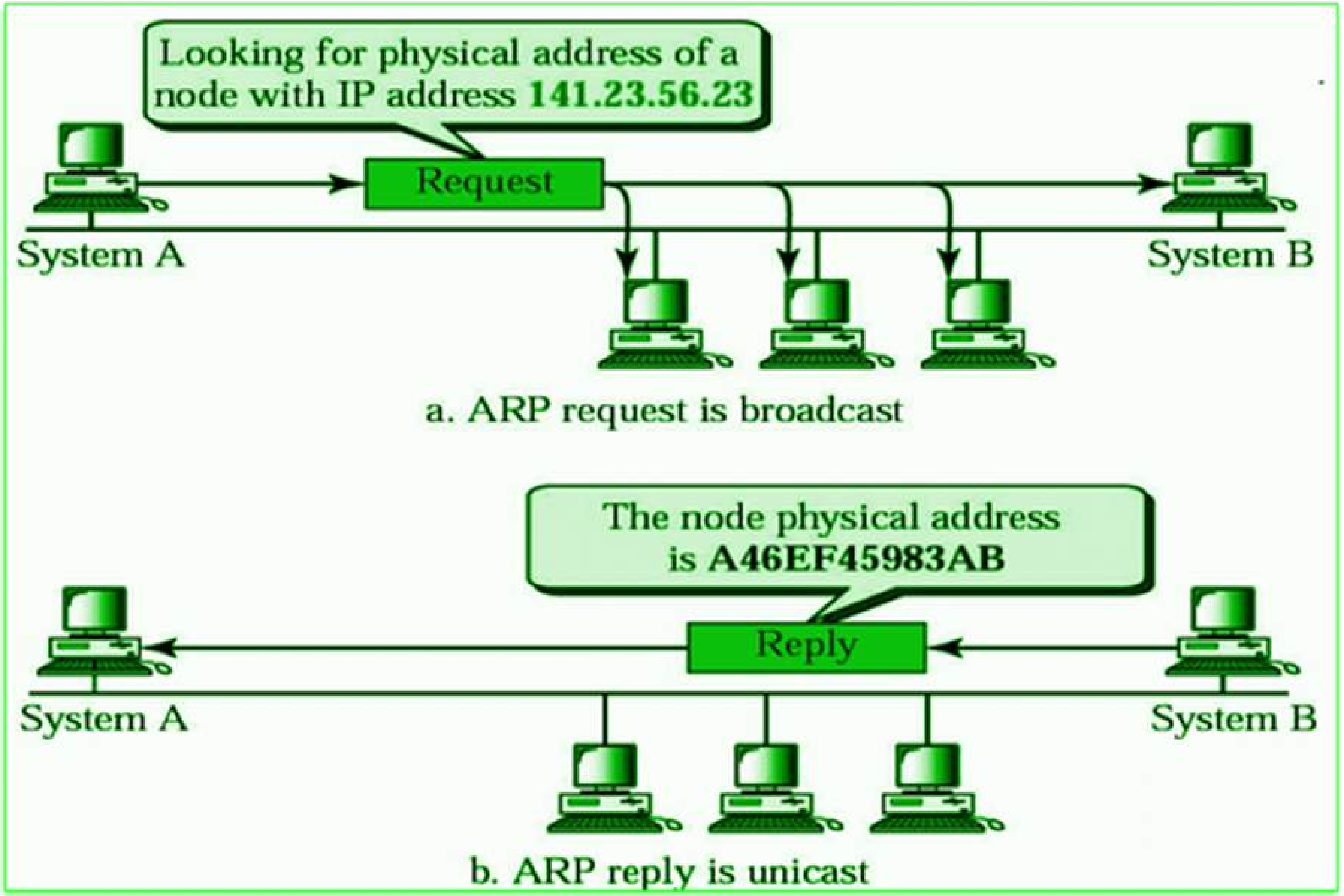
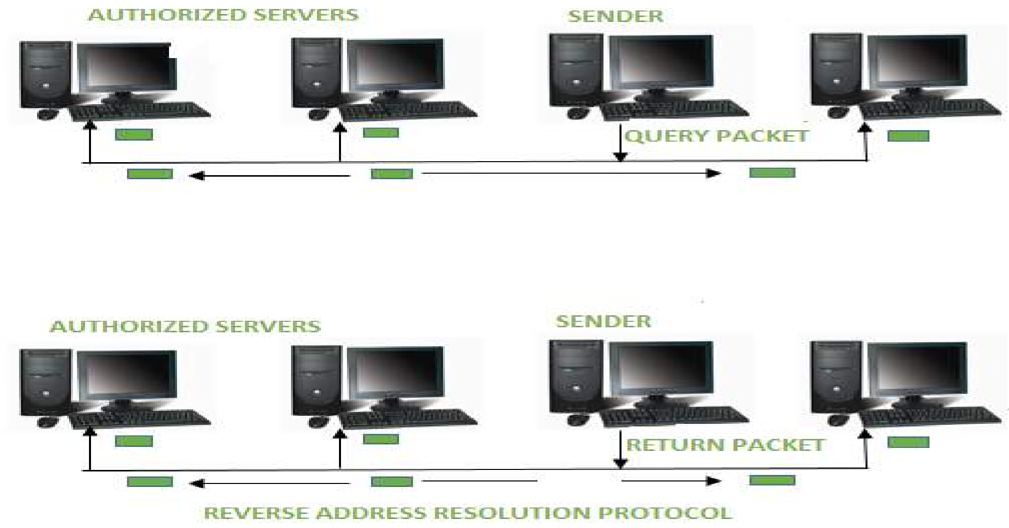
N/W Layer Protocols :ARP

- **1)ARP (Address Resolution Protocol)**
- ARP stands for Address Resolution Protocol.
- ARP is used to **convert the logical address ie. IP** address **into** physical address ie. **MAC address.**
- While **communicating with other nodes**, it is necessary to **know the MAC address or physical address of the destination node.**
- If any of the node in a network wants to know the physical address of another node in the same network,
- the host then sends an ARP query packet. This ARP query packet consists of IP address and MAC address of source host and only the IP address of destination host.
- This ARP packet is then received to every node present in the network. The node with its own IP address recognizes it and sends it MAC address to the requesting node.


