



Data Communication & Networking

Trainer : Sujata Mohite

Email: sujata.mohite@sunbeaminfo.com



Addressing



Addressing



Physical Address/ Link Address

- For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Logical Address

- logical address in the Internet is currently a **32-bit address** that can uniquely define a host connected to the Internet. IP address

Port Address

- computer A can communicate with computer C by using TELNET(login into a remote computer). At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).

Specific Addresses

- Examples include the e-mail address and any Universal Resource Locator (URL)



MAC Address / Physical Address/ Ethernet Address

- used on data link layer
- used to identify every NIC uniquely
- is burnt into the ROM part of NIC once written the MAC address can not be changed
- also known as read only address
- to find the MAC address of NIC
 - windows: ipconfig /all
 - linux/macOS: ifconfig
- e.g. 78 : 4f : 43 : 90 : 13 : d0
- size: 6 bytes = 8 x 6 = 48 bits
- Group of first three bytes(78 : 4f : 43) represent's manufacturer ID and last 3 bytes (90 : 13 : d0) represents NIC's unique address.
- to find the manufacturer, please visit <https://hwaddress.com/>



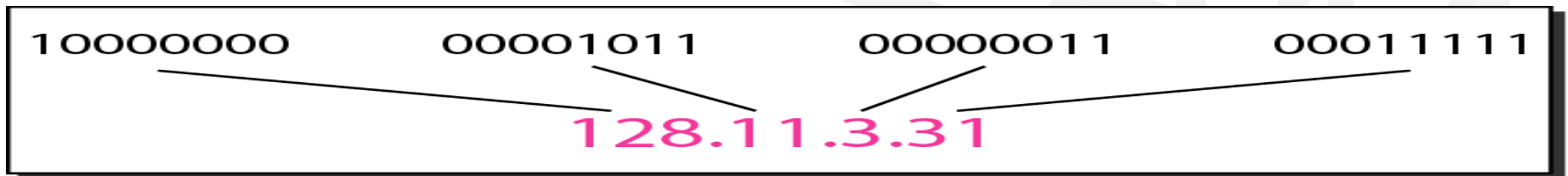
IP Address / Logical Address

- IP address to mean a logical address in the network layer of the TCP/IP protocol suite.
- Identify a machine / device uniquely.
- Size = 4 bytes = 32 bits
- to find the IP address of Machine
 - windows: ipconfig
 - linux/macOS: ifconfig
- IP Versions:
 - IPV4 (32 bits address length)
 - IPV6 (128 bits address length)
- IP addresses are made up of four sets of numbers called **"Octets"**.
- Types
 - Private : used to identify a machine on the LAN and can not be used to connect to internet
 - Public : used to connect to the internet
- e.g.
 - decimal: 192.168.1.6
 - binary : 11000000.10101000.00000001.00000110



IP Addressing Types

- Classful : IP Address is split into 5 classes
- Classless
- IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion)
- **There are two prevalent notations to show an IPv4 address:**
 - binary notation
 - dotted decimal notation



Example

- *Find the error, if any, in the following IPv4 addresses.*

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67



Example

- *Find the error, if any, in the following IPv4 addresses.*

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

- a. There must be no leading zero (045).*
- b. There can be no more than four numbers.*
- c. Each number needs to be less than or equal to 255.*
- d. A mixture of binary notation and dotted-decimal notation is not allowed.*



Classful Addressing

- IP is 32 bit means 2^{32} IP Addresses. (more than 4 billion , so many IP Addresses)
- We need to distribute those that's why we have classes.
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191			
Class C	192–223			
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

