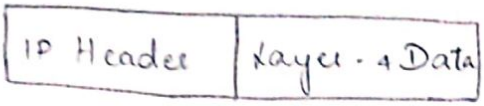
COMPUTER NETWORKS

UNIT - 1

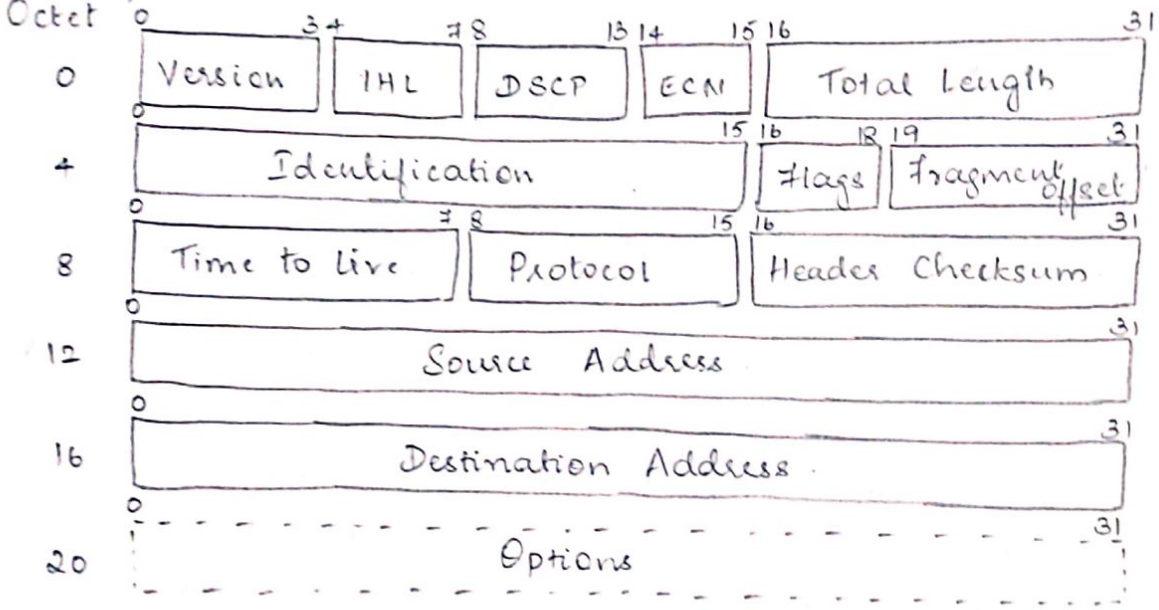
IP Header

- Internet Protocol being a layer-3 protocol (OSI) takes data segments from layer-4 & divides it into packets
- IP packet encapsulates data unit received from above layer & add to its own header information.



IP Encapsulation

- The encapsulated data is referred to as IP Payload.
- IP header contains all the necessary information to deliver the packet at the other end.



IP Header

- IP Header includes many relevant information including Version Number, which in this context is 4.
- Version - Version no. of internet Protocol used.
- IHL - Internet Header Length; length of entire IP header.
- DSCP - Differentiated Services Code Point; this is Type of Service.
- ECN - Explicit Congestion Notification; It carries information about the congestion seen in the route.
- Total length - Length of entire IP Packet (including IP header & IP Payload.
- Identification - If IP packet is fragmented during the transmission, all the fragments contain same identification no. to

identify original IP packet they belong to.

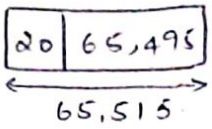
- Flags - As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- Fragment Offset - This offset tells the exact position of the fragment in the original IP Packet.
- Time to live - To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers this packet can cross. At each hop, its value is decremented by one & when the value reaches 0, the packet is discarded.
- Protocol :- Tells the n/w layer at the destination host, to which protocol this packet belongs to. i.e., the next level Protocol. eg: protocol no. of ICMP is 1, TCP is 6 & UDP is 17.
- Header Checksum - This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- Source Address - 32-bit address of the Sender (or source) of the packet.
- Destination Address - 32-bit address of the Receiver of the packet.
- Options - This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record route, Time Stamp etc.