Looking for physical address of a node with IP address 141.23.56.23
Request
System A
System B
a. ARP request is broadcast
The node physical address is A46EF45983AB
Reply
System A
System B
b. ARP reply is unicast

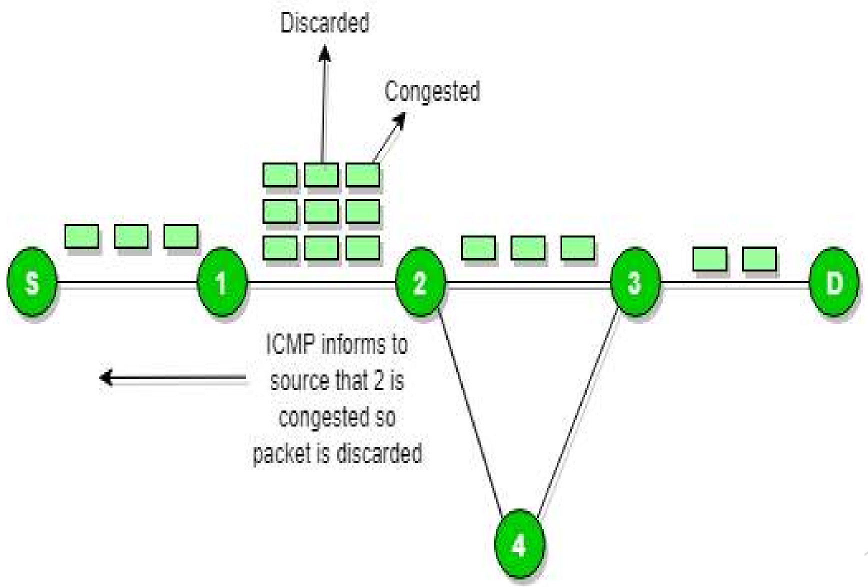
2)RARP

- RARP stands for **Reverse Address Resolution Protocol.**
- RARP works opposite of ARP.
- **Reverse Address Resolution Protocol is used to convert MAC address ie. physical address into IP address ie. logical address.**
- RARP provides with a feature for the systems and applications to get their own IP address from a DNS(Domain Name System) or router.



3)ICMP

- ICMP stands for **Internet Control Message Protocol**.
- ICMP is a part of IP protocol suite.
- ICMP is an **error reporting and network diagnostic protocol.**
- Feedback in the network is reported to the designated host.
- Meanwhile, if any kind of error occur it is then reported to ICMP. ICMP protocol consists of many error reporting and diagnostic messages.



4)IGMP

- IGMP stands for **Internet Group Message Protocol.**
- IGMP is a **multicasting communication protocol.**
- **It utilizes the resources efficiently while broadcasting the messages and data packets.**
- Other **hosts connected in the network and routers makes use of IGMP for multicasting communication.**
- In many networks multicast routers are used in order to transmit the messages to all the nodes.
- Multicast routers therefore receives large number of packets that needs to be sent. But to broadcast this packets is difficult as it would increase the overall network load. Therefore IGMP helps the multicast routers by addressing them while broadcasting

Unit IV
Transport Layer

Introduction

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model.

- **At the sender's side:**
- The **transport layer receives data from the Application layer .**
- then **performs Segmentation**, divides the actual message into segments.
- **adds the source and destination's port numbers** into the header of the segment
- **transfers the message to the Network layer.**
- **-At receiver side:**
- **Network layer sends data to transport layer.**
- Transport layer **check port number.**
- **Send data to those port**

What are the responsibilities of transport layer

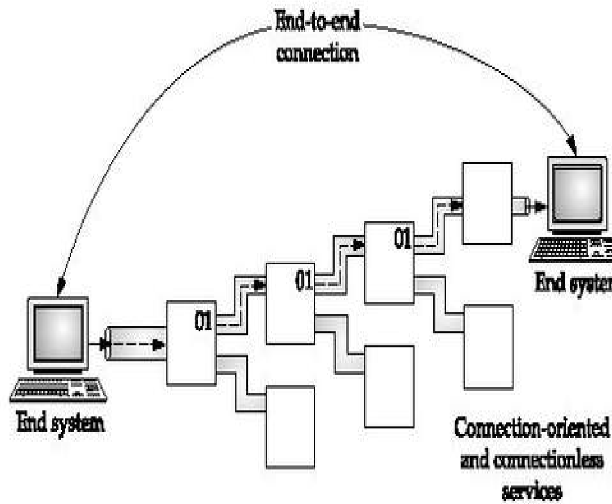
- **Responsibilities of a Transport Layer**
- 1)The Process to Process Delivery
- 2)End-to-End Connection between Hosts
- 3)Multiplexing and Demultiplexing
- 4)Congestion Control
- 5)Data integrity and Error correction
- 6)Flow control

