Unit - 4 : Network Functions & Protocol

Switching

- When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as **switching**.
- Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).
- Network switches operate at layer 2 (Data link layer) in the OSI model.
- Switching is transparent to the user and does not require any configuration in the home network.
- Switches are used to forward the packets based on MAC addresses.
- A Switch is used to transfer the data only to the device that has been addressed. It verifies the destination address to route the packet appropriately.
- It is operated in full duplex mode.
- Packet collision is minimum as it directly communicates between source and destination.
- It does not broadcast the message as it works with limited bandwidth.

Rise of Switching: From Hubs to Switches
As computer networks evolved and the need for high-quality communication expanded, the restrictions of hub-based networks have grown to be obvious. This is about the evolution of network switching, with switches replacing hubs because they are the principal connecting devices. Network switches perform on Layer 2 of the OSI version, facilitating more efficient and selective data transmission. Unlike hubs, switches use MAC addresses to provide information only to the particular device they are meant for, decreasing needless community congestion and enhancing average overall performance.

Differentiate between Circuit Switching, Message Switching, and Packet Switching

Introduction

Switched communication networks route data between a number of intermediate nodes as it travels from source to destination. Nodes accomplish data transmission between certain locations on a network via a mechanism called switching. The three typical switching methods are as follows:

1. Circuit Switching
2. Packet Switching
3. Message Switching

In this topic, we will discuss the three types of switching methods and also differentiate between them.

Types of Switching Methods

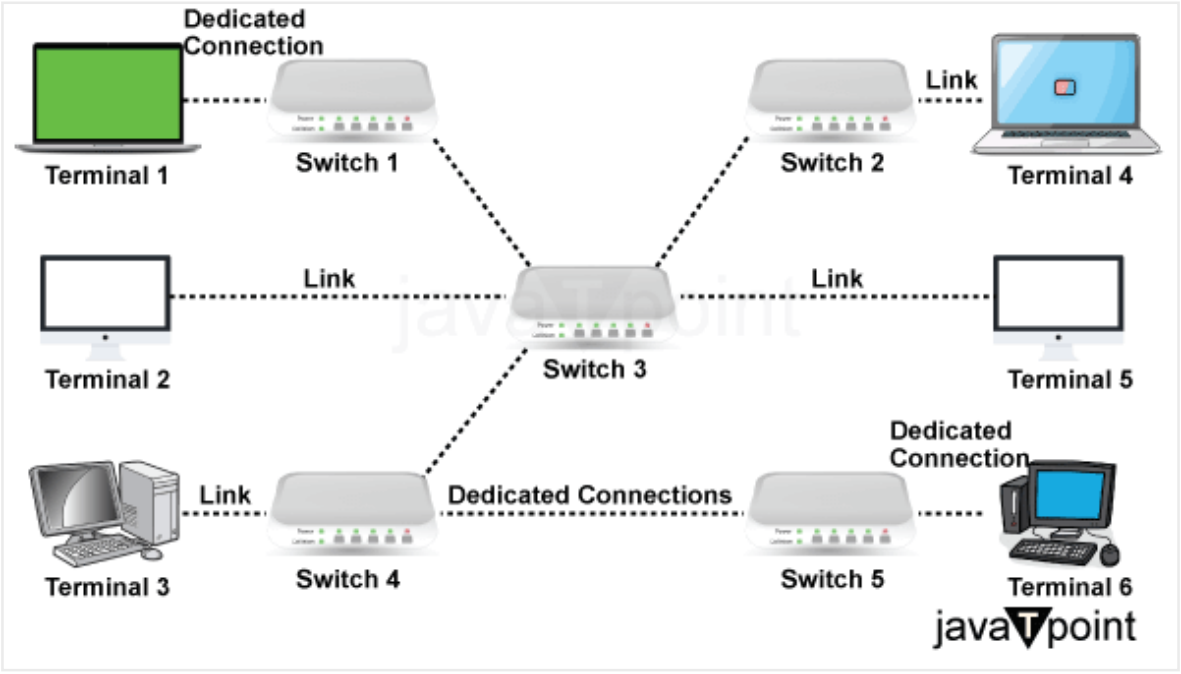
1. Circuit Switching

-> works on physical layer
-> a connection established before transferring the data
-> reservation of resources is the drawback

When constructing a telecommunications network circuit, switching is a technique in which two network nodes first establish a specialized communications channel (circuit) within the network before corresponding with one another. The circuit assures the channel's full bandwidth and maintains connectivity throughout the communication session. The circuit acts as though the nodes were physically connected, exactly like an electrical circuit.

When a dedicated circuit was formed between two phones for the duration of a call by the network in analog telephone networks, circuit switching was first employed. In contrast, trunklines between switching centers in message switching and packet switching systems used in modern digital networks transport data between several nodes in the form of data packets without the use of dedicated circuits.

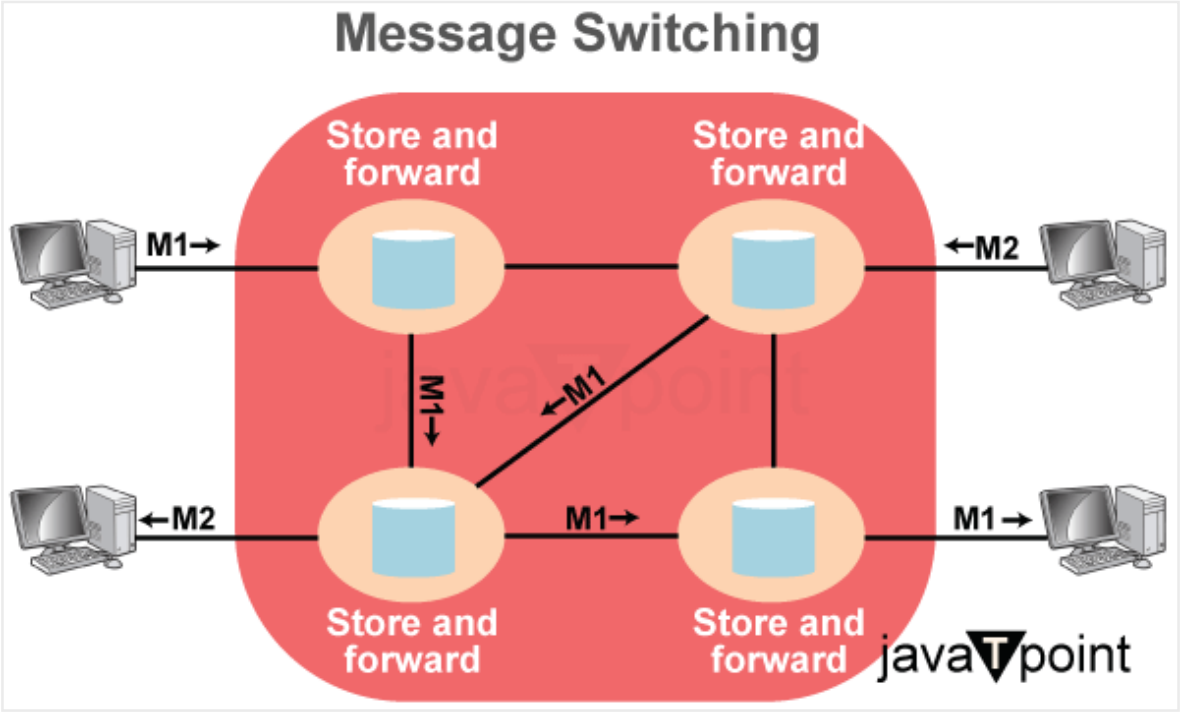
A circuit-switched network's basic example is the **early analog telephone network**. The telephone exchange switches establish a continuous wire circuit between the two phones whenever a call is placed from one phone to the other, lasting throughout the call.



