Date:
Page:

Unit - 1

What's the Internet:

- Millions of connected computing devices:
  - hosts = end systems — PC, server, wireless laptop, smartphone.
  - running network apps.
- Communication links
  - fiber, copper, radio, satellite — wireless links - wired links
  - transmission rate : bandwidth
- Packet switches:
  forward packets (chunks of data)
  - routers and switches.

"fun" internet appliances.

IP Photo frame
Internet refrigerator
Slingbox → watch control cable TV remotely.
Web-enabled toaster + weather forecaster
Internet phones.

What's the Internet: "nuts and bolts"

- Internet "network of networks"
  - Interconnected ISPs.

Date:
Page:

- Protocols control sending, receiving of msgs
  - e.g, TCP, IP, HTTP, Skype, 802.11

- Internet standards
  - RFC : Request for comments.
  - IETF : Internet Engineering Task force.

What's the Internet : a service view

- Infrastructure that provides services to applications :
  - Web, VoIP, email, games, e-commerce, social nets, ..

- provides programming interface to apps
  - hooks that allow sending and receiving app programs to "connect" to Internet.
  - provides service options, analogous to postal service.

What's a protocol?

→ human protocols:
- what's the time?
- I have a question
- introductions

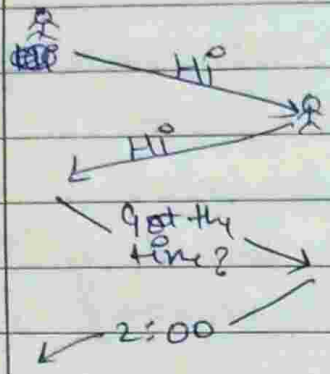
---- specific msgs sent
---- specific actions taken when msgs received, or other events.

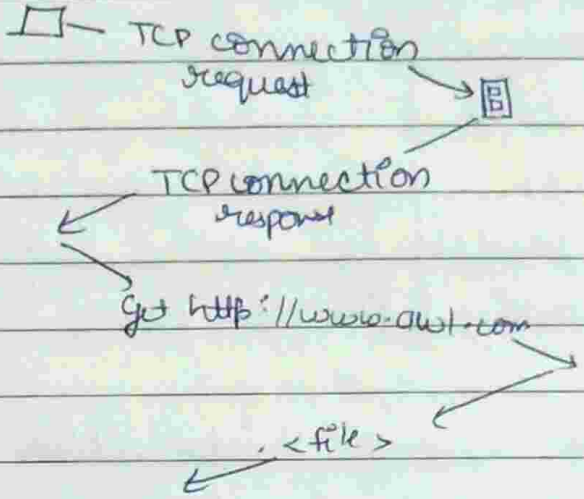
→ network protocols:
- machines rather than humans.
- all communication activity in Internet governed by protocols.

protocols define format, order of msgs sent & received among network entities, and action taken on msg transmission, receipt.

Date:
Page:

a human protocol & a computer network protocol





- Protocol 'layers'

Networks are complex with many pieces:

- hosts
- routers
- links of various media
- applications
- protocols
- hardware, software.

- Organization of air travel.

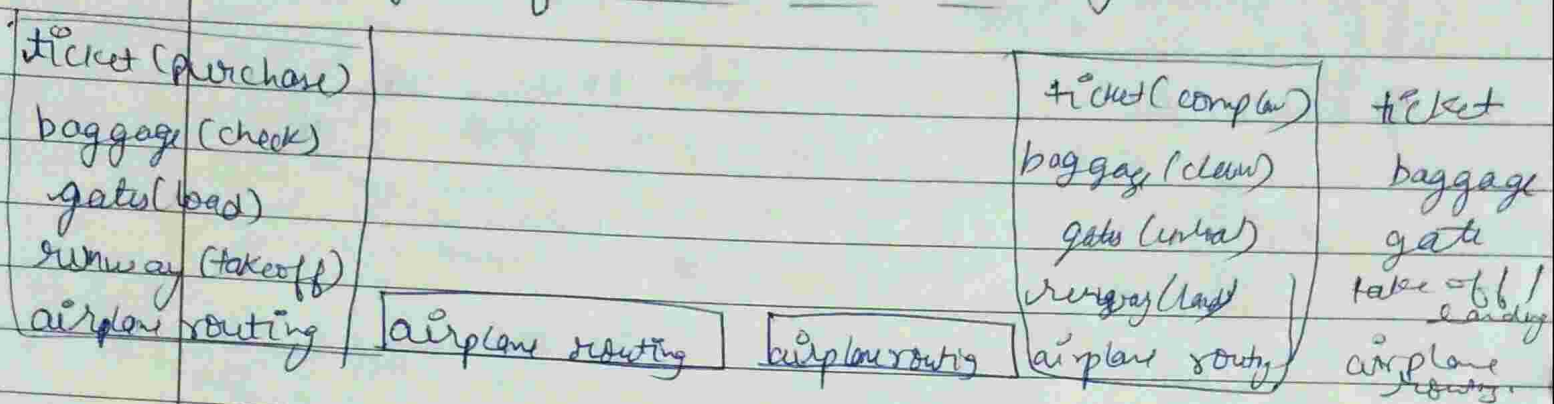
ticket (purchase)
baggage (check)
gates (load)
runway takeoff
airplane routing.

ticket (complain)
baggage (claim)
gates (unload)
runway landing
airplane routing.

airplane routing.

Date:
Page:

Layering of airline functionality



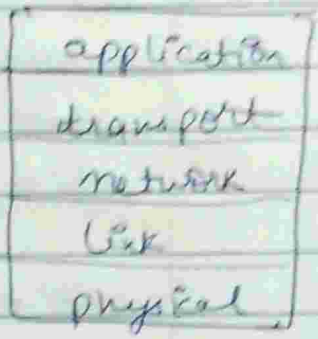
layers: each layer implements a service.
- via its own internal-layer actions.
- relying on services provided by layer

✱ Why layering?

dealing with complex systems:
- explicit structure allows identification, relationship of complex system's pieces.
- modularization eases maintenance, updating of system
  - change of implementation of layer's service transparent to rest of system.
  - e.g. change in gate procedure doesn't affect rest of system.
- layering considered harmful.

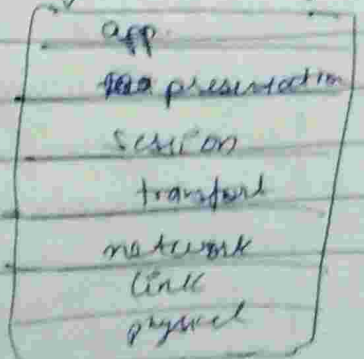
Internet protocol stack

- 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 b/w neighboring network elements.
  - Ethernet, 802.11 (wifi), PPP.
- physical : bits "on the wire"



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)



Access networks & physical media

Q- How to connect end systems to edge router?

1. residential access nets.
2. institutional access networks (school, company).
3. mobile access networks.

Keep in mind
bandwidth (bits per second) of access network?
shared or dedicated.

Access net: Digital subscriber line (DSL)

* use existing telephone line to central office DSLAM.
  - data over DSL phone line goes to internet.
  - voice over DSL phone line goes to telephone set

<2.5 Mbps upstream transmission rate (typically < 1Mbps)

<24 Mbps downstream transmission rate (typically < 1Mbps)

* Wireless access Network.

Shared wireless access network connects end system to router.
Via base station aka "access point".