1)The Process to Process Delivery

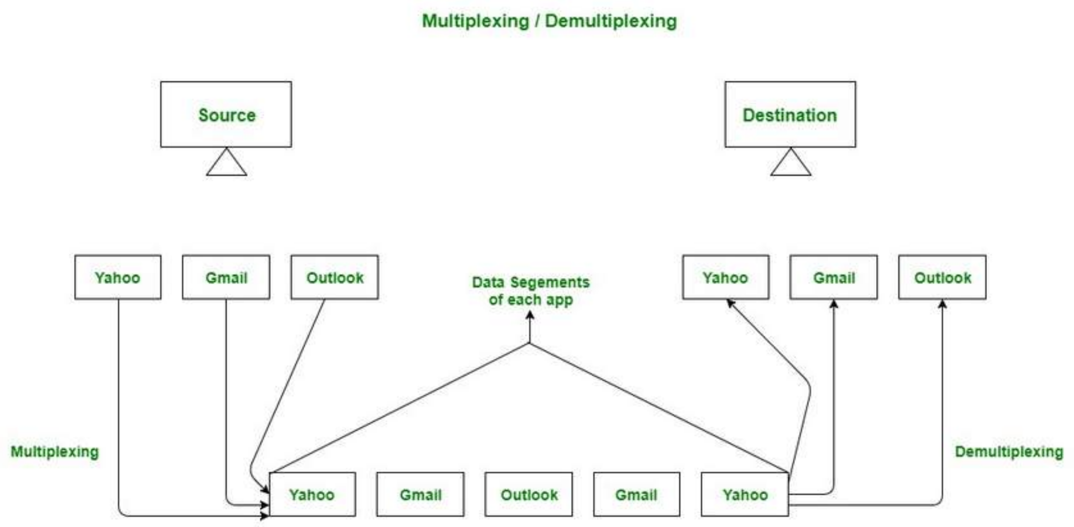
- While **Data Link Layer requires the MAC address** of source-destination hosts to **correctly deliver a frame** and the **Network layer requires the IP address** for appropriate **routing of packets,**
- In a similar way **Transport Layer requires a Port number** to **correctly deliver of segments.**

2. End-to-end Connection between Hosts

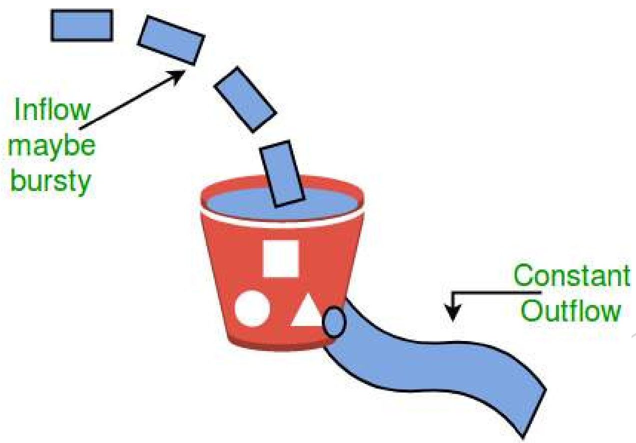
- The transport layer is also responsible for **creating the end-to-end Connection between hosts** for which it mainly uses **TCP and UDP.**
- **TCP is a secure, connection-orientated protocol**. TCP ensures the **reliable delivery of messages** and is used in various applications.
- **UDP, on the other hand, unreliable protocol** .It is **suitable for applications that have little concern with flow or error control**



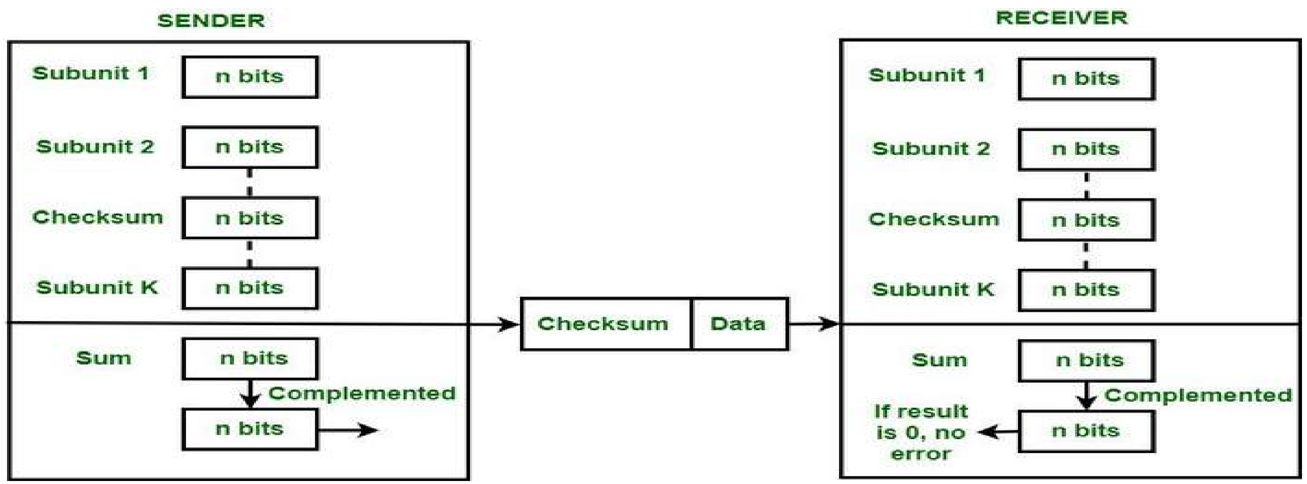
- **3) Multiplexing and Demultiplexing:**
- **Multiplexing:** Multiplexing(many to one) **data is acquired from several processes** from the sender and **merged into one packet** along with headers and **sent as a single packet.**
- **Demultiplexing:** Demultiplexing(one to many) is required at the receiver side when the **message is distributed into different processes.**



- **4. Congestion Control:** Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs.
- As a result, the retransmission of packets from the sources increases the congestion further.
- In this situation, the Transport layer provides Congestion Control in different ways.
- It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network.



- **5.Data integrity and Error Correction: The transport layer checks for errors in the messages coming from the application layer** by using **error detection codes**, and computing checksums
- it checks whether the received data is not corrupted and uses the ACK and NACK services.