As contrasted to **packet switching,** where packet queues may result in variable and potentially endlessly long packet transfer delays, the bit delay in circuit switching remains constant throughout a connection. No circuit can be compromised by competing users since it is shielded from use until the circuit is released and a fresh connection is established. The channel is still restricted and shielded from rival users, even if no communication is actually happening. Although circuit switching is typically used to connect voice circuits, the concept of a dedicated conduit being constant between two communication parties or nodes can be expanded to communicate material other than voice. The benefit of employing circuit switching is that it offers continuous transfers without the overhead associated with packets, maximizing the utilization of available bandwidth for that connection. Its potential for being relatively inefficient comes from the fact that other connections on the same network cannot utilize unused capacity pledged to a connection. Furthermore, if the circuit is disrupted, calls are not possible and will be dropped.

2. Message Switching

Before packet switching was discovered, a method called message switching was created as a complement to circuit switching. By communicating through messages that contain the entire amount of information to be transmitted, end users converse through message switching. A message is the most basic form of a unit.



The sender and receiver do not have a direct connection. Many intermediate nodes are involved in data transport and making sure the message gets to its designated location. Thus, message-switched data networks are sometimes known as **hop-by-hop systems**.
They offer two separate and significant qualities:

- **Store and forward:** The intermediate nodes are in charge of sending the whole message to the following node. As a result, each node needs to have storage space. If the following hop and the link that connects them are unavailable, a message won't be delivered and will instead be kept indefinitely. A store-and-forward switch will only forward a message if there are enough resources and an accepted next hop. The store-and-forward property is what is meant by this.
- **Message delivery:** Delivering a message entails transmitting data from the source to the destination node while enclosing it all in a single message. The source and destination of each message must be included in the header, which also carries the message routing information.

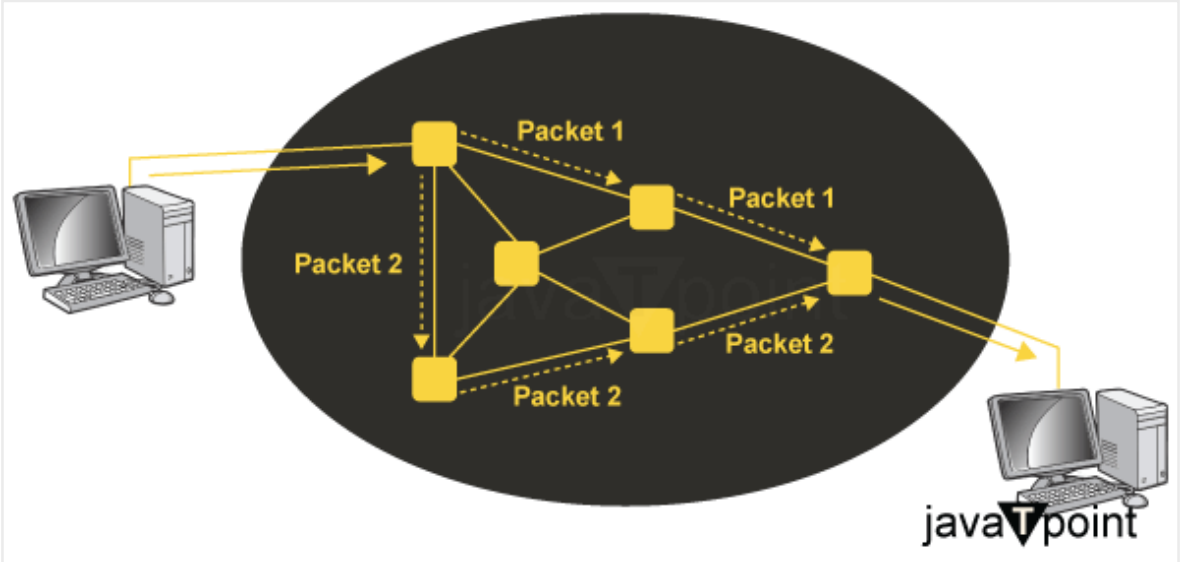
Characteristics of Message Switching

The benefit of message switching is that it makes it possible to use network resources effectively. Additionally, traffic may be easily regulated and monitored because of the store-and-forward functionality of intermediary nodes. Another advantage is the delivery of messages as a whole rather than in pieces.
Message switching, however, also has certain drawbacks. Switches

need a lot of storage space since messages are perpetually held at each intermediate node. They move very slowly as well. This is due to the fact that each node must wait until it has received the complete message before processing the next node and any linkages to it, which depends on channel traffic and availability. The use of message switching in real-time or interactive applications, such as video conferences, is therefore not possible.

3. Packet Switching
-> Works on data link layer as virtual circuit & Network layer as Datagram service
-> its the enhancement of message switching with the same store and forward concept
-> here the data is divided into packets by data link and network layer then sent by different different routes to increase the efficiency and bandwidth utilization
-> delay is high as compared to circuit switches

Small bits of data are moved between networks through a process called packet switching. These data "chunks" or "packets" allow for quicker, more efficient data transmission.
Normally, when a user transmits a file across a network, it is sent in fewer data packets rather than all at once. As an illustration, a 3MB file will be separated into packets, with the header of each packet providing the sequence number, the origin IP address, the destination IP address, the number of packets in the full data file, and the number of packets in the file.



The two main categories of packet switching are:
1. Connection-less packet switching: Each packet in this traditional

form of packet switching is routed separately. As a result, each packet has complete routing information. The shifting loads on the network's nodes (adapters, switches, and routers) also make it possible for different transmission techniques and out-of-order delivery. Datagram switching is another name for this form of packet switching.
In connectionless packet switching, the header section of each packet contains the following data:

1. **Source address**
2. **Destination address**
3. **Total number of packets**

Sequence number (Seq#) for reassembly
The receiving devices rearrange the packets once they have arrived at their destination via numerous paths to create the original message.
2. Connection-Oriented Packet Switching: The data packets are assembled before being numbered in connection-oriented packet switching. It is also known as virtual circuit switching or circuit switching. They then go consecutively along a predetermined route. Since all packets are sent in order while using circuit switching, address information is not required.
Difference between Circuit Switching, Message Switching, and Packet Switching

Parameters	Circuit Switching	Message Switching	Packet Switching
1. Dedicated Path	There is a dedicated path in circuit switching	There is no dedicated path in message Switching	There is no dedicated path in packet switching

2. Connection	By establishing a dedicated path between the source and destination, connection is made possible.	Between each node along the route, a link is individually generated.	Between each node along the route, a link is individually generated.
3. Routing	Between the source and the destination, there is just one dedicated path.	Messages travel a separate path to their destination.	To carry the destination, packets take an autonomous path.
4. Data Segmentation	Entire message	Entire message	Into Packets
5. Routing Flexibility	There is no routing flexibility in Circuit Switching	There is limited Routing flexibility in message switching	There is Routing flexibility in Packet switching
6. Bandwidth Reservation	Yes	No	No
7. End Terminal	Telegraph, Teletype	Telephone, modem	Computer
8. Addressing scheme	Geographical addresses	Hierarchical numbering plan	Hierarchical address space
9. Data Transmission	Real-time	Non-real-time	Both Real-time and Non-real-time

10. Network Resource Efficiency	There is low Network Resource Efficiency(dedicated path)	There is low Resource Efficiency(per message)	There is high Resource Efficiency(Shared)
11. Multiplexing Scheme	Character message multiplexing	Circuit multiplexing	Character multiplexing shared media access networks
12. Examples	Traditional Telephone is an example of Circuit Switching	Telex Systems is an example for Message Switching	Internet and Ethernet are examples for Packet Switching

Types of Network Switching
A multifaceted approach to network switching has developed into numerous types, each catering to specific requirements and conditions.
The primary kinds are discussed below:

Circuit Switching:
-:>Will find out the shortest path and then transmit data after establishing the shortest possible connection.
-> Drawback its slow due to connection oriented

In traditional smartphone networks, circuit switching establishes a dedicated communication route amongst devices during their verbal exchange. While effective, it has boundaries in terms of scalability and overall performance.

