **Application layer protocols :**
  - **SNMP (*Simple Network Management Protocol*)** — Used to control the connected networking devices.
  - **TFTP (*Trivial File Transfer Protocol*)** — Used to transfer the files rapidly.
  - **DNS (*Domain Naming System*)** — Used to translate the name with IP address and vice versa.
  - **DHCP (*Dynamic Host Configuration Protocol*)** — Used to assign IP address and DNS information automatically to hosts.
  - **Telnet** — used to connect remote devices.
  - **HTTP (*Hypertext Transfer Protocol*)** — Used to browse web pages.
  - **FTP (*File Transfer Protocol*)** — Used to reliably sends/retrieves files.
  - **SMTP (*Simple Mail Transfer Protocol*)** — Used to sends email.
  - **POP3 (*Post office proocol*):- *Used to retrieve email.***
  - **NTP (*Network Time Protocol*)** — Used to synchronizes clocks.

Data Exchange Process

On sending computer

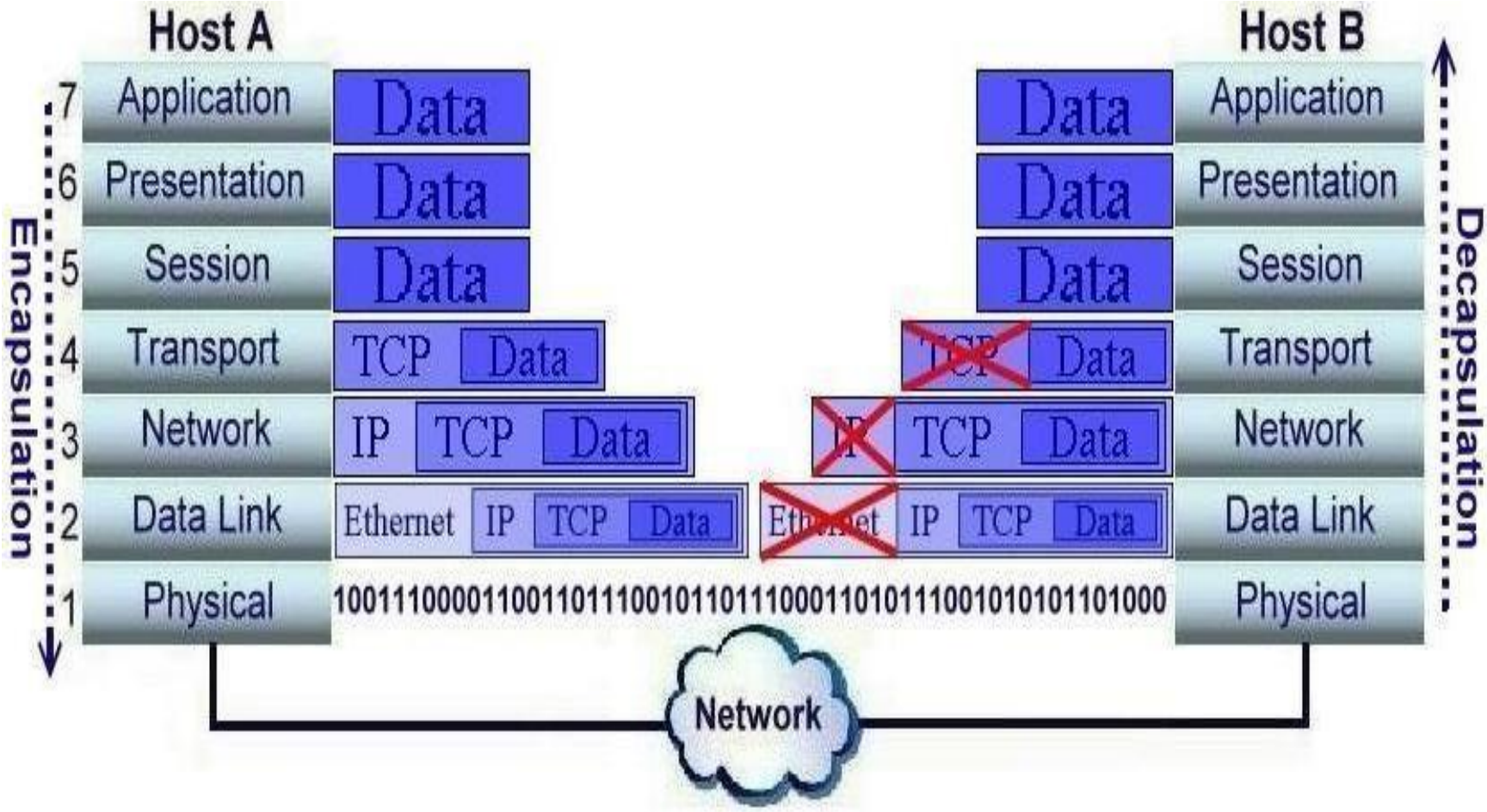
- Sending application access the application layer.
- Application provides data to the presentation layer.
- Presentation layer format the data as per network requirement and forward it's to session layer.
- Session layer initiate the connection and forward the data to the transport layer.
- Transport layer broke down the large data file in smaller segments and add a header with control information, which are bits designated to describe how to determine whether the data is complete, uncorrupted, in the correct sequence, and so forth.
- Segments are forwarded to the network layer. Network layer add its header, with logical address and convert it in packet. Network layer forwards packet to data link layer.
- Data link layer attach its header and footer to the packet and convert it in frame.
- Frames are forwarded to the physical layers that convert them in signals. These signals are loaded in media.

