

**Computer Network:**

An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.

**OSI:**

OSI stands for **Open Systems Interconnection**. It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.

**Protocol:**

A protocol is the set of rules or algorithms which define the way how two entities can communicate across the network and there exists different protocol defined at each layer of the OSI model. Few of such protocols are TCP, IP, UDP, ARP, DHCP, FTP and so on.

**Host name:**

Each device in the network is associated with a unique device name known as Hostname.

**IP Address (Internet Protocol address):**

Also known as the Logical Address, the IP Address is the network address of the system across the network.

To identify each device in the world-wide-web, the Internet Assigned Numbers Authority (IANA) assigns an IPV4 (Version 4) address as a unique identifier to each device on the Internet.

The length of an IPv4 address is 32-bits, hence, we have  $2^{32}$  IP addresses available. The length of an IPv6 address is 128-bits.

**MAC Address (Media Access Control address):**

Also known as physical address, the MAC Address is the unique identifier of each host and is associated with its NIC (Network Interface Card).

A MAC address is assigned to the NIC at the time of manufacturing.

The length of the MAC address is : 12-nibble/ 6 bytes/ 48 bits

**Port:**

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on which they are running.

**Socket:**

The unique combination of IP address and Port number together are termed as Socket.

**DNS Server:****DNS stands for Domain Name system.**

DNS is basically a server which translates web addresses or URLs (ex: www.google.com) into their corresponding IP addresses. We don't have to remember all the IP addresses of each and every website.

1. **Repeater** – A repeater operates at the physical layer. important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. **It is a 2 port device.**

2. **Hub** – **A hub is basically a multiport** and work on physical layer . they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.And it can send data by one path only.

**i)Active Hub:**

active hub is also known multi port repeater. It regenerate and amplify the signal along the network. It require external power.

**ii)Passive Hub:**

Passive hub is also known multi port repeater.opposite of active hub

**iii)Intelligent Hub:**

[What are smart or intelligent hubs?](#)

Smart hubs are similar to active hubs but they also

contains some type of software that manage the

clients and if an error occur it is compatible to isolate them.

**Difference:**

Connection oriented and Connection-less service

In **connection oriented service** authentication is needed, while connection-less service does not need any authentication.

Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs, while **connection-less service protocol** does not guarantees a message delivery.

Connection oriented service is more reliable than connection-less service.

Connection oriented service interface is stream based and connection-less is message based.

**Difference between Active and passive hub:**

- Active hub strengthen the signal where passive hub repeat/copy signals.
- Active hub need Electricity whereas passive hub work without it.

- Active hub more smarter then passive hub.
- Passive hub is just a connector which connects wire coming from other devices.
- Active hub is multi-point repeater with capability of regeneration of signals.
- Active hub can process and monitor information while passive hub cannot do this.

## Difference Between Hub and Repeater?

Repeater is use to repeat the signals which has two ports: One for incoming signal and the output received is boosted signal. On the other hand **Hub is able to join more than two signals**. It takes the signal, “boosts” it, and transmits to all its ports. Typically hub can connect from 8 to 24 connections together.

## Can we connect small size of computers to smart hubs?

Smart hubs come at a price, most of the offices that simply want to connect few PC's they never go for these hubs.

## Do active hubs or passive hubs, smart hubs have management software?

---

Most switches contain the admin panel software built in which allow the user

---

or administrator to control manage or configure the devices. (active hubs,

---

smart hubs have admin panels).

## Why people choose switch over hub? or why is switch better than hub?

---

A switch is more intelligent than a hub that is why people choose switch over hub.

---

**Hub:** A hub is use to connect the computers only with one another and normally fall in the category of passive hubs.

---

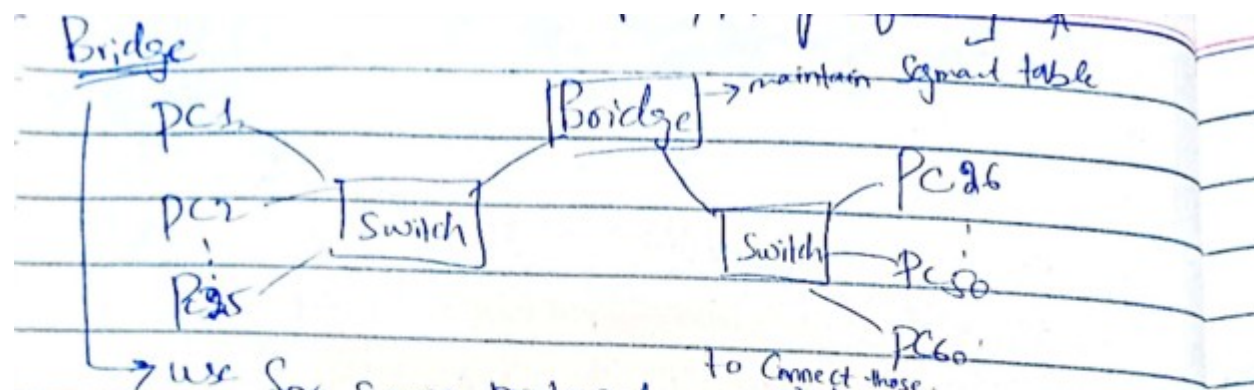
**Switch:** A switch is capable of connecting device and use to manage them as well. An admin panel is available to manage them to block or manage them. However, a switch is more efficient at passing along traffic. ... If the destination address is not in the table, the switch sends the traffic to all the connected computers.