Message Switching:
-> Here we will send from node to node entire data is stored from one node to another until it reaches the destination node.
->Drawback : In btw some nodes might not have storage where it can store
Message switching includes the whole message being sent from delivery to destination. In current computer networks, it changed into an early form of data transmission.

Cell -> Fixed length of packets
/ Packet Switching: -> 1000 - 1500 bytes packet size
-> data is transferred in packets form by different different paths
-> Increase the chance of packet loss and reliability
Packet switching, in contrast to circuit switching, breaks down records into packets, which might be transmitted independently across the network. This method, employed via the internet, allows for greater, inexperienced use of bandwidth and superior scalability.

Virtual Circuit Switching: Combining factors of both circuit and packet switching, digital circuit switching establishes a dedicated path in the path of a conversation consultation, just like circuit switching; however, it makes use of packet-like transmission to maintain overall performance.

Ethernet Switching: Ethernet switching has come to be the fundamental form of community switching in local location networks (LANs). It operates at Layer 2 of the OSI version. The usage of MAC addresses beforehand the facts simplest to the supposed recipient.

Why is Switching Concept required?
Switching concept is developed because of the following reasons:

- **Bandwidth:** It is defined as the maximum transfer rate of a cable. It is a very critical and expensive resource. Therefore, switching techniques are used for the effective utilization of the bandwidth of a network.
- **Collision:** Collision is the effect that occurs when more than one device transmits the message over the same physical media, and they collide with each other. To overcome this problem, switching technology is implemented so that packets do not collide with each other.

Advantages of Switching:

- Switch increases the bandwidth of the network.
- It reduces the workload on individual PCs as it sends the information to only that device which has been addressed.
- It increases the overall performance of the network by reducing the traffic on the network.

- There will be less frame collision as switch creates the collision domain for each connection.

Disadvantages of Switching:

- A Switch is more expensive than network bridges.
- A Switch cannot determine the network connectivity issues easily.
- Proper designing and configuration of the switch are required to handle multicast packets.

Challenges and Future Trends

While community switching has come in a protracted manner, it continues to present demanding situations and opportunities for development. Some key concerns and future developments consist of the following:

Security Concerns: As networks become more interconnected, safety threats also evolve. Switches play an important role in network protection, and improvements in encryption, access management, and risk detection are crucial for safeguarding sensitive information.

5G Integration: The creation of 5G technology introduces new opportunities and demanding situations for network switching. The prolonged pace and functionality demand switching infrastructures to help the growing extensive sort of related gadgets and packages.

Edge Computing: The upward push of edge computing, wherein processing happens in the direction of the flow of technology, needs network switching capable of managing allotted and decentralized architectures correctly.

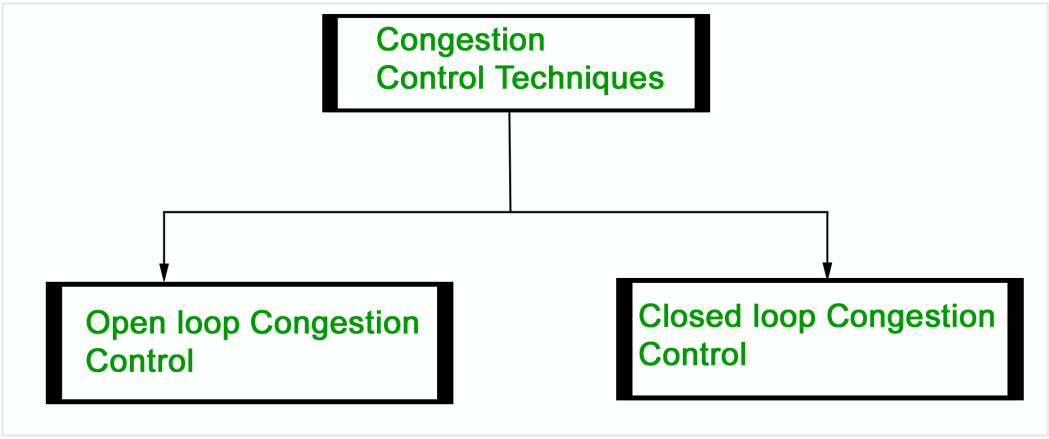
Artificial Intelligence (AI) Integration: Integrating AI network switches can beautify automation, predictive protection, and adaptive community optimization. Machine-learning algorithms can analyze community traffic patterns to anticipate and prevent functionality issues.

Quantum Networking: With the exploration of quantum computing and verbal exchange, the panorama of network switching might also witness revolutionary adjustments. Quantum switches, harnessing the concepts of quantum entanglement, must redefine the way information is transmitted.

Congestion Control

Congestion Control techniques in Computer Networks

Heavy traffic of packets over a network.
Congestion control refers to the techniques used to control or prevent congestion. Congestion control techniques can be broadly classified into two categories:



Open Loop Congestion Control

Open loop congestion control policies are applied to prevent congestion before it happens. The congestion control is handled either by the source or the destination.

Policies adopted by open loop congestion control –

1. **Retransmission Policy :**
   It is the policy in which retransmission of the packets are taken care of. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network.
   To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency.

2. **Window Policy :**
   The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received successfully at the receiver side. This duplication may increase the congestion in the network and make it worse.
   Therefore, Selective repeat window should be adopted as it sends the specific packet that may have been lost.

3. **Discarding Policy :**
   A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message.
   In case of audio file transmission, routers can discard less sensitive packets to prevent congestion and also maintain the quality of the audio file.

4. **Acknowledgment Policy :**
   Since acknowledgements are also the part of the load in the network, the acknowledgment policy imposed by the receiver may also affect congestion. Several approaches can be used to prevent congestion related to acknowledgment.
   The receiver should send acknowledgement for N packets rather than sending acknowledgement for a single packet.
   The receiver should send an acknowledgment only if it has to send a packet or a timer expires.

5. **Admission Policy :**
   In admission policy a mechanism should be used to prevent congestion. Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion.

All the above policies are adopted to prevent congestion before it happens in the network.