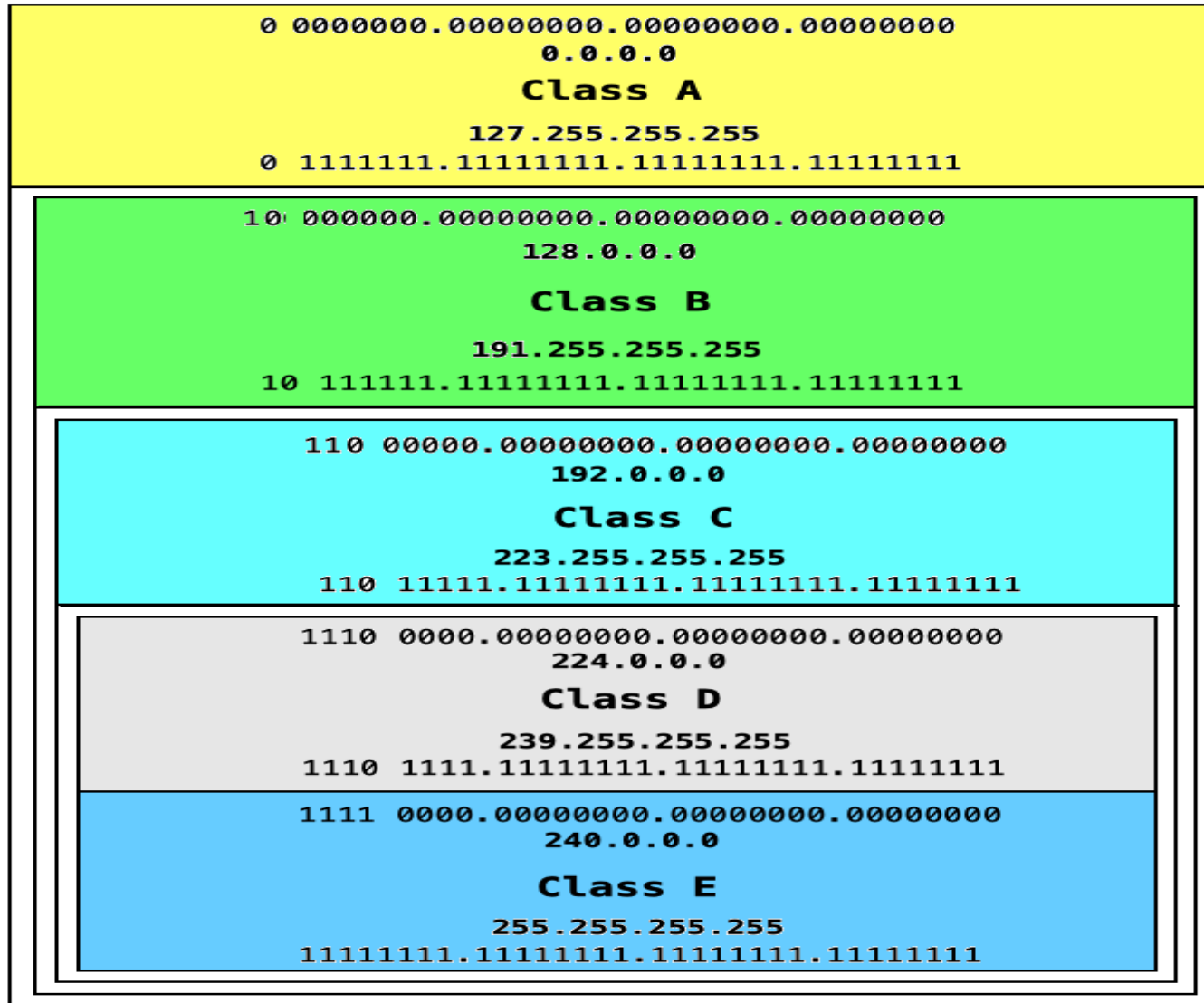


How range of IP Address is defined

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0		
128	64	32	16	8	4	2	1		Range
0	x	x	x	x	x	x	x	Class A	0-127
1	0	x	x	x	x	x	x	Class B	128-191
1	1	0	x	x	x	x	x	Class C	192-223
1	1	1	0	x	x	x	x	Class D	224-239
1	1	1	1	x	x	x	x	Class E	240-255



IP Classful Addressing



- IP addresses starting with 0
- 0.0.0.0 - 127.255.255.255

- IP addresses starting with 10
- 128.0.0.0 - 191.255.255.255

- IP addresses starting with 110
- 192.0.0.0 - 223.255.255.255

- IP addresses starting with 1110
- 224.0.0.0 - 239.255.255.255

- IP addresses starting with 1111
- 240.0.0.0 - 255.255.255.255



Example

- Find the class of each address.
 1. 00000001 00001011 00001011 11101111
 2. 11000001 10000011 00011011 11111111
 3. 14.23.120.8
 4. 252.5.15.111



Example

- Find the class of each address.
 1. 00000001 00001011 00001011 11101111
 2. 11000001 10000011 00011011 11111111
 3. 14.23.120.8
 4. 252.5.15.111

Solution

1. The first bit is 0. This is a class A address.
2. The first 2 bits are 1; the third bit is 0. This is a class C address.
3. The first byte is 14 (between 0 and 127); the class is A.
4. The first byte is 252 (between 240 and 255); the class is E.



