Network Layers Part - 1

Prep Smart. Stay Safe. go Gradeup

gradeup.co

Network Layer Part-1

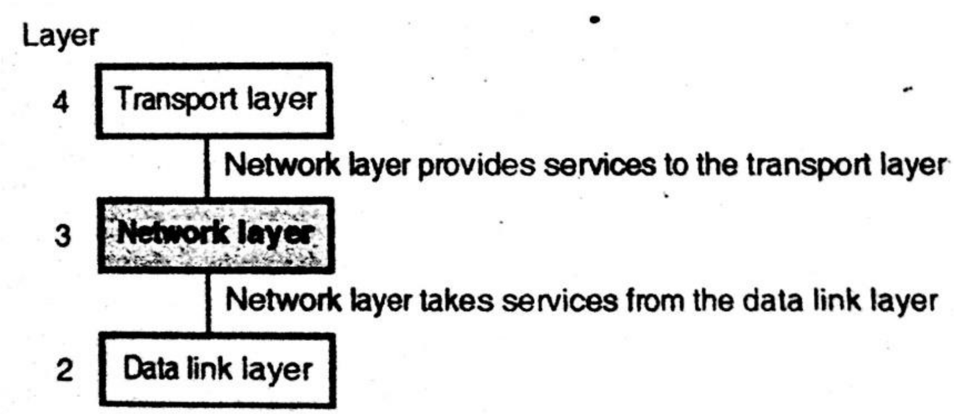
Content :

Network Layer

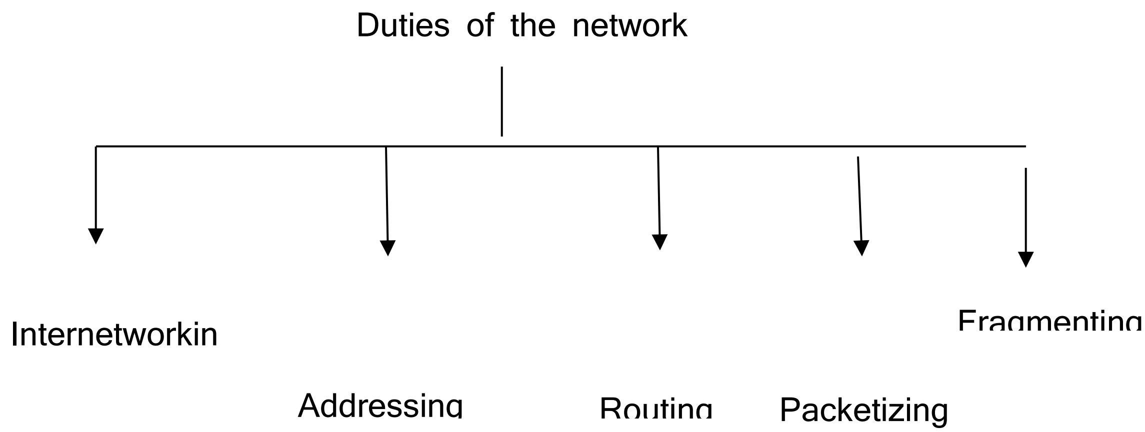
- The network layer is responsible for carrying the packet from the source all the way to destination . In short it is responsible for host-to-host delivery
- The network layer has a higher responsibility than the data link layer because the DLL is only supposed to more the frames from one end of the wire to the other end
- Thus network layer is the lower layer that deals with end to end transmission

Position of Network layer :

- Diagram shows the position of network layer in the OSI model .



Network Layer Duties :



1. **Internetworking :**

   It is the main duty of network layer . It provide the logical connection between different types of networks

2. **Addressing :**
   1. Addressing is necessary to identify each device on the internet uniquely . This is similar to the telephone system
   2. The address used in the network layer should uniquely and universally define the connection of a computer

3. **Routing :**
   a. In a network , there are multiple roots available from source to destination and one of them is to be chosen
   b. The network layer decides the root to be taken . This is called as routing and it depends on various criterions

4. **Packetizing :**
   a. As discussed earlier , the networks layer encapsulates the packets received from upper layer protocol and makes new packets
   b. This is packetizing . It is done by a network layer protocol known as IP (internetworking protocol)

5. **Fragmenting :**

   The datagram can travel through different network . Each router encapsulates the IP datagram from the received frame, then the datagram is processed and encapsulated in another frame.