---

**Do switch and routers has firewall?**

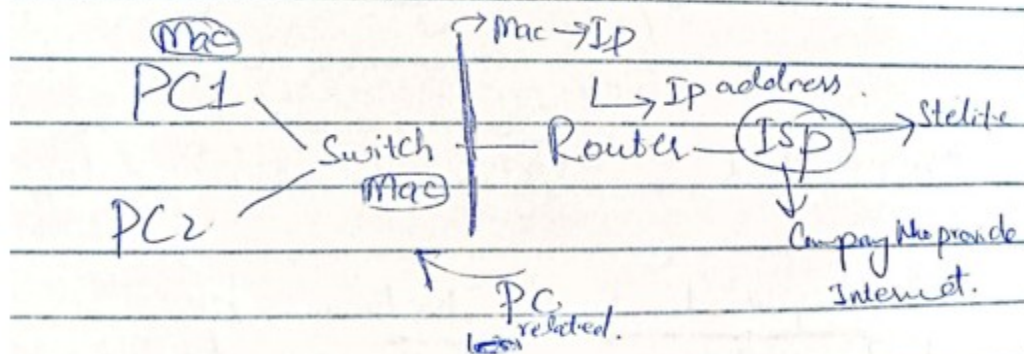
Most of the switch are controlled by your internet service provider and has capability to connect them with firewall. Read more about firewall and routers.

## Bridge



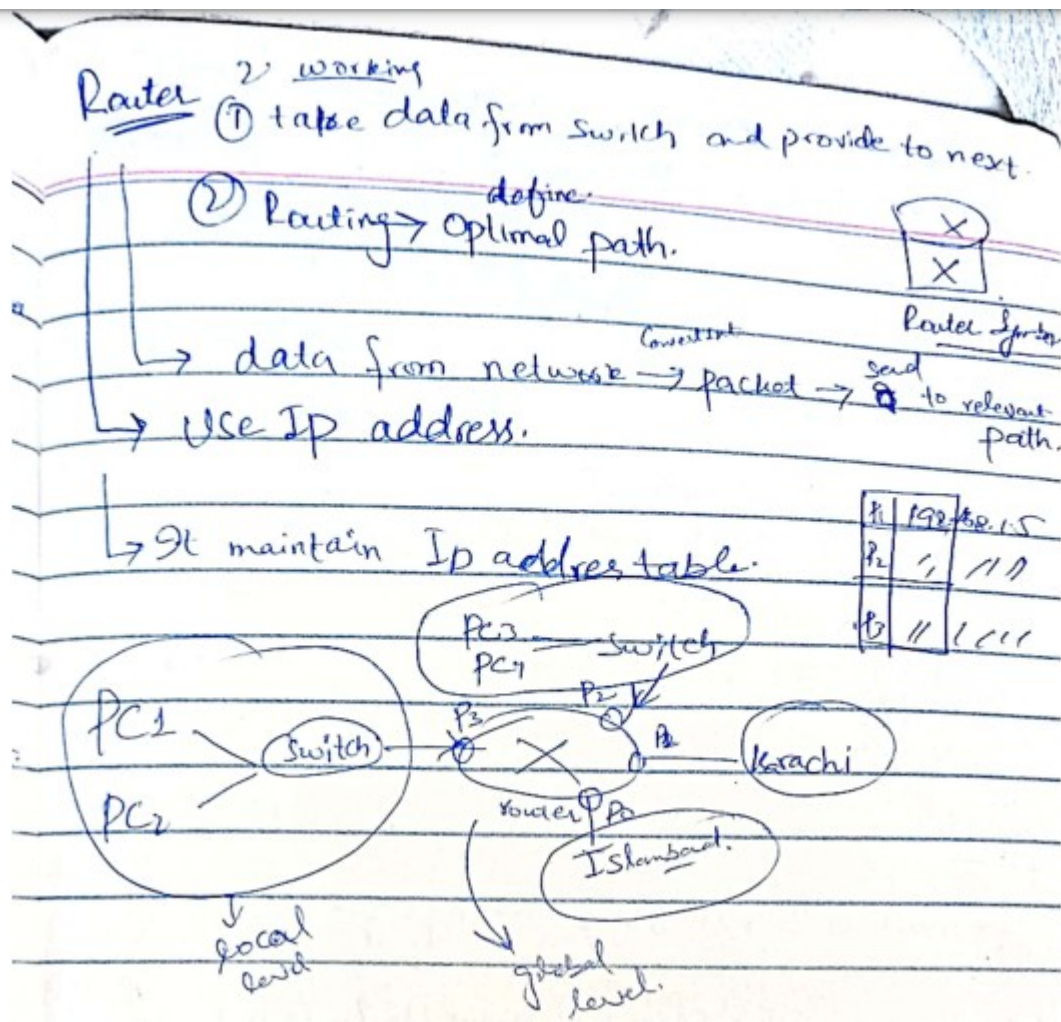
② Switch → advance than Hub

MAC Address / physical address → Provide by Manufacturer  
 IP Address / logical address / ISP → Provide by Internet.