IP fragmentation:

- Fragmentation is done by the n/w layer when the maximum size of datagram is greater than maximum size of data that can be held in a frame. i.e., its Maximum Transmission Unit (MTU).
- The n/w layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.
- Since there are 16 bits for total length in IP header so, max size of IP datagram =

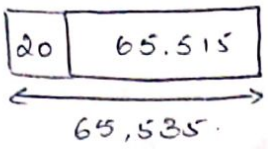
$= 2^{16} - 1 = 65,535$ bytes.

Transport layer (segment)



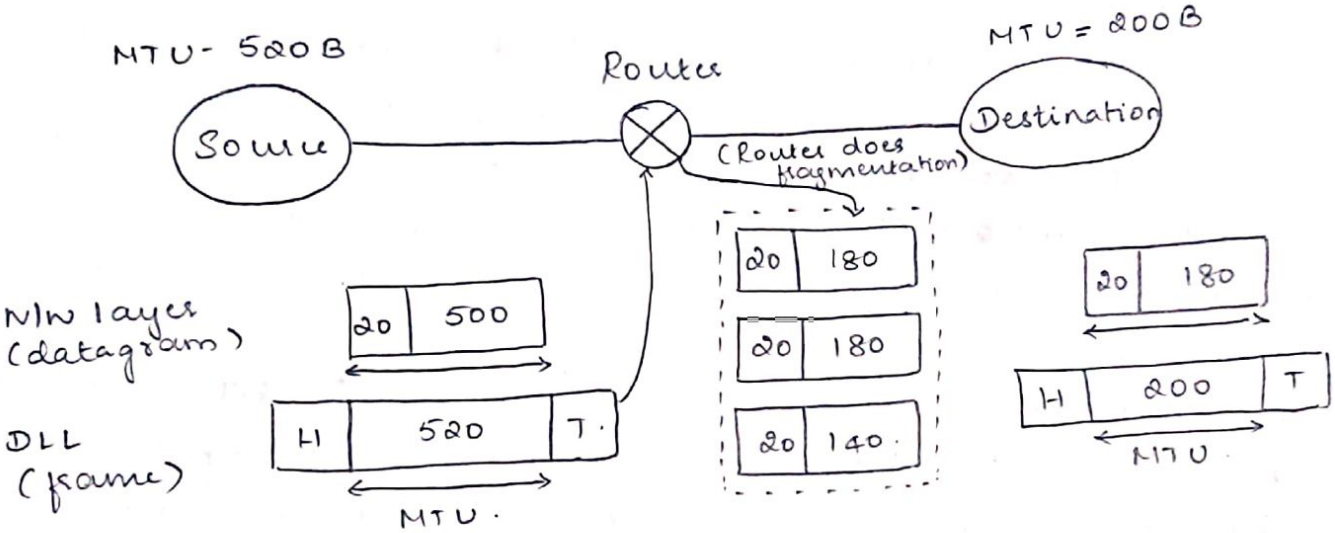
Max. size of data in segment
$= 65515 - 20 = 65495$ B

Network layer (datagram)



Max. size of data in datagram
$= 65535 - 20 = 65515$ B

- It is done by n/w layer at the desti. side & is usually done at routers.
- Source side does not require fragmentation due to wise segmentation by transport layer.



Fragmentation.

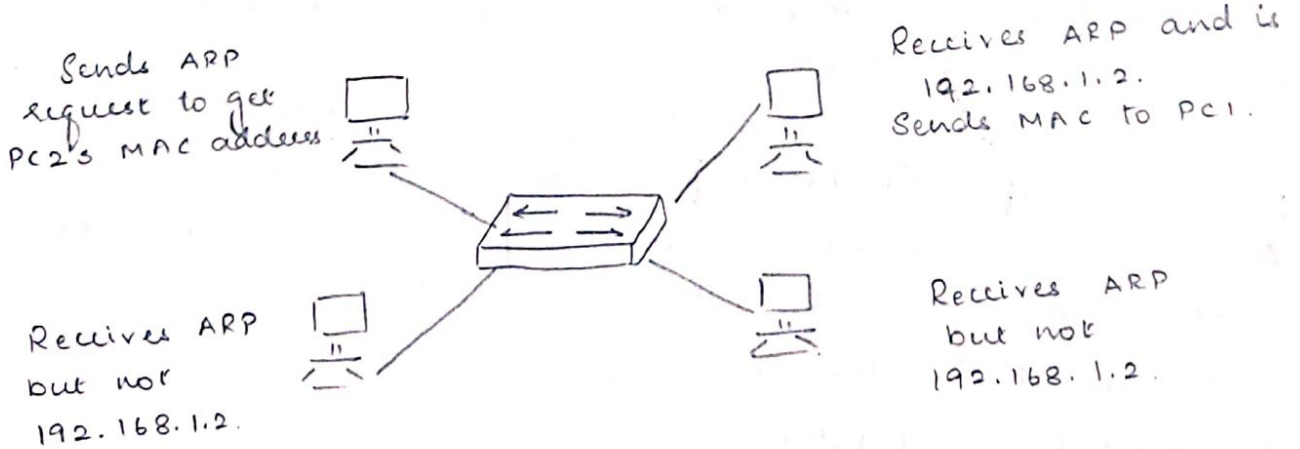
- Receiver identifies the frame with the identification (16 bits) field in IP header. Each fragment of a frame has same identification no.
- Receiver identifies sequences of frames using the fragment offset (13 bits) field in IP header.
- An overhead at n/w layer is present due to extra header introduced due to fragmentation.

