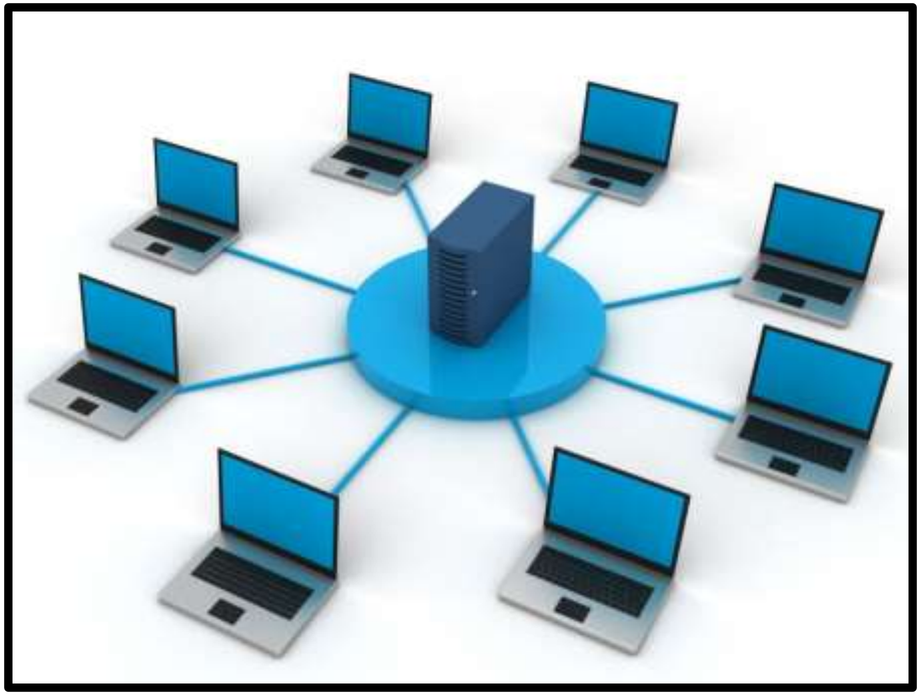
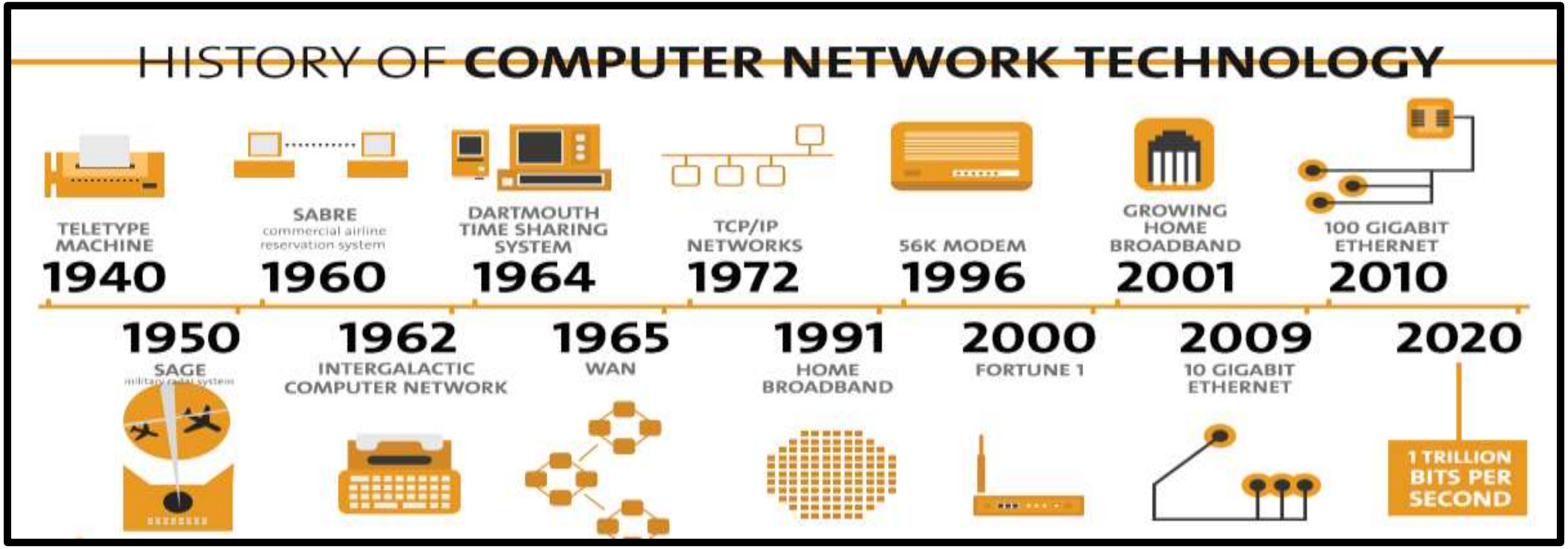
CN - DEFINITION

✓ A **computer network** is a group of **computers** that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the **network** nodes.



HISTORY



HISTORY OF COMPUTER NETWORK TECHNOLOGY

TELETYPE MACHINE 1940

SAGE military radar system 1950

SABRE commercial airline reservation system 1960

INTERGALACTIC COMPUTER NETWORK 1962

DARTMOUTH TIME SHARING SYSTEM 1964

WAN 1965

TCP/IP NETWORKS 1972

HOME BROADBAND 1991

56K MODEM 1996

FORTUNE 1 2000

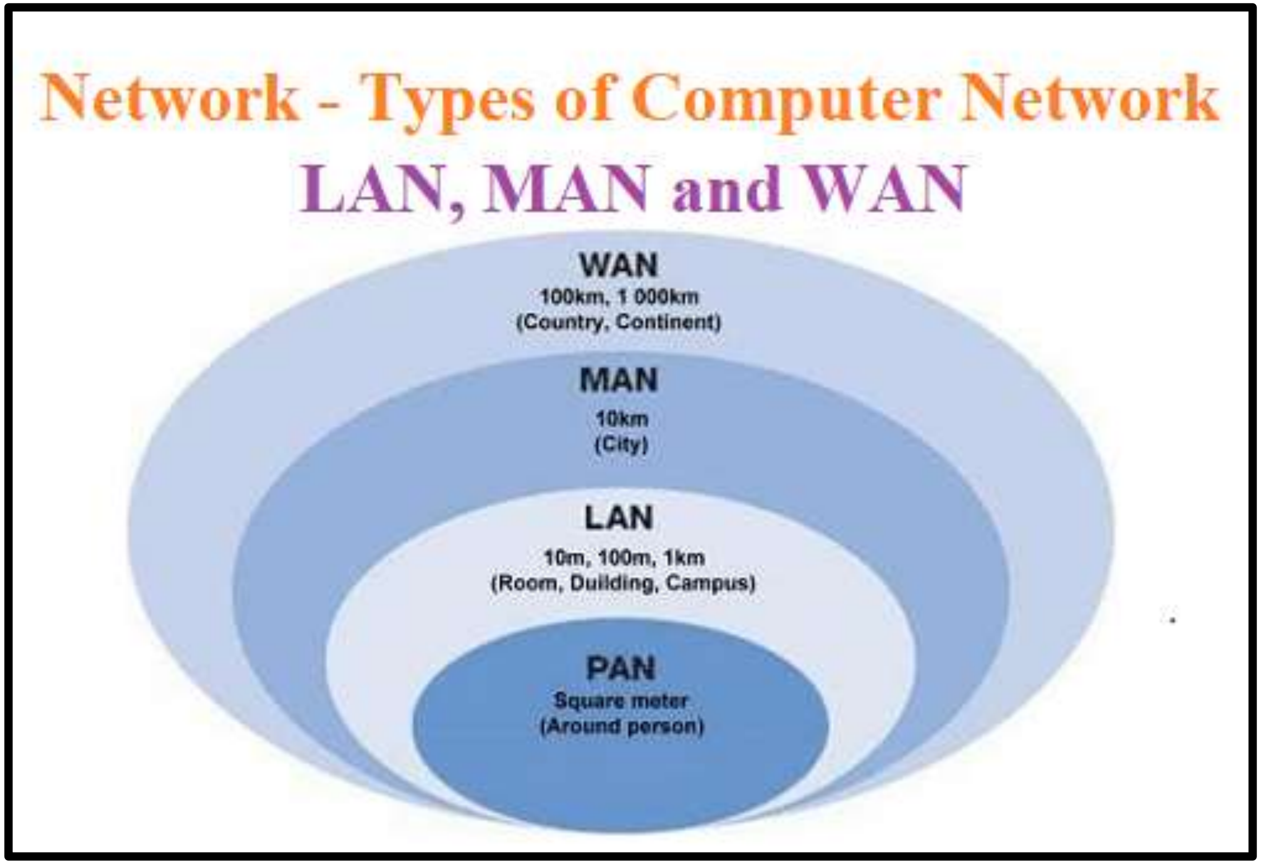
GROWING HOME BROADBAND 2001

10 GIGABIT ETHERNET 2009

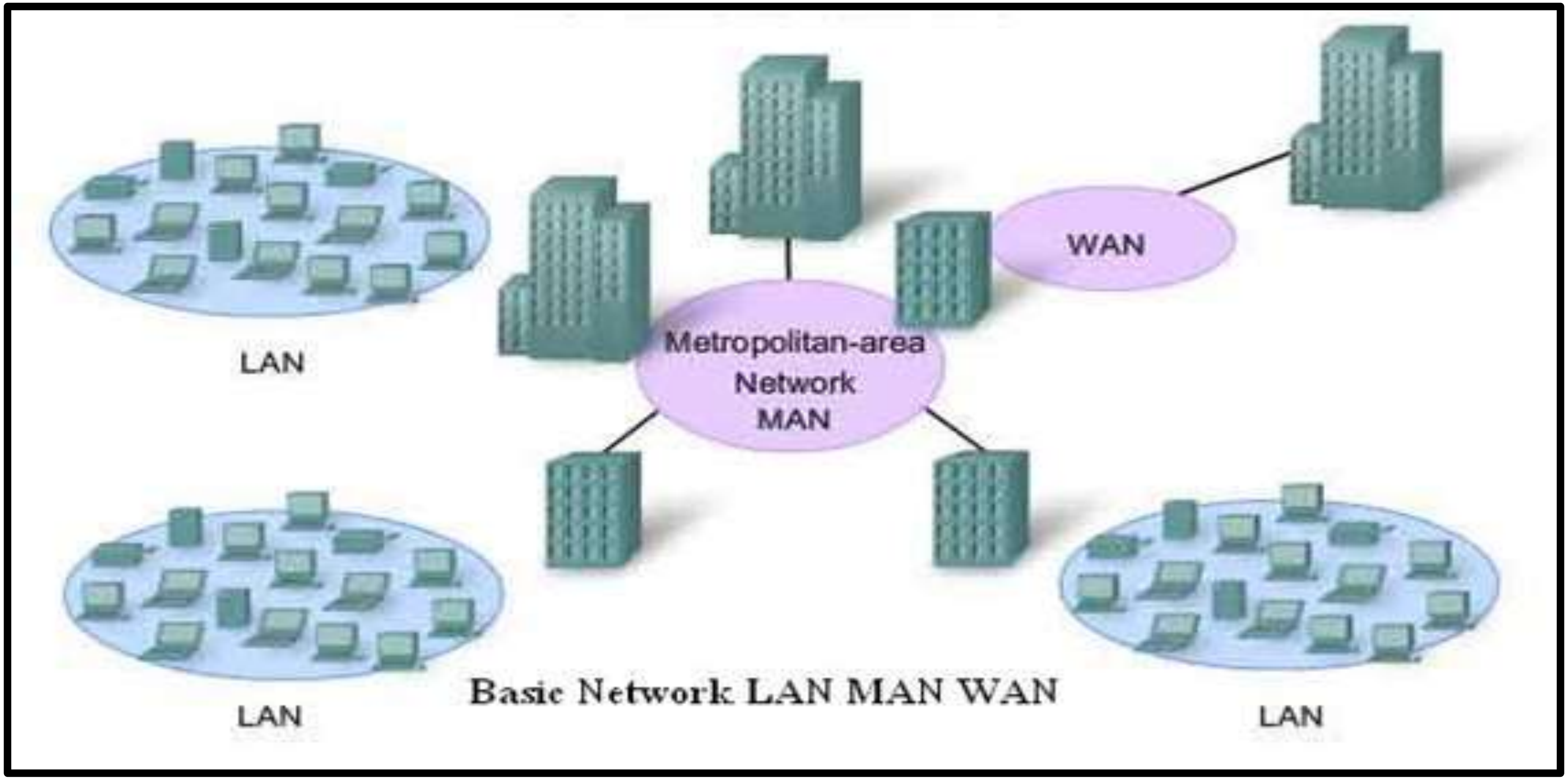
100 GIGABIT ETHERNET 2010

2020 1 TRILLION BITS PER SECOND

LAN MAN WAN

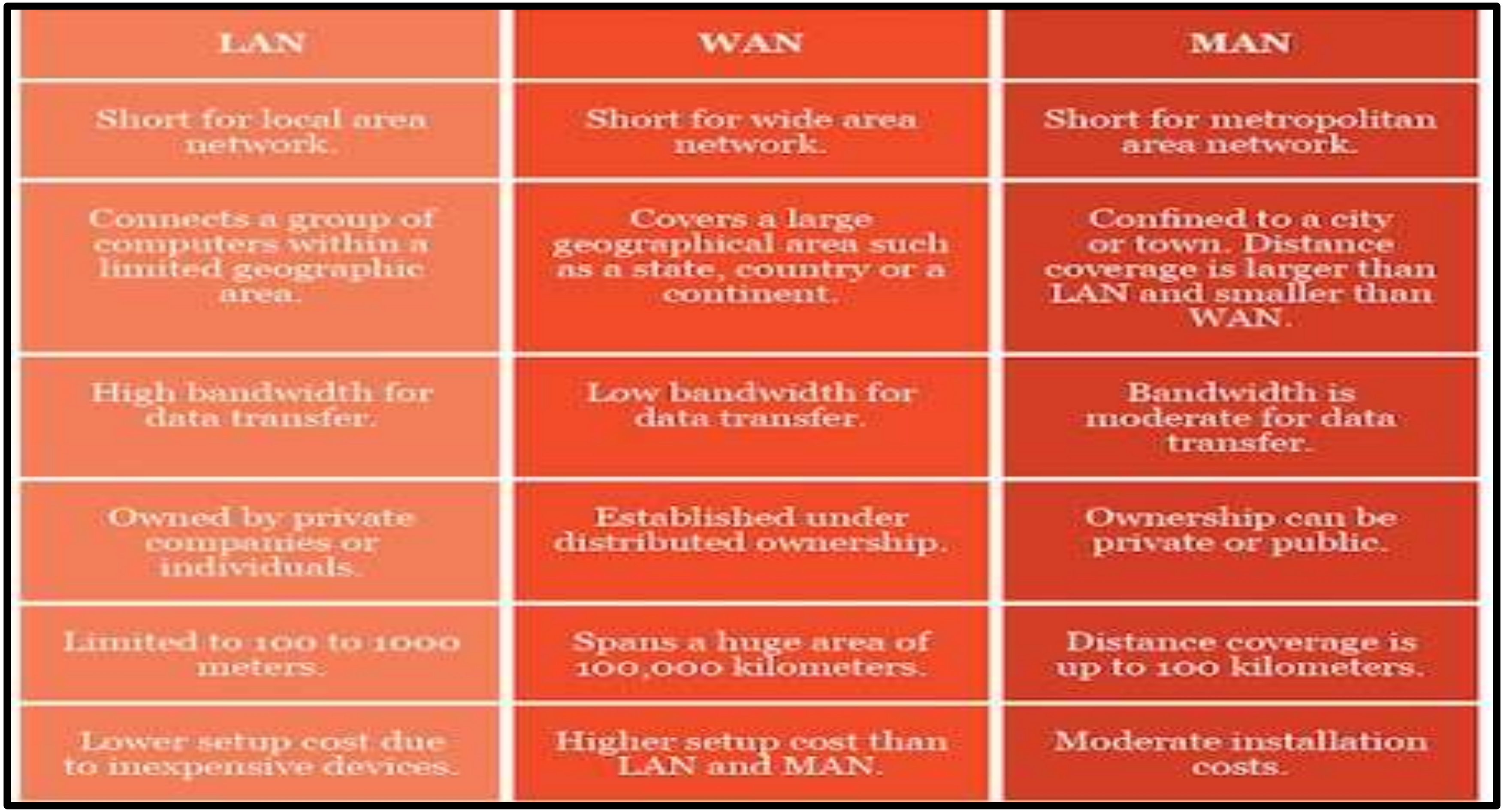

Network - Types of Computer Network
LAN, MAN and WAN
WAN
100km, 1 000km
(Country, Continent)
MAN
10km
(City)
LAN
10m, 100m, 1km
(Room, Duilding, Campus)
PAN
Square meter
(Around person)

LAN MAN WAN



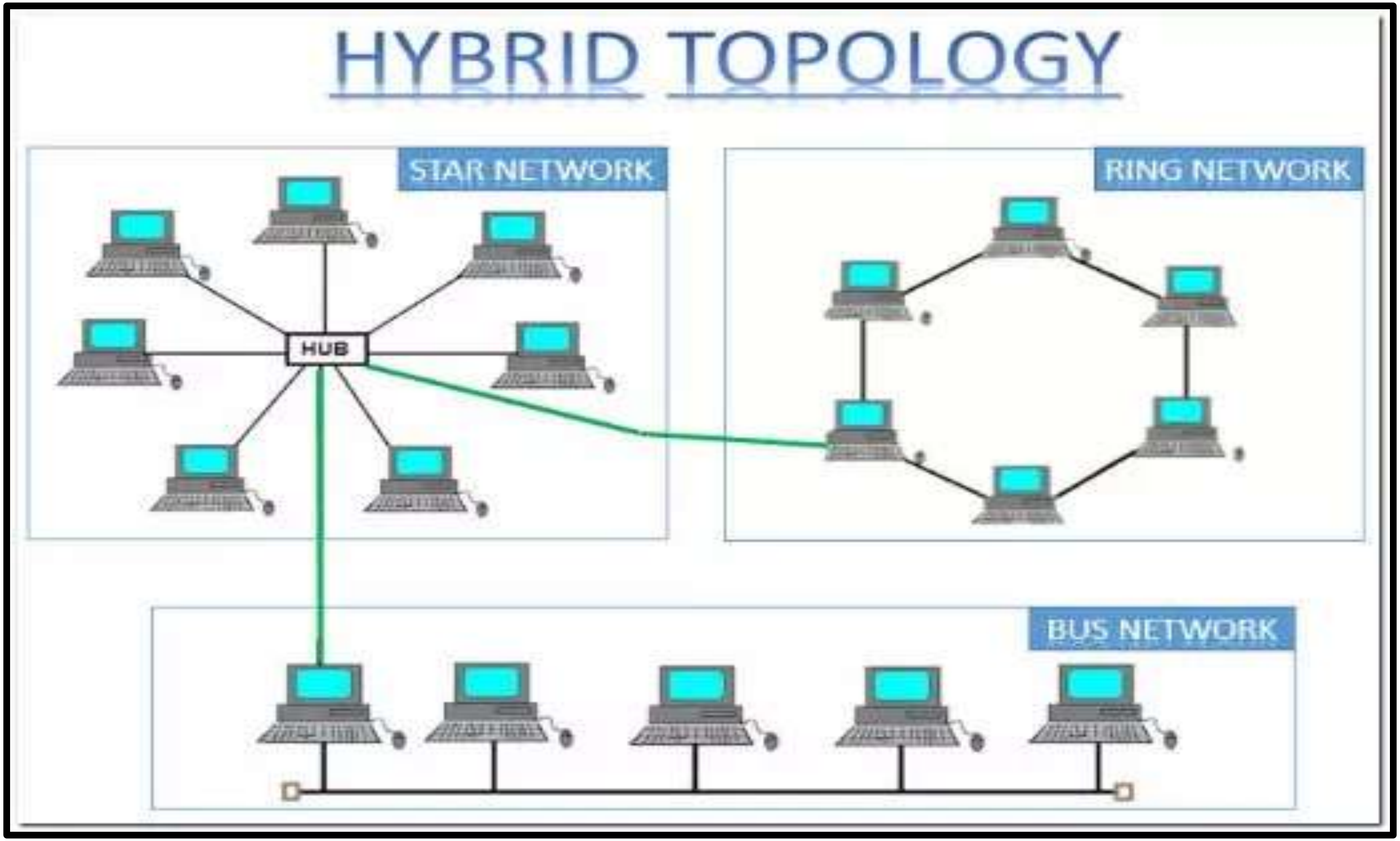
Basic Network LAN MAN WAN

LAN MAN WAN

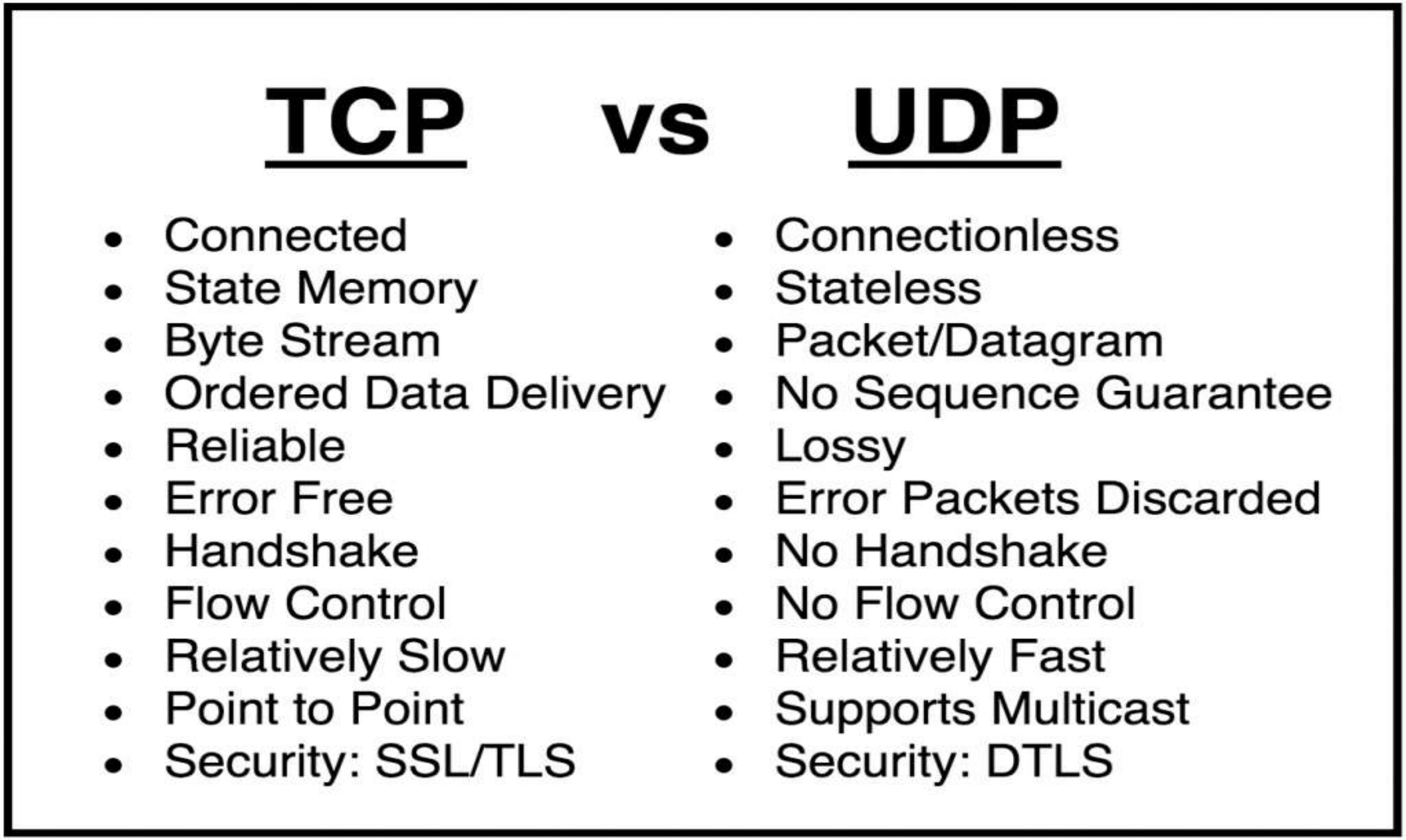


LAN	WAN	MAN
Short for local area network.	Short for wide area network.	Short for metropolitan area network.
Connects a group of computers within a limited geographic area.	Covers a large geographical area such as a state, country or a continent.	Confined to a city or town. Distance coverage is larger than LAN and smaller than WAN.
High bandwidth for data transfer.	Low bandwidth for data transfer.	Bandwidth is moderate for data transfer.
Owned by private companies or individuals.	Established under distributed ownership.	Ownership can be private or public.
Limited to 100 to 1000 meters.	Spans a huge area of 100,000 kilometers.	Distance coverage is up to 100 kilometers.
Lower setup cost due to inexpensive devices.	Higher setup cost than LAN and MAN.	Moderate installation costs.

HYBRID TOPOLOGY

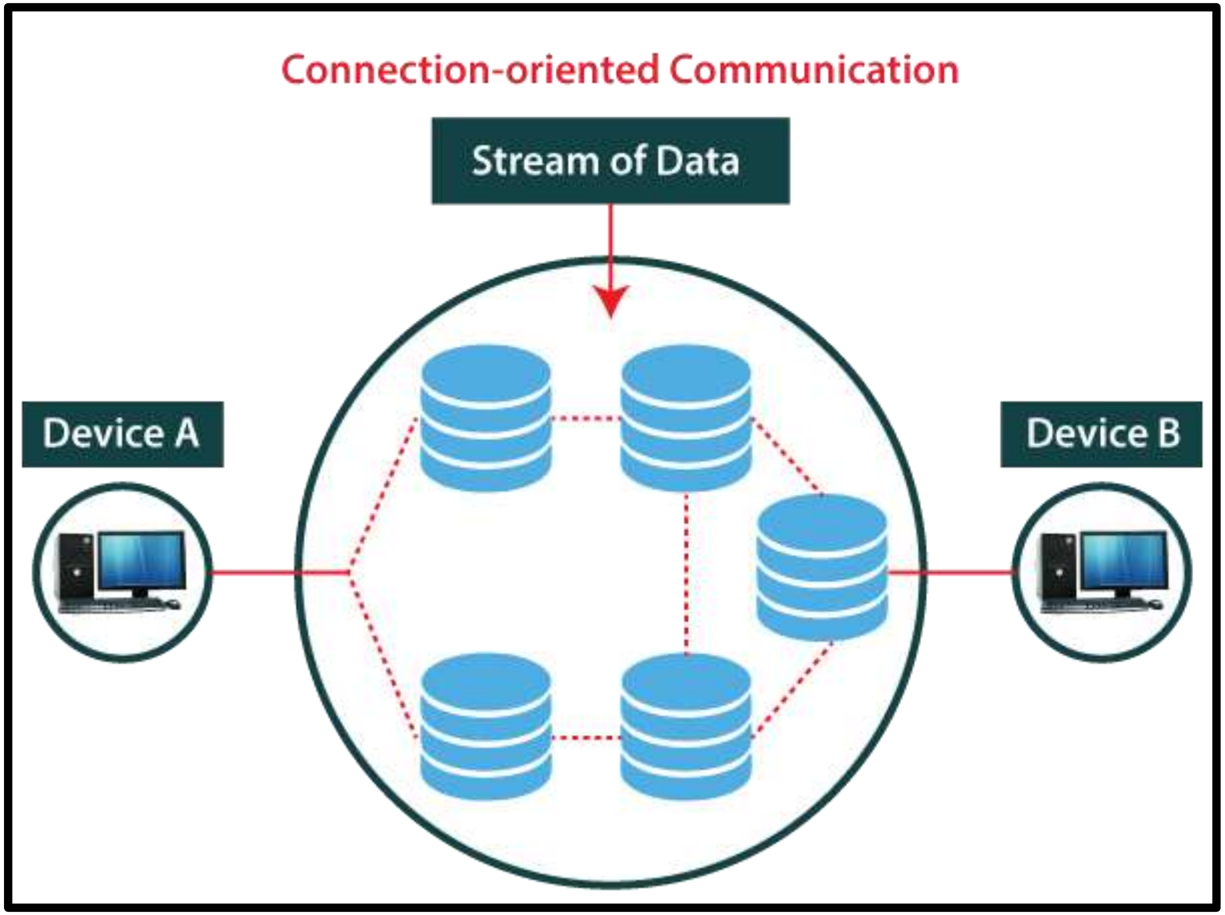


TCP & UDP

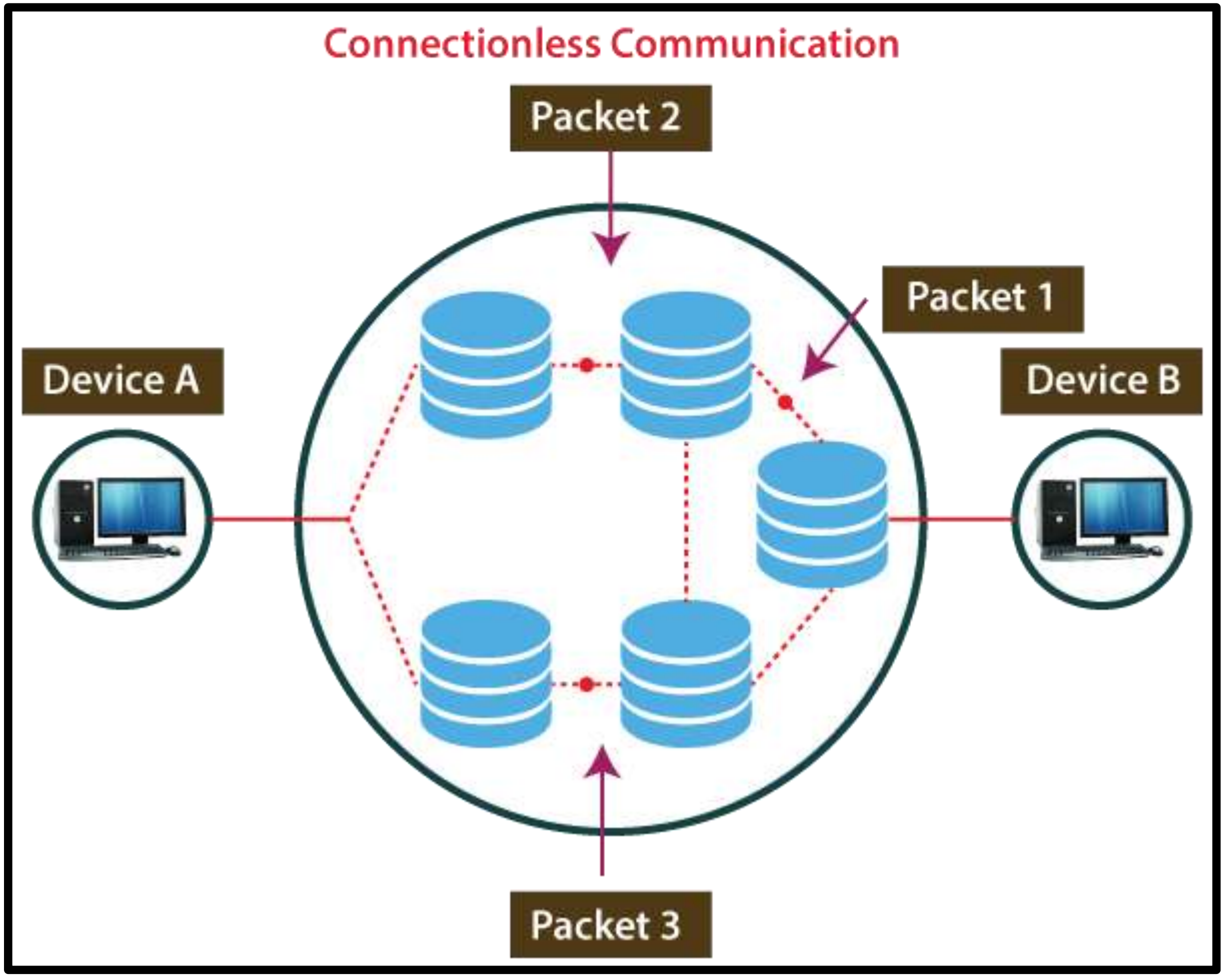


TCP	vs	UDP
Connected		Connectionless
State Memory		Stateless
Byte Stream		Packet/Datagram
Ordered Data Delivery		No Sequence Guarantee
Reliable		Lossy
Error Free		Error Packets Discarded
Handshake		No Handshake
Flow Control		No Flow Control
Relatively Slow		Relatively Fast
Point to Point		Supports Multicast
Security: SSL/TLS		Security: DTLS