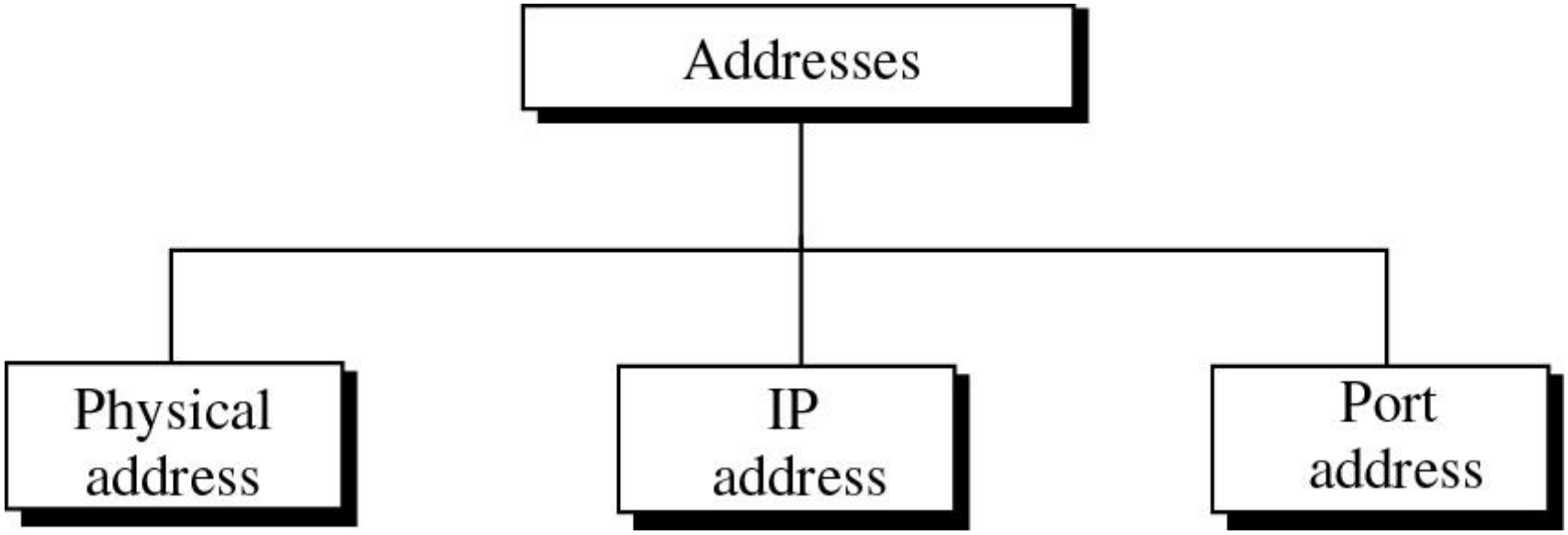
Data Exchange Process

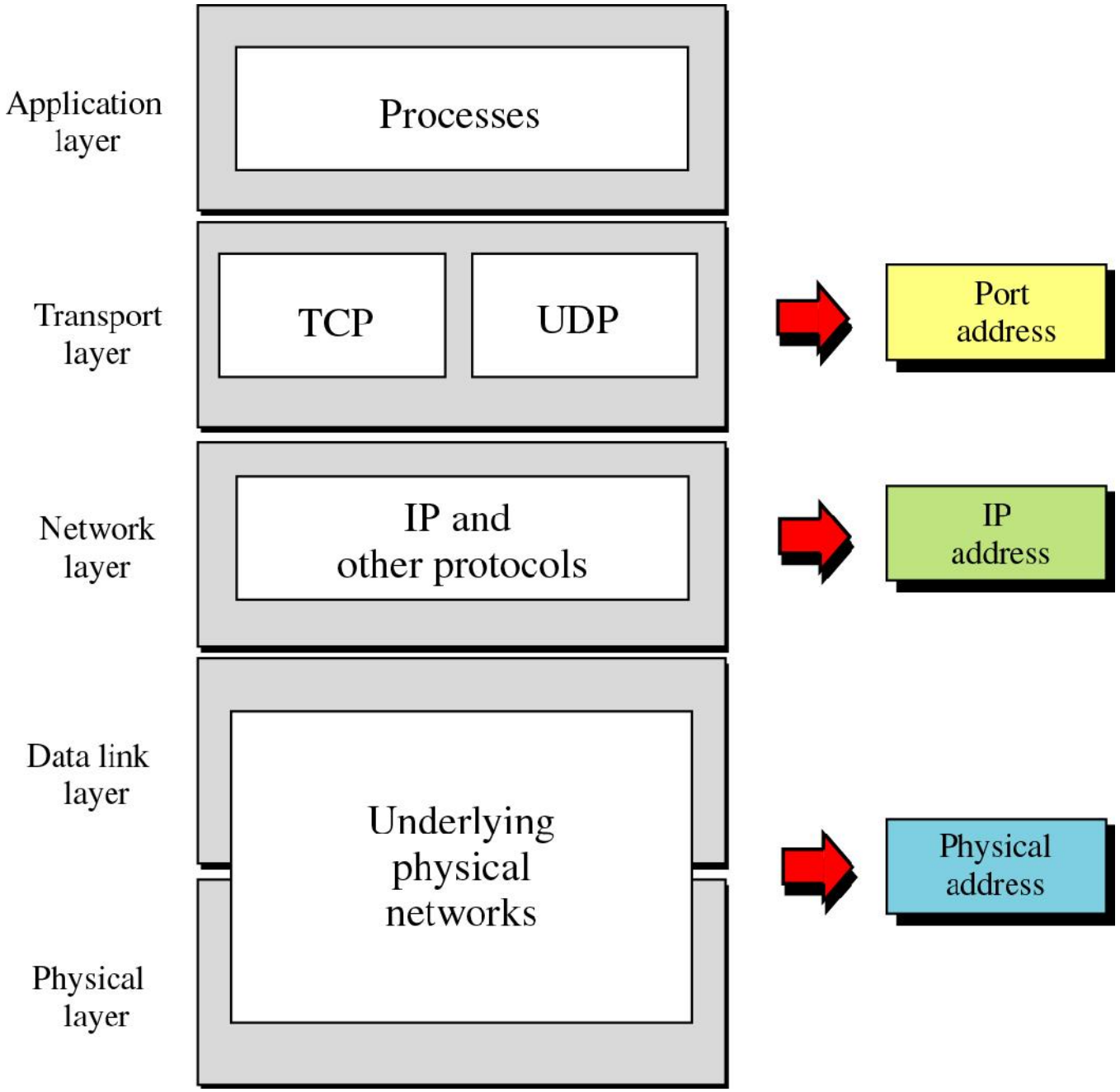
On receiving computer:

- Physical layer receive signals from media and convert them in frames. Frames are forwarded to the data link layer.
- Data link layer check the frame. All tampered frame are dropped here. If frame is correct, data link layer strip down its header and footer from frame and hand over packet to network layer.
- Network layer check the packet with its own implementations. If it's found everything fine with packet, it strips down its header from packet and hand over segment to transport layer.
- Transport layer again do the same job. It verifies the segments with its own protocol rules. Only the verified segments are processed. Transport layer remove its header from verified segments and reassemble the segments in data. Data is handed over the session layer.
- Session layer keep track of open connection and forwarded the receiving data to presentation layer.
- Presentation form the data in such a way that application layer use it.
- Application layer on receiving computer find the appropriate application from the computer and open data within particular application.

