Internet layer protocols (Network layer protocols)

- The Internet layer is responsible for packaging, addressing, and routing the data.
- Protocols used in Internet layer are as follows:

1. IP
2. ARP
3. RARP
4. ICMP
5. IGMP
6. OSPF
7. RIP

1. IP (Internet Protocol):

- It is **connectionless** datagram protocol because it does not establish a session with a remote computer before sending data.
- It is **unreliable** protocol because it does not provide any error or flow control.
- It provides best effort delivery service.
- It transports data packets called datagrams that travel over different routes across multiple nodes.
- At destination, datagrams can arrive out of sequence or they can be duplicated.
- IP doesn't keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.
- It has no error reporting or error correcting mechanism. Recovery is the responsibility of higher layer protocols.
- There are two version of IP (IPv4 and IPv6).

2. ARP (Address Resolution Protocol):

- On a typical physical network such as LAN, each device on a link is identified by a physical address (MAC address) which is imprinted on Network Interface Card (NIC).
- Each NIC also is assigned an IP address that is unique to the network.
- ARP is responsible for mappings of IP addresses to MAC addresses.

3. RARP (Reverse Address Resolution Protocol):

- RARP is responsible for mappings of MAC addresses to IP addresses.

4. ICMP (Internet Control Message Protocol):

- It is responsible for handling errors related to IP packets that cannot be delivered. But it does not correct them.
- It is a supporting protocol and used by networks devices like routers for sending the error messages and operations information.
- For example, some sender wants to send the message to some destination, but the router couldn't send the message to the destination. In this case, the router sends the message to the sender that I could not send the message to that destination.

5. IGMP (Internet Group Message Protocol):

- The IP protocol supports two types of communication:
    - **Unicasting:** It is a communication between one sender and one receiver. Therefore, we can say that it is one-to-one communication.
    - **Multicasting:** Sometimes the sender wants to send the same message to a large number of receivers simultaneously. This process is known as multicasting which has one-to-many communication.
- The IGMP protocol is used to provide multicasting.

6. OSPF (Open Shortest Path First):

- It is a link-state routing protocol.
- It is used to find the best path between the source and the destination router.

7. RIP (Routing Information Protocol):

- It is a distance vector routing protocol.
- It is a protocol used by routers to exchange routing information on a network.

⇨ Transport Layer protocols:

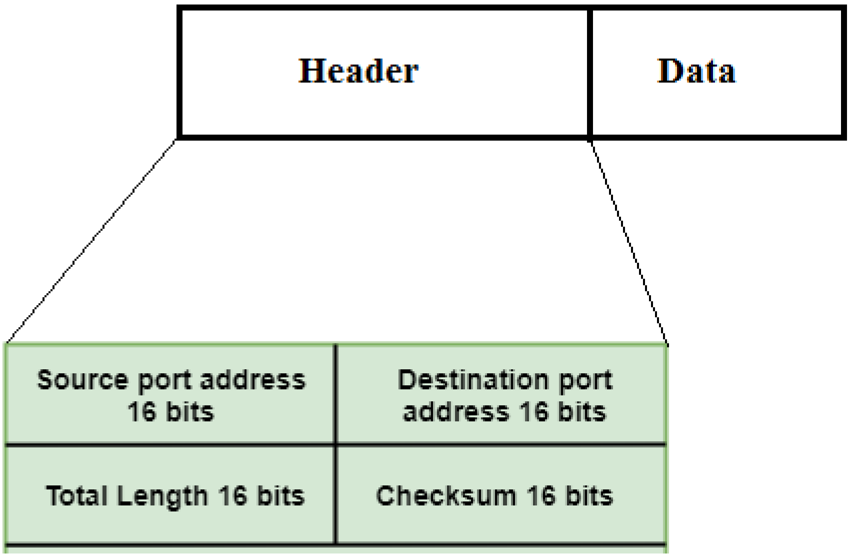
- Transport layer is responsible for the reliability, flow control, and correction of data which is sent over the network.
- It also ensures that data units are in sequence and provides acknowledgment of the successful data transmission.
- There three protocols used in the transport layer:

    1. UDP (User Datagram Protocol)
    2. TCP (Transmission control protocol)
    3. SCTP (Stream Control Transmission Protocol)

1. UDP (User Datagram Protocol) :

- 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 (**format of User Datagram):**



Here, header includes four fields which are listed below:

1. **Source port address:** It defines the address of the application process that has created a message. The source port address is of 16 bits address.
2. **Destination port address:** It defines the address of the application process that will receive the message. The destination port address is of a 16-bit address.
3. **Total length:** It defines the total length of the user datagram in bytes. It is a 16-bit field.
4. **Checksum:** It is a 16-bit field which is used in error detection.