Fields in IP header for fragmentation.

- Identification (16 bits)
- Fragment offset (13 bits)
- More fragments (MF = 1 bit)
- Don't fragment (DF = 1 bit).

ARP (Address Resolution Protocol)

- ARP is a communication protocol used for discovering physical address associated with given network address.
- Typically, ARP is a n/w layer to DLL mapping process, which is used to discover MAC address for given IP Address.
- In order to send the data to destination, having IP address is necessary but not sufficient; we also need the physical address of the destination machine.
- ARP is used to get the physical address of destination machine.
- Before sending the IP packet, the MAC address of destination must be known.
- If not so, then sender broadcasts the ARP-discovery packet requesting the MAC address of intended destination.
- Since ARP discovery is broadcast, every host inside that network will get this msg but the packet will be discarded by everyone except that intended receiver host whose IP is associated.
- Now this receiver will send a unicast packet with its MAC address to the sender of ARP-discovery packet.
- After the original sender receives the ARP reply, it updates ARP-cache & start sending unicast msg to the destination.



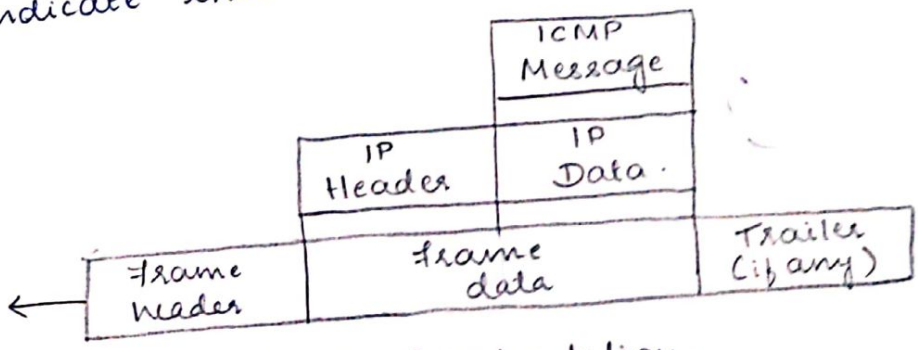
RARP - Reverse Address Resolution Protocol.

- Reverse ARP is a networking protocol used by a client machine in a local area network to request its IP address (IPv4) from the gateway-router's ARP table.

- The network administor creates a table in gateway source, which is used to map the MAC address to corresponding IP address.
- When a new machine is setup or any machine which don't have memory to store IP address, needs an IP address for its own use.
- So the machine sends a RARP broadcast packet which contains its own MAC address in both sender & receiver hardware address field.
- A special host configured inside the local area network, called as RARP-server is responsible to reply for these kind of broadcast packets.
- Now the RARP server attempt to find out the entry in IP to MAC address mapping table.
- If any entry matches in table, RARP server send the response packet to the requesting device along with IP address.
  - LAN Technologies like Ethernet, Ethernet II, Token Ring and FDDI support the address resolution protocol.
  - RARP is not being used in today's networks. Because we have much great featured protocols like BOOTP and DHCP.

ICMP - Introduction:

- ICMP - network layer protocol.
- Messages are not passed directly to the data link layer.
- Msgs are encapsulated inside IP datagrams before going to the lower layer.
- The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.