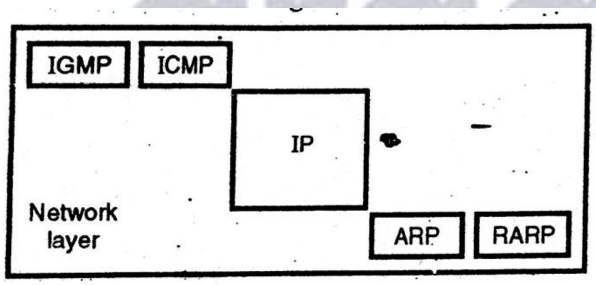
Other Issues :

The other issues which are not directly related to the duties of networks layer but need to be discussed are :

1. Address resolution
2. Multicasting
3. Routing Protocol

Various Network Layer Protocol :

- In the internet model , or the TCP/IP suite, there are five main network layer protocol: ARP , RARP , IP , ICMP and IGMP as shown below :



- The main protocol in this layer is Internet Protocol(IP). It is responsible for host to host delivery of datagrams from a source to destination. But IP needs service of other protocols.
- IP needs a protocol called ARP in order to find the MAC(physical) address to next hop.
- IP needs the services of ICMP during the delivery of the datagram packets to handle unusual situations such as occurrence of an error

- IP is basically designed for unicast delivery . But the multimedia and some new applications in the internet need multi case delivery.
- So for multicasting , IP has the services of another protocol called IGMP
- IPv4 is the current version of IP whereas IPv6 is the latest version of IP .

ARP(Address Resolution Protocol)

- An internet consists of various types of networks and the connecting device like routers
- A packet start from the source host , passes through many physical networks and finally reaches the destination host
- At the networks level , the hosts and routers and recognized by their IP addresses.

IP Address

- An IP address is an inter network address. It is a universally unique address
- Every protocol involved in internetwork requires IP addresses

MAC Address

- The packets from source to destination posts pass through physical networks. At the physical level IP address is not useful but the routers and hosts are recognized by their MAC addresses.
- A MAC addresses is a local address . It is unique locally but it is not universally
- The IP and MAC address are two different identifiers and both of them are needed , because a physical networks can have two different protocols at the networks layer at the same time.
- In the same way a packet may pass through different physical networks

- So to deliver a packet to a host or a router , we require two levels of addressing namely IP addressing and MAC addressing
- Importantly we should be able to map the IP address into a corresponding MAC address.

MAPPING OF IP ADDRESS INTO A MAC ADDRESS:

- We have seen the of mapping an IP address into a MAC address
- Such a mapping can be of two types :
  1. Static mapping   2. Dynamic mapping

1. **Static Mapping :**
    - In static mapping a table is created and stored in each machine . This table associates an IP address with MAC addresses
    - If a machine knows the IP address of another machine hen it can search for the corresponding MAC address in its table.
    - The limitation of static mapping(SM) is that the MAC addresses can change. To implement static mapping static mapping table needs to be updated periodically
2. **Dynamic Mapping :**
    - In dynamic mapping technique a protocol is used for finding to other address when one type of address is known
    - Two protocols are designed to perform the dynamic mapping. They are:
      1. Address Resolution Protocol(ARP)
      2. Reserve Address Resolution Protocol(RARP)

    - The ARP maps an IP address to MAC address whereas the RARP maps a MAC address to an IP address

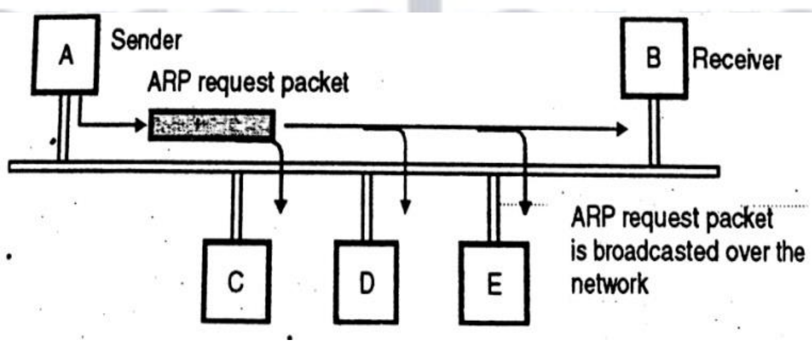
ARP :