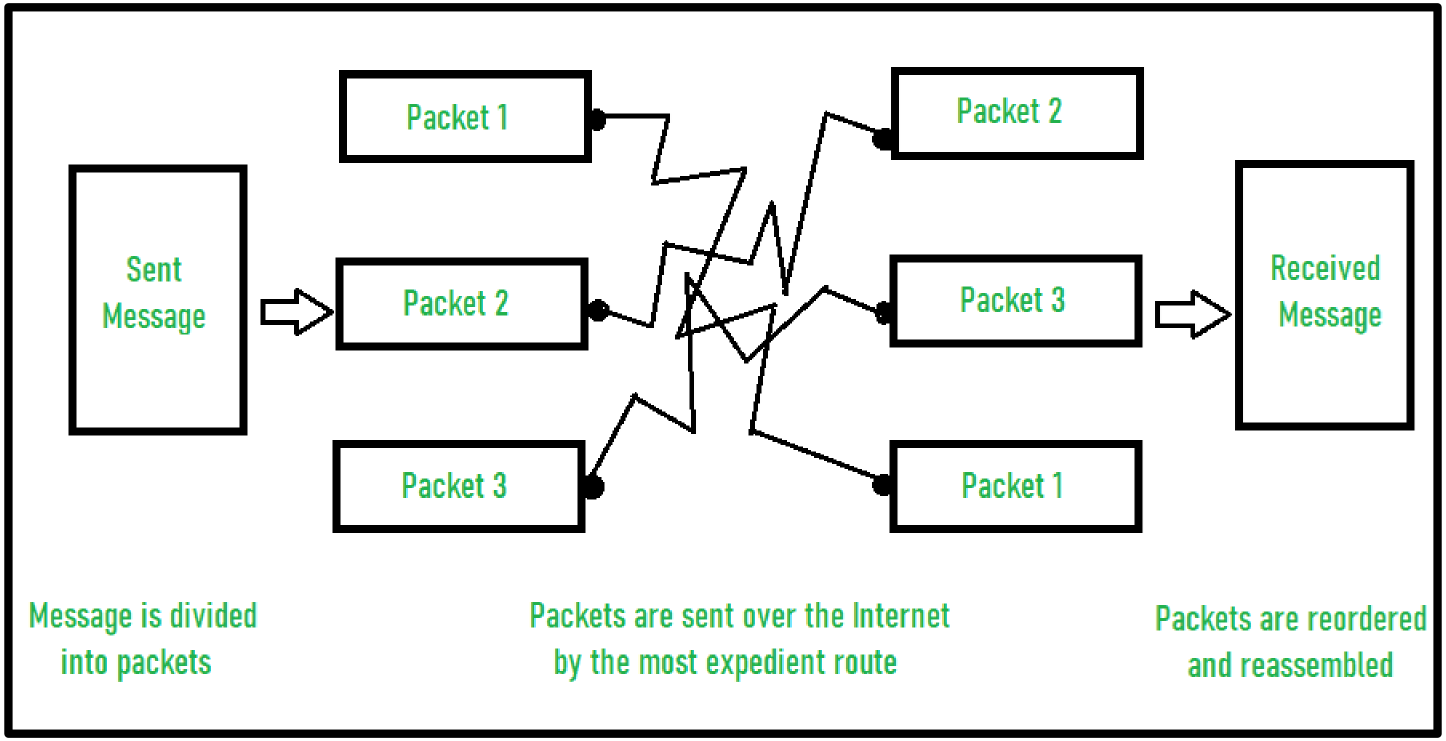
TCP & UDP


Connection-oriented Communication
Stream of Data
Device A
Device B

TCP & UDP


Connectionless Communication
Packet 2
Packet 1
Device A
Device B
Packet 3

PACKET SWITCHING



Sent Message

Packet 1

Packet 2

Packet 3

Packet 2

Packet 3

Packet 1

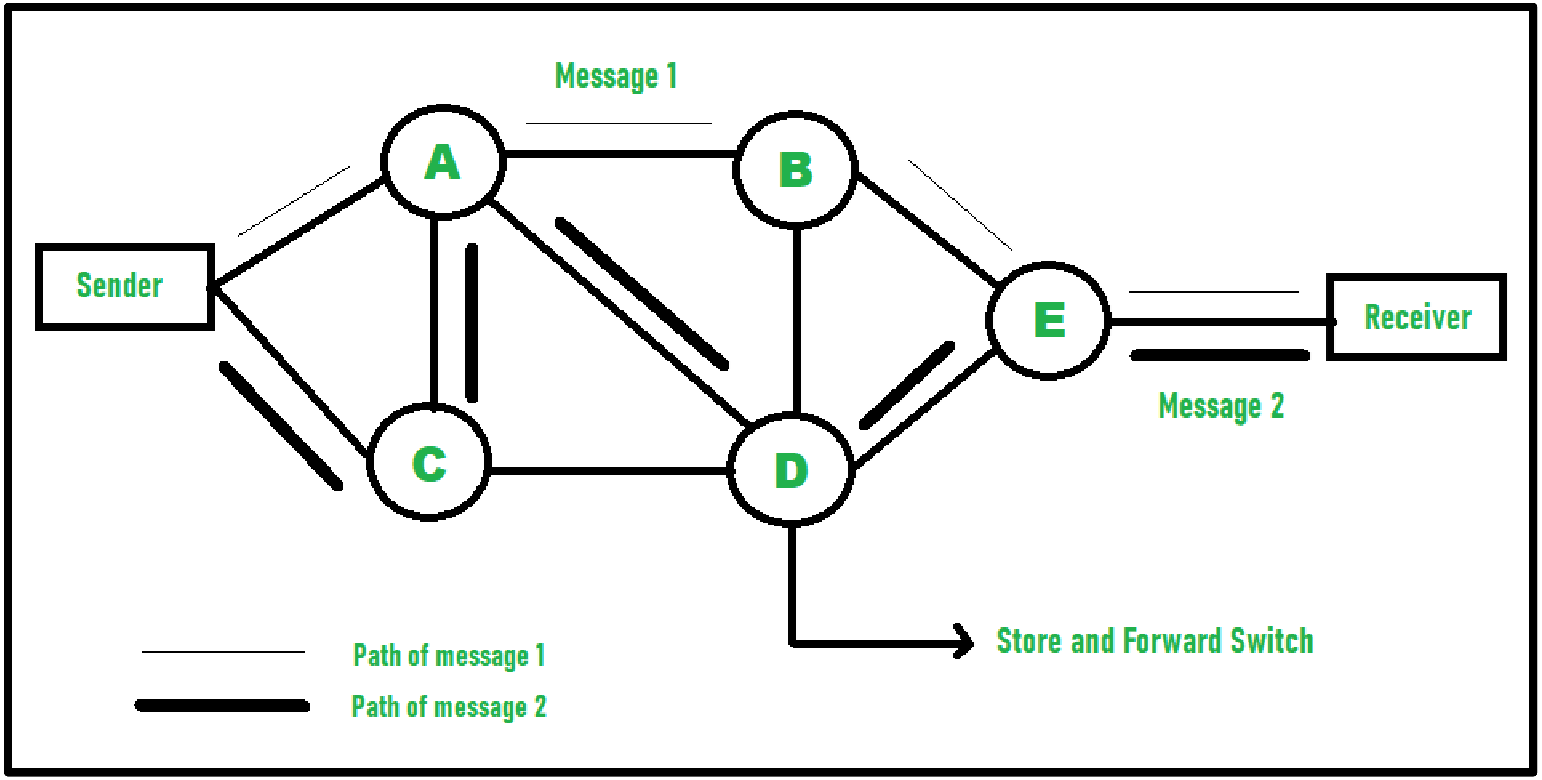
Received Message

Message is divided into packets

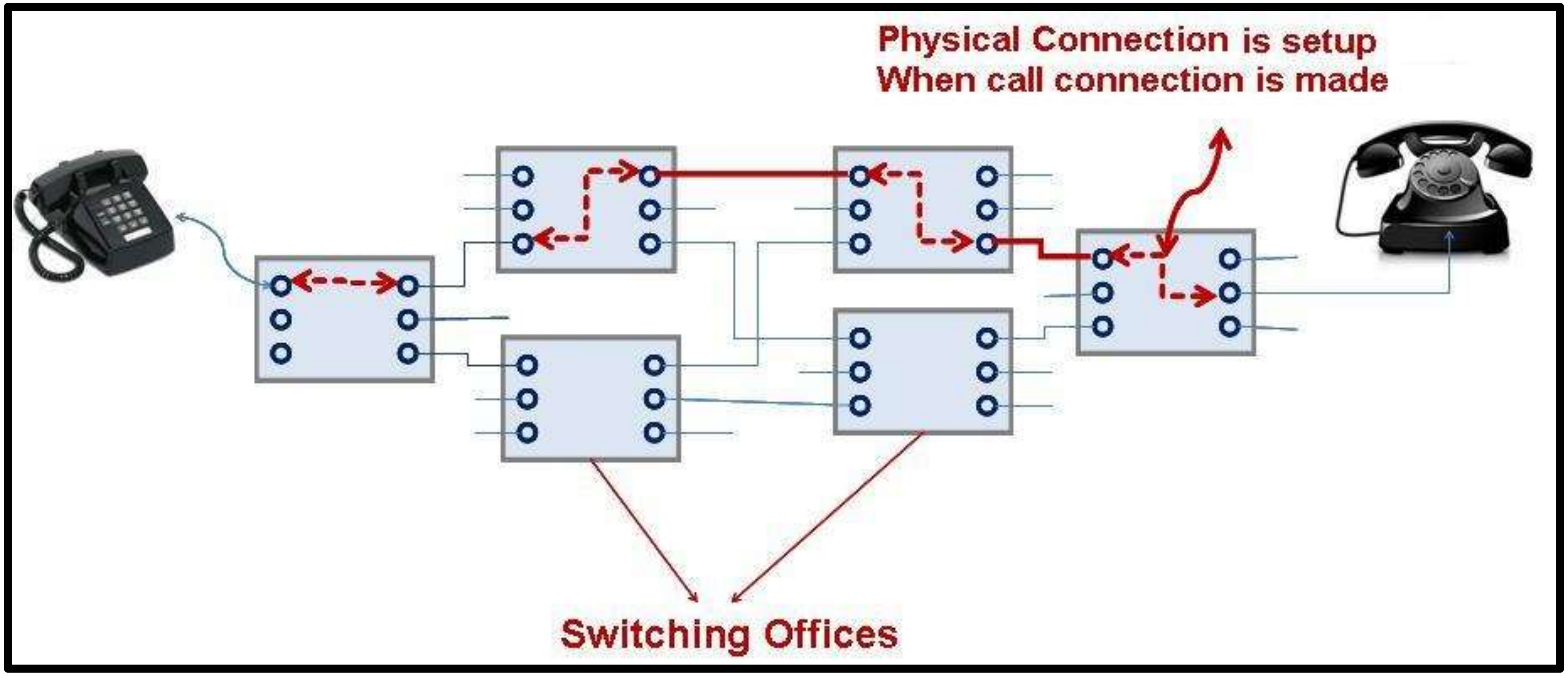
Packets are sent over the Internet by the most expedient route

Packets are reordered and reassembled

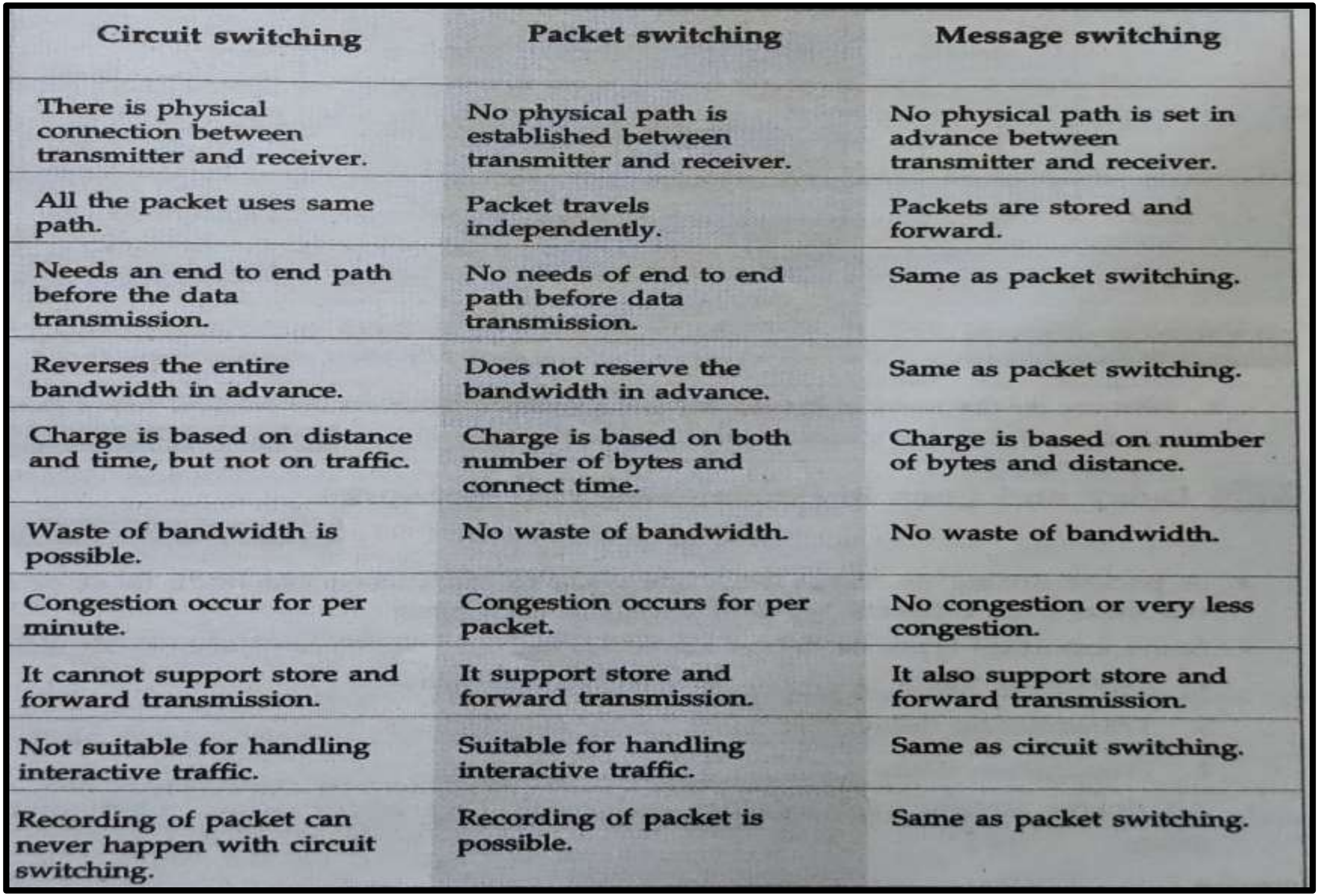
MESSAGE SWITCHING



CIRCUIT SWITCHING



CIRCUIT SWITCHING



Circuit switching	Packet switching	Message switching
There is physical connection between transmitter and receiver.	No physical path is established between transmitter and receiver.	No physical path is set in advance between transmitter and receiver.
All the packet uses same path.	Packet travels independently.	Packets are stored and forward.
Needs an end to end path before the data transmission.	No needs of end to end path before data transmission.	Same as packet switching.
Reverses the entire bandwidth in advance.	Does not reserve the bandwidth in advance.	Same as packet switching.
Charge is based on distance and time, but not on traffic.	Charge is based on both number of bytes and connect time.	Charge is based on number of bytes and distance.
Waste of bandwidth is possible.	No waste of bandwidth.	No waste of bandwidth.
Congestion occur for per minute.	Congestion occurs for per packet.	No congestion or very less congestion.
It cannot support store and forward transmission.	It support store and forward transmission.	It also support store and forward transmission.
Not suitable for handling interactive traffic.	Suitable for handling interactive traffic.	Same as circuit switching.
Recording of packet can never happen with circuit switching.	Recording of packet is possible.	Same as packet switching.

CIRCUIT SWITCHING

✓ Establishes a **dedicated path** between sender and receiver.

✓ Once the connection is established then the dedicated path will remain to exist **until the connection is terminated**.

✓ Similar as the **telephone** works.

✓ When any user wants to send the data a request signal is sent to the receiver then the **receiver sends back the acknowledgment** to ensure the availability of the dedicated path.

✓ After receiving the **acknowledgment**, dedicated path transfers the data.

MESSAGE SWITCHING

✓ Message is transferred as a complete unit and routed through intermediate nodes at which it is **stored and forwarded**.

✓ There is **no establishment of a dedicated path**.

✓ The **destination address** is appended to the message.

✓ Message Switching provides a dynamic routing as the message is routed through the intermediate nodes **based on the information available** in the message.

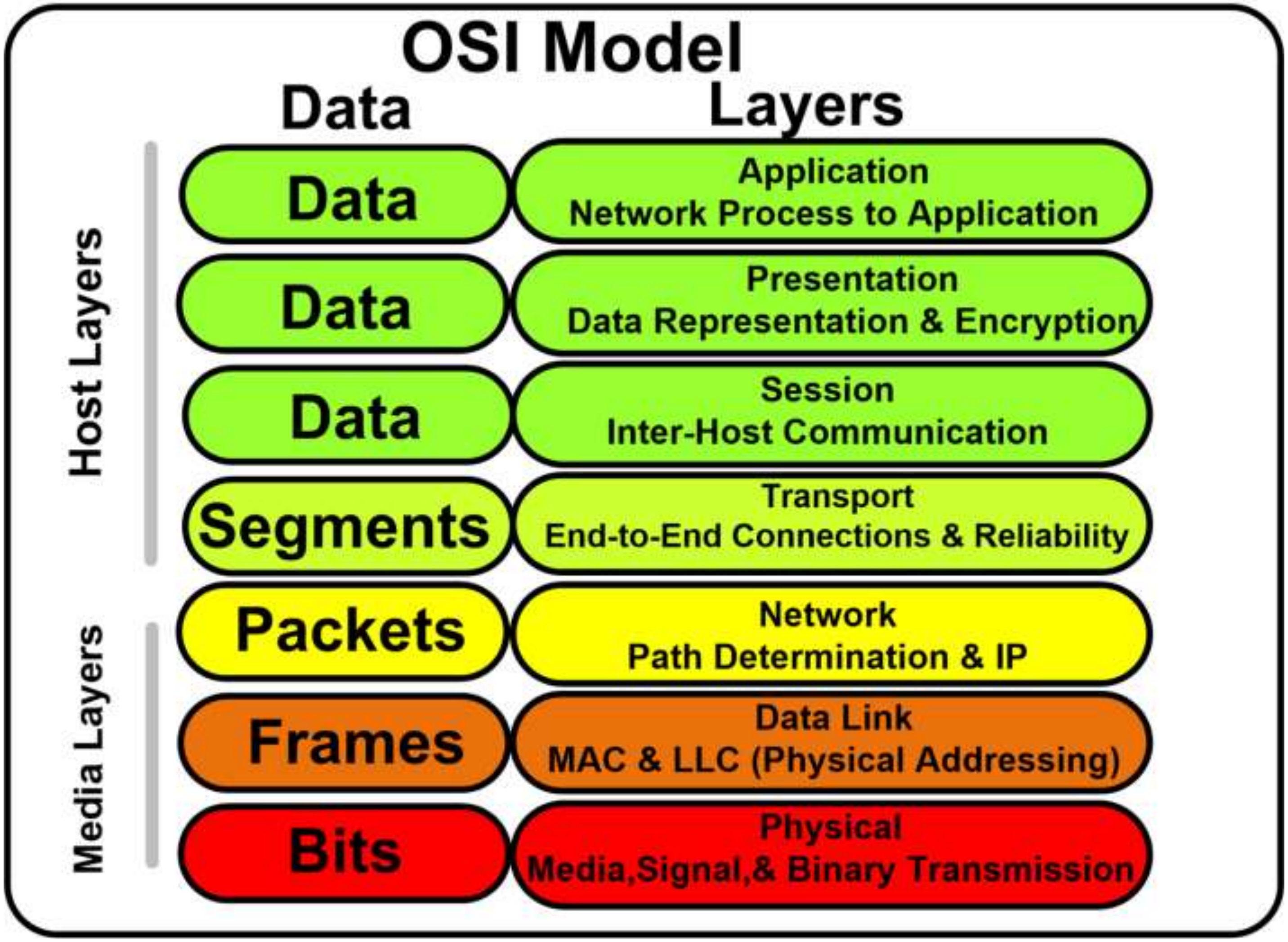
✓ Message switches are programmed in such a way so that they can provide the **most efficient routes**.

✓ Message switching treats each message as an

PACKET SWITCHING

- ✓ The message splits into **smaller pieces known as packets**. Packets are given a **unique number** to identify their order at the receiving end.
- ✓ Every packet contains some **information in its headers** such as source address, destination address and sequence number.
- ✓ Packets will travel across the network, taking the **shortest path** as possible. All the packets are **reassembled at the receiving end** in correct order.
- ✓ If any packet is **missing or corrupted**, then the message will be sent to **resend** the message. If the **correct order** of the packets is reached, then the **acknowledgment** message will be sent.

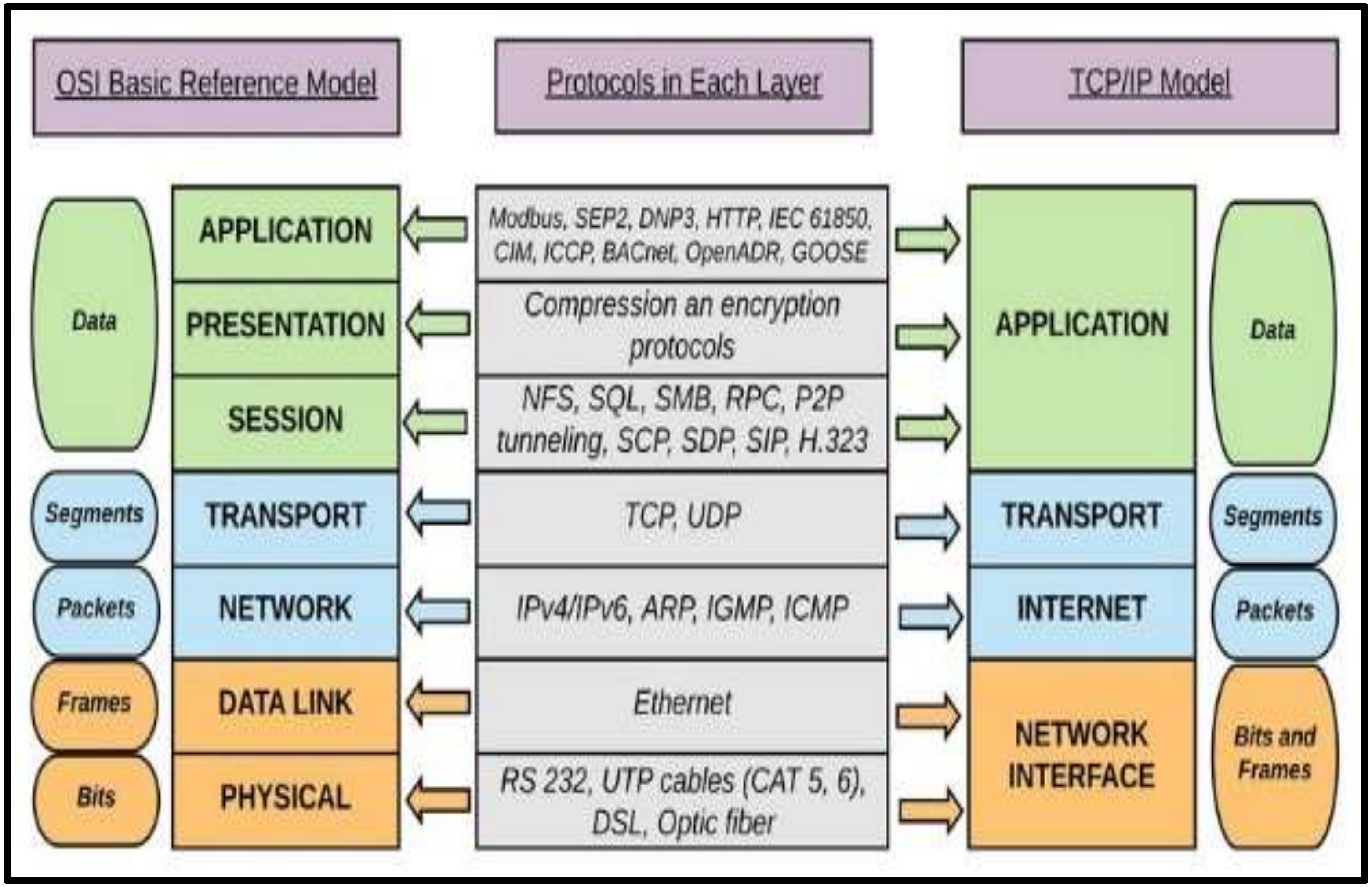
OSI MODEL



OSI Model

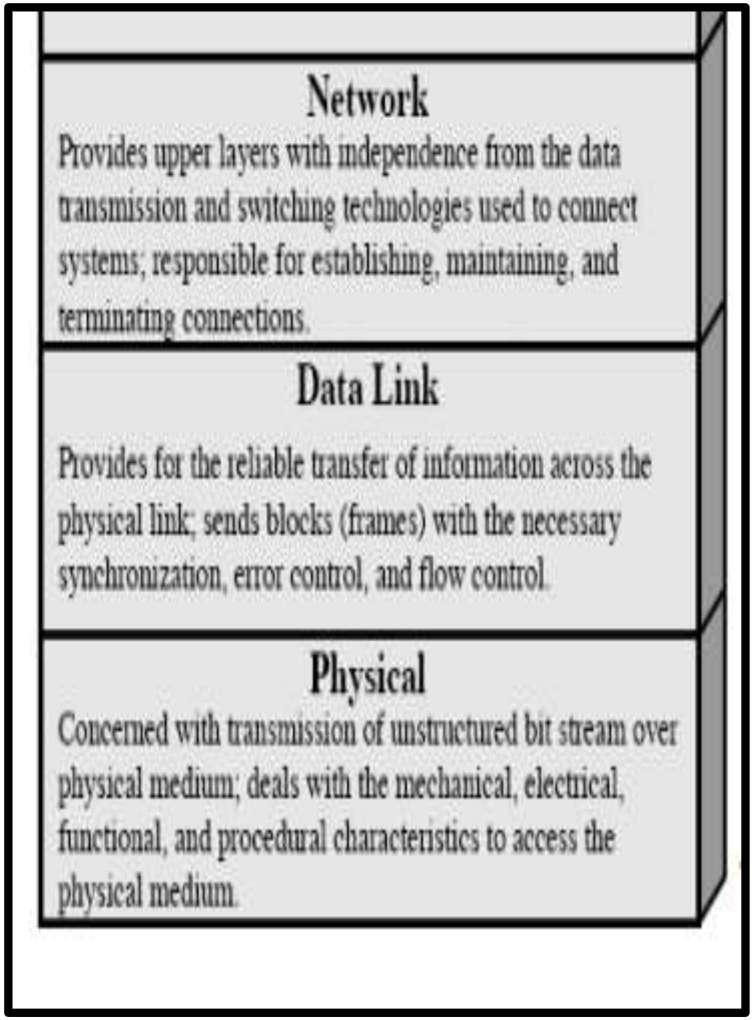
	Data	Layers
Host Layers	Data	Application Network Process to Application
	Data	Presentation Data Representation & Encryption
	Data	Session Inter-Host Communication
	Segments	Transport End-to-End Connections & Reliability
Media Layers	Packets	Network Path Determination & IP
	Frames	Data Link MAC & LLC (Physical Addressing)
	Bits	Physical Media,Signal,& Binary Transmission

TCP/IP MODEL



	OSI Basic Reference Model	Protocols in Each Layer	TCP/IP Model	
Data	APPLICATION	Modbus, SEP2, DNP3, HTTP, IEC 61850, CIM, ICCP, BACnet, OpenADR, GOOSE	APPLICATION	Data
	PRESENTATION	Compression an encryption protocols		
	SESSION	NFS, SQL, SMB, RPC, P2P tunneling, SCP, SDP, SIP, H.323		
Segments	TRANSPORT	TCP, UDP	TRANSPORT	Segments
Packets	NETWORK	IPv4/IPv6, ARP, IGMP, ICMP	INTERNET	Packets
Frames	DATA LINK	Ethernet	NETWORK INTERFACE	Bits and Frames
Bits	PHYSICAL	RS 232, UTP cables (CAT 5, 6), DSL, Optic fiber		

LAYERS



Network

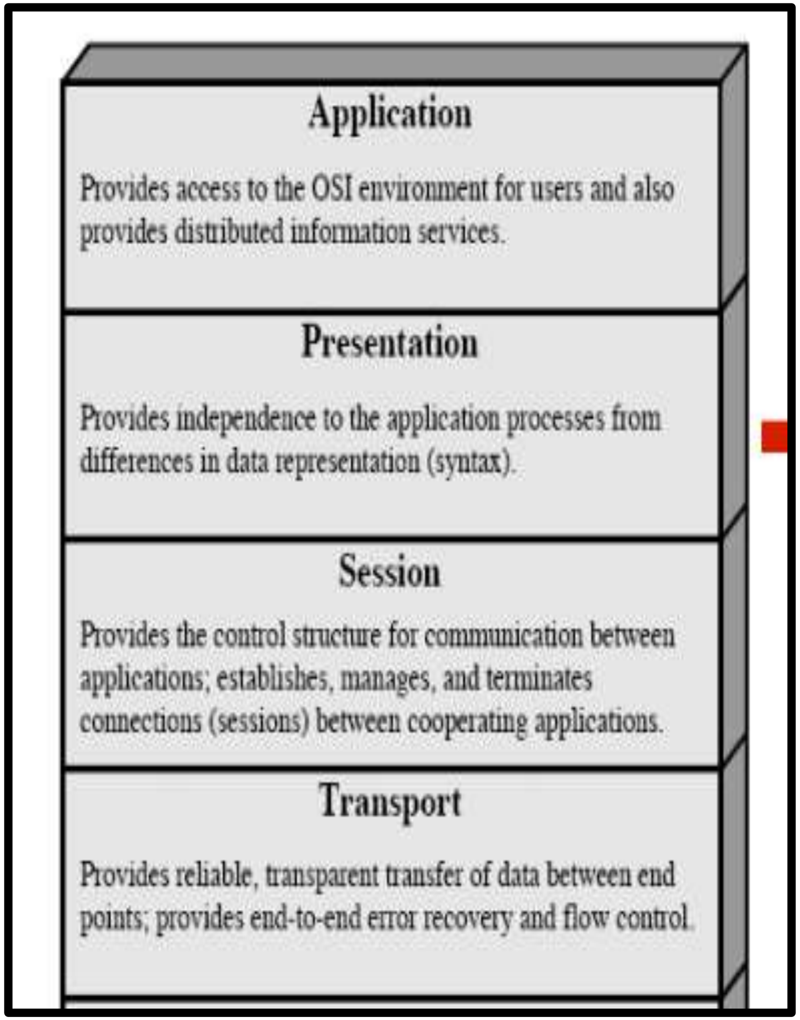
Provides upper layers with independence from the data transmission and switching technologies used to connect systems; responsible for establishing, maintaining, and terminating connections.

Data Link

Provides for the reliable transfer of information across the physical link; sends blocks (frames) with the necessary synchronization, error control, and flow control.

Physical

Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional, and procedural characteristics to access the physical medium.



Application

Provides access to the OSI environment for users and also provides distributed information services.

Presentation

Provides independence to the application processes from differences in data representation (syntax).

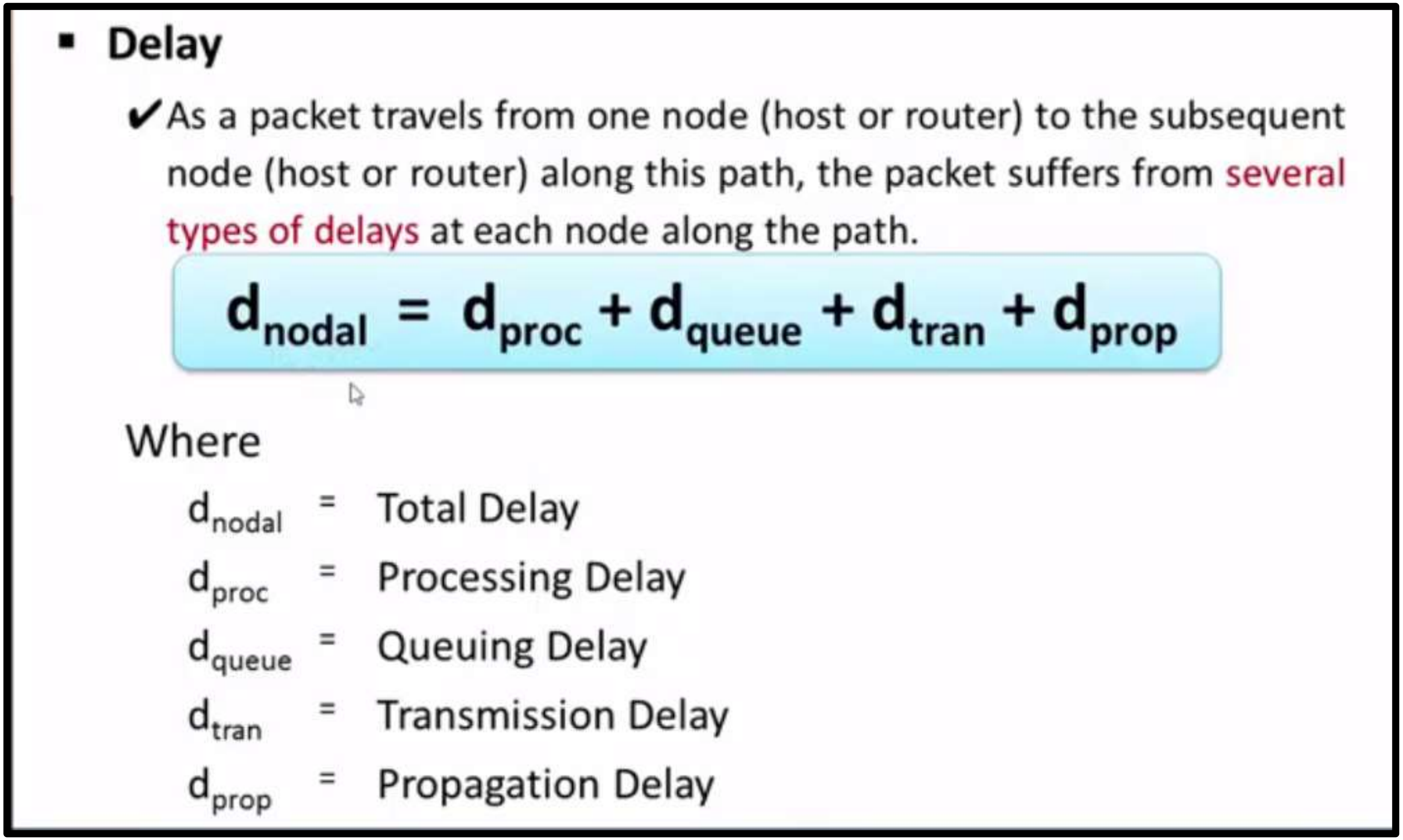
Session

Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications.

