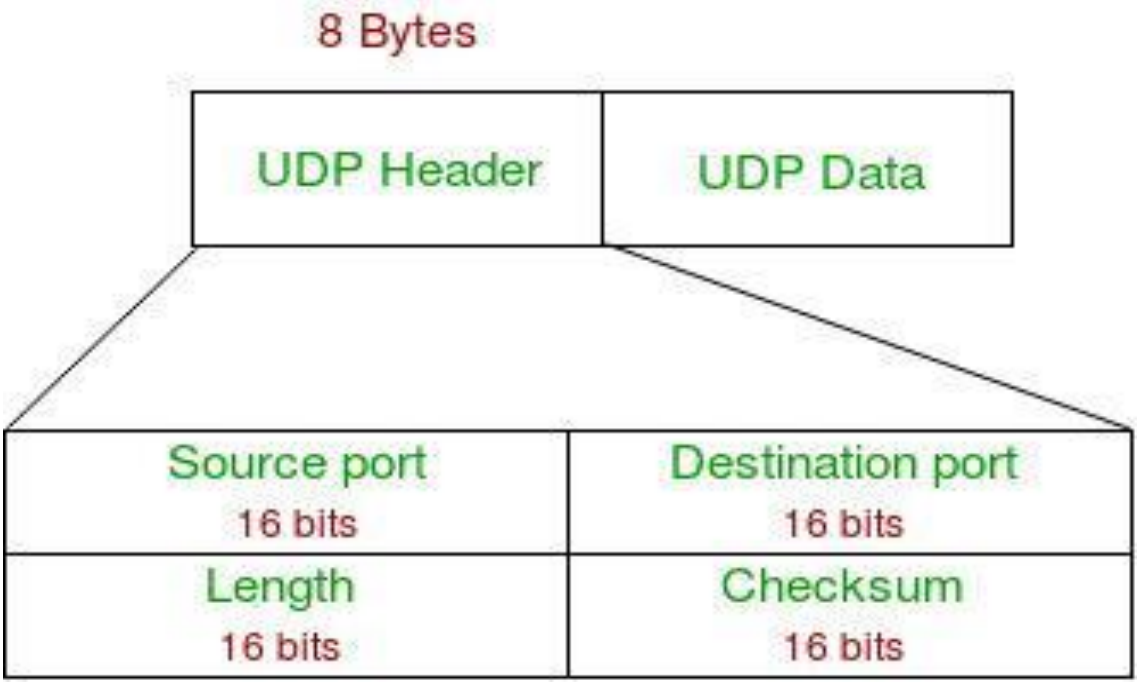
UDP Protocol

1. What is UDP and How it Operates :

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 playback or DNS lookups. Unlike Transmission Control Protocol (TCP), UDP is connectionless and does not guarantee delivery, order, or error checking, making it a lightweight and efficient option for certain types of data transmission.

Working principles:

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.



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.

2.Applications of UDP:

1. Used for simple request-response communication when the size of data is less and hence there is lesser concern about flow and error control.

2.It is a suitable protocol for multicasting as UDP supports packet switching.

3. used for some routing update protocols like RIP(Routing Information Protocol).

4. used for real-time applications which can not tolerate uneven delays between sections of a received message.

5. VOIP (Voice over Internet Protocol) services, such as Skype and WhatsApp, use UDP for real-time voice communication. The delay in voice communication can be noticeable if packets are delayed due to congestion control, so UDP is used to ensure fast and efficient data transmission.

6. DNS (Domain Name System) also uses UDP for its query/response messages. DNS queries are typically small and require a quick response time, making UDP a suitable protocol for this application.

3.Advantages of UDP:

Speed: UDP is faster than TCP because it does not have the overhead of establishing a connection and ensuring reliable data delivery.

Lower latency: Since there is no connection establishment, there is lower latency and faster response time.

Simplicity: UDP has a simpler protocol design than TCP, making it easier to implement and manage.

Broadcast support: UDP supports broadcasting to multiple recipients, making it useful for applications such as video streaming and online gaming.

Smaller packet size: UDP uses smaller packet sizes than TCP, which can reduce network congestion and improve overall network performance.

User Datagram Protocol (UDP) is more efficient in terms of both latency and bandwidth.

4.Disadvantages of UDP:

No reliability: UDP does not guarantee delivery of packets or order of delivery, which can lead to missing or duplicate data.

No congestion control: UDP does not have congestion control, which means that it can send packets at a rate that can cause network congestion.

Vulnerable to attacks: UDP is vulnerable to denial-of-service attacks, where an attacker can flood a network with UDP packets, overwhelming the network and causing it to crash.

Limited use cases: UDP is not suitable for applications that require reliable data delivery, such as email or file transfers, and is better suited for applications that can tolerate some data loss, such as video streaming or online gaming.