Points to be noted

- Any IP Address start with 127, That is : 127.x.x.x means its **a loop back series** that is used for **self testing**.
- E.g. Ping 127.0.0.1 (ping to yourself)
- That is 127.0.0.1 is **Universal IP** ,
- We can not configure **universal IP**. Its by default configured.
- PING (Packet Internet Groper) is a tool used to troubleshoot networking issues .

IANA(Inter Associated Number Association) manages private IP's.

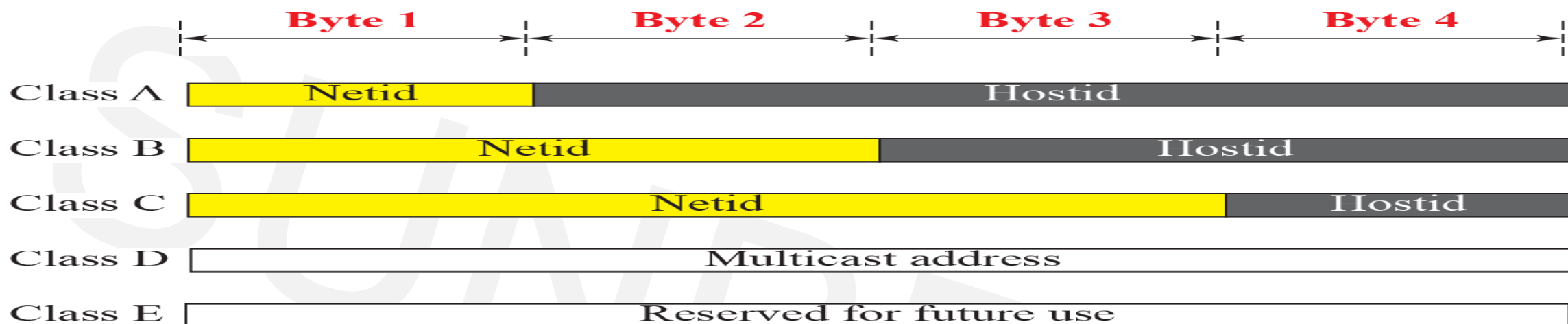
Regular Private IP Addresses

Address Class	Reserved Private IP Addresses
Class A	10.0.0.0 - 10.255.255.255
Class B	172.16.0.0 - 172.31.255.255
Class C	192.168.0.0 - 192.168.255.255

Private network will have private IP's means devices that we connect to our router will get private IP addresses provided by IANA.



Netid and hostid of A, B, and C Classes



Class	Network bits	Networks	Host bits	Hosts Per Network	Suitable for
Class A	8	$2^8=256$	24	$2^{24} - 2^* = 16,777,214$ maximum hosts	For large organizations like Apple/Google/MS/Amazon
Class B	16	$2^{16}=65536$	16	$2^{16} - 2^* = 65,534$ maximum hosts	for medium scaled organizations like Sunbeam
Class C	24	$2^{24}=16\text{million}$	8	$2^8 - 2^* = 254$ maximum hosts	for small organizations/home network

** Subtracting the network and broadcast address*



Example: What is the type of the given IP address

1. 11.34.56.66
2. 10.46.34.67
3. 156.46.36.46
4. 172.20.34.56
5. 172.45.66.77
6. 192.168.2.5
7. 192.169.34.6

1. 11.34.56.66 : public
2. 10.46.34.67 : private
3. 156.46.36.46 : public
4. 172.20.34.56 : private
5. 172.45.66.77 : public
6. 192.168.2.5 : private
7. 192.169.34.6 : public



Example (Solution): What is the type of the given IP address

1. 11.34.56.66 : public
2. 10.46.34.67 : private
3. 156.46.36.46 : public
4. 172.20.34.56 : private
5. 172.45.66.77 : public
6. 192.168.2.5 : private
7. 192.169.34.6 : public



Example : which class needs to be used for following number of Devices?