Transport

Provides reliable, transparent transfer of data between end points; provides end-to-end error recovery and flow control.

DELAY



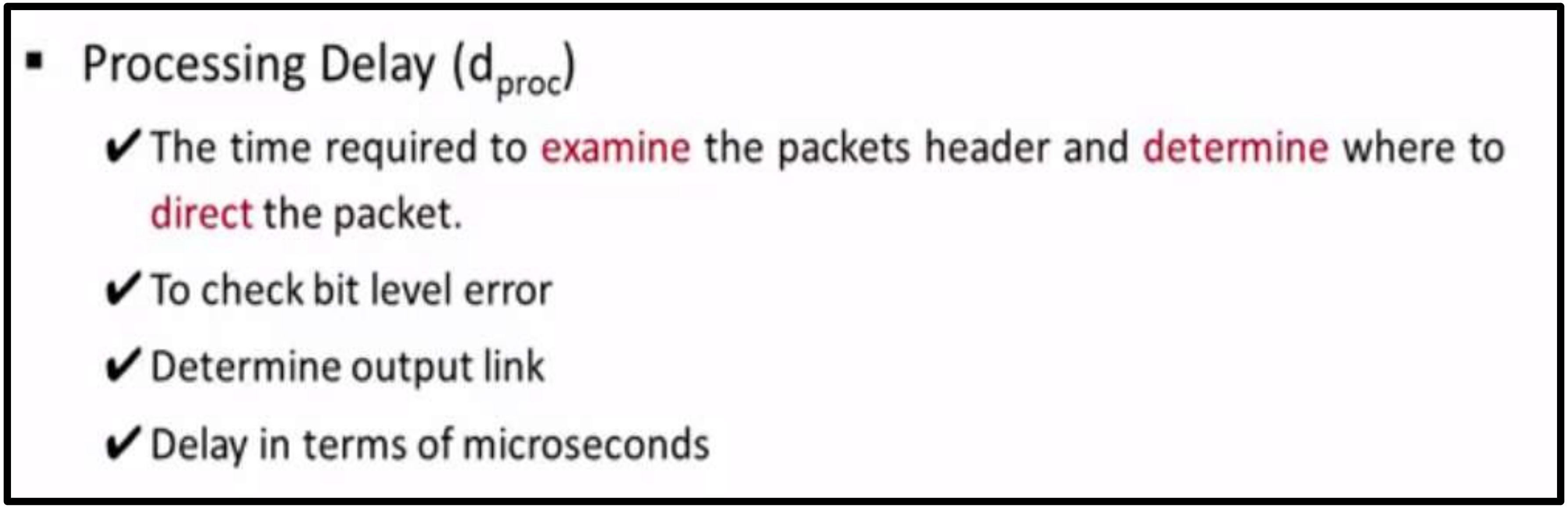
- **Delay**
  - ✔ As a packet travels from one node (host or router) to the subsequent node (host or router) along this path, the packet suffers from several types of delays at each node along the path.

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

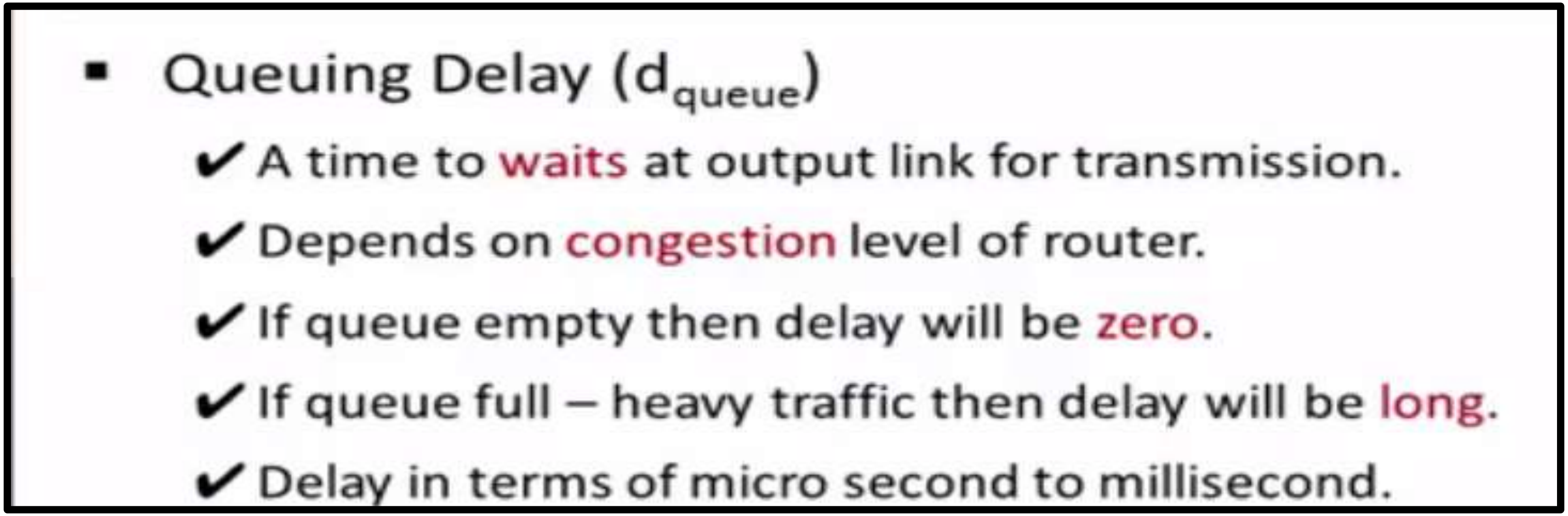
Where

d_{nodal}	=	Total Delay
d_{proc}	=	Processing Delay
d_{queue}	=	Queuing Delay
d_{tran}	=	Transmission Delay
d_{prop}	=	Propagation Delay

DELAY

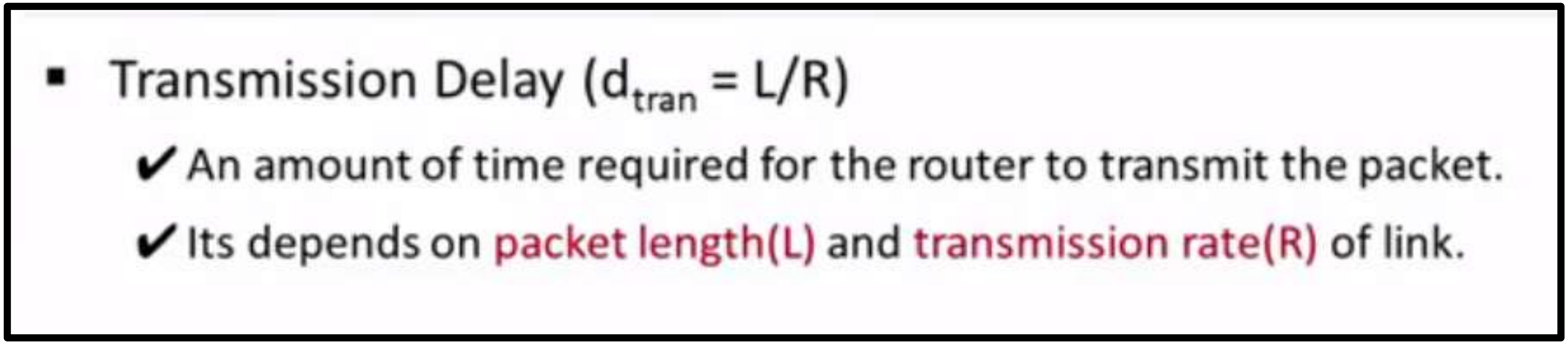


- Processing Delay (d_{proc})
  - ✔ The time required to examine the packets header and determine where to direct the packet.
  - ✔ To check bit level error
  - ✔ Determine output link
  - ✔ Delay in terms of microseconds

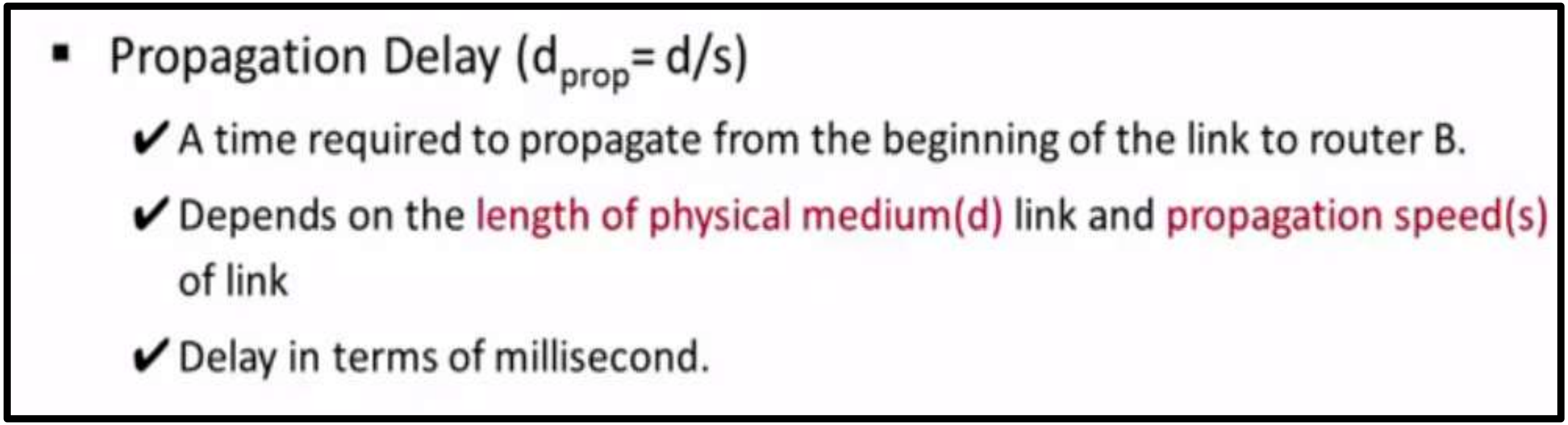


- Queuing Delay (d_{queue})
  - ✔ A time to waits at output link for transmission.
  - ✔ Depends on congestion level of router.
  - ✔ If queue empty then delay will be zero.
  - ✔ If queue full – heavy traffic then delay will be long.
  - ✔ Delay in terms of micro second to millisecond.

DELAY

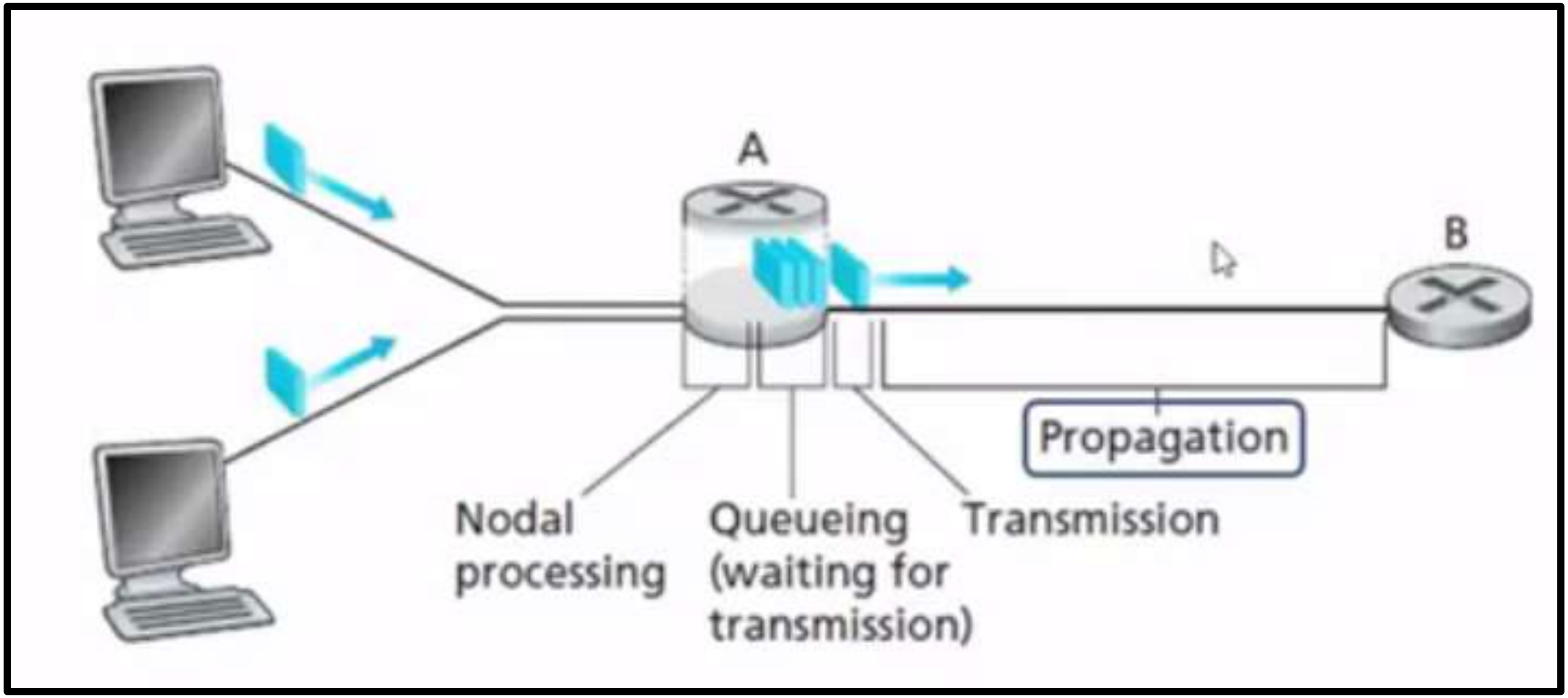


- Transmission Delay (d_{tran} = L/R)
  - ✔ An amount of time required for the router to transmit the packet.
  - ✔ Its depends on packet length(L) and transmission rate(R) of link.



- Propagation Delay (d_{prop}= d/s)
  - ✔ A time required to propagate from the beginning of the link to router B.
  - ✔ Depends on the length of physical medium(d) link and propagation speed(s) of link
  - ✔ Delay in terms of millisecond.

DELAY


A
B
Propagation
Nodal
processing
Queueing
(waiting for
transmission)
Transmission

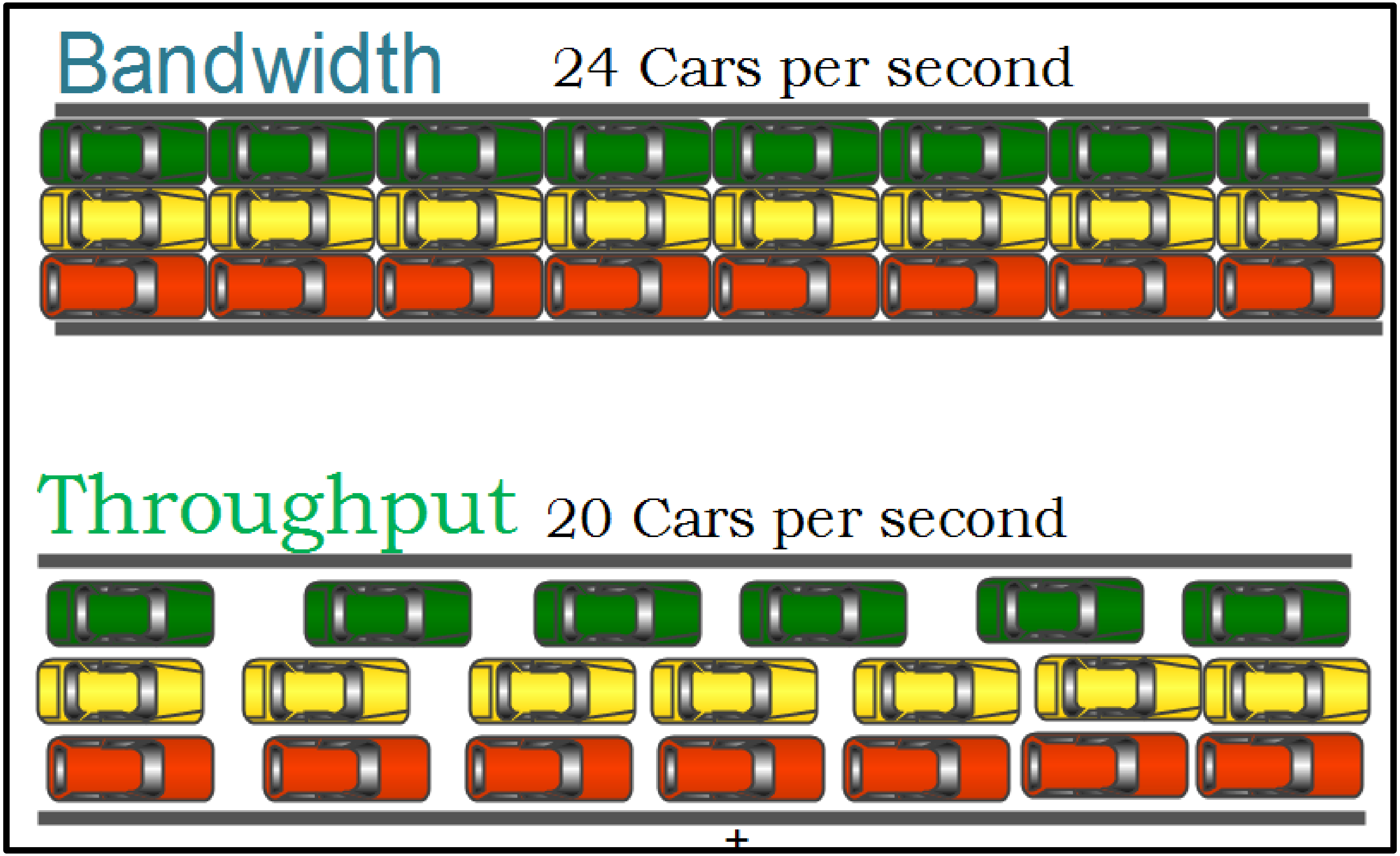
THROUGHPUT

✓ Throughput is the number of messages successfully transmitted per unit time.

✓ The terms ‘throughput’ and ‘bandwidth’ are often thought of as the same, yet they are different. Bandwidth is the potential measurement of a link, whereas throughput is an actual measurement of how fast we can send data.

✓ Usually resulting in the unit of bits per second(bps).

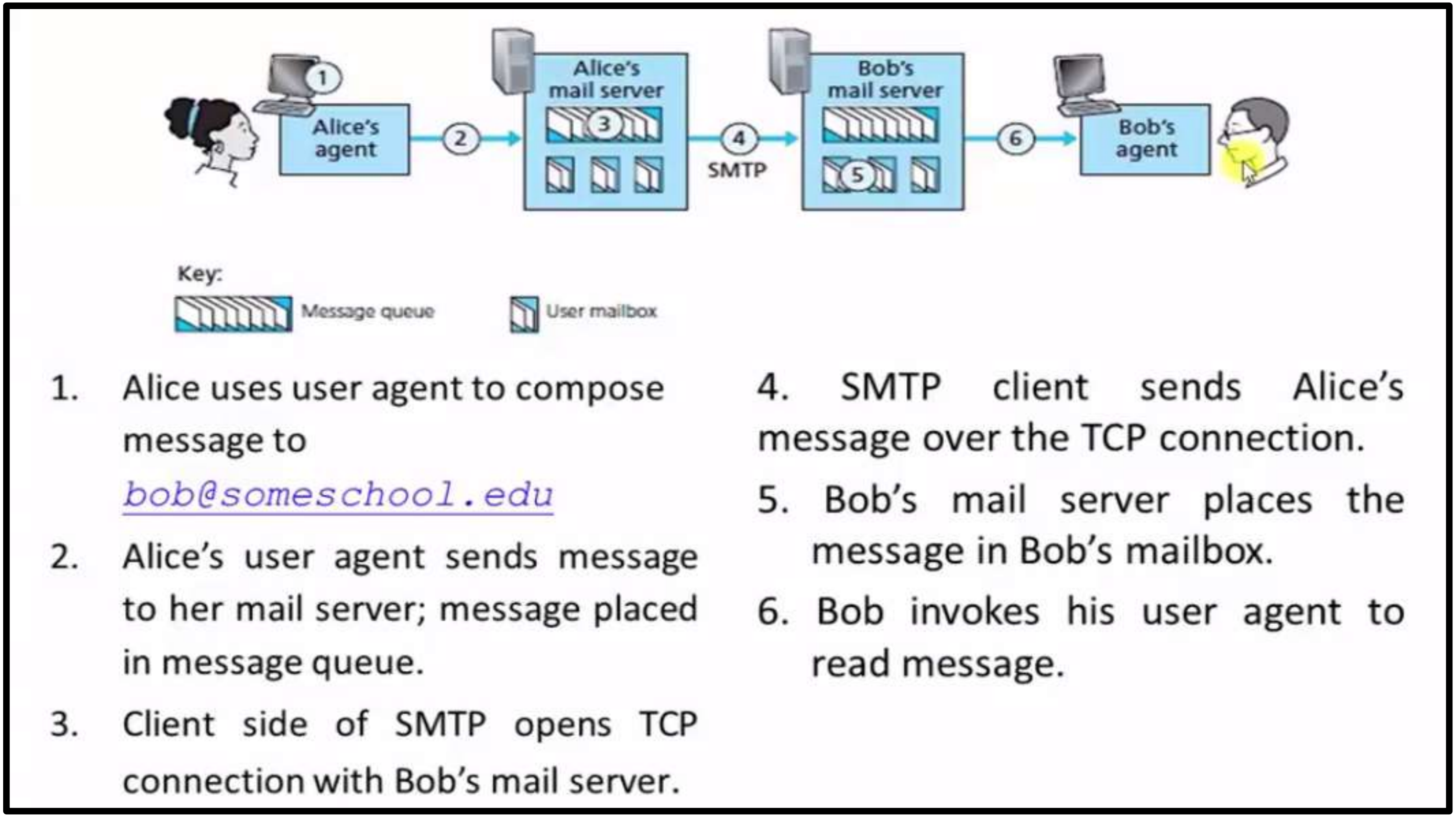
THROUGHPUT



Bandwidth 24 Cars per second

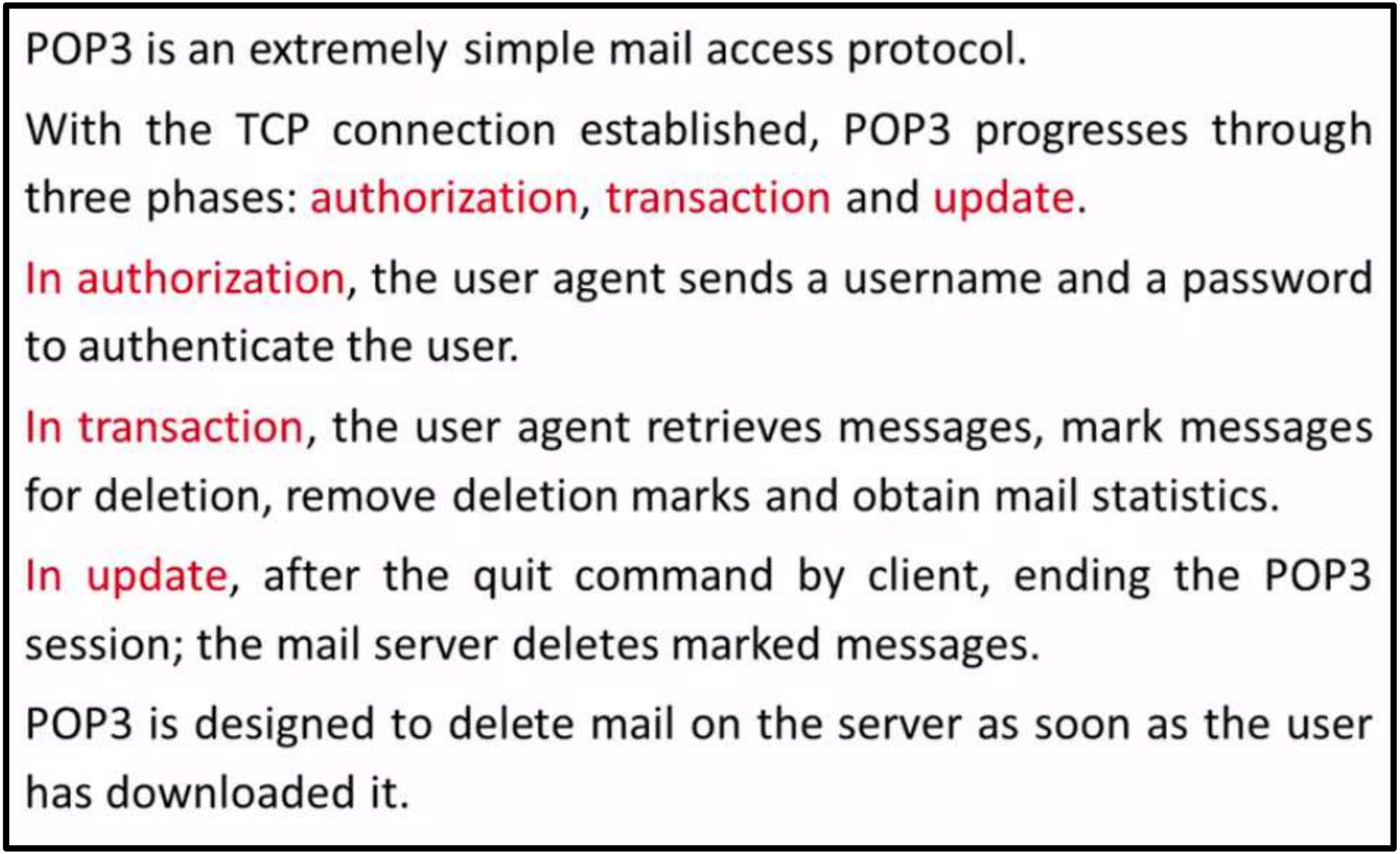
Throughput 20 Cars per second

EMAIL SMTP Simple Mail Transfer Protocol



1. Alice uses user agent to compose message to *bob@someschool.edu*
2. Alice's user agent sends message to her mail server; message placed in message queue.
3. Client side of SMTP opens TCP connection with Bob's mail server.
4. SMTP client sends Alice's message over the TCP connection.
5. Bob's mail server places the message in Bob's mailbox.
6. Bob invokes his user agent to read message.

POP3 Post Office Version 3



POP3 is an extremely simple mail access protocol.

With the TCP connection established, POP3 progresses through three phases: authorization, transaction and update.

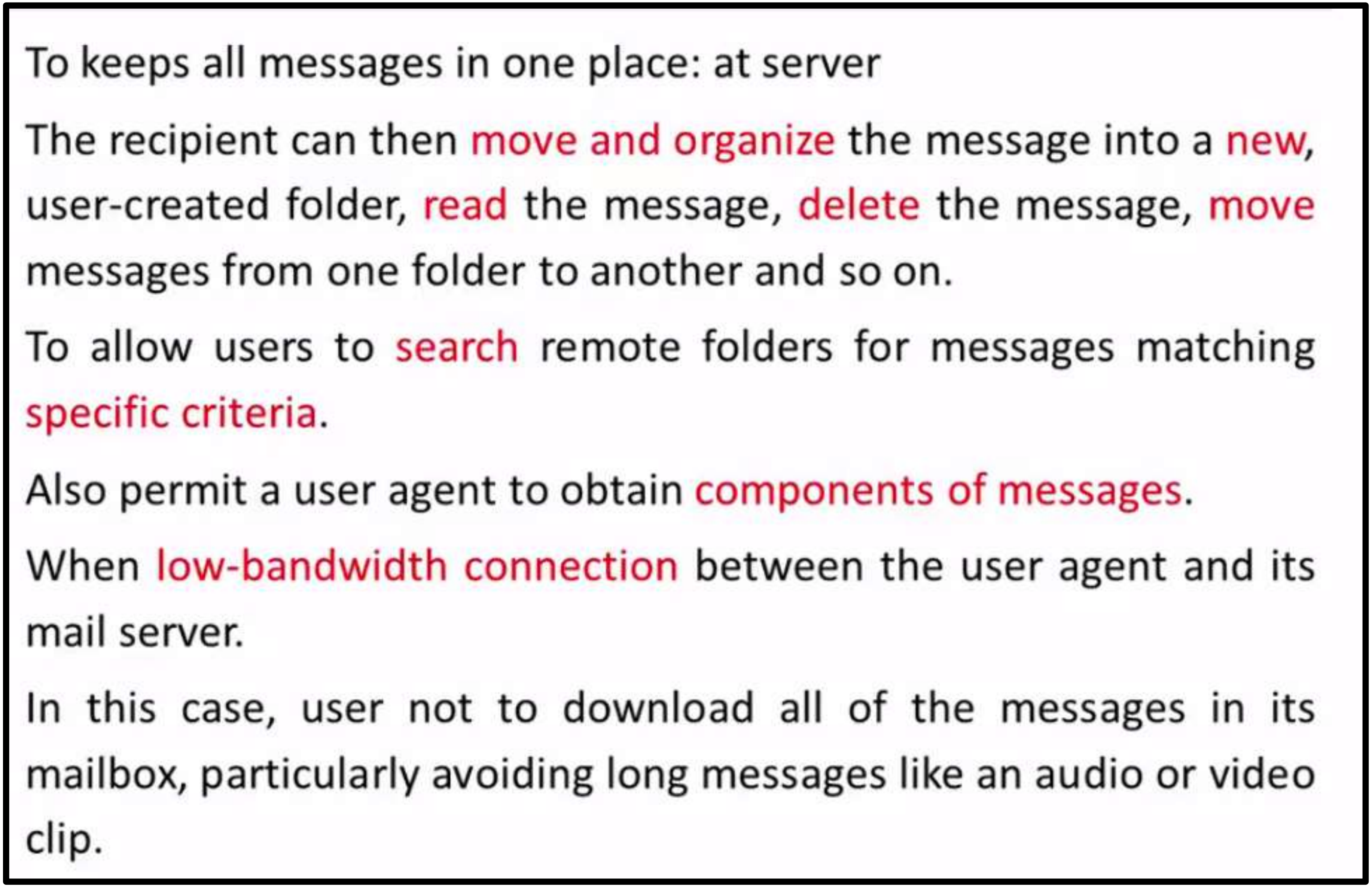
In authorization, the user agent sends a username and a password to authenticate the user.

In transaction, the user agent retrieves messages, mark messages for deletion, remove deletion marks and obtain mail statistics.

In update, after the quit command by client, ending the POP3 session; the mail server deletes marked messages.

POP3 is designed to delete mail on the server as soon as the user has downloaded it.

IMAP Internet Mail Access Protocol



To keeps all messages in one place: at server

The recipient can then move and organize the message into a new, user-created folder, read the message, delete the message, move messages from one folder to another and so on.