ICMP Encapsulation.

ICMP - Message

- ICMP message is of Two categories.

1. Errors-reporting messages:
   - This report problems that a router or a host may encounter when it processes an IP packet.
2. The query messages:
   - Helps network manager get specific info from a router to another host.

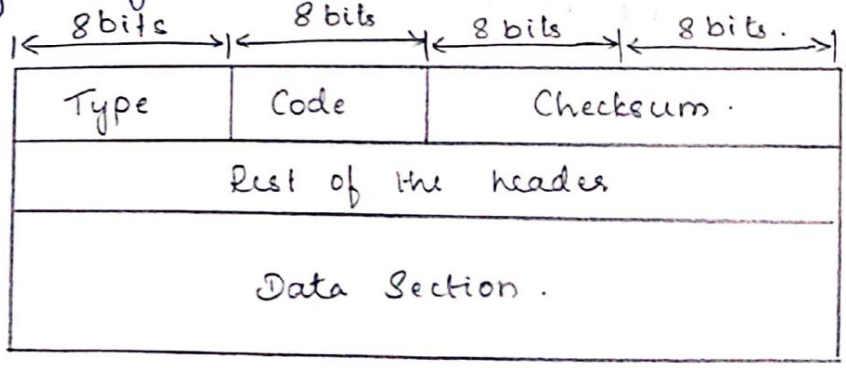
eg: Nodes can discover their neighbours.

Category	Type	Message
Errors-reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query Messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

ICMP Messages.

ICMP - Message format:

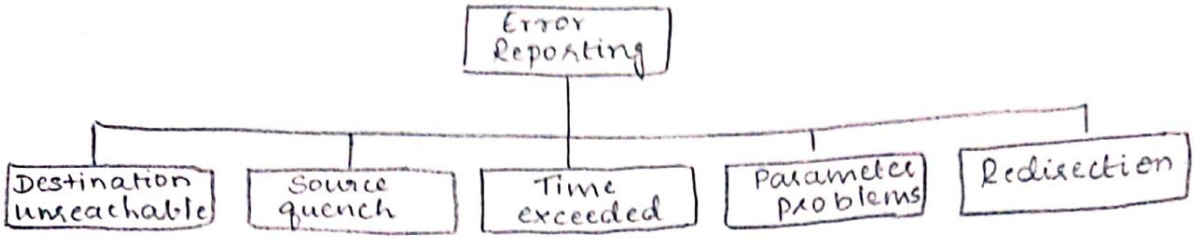
- 8 byte header
- Variable-size data section.
- The first field, ICMP type, defines the type of the msg.
- The code specifies the reason for the particular msg type.
- The checksum field.
- The rest of the header is specific for each msg type.
- The data section in error msgs carries info for finding the original packet that had the error.



General format of ICMP message

Error Reporting Messages:

- One of the main responsibilities of ICMP is to report errors.
- IP is an unreliable protocol, error checking & error control are not a concern of IP.
- ICMP always reports error msgs to the original source.
- Error correction is left to the higher-level protocols.
- Error msgs are always sent to the original source.



- Important ICMP error msgs:
  - No ICMP error msgs will be generated in response to a datagram carrying an ICMP error msg.
  - No ICMP error msg will be generated for a fragmented datagram that is not the first fragment.
  - No ICMP error msg will be generated for a datagram having a multicast address.
  - No ICMP error msg will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Destination unreachable:

- A router cannot route a datagram or a host cannot deliver a datagram then the datagram is discarded.
- The router or the host sends a destination-unreachable msg back to the source host.

Type 3	Code: 0 to 15	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

- The code field of this type specifies the reason for discarding the datagram:
  - Code 0: The network is unreachable. ~~An~~ IP datagram can carry, possibly due to hardware failure.
  - Code 1: The host is unreachable. This can also be due to hardware failure.

Code 2: The protocol is unreachable.
Code 3: The port is unreachable.
Code 4: Fragmentation is required, but the DF field of the datagram has been set.
Code 5: Source routing cannot be accomplished.
Code 6: Destination network is unknown.
Code 7: The destination host is unknown.
Code 8: The source host is isolated.
Code 9: Communication with the destination network is administratively prohibited.
Code 10: Communication with the destination host is administratively prohibited.
Code 11: The network is unreachable for the specified type of service.
Code 12: The host is unreachable for the specified type of service.
Code 13: The host is unreachable because the administrator has put a filter on it.
Code 14: The host is unreachable because the host precedence is violated.
Code 15: The host is unreachable because its precedence was cut off.