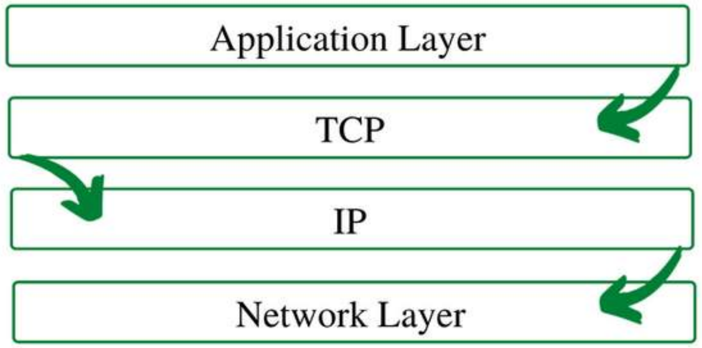


- **6. Flow Control:**The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also **prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques**.

- **Protocols of Transport Layer**
- **Transmission Control Protocol (TCP)**
- **User Datagram Protocol (UDP)**
- **Stream Control Transmission Protocol (SCTP)**

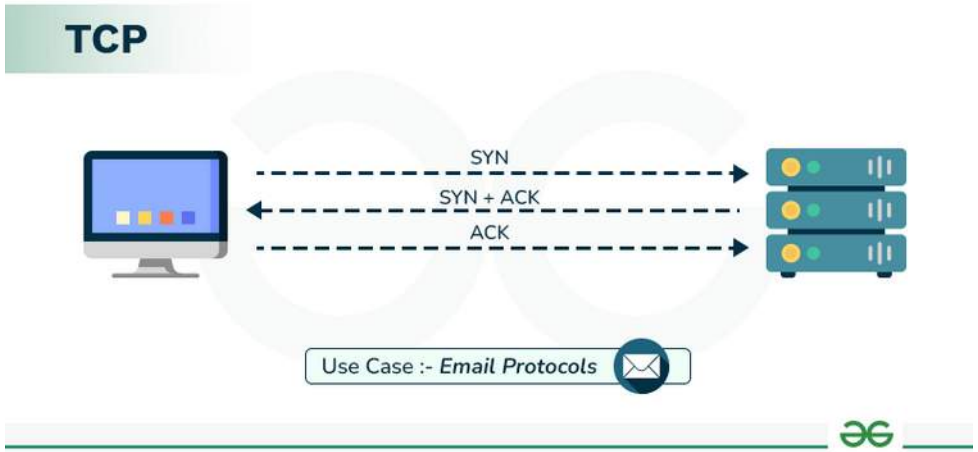
Transmission Control Protocol (TCP)

- **What is TCP:**
- **Transmission Control Protocol (TCP)** is a **connection-oriented protocol for communications** that helps in the exchange of messages between different devices over a network. The Internet Protocol (IP), which establishes the technique for sending data packets between computers, works with TCP.
- **What is IP:**
- **IP is a method that is useful for sending data from one device to another from all over the internet.** It is a set of rules governing how data is sent and received over the internet. **It is responsible for addressing and routing packets of data**



Working of Transmission Control Protocol (TCP)

- When a **user requests a web page on the internet**, **the server processes that request and sends back an HTML Page to that user.**
- The **server makes use** of a protocol called the **HTTP Protocol.** The HTTP **then requests the TCP** layer to set the required **connection.**
- Now, the **TCP breaks the data into small packets and forwards it toward the Internet Protocol (IP) layer**. The **packets are then sent to the destination** through different routes.



- **Features of TCP/IP:**

1)Segment Numbering System:

2)Connection Oriented:

3)Full Duplex: Full duplex communication is a type of data transfer where **two or more devices can send and receive data at the same time**

4)Flow Control:

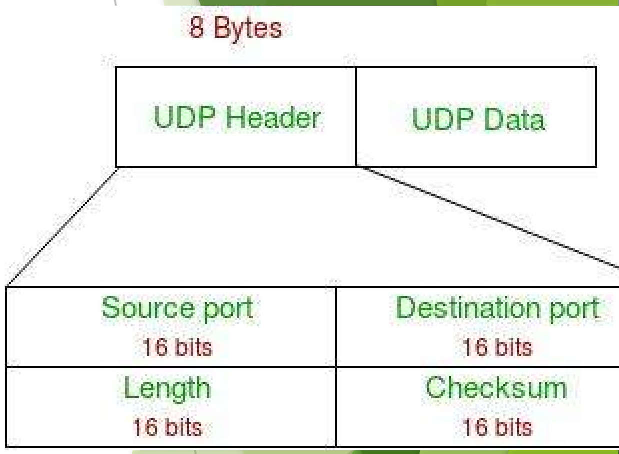
5)Error Control:

6)Congestion Control:

- **Advantages of TCP**
- It is a **reliable** protocol.
- It provides an **error-checking** mechanism.
- It gives **flow control**.
- **It makes sure that the data reaches the proper destination** in the exact order that it was sent.
- It **works in conjunction with IP (Internet Protocol)** to establish connections between devices on a network.
- **Disadvantages of TCP**
- TCP is made for **Wide Area Networks**
- TCP runs several layers so **it can slow down the speed of the network**.
- It is **not generic in nature.** Meaning, it cannot represent any protocol stack other than the TCP/IP suite. E.g., it cannot work with a Bluetooth connection.

User Datagram Protocol (UDP)

- **User Datagram Protocol**
- User Datagram Protocol (UDP) is one of the core protocols of the Internet Protocol (IP) suite.
- **It is a communication protocol used across the internet for time-sensitive transmissions such as video**.
- ,**UDP is connectionless and does not guarantee delivery, order, or error checking**
- **UDP Header**
- UDP header is an **8-byte** fixed and simple header,
- The first 8 Bytes contain all necessary header information and the remaining part consists of data.