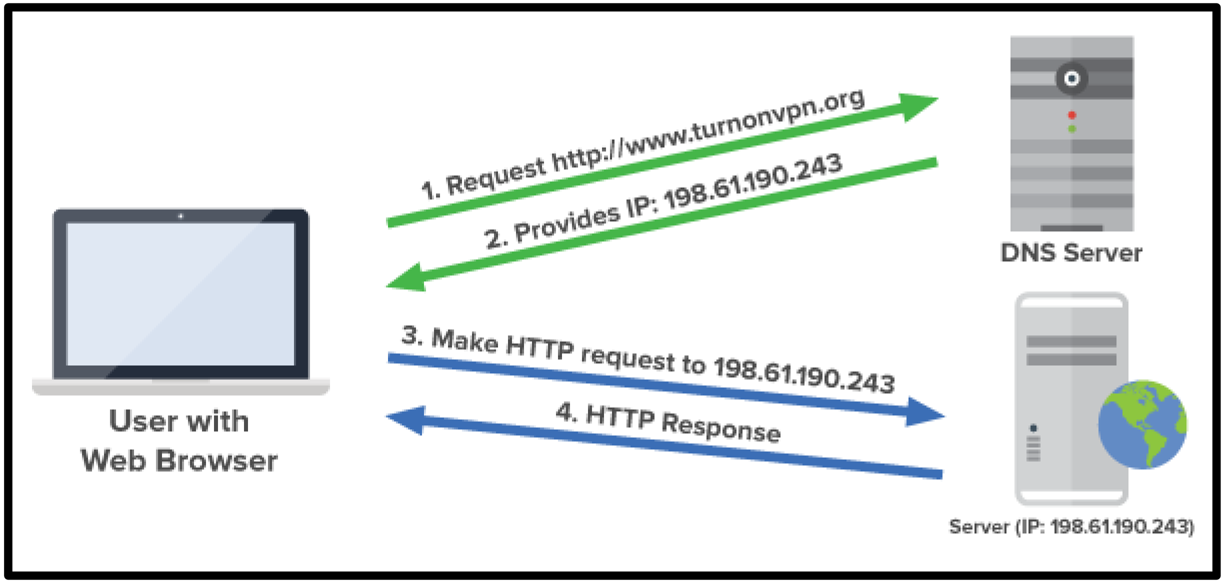
To allow users to search remote folders for messages matching specific criteria.

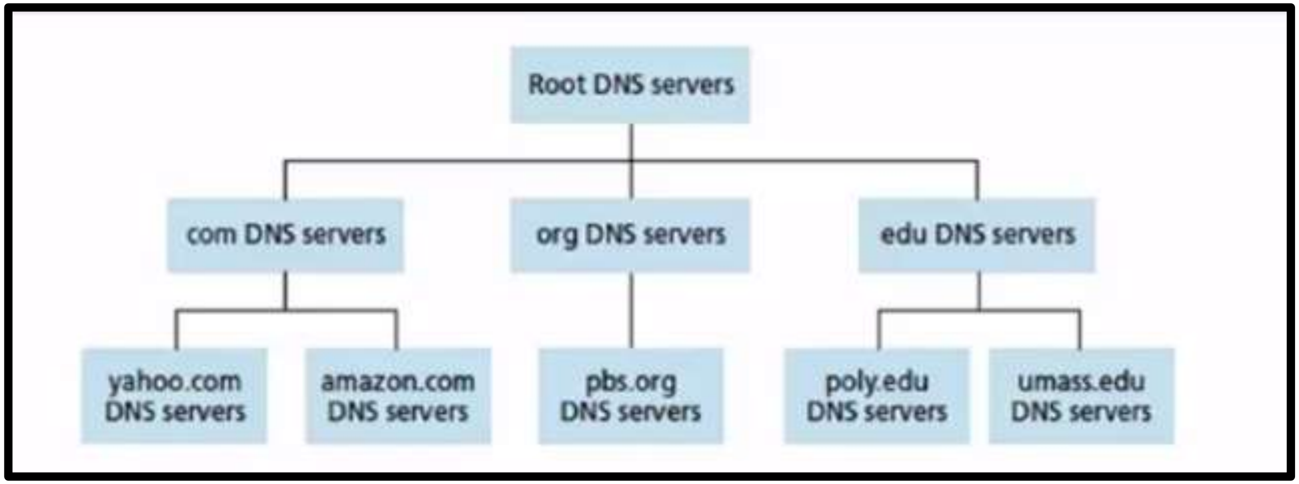
Also permit a user agent to obtain components of messages.

When low-bandwidth connection between the user agent and its mail server.

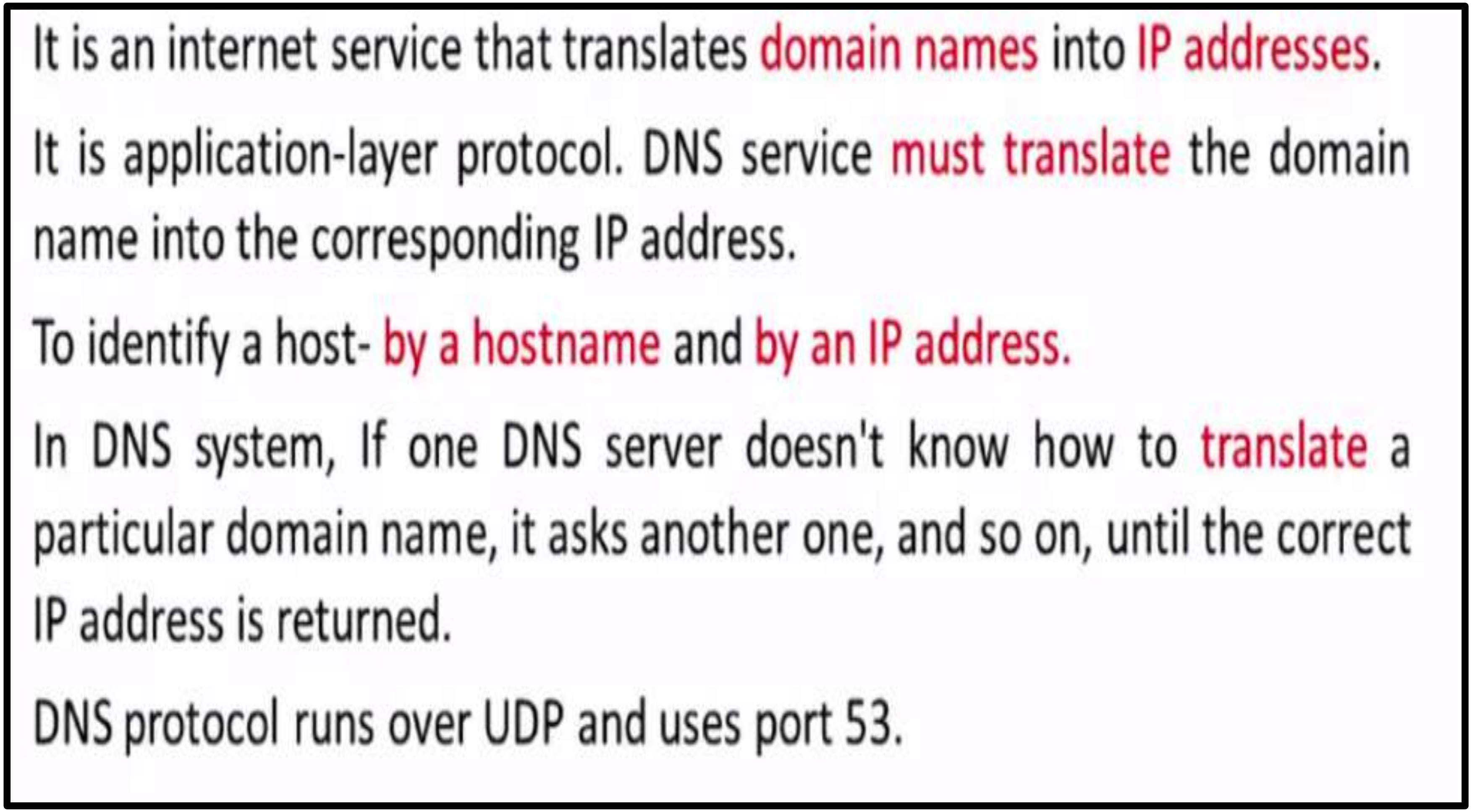
In this case, user not to download all of the messages in its mailbox, particularly avoiding long messages like an audio or video clip.

DOMAIN NAME SYSTEM


1. Request http://www.turnonvpn.org
2. Provides IP: 198.61.190.243
DNS Server
User with
Web Browser
3. Make HTTP request to 198.61.190.243
4. HTTP Response
Server (IP: 198.61.190.243)



DOMAIN NAME SYSTEM



It is an internet service that translates domain names into IP addresses.

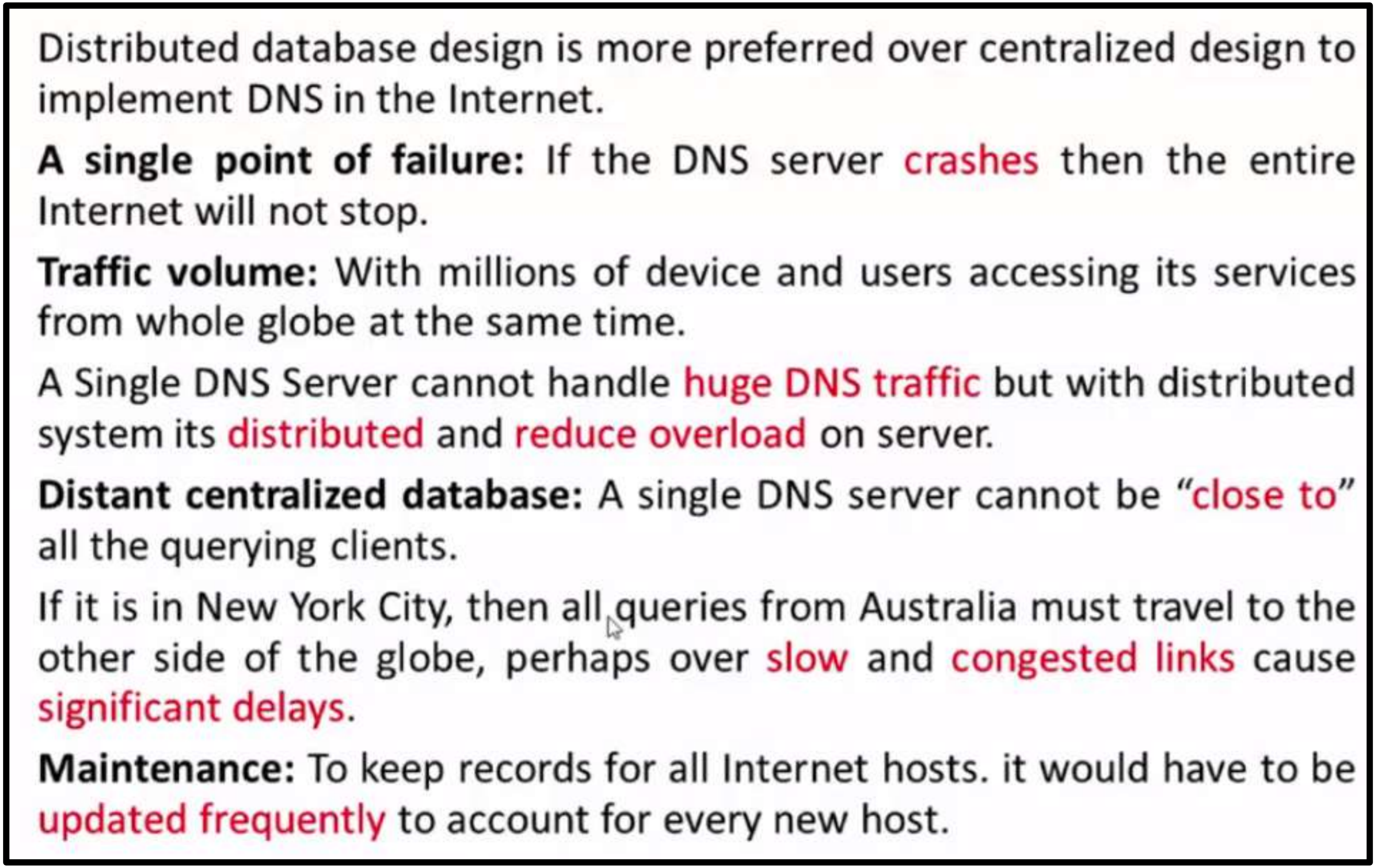
It is application-layer protocol. DNS service must translate the domain name into the corresponding IP address.

To identify a host- by a hostname and by an IP address.

In DNS system, If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

DNS protocol runs over UDP and uses port 53.

DOMAIN NAME SYSTEM



Distributed database design is more preferred over centralized design to implement DNS in the Internet.

A single point of failure: If the DNS server crashes then the entire Internet will not stop.

Traffic volume: With millions of device and users accessing its services from whole globe at the same time.

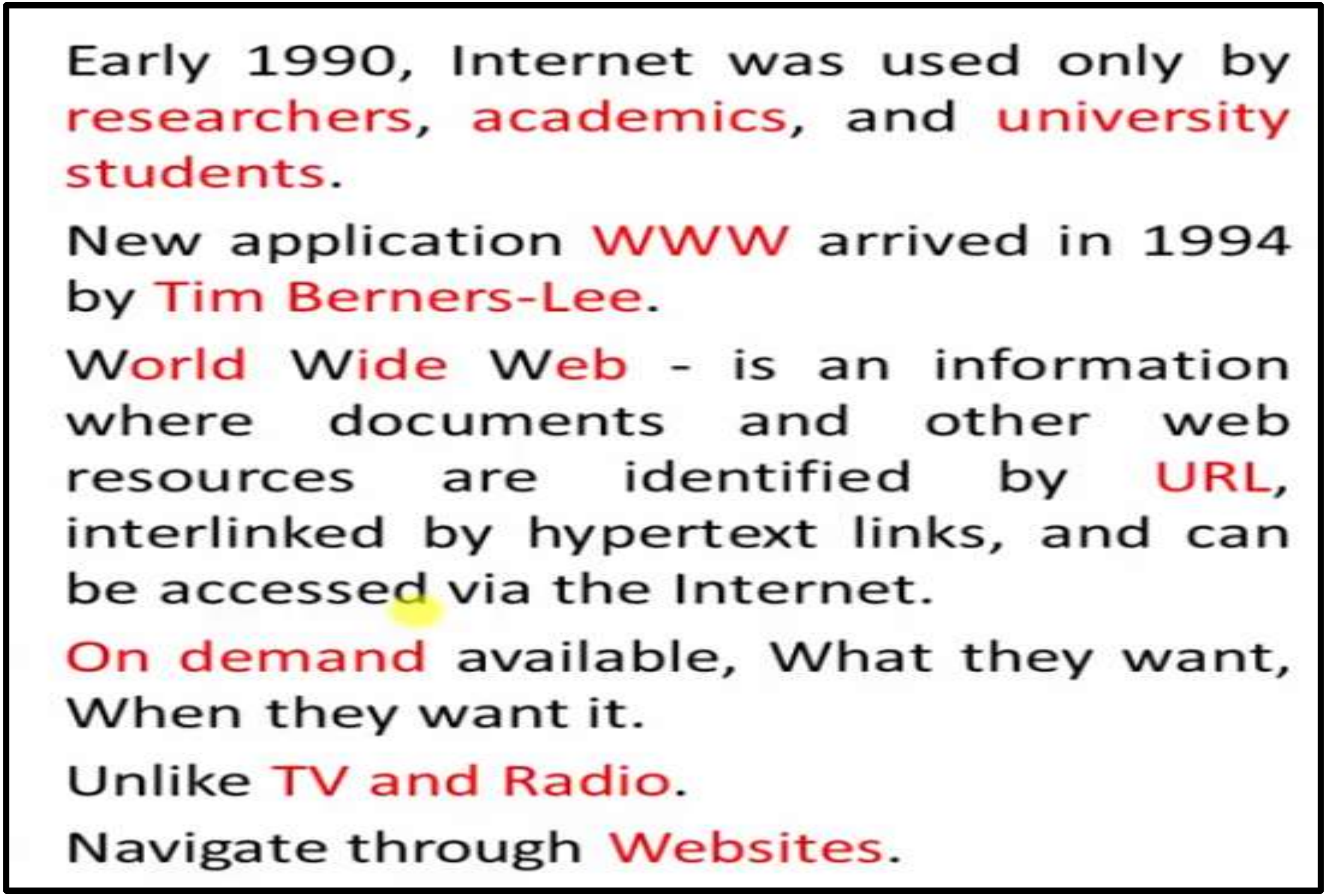
A Single DNS Server cannot handle huge DNS traffic but with distributed system its distributed and reduce overload on server.

Distant centralized database: A single DNS server cannot be “close to” all the querying clients.

If it is in New York City, then all queries from Australia must travel to the other side of the globe, perhaps over slow and congested links cause significant delays.

Maintenance: To keep records for all Internet hosts. it would have to be updated frequently to account for every new host.

WEB/INTERNET



Early 1990, Internet was used only by researchers, academics, and university students.

New application WWW arrived in 1994 by Tim Berners-Lee.

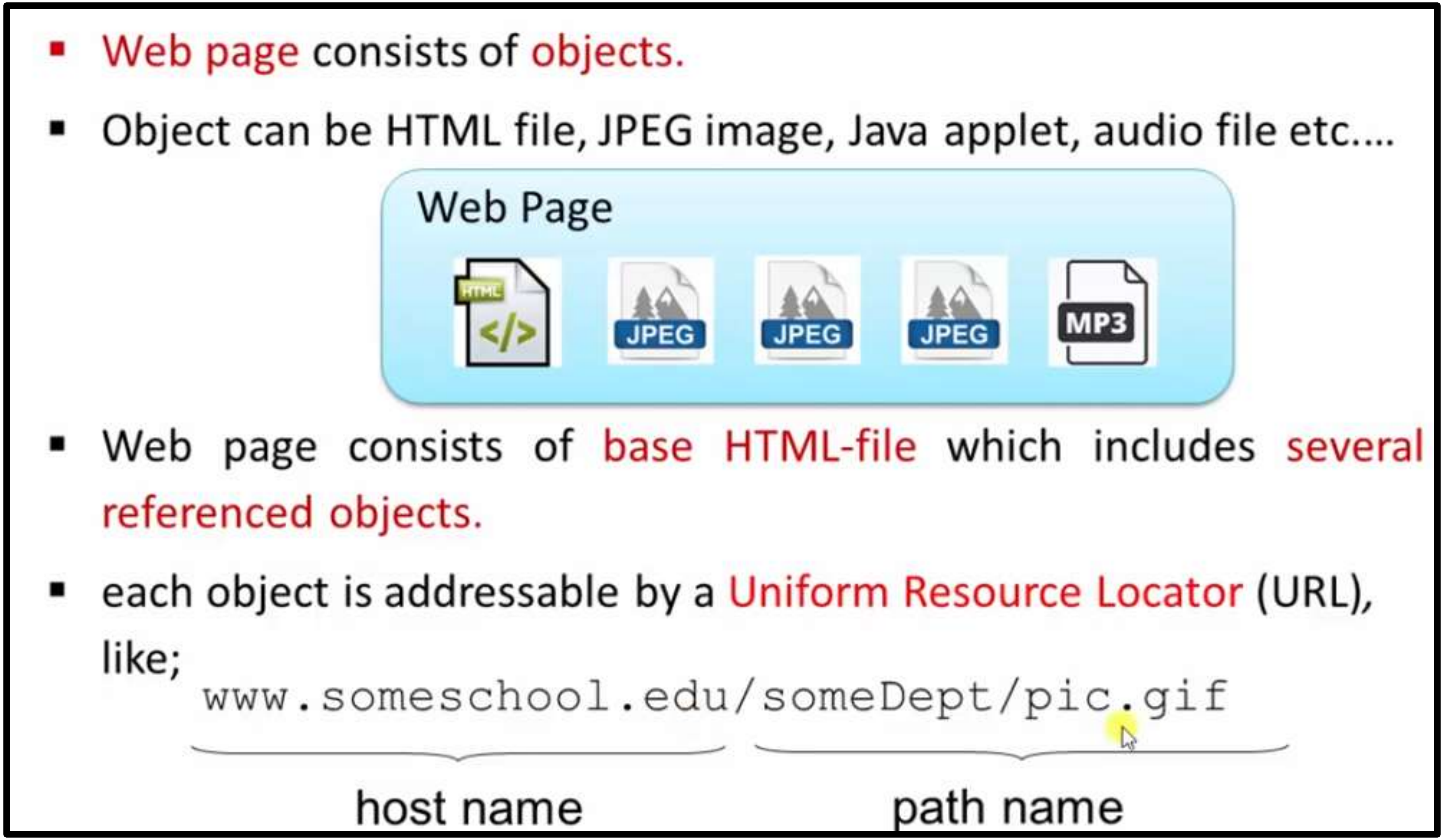
World Wide Web - is an information where documents and other web resources are identified by URL, interlinked by hypertext links, and can be accessed via the Internet.

On demand available, What they want, When they want it.

Unlike TV and Radio.

Navigate through Websites.

WEB/INTERNET

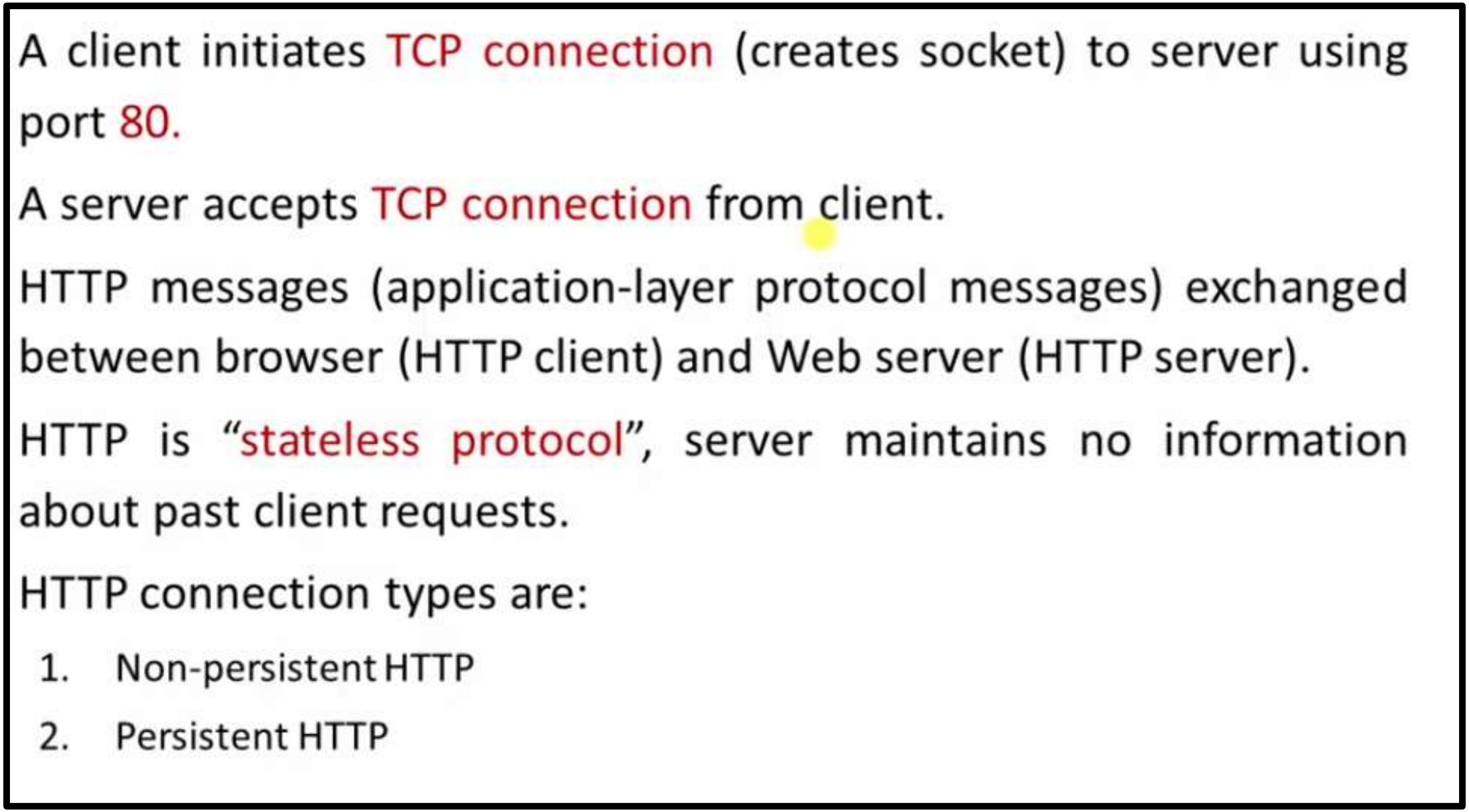


- Web page consists of objects.
- Object can be HTML file, JPEG image, Java applet, audio file etc....

- Web page consists of base HTML-file which includes several referenced objects.
- each object is addressable by a Uniform Resource Locator (URL), like;

$$\underbrace{\texttt{www.someschool.edu}}_{\text{host name}}\underbrace{\texttt{/someDept/pic.gif}}_{\text{path name}}$$

WEB/INTERNET



A client initiates TCP connection (creates socket) to server using port 80.

A server accepts TCP connection from client.

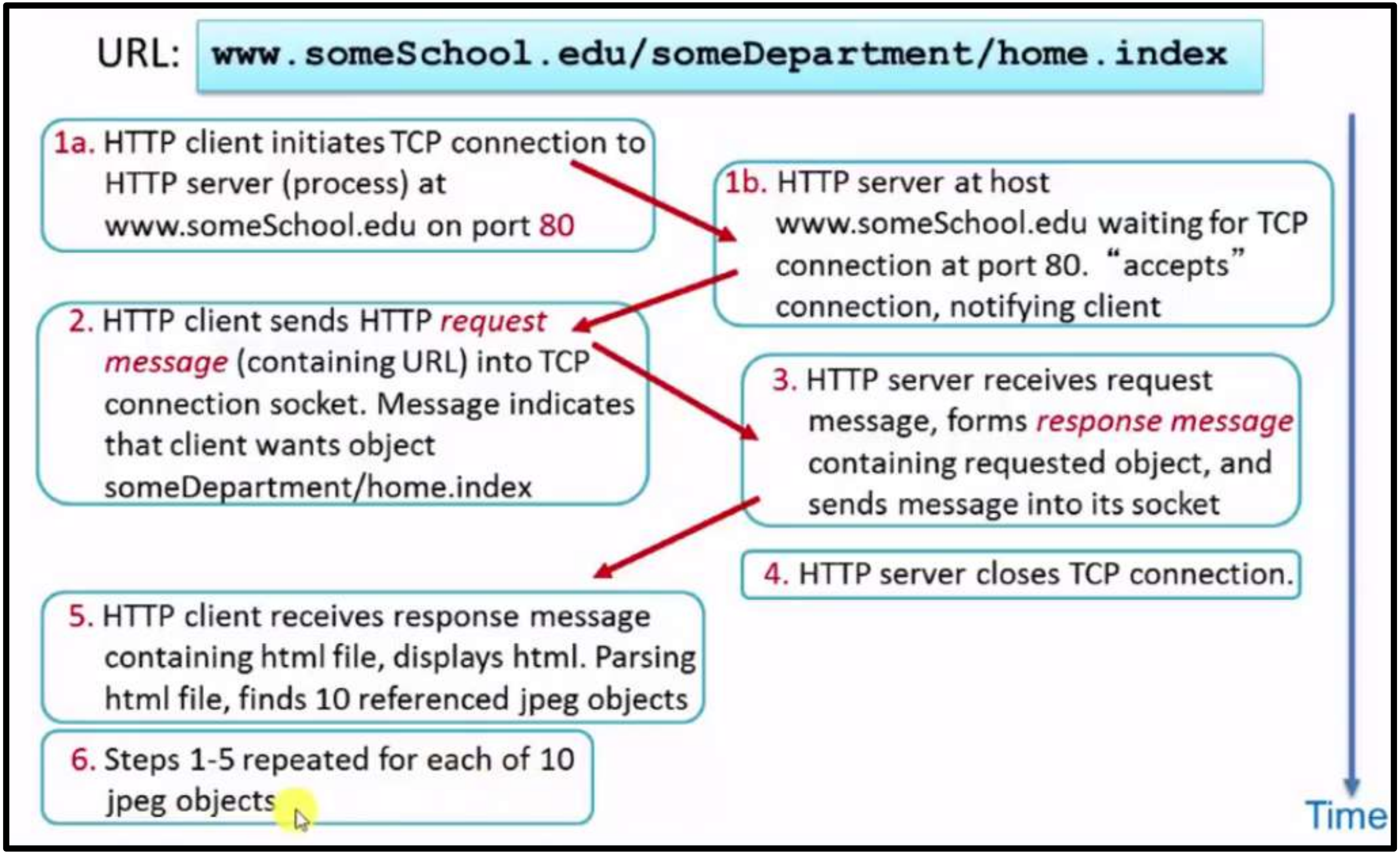
HTTP messages (application-layer protocol messages) exchanged between browser (HTTP client) and Web server (HTTP server).

HTTP is "stateless protocol", server maintains no information about past client requests.

HTTP connection types are:

1. Non-persistent HTTP
2. Persistent HTTP

NON PERSISTENT HTTP



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

1a. HTTP client initiates TCP connection to HTTP server (process) at www.someSchool.edu on port 80

1b. HTTP server at host www.someSchool.edu waiting for TCP connection at port 80. “accepts” connection, notifying client

2. HTTP client sends HTTP *request message* (containing URL) into TCP connection socket. Message indicates that client wants object someDepartment/home.index

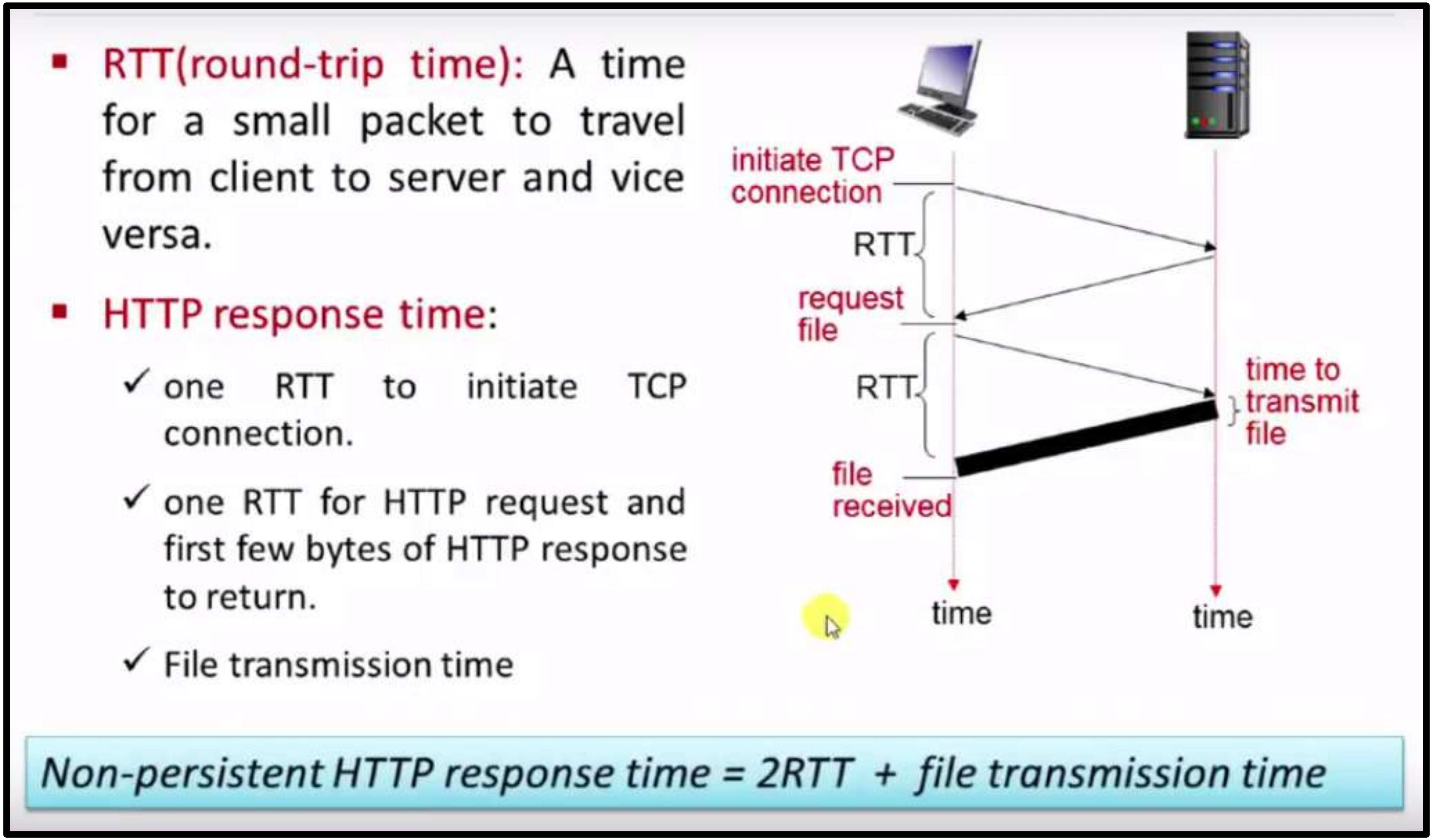
3. HTTP server receives request message, forms *response message* containing requested object, and sends message into its socket

4. HTTP server closes TCP connection.

5. HTTP client receives response message containing html file, displays html. Parsing html file, finds 10 referenced jpeg objects

6. Steps 1-5 repeated for each of 10 jpeg objects

NON PERSISTENT HTTP



- **RTT(round-trip time):** A time for a small packet to travel from client to server and vice versa.
- **HTTP response time:**
  - ✓ one RTT to initiate TCP connection.
  - ✓ one RTT for HTTP request and first few bytes of HTTP response to return.
  - ✓ File transmission time

Non-persistent HTTP response time = 2RTT + file transmission time

PERSISTENT HTTP

Server leaves the TCP connection open after sending responses.