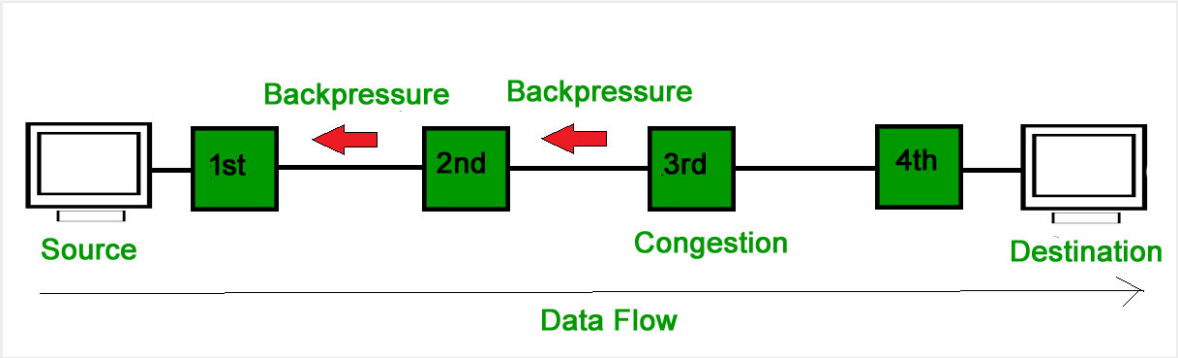
Closed Loop Congestion Control

Closed loop congestion control techniques are used to treat or alleviate congestion after it happens. Several techniques are used by different protocols; some of them are:

1. Back pressure :

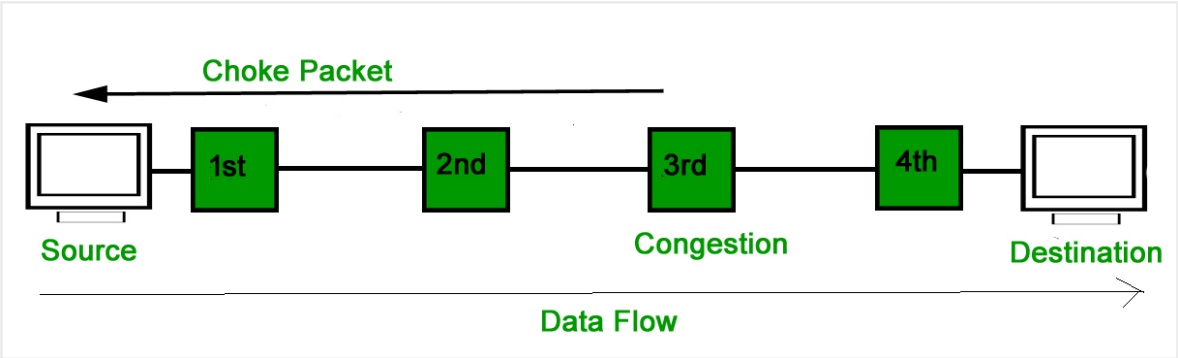
Back pressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject receiving data from above nodes. Back pressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow. The

back pressure technique can be applied only to virtual circuit where each node has information of its above upstream node.



In above diagram the 3rd node is congested and stops receiving packets as a result 2nd node may be get congested due to slowing down of the output data flow. Similarly 1st node may get congested and inform the source to slow down.

2. Choke Packet Technique :
Choke packet technique is applicable to both virtual networks as well as datagram subnets. A choke packet is a packet sent by a node to the source to inform it of congestion. Each router monitors its resources and the utilization at each of its output lines. Whenever the resource utilization exceeds the threshold value which is set by the administrator, the router directly sends a choke packet to the source giving it a feedback to reduce the traffic. The intermediate nodes through which the packets has traveled are not warned about congestion.



3. Implicit Signaling :
In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4. Explicit Signaling :
In explicit signaling, if a node experiences congestion it can explicitly sends a packet to the source or destination to inform about congestion. The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique.
Explicit signaling can occur in either forward or backward direction.

- **Forward Signaling :** In forward signaling, a signal is sent in the direction of the congestion. The destination is warned about congestion. The receiver in this case adopt policies to prevent further congestion.
- **Backward Signaling :** In backward signaling, a signal is sent in the opposite direction of the congestion. The source is warned about congestion and it needs to slow down.

What is Routing

- A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
- A Router works at the network layer in the OSI model and internet layer in TCP/IP model
- A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
- The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
- The routing algorithm initializes and maintains the routing table for the process of path determination.

Routing Metrics and Costs
Routing metrics and costs are used for determining the best route to

the destination. The factors used by the protocols to determine the shortest path, these factors are known as a metric.
Metrics are the network variables used to determine the best route to the destination. For some protocols use the static metrics means that their value cannot be changed and for some other routing protocols use the dynamic metrics means that their value can be assigned by the system administrator.

The most common metric values are given below:

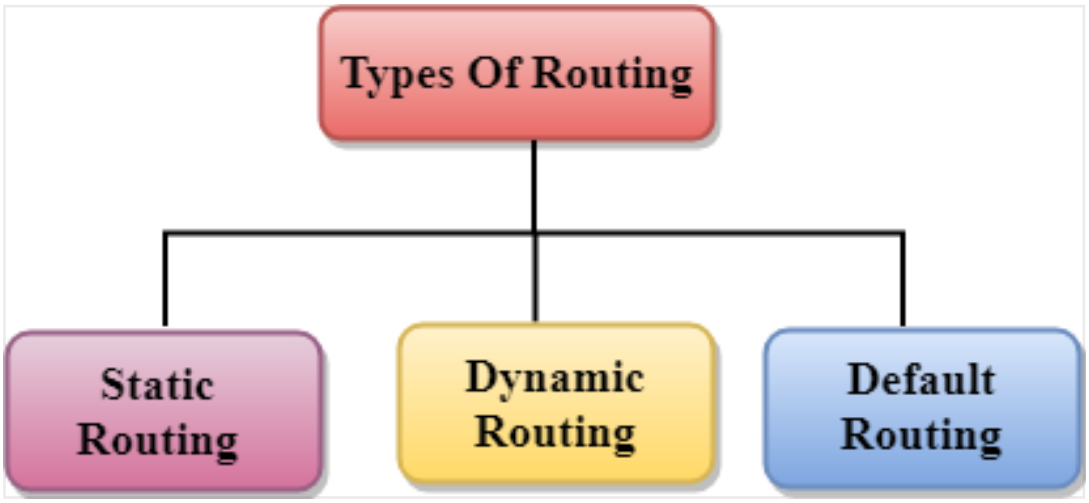
- **Hop count:** Hop count is defined as a metric that specifies the number of passes through internetworking devices such as a router, a packet must travel in a route to move from source to the destination. If the routing protocol considers the hop as a primary metric value, then the path with the least hop count will be considered as the best path to move from source to the destination.
- **Delay:** It is a time taken by the router to process, queue and transmit a datagram to an interface. The protocols use this metric to determine the delay values for all the links along the path end-to-end. The path having the lowest delay value will be considered as the best path.
- **Bandwidth:** The capacity of the link is known as a bandwidth of the link. The bandwidth is measured in terms of bits per second. The link that has a higher transfer rate like gigabit is preferred over the link that has the lower capacity like 56 kb. The protocol will determine the bandwidth capacity for all the links along the path, and the overall higher bandwidth will be considered as the best route.
- **Load:** Load refers to the degree to which the network resource such as a router or network link is busy. A Load can be calculated in a variety of ways such as CPU utilization, packets processed per second. If the traffic increases, then the load value will also be increased. The load value changes with respect to the change in the traffic.
- **Reliability:** Reliability is a metric factor may be composed of a fixed value. It depends on the network links, and its value is measured dynamically. Some networks go down more often than others. After network failure, some network links repaired more easily than other network links. Any reliability factor can be considered for the assignment of reliability ratings, which are generally numeric values assigned by the

system administrator.