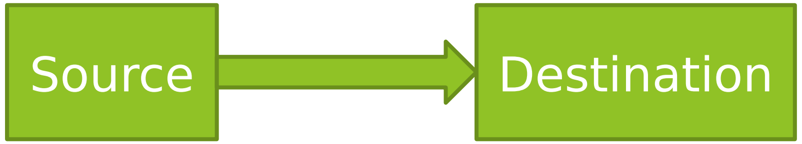
Hexadecimal conversion to decimal

- F A 8.2

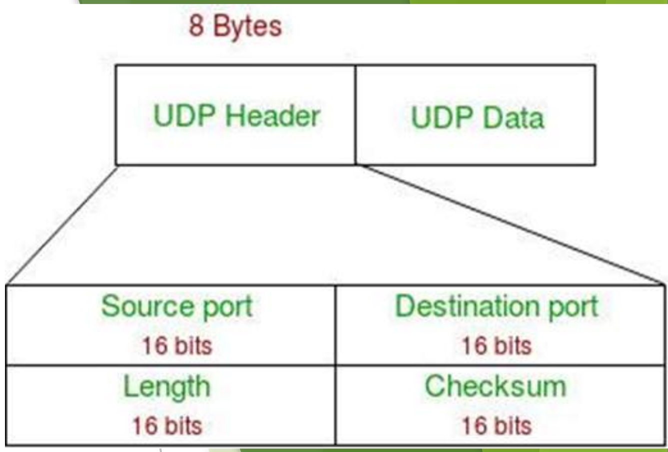
F	A	8	.2
16^2	16^1	16^0	.16^-1
(16^2 *15)	(16^1 *10)	(16^0 * 8)	.(16^-1 *2)
3840	160	8	.125
4008.125			

Denary/Decimal	Binary	Hexadecimal
Base 10 Number System	Base 2 Number System	Base 16 Number System
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

- Explain UDP header.the following is a dump of a UDP header in hexadecimal format)**0632 000D 001C E217**
- 1.What is source port number?= **(0632)H->434**
- 2.What is destination port number**?=(000D)H->13**
- 3.What is the total length of the user datagram**?=(001C)->30**
- 4.What is the length of the data?=(total length-header**)=(30-8)=22**
- 5.Is the packet directed from a client to server or vice versa?



- Well known port number start from 0-1023=packet travel from client to server



- Explain UDP header.the following is a dump of a UDP header in hexadecimal format)**CB84 000D 001C 001C**
- 1.What is source port number?=
- 2.What is destination port number**?=**
- 3.What is the total length of the user datagram**?=**
- 4.What is the length of the data?=(total length-header**)=**
- 5.Is the packet directed from a client to server or vice versa?

- Given a DUMP of a UDP header in hexadecimal format **0421 00 0B 002A E217.** Find the following:-
- Source port number?
- Destination port number?
- Length of user datagram?
- Length of the data?

- Given a DUMP of a UDP header in hexadecimal format 0361 10 1A 104C E242.
- Find the following:-
- Source port number?
- Destination port number?
- Length of user datagram?
- Length of the data?

- **Advantages of UDP**

1.Speed: UDP is faster than TCP

2.Simplicity: UDP has a simpler protocol design than TCP

3.Broadcast support: UDP supports broadcasting to multiple recipients,

4.Smaller packet size: UDP uses smaller packet sizes than TCP

Disadvantages of UDP

1.No reliability:

2.No congestion control:

3.Limited use cases: UDP is not suitable for applications that require reliable data delivery, such as email or file transfers,

- SCTP stands for **Stream Control Transmission Protocol**.
- **It is a connection- oriented protocol in computer networks** which provides a full-duplex association
- i.e., **transmitting multiple streams of data between two end points** at the same time .It is sometimes referred to as next generation TCP .
- SCTP makes it easier to support **telephonic conversation on Internet.**
- **A telephonic conversation requires transmitting of voice along with other data** at the same time on both ends.

- **Characteristics of SCTP :**
- **Unicast with Multiple properties –**
  It is a point-to-point protocol which can use different paths to reach end host.
- **Reliable Transmission –**
  It uses SACK and checksums to **detect damaged, corrupted, discarded, duplicate and reordered data.**
- **Message oriented –**
  Each **message can be framed** and we can keep order of datastream
- **Multi-homing –**
  It can **establish multiple connection paths between two end points**
- **Security –**
  Another characteristic of SCTP that is **security**.

- **Advantages of SCTP :**

1)It is a **full- duplex connection** i.e. users can send and receive data simultaneously.

2)The **message’s boundaries are maintained** and application doesn’t have to split messages.