Subsequent HTTP messages between same client and server sent over open connection.

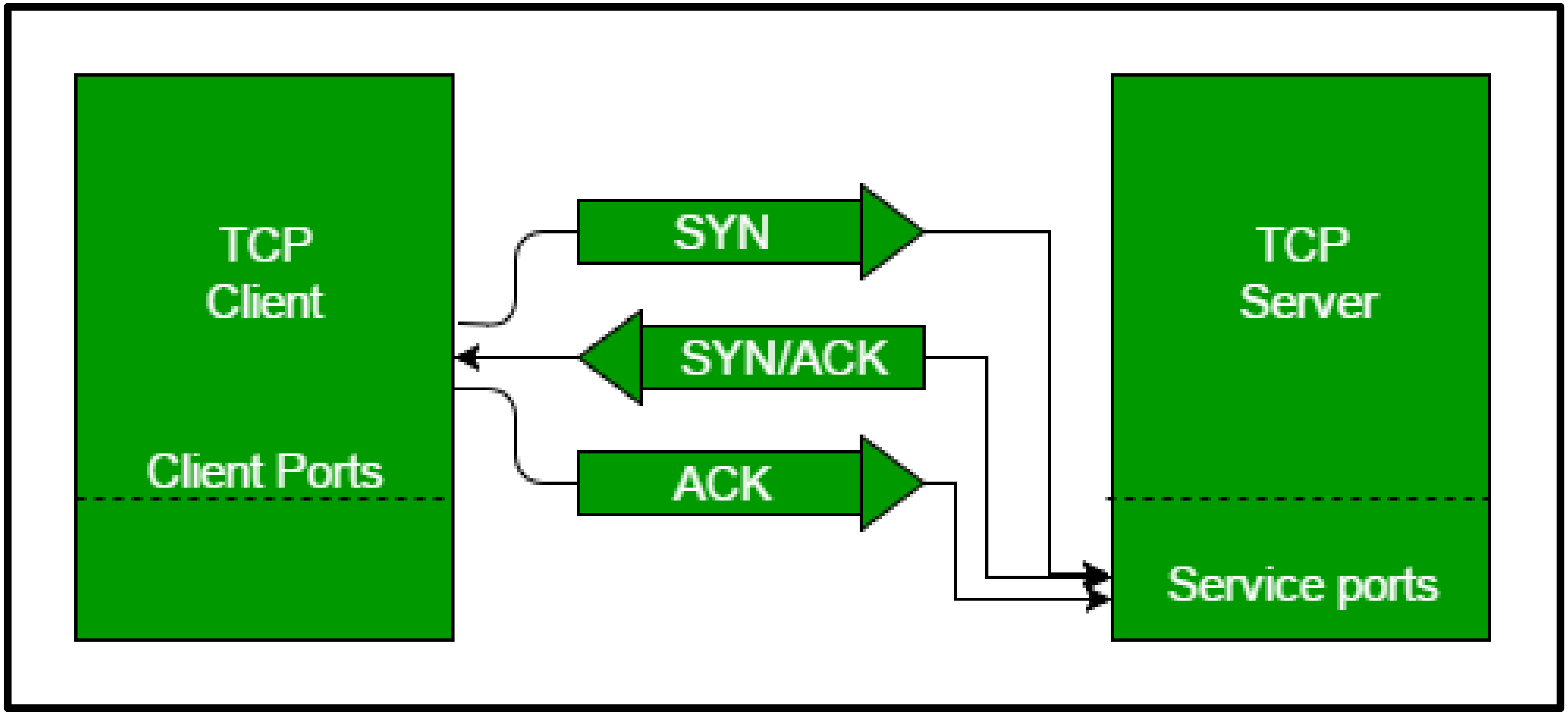
The server closes the connection only when it is not used for a certain configurable amount of time.

It requires as little as one round-trip time (RTT) for all the referenced objects.

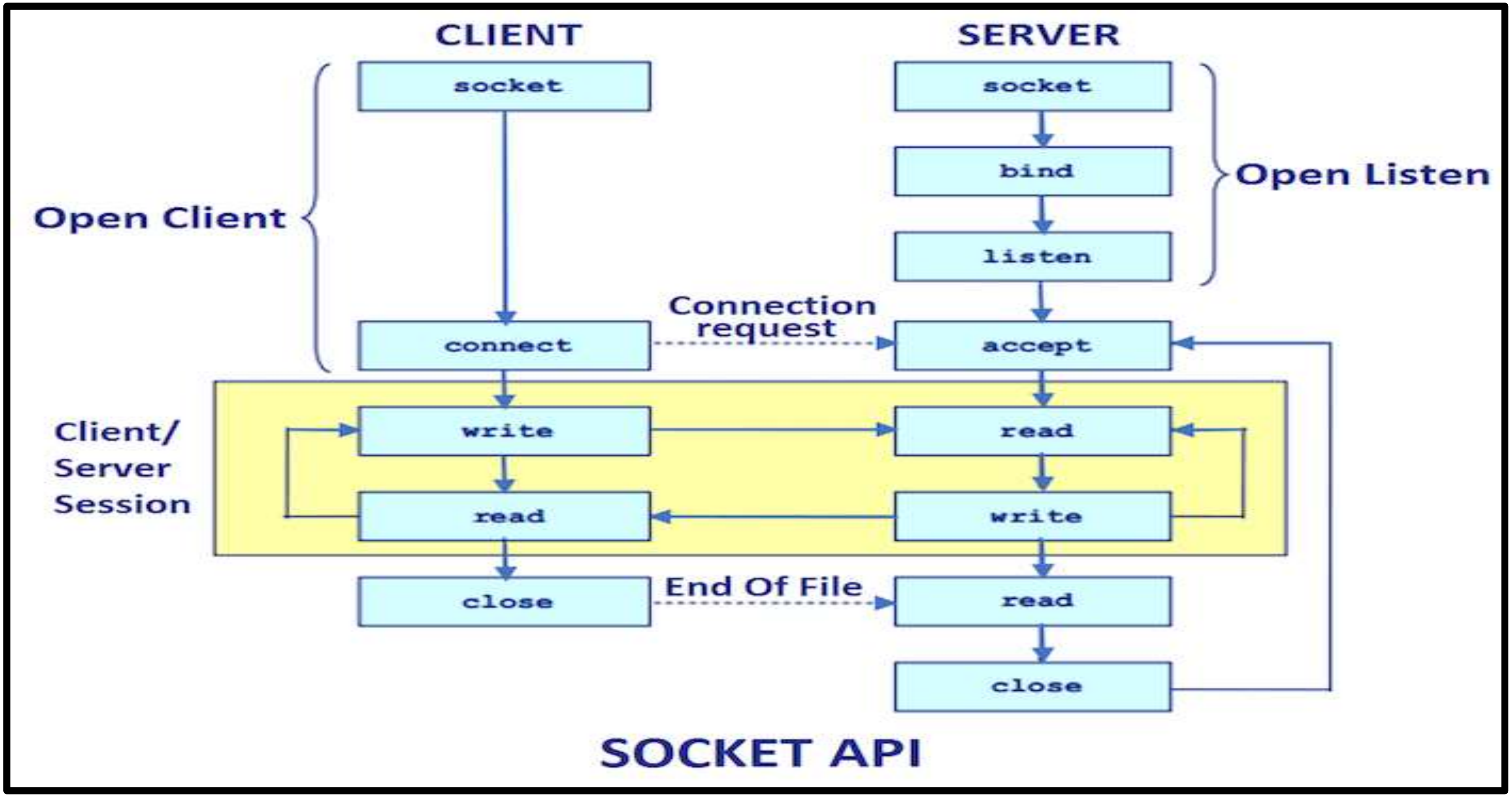
With persistent connections, the performance is improved by 20%.

Persistent connections are the default mode for HTTP/1.1.

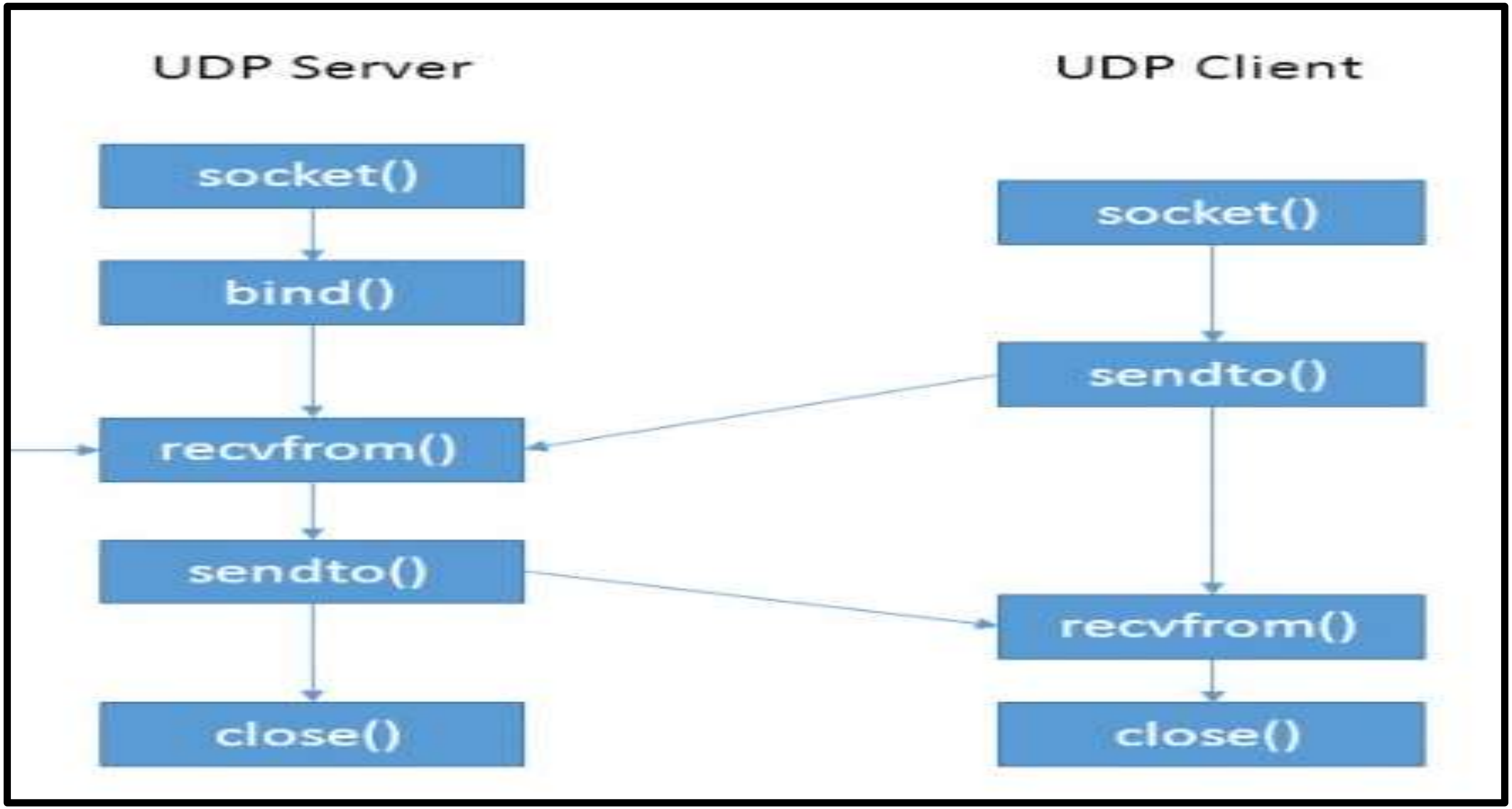
TCP 3 WAY HANDSHAKE



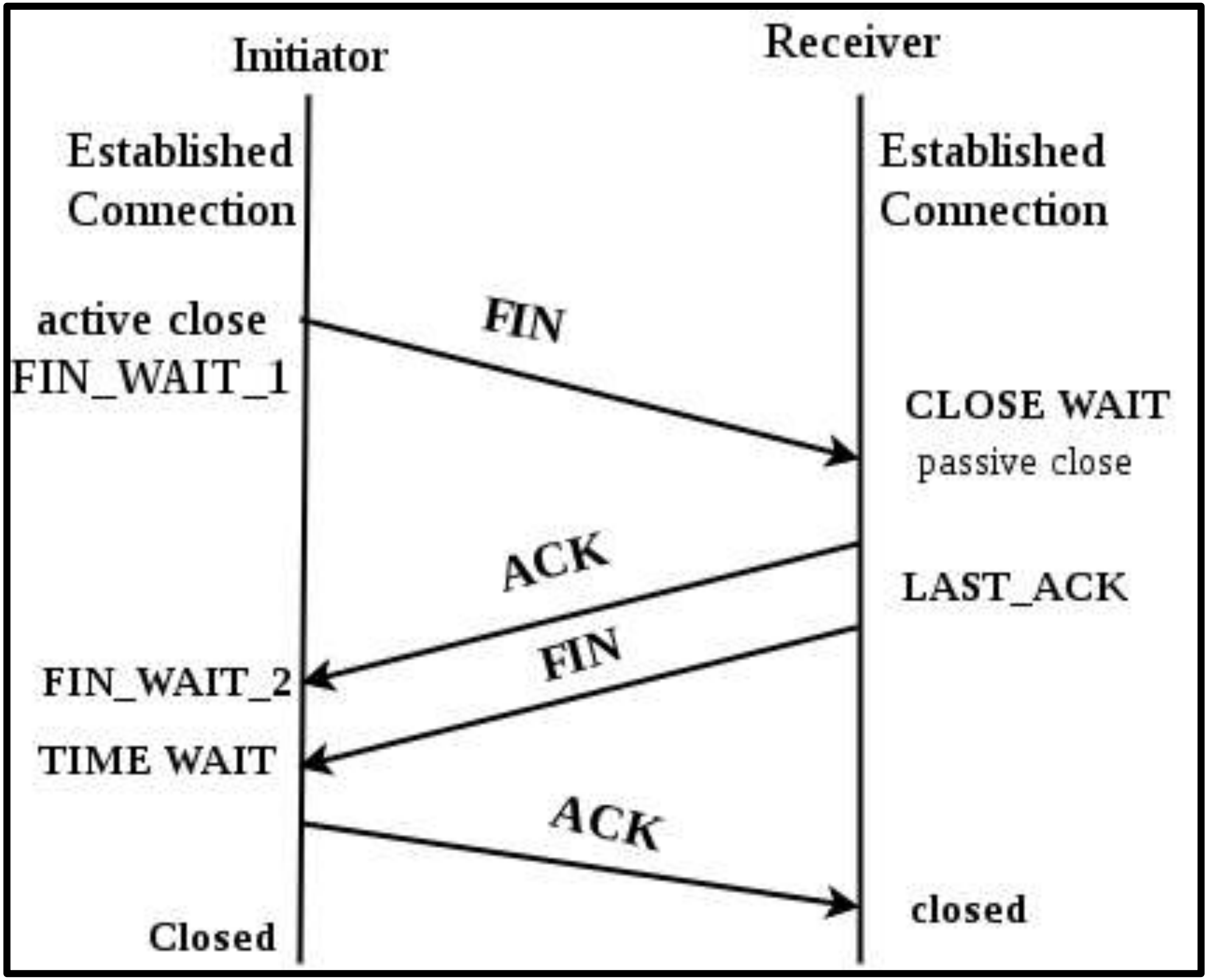
SOCKET PROG TCP



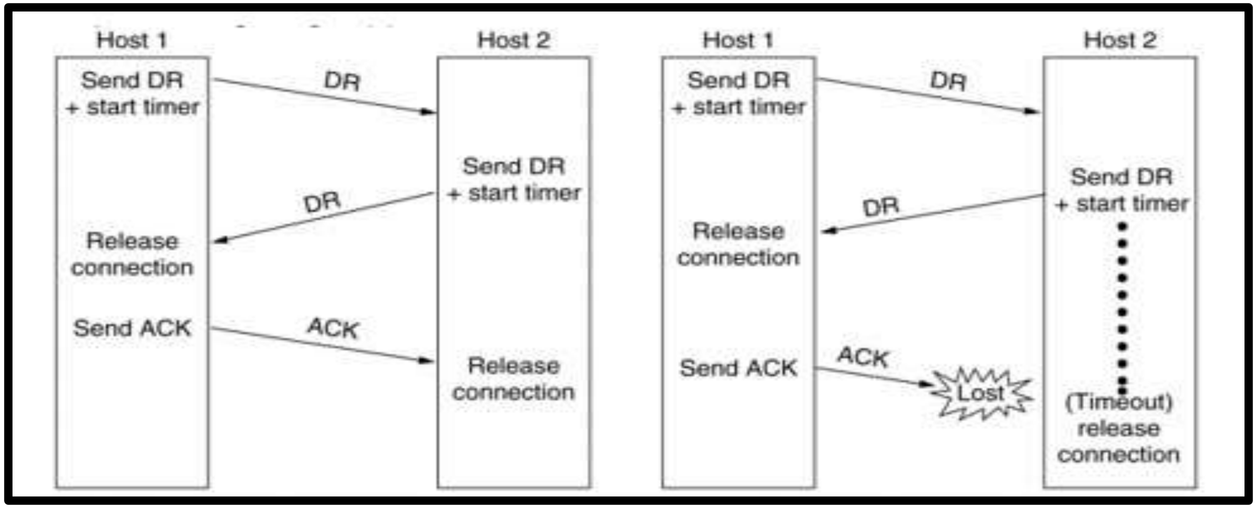
SOCKET PROG UDP

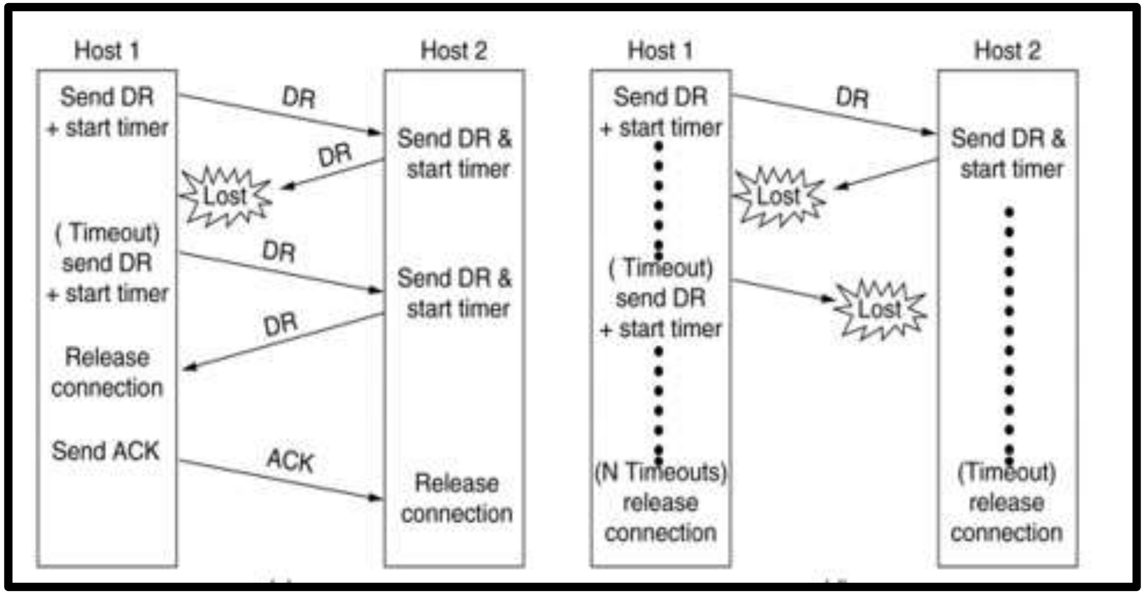


CONNECTION RELEASE

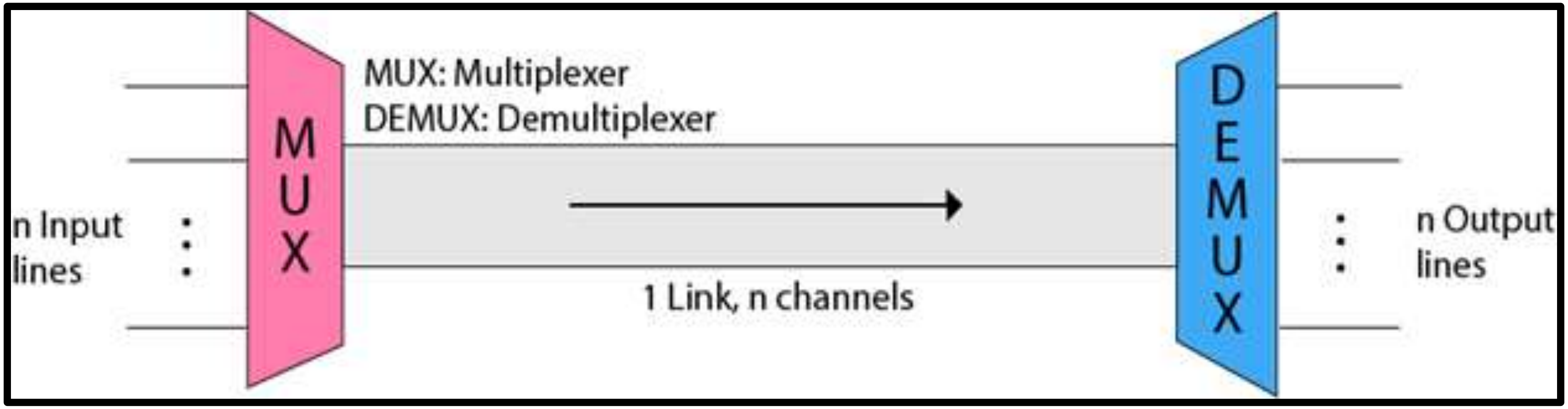


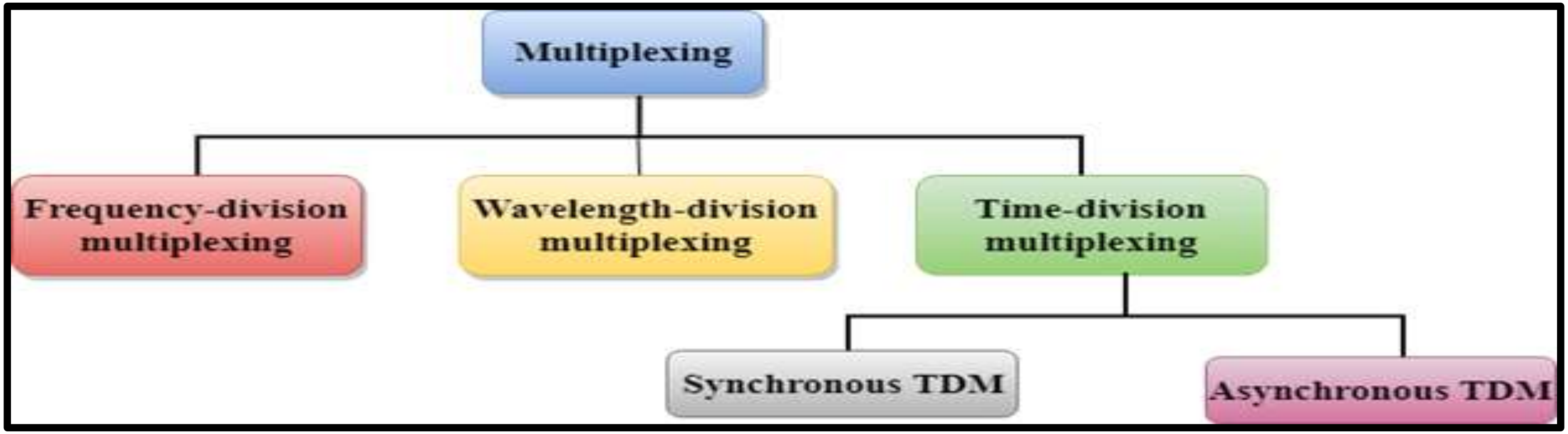
FOUR SCENARIO



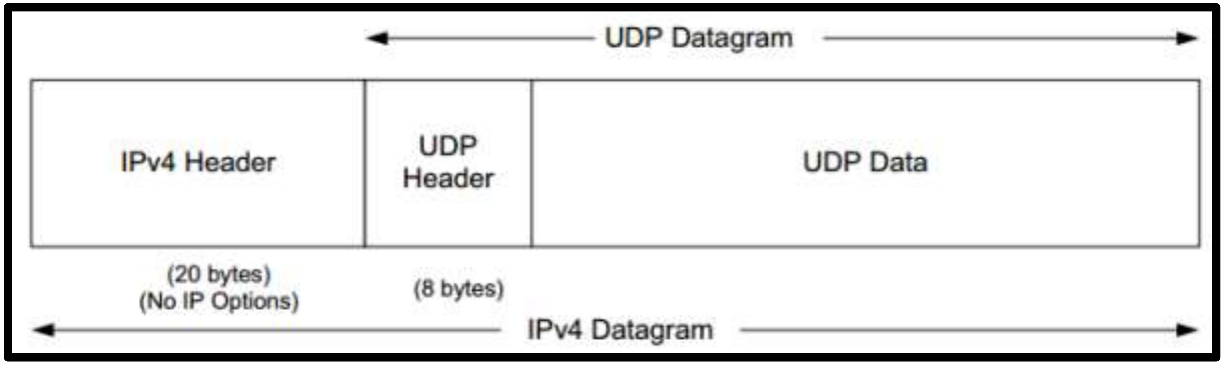


MUX DEMUX


MUX: Multiplexer
DEMUX: Demultiplexer
n Input lines
MUX
1 Link, n channels
DEMUX
n Output lines


Multiplexing
Frequency-division multiplexing
Wavelength-division multiplexing
Time-division multiplexing
Synchronous TDM
Asynchronous TDM

UDP HEADER



UDP Datagram

IPv4 Header

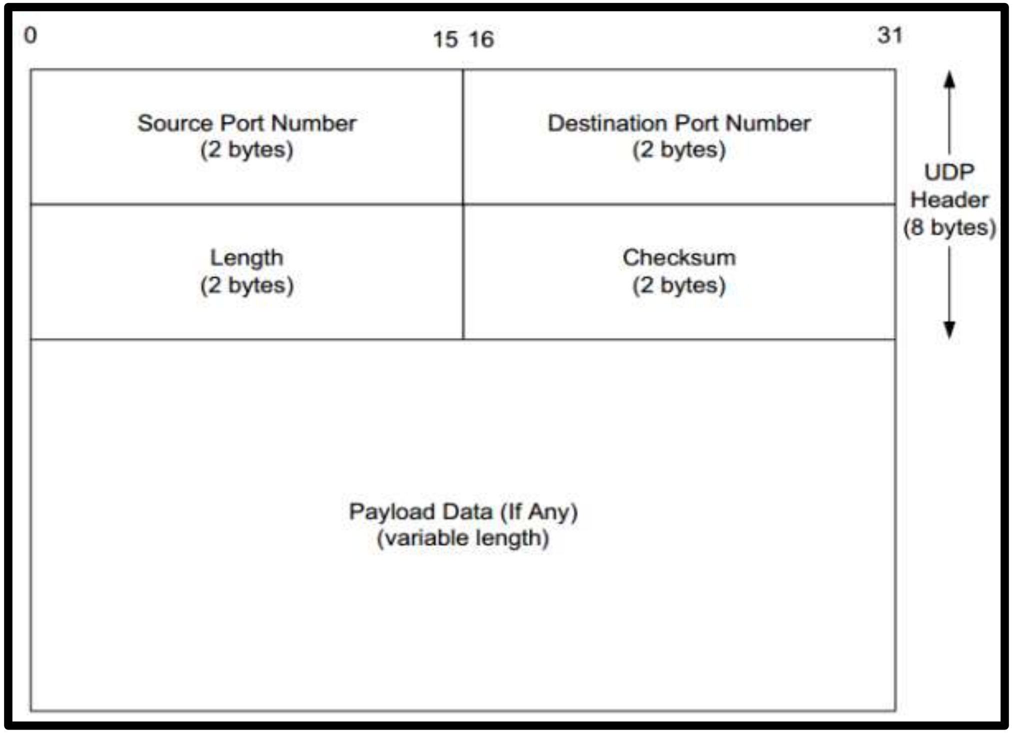
UDP Header

UDP Data

(20 bytes)
(No IP Options)

(8 bytes)

IPv4 Datagram



0 15 16 31

Source Port Number
(2 bytes)

Destination Port Number
(2 bytes)

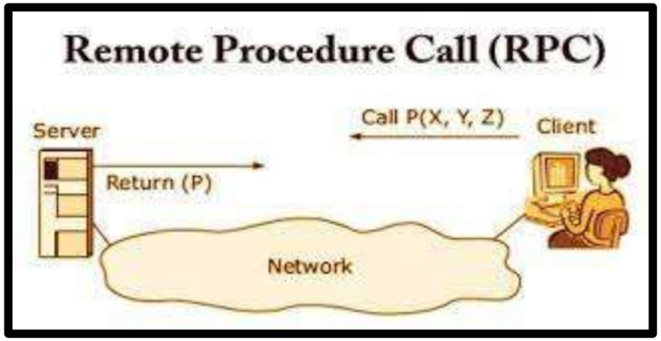
Length
(2 bytes)

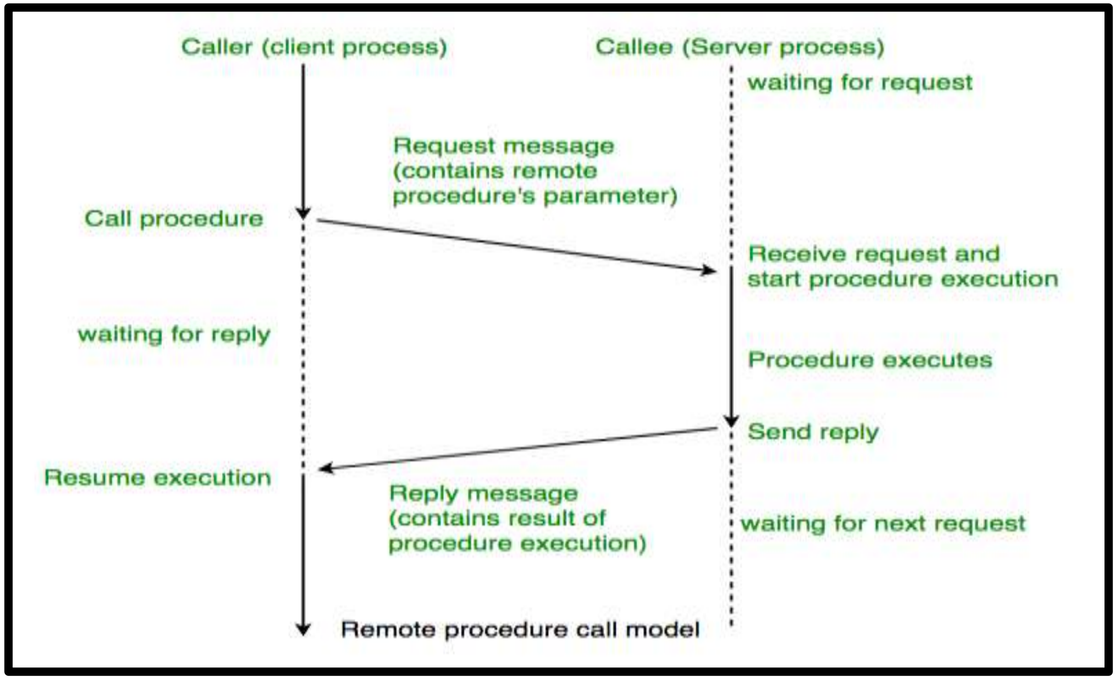
Checksum
(2 bytes)

UDP Header
(8 bytes)

Payload Data (If Any)
(variable length)