Wireless LAN's
within building (100 ft)
802.11b/g (wifi): 11, 54
Mbps transmission rate.

with area wireless access provided by telco operator 10's Km b/w 1 and 10Mbps 3G, 4G LTE.

Page:

Packet switching

used in internet and as we do divide the complete message into number of messages chucks & as these chucks reach to network layer they became packets so that's why they are called as packet switching i.e. individually packet has got the capability to reach its destination.

- mesh of interconnected routers.
- packet-switching: hosts break application-layer messages into packets.
- forward packets from one router to the next across links on path from source to destination.

Each packet transmitted at full link capacity.

(1) Packet-switching: store & forward

⊗ - router / store & forward switch.

L - bits per packets.

R - rate of transmission that depends on links.

Transmission delay: Time required by a node or a router to push all the bits present in a packet into the link is called TD.

formula L/R. seconds to transmit L bit packet into link at Rbps.

- store & forward: entire packet must arrive at router before it can be transmitted on next link.

- end-end delay - 2L/R (assuming a propagation delay) more or delay shortly.

Page:

Packet switching

used in internet and as we do divide the complete message into number of messages chucks & as there chucks reach to network layer they became packets so that's why they are called as packet switching i.e. individually packet has got the capability to reach its destination.

- mesh of interconnected routers.
- packet-switching: hosts break application-layer messages into packets.
- forward packets from one router to the next across links on path from source to destination.
  Each packet transmitted at full link capacity.

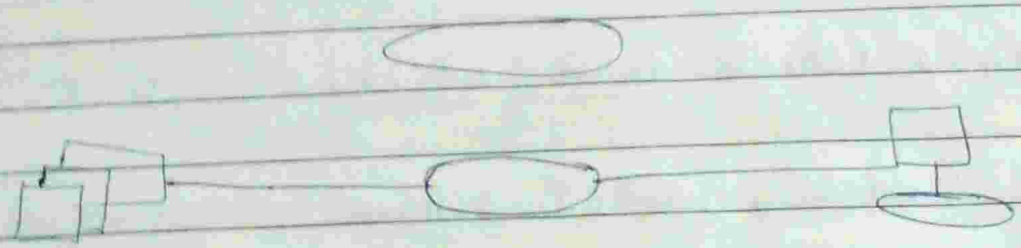
① Packet-switching: store & forward

⊗ - router / store & forward switch.
L - bits per packets.
R - rate of transmission that depends on links.

Transmission delay: Time required by a node or a router to push all the bits present in a packet into the link is called TD.
formula L/R. seconds to transmit L bit packet into link at Rbps.

- store & forward: entire packet must arrive at router before it can be transmitted on next link.

- end-end delay - 2L/R (assuming a propagation delay) more or delay finally.



(2) Queuing delay loss.

Queuing and loss:
If arrival rate (in bits) to link exceeds transmission rates of link for a period of time:
packets will queue, wait to be transmitted on link.
packets can be dropped (lost) if memory (buffer) up.

Queuing delay → no. of packets ahead X L/R.

Two Key Network core functions

Routing: determines source destination route taken by packs routing algorithm.
forwarding: move packets from routers input to appropriate router output.

Placing the packet from input cook to the correct O/P cod is called packet forwarding.

routing: path taken by the packet from source to the destination & this is done with the help of routing algorithm → used for find the shortest path to reader.

Alternative Core : Circuit Switching

Circuit switching works in 3 phases
(1) Data connection.
(2) " Transmission.
(3) connection Termination

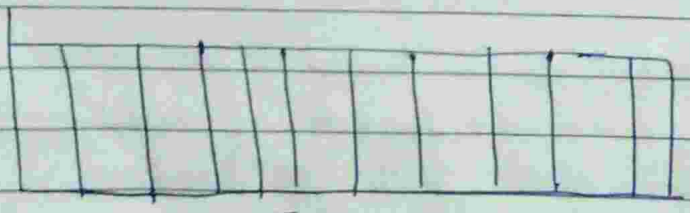
end-to-end resources allocated to reserved for call b/w source & destination.

* In diagram each link has 4 circuits.
  • call gets 2nd circuit in top link & 1st circuit in right link.
* dedicated resources : no sharing.
  • circuit like (guarnted performance)
* circuit segment idle if not used by call (no sharing)
  commonly used in traditional.

FDM versus TDM

FDM →

TDM



Internet

↳ structure : network of networks

↳ Infrastructure that provides services to various other application.

End systems connect to internet via access ISPs (Internet service providers)

Residential, company & University ISPs.

Access ISPs in turn must be interconnected so that 2 hosts can send packets to each other.

* Resulting network of networks is very complex.
* Evolution was driven by economics & national policies.
* Let's take a stepwise approach to describe current internet structure.

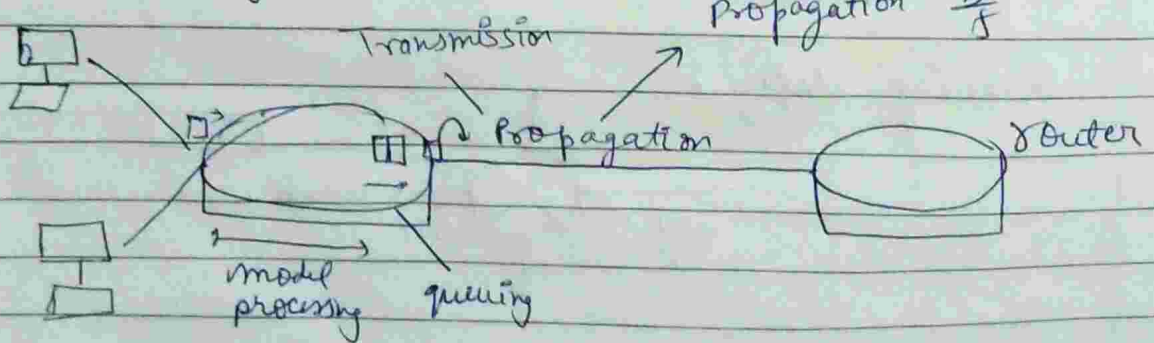
End-to-End delay

How do loss & delay occur.

packets queue in router buffers.

Packet arrival rate to link (temporarily) exceeds output link capacity. Packet queue, wait for turn.

4 sources of packet delay



Date:
Page:

$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$

d_{proc} : nodal processing
- check bit errors
- determine output link
- typically < msec

d_{queue} : queuing delay
- time waiting at o/p link for transmission.
- depends on congestion level of router.

Imp (1) Transmission Delay : To push all the packets present in router to the link.

$$L/R = \frac{\text{No. of bits just in a packet}}{\text{Transmission rate}}$$

→ bps.

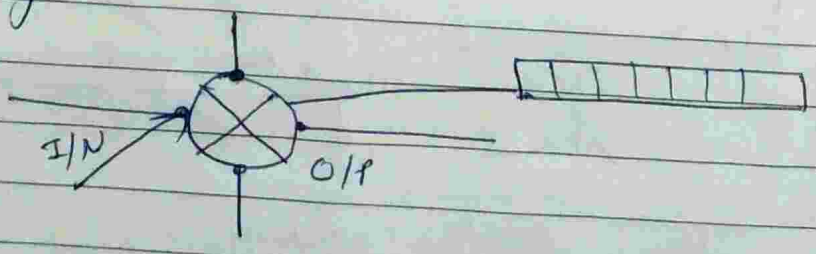
(2) Processing delay : Time required by a router to forward a particular packet from its input port to the output port is called processing delay.