Switch intelligence device → Maintain → Mac table

P0	P0	P0 mac01	P0
P1	P1	P002	P1
P2	P2	mac03	P2
P2	P3	mac04	P3



## Gateway

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally



more complex than switches or routers. Gateway is also called a protocol converter.

## What is Point-to-Point Communication?

In telecommunications, a point-to-point connection is a communications link between two communication endpoints or nodes. A telephone call is an example of this, in which two phones are linked, and what one caller says can only be heard by the other.

Key	Point-to-Point Communication	Multi-point Communication
Definiti on	Point-to-point communication is a method in which the channel of communication is shared only between two devices or nodes.	Multi-point communication is a form of communication in which the channel is shared among multiple devices or nodes.

Error Prone	Point-to-point communication is more error prone as compared to Multi-point communication.	Multi-point communication is less error prone as compared to Point-to-point communication.
Security and Privacy	Point-to-point communication is more secure and private as compared to Multi-point communication.	Multi-point communication is less secure and private as compared to Point-topoint communication.

## Frequency Division Multiplexing :

*Divides into multiple bands*

Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands, where each sub-band carries different signals. Practical use in radio spectrum & optical fibre to share multiple independent signals.

#### •Time Division Multiplexing :

*Divides into frames*

Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user.

Time division multiplexing (TDM) is also known as a digital circuit switched.

#### **Application of FDM:**



1. In the first generation of mobile phones, FDM was used.
2. The use of FDM in television broadcasting
3. FDM is used to broadcast FM and AM radio frequencies.

## **Difference between Datagram switching & Virtual circuit switching :**

<b>Datagram Switching</b>	<b>Virtual Circuit</b>
It is connection less service. There is no need for reservation of resources as there is no dedicated path for a connection session.	Virtual circuits are connection-oriented, which means that there is a reservation of resources like buffers, bandwidth, etc. for the time during which the new setup VC is going to be used by a data transfer session.
All packets are free to use any available path. As a result, intermediate routers calculate routes on the go due to dynamically changing routing tables on routers.	The first sent packet reserves resources at each server along the path. Subsequent packets will follow the same path as the first sent packet for the connection time.
Data packets reach the destination in random order, which means they need not reach in the order in which they were sent out.	Packets reach in order to the destination as data follows the same path.
Every packet is free to choose any path, and hence all the packets must be associated with a header containing information about the source and the upper layer data.	All the packets follow the same path and hence a global header is required only for the first packet of connection and other packets will not require it.
Datagram networks are not as reliable as Virtual Circuits.	Virtual Circuits are highly reliable.
Efficiency high, delay more	Efficiency low and delay less
Widely used in Internet	Used in X.25, ATM(Asynchronous Transfer Mode)

## **Access Network**

- Access network is a physical link that connects edges or end systems to the edge router. Edge router is the first router on a path from end system to ISP
  - Home Access
  - Enterprise Access
  - Mobile Access

### **Home Access**

- **Dial Up modem:** Connection established by using modem. Modem is connected to a telephone line to which is connected to ISP. It uses PSTN to connect to ISP.
- **DSL:** (Digital Subscriber Line) a modem technology that uses existing telephone lines to transport high-bandwidth data, such as multimedia and video, to service subscribers. DSL

provides dedicated, point-to-point, public network access. This DSL connection is typically between a network service provider (NSP) central office and the customer site.

Difference: DSL is hundred times faster than Dial Up modem. DSL allow you to use internet while using telephone whereas Dial Up dont.

- **HFC**: (Hybrid Fiber Coaxial cables) architecture tha use a combination of fiber optic cabling and coaxial cabling to distribute video, data and voice content to/from the headend and the subscribers.

## Enterprise Access

- Uses **Ethernet** to connect an enterprise network to ISP

## Mobile Access

- Mobile devices are connected to **base station**, base station connect them to the wired network.

## Broadband

Broadband is the **transmission of wide bandwidth data over a high speed internet connection**. So what is broadband? According to the FCC, the definition of broadband internet is a minimum of 25 Mbps download and 3 Mbps upload speeds.