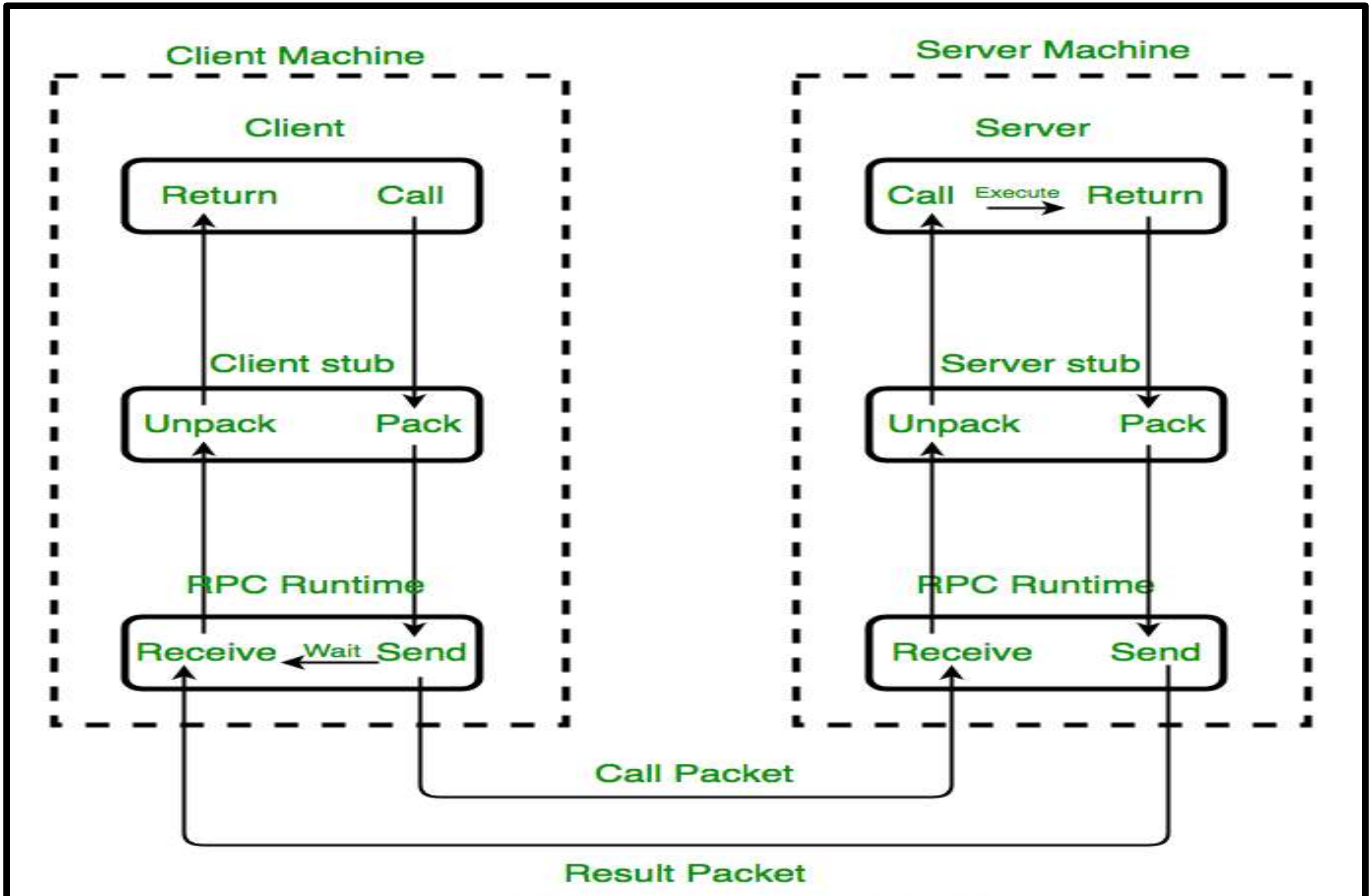
RPC





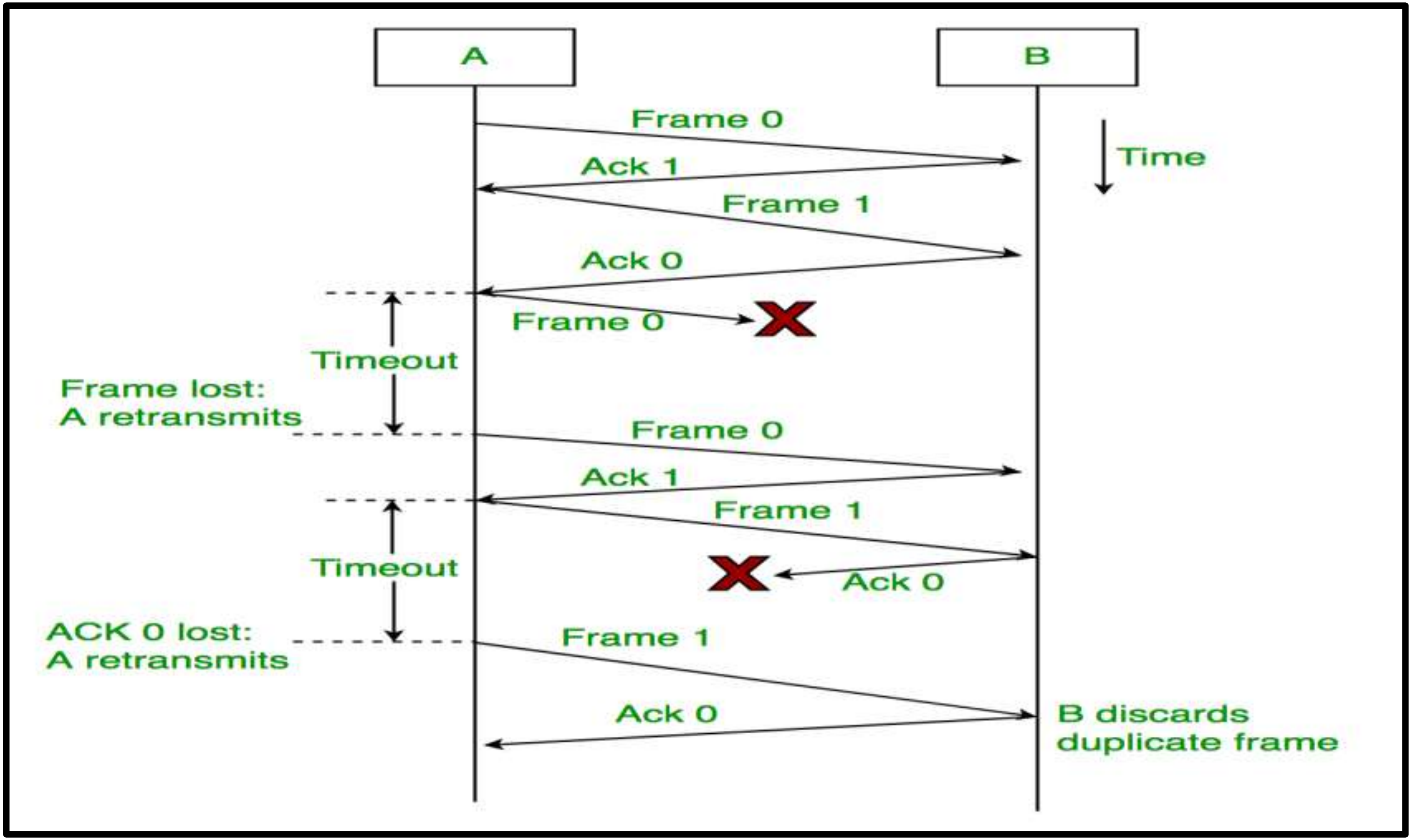
Remote procedure call model

RPC

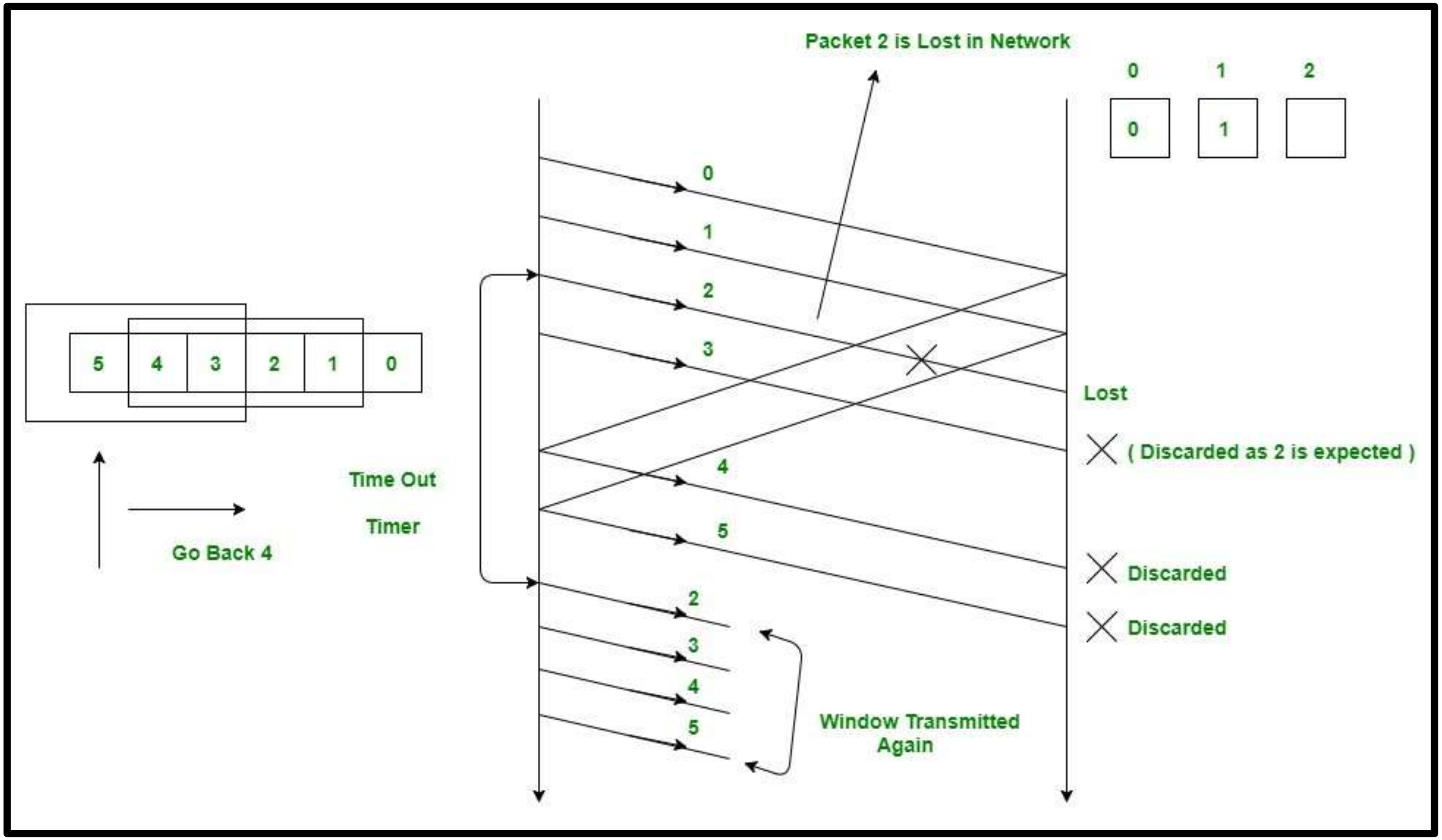


Implementation of RPC mechanism

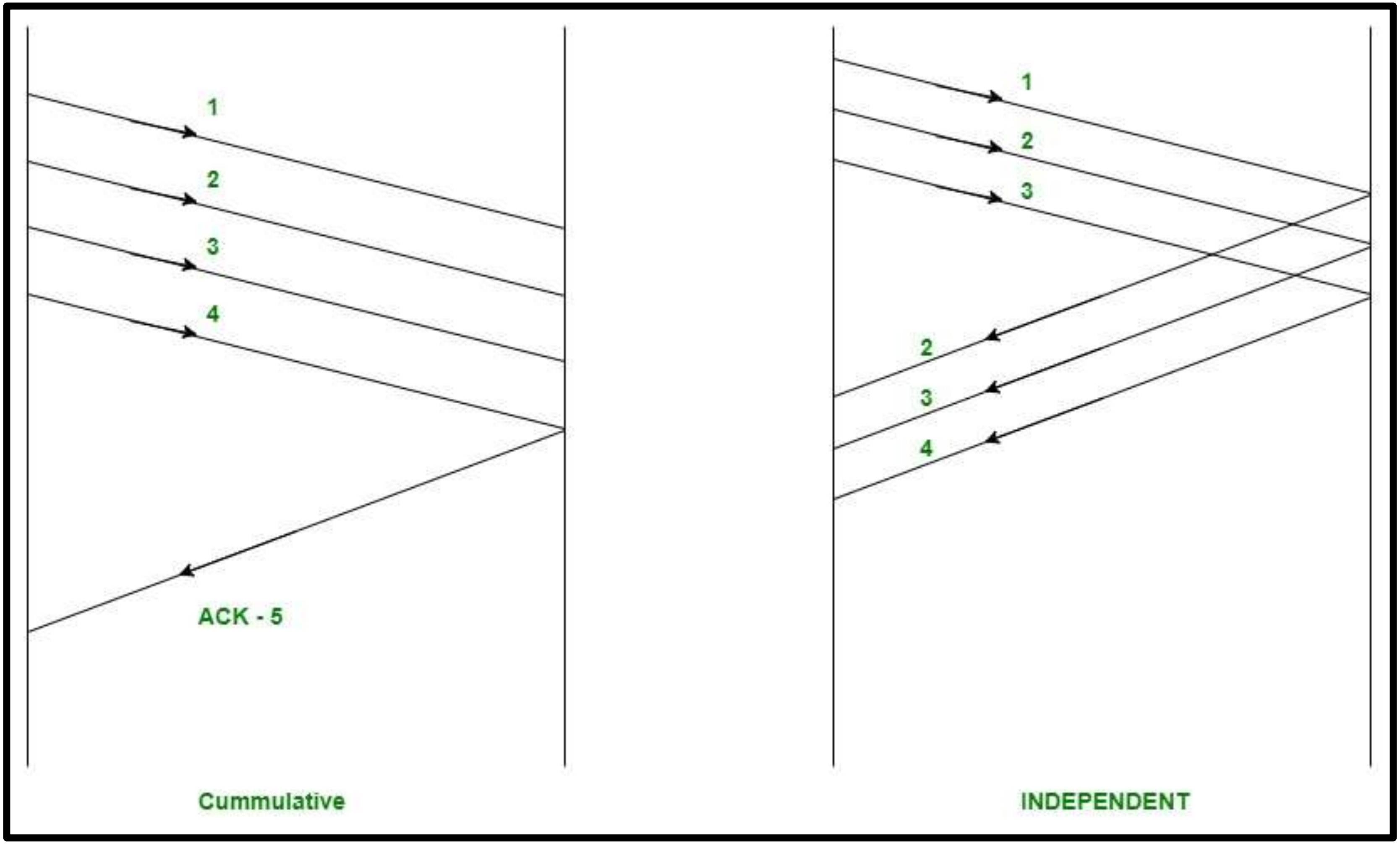
STOP AND WAIT



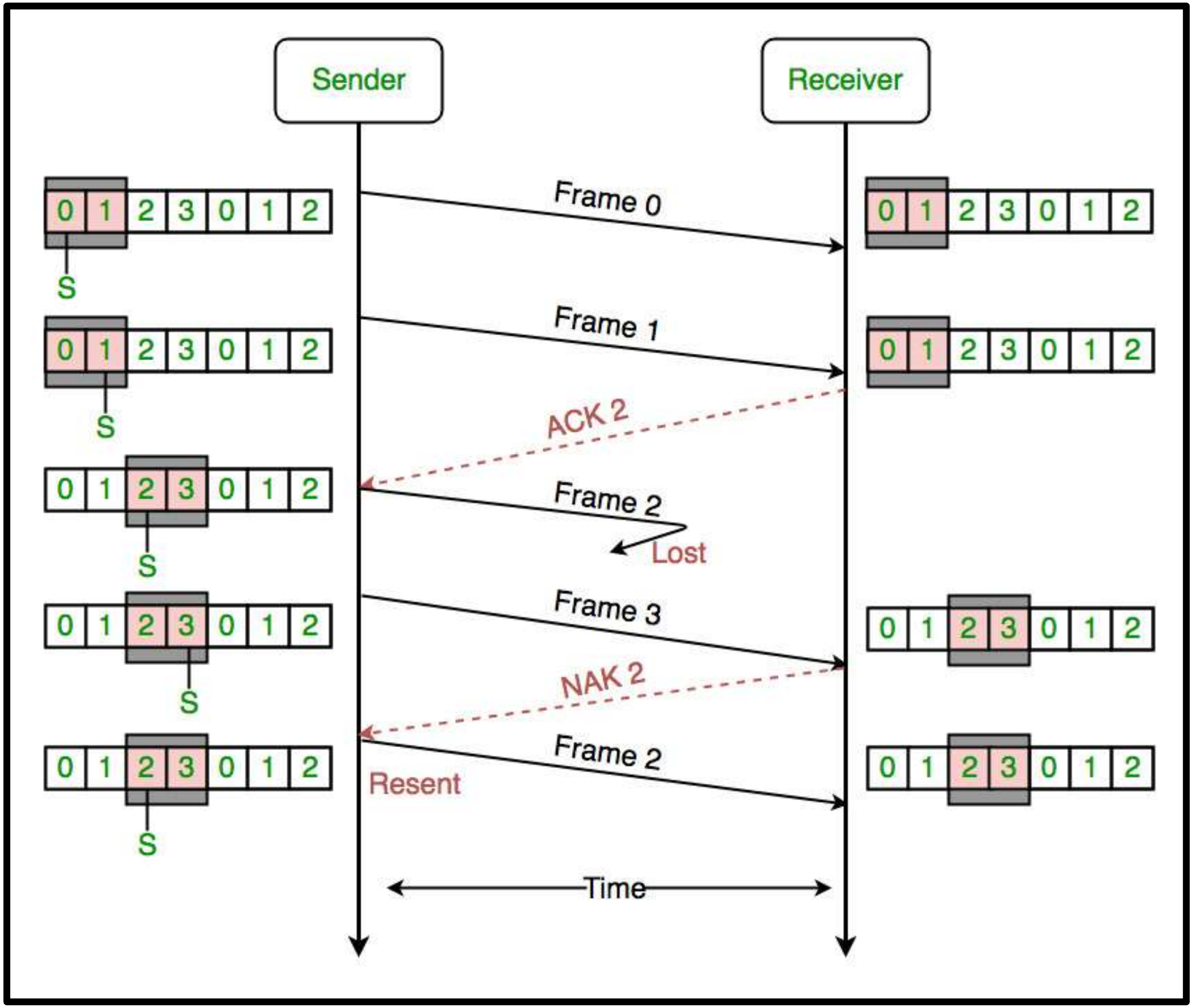
GO BACK N (WS = 4, WR = 1)



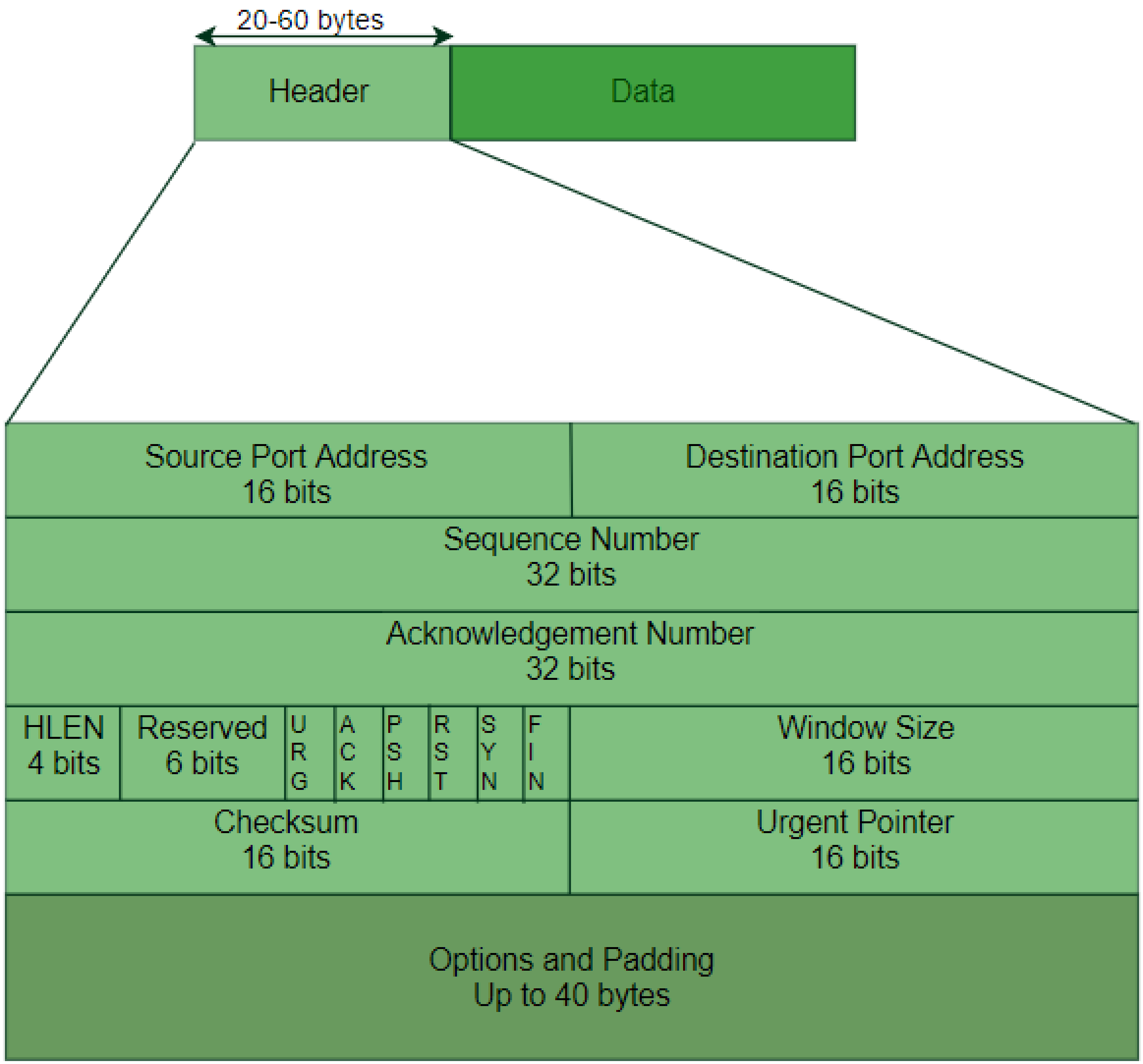
GO BACK N (WS = 4, WR = 1)



SELECTIVE REPEAT WS = WR = 2



TCP HEADER



20-60 bytes

Header

Data

Source Port Address
16 bits

Destination Port Address
16 bits

Sequence Number
32 bits

Acknowledgement Number
32 bits

HLEN
4 bits

Reserved
6 bits

URG

ACK

PSH

RST

SYN

FIN

Window Size
16 bits

Checksum
16 bits

Urgent Pointer
16 bits

Options and Padding
Up to 40 bytes

TCP HEADER

- ✓ Source Port Address 16 bit field that holds the port address of the application that is sending the data segment.
- ✓ Destination Port Address 16 bit field that holds the port address of the application in the host that is receiving the data segment.
- ✓ Sequence Number 32 bit field that holds the sequence number, i.e, the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end if the segments are received out of order.
- ✓ Acknowledgement Number 32 bit field that holds the acknowledgement number, i.e, the byte number that the receiver expects to receive next. It is an acknowledgement for the previous bytes being received successfully.

TCP HEADER

- ✓ Header Length (HLEN) This is a 4 bit field that indicates the length of the TCP header by number of 4-byte words in the header, i.e, if the header is of 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.
- ✓ Control flags These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc.

URG: Urgent pointer is valid

ACK: Acknowledgement number is valid(used in case of cumulative acknowledgement)

PSH: Request for push

RST: Reset the connection

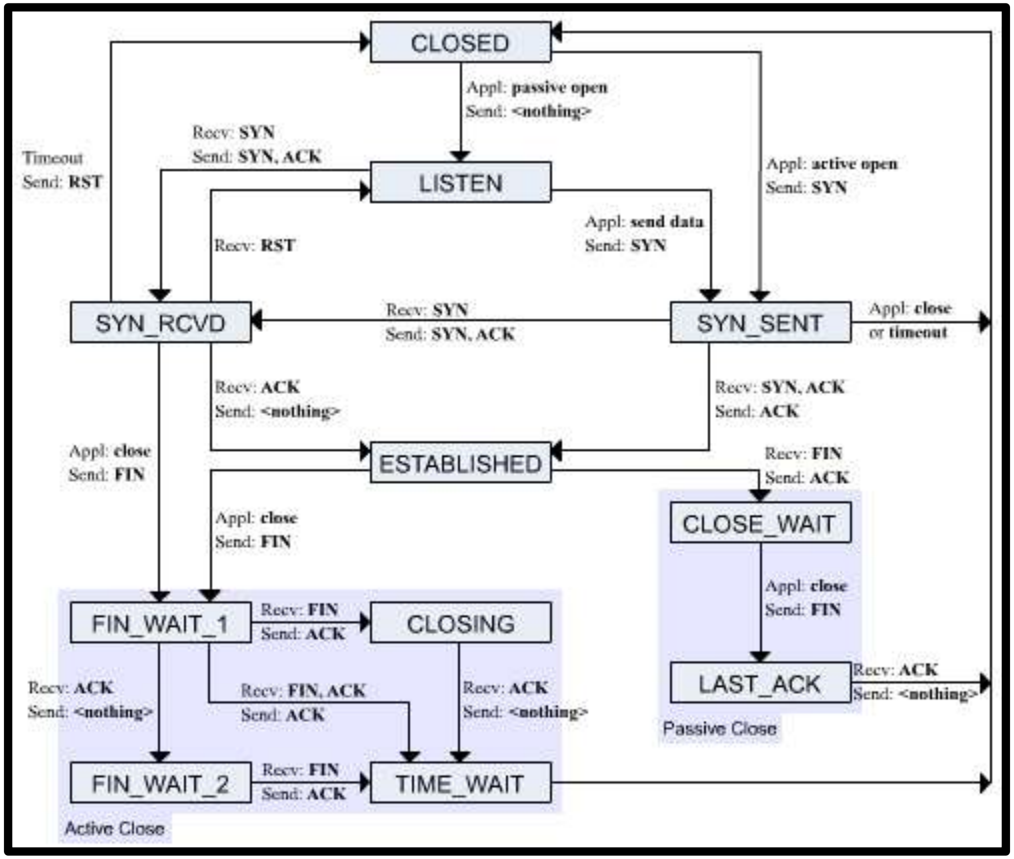
SYN: Synchronize sequence numbers

FIN: Terminate the connection

TCP HEADER

- ✓ Window size This field tells the window size of the sending TCP in bytes.
- ✓ Checksum This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.
- ✓ Urgent pointer This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

TCP FINITE STATE MACHINE



LEACKY BUCKET

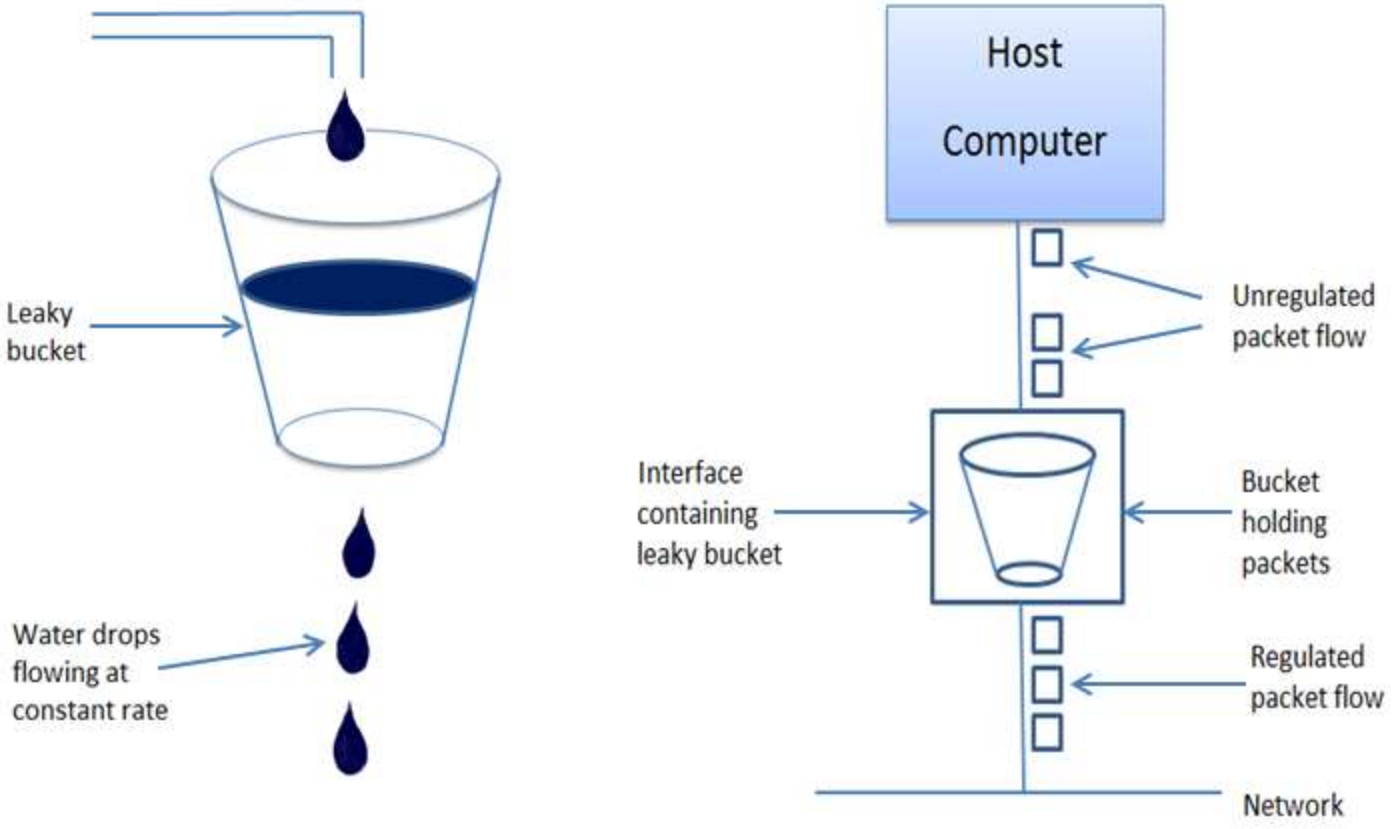
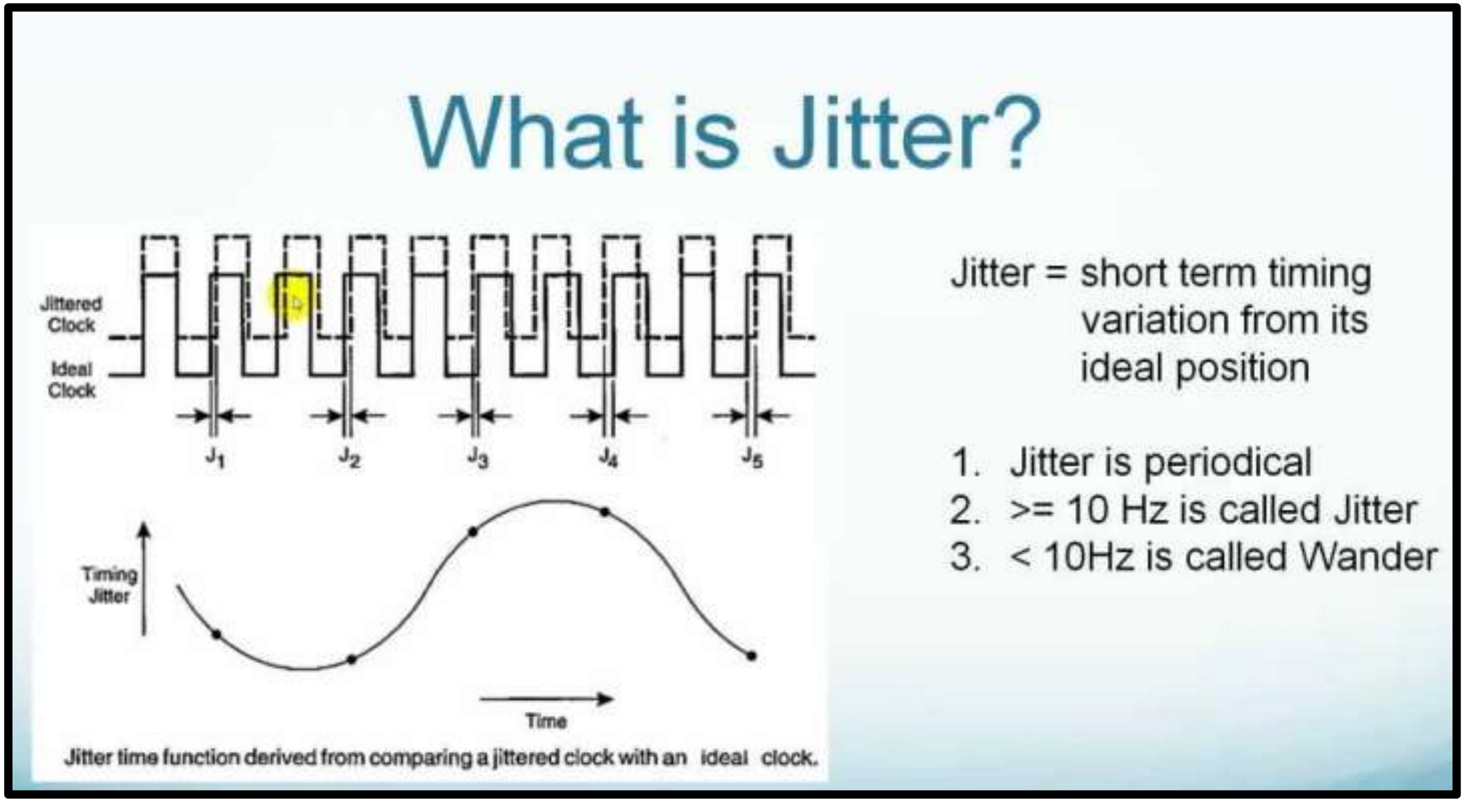


Fig: Leaky Bucket Algorithm

JITTER

- ✓ Information is transported from your computer in data packets across the internet. They are usually sent at regular intervals and take a set amount of time. Jitter is when there is a time delay in the sending of these data packets over your network connection. This is often caused by network congestion, and sometimes route changes.
- ✓ Essentially, the longer data packets take to arrive, the more jitter can negatively impact the video and audio quality.