Imp (3) Propagation delay :

So time required by a single bit of information to reach from this point to other point.

$$t = \frac{\text{dist}}{\text{speed}} \quad m \\ m/s$$

(4) Queuing delay :



(1) Network devices
(Router, hub, bridge, switch - - -)
(2) Transmission media in CNN.
(3) Topologies.

What is OSI?
What is TCP/IP?
Difference b/w OSI & TCP/IP?

Transmission Mode

(1) Simplex : Sender always sends & receiver always receives.

Keyword - sender
mention - receiver.

(2) Half Duplex Mode : first sender will send & receiver receives & after receiver will send & sender receives the msg / data.

(Walky Talky)

(3) Full Duplex Mode : Both sender & receiver will send & receive at the same time. (Phone)

transmission media.

(2) Data Linking - in form of frames.
LLC (handle error portion) like msg corruption.
MAC flow control

(3) Network - In form of Packets.

(4) Transport

(5) Session

(6) Presentation

(7) Application : Contains Data.

> Network must be able to need certain no. of category
> performance : (1) performance of network depends on no. of users.
Types of transmission medium : hardware & software.
(2) can be measured by transmit time & response time.

> Network Reliability : measured by frequency of failures, recovery time of network after failure & network toburthness.

> Security : protecting data from un-authorized access & viruses.

Types of connection → point to point multipoint.
Transmission mode : Simplex, Half Duplex, Full Duplex.
LAN, MAN, WAN.

(1) Physical layer : bit synchronization
Data rate
Topologies
Transmission modes.
Line configuration
representation of bits.

data loss
Simplex, Half, Duplex, Full Duplex.

(2) Data Link Layer : framing - divide the data in frames. & correcty errors.
physical addressing
flow control
error control
acess control.

(3) Network Layer : Routing logical addressing.

(4) Transport layer : Segmentation & reassembling.
Sevice point addressing.
connection control
Error & flow control.
connection con.

(5) Session layer : Dialogue control
Synchronization
session establishment
maintain & termination.

(6) Presentation layer : Translation.
used for file. encryption & decryption compression.

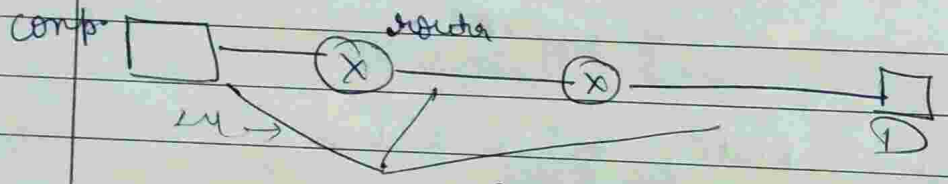
(7) Application layer : Mail services, Directory services.
file transfer acess & managment
& network virtual terminal.

The Physical layer is responsible for movements of individual bits from one hop (nodes) to the next.

End-to-End Delay numericals

Q- Msg size $= 8 \times 10^6$ bits
Trans. Rate $= 2$ Mbytes.
Transmission Delay $= L/R$.

Computer Network I



2Mbps $= 2 \times 10^6$ bits/sec
Msg size $= 8 \times 10^6$ bits.

(i) $TD = L/R = \frac{8 \times 10^6}{2 \times 10^6}$
$= 4$ sec.

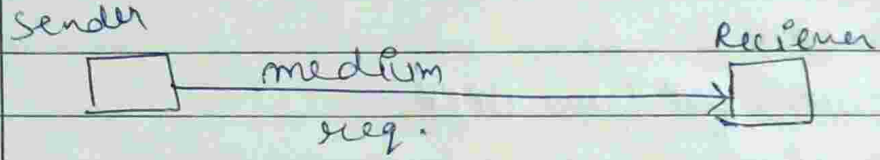
(ii) End to End $= 4R + L/R + 4R = 12$ sec.

Q- 300 Packet.
P. Size $= 10000$ bits/sec.
$\frac{8 \times 10^6}{800} = 10,000$ bits.

(i) $TD = L/R = \frac{10,000}{2 \times 10^6} = \frac{5000}{10^6} = .005$

(ii) first Packet = $\frac{100000}{2\times10^6} + \frac{100000}{2\times10^6} + \frac{10000}{2\times10^6}$

$= 3 \times \frac{10000}{2\times10^6} + 799 \times \left(\frac{10000}{2\times10^6}\right)$.



Protocol → set of instruction.

(1) Physical Layer -
is responsible for movements of individual bits from one node to the next.

(2) Data link -
is responsible for moving frames from one hop (node) to next

(3) Network
is responsible for delivery of individual packets from the source host to destination host.

(4) Transport layer
is responsible for delivery of a message from one proces to another.

(5) Session
is responsible for dialogue control & synchronization.

(6) Presentation layer
is responsible for Translation compression & encryption.

Page:

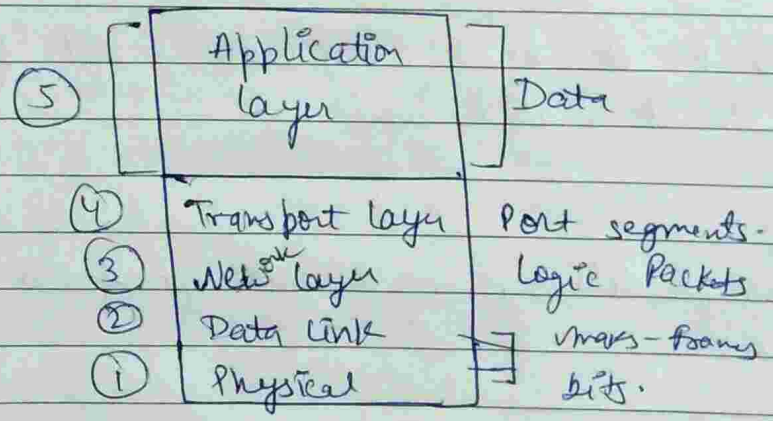
(7) Application Layer
is responsible for providing services to the user.

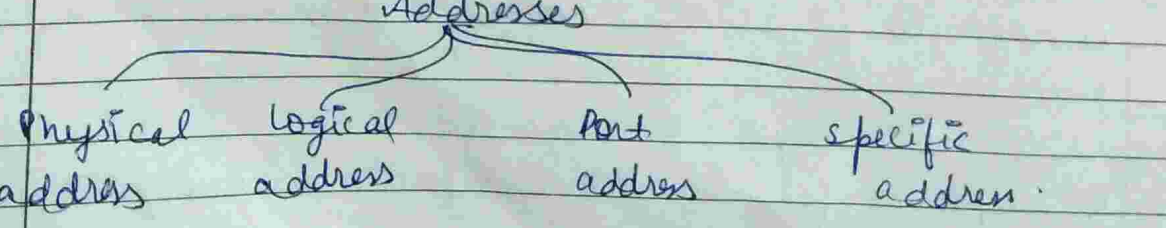
TCP/IP
↓
used in internet
TCP/IP - comes from ARPA.
Transmission/
TCP - Transfer control protocol (used for reliable communication)
IP - Internet Protocol.

end to end delivery:

dynamic : the path is decided by the router on the spot.