# Layered Architectures

OSI (**Open Systems Interconnection**.)Reference model

TCP/IP model

# ISO/OSI Reference Model

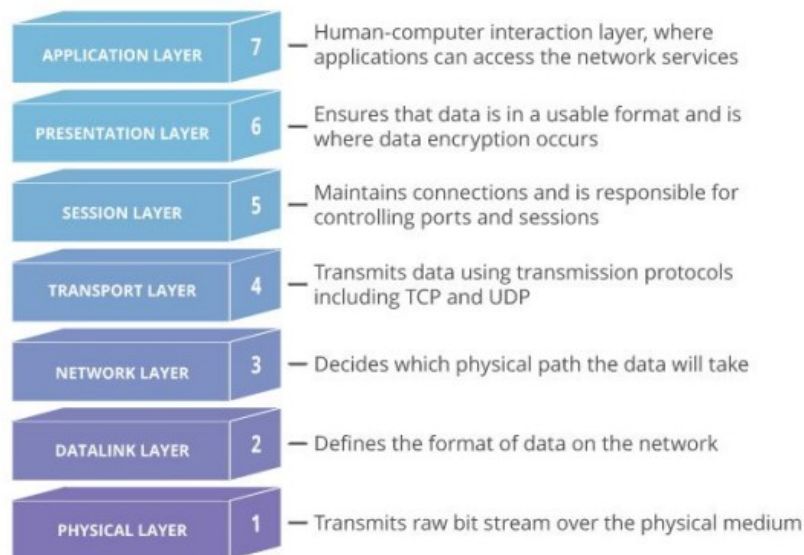
Open System Interconnection developed by International Standard for Organizations.

It is a model or a set of guidelines for designing a network that is robust, flexible, and interoperable.

It is just a guideline, neither a software nor a protocol and therefore is called OSI reference model.

Purpose is to facilitate communication between two systems without getting into underlying hardware and software of the system.

## OSI Reference Model



## Application

- To allow access to network resources

## Transport

- To provide reliable process to process message delivery and error delivery

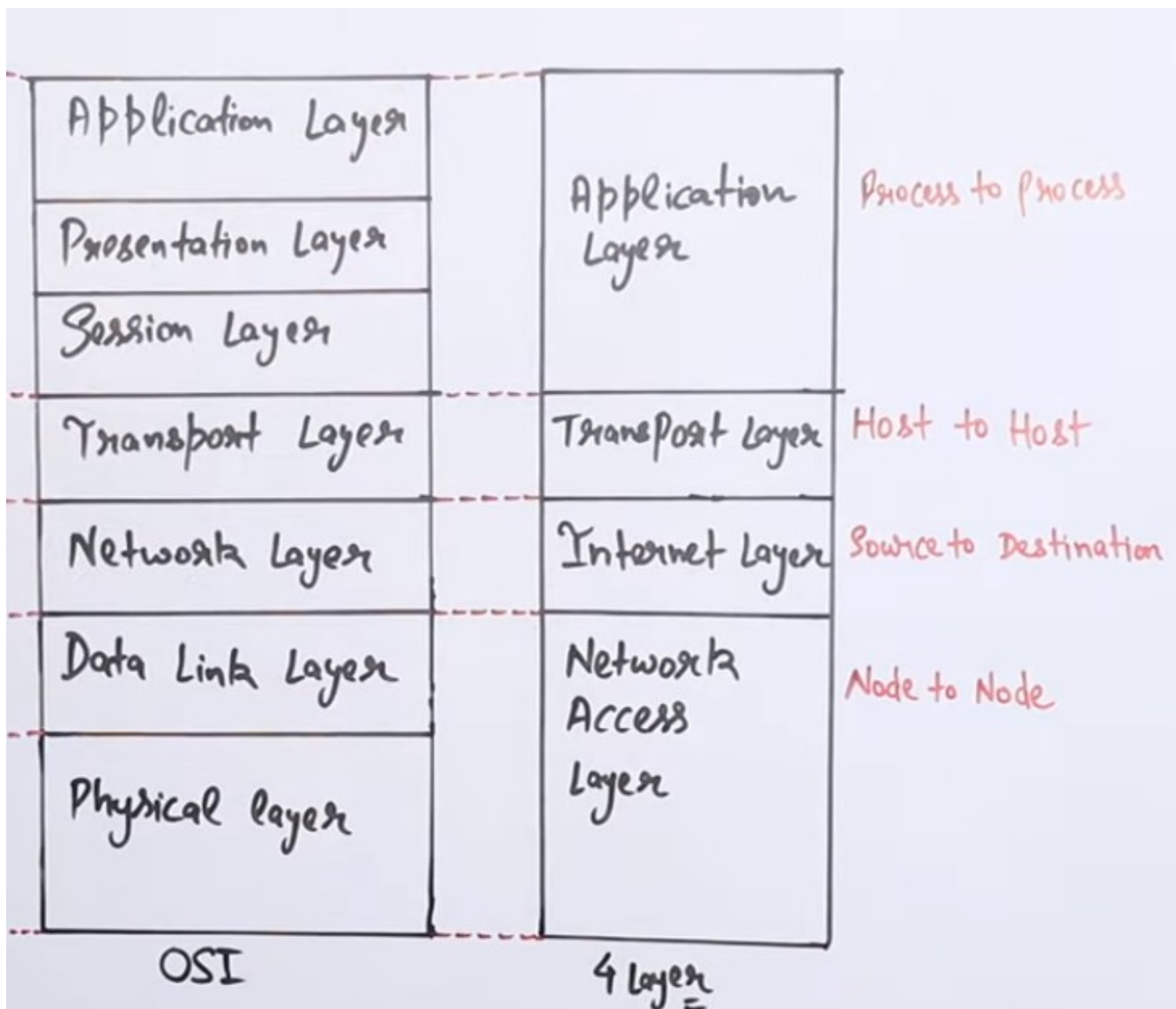
## Internet

- To move packets from source to destination
- To provide internetworking

## Network Interface

Responsible for the transmission for the between two device on the same network.