Source Quench:

- There is no flow-control & congestion control mechanism in the IP protocol.
- A source quench msg informs the source that a datagram has been discarded due to congestion in a router or the destination host.
- The source must slow down the sending of datagrams untill the congestion is relieved.

Time Exceeded:

- Time exceeded message is generated in 2 forms:

1. Whenever a router decrements a datagram with a time-to-live value to zero. It discards the datagram & sends a time-exceeded msg to the original source.

2. When the final destination does not receive all the fragments in a set time, it discards the received fragment & sends a time-exceeded msg to the original source

- In a time-exceeded msg, code 0 is used only by routers to show that the value of the time-to-live field is 0. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time.

Parameter Problem

- If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram & sends a parameter-problem message back to the source.

Code 0: There is an error or ambiguity in one of the header fields.

Code 1: The required part of an option is missing.

Echo Request and Reply:

- An echo-request msg can be sent by a host or router. An echo-reply msg is sent by the host or router that receives an echo-request msg.
- Echo-request & echo-reply msgs can be used by network managers to check the operation of the IP protocol.
- Echo-request & echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command.

Timestamp Request & Reply:

- The timestamp-request & timestamp-reply msgs to determine the round-trip time needed for an IP datagrams to travel between them.

  sending time = receive timestamp - original timestamp
  receiving time = returned time - transmit timestamp
  round-trip time = sending time + receiving time.

- Timestamp-request and timestamp-reply msg can be used to calculate the round-trip time b/w a source & a destination machine even if their clocks are not synchronized
- The timestamp-request & timestamp-reply msgs can be used to synchronize two clocks in two machines if the

exact one-way time duration is known.

Type 8: Echo request
Type 0: Echo reply

Type: 8 or 0	Code: 0	Checksum
Identifier		Sequence number
Optimal data Sent by the request msg, repeated by the reply msg		

Echo-request & echo-reply msg

Type 13: request
Type 14: reply

Type: 13 or 14	Code: 0	Checksum
Identifier		Sequence Number
Original timestamp		
Receive timestamp		
Transmit timestamp		

Timestamp-request & timestamp-reply message format

Checksum Calculation:

The sender follows these steps using one's complement arithmetic.

1. The checksum field is set to 0.
2. The sum of all the 16-bit words is calculated.
3. The sum is complemented to get the checksum.
4. The checksum is stored in the checksum field.

ICMP - Debugging tool:

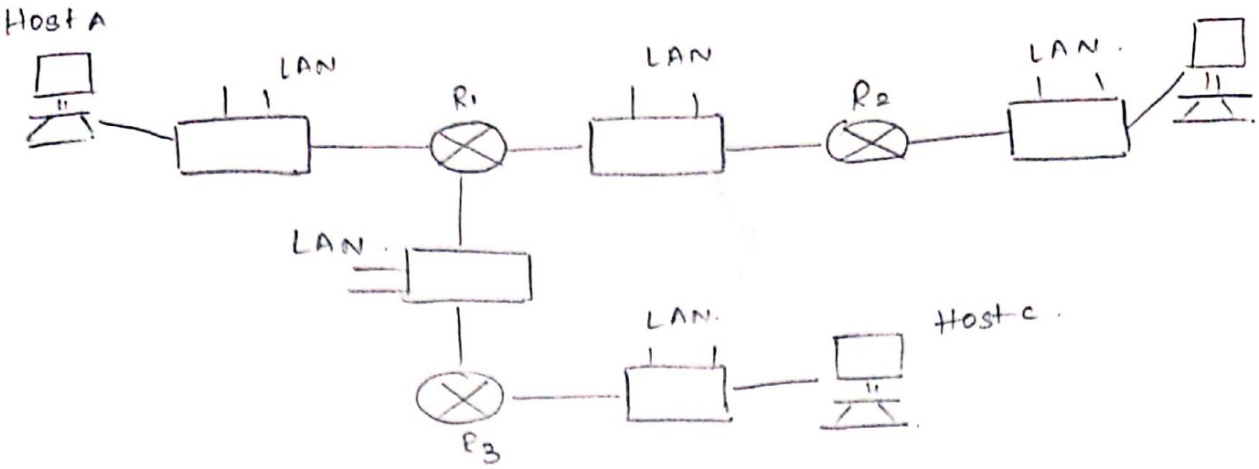
- To check whether host or router is alive & running.
- To trace the route of a packet.
- Two tools that use ICMP for debugging: ping & traceroute