5 Layer

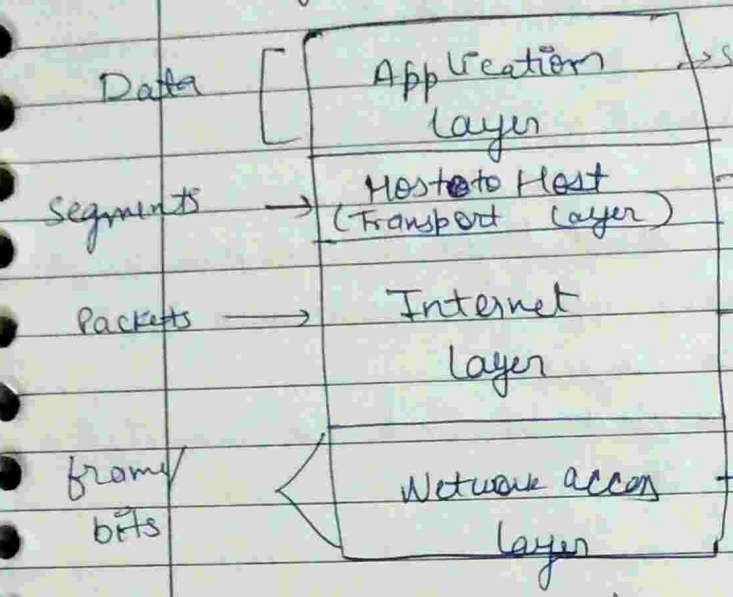




Page:

DNS (Domain name system)

4 layer TCP/IP



[all IP address are there in Packets]

[Port, some are fix & some are manually]

[Logical add. → IP add.]

transfer control

TCP → transport protocol

IP → Internet protocol

[for solving the problems like connect the people of two countries.

- ARPA
handled by American defence.

TCP/IP →

→ end-to-end verification

→ Dynamic Routing.

It should be end-to-end that only sender & receiver should be shown no b/w routes/nodes should be known.

Sender. Data . receiver

Dynamic routing should be there so that routes/nodes changes everytime, so that no one can attack on data.

TCP → used on non-real application.
UDP → " " real application e.g. vedio call.

Date:
Page:

- Application layer provides services to the end-u to work over the network or Internet.
  for eg → file transport.
  Protocols → HTTP, FTP, SMTP, Telnet.

- Transport layer / Host-to-Host layer is responsible transporting data & setting up communication b/w the application layer & lower layers.
  This layer is responsible for end-to-end communicat & error-free delivery of it.
  layer - TCP, UDP.

- Internet layer - defines the protocol which are responsible for logical transmission of data over the entire network (connection oriented). It is responsible for delivery packets from source host to the destination host by looking at the IP address in the packet header.

- Network Access layer - It is a combination of physical & data link of OSI & it looks out for hardware address or MAC Address.

END-TO-END Delay :

1- Transmission delay :
2- propagation delay :
3- Queuing delay :
4- Processing delay :

1- Transmission Delay - Time taken to put the data packet on the transmission link is called as transmission delay.

$$\text{Transmission delay} = \frac{\text{Length / size of data packet}}{\text{Bandwidth of network}}.$$

2- Propogation delay - Time taken for one bit to travel from sender to receiver on transmission speed is called propogation delay.

$$\text{Propogation delay} = \frac{\text{Distance b/w sender \& receiver}}{\text{Transmission speed}}.$$

3- Queuing delay - Time spent by the data packet waiting in the queue before it is taken for execution is called as queuing delay.
It depends on the congestion in the network.

4- Processing delay - Time taken by the processor to process the data packet is called as processing delay.
It depends on the speed of the processor.

by default 70 % $3 \cdot 8 \times 10^8$

Date:
Page:

End-to-end delay =
Transmission delay + Propagation delay + Queuing delay + Processing delay.

Ques- What is the propogation time if the distance b/w the two point is 12000 km & propogation speed $2 \cdot 4 \times 10^8$ m/s.

Sol $P.D = \frac{\text{Distance b/w two point}}{\text{speed}}$

$= 0 \cdot 5$ sec. / 50 millisecond.

Ques What is the end-to-end packet latency in this store & forward subnet from router 1 to router 8?
Assume: All links: 2.5Km ; C = 100Mbps (Bandwidth) ; propogation sped = 200 m/microsec ; queuing delay = processing delay = 0; packet size = 1000 byte.

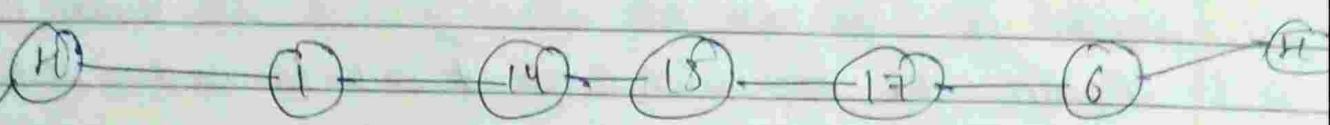
Sol link delay = PROC + QD + TRANS + PROP
= 0 + 0 + trans + prop.

$\text{transmission} = \frac{1000 \text{ byte}}{100 \text{ Mbps}} = \frac{8 \times 10^3 \text{ bit}}{10^8 \text{ bps}} = 8 \times 10^{-5}$
$= 80$ microseconds

$\text{prop} = \frac{2500 \text{ m}}{200 \text{ m/microsec}} = 12 \cdot 5$ microseconds.

link = 92.5 microseconds.
end-to-end subnet = $4 \times 92 \cdot 5 = 370$ microseconds.

Q- Refer the previous ques. with assumptions → when a packet from router 1 arrives at router 15 there are 3 packet in queued for the link to router 17.



trans. $= \frac{1000 \text{ bytes}}{100 \text{ Mbps}} = \frac{8 \times 10^3 \text{ bits}}{10^8 \text{ bps}} = 8 \times 10^{-5}$
$= 80$ microsecond
$= 80 \times 4 = 320$

prop. $= \frac{2500 \text{ m}}{200 \text{ m/micro}} = 12.5$ microsecond.
$= 12.5 \times 4 = 50.$

~~End to end 370 microseconds~~.

3 packet $= 80 \times 3 = 240$ microseconds.

as it is waiting on 15 & three packets are already in queue so, we have to multiply 80 by 3.

Q1- All links = 2.5 km , propogation speed = 200 m/micro
Bandwidth = 10 Mbps) queuing delay = processing delay = 0;
packet size = 1000 byte.

Q All links = 25 km , bandwidth = 100 Mbps and every thing same as 1

Q- processing delay = 10 microsec , packet size = 3000 bytes.
& every thing same as 1.

Q- Consider two host A & B connected by a link of rate R bps. Suppose that two host are separated by m meters and suppose the propogation speed along the link is s m/s. Host A is sends a packet of size L bits to host B.

i) Obtain the expression for end-to-end delay.

Processing = queuing time = 0.

End-to-End = transmission + propogation + queuing + processing.

= transmission + propogation.

$$\text{transmission} = \frac{L}{R}$$

$$\text{propogation} = \frac{m}{s}$$

$$\text{End-to-end} = \left(\frac{m}{s} + \frac{L}{R}\right) \text{sec.}$$

(i) given $s = 2.5 \times 10^8$ m/s.

