# Chapter 4 – Internet and Higher Layer Protocols

* Router examines all headers of the datagrams passing through it.
* Network Layer Functions –
  + Forwarding: Move packets from routers’ input to appropriate router’s output
    - Decentralized Switching: It views headers to lookup for output ports using forwarding table in input ports.
    - Generalized Switching
  + Routing: Determine the route taken from source to destination
* If it forwards only on destination IP address, then it is destination-based forwarding.
* Input buffer Overflow – It happens due Queuing delay and loss.
* Datagram packets can be lost due to congestion, lack of buffers
* Scheduling – choose what packets to send
  + FIFO – Send In order of arrival
  + Priority – send highest priority queued packet first.
* Fragmentation –
  + Many Links have MTU Maximum Transfer size hence, the datagrams are divided in to sub datagrams known as fragments within the network.
  + These datagrams are only reassembled at the Destination.
  + The order of the fragments is identified by the IP Header bits in each fragment.
* IP Addressing –
  + IP is a 32-bit identifier for host/router interfaces, where interfaces are a connection between the hosts/routers source and the destinations.
  + There can be multiple interfaces for same routers, whereas a host can have only one/ two interfaces like Wired Ethernet or Wireless 802.11.a/n
* Subnets –
  + IP Address consists of 2 parts: Subnet Part and the Host Part.
  + Subnet – It is a device interfaces with same part of the IP Address.
  + They do not require a router to physically communicate with each other.
  + To determine if there are subnets or no detach the interfaces from the host router and create an isolated network. This isolated network is called as Subnet.
* Classless Inter Domain Routing (CIDR) –
  + If a.b.c.d/x is an IP Address then, x is the number of bits in the subnet portion of the address of arbitrary length.
  + Therefore, in an Address as 200.23.16.0/23  
    **11011000 00010111 0001000** 0 00000000 (Bold is Subnet and other is host)
* Dynamic Host Configuration Protocol (DHCP) –   
   In this process, the system receives an IP Address dynamically from the server.
  + If a process is entered it receives an address for a certain period of time.  
    It allows the system to increase its reusability by renewing the lease of the address it is connected on.
  + It works in a certain way, where the host broadcasts a “DHCP Discover” message.  
    The DHCP Server responds with the “DHCP OFFER” message. Then to which the host requests an IP Address as “DHCP Request” and the Server provides an address with the acknowledgement with a “DHCP ACK” message.
* Network Address Translation:
  + Local Network just uses a single IP Address for the outer world. It isn’t required to have a range of IP Address from the ISPs.
  + NAT can change the addresses of the devices without notifying the outside world. Hence, the devices of the local network cannot be explicitly addressed by the outer network less chance of any vulnerability.
    - Every outgoing datagrams of the n/w Source - Local (IP Addr, Port No #) are replaced by the NATs (IP Addr, Port no #)
    - Every incoming datagrams of the n/w Source - NATs (IP Addr, Port no #) are replaced by the Local (IP Addr, Port No #) from the NAT Table
    - Every NAT has a 16-bit port no # field, which can have up to 60000 connections simultaneously for a single LAN-side IP Address.