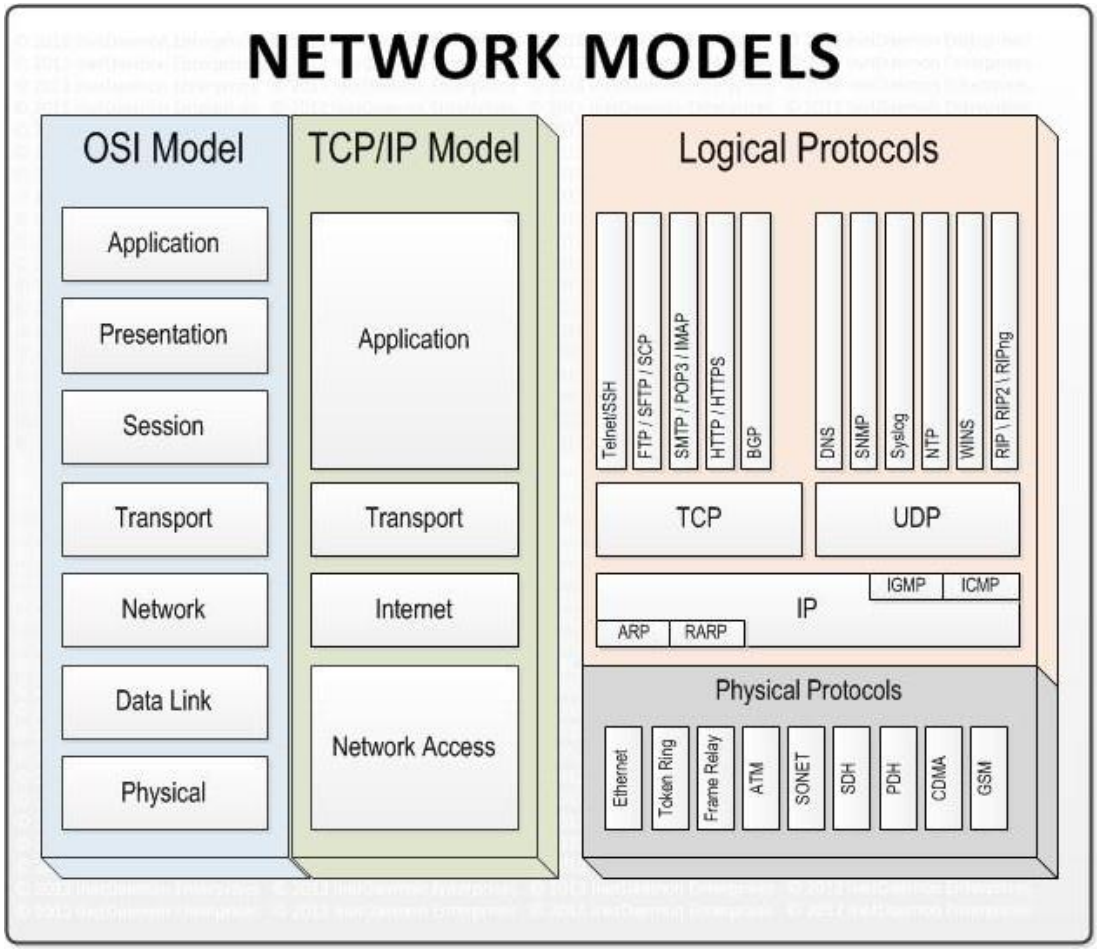
Encapsulation and Decapsulation Process




Addresses
Physical address
IP address
Port address


Application layer
Processes
Transport layer
TCP
UDP
Port address
Network layer
IP and other protocols
IP address
Data link layer
Underlying physical networks
Physical address
Physical layer

OSI vs. TCP/IP


NETWORK MODELS
OSI Model
Application
Presentation
Session
Transport
Network
Data Link
Physical
TCP/IP Model
Application
Transport
Internet
Network Access
Logical Protocols
Telnet/SSH
FTP / SFTP / SCP
SMTP / POP3 / IMAP
HTTP / HTTPS
BGP
DNS
SNMP
Syslog
NTP
WINS
RIP \ RIP2 \ RIPng
TCP
UDP
IGMP
ICMP
IP
ARP
RARP
Physical Protocols
Ethernet
Token Ring
Frame Relay
ATM
SONET
SDH
PDH
CDMA
GSM

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
Follows vertical approach.	Follows horizontal approach.
OSI model has a separate Presentation layer and Session layer.	TCP/IP does not have a separate Presentation layer or Session layer.
OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	TCP/IP model is, in a way implementation of the OSI model.
Transport layer of OSI model provides both connection oriented and connectionless service.	The Transport layer in TCP/IP model provides connectionless service.
OSI model has a problem of fitting the protocols into the model.	TCP/IP model does not fit any protocol
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
It has 7 layers	It has 4 layers