$L = 120$ bits

$R = 56$ Kbps.

find the distance in case when transmission = propogation.

$$\therefore \frac{L}{R} = \frac{m}{s}$$

$$\frac{120}{56 \times 10^3} = \frac{m}{2.5 \times 10^8}.$$

$$\frac{120 \times 2.5 \times 10^8}{56 \times 10^3 \times 10} = 5.35 \times 10^5 \text{ m}$$

5.35×10^2 km

dist = 535 km.

Q2 (a) In modern packet-switched networks, including the Inter the source host segments long application-layer messages (for example, an image or a music file) into small packets & sends the packets into the network. The receiver then reassembles the packets back into the original message. We refer to this process as message segmentation. Consider a message that is 8×10^6 bits long that is to be sent from host A & B with two packet-switches in b/w. Suppose each link is 2Mbps. Ignore propagation, queuing & processing delays.

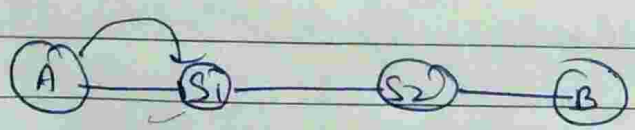
a) Consider sending the message from A to B without message segmentation. How long does it take to move the message from host A to first packet switch. Keeping in mind that each switches used store & forward packet switches.

(b) What is the total to move the money from A to B.

$$\text{Transmission delay} = \frac{8 \times 10^6}{2 \times 10^6}$$

$$= 4 \text{ sec.}$$

$$\text{Total} = 4 + 4 + 4 = 12.$$



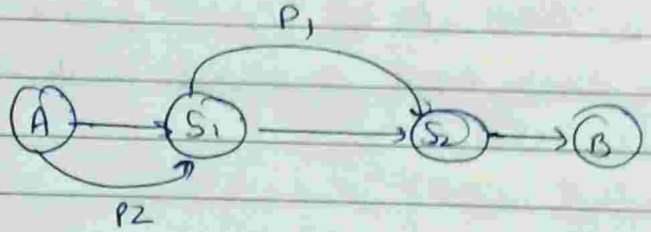
Date:
Page:

800

Q2- Suppose that the message is segmented into packets with each packet 10,000 width long. How long does it take to move the first packet from A to the first switch.
When the 1st packet is being send from the first switch to the second switch, the second packet is being send from A to first switch? What time will the second be freely received at the 1st switch?

Sol Transmission delay = $\frac{10,000}{2 \times 10^6} = \frac{1}{200} = 0.005$ sec.

= 5 millisec



Time taken by packet 2 = 0.005 + 0.005
= 0.010 sec
= 10 millisec.

Q3- How long does it take to move the file from A to B, when message segmentation is used.

Sol for P_1 = 15 millisec

for 799 = 799 × 5 = 3995 millisec.

For 800 packet = 3995 + 15
= 4010 millisec.

Q- We consider sending real-time voice from Host A to Host B over a packet-switched network (VoIP). Host A converts analog voice to a digital 64kpbs bit stream on the fly. Host A then groups the bits into 56-byte packets. There is one link b/w Host A & B, its transmission rate is 2Mbps & its propagation delay is 10 msec.
As soon as Host B receives an entire packet. It converts the packet's bit to an analog signal. How much time elapses from the time a bit is created (from the original analog signal at Host A) until the bit is decoded (as part of the analog signal at Host B)?

Sol. Transmission delay = $\frac{56 \text{ byte}}{2 \text{ mbps}}$ = 28

$= \frac{56 \times 8 \text{ bits}}{2 \times 10^6 \text{ bps}}$ $= 28 \times 8 \times 10^{-6}$

$= 224 \times 10^{-6}$

= 224 microseconds.

propagation delay = 10 msec.

a) Consider the 1st bit in a packet, before this bit can be translated all of the bit in the packet must be generated which require time.

Processing $\frac{56 \times 8}{64 \times 10^3}$

7×10^{-3} = 7 msec.

T_o = Transmission + prop + process

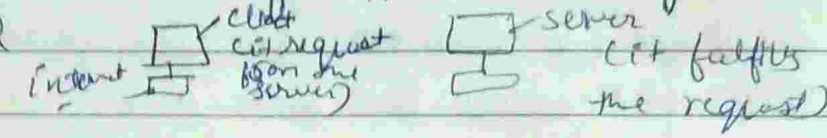
= 224 Nsec + 10 msec + 7×10^{-3}.

UDP - User data Protocol.

Date:
Page:

Q- What are the main function of Application layer?

Q. Client - server model



★ Domain Name System (DNS) (Application layer)
(client/server)

main function is To mapping the Domain name with IP address.

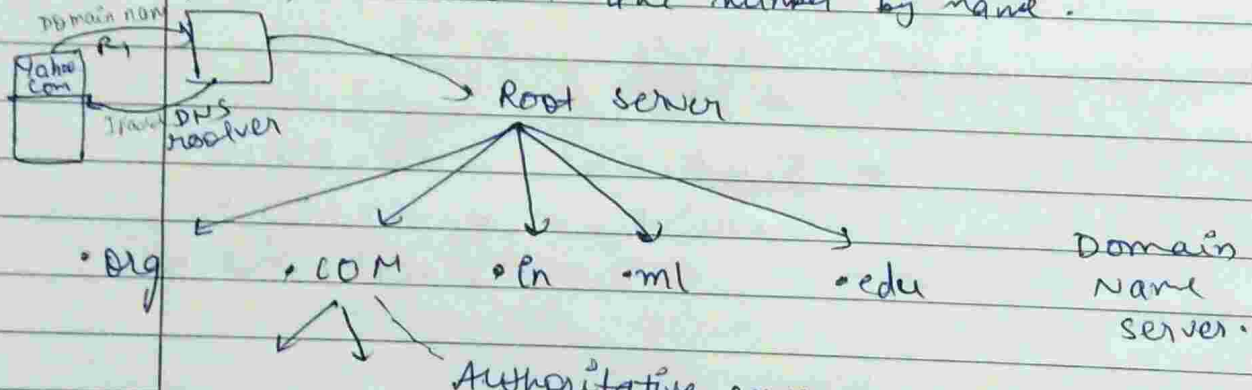
port-no 53] (Client-server model)

DNS works on application layer.

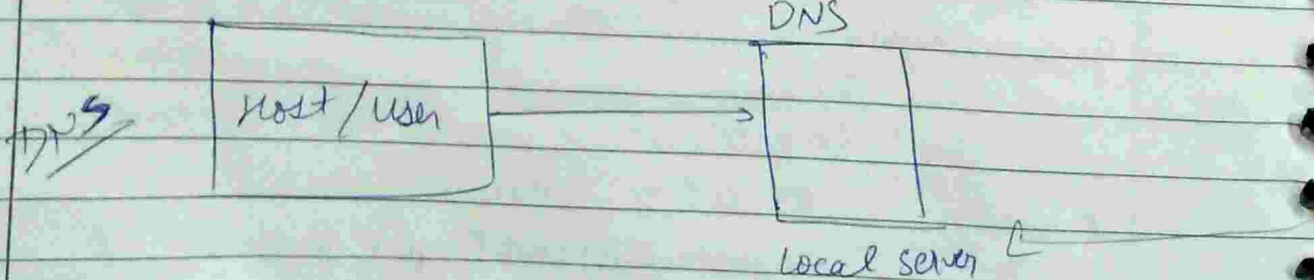
Domain name system used to map the Domain name with the IP address.

Because its very difficult to remember IP address but easy to remember domain name.