3)It has properties of both **TCP and UDP protocol.**

- **Disadvantages of SCTP :**

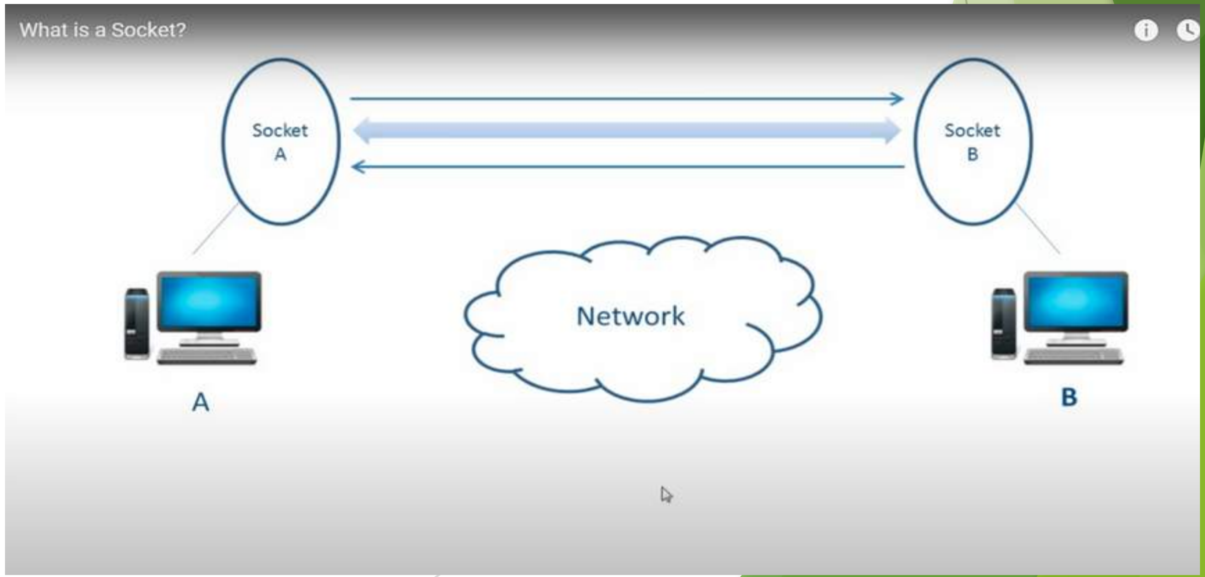
1)One of key challenges is that it requires changes in transport stack on node.

2)Applications need to be modified to use SCTP instead of TCP/UDP.

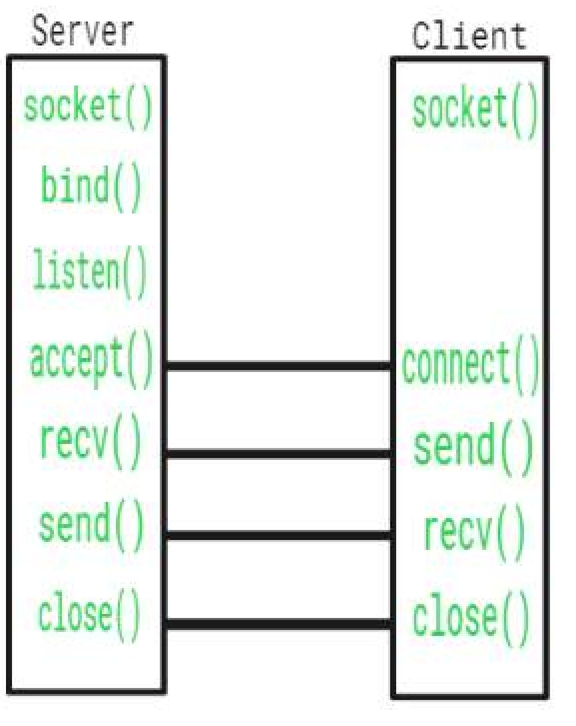
3)Applications need to be modified to handle multiple simultaneous streams.

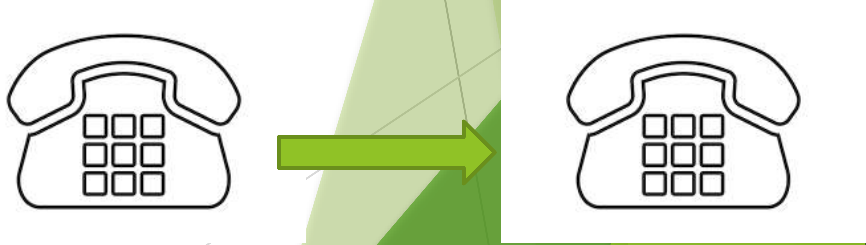
What is socket

- A **socket** is **endpoint ,nodes**
- provides a **two way** communication link between two programs running on the network.
- Shows How applications are communicate with each other
- sockets is created using **‘socket’** system call. The socket provides bidirectional **FIFO** Communication facility over the network.
- Each socket has a **specific address**. This address is composed of an **IP address** and a **port number.**



Function Call	Description
Socket()	To create a socket.Activate the end point. (Domain,Type,Protocol) Type(TCP(SOCK_STREAM),UDP(SOCK_DGRAM))
Bind()	It’s a socket identification like a telephone number to contact(IP+Port No)
Listen()	Ready to receive a connection from client(queue)
Connect()	Ready to act as a sender
Accept()	Confirmation, it is like accepting to receive a call from a sender
Write()	To send data
Read()	To receive data
Close()	To close a connection