JITTER



What is Jitter?

Jitter time function derived from comparing a jittered clock with an ideal clock.

Jitter = short term timing variation from its ideal position

1. Jitter is periodical
2. >= 10 Hz is called Jitter
3. < 10Hz is called Wander

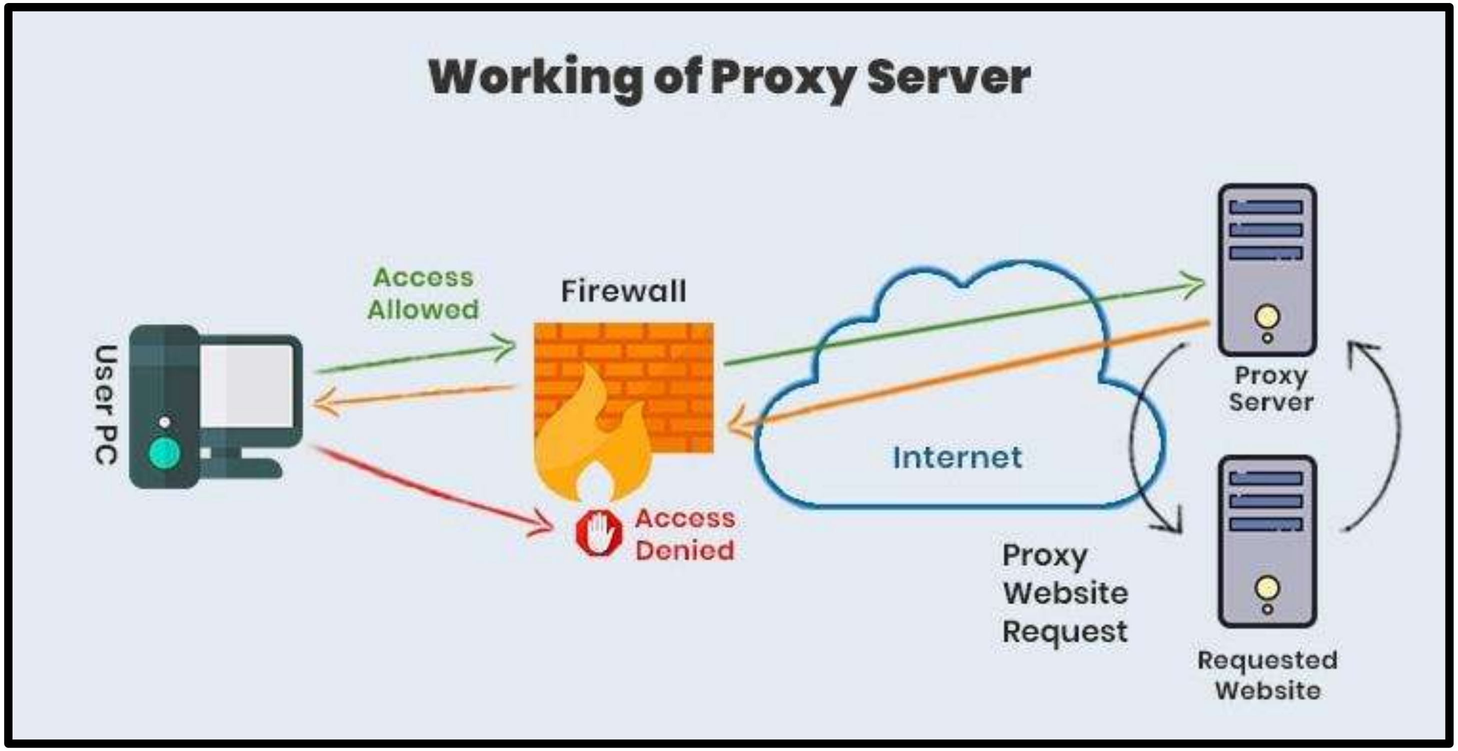
PROXY SERVER

- ✓ In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources. A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

PROXY SERVER

- ✓ Instead of connecting directly to a server that can fulfill a requested resource, such as a file or web page, the client directs the request to the proxy server, which evaluates the request and performs the required network transactions. This serves as a method to simplify or control the complexity of the request, or provide additional benefits such as load balancing, privacy, or security. Proxies were devised to add structure and encapsulation to distributed systems.

PROXY SERVER



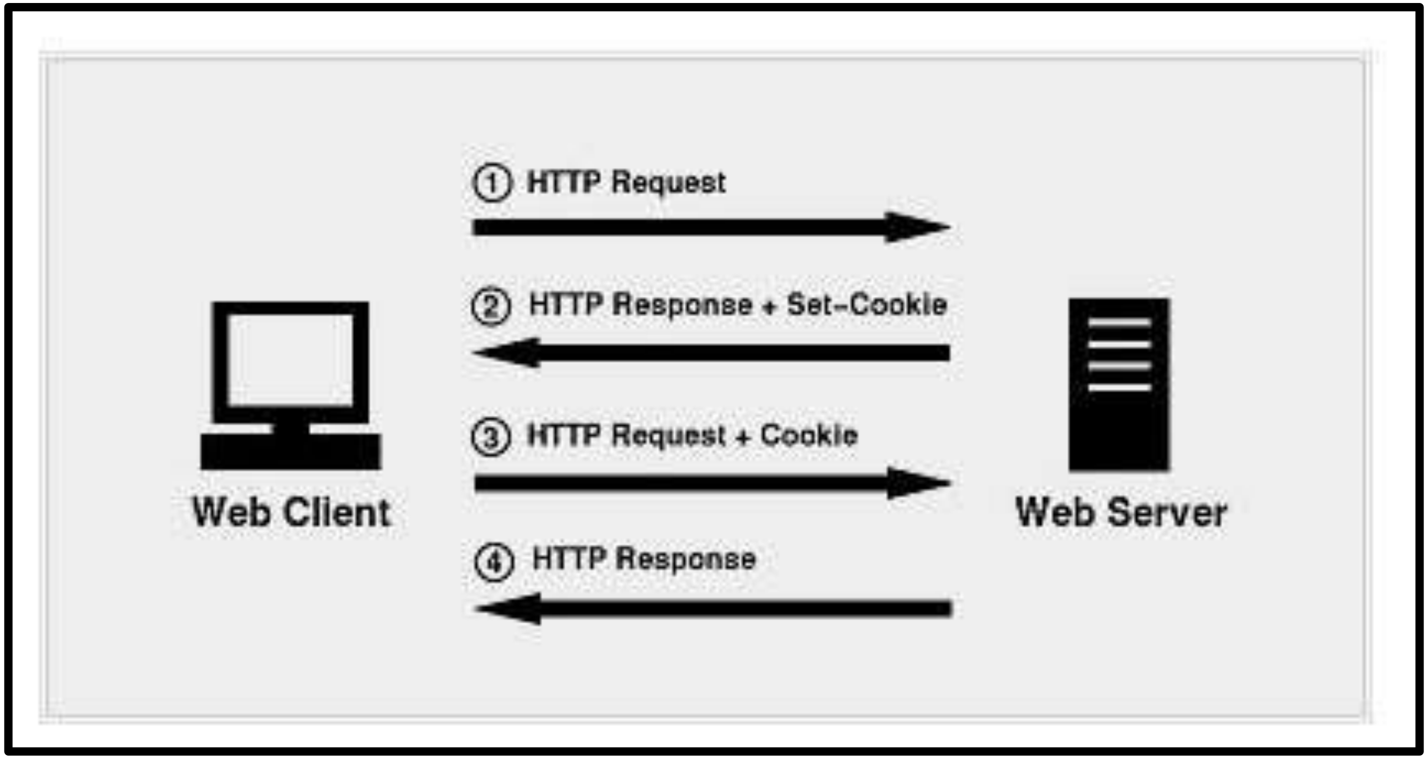
WEB COOKIES

- ✓ A lot of websites send a request to you when browsing their site. The message will appear in your browser saying that you need to allow cookies for best experience.
- ✓ Cookies, which are small files, are then stored on person’s computer.
- ✓ In terms, they also store personal data about you. Data within cookies will create a connection between a user and a particular website and can be accessed at any time either by web server or by client’s computer.

WEB COOKIES

- ✓ By using this data a website can create personalized experience.
- ✓ Main reason why sites add cookies in the first place is because they can’t store all this user data in one place as it would overburden their servers. Through cookies, a server is able to instantly access your data on the next visit and continue your daily session as if you never left the site.

WEB COOKIES


① HTTP Request
② HTTP Response + Set-Cookie
③ HTTP Request + Cookie
④ HTTP Response
Web Client
Web Server

HTML

- ✓ HTML stands for Hyper Text Markup Language
- ✓ HTML is the standard markup language for creating Web pages
- ✓ HTML describes the structure of a Web page
- ✓ HTML consists of a series of elements
- ✓ HTML elements tell the browser how to display the content
- ✓ HTML elements label pieces of content such as "this is a heading", "this is a paragraph", "this is a link", etc.

XML

✓ XML stands for eXtensible Markup Language

✓ XML is a markup language much like HTML

✓ XML was designed to store and transport data

✓ XML was designed to be self-descriptive

✓ XML is a W3C Recommendation

XSLT

✓ XSLT (eXtensible Stylesheet Language Transformations) is the recommended style sheet language for XML.

✓ XSLT is far more sophisticated than CSS. With XSLT you can add/remove elements and attributes to or from the output file. You can also rearrange and sort elements, perform tests and make decisions about which elements to hide and display, and a lot more.

✓ XSLT uses XPath to find information in an XML document.

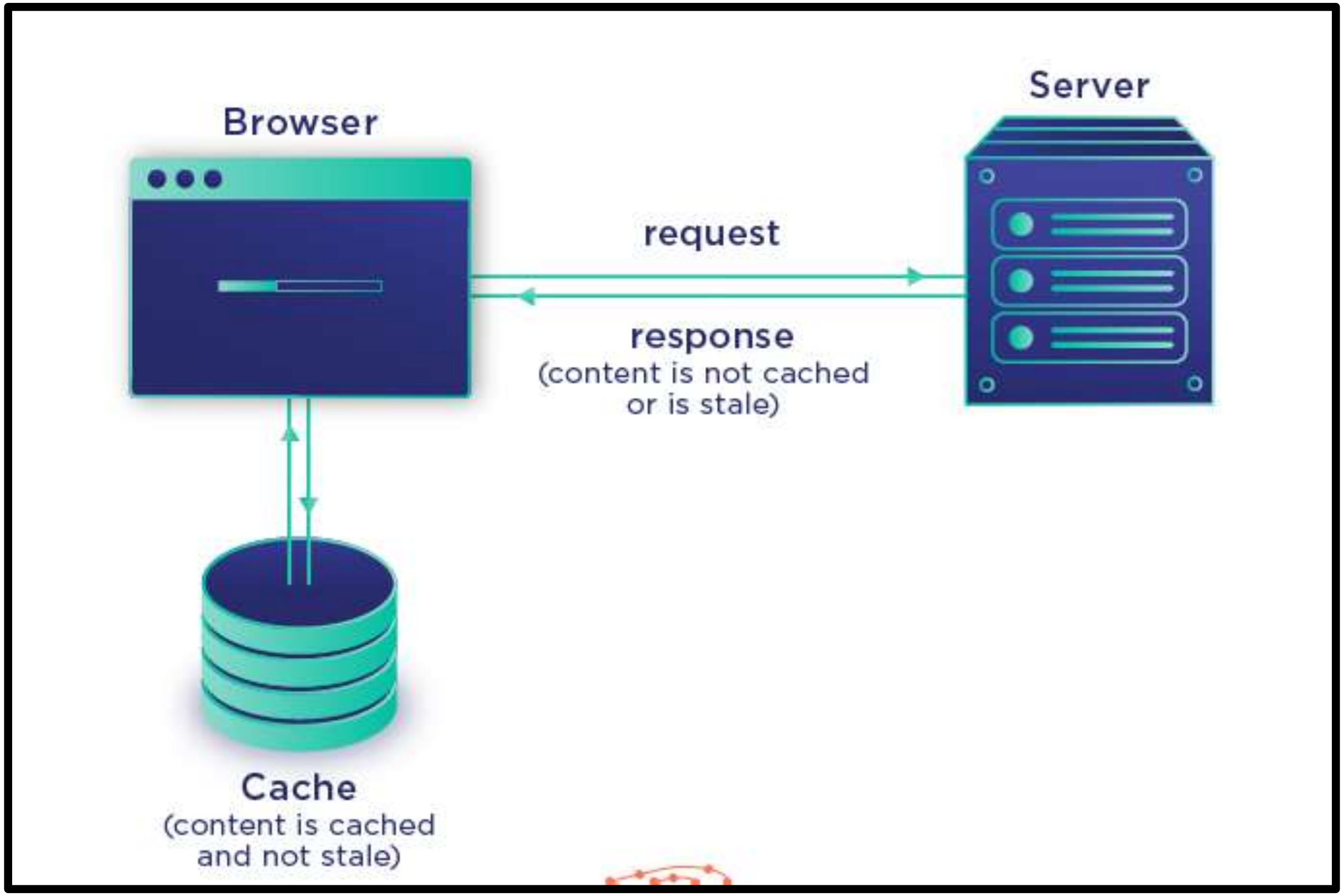
XHTML

- ✓ XHTML stands for Extensible Hypertext Markup Language
- ✓ XHTML is a stricter, more XML-based version of HTML
- ✓ XHTML is HTML defined as an XML application
- ✓ XHTML is supported by all major browsers

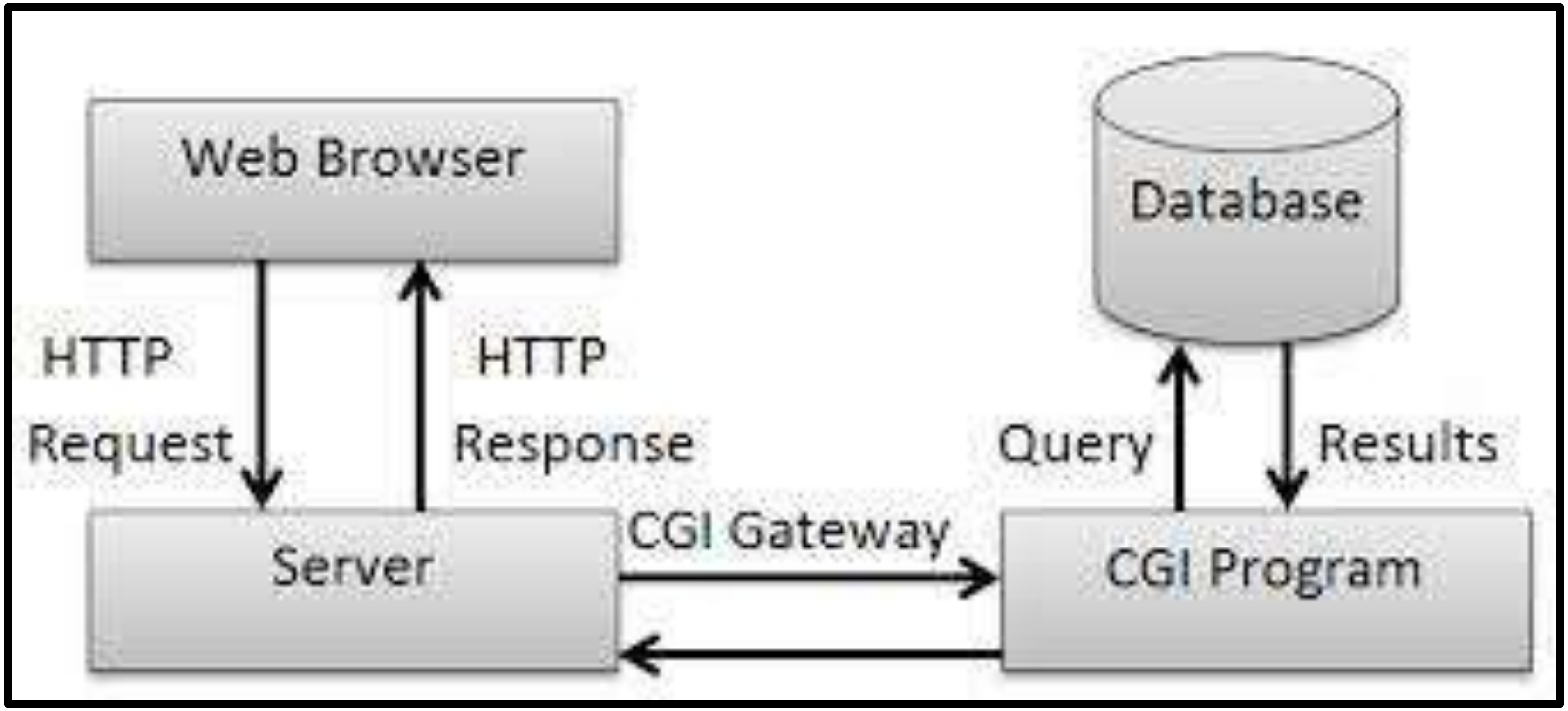
XHTML

- ✓ **Differences from HTML**
- ✓ <!DOCTYPE> is mandatory
- ✓ The xmlns attribute in <html> is mandatory
- ✓ <html>, <head>, <title>, and <body> are mandatory
- ✓ Elements must always be properly nested
- ✓ Elements must always be closed
- ✓ Elements must always be in lowercase
- ✓ Attribute names must always be in lowercase
- ✓ Attribute values must always be quoted

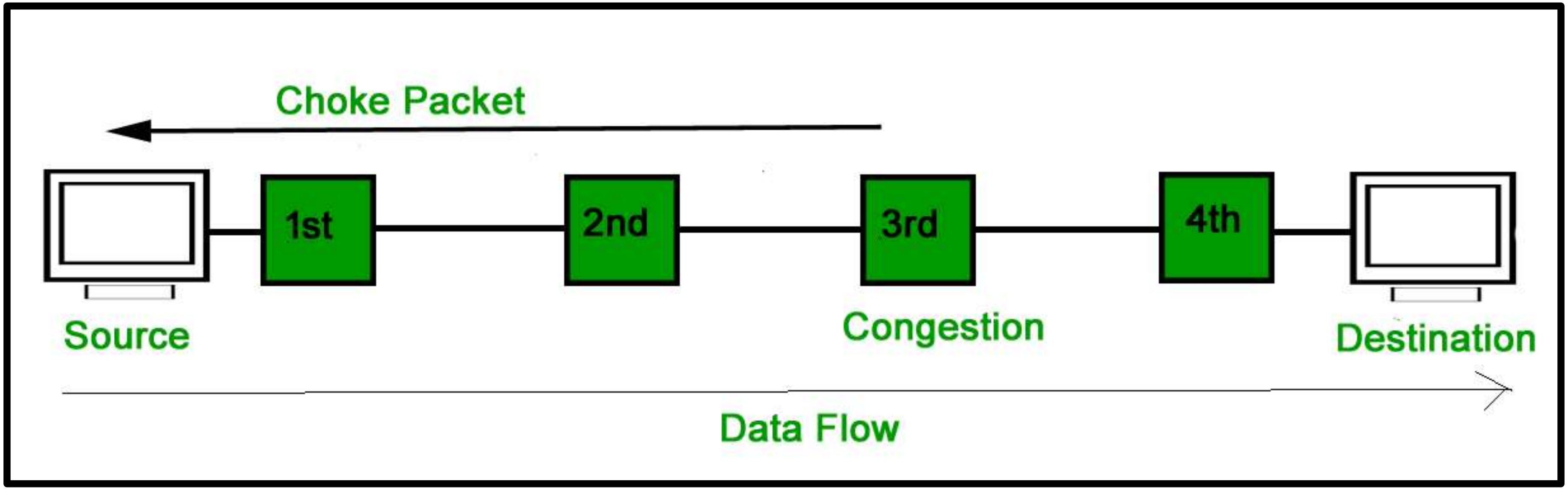
CACHE MEMORY



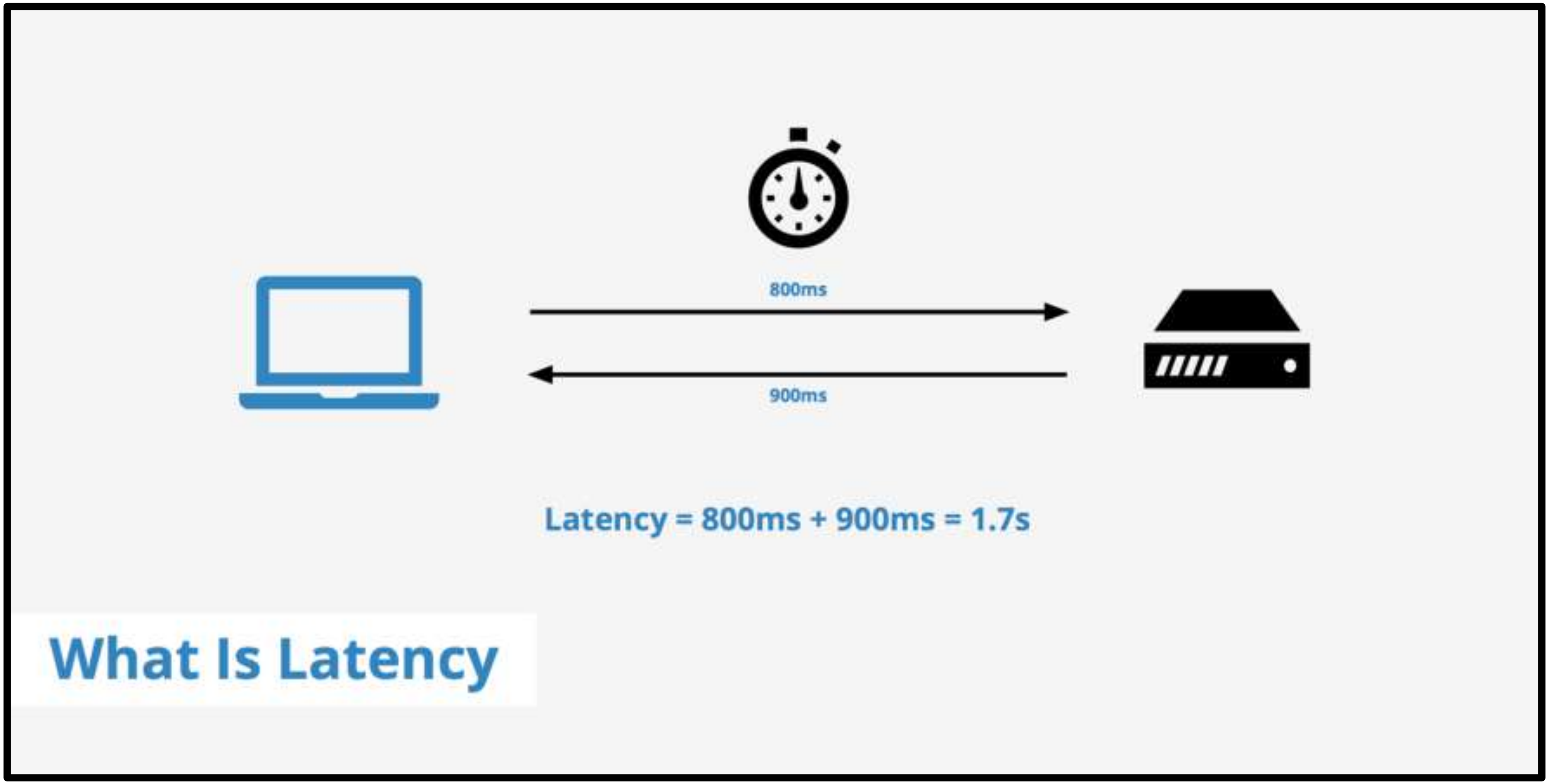
COMMON GATEWAY INTERFACE



CHOKE PACKETS



LATENCY



800ms

900ms

Latency = 800ms + 900ms = 1.7s

What Is Latency

EXAMPLE

1) Consider a source computer (S) transmitting a file of size 106 bits to a destination computer (D) over a network of two routers (R1 and R2) and three links (L1, L2 and L3). L1 connects S to R1;L2 connects R1 to R2; and L3 connects R2 to D. Let each link be of length 100km. Assume signals travel over each link at a speed of 10^8 meters per second. Assume that the link bandwidth on each link is 1Mbps. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D?

(A) 1005ms

(B) 1010ms

(C) 3000ms

(D) 3003ms

EXAMPLE

- ✓ Propagation delay to travel from S to R1 = (Distance) / (Link Speed) = 10^5/10^8 = 1ms
  Total prorogation delay to travel from S to D = 3*1 ms = 3ms
- ✓ Total Transmission delay for 1 packet = 3 * (Number of Bits) / Bandwidth = 3*(1000/10^6) = 3ms.

The first packet will take 6ms to reach D. While first packet was reaching D, other packets must have been processing in parallel.

So D will receive remaining packets 1 packet per 1 ms from R2. So remaining 999 packets will take 999 ms. And total time will be 999 + 6 = 1005 ms

EXAMPLE

m1:Send an email from a mail client to mail server

m2:Download an email from mailbox server to a mail client

m3:Checking email in a web browser

(A) m1:HTTP, m2:SMTP, m3:POP

(B) m1:SMTP, m2:FTP, m3:HTTP

(C) m1:SMTP, m2:POP, m3:HTTP

(D) m1:POP, m2:SMTP, m3:IMAP

EXAMPLE

m1:Send an email from a mail client to mail server

m2:Download an email from mailbox server to a mail client

m3:Checking email in a web browser

(A) m1:HTTP, m2:SMTP, m3:POP
(B) m1:SMTP, m2:FTP, m3:HTTP
(C) m1:SMTP, m2:POP, m3:HTTP
(D) m1:POP, m2:SMTP, m3:IMAP

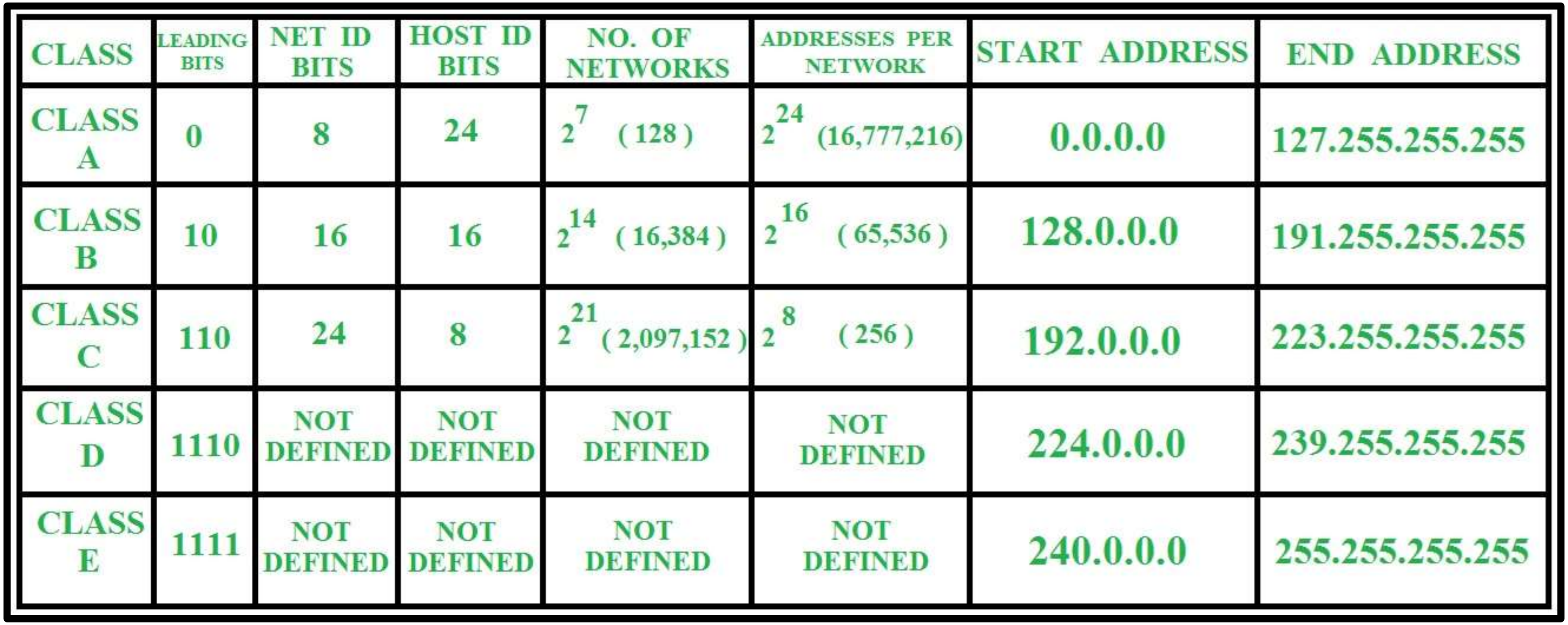
Answer (C)

Simple Mail Transfer Protocol (SMTP) is typically used by user clients for sending mails.

Post Office Protocol (POP) is used by clients for receiving mails.

Checking mails in web browser is a simple HTTP process.

CLASSFUL ADDRESSING



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^{7} (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^{8} (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

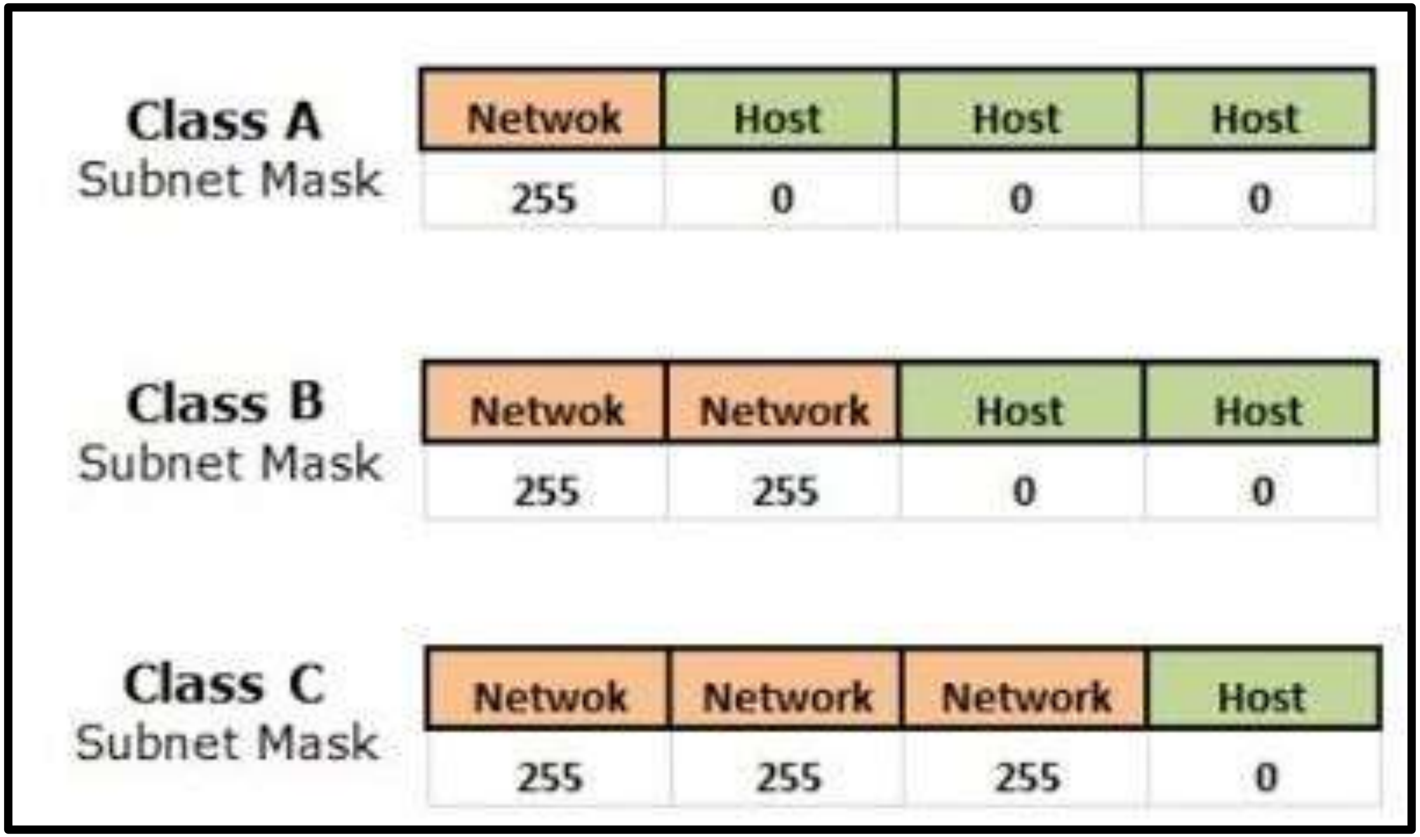
EXAMPLE

- ✓ **In the IPv4 addressing format, the number of networks allowed under Class C addresses is**
  (A) 2^14
  (B) 2^7
  (C) 2^21
  (D) 2^24
- ✓ Answer (C)
  In class C, 8 bits are reserved for Host Id and 24 bits are reserved for Network Id. Out of these 24 Network Id bits, the leading 3 bits are fixed as 110. So remaining 21 bits can be used for different networks.