Types of Routing

Routing can be classified into three categories:

- Static Routing
- Default Routing
- Dynamic Routing



Static Routing

- Static Routing is also known as Nonadaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
- A Router can send the packets for the destination along the route defined by the administrator.
- In this technique, routing decisions are not made based on the condition or topology of the networks

Advantages Of Static Routing

Following are the advantages of Static Routing:

- **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- **Bandwidth:** It has not bandwidth usage between the routers.
- **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

Advantages of Dynamic Routing:

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

Disadvantages of Dynamic Routing:

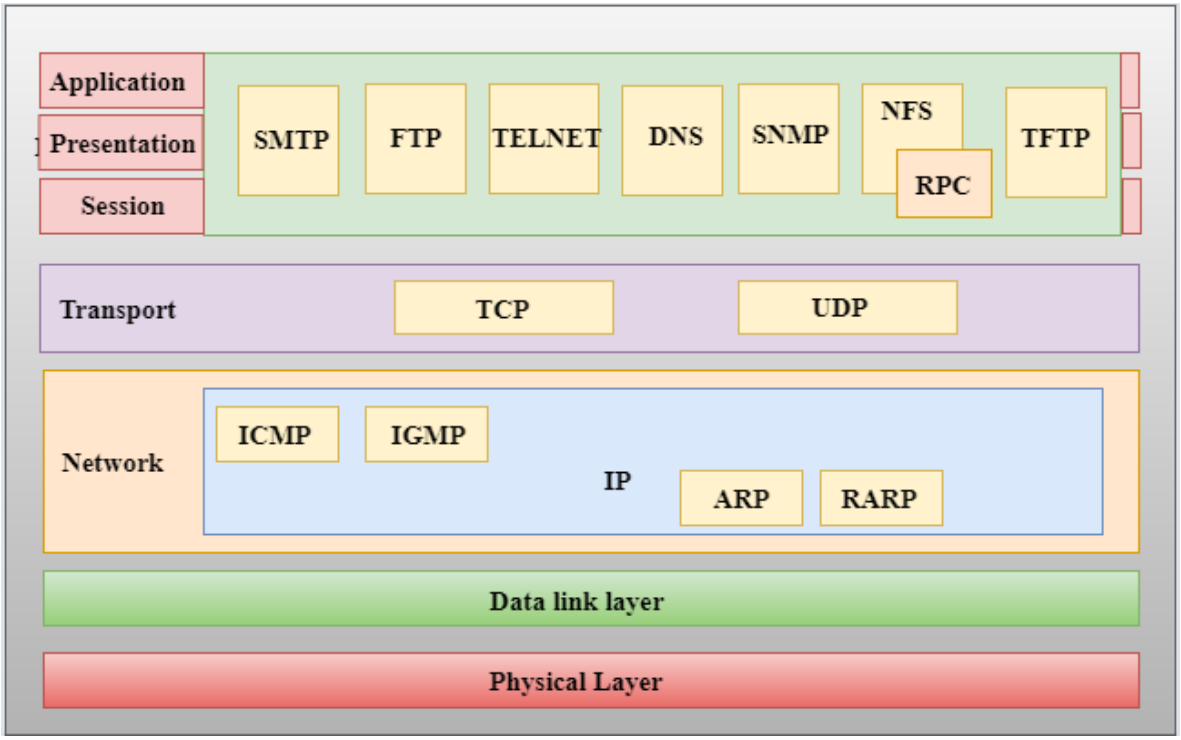
- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing.

TCP/IP model

- The TCP/IP model was developed prior to the OSI model.
- The TCP/IP model is not exactly similar to the OSI model.
- The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
- The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

Functions of TCP/IP layers:



Network Access Layer

- A network layer is the lowest layer of the TCP/IP model.
- A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
- It defines how the data should be sent physically through the network.

- This layer is mainly responsible for the transmission of the data between two devices on the same network.
- The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
- The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

Internet Layer

- An internet layer is the second layer of the TCP/IP model.
- An internet layer is also known as the network layer.
- The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

IP Protocol: IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant

network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

ARP Protocol

- ARP stands for **Address Resolution Protocol**.
- ARP is a network layer protocol which is used to find the physical address from the IP address.
- **The two terms are mainly associated with the ARP Protocol:**
  - **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  - **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

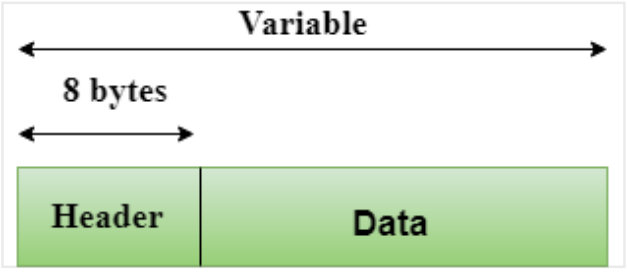
ICMP Protocol

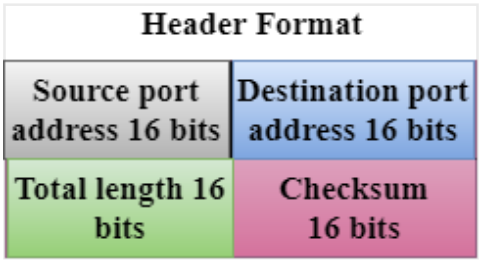
- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
- An ICMP protocol mainly uses two terms:
  - **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  - **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
- The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
- ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the

addresses of the source and destination but not of the router that it is passed to.

Transport Layer
The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.
The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

- **User Datagram Protocol (UDP)**
  - It provides connectionless service and end-to-end delivery of transmission.
  - It is an unreliable protocol as it discovers the errors but not specify the error.
  - User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  - **UDP consists of the following fields:**
    Source port address: The source port address is the address of the application program that has created the message.
    Destination port address: The destination port address is the address of the application program that receives the message.
    Total length: It defines the total number of bytes of the user datagram in bytes.
    Checksum: The checksum is a 16-bit field used in error detection.
  - UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.





- **Transmission Control Protocol (TCP)**
  - It provides a full transport layer services to applications.
  - It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  - TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  - At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  - At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

Application Layer

- An application layer is the topmost layer in the TCP/IP model.
- It is responsible for handling high-level protocols, issues of representation.
- This layer allows the user to interact with the application.
- When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
- There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

- **HTTP:** HTTP stands for Hypertext transfer protocol. This

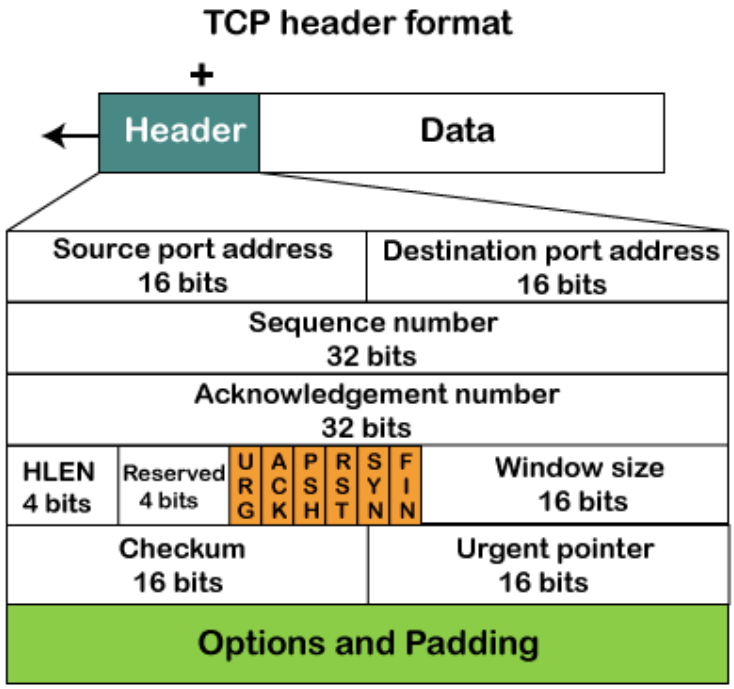
protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

- **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
- **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
- **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
- **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
- **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Next TopicDigital Transmission

TCP HEADER

TCP Header Format



- **Source port:** It defines the port of the application, which is sending the data. So, this field contains the source port address, which is 16 bits.
- **Destination port:** It defines the port of the application on the receiving side. So, this field contains the destination port address, which is 16 bits.
- **Sequence number:** This field contains the sequence number of data bytes in a particular session.
- **Acknowledgment number:** When the ACK flag is set, then this contains the next sequence number of the data byte and works as an acknowledgment for the previous data received. For example, if the receiver receives the segment number 'x', then it responds 'x+1' as an acknowledgment number.
- **HLEN:** It specifies the length of the header indicated by the 4-byte words in the header. The size of the header lies between 20 and 60 bytes. Therefore, the value of this field would lie between 5 and 15.
- **Reserved:** It is a 4-bit field reserved for future use, and by default, all are set to zero.
- **Flags**
  There are six control bits or flags:
  1. **URG:** It represents an urgent pointer. If it is set, then the data is processed urgently.