Ping:

- The ping pgm to find if a host is alive & responding.
- Command: ping the ip of the host. (ping 152.18.1.3)
- The source host sends ICMP echo request msgs. (type: 8, code: 0);
- The destination, if alive, responds with ICMP echo reply msgs

Trace route:

- The traceroute pgm in UNIX & tracert in Windows.
- It is used to route the packets from source to destination.



Traceroute Program Operation.

ICMP Package.

- To handle the ICMP sending & receiving msgs
- ICMP package is made of 2 modules.
  - L> I/P module
  - L> O/P module.

I/P module pseudo code:

```
ICMP_Input_module (ICMP_Packet)
{  if (the type is a request)
   {
      Create a reply
      Send the reply
   }
   If (the type defines a redirection)
   {
      Modify the routing table
   }
   if (the type defines other error messages)
      {  inform the appropriate source protocol
      }
   return
}
```

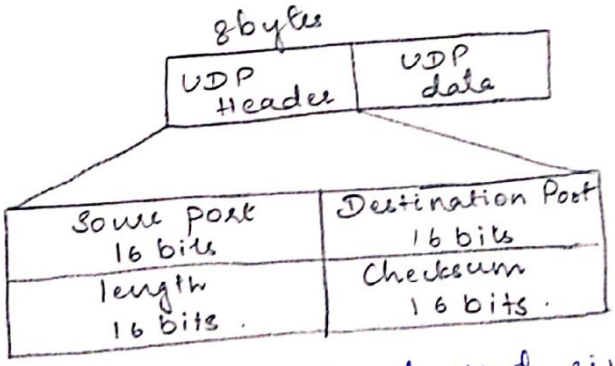
O/P module pseudo code

```
ICMP_Output_module (demand)
{  if (the demand defines an error msg)
```

```
{
  if (demand comes from IP AND is forbidden)
  { return
  }
  if (demand is a valid redirection msg)
  { return
  }
}
create an error msg
{ if (demand defines a request)
  { create a request msg
  }
  Send the msg
  Return
}
```

UDP

- User Datagram Protocol (UDP) is a Transport layer Protocol.
- UDP is a part of Internet Protocol suite, referred as UDP/IP suite.
- Unlike TCP, it is unreliable and connectionless protocol. So there is no need to establish connection prior to data transfer.
- Though TCP is a dominant transport layer protocol used with most of internet services; provides assured delivery, reliability & much more.
- UDP is used in realtime services like computer gaming.



- UDP header is 8 bytes fixed and simple header, while for TCP it may vary from 20 bytes to 60 bytes.
- first 8 bytes contains all necessary header information & remaining part consist of data.
- UDP port no. fields are each 16 bits long, ∴ range for port numbers defined from 0 to 65535; port no 0 is reserved.

1. Source port: is a byte long field used to identify port number of source.
2. Destination Port: a byte long field, used to identify the port of destined packet.
3. Length: length of UDP including headers & the data. 16 bit field.
4. Checksum: 2 bytes long field. It is the 16-bit one's complement of the one's complement sum of the UDP header, pseudo header of information from the IP header & the data, padded with zero octets at the end to make a multiple of 2 octets.

UDP Services:

- Process to process communication
- Connectionless services
- Error control
- Checksum
- Congestion control
- Encapsulation & decapsulation