SUBNET MASK

- ✓ A subnet mask is a 32 bits address used to distinguish between a network address and a host address in IP address.
- ✓ A subnet mask identifies which part of an IP address is the network address and the host address.
- ✓ They are not shown inside the data packets traversing the Internet. They carry the destination IP address, which a router will match with a subnet.

SUBNET MASK



Class A
Subnet Mask

Netwok	Host	Host	Host
255	0	0	0

Class B
Subnet Mask

Netwok	Network	Host	Host
255	255	0	0

Class C
Subnet Mask

Netwok	Network	Network	Host
255	255	255	0

EXAMPLE

✓ **An organization has a class B network and wishes to form subnets for 64 departments. The subnet mask would be:**

(a) 255.255.0.0
(b) 255.255.64.0
(c) 255.255.128.0
(d) 255.255.252.0

Answer (d)

The size of network ID is 16 bit in class B networks. So bits after 16th bit must be used to create 64 departments. Total 6 bits are needed to identify 64 different departments. Therefore, subnet mask will be 255.255.252.0.

EXAMPLE

- ✓ Considering the IP addresses 193.62.83.10 and 193.62.83.108 and an associated mask of 255.255.255.224
- ✓ 11000001 00111100 01010011 00001010 193.62.83.10
- ✓ 11111111 11111111 11111111 11100000 255.255.255.224
- ✓ 11000001 00111100 01010011 00000000 193.62.83.0
- ✓ So IP address 193.62.83.10 lies within the subnet that starts at 193.62.83.0.
- ✓ 11000001 00111100 01010011 01101100 193.62.83.108
- ✓ 11111111 11111111 11111111 11100000 255.255.255.224
- ✓ 11000001 00111100 01010011 01100000 193.62.83.96
- ✓ So IP address 193.62.83.108 lies within the subnet that starts at 193.62.83.96

EXAMPLE

✓ What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?

✓ A. 14

✓ B. 15

✓ C . 16

✓ D. 30

✓ D A /27 (255.255.255.224) is 3 bits on and 5 bits off. This provides 8 subnets, each with 30 hosts.

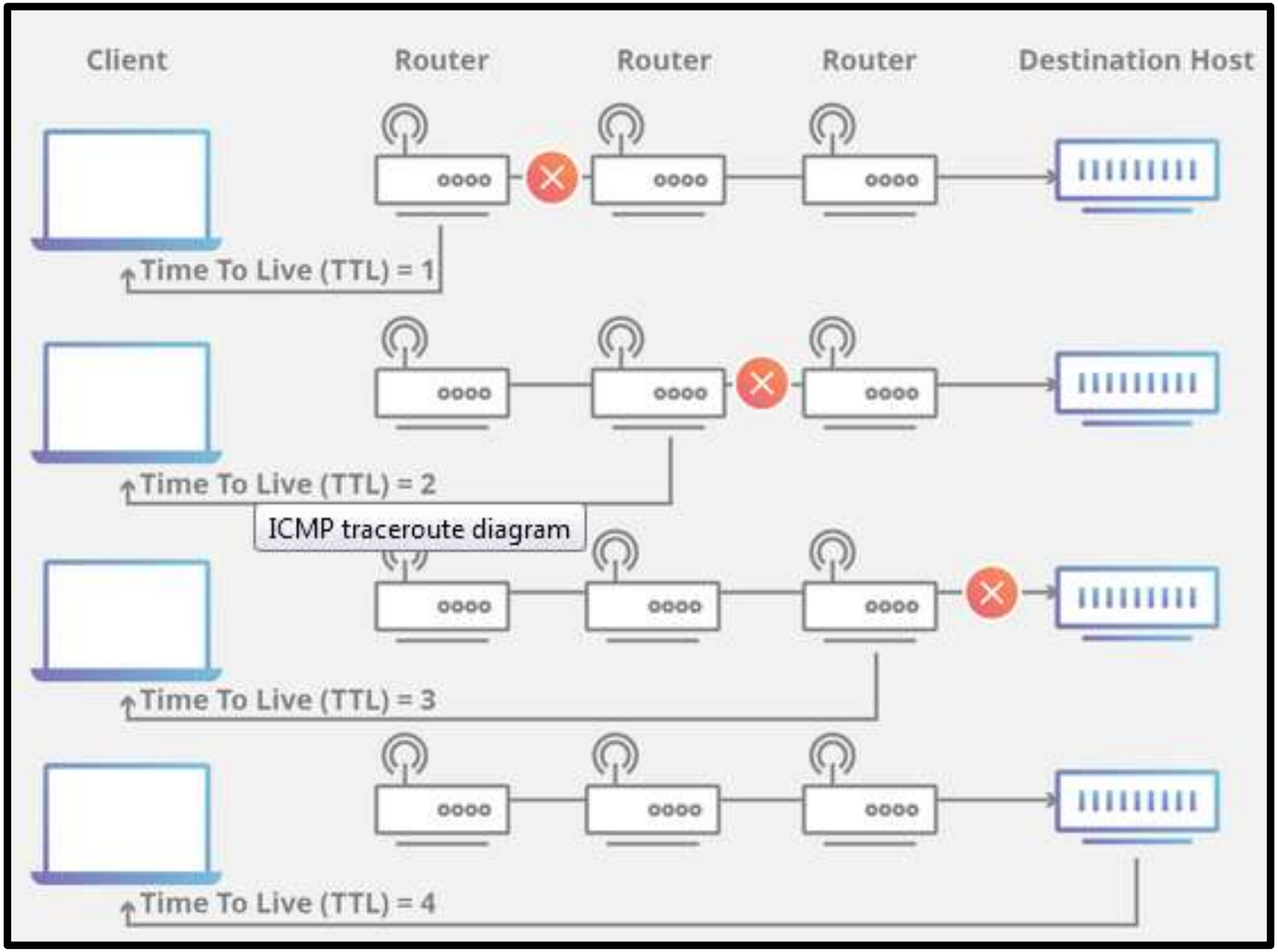
EXAMPLE

- ✓ You have a network that needs 29 subnets while maximizing the number of host addresses available on each subnet. How many bits must you borrow from the host field to provide the correct subnet mask?
- ✓ A. 2
- ✓ B. 3
- ✓ C. 4
- ✓ D. 5
- ✓ D A 240 mask is 4 subnet bits and provides 16 subnets, each with 14 hosts. We need more subnets, so let's add subnet bits. One more subnet bit would be a 248 mask. This provides 5 subnet bits (32 subnets) with 3 host bits (6 hosts per subnet). This is the best answer.

TIME-TO-LIVE (TTL)

✓ When a packet of information is created and sent out across the Internet, there is a risk that it will continue to pass from router to router indefinitely. To mitigate this possibility, packets are designed with an expiration called a time-to-live or hop limit. Packet TTL can also be useful in determining how long a packet has been in circulation, and allow the sender to receive information about a packet’s path through the Internet.

TIME-TO-LIVE (TTL)



EXAMPLE

- ✓ **One of the header fields in an IP datagram is the Time to Live (TTL) field. Which of the following statements best explains the need for this field?**
  (A) It can be used to prioritize packets
  (B) It can be used to reduce delays
  (C) It can be used to optimize throughput
  (D) It can be used to prevent packet looping

ROUTING

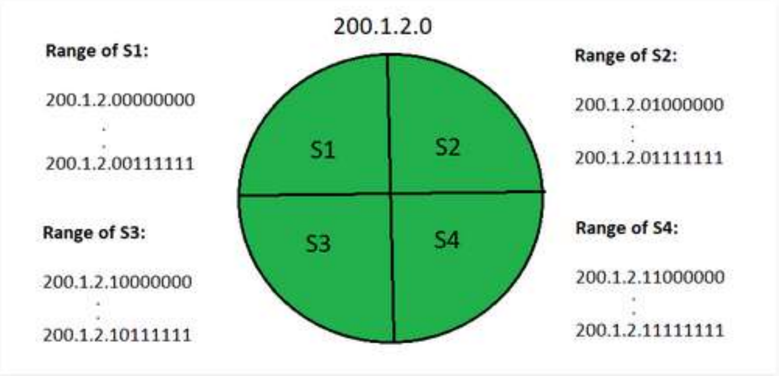
- ✓ Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.
- ✓ A table is maintained by the internal router called as **Routing table**.
- ✓ It helps the internal router to decide on which interface the data packet should be forwarded.
- ✓ **Routing table consists of the following three fields-**
  - ✓ IP Address of the destination subnet
  - ✓ Subnet mask of the subnet
  - ✓ Interface

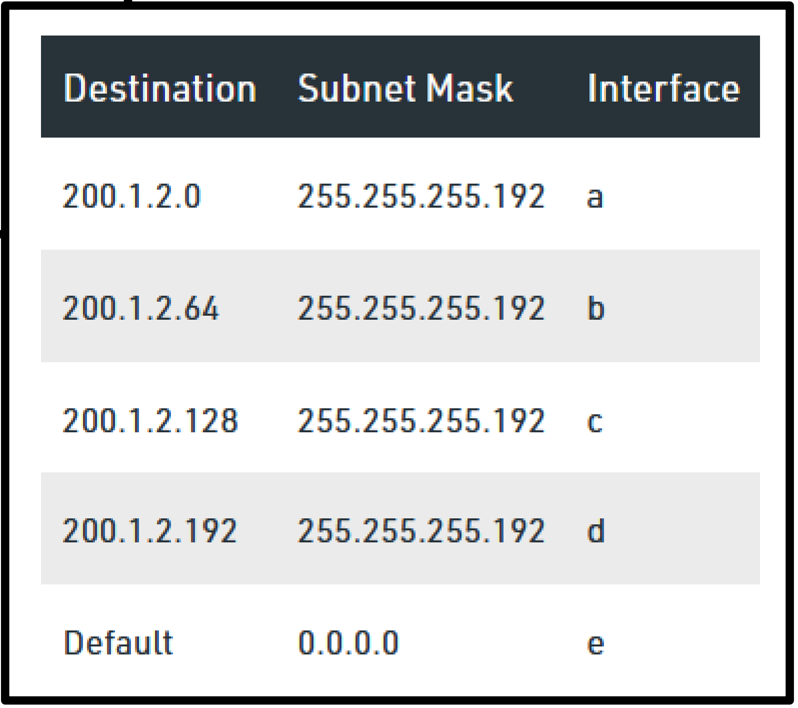
ROUTING

Route Determination Process (finding Subnet ID using Routing Table):

Consider a network is subnetted into 4 subnets as shown in the above picture. The IP Address of the 4 subnets are:

```
200.1.2.0 (Subnet a)
200.1.2.64 (Subnet b)
200.1.2.128 (Subnet c)
200.1.2.192 (Subnet d)
```



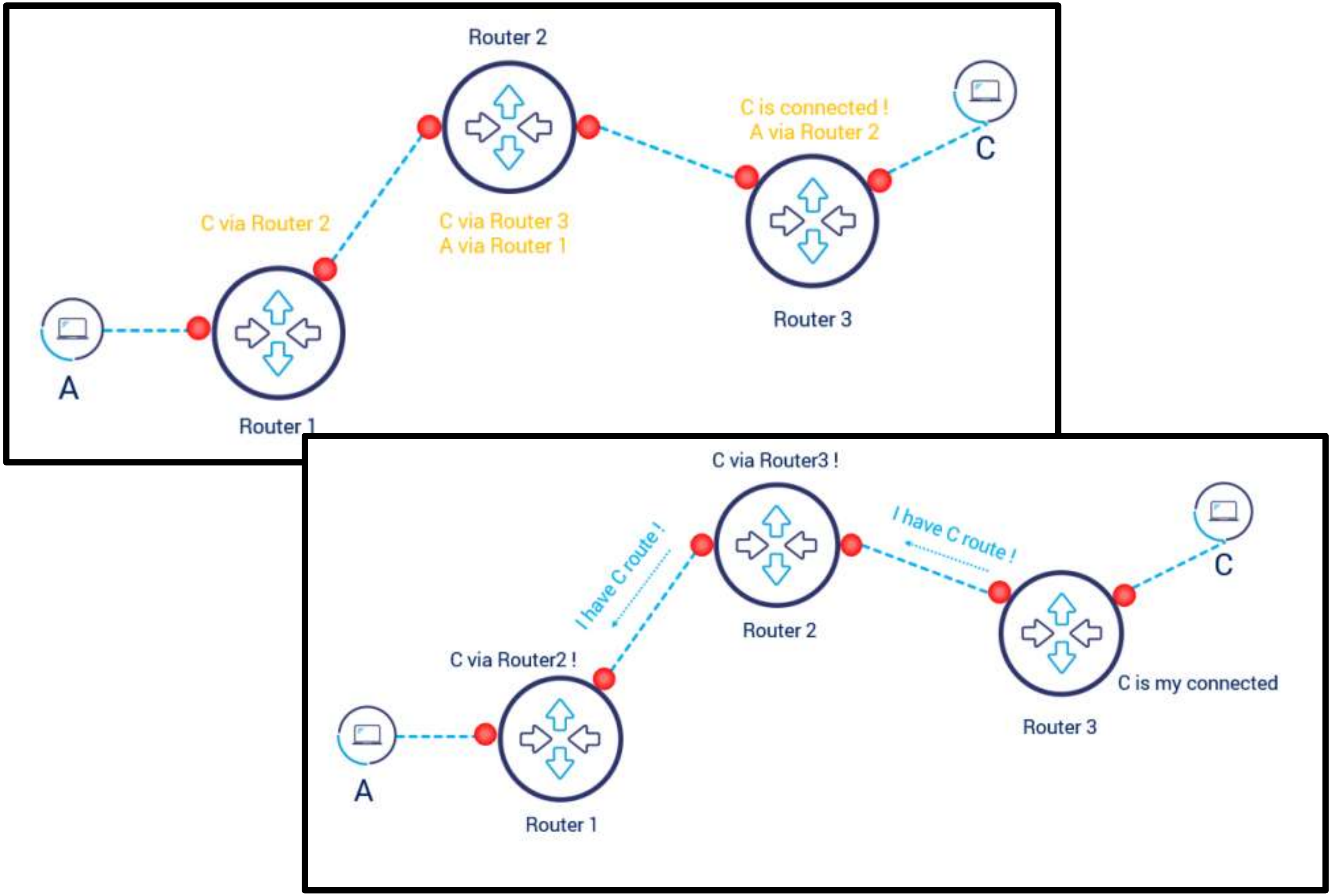


Destination	Subnet Mask	Interface
200.1.2.0	255.255.255.192	a
200.1.2.64	255.255.255.192	b
200.1.2.128	255.255.255.192	c
200.1.2.192	255.255.255.192	d
Default	0.0.0.0	e

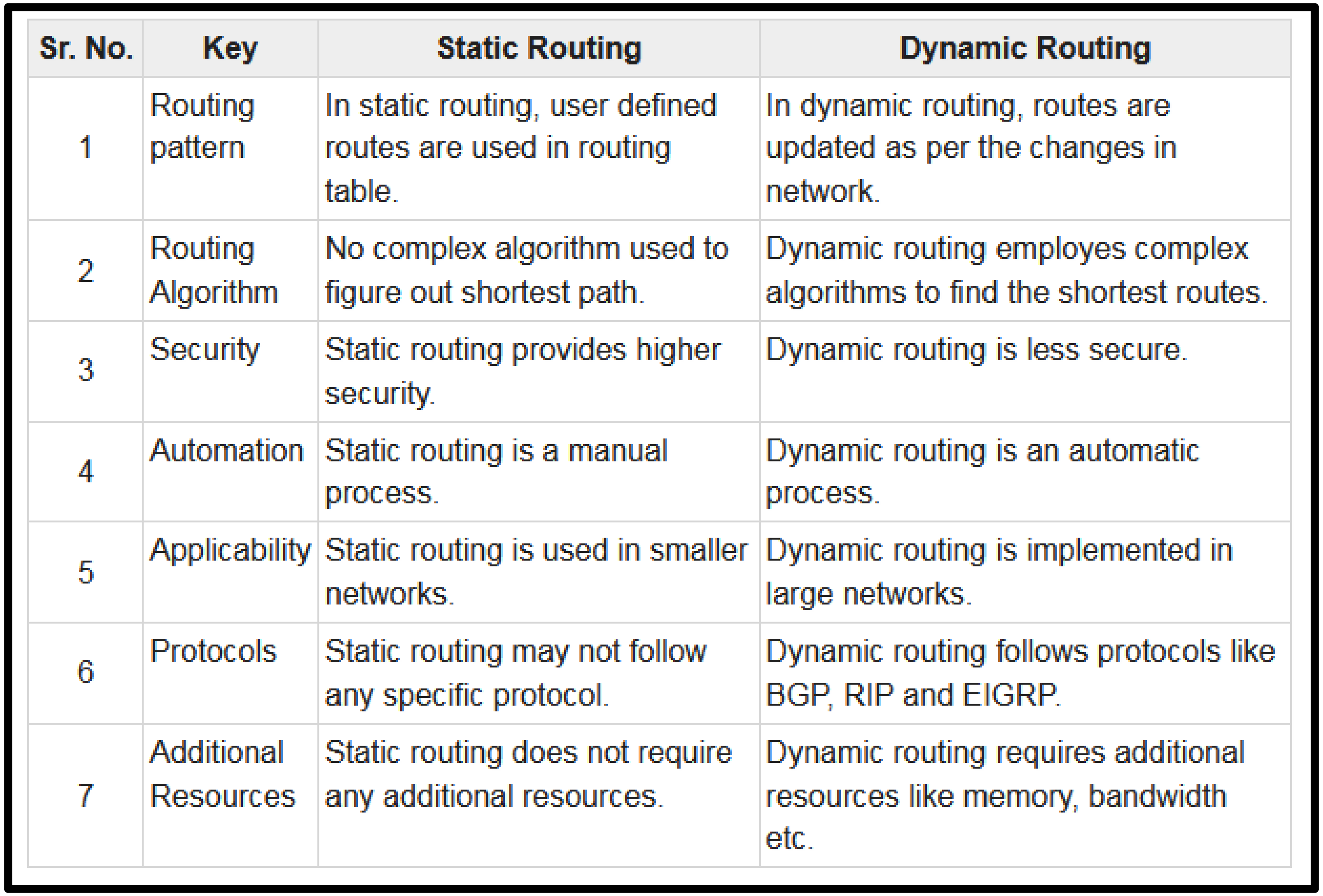
ROUTING

- ✓ **Static Routing or Non-Adaptive Routing**, follows user defined routing and routing table is not changed until network administrator changes it. Static Routing uses simple routing algorithms and provides more security than dynamic routing.
- ✓ **Dynamic Routing or Adaptive Routing**, as name suggests changes the routing table once any changes to network occurs or network topology changes. During network change, dynamic routing sends a signal to router, recalculates the routes and send the updated routing information.

ROUTING


Router 2
C is connected !
A via Router 2
C
C via Router 2
C via Router 3
A via Router 1
Router 3
A
Router 1
C via Router3 !
I have C route !
I have C route !
C
Router 2
C via Router2 !
C is my connected
Router 3
A
Router 1

ROUTING



Sr. No.	Key	Static Routing	Dynamic Routing
1	Routing pattern	In static routing, user defined routes are used in routing table.	In dynamic routing, routes are updated as per the changes in network.
2	Routing Algorithm	No complex algorithm used to figure out shortest path.	Dynamic routing employes complex algorithms to find the shortest routes.
3	Security	Static routing provides higher security.	Dynamic routing is less secure.
4	Automation	Static routing is a manual process.	Dynamic routing is an automatic process.
5	Applicability	Static routing is used in smaller networks.	Dynamic routing is implemented in large networks.
6	Protocols	Static routing may not follow any specific protocol.	Dynamic routing follows protocols like BGP, RIP and EIGRP.
7	Additional Resources	Static routing does not require any additional resources.	Dynamic routing requires additional resources like memory, bandwidth etc.

ROUTING

- ✓ When a data packet arrives to the internal router, it follows the following steps-
- ✓ <u>**Step-01:**</u>
- ✓ Router performs the bitwise ANDing of-
- ✓ Destination IP Address mentioned on the data packet
- ✓ And all the subnet masks one by one.
- ✓ <u>**Step-02:**</u>
- ✓ Router compares each result with their corresponding IP Address of the destination subnet in the routing table.

ROUTING

- ✓ **Case-01:**
- ✓ If there occurs only one match,
- ✓ Router forwards the data packet on the corresponding interface.
- ✓ **Case-02:**
- ✓ If there occurs more than one match,
- ✓ Router forwards the data packet on the interface corresponding to the longest subnet mask.
- ✓ **Case-03:**
- ✓ If there occurs no match,
- ✓ Router forwards the data packet on the interface corresponding to the default entry.

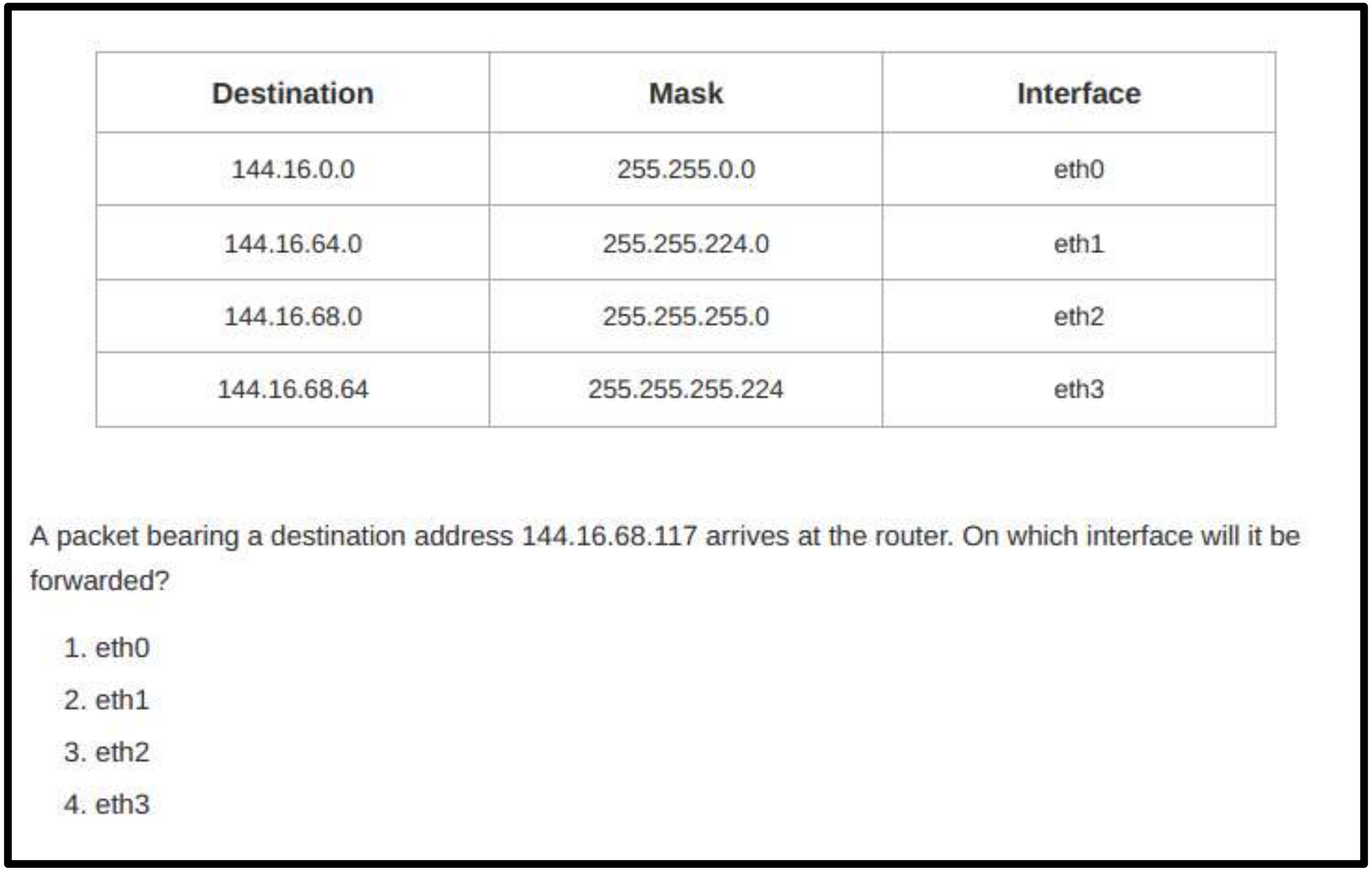
ROUTING

- ✓ **In fixed length subnetting**
- ✓ All the subnets have the same subnet mask.
- ✓ So, bitwise ANDing is performed only once.
- ✓ If the result matches to any of the destination subnet IP Address,
- ✓ Router forwards the data packet on its corresponding interface.
- ✓ Otherwise, it is forwarded on the default interface.
- ✓ **In variable length subnetting**
- ✓ All the subnets do not have the same subnet mask.
- ✓ So, bitwise ANDing is performed once with each subnet mask.
- ✓ Then, the above three cases are followed.

ROUTING

- ✓ A host may also be directly connected to the router.
- ✓ In that case, there exists a host specific route from the router to the host.
- ✓ Router saves the IP Address of that host in the “Destination Network” column.
- ✓ Router saves 255.255.255.255 in the “Subnet Mask” column.
- ✓ The ANDing of its destination address and subnet mask yields the IP Address of the host.
- ✓ When a data packet arrives for that specific host, bitwise ANDing is performed.
- ✓ When the result of ANDing is the IP Address of the host, packet is forwarded to its host specific route.
- ✓ Subnet mask for default route = 0.0.0.0
- ✓ Subnet mask for host specific route = 255.255.255.255

ROUTING



Destination	Mask	Interface
144.16.0.0	255.255.0.0	eth0
144.16.64.0	255.255.224.0	eth1
144.16.68.0	255.255.255.0	eth2
144.16.68.64	255.255.255.224	eth3

A packet bearing a destination address 144.16.68.117 arrives at the router. On which interface will it be forwarded?

1. eth0
2. eth1
3. eth2
4. eth3

ROUTING

Router performs the bitwise ANDing of-

Destination address mentioned on the data packet

And each subnet mask one by one.

1st Row- 144.16.68.117 AND 255.255.0.0

= 144.16.0.0

Since result is same as the given destination address, so a match occurs.

2nd Row- 144.16.68.117 AND 255.255.224.0

= 144.16.64.0

01000100 11100000 01000000

Since result is same as the given destination address, so a match occurs.

ROUTING

3rd Row-

144.16.68.117 AND 255.255.255.0

= 144.16.68.0

Since result is same as the given destination address, so a match occurs.

4th Row-

144.16.68.117 AND 255.255.255.224

= 144.16.68.96

01110101 11100000 01100000

Since result is not same as the given destination address, so a match does not occur.

ROUTING

Now,

Clearly, there occurs more than one match.

So, router forwards the packet on the interface corresponding to the longest subnet mask.

Out of all, 255.255.255.0 is the longest subnet mask since it has maximum number of 1s.

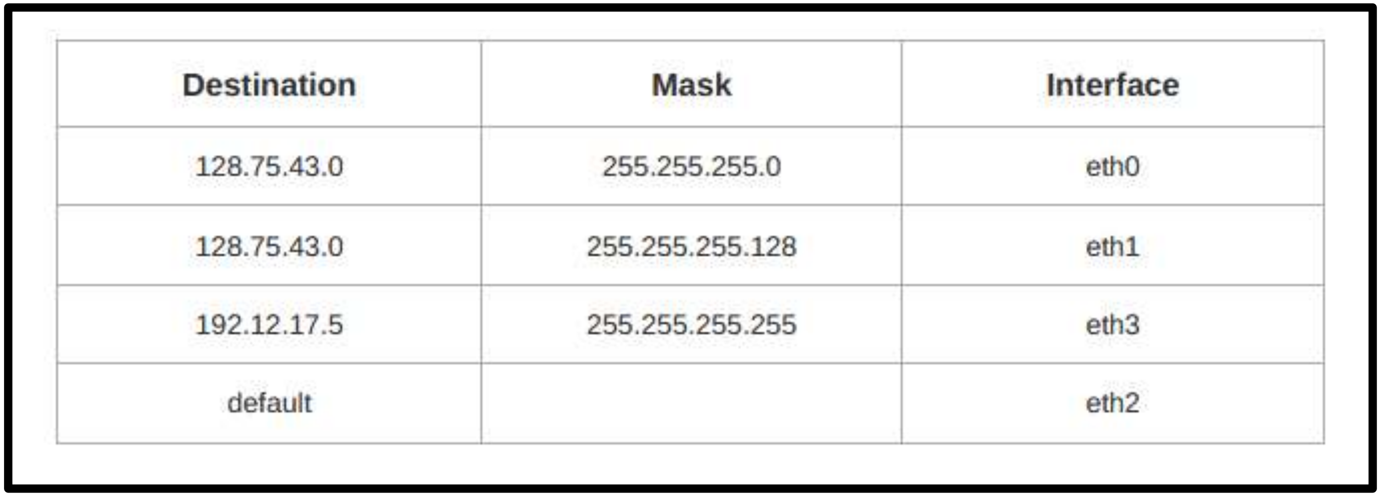
So,

Router forwards the packet on the interface corresponding to the subnet mask 255.255.255.0.

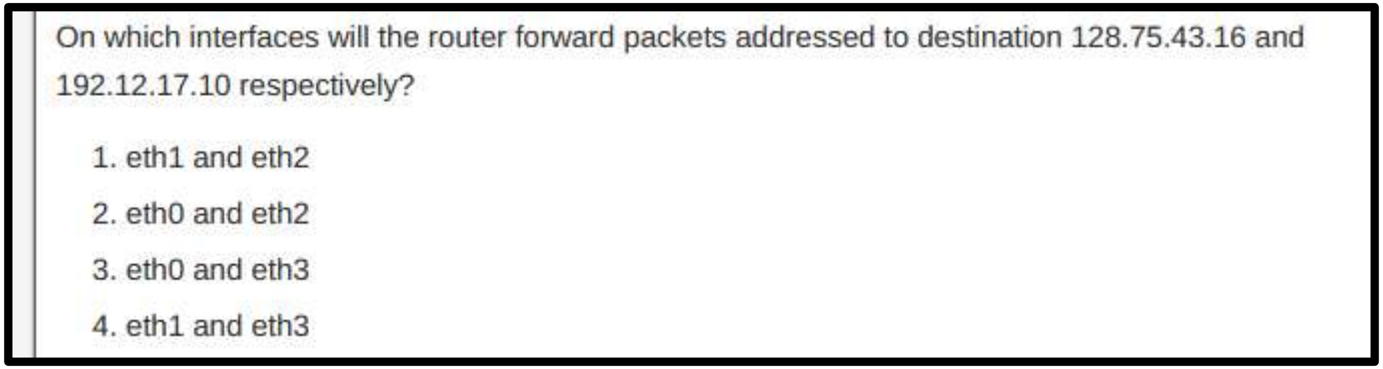
The corresponding interface is eth2.

Thus, Option (C) is correct.

ROUTING



Destination	Mask	Interface
128.75.43.0	255.255.255.0	eth0
128.75.43.0	255.255.255.128	eth1
192.12.17.5	255.255.255.255	eth3
default		eth2



On which interfaces will the router forward packets addressed to destination 128.75.43.16 and 192.12.17.10 respectively?

1. eth1 and eth2
2. eth0 and eth2
3. eth0 and eth3
4. eth1 and eth3

ROUTING

Router performs the bitwise ANDing of-

Destination address mentioned on the data packet

And each subnet mask one by one.

Packet With Destination Address 128.75.43.16-

1st Row-

128.75.43.16 AND 255.255.255.0

= 128.75.43.0

Since result is same as the given destination address, so a match occurs.

2nd Row-

128.75.43.16 AND 255.255.255.128

= 128.75.43.0

Since result is same as the given destination address, so a match occurs.

ROUTING

3rd Row-

128.75.43.16 AND 255.255.255.255

= 128.75.43.16

Since result is not same as the given destination address, so a match does not occur.

Now,

Clearly, there occurs more than one match.

So, router forwards the packet on the interface corresponding to the longest subnet mask.

Out of all, 255.255.255.128 is the longest subnet mask since it has maximum number of 1s.

So, Router forwards the packet on the interface corresponding to the subnet mask 255.255.255.128.

The corresponding interface is eth1.

ROUTING

Packet With Destination Address 192.12.17.10-

1st Row-

192.12.17.10 AND 255.255.255.0

= 192.12.17.0

Since result is not same as the given destination address, so a match does not occur.

2nd Row-

192.12.17.10 AND 255.255.255.128

= 192.12.17.0

Since result is not same as the given destination address, so a match does not occur.

3rd Row-

192.12.17.10 AND 255.255.255.255

= 192.12.17.10

ROUTING

Since result is not same as the given destination address, so a match does not occur.

Now,

Clearly, there occurs no match.

So, router forwards the packet on the interface corresponding to the default entry.

The corresponding interface is eth2.

Thus, Option (A) is correct.