Four Layers of TCP/IP model



# Application architectures

## 2: peer-to-peer (P2P)

### peer-to-peer architecture :-

peer-to-peer network also known as point-to-point network in which all the computers are ~~linked to~~ directly linked together with equal privileges and responsibilities for sharing the data.

There is no server in it.

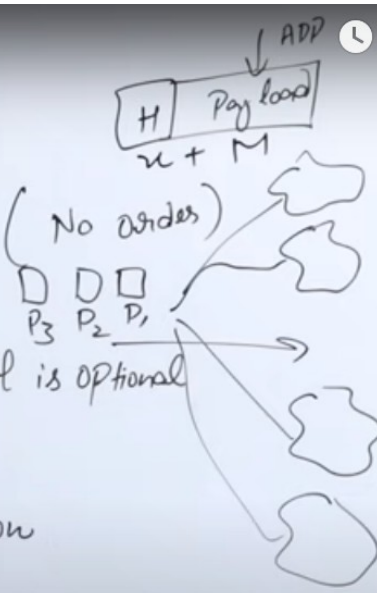
## client-server architecture

### Client-Server architecture :-

Client-Server architecture also known as request-response architecture. In this architecture client makes a request to the server, and server will fulfill the response.



TCP	UDP
1) Connection oriented	1) Connectionless
2) Reliable <u>Ordering</u> .	2) Less Reliable (No order)
3) Error Control is mandatory	3) Error Control is optional
4) Slow transmission	4) Fast transmission
5) More overhead (20-60 B)	5) Less overhead (8 B)
6) Flow Control, Congestion Control	6) No FC, CC



TCP	UDP
HTTP	DNS
FTP	BOOTP
	DHCP
	RDP

## What is a Socket?

Sockets allow communication between two different processes on the same or different machines. It is the door to communicate with other device.

# Chapter 2: summary

*our study of network apps now complete!*

- application architectures
  - client-server
  - P2P
- application service requirements:
  - reliability, bandwidth, delay
- Internet transport service model
  - connection-oriented, reliable: TCP
  - unreliable, datagrams: UDP
- specific protocols:
  - HTTP
  - SMTP, POP, IMAP
  - DNS
  - P2P: BitTorrent
- video streaming, CDNs
- socket programming:  
TCP, UDP sockets




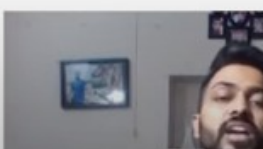
- Port no 80 ✓
- Itself not reliable but use TCP to achieve reliability
- Inband Protocol
- Stateless ✓
- HTTP 1.0 Non-Persistent ✓
- HTTP 1.1 Persistent
- Commands(Head, Get, Post, Put, Delete, Connect)

HTTP → Commands } 80

Data

Connections





## HTTP overview (continued)

### *uses TCP:*

- client initiates TCP connection (creates socket) to server, port 80
- server accepts TCP connection from client
- HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server)
- TCP connection closed

### *HTTP is “stateless”*

- server maintains no information about past client requests

*asid*

protocols that maintain “state” are complex!

- past history (state) must be maintained
- if server/client crashes, their views of “state” may be inconsistent, must be reconciled

# FTP

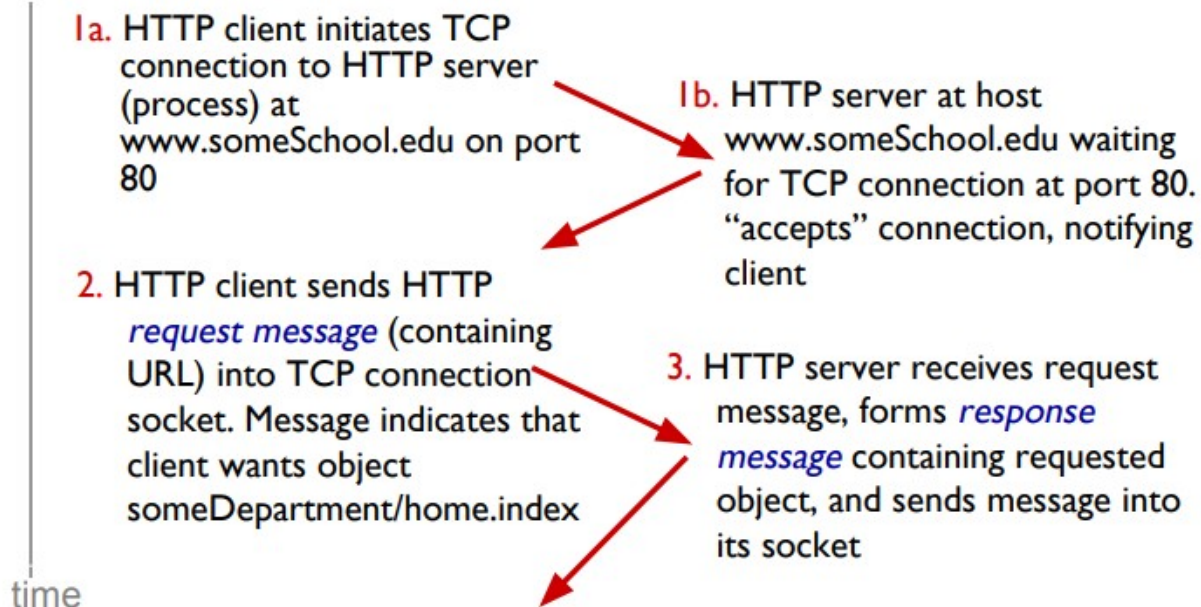
- Port no 20(DATA) & 21(Control)
- Data connection is non-persistent
- Control connection is persistent
- Not Inband
- Reliable
- Stateful