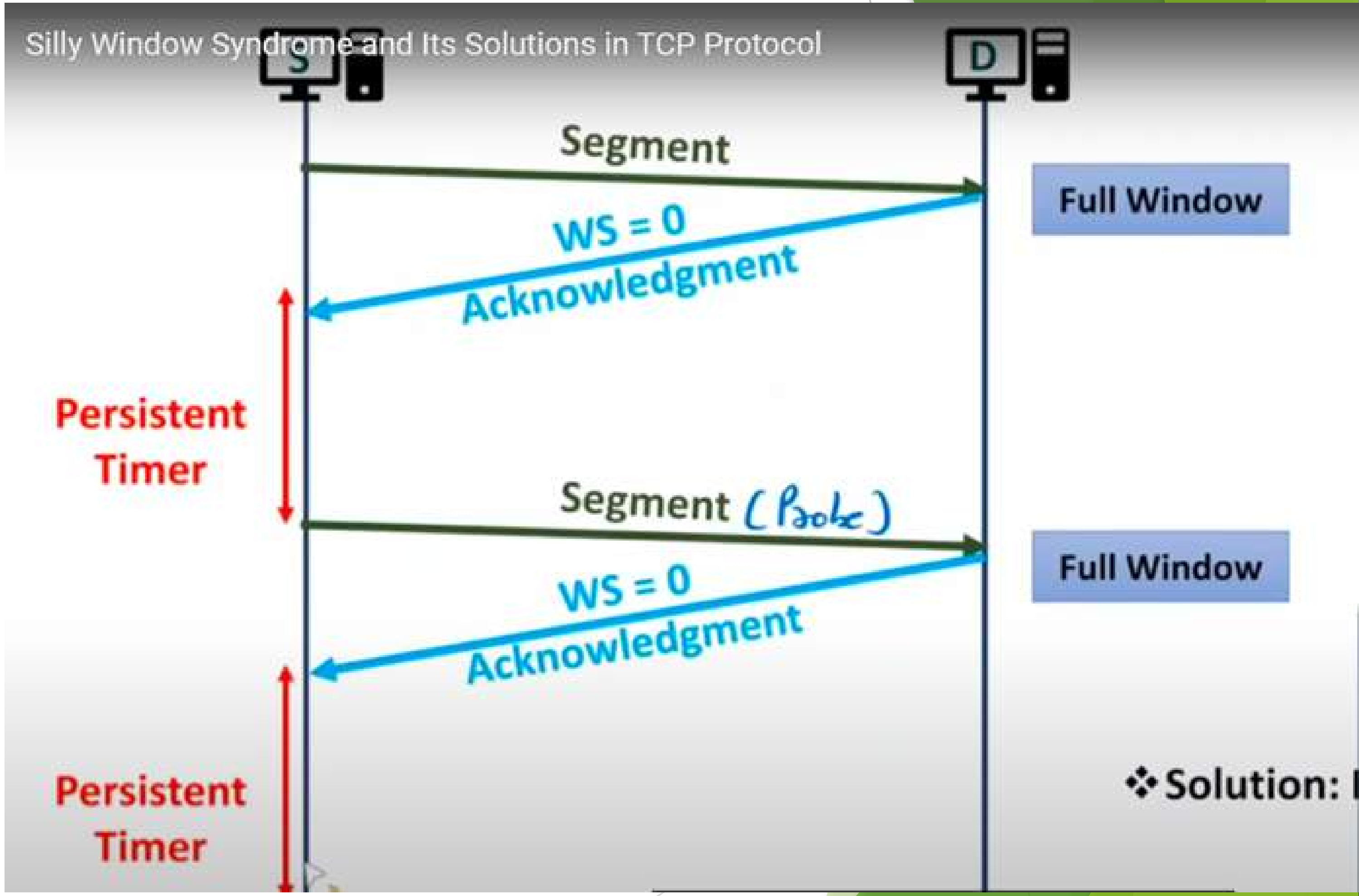




- **Types of Sockets :** There are two types of Sockets: the **datagram** socket and the **stream** socket.
- **Datagram Socket :** This is a type of network which has **connection less point for sending and receiving packets.** It is similar to **mailbox.** The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).
- **Stream Socket** network socket which provides a **connection-oriented, sequenced, and unique flow of data** without record boundaries with well defined mechanisms for creating and destroying connections and for detecting errors. **It is similar to phone. A connection is established between the phones (two ends) and a conversation (transfer of data) takes place.**

What is Silly Window Syndromes.& what are solutions of the silly window syndrome? 8M

- Silly window syndrome are associated with ineffective utilization of bandwidth & resources
- **1)Window size is full**
- 2)Slower Sender
- 3)Slower Receiver



- **Solution is:Reset the connection.**

- **2)Slower Sender**
- **Solution:Nagles Algorithm**
- Wait for RTT to send data.