ARP is used for associating an IP address to its MAC address. For a LAN , each device has its own physical or station address as identification. This address is imprinted on the NIC(Network Interface Card)

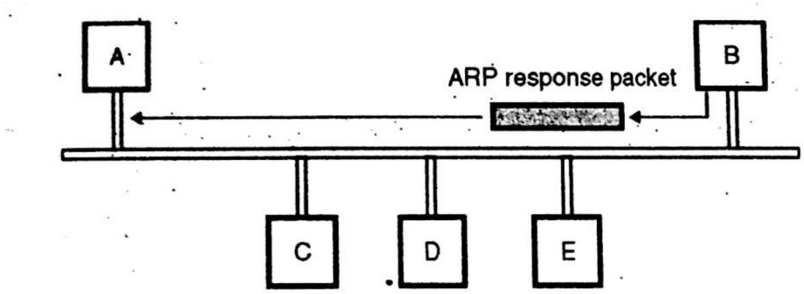
How to find the MAC Address?

When a router or a host needs find the MAC address of another host or network the sequence of the events taking place is as follows :

- The router or host A wants to find the MAC address of some other router , sends an ARP request packet. This packet consists of MAC and IP addresses of the sender A and the IP address of the receiver(B)
- This request packet is broadcasted over the networks as shown below :



- Every router and host on the network receives and processes the ARP request packet but only intended receiver(B) recognizes its IP address in the request packet and sends back an ARP response packet.
- The ARP response packet contains the physical and IP addresses of the receiver (B). This packet is delivered only to A (unicast) using A's physical address in the ARP request packet. As shown below :



ARP packet format :

Hardware Type(16 BITS)		Protocol Type(16 BITS)
Hardware Length	Protocol Length	Operation Request 1, Reply 2
Sender hardware address		
Sender protocol		
Target hardware address		
Target protocol address		

Operation Of ARP on Internet :

- The services of ARP can be used to under the following working conditions when it is being operated on internet :
  1. Sender is a host and wants to send a packet to another host on the same net
  2. Sender is a host and wants to send a packet to another host on another network
  3. The sender is a route which has received a datagram destined for a host on another networks
  4. Sender is a router that has received a datagram destined for a host in the same network.
- Now let us see how ARP works on the internet

Operation :

1. The sender (host or router) knows the IP address of the target.
2. IP order ARP to create an ARP request message. The request packetconsists of senders physical and IP address plus the IP address of the target
3. This ARP request packet Is packet is sent to the data link layer. Here it is encapsulated in a frame
4. Every route or host receives this frame because it is broadcast . All the machines except the target drop this packet
5. The target machine replies back with an ARP reply packet which contains the target's physical address. This reply is unicast
6. The sender receives the reply packet . which is now knows the physical address of the target
7. The IP address carrying data for the target machine is encapsulated in a frame and the frame is unicast to the destination.

Reverse Address Resolution Protocol (RARP) :

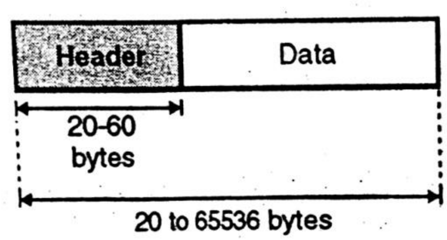
- RARP (reverse address resolution protocol) is part of the TCP/IP protocol suite . It allows a computer , particularly a dislikes workstation , to obtain an IP address from a server. When a diskless TCP/IP workstation is booted on a networks , its broadcasts a RARP request packet on the local network
- This address packet is broadcast on the networks for all to receiver because the workstation does not know the IP address of the server that can supply it with an address
- It incudes its own physical network address (the MAC address) in the request so the server will know where to return a reply
- The server that receives the request looks in a table and matches the MAC address with IP address , and then returns the IP address to the diskless workstation. See also "ARP(Address resolution Protocol)

Internet Protocol (IP) :

- This is host to host networks layer delivery protocol designed for the internet
- Internet protocol(IP) is a connectionless datagram protocol with no guarantee of reliability
- IP is an unreliable protocol because it does not provide any error control or flow control
- IP can only detect the error and discard the packet if it is corrupted
- If it is to be made more reliable , then it must be paired with a reliable protocol such as TCP at the transport layer
- Each Internet protocol(IP) datagram is handled independently and each one can follow a different route to the destination
- So there is a possibility of receiving out order packets at the destination. Some packets may even be lost or corrupted
- IP replies on higher level protocol to take care of all these problems.