# Non-persistent HTTP

suppose user enters URL:

`www.someSchool.edu/someDepartment/home.index`

(contains text,  
references to 10  
jpeg images)



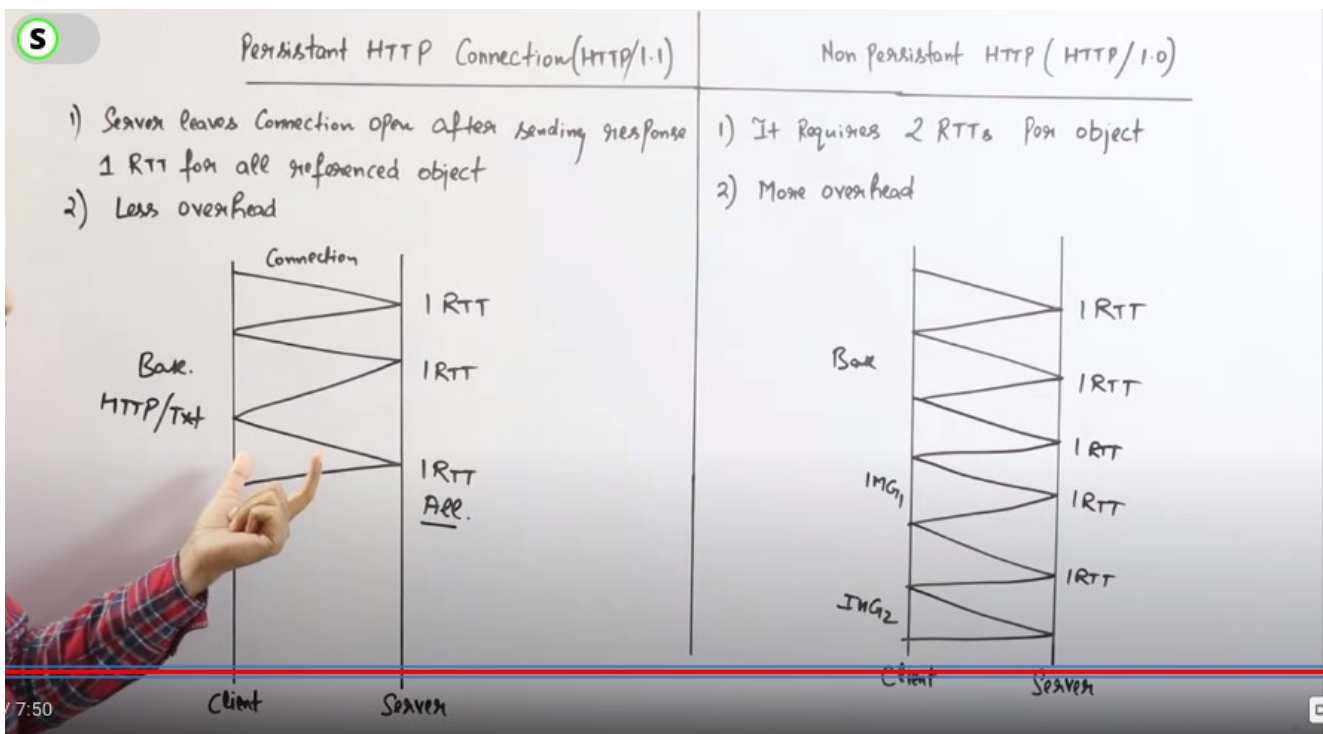
## HTTP connections

### *non-persistent HTTP*

- at most one object sent over TCP connection
  - connection then closed
- downloading multiple objects required multiple connections

### *persistent HTTP*

- multiple objects can be sent over single TCP connection between client, server



## HTTP response status codes

- status code appears in 1st line in server-to-client response message.
- some sample codes:

### 200 OK

- request succeeded, requested object later in this msg

### 301 Moved Permanently

- requested object moved, new location specified later in this msg (Location:)