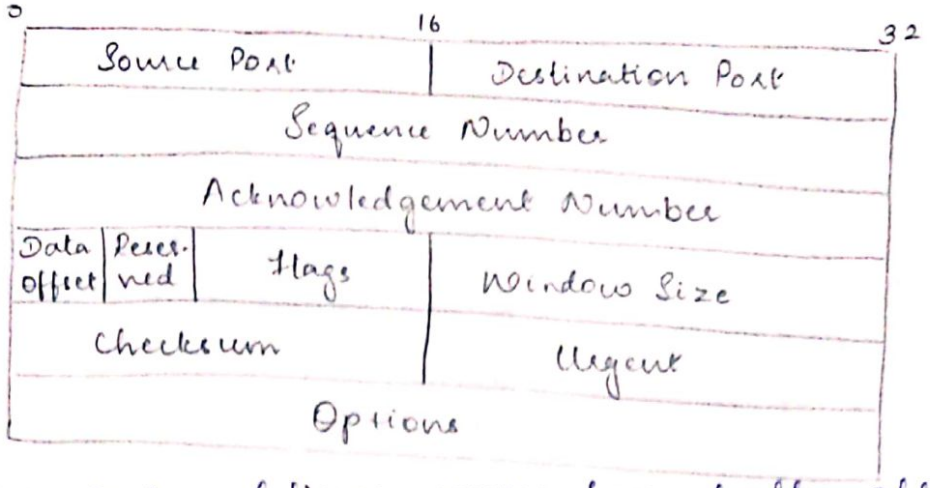
Applications:

- Used for simple request response communication when size of data is less hence there is lesser concern about flow & error control.
  It is suitable protocol for multicasting as UDP support packet switching.

TCP Header:

- The Transmission Control Protocol (TCP) is one of the most important protocols of internet protocol suite.
- TCP is a reliable protocol.
- It ensures that the data reaches intended destination in the same order it was sent.
- TCP is connection oriented.
- TCP provides error-checking and recovery mechanism.
- TCP provides end-to-end communication.
- TCP provides flow control & quality of service.
- TCP operates in Client/Server point-to-point mode.
- TCP provides full duplex servers.

TCP Header:



- Source port: defines source port of the application process on the sending device.
- Destination port: identifies destination port of the application process on the receiving device.
- Sequence no: seq. no. of data bytes of a segment in a session.
- Ack no: When ACK flag is set, this no. contains the next sequence no. of the data byte expected & works as ack of the previous data received.
- Data offset: This field implies both, the size of TCP header & the offset of data in current packet in the whole TCP segment.
- Reserved: Reserved for future use.
- Flags: 1 bit each.
- Window Size: This field is used for flow control b/w 2 stations & indicates the amount of buffer the receiver has allocated for a segment.
- Checksum: This field contains the checksum of Header, Data and Pseudo headers.
- Urgent Pointer: It points to the urgent data byte if URG flag is set to 1.
- Options: It facilitates additional options which are not covered by the regular header.

Addressing:

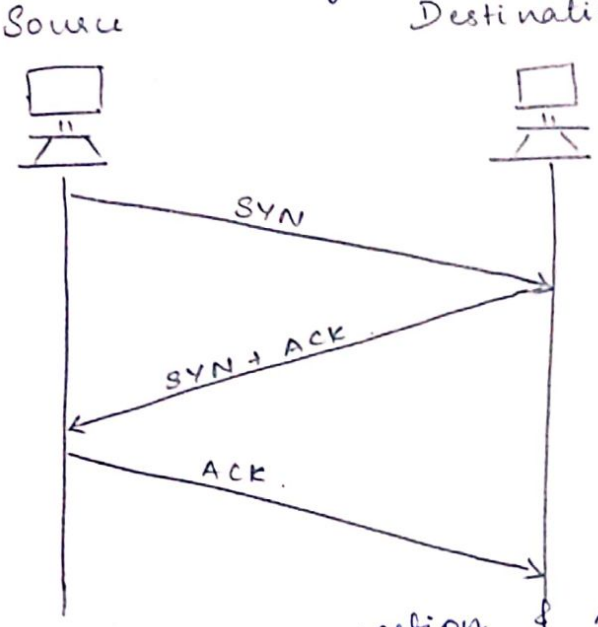
- TCP communication b/w 2 remote hosts is done by means

of port numbers. Port numbers can range from 0-65535 which are divided as:

- System Ports (0-1023)
- User Ports (1024-49151)
- Private / Dynamic Ports (49152-65535).

Connection Mgmt:

- TCP communication works in Server/Client model.
- The client initiates the connection & the server either accepts or rejects it.
- Three-way handshaking is used for connection mgmt.



- Client initiates the connection & sends the segment with a seq. no.
- Server acknowledges it back with its own seq. no. & ACK of client's seq. no.
- Client after receiving ACK of its segment sends an acknowledgement of server's response.
- Either of server & client can send TCP segment with FIN flag set to 1.
- When the receiving end responds it back by ACK FIN, that direction of TCP communication is closed & connection is released.