1. 200 devices
2. 3000 devices
3. 50000 devices
4. 200000 devices

1. 200 devices : class C
2. 3000 devices : class B
3. 50000 devices : class B
4. 200000 devices : class A



Example (Solution) : which class needs to be used for following number of Devices?

1. 200 devices : class C
2. 3000 devices : class B
3. 50000 devices : class B
4. 200000 devices : class A



Protocol



Protocol and Standards

- ***Protocols define the format and order of messages sent and received among network entities, and actions taken on message transmission and receipt.***
- A protocol defines what, how, when it communicated.
- **The key elements of a protocol :**
 - **syntax :** structure and format of the information data
 - **Semantics:** meaning of each section of bits. an route identify the route to be taken or the final destination of the message
 - **Timing:** when data should be sent and how fast it should be sent

Standards

- Standards are developed by cooperation among standards creation committees, forums, and government regulatory agencies.
- Standards Creation Committees
 1. International Standards Organization (ISO)
 2. International Telecommunications Union (ITU)
 3. American National Standards Institute (ANSI)
 4. Institute of Electrical and Electronics Engineers (IEEE)



OSI Model & Layers

- Established in 1947, **the International Standards Organization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- We can not see standard but we can represent them.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection (OSI)** model.
- OSI model is now considered the primary Architectural model for inter-computer communications.
- **Term “open” denotes the ability to connect any two systems which conform to the reference model and associated standards.**



OSI Layers

Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1



Application Layer

- Interacts with application programs and is the highest level of OSI model.
- contains management functions to support distributed applications.
- enables the user, whether human or software, to access the network
- Examples : browser , applications such as file transfer, electronic mail, remote login etc.
- Protocols
 - http [80]: hyper text transfer protocol
 - https [443]: secure hyper text transfer protocol
 - ftp [20/21]: file transfer protocol
 - Sntp (25) : simple mail transfer protocol
 - Pop3 (110) : post office protocol
 - telnet(23) : used to connect to the remote machine
 - ssh [22]: secure shell
 - dns (53) : domain name service (used to get the IP address from the domain name)



Presentation Layer

Translation

- On sender side : translates from ASCII to EBDIC (Extended Binary Coded Decimal Interchange Code)
- On receiver side: translates from EBDIC to ASCII

Encryption/Decryption

- Plain Text to Cipher Text
- Algorithms : RSA, SHA

Compression / Decompression

- Sender Side : Compression
- Receiver Side : Decompression

Data Representation [Content-type] (Used to Decide Common File Formats)

- For text (plain: text/plain , html: text/html , json: application/json , xml: text/xml)
- For image (bmp: image/bmp , png: image/png , jpg: image/jpg , jpeg: image/jpeg)
- For audio & Video (wave: audio/wav, mp3: audio/mp3, mp4: video/mp4, flv: video/flv)



Session Layer

- **To start/manage/terminate the session.**
 - how to start, control and end conversations (called sessions) between applications.
 - log-on or password validation is also handled by this layer.
- **The session layer is the network *dialog controller*.**
 - mechanism for controlling the dialogue between the two end systems and synchronization.
 - Allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization**
 - Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.
 - It establishes, maintains, and synchronizes the interaction among communicating systems.
- **Protocols**
 - SIP: session initiation protocol
 - NetBIOS : Network Basic Input Output Service
 - RPC: Remote Procedure Call