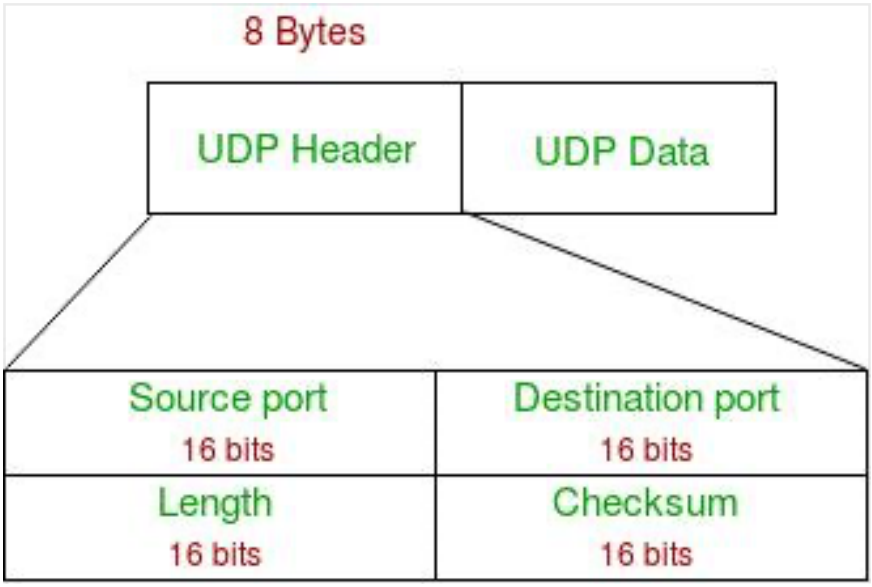
2. **ACK:** If the ACK is set to 0, then it means that the data packet does not contain an acknowledgment.
3. **PSH:** If this field is set, then it requests the receiving device to push the data to the receiving application without buffering it.
4. **RST:** If it is set, then it requests to restart a connection.
5. **SYN:** It is used to establish a connection between the hosts.
6. **FIN:** It is used to release a connection, and no further data exchange will happen.

- **Window size**
  It is a 16-bit field. It contains the size of data that the receiver can accept. This field is used for the flow control between the sender and receiver and also determines the amount of buffer allocated by the receiver for a segment. The value of this field is determined by the receiver.
- **Checksum**
  It is a 16-bit field. This field is optional in UDP, but in the case of TCP/IP, this field is mandatory.
- **Urgent pointer**
  It is a pointer that points to the urgent data byte if the URG flag is set to 1. It defines a value that will be added to the sequence number to get the sequence number of the last urgent byte.
    - **Options**

It provides additional options. The optional field is represented in 32-bits. If this field contains the data less than 32-bit, then padding is required to obtain the remaining bits.

UDP Header

UDP header is an **8-byte** fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes. The first 8 Bytes contain all necessary header information and the remaining part consists of data. UDP port number fields are each 16 bits long, therefore the range for port numbers is defined from 0 to 65535; port number 0 is reserved. Port numbers help to distinguish different user requests or processes.



UDP Header

- **Source Port:** Source Port is a 2 Byte long field used to identify the port number of the source.
- **Destination Port:** It is a 2 Byte long field, used to identify the port of the destined packet.
- **Length:** Length is the length of UDP including the header and the data. It is a 16-bits field.
- **Checksum:** Checksum is 2 Bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, the pseudo-header of information from the IP header, and the data, padded with zero octets at the end (if necessary) to make a multiple of two octets.

Notes – Unlike TCP, the Checksum calculation is not mandatory in UDP. No Error control or flow control is provided by UDP. Hence UDP depends on IP and ICMP for error reporting. Also UDP provides port numbers so that is can differentiate between users requests.

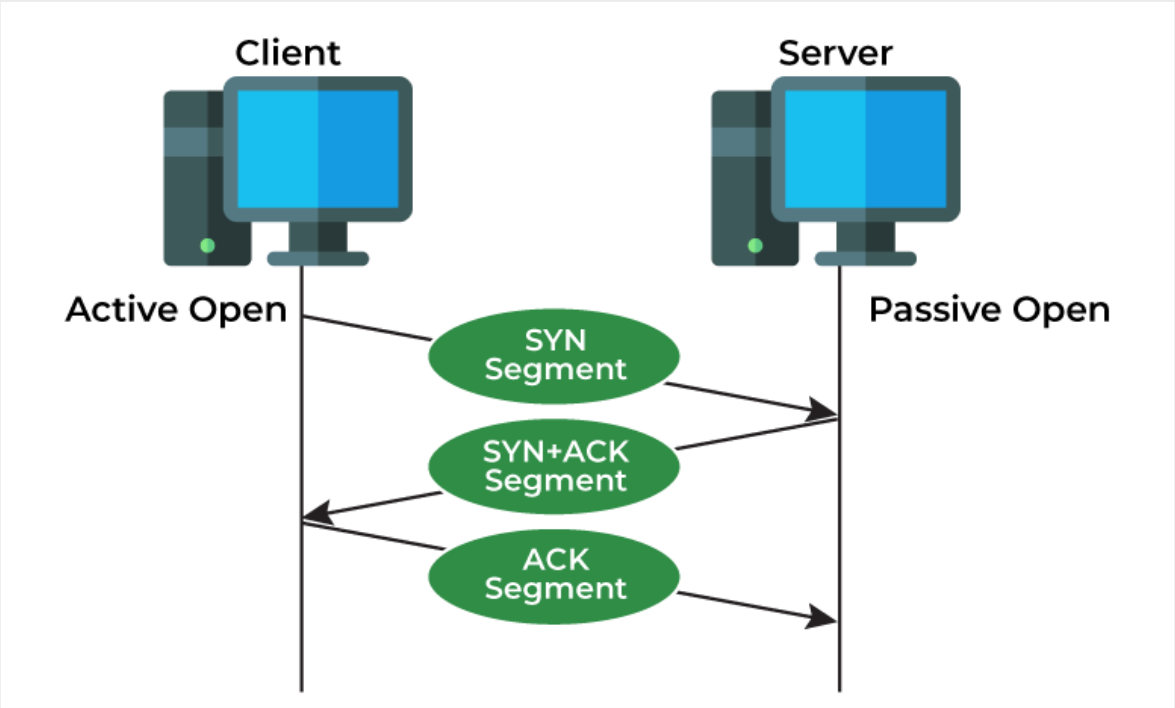
Differences between TCP and UDP

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) both are protocols of the Transport Layer Protocols. TCP is a connection-oriented protocol whereas UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. In this article, we will discuss the differences between TCP and UDP.