Domain name provides us the IP address just like in phone, we search the number by name.



works on Transport layer. DNS uses UDP as UDP works faster than TCP.



1) Root name server
2) Top level server / Domain name server
3) Authoritative server

1) Root name server.
It is contacted by name servers that can't resolve the name, it contacts authoritative name server if name mapping is not known it then gets the mapping & retu -rns the IP address to the host.

2) Top level server / Domain name server
They have inf. about authoritative domain servers & know names & IP addresses of each authoritative name server for the second level domain.

3) Authoritative server -
Providing authoritative post name to IP mapping for organisation servers. It can maintained by organisation & service provider.

4) Components of DNS
Domain Name
Name Space
Name server
Name resolver

Inverse Domain
Mapping
IP to
URL

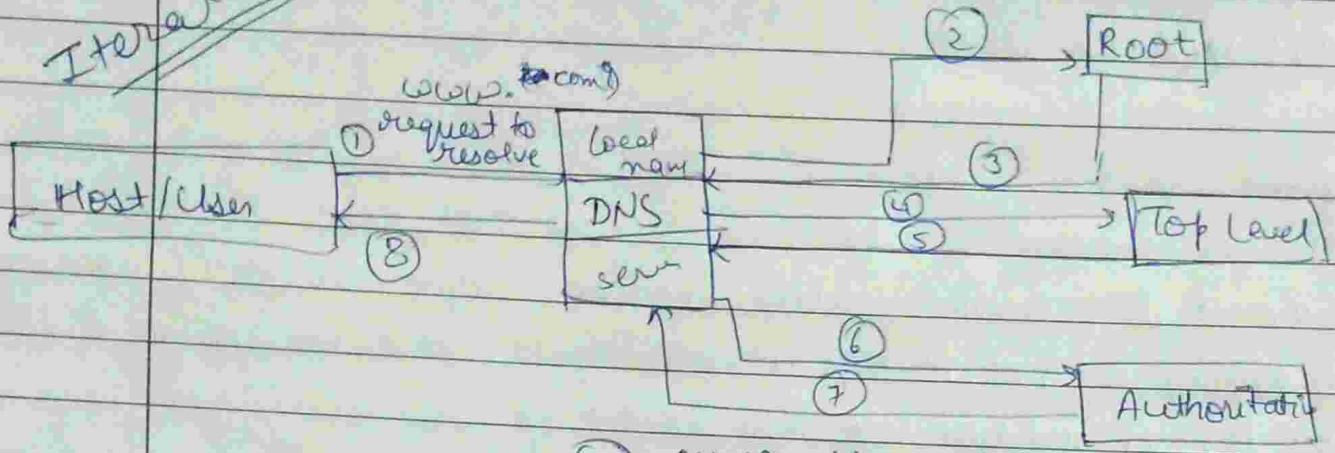
Country Domain
• in
• ca

Generic Domain
• com
• org
• edu

execution

flat / heirarchal structure

Iterative



(3) All IP address of name server authoritative for the top level domain .in

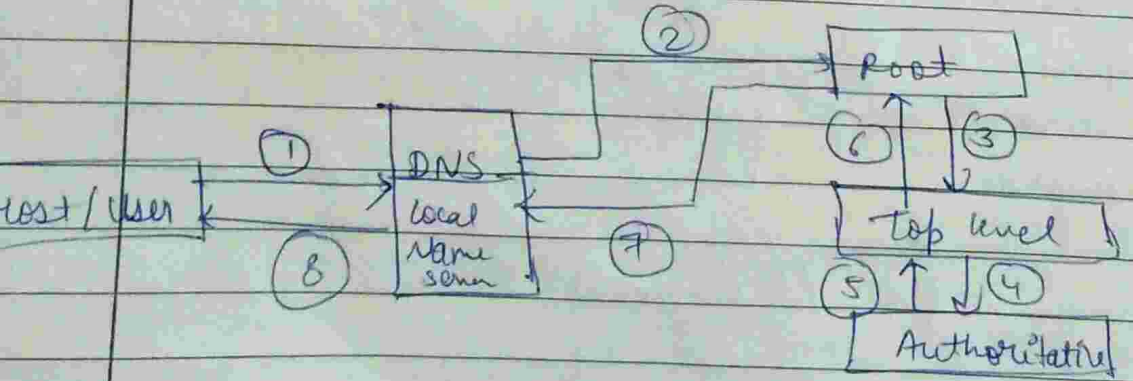
(5) All IP address of name server authoritative for the domain www.

(7) IP address for the domain (www. server)

(8) IP address (e.g. 192.168.1.1)

Queries 2 type of
i) recursive
ii) Iterative

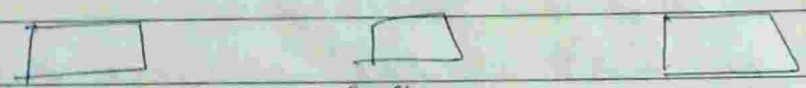
recursive

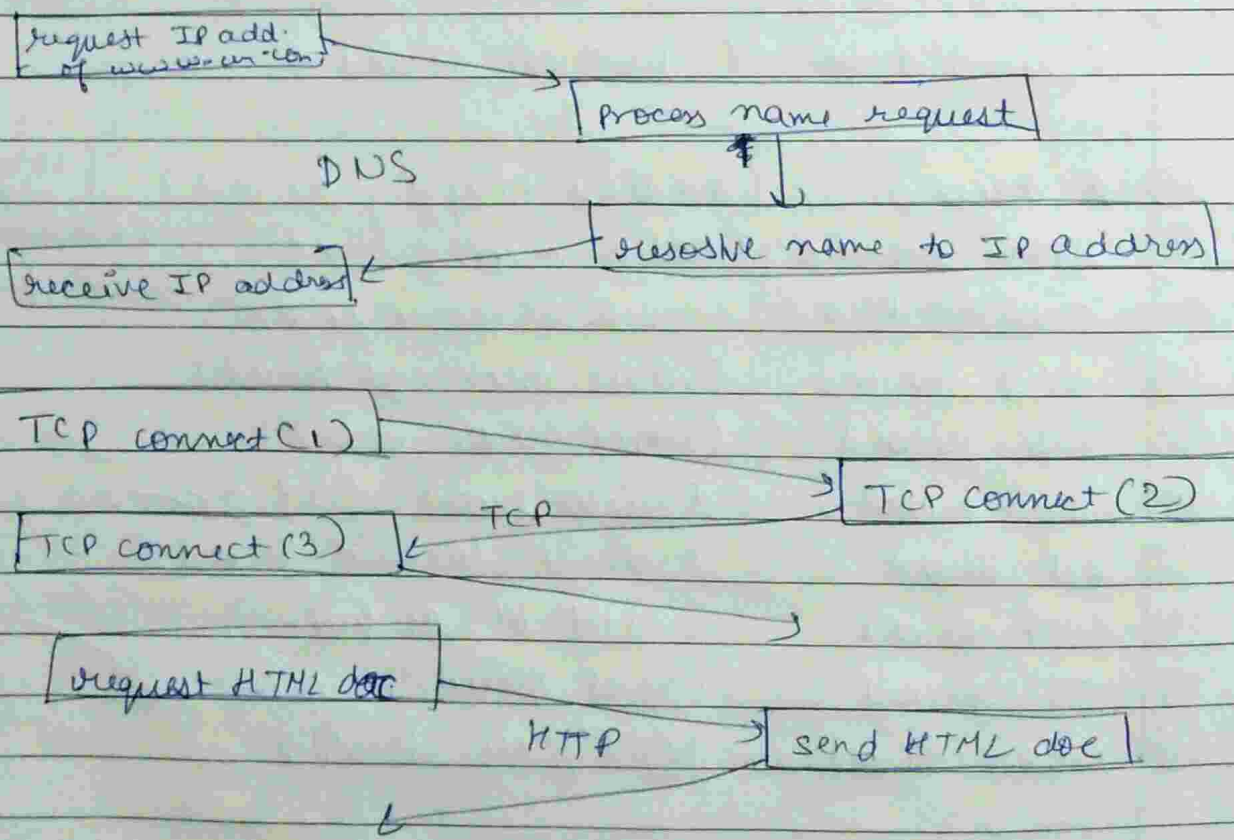


Example 1 (P3)