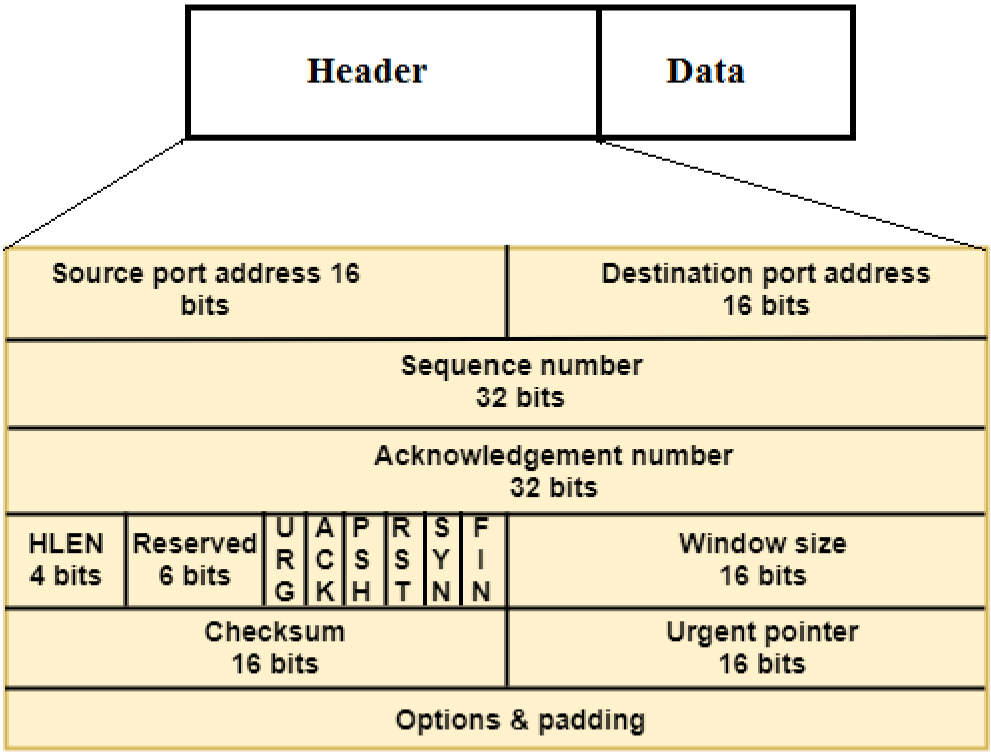
Disadvantages of UDP protocol:

- UDP provides basic functions needed for the end-to-end delivery of a transmission.
- It does not provide any sequencing or reordering functions and does not specify the damaged packet when reporting an error.
- UDP can discover that an error has occurred, but it does not specify which packet has been lost as it does not contain sequencing number of a particular data segment.

2. TCP (Transmission control protocol):

- It provides full transport layer services to applications.

- It is a connection-oriented protocol means the connection must be established between both the ends of the transmission.
- It is a reliable protocol that is acknowledgement is sent for each received packet.
- At the sender side, TCP divides an data into segments and assigns a unique sequence number to each segment.
- At the receiving side, TCP reorders the segments and sends an acknowledgment to the sender for correct receipt of segments.
- TCP **Segment** Format is shown in the following diagram:



1. **Source port address:** It is used to define the address of the application program in a source computer. It is a 16-bit field.
2. **Destination port address:** It is used to define the address of the application program in a destination computer. It is a 16-bit field.
3. **Sequence number:** A stream of data is divided into two or more TCP segments. It represents the position of the data in an original data stream.
4. **Acknowledgement number:** It is of 32-bits field. It is used to acknowledge the data from other communicating devices. If ACK field is set to 1, then it specifies the sequence number that the receiver is expecting to receive.

5. **Header Length (HLEN):** It is of 4-bits. It specifies the size of the TCP header in 32-bit words. The 4-bits can define a number upto 15. Therefore, the maximum size of the TCP header is 60 bytes (4*15).
6. **Reserved:** It is a 6-bit field which is reserved for future use.
7. **Control bits:** Each bit of a control field functions individually and independently. A control bit defines the use of a segment or serves as a validity check for other fields.

   There are total six types of flags in control field:

   a) **URG:** It indicates that the data in a segment is urgent.

   b) **ACK:** When ACK field is set, then it validates the acknowledgement number.

   c) **PSH:** It is used to inform the sender that higher throughput is needed. so if possible, data must be pushed with higher throughput.

   d) **RST:** It is used to reset the TCP connection when there is any confusion in the sequence numbers.

   e) **SYN:** It is used to synchronize the sequence numbers in three types of segments:

      - connection request
      - connection confirmation (with the ACK bit set)
      - confirmation acknowledgement.

   f) **FIN:** It is used to inform the receiving TCP module that the sender has finished sending data. It is used in connection termination in three types of segments:

      - termination request
      - termination confirmation
      - acknowledgement of termination confirmation

8. **Window Size:** It is a 16-bit field that defines the size of the window.
9. **Checksum:** It is a 16-bit field used in error detection.
10. **Urgent pointer:** If URG flag is set to 1, then this 16-bit field is an offset from the sequence number indicating that it is a last urgent data byte.
11. **Options and padding:** It defines the optional fields that convey the additional information to the receiver.

3. SCTP (Stream Control Transmission Protocol):

- It combines the features of both TCP and UDP.
- It is used for network applications such as voice over the Internet.

Application Layer protocols:

- Application layer protocols are as follows:

1. FTP (File Transfer Protocol):

- FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

2. Telnet:

- It stands for **Terminal Network.**
- It establishes the connection between the local and remote computer.
- It establishes connection in such a manner that you can simulate your local system at the remote system.

3. SMTP (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/email to another e-mail address.
- It sets the rules and semantics for sending and receiving electronic mails (e-mails).

4. HTTP (Hyper Text Transfer Protocol):

- This protocol allows us to access the data over the World Wide Web.
- It is used for transferring webpages and other such resources from the HTTP server to the HTTP client.
- It defines how hypermedia messages are formatted and transmitted.

5. SNMP (Simple Network Management Protocol):

- It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.

6. DNS (Domain Name System):

- A DNS service translates the domain names into the corresponding IP addresses.
- For example, the domain name **www.abc.com** might translate to IP address **198.105.232.4.**