### 400 Bad Request

- request msg not understood by server

### 404 Not Found

- requested document not found on this server

### 505 HTTP Version Not Supported

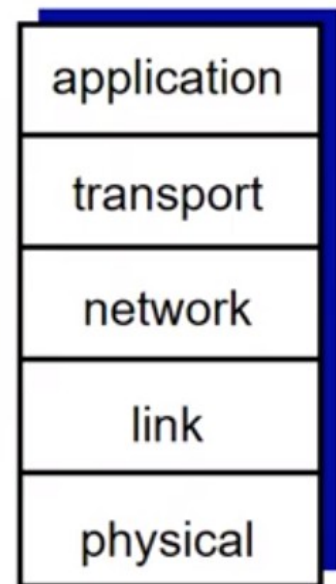


Cookies      <https://youtu.be/gTTpNmWTOig>

Here are the major differences between GET and POST:

GET	POST
In GET method, values are visible in the URL.	In POST method, values are not visible in the URL.
GET has a limitation on the length of the values, generally 255 characters.	POST has no limitation on the length of the values since they are submitted via the body of HTTP.
GET performs are better compared to POST because of the simple nature of appending the values in the URL.	It has lower performance as compared to GET method because of time spent in including POST values in the HTTP body.
This method supports only string data types.	This method supports different data types, such as string, numeric, binary, etc.
GET results can be bookmarked.	POST results cannot be bookmarked.
GET request is often cacheable.	The POST request is hardly cacheable.
GET Parameters remain in web browser history.	Parameters are not saved in web browser history.

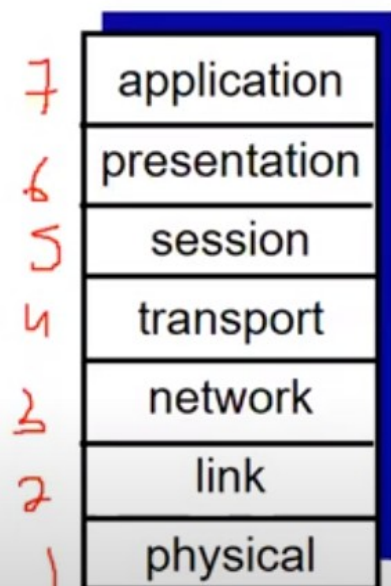
- ❖ **application:** supporting network applications
  - FTP, SMTP, HTTP
- ❖ **transport:** process-process data transfer
  - TCP, UDP
- ❖ **network:** routing of datagrams from source to destination
  - IP, routing protocols
- ❖ **link:** data transfer between neighboring network elements
  - Ethernet, 802.111 (WiFi), PPP
- ❖ **physical:** bits “on the wire”



Activate  
Go to Seti

## ISO/OSI reference model

- ❖ **presentation:** allow applications to interpret meaning of data, e.g., encryption, compression, machine-specific conventions
- ❖ **session:** synchronization, checkpointing, recovery of data exchange
- ❖ Internet stack “missing” these layers!
  - these services, *if needed*, must be implemented in application
  - needed?



Activate





# Diagram Layer

## Cookies

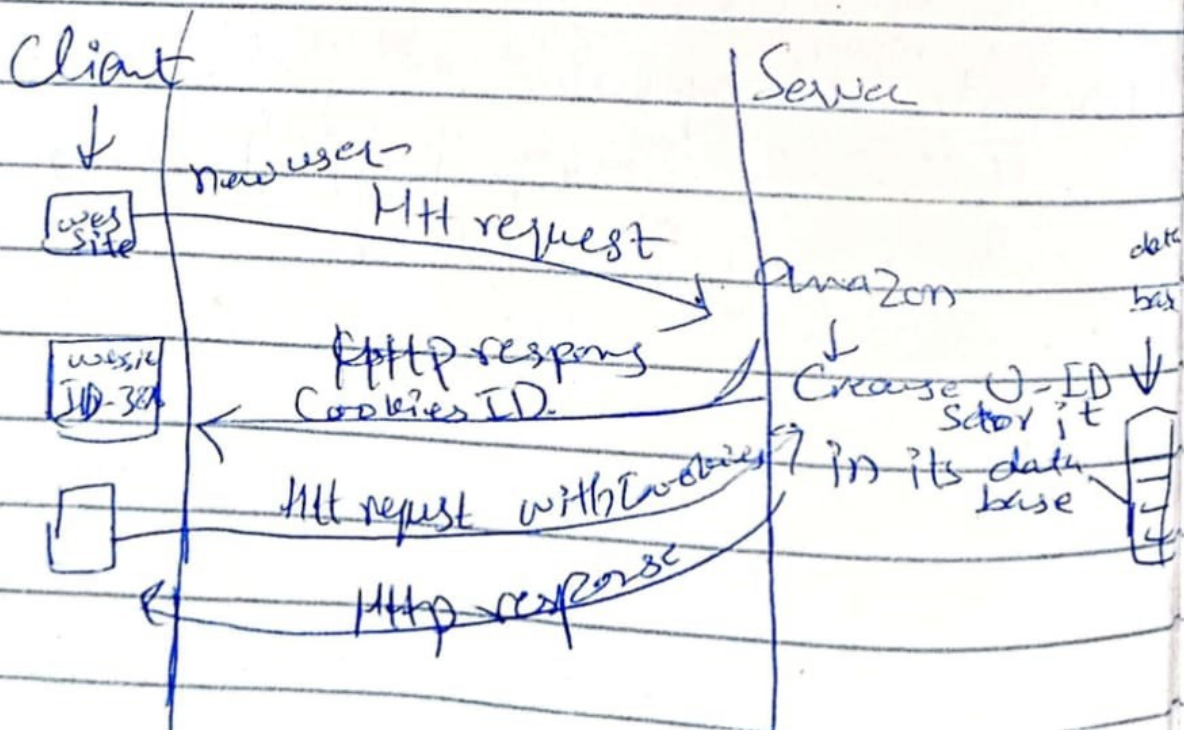
↳ server is Stateless (do not store data about user).