Error Control & Flow Control

- TCP uses port no. to know what application process it needs to handover the data segment.
- Along with that, it uses seq. no. to synchronise itself with the remote host.

- All data segments are sent & received by the seqno.
- The sender knows which last data segment was received. by the receiver when it gets ACK.
- The Receiver knows about the last segment sent by the sender by referring to the seq. no. of recently received packet
- If the seq. no of a segment recently received does not match with the seq. no. the receiver was expecting, then it is discared with NACK is sent back.

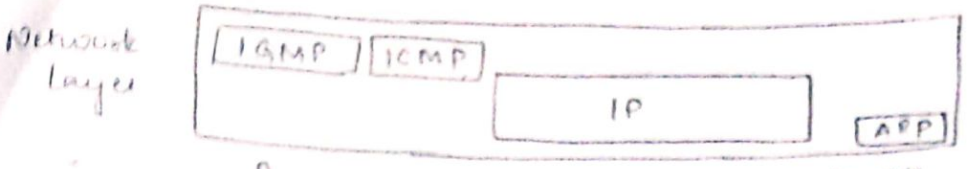
Congestion Control:
- When large amount of data is fed to system which is not capable of handling it, congestion occurs.
- TCP controls congestion by means of Window mechanism.
- TCP sets a window size telling the other end how much data segment to send.
- TCP may use 3 algorithms for congestion control:
  - L> Additive increase, Multiplicative Decrease.
  - L> Slow start
  - L> Timeout Reack.

Multicasting:
- One source & one group of destinations.
- Relationship b/w source & destination: One to many
- Source address: Unicast address
- Destination address: Group of one/more destination networks.

Unicasting:
- One source & one destination network.
- Relationship b/w source & destination: One to one.
- Each router in the datagram path forwards packets to only one interface.

IGMP: Internet Group Management Protocol.
- Multicast Communication: Msg sent by senders to receipients of same group.
- Multicast routers know list of groups & minimum one loyal member related to each interface.
- Information about members to be shared b/w multicast route
- Information collected at 2 levels:

- locally (collected by IGMP)
- Globally (propagated to other routers).



Position of IGMP in network layer.

- IGMP collects & interprets information about group members in a network locally.
- IGMP manages group membership.
  - provides info to the multicast routers about membership status of routers connected to a network.
- Versions of IGMP : 1, 2 & 3.
- Version 1 & 2 provides any source multicast (ASM)
- Version 3 provides source specific multicast (SSM).
- IGMP v3 msgs:
  - L> 2 types of msgs
    1) Membership Query msg.
       - L> General
       - L> Group specific
       - L> Group & source specific.
    2) Membership Report Message.

Routing protocols:

- Unicast routing protocols use graphs while multicast routing protocols use trees, i.e; spanning tree to avoid loops.
- The optimal tree is called shortest path spanning tree.
- DVMRP - Distance Vector Multicast Routing Protocol.
- MOSPF - Multicast Open Shortest Path First.
- CBT - Core Based Tree.
- PIM - Protocol independent Multicast
  - L> PIM Dense Mode: This mode uses source-based trees. It is used in dense environment such as LAN.
  - L> PIM Sparse Mode: This mode uses shared trees. It is used in sparse environment such as WAN.

Routing Algorithms:

Flooding: is simplest method packet forwarding.

- When a packet is received, the routers send it to all the

interfaces except the one on which it was received.
- This creates too much burden on the network & lots of duplicate packets wandering in the network.
- TTL can be used to avoid infinite looping of packets.

SCTP (Stream Control Transmission Protocol)
- Reliable, Message-oriented general purpose transport layer protocol.
- Capable of handling multimedia & stream traffic.
- Designed for Internet applications.
- Lies b/w application & n/w layer.
- Serves as a middlemen b/w application pgms & network operations.
- Combines best features of UDP & TCP.
- SCTP preserves msg boundaries.
- Detects lost data, duplicate data & out-of-order data.
- Congestion control & flow control mechanisms available in SCTP.

Characteristics of SCTP:
- Confirmed Transmission
- Data fragmentation
- Sequenced delivery
- Binding
- Fault tolerance at Network level.

Key features of SCTP:
- No head-of-line blocking
- Msg-based data transfer
- Multihoming
- Protection against connection flooding.