Consider an HTTP client that wants to retrieve a Web document at a given URL. The IP adress of the HTTP server is initially unknown. What transport & application layer protocols besides HTTP are needed in this scenario?

Sol Application layer protocols : DNS & HTTP
Transport layer protocols : UDP for DNS ; TCP for HTTP.





Date:
Page:

DNS Resource Record

- Name,
- value,
- class ⟶ IN
- Type
- TTL

Name, value depends on Type.
TTL - is Time to live of the resource record, it determines the time at which a resource record should be removed from the cache.

Different types of Resource Record :

1. A record (Address mapping record). [IPV4 address — Internet Protocol]
2. AAAA record (Address mapping record) (IPV6 address)
3. CNAME Record (canonical name record) → indicate domain to domain
4. MX Record (mail exchanger record)
5. NS Record. (Name server record)
6. PTR Record. (pointer record) (IP & Domain name)
7. SRV Record (servile location record).
8. SOA Record (Start of authority)
9. Txt record (Text record)
10. CERT Record. (certificate record)

→ CNAME allow using diff. name for the same record.
→ MX → used for mapping a DNS domain name to a mail server & used to route outgoing mails to

an email server.

→ NS specifies DNS zone such a
dedicated to a specific author
& it provide the address of that

→ PTR used to reverse from IP d

→ SRV used to map all available ser

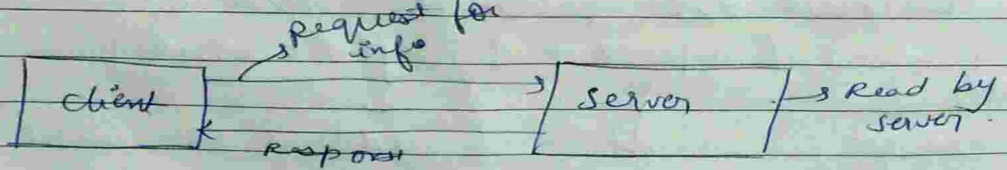
→ SOA appears at the beginning of DNS z
indicates the authoritave name server
current DNS zone & all other inform
zone.

→ Txt - Typically carries the machine rea

→ CERT → It stores the encryption certi

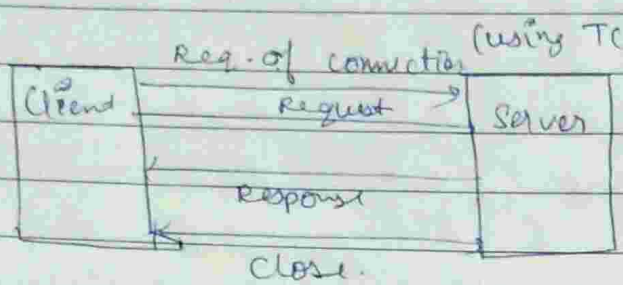
HTTP (Hyper Text tranfer Protocol) (mainly usi
↓
port no → 80 / working on Application layer.

The purpose of HTTP is to transfer hyper medi
document is HTTP.
Port no. used is 80.



Date:
Page:

Working / HTTP Transaction



There are 4 components →

① → Request of connection (using TCP)
② → actual request
③ → response
④ → close

(1) http://xyz.com
↳ 192.168.0.2:80 [DNS]

The client program connects to a server by a TCP TCP connection at address specified by url.

(2) request

HTTP Request — Simple HTTP Request — Full Request

Simple request is just single GET line naming the page desired without the protocol version.

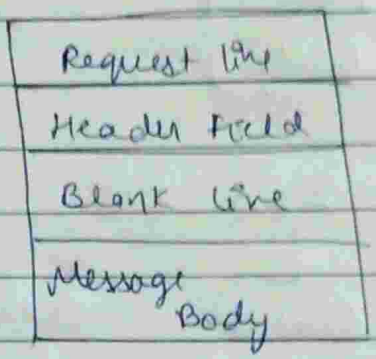
e.g → GET / Hypertext / Project.html

- GET → request method
- Hypertext → Protocol without version.
- Project.html → address of web/ requested page.

full request - it include version also.
→ contains the command page desired & the protocol with version.

e.g → GET / home.html / HTTP/1.1

- GET → req. method
- /home.html → address
- HTTP/1.1 → Protocol with version



Request line

Request type : GET / move / delete / trace.

Resource : url is used to access inf. from the internet

HTTP version :

http://www.xyz.com/home.html

http	Protocol
www	Sub-domain name
xyz	domain-name
com	top-level domain
home.html	File Path

e.g. http://192.162.1.2:80/home.html

- http → Protocol
- 192.162.1.2 → host
- 80 → port
- /home.html → Path.

Date:
Page:

(3) Response

Once the server receive the http request from the client, it return http response.

Status line
header field
Blank line
Message Body

e.g. HTTP/1.1 200 OK

- HTTP/1.1 → http version
- 200 → Status code
- OK → Status Phrase.

eg. 301 - moved permanently (request object move)

200 OK → (request succeed).

400 → bad Request → request msg. is not understood by the server.

404 (not found) → request document is not found on server.

505 (http version not supported) → request http version not supported).

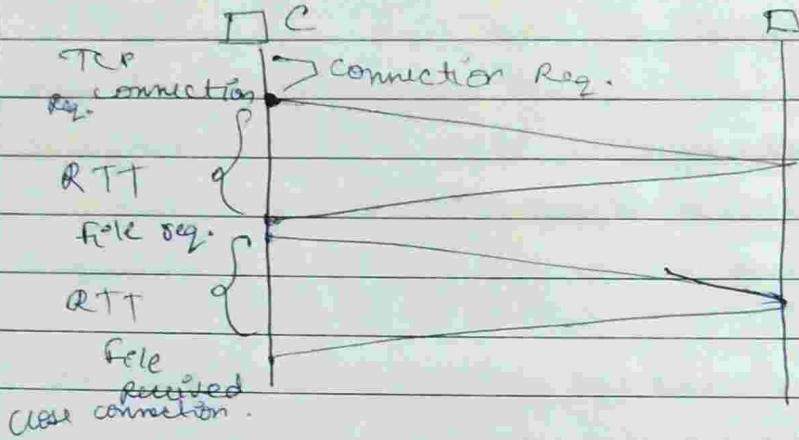
(4) Close → after the client & server has exchanged the inf. by sending the request & response, both parties may end transaction by closing the connection.

diff. b/w OSI & TCP (or) Model & switching (or)
circuit switching & Packet switching (or)
Persitent & non-Persitent.