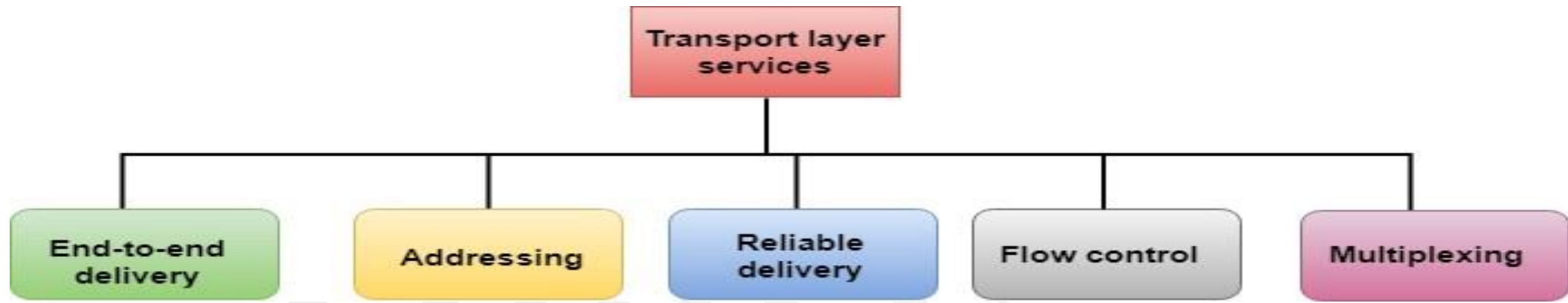


Transport Layer

- Most Important Layer of OSI
- Responsible **for process-to-process/ End to End delivery** of the entire message.
- Provide a reliable mechanism for the **exchange of data between two processes** in different computers.
- Segment
 - smaller part of session PDU
 - every segment contains sequence number
 - every segment contains checksum for error checking
 - Segment contains:
 - **data** (from the session layer PDU)
 - **sequence number** : used for re-assembling the segments on the receiver machine
 - **checksum** : used to check if the data is not damaged



Responsibilities of Transport Layer



End –to-End delivery

- The transport layer transmits the entire message to the destination

Addressing

- The transport layer provides the user address which is specified as a station or port.

Reliable delivery

- provides reliability services by retransmitting the lost and damaged packets
- Error control, sequence control, loss control, duplicate control.

Error Control

- performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

Flow Control

- Flow control is used to prevent the sender from overwhelming the receiver.
- If the receiver is overloaded with too much data, then the receiver discards the packets & ask for retransmission of packets.

Multiplexing

- uses the multiplexing to improve transmission efficiency.



Transport Layer Protocol

TCP

- Transmission Control Protocol (Reliable)
- connection oriented protocol
 - connection will be kept alive till the data transfer in progress
- flow control, error checking and sequencing
- slower than UDP
- E.g. Email (no data loss)

UDP

- User Datagram Protocol (Unreliable)
- Connection Less Protocol
- does not provide error checking/flow control
- Faster than TCP because no ACK only sending of data packets
- E.g: Online Games, Streaming



Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
 - Segment Contains :
 - data
 - source IP address
 - destination IP address
 - **Network Layer Responsibilities:**
 - Logical Addressing : The network layer translates the logical addresses into physical addresses
 - Routing : sending the data across the network
 - Internetworking : provides the logical connection between different types of networks
 - Fragmentation : breaking the packets into the smallest individual data units that travel through different networks.
 - **Protocols :**
 - IP : internet protocol
 - IPx : internetwork packet exchange
 - ICMP : Internet Control Messaging Protocol
 - NAT : Network Address Translation
 - ARP : Address Resolution Protocol
 - PPP: Point to Point Protocol
 - **Device : Router**



Data Link Layer

- Data link layer attempts to provide reliable communication over the physical layer interface.
- **DATA LINK Layer Responsibilities :**
 - **Framing:**
 - Breaks the outgoing data into frames and reassemble the received frames.
 - every frame contains (Source MAC address and Destination MAC address)
 - **Physical Addressing:**
 - uses MAC address to identify every NIC uniquely
 - **Flow Control:**
 - A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
 - **Error Control:**
 - Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
 - **Access Control:**
 - Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.
- **Protocols**
 - ARP(Address Resolution Protocol) : getting physical address from logical address
 - RARP: Reverse Address Resolution Protocol
- **Device : Switch**



Physical Layer

- Provides physical interface for transmission of information.
- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication. Characteristics like voltage levels, timing of voltage changes, physical data rates, etc.
- send data in the form of 1's and 0's.
- senders and receivers clock must be synchronized.
- **Transmission mode:**
 - Defines direction of transmission simplex, half duplex and full duplex
- **Devices:**
 - NIC , Cables , hubs , repeaters , connectors



7 Layers of OSI Model

Application

(PDU : Data)

- End user Layer
- HTTP, FTP, IRC, SSH, DNS

Presentation

(PDU : Data)

- Syntax Layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

Session

(PDU : Data)

- Synch and Send to port
- API's, Sockets

Transport

(PDU : Segment)

- End to end Connections
- TCP , UDP

Network

(PDU : Packet)