Datagram :

- Packets in internet protocol(IP) layer are called datagram . Below diagram shows the datagram format
- A datagram is variable length packet which have two parts i.e. the header and data
- The length of header is 20 bytes to 60 bytes . It contains the information essential for delivery and routing
- The other part of the datagram is the data filed which is of variable length



Structure of IP frame Header :

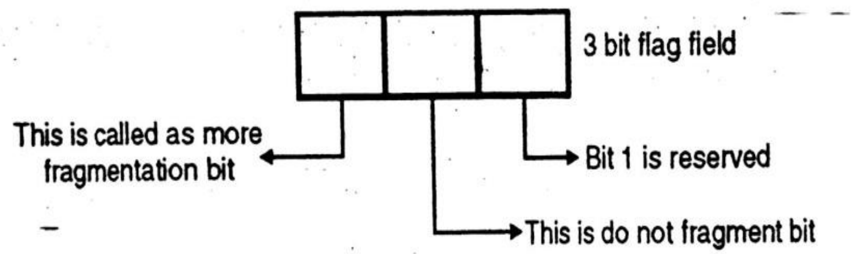
The IP frame Header contains control information and routing information associated with datagram delivery . The IP header structure is shown below :

4	8	16		32 bits
VER	HLEN	D.S. type of service	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset (13 bits)
Time to live		Protocol	Header checksum (16 bits)	
Source IP address				
Destination IP address				
Option + Padding				

Fields in the IP header are as follows :

1. **VER(version) :**Filed defines the version of IP. The current version of IP is IPV4 and the latest version of IP is IPV6 . It is a four bit long filed
2. **HLEN(Header length) :**Filed defines the length of the datagram header in 4-byte word. Value must be multiplied by 4 to give the length in bytes
3. **Different Service(DS) :** This field defines the class of the datagram for quality of service purpose. Network may offer service precedence , meaning that they accept traffic only above certain precedence at time of high load. There is three way trade off between low delay , high reliability and through put .
4. **Total Length :** This filed defines the total length of the IP datagram. The total length includes the length of header as well as the data field :
    - The field length of this field is 16bits so that the total length of the IP datagram is restricted to (2^{16} -1) = 65535 bytes of which 20 to 60 bytes are the header and the remaining are data.
    - This field allows the length of a datagram to be upon 65,535 bytes, although such long datagram are impractical for the most hosts and networks
    - It is recommended that the hosts send datagram larger than 576 bytes only if the destination is prepared to accept larger datagram
    - All hosts must be prepared to accept datagram of upto 576 bytes , regardless of whether they arrive whole or in fragments
5. **Identification , flag and offset :**
    - **Identification :**Field identifies the datagram originating from the source host. When a datagram is fragmented , the value in the identification filed is copied into all fragments.

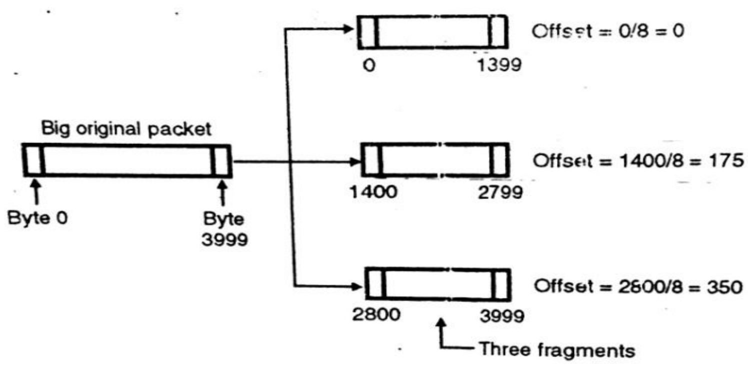
- **Flag:** This is three bit filed. The 3 bits are shown below :



- The first bit is reserved and it should be 0
- The second bit is known as " Do Not Fragment" bit. If this bit is 1 then machine should not fragment the datagram
- But if the value off this bit is 0 then the machine should fragment the datagram if and only if necessary
- The third bit is Known as " More Fragment Bit" . If it is 1 it means that the datagram is not the last fragment but if its value is 0 it shows that this is the last or the only fragment

Fragmentation Offset:

- This is a 12 bit filed which shows the relative position of this fragment with respect to the whole datagram
- It is the offset of the data in the original datagram measured in units of 0 bytes
- Below diagram is show to understand this
- The original IP packet(datagram) contains 4000 bytes numbered from 0 to 3999 . It is fragmented into three fragments.