① we request for HTTP there is cookie headline of HTTP response message

② Next time for HTTP request cookie headline is in request message

③ cookies file store on ~~user agent~~ browser.

④ cookies <sup>header</sup> also store in database - backend.



Cookie used

① authorization      ③ Shopping Carts

② recommendation      ④ uses session state

notice  
user

behavior



TCP IP

data  
with  
extra  
info.

① first stage  
"message"

② Segment

③ packet

④ frame

⑤ bit

Application

transport

network

Data link

Physical





## Delays

$$\text{Bandwidth} = \text{Transmission rate}$$

→ Transmission delay: Time taken to put a message or packet on transmission medium → Formula →  $T_D = \frac{L \text{ of message}}{\text{Bandwidth}}$

→ Propagation delay: Amount of time taken to transfer a message from source to destination →  $= \frac{\text{Distance}}{\text{Speed}}$   
 $P_D = \frac{\text{Distance}}{\text{No. of hops} \times P = \text{speed in medium}}$

→ Queuing delays: Amount of time a packet wait in buffer before transmit → No formula.

→ Processing delays: Amount of time a router takes in processing a packet before transmit → No formula.

→ Node delay: Time taken to process a packet in network node (router, switch, hub etc).

→ End to End delays:-

Time taken for a

packet ~~access~~ to be transmitted

$$E2E_D = (\text{propagation delay} + \text{transmission delay}) \times \text{no of hops}$$



$\frac{d}{t} = v$

## Delays

$$\text{Bandwidth} = \text{Transmission rate}$$

→ Transmission delay: Time taken to put a message or packet on transmission medium → Formula →  $TD = \frac{L \text{ of message}}{\text{Bandwidth}}$

→ Propagation delay: Amount of time taken to transfer a message from source to destination →  $PD = \frac{\text{Distance}}{\text{Speed}}$   
 $PD = \frac{\text{Distance}}{\text{No. of hops} \times P = \text{speed in medium}}$

→ Queuing delay: Amount of time a packet wait in buffer before transmit → No formula.

→ Processing delay: Amount of time a router takes in processing a packet before transmit → No formula.

→ Node delay: Time taken to process a packet in network node (router, switch, hub etc).

→ End to End delays:-

Time taken for a

packet ~~access~~ to be transmitted

$$E2E = (\text{propagation delay} + \text{transmission delay}) \times \text{no of hops}$$



$\frac{d}{v} + \frac{L}{C}$



## Circuit Switching

Setup time = time require to establish connection

Transmission time =  $\frac{\text{message length}}{\text{Bandwidth}}$

Propagation delay =  $\text{Distance} / \text{speed}$

Tear down time = Time for releasing sources

$$\boxed{\text{Total Transmission time}} = \text{Setup time} + T_t + P_d + \text{Tear down time}$$

$\Downarrow$  also equals to

$$\boxed{\text{Total delay}} = //$$

$+ \text{processing delay}$   
 $+ \text{queuing delay}$

## Packet Switching

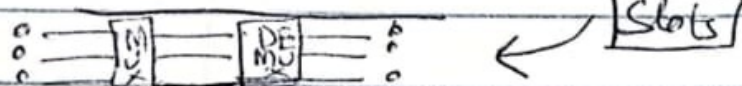
no. of routers =  $n$ .

Transmission time =  $\text{No. of bits} / \text{bandwidth}$   $\rightarrow$  Same CS

Propagation delay =  $\text{Distance} / \text{speed}$   $\rightarrow$  Same CS

Total transmission time =  $n(T \text{ time}) + \text{Propagation delay}$

FDM



Total transmission time =  $\text{Setup time} + T_t + P_{\text{delay}} + \text{Tear down time}$

Here Bandwidth =  $\text{total Bandwidth} / \text{No of Slots}$

TDM



$TT = \text{Setup time} + T_t + \text{Propagation delay} + \text{Tear down}$

Bandwidth per frame =  $\text{Total bandwidth} / \text{No. of frames}$   
bits in each frame