What is Transmission Control Protocol (TCP)?

TCP (Transmission Control Protocol) is one of the main protocols of the Internet protocol suite. It lies between the Application and

Network Layers which are used in providing reliable delivery services. It 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.



Transmission Control Protocol

Features of TCP

- TCP keeps track of the segments being transmitted or received by assigning numbers to every single one of them.
- Flow control limits the rate at which a sender transfers data. This is done to ensure reliable delivery.
- TCP implements an error control mechanism for reliable data transfer.
- TCP takes into account the level of congestion in the network.

Applications of TCP

- **World Wide Web (WWW)** : When you browse websites, TCP ensures reliable data transfer between your browser and web servers.
- **Email** : TCP is used for sending and receiving emails. Protocols like **SMTP** (Simple Mail Transfer Protocol) handle email delivery across servers.
- **File Transfer Protocol (FTP)** : FTP relies on TCP to transfer large files securely. Whether you're uploading or downloading files, TCP ensures data integrity.
- **Secure Shell (SSH)** : SSH sessions, commonly used for

remote administration, rely on TCP for encrypted communication between client and server.
- **Streaming Media** : Services like Netflix, YouTube, and Spotify use TCP to stream videos and music. It ensures smooth playback by managing data segments and retransmissions.

Advantages of TCP

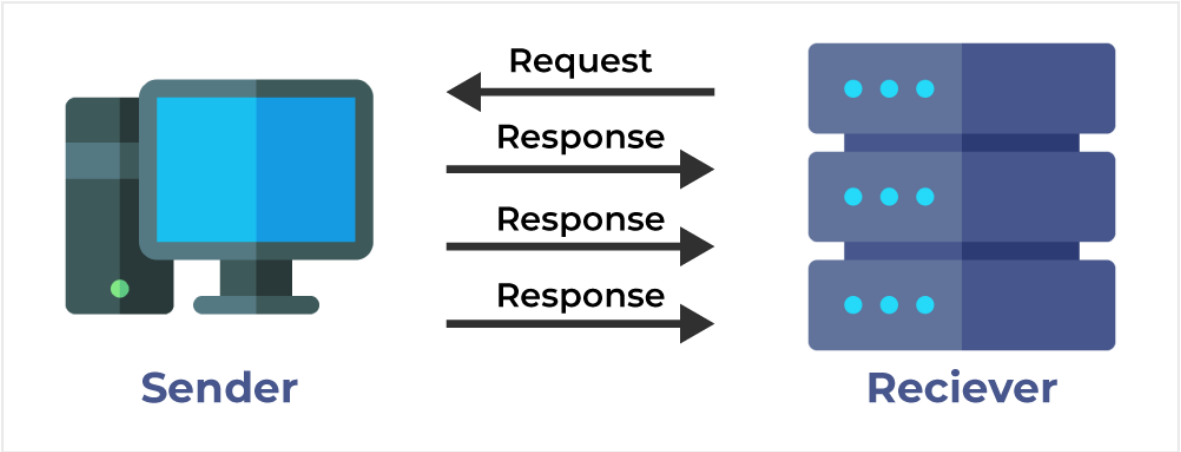
- It is reliable for maintaining a connection between Sender and Receiver.
- It is responsible for sending data in a particular sequence.
- Its operations are not dependent on Operating System .
- It allows and supports many routing protocols.
- It can reduce the speed of data based on the speed of the receiver.

Disadvantages of TCP

- It is slower than UDP and it takes more bandwidth.
- Slower upon starting of transfer of a file.
- Not suitable for LAN and PAN Networks.
- It does not have a multicast or broadcast category.
- It does not load the whole page if a single data of the page is missing.

What is User Datagram Protocol (UDP)?

User Datagram Protocol (UDP) is a Transport Layer protocol. UDP is a part of the Internet Protocol suite, referred to as the UDP/IP suite. Unlike TCP, it is an unreliable and connectionless protocol. So, there is no need to establish a connection before data transfer. The UDP helps to establish low-latency and loss-tolerating connections establish over the network. The UDP enables process-to-process communication.



User Datagram Protocol

Features of UDP

- Used for simple request-response communication when the

size of data is less and hence there is lesser concern about flow and error control.
- It is a suitable protocol for multicasting as UDP supports packet switching .
- UDP is used for some routing update protocols like RIP(Routing Information Protocol) .
- Normally used for real-time applications which can not tolerate uneven delays between sections of a received message.

Application of UDP

- **Real-Time Multimedia Streaming** : UDP is ideal for streaming audio and video content. Its low-latency nature ensures smooth playback, even if occasional data loss occurs.
- **Online Gaming** : Many online games rely on UDP for fast communication between players.
- **DNS (Domain Name System) Queries** : When your device looks up domain names (like converting “www.example.com” to an IP address), UDP handles these requests efficiently ·
- **Network Monitoring** : Tools that monitor network performance often use UDP for lightweight, rapid data exchange.
- **Multicasting** : UDP supports packet switching, making it suitable for multicasting scenarios where data needs to be sent to multiple recipients simultaneously.
- **Routing Update Protocols** : Some routing protocols, like RIP (Routing Information Protocol), utilize UDP for exchanging routing information among routers.

Advantages of UDP

- It does not require any connection for sending or receiving data.
- Broadcast and Multicast are available in UDP.
- UDP can operate on a large range of networks.
- UDP has live and real-time data.
- UDP can deliver data if all the components of the data are not complete.

Disadvantages of UDP

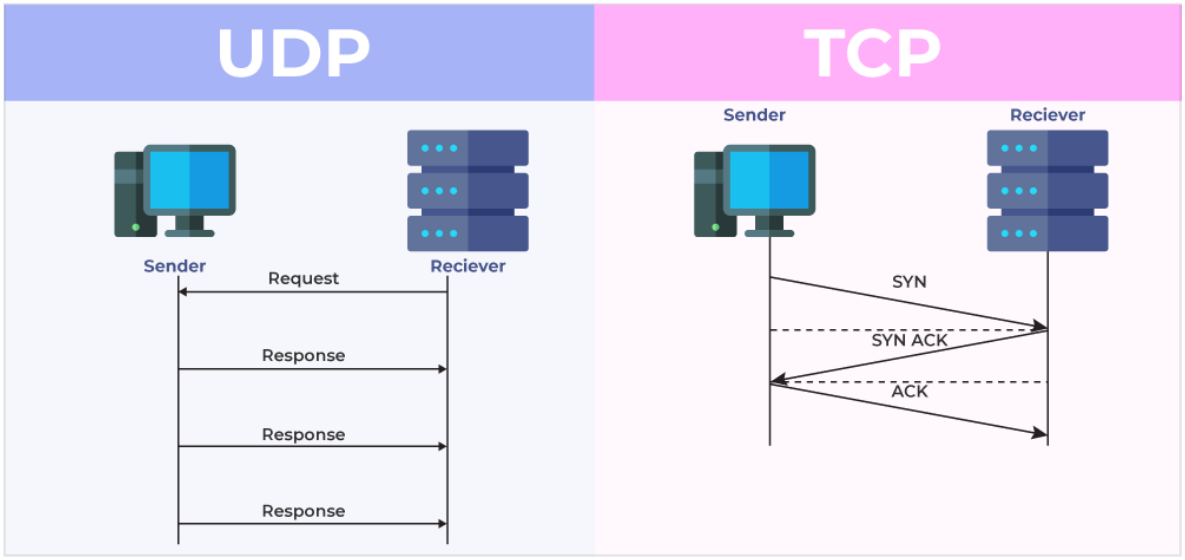
- We can not have any way to acknowledge the successful transfer of data.
- UDP cannot have the mechanism to track the sequence of

data.