- The first fragment contains 1400 bytes numbered from 0 to 1399 . The offset for this fragment is 0/8 which is equal to 0 . Similarly the offset for the other two fragments are 1400/8 =175 and 2800/8 =350 respectively as shown above
- Offset is measured in units of 8 bytes . because the length of offset filed is 12 bits
- So the fragments should be of size such that first byte number is divisible by 8

6. Time to live :

This is an 8 bit long field which control the maximum number of routes visited by the datagram

7. Protocol:

- The field defines the higher-level protocol which uses the services of the IP layer . An IP datagram can encapsulate data from various higher level protocol such as TCP , UDP , ICMP and IGMP
- The protocol field specifies the final destination protocol to which the IP datagram should be delivered
- Since IP multiplexes and de-multiplexes data from different higher level protocols , the value of protocol field helps in de-multiplexing at the final destination

8. Header checksum :

A checksum in IP packets covers on the header only . Since some header fields change , this field is recomputed and verified at each point that the internet header is processed

9. **Source address :** This field is used for defining the IP address of the source
10. **Destination address :** This field is used for defining the IP address of the destination

11. Option :

- Options are not required for every datagram. The are used for networks testing and debugging
- IP provides several optional features , allowing a packet's sender to set requirements on the path it takes through the network (source networking) , trace the route a packet takes (record route) and label packets with security features .

SERVICES PROVIDED

IP provides following services:

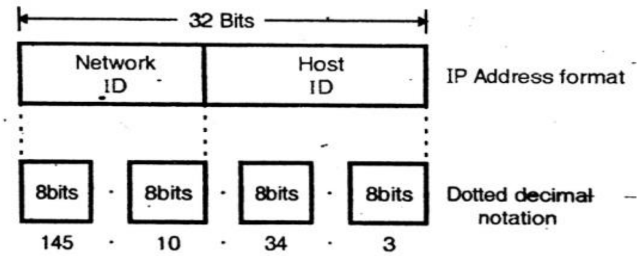
- **Addressing:** IP headers contain 32-bit addresses which identify the sending and receiving hosts ,these addresses are used by intermediate routers to select a path through the network for the packet.
- **Fragmentation:** IP packets may be split, or fragmented, into smaller packets. This permits a large packet to travel across network whichcan only handle smaller packets. IP fragments and reassembles packets transparently.
- **Packet timeout:** Each IP packet contains a Time to Live (TTL) field, which is decremented every time a router handles the packet. If Time To Live(TTL) reaches zero, the packet is discarded, and preventing packets from running in circles forever and flooding a network.
- **Type of Service:** IP supports traffic prioritization by allowing packets to be labeled with an abstract type of service.

IP ADDRESSES

- As already stated every host and router on the internet has a unique IP address.
- All the IP addresses are 32 bit long and they are used in the source address and destination address fields of the IP header.
- Below figures shows the IP addresses format. It consists of two fields called Network ID and Host ID.
- The IP numbers (addresses) for the hosts are assigned by the networks administrator. For a public networks on the internet, we have to obtain a network number assigned by the network information center.
- An IP address consists of two parts. The first part of the address called the network number, identifies a network on the internet; the remainder, called host ID, identifies and individual host on that network.

IP ADDRESSES FORMAT

- The 32 bit IP addresses is grouped into groups of eight bits, separated by dots. Each 8 bit group is then converted into its equivalent binary number as shown in below figure.



- Thus each octet (8 bit) can take value from 0 to 225. The IP in the dotted decimal notation can range from 0.0.0.0 to 255.255.255.255.
- For example the IP address of 1001 0001.00001010 00100010 00000011 is denoted in the dotted decimal form as 145.10.34.3.