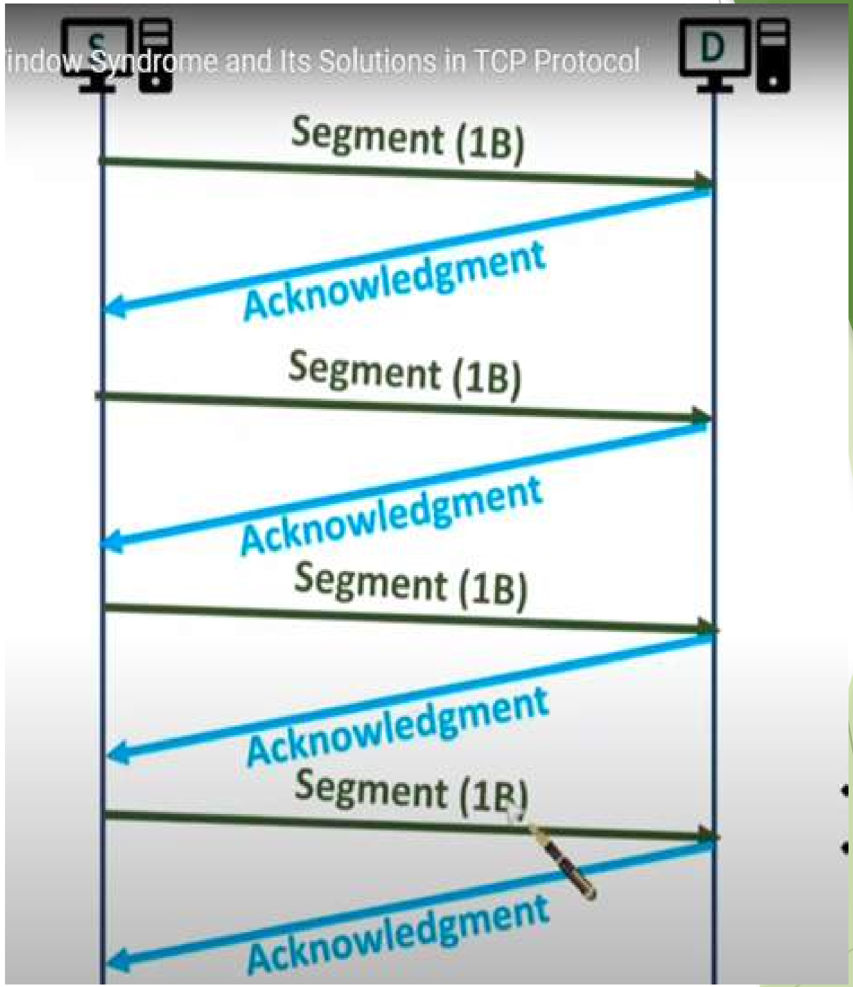
AL

TL

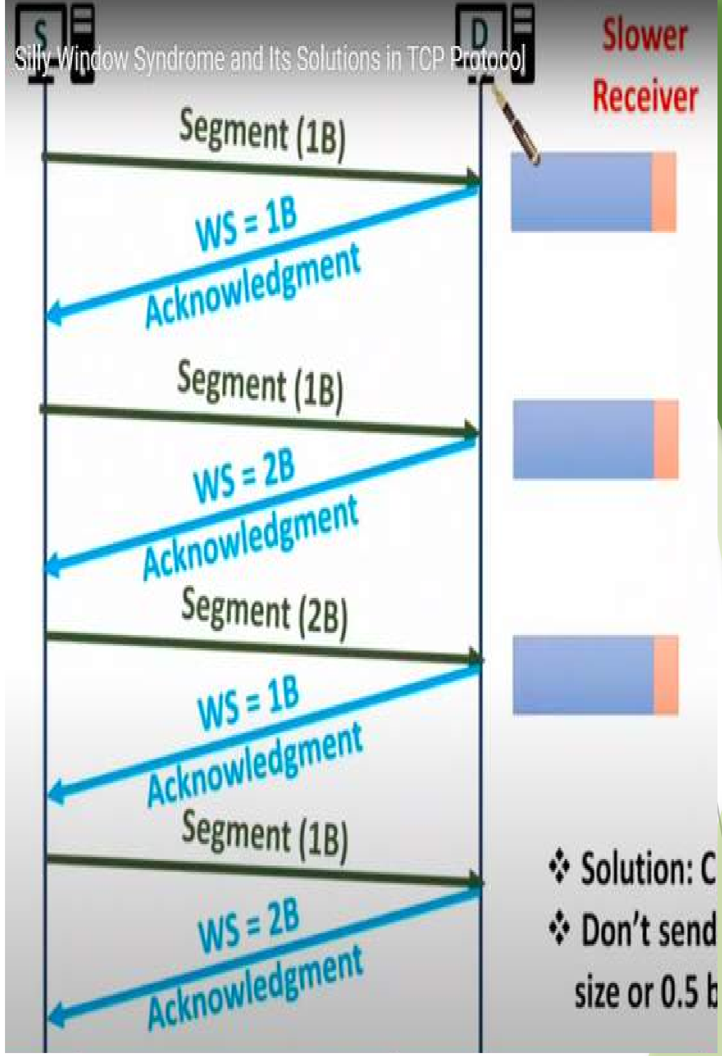
NL

DLL

PL



- **3)Slower Receiver**



- **Solution:Clark's Solution**
- **Don't send ACK till the maximum segment size or 0.5 buffer is free**

- Quality of Service (QoS) is an important concept, particularly when working with multimedia applications. Multimedia applications, such as **video conferencing, streaming services, and VoIP (Voice over IP),** require certain bandwidth, latency, jitter, and packet loss parameters. QoS methods help ensure that these requirements are satisfied, allowing for seamless and reliable communication.
- **QoS Parameters**
- **Packet loss:** This occurs when network connections get congested, and routers and switches begin losing packets.
- **Jitter:** This is the result of network congestion, time drift, and routing changes. Too much jitter can reduce the quality of voice and video communication.
- **Latency:** This is how long it takes a packet to travel from its source to its destination. The latency should be as near to zero as possible.
- **Bandwidth:** This is a network communications link's ability to transmit the majority of data from one place to another in a specific amount of time.
- **Mean opinion score:** This is a metric for rating voice quality that uses a five-point scale, with five representing the highest quality.

- **How does QoS Work?**
- **Quality of Service (QoS)** ensures the performance of critical applications within limited network capacity.
- **Packet Marking**: QoS marks packets to identify their service types. For example, it distinguishes between voice, video, and data traffic.
- **Virtual Queues**: Routers create separate virtual queues for each application based on priority. Critical apps get reserved bandwidth.
- **Handling Allocation**: QoS assigns the order in which packets are processed, ensuring appropriate bandwidth for each application

Differences between TCP and UDP

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection..
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Acknowledgment	An acknowledgment segment is present.	No acknowledgment segment.
Sequence	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in order at the receiver.	There is no sequencing of data in UDP. If the order is required, it has to be managed by the application layer.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.

- **Real Time Transport Protocol (RTP)**
- A protocol is designed to handle real-time traffic (like audio and video) of the Internet, is known as **Real Time Transport Protocol (RTP)**.
- RTP must be used with UDP.
- It does not have any delivery mechanism like multicasting or port numbers.
- RTP supports different formats of files like MPEG and MJPEG.
- **Applications of RTP :**
- RTP mainly helps in media mixing, sequencing and time-stamping.
- Voice over Internet Protocol (VoIP)
- Video Teleconferencing over Internet.
- Internet Audio and video streaming.

- **Version :** This 2-bit field defines version number.
- **X –** The length of this field is also 1-bit. If value of this field is set to 1, then its indicates an extra extension header
- **Contributor count –** This 4-bit field indicates number of contributors
- **M –** The length of this field is 1-bit and it is used as end marker
- **Payload types –** This field is of length 7-bit to indicate type of payload.
- **Sequence Number –** The length of this field is 16 bits. It is used to give serial numbers to RTP packets.
- **Time Stamp –** The length of this field is 32-bit. It is used to find relationship between times of different RTP packets.
- **Synchronization Source Identifier –** This is a 32-bit field used to identify and define the source.
- **Contributor Identifier –** This is also a 32-bit field used for source identification where there is more than one source present in session.