- UDP is connectionless, and due to this, it is unreliable to transfer data.
- In case of a Collision, UDP packets are dropped by Routers in comparison to TCP.
- UDP can drop packets in case of detection of errors.

Which Protocol is Better: TCP or UDP?

The answer to this question is difficult because it totally depends on what work we are doing and what type of data is being delivered. UDP is better in the case of online gaming as it allows us to work lag-free. TCP is better if we are transferring data like photos, videos, etc. because it ensures that data must be correct has to be sent. In general, both TCP and UDP are useful in the context of the work assigned by us. Both have advantages upon the works we are performing, that's why it is difficult to say, which one is better.



Difference Between TCP and UDP

Where TCP is Used?

- Sending Emails
- Transferring Files
- Web Browsing

Where UDP is Used?

- Gaming
- Video Streaming
- Online Video Chats

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. UDP is efficient for broadcast and multicast types of network transmission.
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.
Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Weight	TCP is heavy-weight.	UDP is lightweight.
Handshaking Techniques	Uses handshakes such as SYN, ACK, SYN-ACK	It's a connectionless protocol i.e. No handshake
Broadcasting	TCP doesn't support Broadcasting.	UDP supports Broadcasting.
Protocols	TCP is used by HTTP, HTTPs , FTP , SMTP and Telnet .	UDP is used by DNS , DHCP , TFTP, SNMP , RIP , and VoIP .
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.
Overhead	Low but higher than UDP.	Very low.

Applications	This protocol is primarily utilized in situations when a safe and trustworthy communication procedure is necessary, such as in email, on the web surfing, and in military services.	This protocol is used in situations where quick communication is necessary but where dependability is not a concern, such as VoIP, game streaming, video, and music streaming, etc.

Example: Suppose there are two houses, H1 and H2, and a letter has to be sent from H1 to H2. But there is a river in between those two houses. Now how can we send the letter?
Solution 1: Make a bridge over the river and then it can be delivered.
Solution 2: Get it delivered by a pigeon.

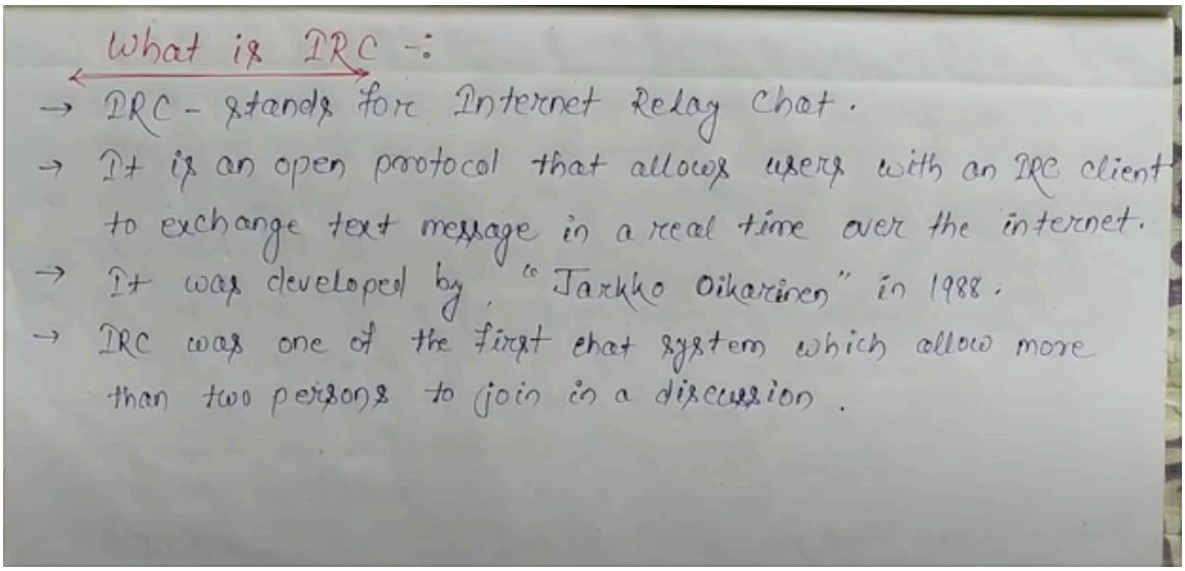
- Consider the first solution as **TCP** . A connection has to be made (bridge) to get the data (letter) delivered. The data is reliable because it will directly reach another end without loss of data or error.
- The second solution is **UDP** . No connection is required for sending the data. The process is fast as compared to TCP, where we need to set up a connection(bridge). But the data is not reliable: we don't know whether the pigeon will go in the right direction, will drop the letter on the way, or some issue is encountered mid-travel.

Conclusion
To summarise, TCP and UDP are both important Transport Layer protocols with distinct properties and uses. TCP offers dependable, orderly, and error-free data transmission, making it ideal for operations that require precision, such as file transfers and web browsing. UDP, on the other hand, provides quicker, connectionless communication that is excellent for real-time applications such as gaming and video streaming, when speed is critical and minor data loss is acceptable. The exact requirements of the task at hand determine whether TCP or UDP should be used.

Frequently Asked Questions on TCP and UDP – FAQs

Which is faster: TCP or UDP?
UDP is faster than TCP. The reason for the faster UDP is its non-existent acknowledge packet (ACK) which allows the streaming of continuous packets where as TCP always works on the acknowledgment of a set of packets calculated with the help of TCP window size and Round Trip Time (RTT) .
Which is better for Video Conferencing?
Both Protocols, TCP and UDP have several practical uses in day-to-day life, but TCP has come as a better solution nowadays in the modern era as a solution for this question of who is better at Video Conferencing.
How is UDP used in real life?
Streaming media, real-time multiplayer games and voice over IP (VoIP) .

INTERNET RELAY CHAT



Key Network Protocols and Concepts

File Transfer Protocol (FTP)
FTP is a standard network protocol used to transfer computer files between a client and a server on a computer network. It uses a client-server model, where the client initiates the connection and sends commands to the server to transfer files.

Email

Email is a method of electronic communication that allows users to send and receive messages over computer networks. It uses various protocols for different stages of communication:

- **SMTP (Simple Mail Transfer Protocol):** Used for sending email messages.
- **POP3 (Post Office Protocol):** Used for retrieving email messages from a mail server.
- **IMAP (Internet Message Access Protocol):** Allows users to access and manage email messages on a mail server.

World Wide Web
The World Wide Web (WWW) is a system of interlinked hypertext documents accessed via the Internet. It uses the **HTTP (Hyper text Transfer Protocol)** to transmit data between web servers and web browsers.

Client-Server Environment
A client-server environment is a network architecture where a client computer requests services from a server computer. The server provides the requested services, such as file storage, web pages, or database access.

DNS (Domain Name System)
DNS is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It translates domain names (like [invalid URL removed]) into IP addresses (like 142.250.186.142), making it easier for users to access resources on the internet.

In essence, these technologies work together to facilitate communication and information exchange over the internet:

1. **DNS:** Translates domain names into IP addresses.
2. **HTTP:** Enables the transfer of web pages and other resources.
3. **FTP:** Allows for file transfer between computers.
4. **Email Protocols:** Facilitate email communication.
5. **Client-Server Model:** Underpins the interaction between devices on a network.

By understanding these fundamental concepts, you can better appreciate how the internet works and how it enables a wide range of

online activities.