Date:
Page:

Round Trip Time (RTT)

A Time for a small packet to travel from client to server & server to client.



$RTT = T_p + T_p$
$\approx 2 \times T_p$

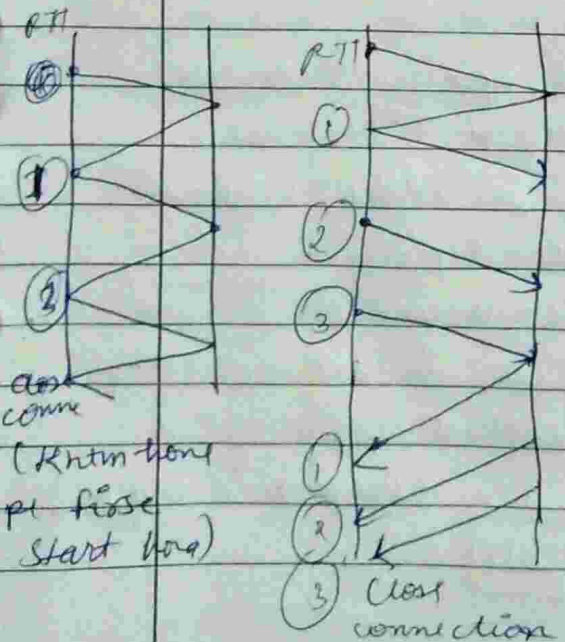
HTTP Response time = RTT + RTT + file

M.1: Persitent and non-Persitent

Persitent → object
11 = 12 RTT.

non-Persitent → object
11 → 22 RTT

Without pipelining | With pipelining



Date:
Page:

HTTP Headers -

1) Host Header
2) User agent Header
3) Except Header
4) Authorisation Header
5) Proxy Authorisation Header
6) Connection Header
7) if - MATCH Header
8) if - NONEMATCH Header
9) if - MODIFY-SINCE Header
10) if UNMODIFY-SINCE Header

If Yes, status 200
If No, status 304.

Types of headers :-

1) General header (Host, User agent Header)
2) Request header (Authorisation Header ne request kiya)
3) Response header (Authorisation Header ne respone kiya)
4) entity header (for meta header)
5) Cache Control Header → Used to specify browser caching policy in both client request & response. Policies includes how a resource is cache, where it is cache, the maximum age before expiring.

Parts of Cache Control Header (Header used for response & request).

5.(1) Cache-Control MAX-Age - defines in seconds the amount of time it takes for a cached copy of a resource to expire. (Response & Request)

Cache Control : MAX Age = 180

5.2 Cache-control : Nocache - (response & request)
means browser may cache a respons but first submit a validation request to the origin savice.

5.3 Cache-control : No store - (response & Req)
the browsers are not allowed to cache a response & must pull it from server each time it is requested.

5.4 Cache-control : Public - (Response only)
it indicates that a store can be cached by ~~any kind of~~ only ~~method. (public or private)~~ public method.
Basically indicates that response can be stored in a shared cache.

5.5. Cache-control : Private (Response only)
indicates that a resource is user-specific but it can still cash but only on client device.

5.6 Cache-control : must-Revalidate (Response only)
indicates that the response can be stored in cache & can be used while fresh, if not must be validate with the origin server before use.

5.7 Cach-control : only if cache (Request only)
the client indicated that cach should obtain an ~~only~~ already cache response if a cache has stored a response, it is reused.

E-mail

1. User Agent → Mail Reader
2. Mail Server (store the data)
3. SMTP (Simple Mail Transfer protocol) → Port no - 25 with TCP connection

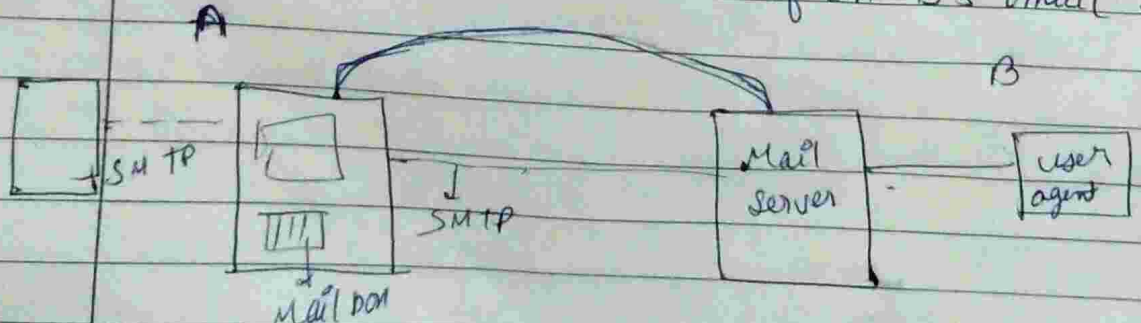
POP3 (Post office Protocol)

Mail functioning -

1) Composition
2) Displaying
3) Reporting
4) Transfering
5) Disposition.

Explain SMTP

Step 1) A user agent to compose message to b@gmail.com
Step 2) A's user agent sends message to his mail server & that message placed in message queue.
Step 3) A's mail server SMTP open TCP connection with B's mail server. (Port no 25, TCP connection)
Step 4) SMTP sends A's message over the TCP connection.
Step 5) B's mail server places the messages in B's mail box.
Step 6) B's user agent access mail from B's mail server.



Date:
Page:

E-

(1) HELO/EHLO [For extension SMTP → EHLO is used otherwise HELO is used]
It is used to initiates the session.
Argument passed in this is domain server.

(2) RCPT TO
Argument passed in this is address of receiver.
(abc@gmail.com) or destination mail box.

(3) MAIL FROM
Argument passed is the address from where the mail is originated.

(4) DATA - (354) positive
(450, 451, 550, 503, ---) negative.

(5) NOOP - (No operation) & (250 OK response) -
It checks whether the server is responding or not.
No argument are passed.

(6) VRFY (verify) - whether the mail box in the argument exists or not.

(7) EXPN - specify the mailing list to be expanded.

(8) RSET - Reset the SMTP connection.

(9) HELP

(10) QUIT - terminate the SMTP session once the server respons to 221, client closes the SMTP connection.

(11) AUTH - used to authenticate client to the server.
(235, 334 positive response)

(12) TURN/ATRN
TURN: reversing the role of sender & receiver.
ATRN: basically it provide the additional feature of authentication.
and it is also available for dynamically assigned IP address.

(13) SEND - It send mail to the terminal

(14) SOML - It send mail to the terminal if possible otherwise to mail box.

(15) SAML - send mail to terminal & mail box.

* 3-digits codes (These are the commands & we get the positive & negative respond).

220 - positive respons / 554 - negative response
↓ ↓
code from 2 or 3 code from 4 or 5

For eg → HELO command → negative 451
positive 250 respons " 452
becs it starts with 2 " 455
" 503
" 550

AUTH	DATA	
235 positive	354	450, 451, 503, 550
334	(positive)	(negative)

QUIT - 221 (positive)

VRFY - 250, 251, 252 (positive)
502, 504, 550 (negative)

HELP - 211, 214 (positive)
502, 504 (negative)

POP (Post office Protocol)

1) Mail Access protocol
It is used to transfer e-mail from a mail server to client software. Port no is 110 with TCP connection.

2) Mail sending Protocol

3 Phases -
① Authorization
② Transaction
③ Updation.