- Packets
- IP, ICMP, IPSec, IGMP

Data Link

(PDU : Frame)

- Frames
- Ethernet, PPP. Switch, Bridge

Physical

(PDU : Bits)

- Physical Structure
- Coax, Fiber, Wireless, Hubs, Repeaters

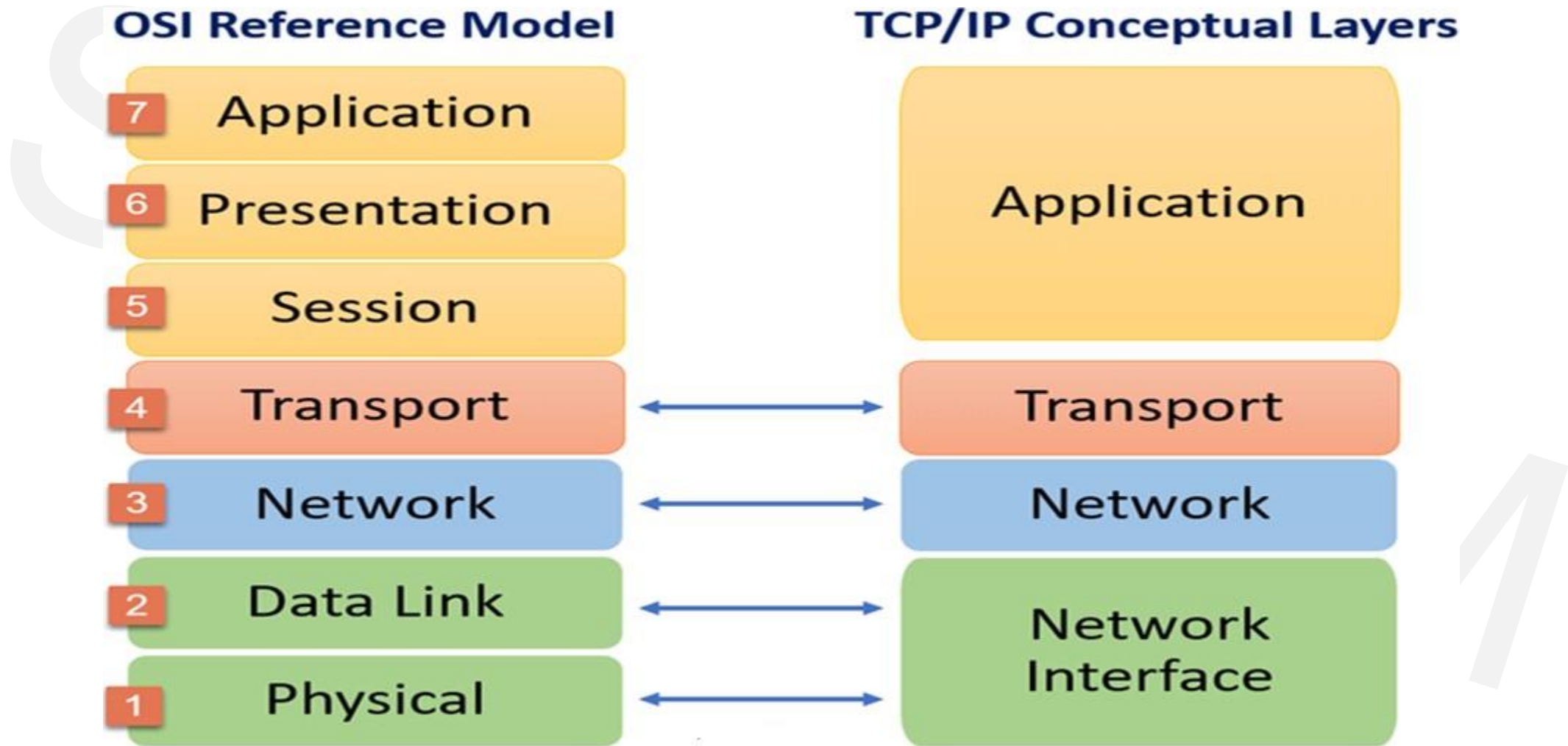


OSI and TCP/IP Model

- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
- The OSI has seven layers while the TCP/IP has four layers.



OSI and TCP/IP Model



Thank You!!

