Unit-III

Network layer

→ Network layer is the third layer in the OSI mo
its main function is to transfer packets from source to destination. it is involved both at the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsu-ates it in a datagram and then deliver the packet to the data link layer so that it can furthe be sent to the receiver. At the destination, the datagram is decapsulated the packet is extracted and delivered to the corresponding transport layer

Functionalities:-

Device which work on nlw layer mainly focus on routing.

→ Addressing devices and nlws
→ populating routing tables or static routes
→ Queuing incoming and outgoing data and then forwarding them according to quality of service constraints set for those packets
→ internetworking blw two different subnets.
→ Delivering packets to destination with best efforts.
→ provides connection oriented and connection less mechanism.

Features:-

→ Quality of service management
→ load balancing and link management
→ ~~too~~ security
→ interrelation of different protocols and subnet with different scheme
→ Different logical nlw design over the physical nlw design.

Address mapping:- An internet is made of combina-tion of physical nlws connected by internetwork-ing devices such as routers.

the hosts and routers are recognized at the nlw level by their logical (IP) addresses.

Forwarding:-

→ Forwarding means to place the packet in its route to its destination

→ Forwarding requires a host or a router to have a routing table. when a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

→ However, this simple solution is impossible today in an internetwork such as the internet because the no. of entries needed in the routing table would make table lookups inefficient.

we have

→ Forwarding techniques

→ Forwarding process

→ Routing table

1) Forwarding techniques:-

There are several techniques which can make the size of routing table manageable and also handle issues like security. they are

a) Next-Hop method versus Route method.

b) network-specific method versus Host-specific method

c) Default method.

a) Next-Hop method versus Route method:-

→ one technique to reduce the contents of a routing table is called next-Hop method.

→ In this technique, the routing table holds only the address of the next hop instead of information about the complete route. The entries of a routing table must be consistent with one another

a) Routing tables based on route

Destination	Route
Host B	R1, R2, Host B

Routing table for Host A

Destination	Route
Host B	R2, Host B

Routing table for R1

Destination	Route
Host B	Host B

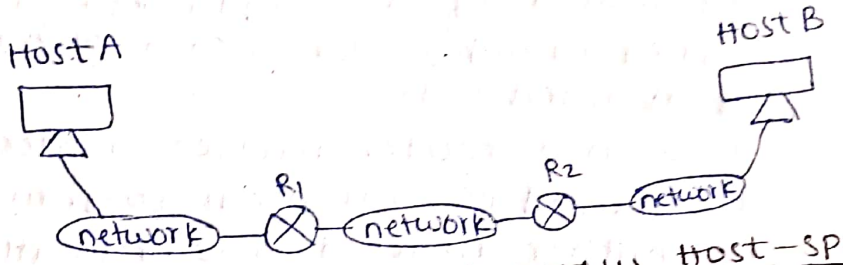
Routing table for R2

b) Routing tables based on next hop

Destination	nexthop
Host B	R1

Destination	nexthop
Host B	R2

Destination	Nexthop
Host B	—



b) network-specific method versus host-specific method.

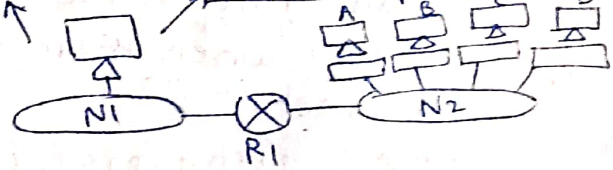
→ A second technique to reduce the routing table and simplify the searching process is called the nlw-specific method.

→ Here, instead of having an entry for every destination host connected to the same physical nlw. we have only one entry that defines the address of the destination nlw itself.

→ Host-specific routing is used for purposes such as checking the route or providing security measu -res

Destination	Nexthop
A	R1
B	R1
C	R1
D	R1

Destination	Nexthop
N2	R1



c) Default method :-

→ Another technique to simplify routing is called the default method.

→ The Host A is connected to nlw 2. However, for the rest of the internet, router R_2 is used.

→ So instead of listing all nlws in the entire internet, host A can just have one entry called Default.

Forwarding process :-

→ Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces.

→ When a router receives a packet from one of its attached nlws, it needs to forward the packet to another attached nlw, or to attached nlw's

Routing :-

→ These are two other services offered by the nlw layer In a nlw, there are a number of routes available from source to destination.

→ The nlw layer has some strategies which find out the best possible route. This process is refered to as routing.

→ There are a number of routing protocols which are used in this process and they should be run to the help the routers, coordinate with each other and help in establishing communication throughout the nlw.

Unicast routing protocols :-

→ A routing table can be either static or dynamic

→ A static table is one with manual entries and a dynamic table is one that is updated, automa-tically when there is a change somewhere in the internet.

→ A routing protocol is a combination of rules and procedures that lets routers in the

internet in the form each other of changes.

~~Distance vector~~

Intra domain Routing :-

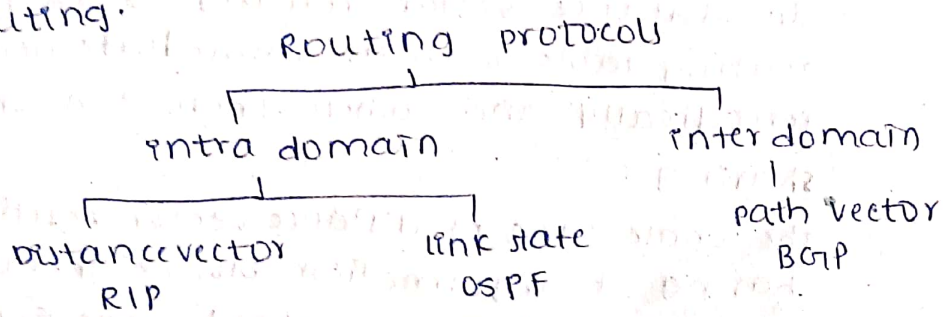
As name suggests is a protocol in which routing algorithm works only within the domain.

→ Routing is less complex and lesser interdependent as compared to that of inter domain routing.

Inter domain routing :-

As name suggests is the protocol in which routing algorithm works within and between domains.

→ Inter domain routing is more complex and more dependent as compared to that of intra domain routing.

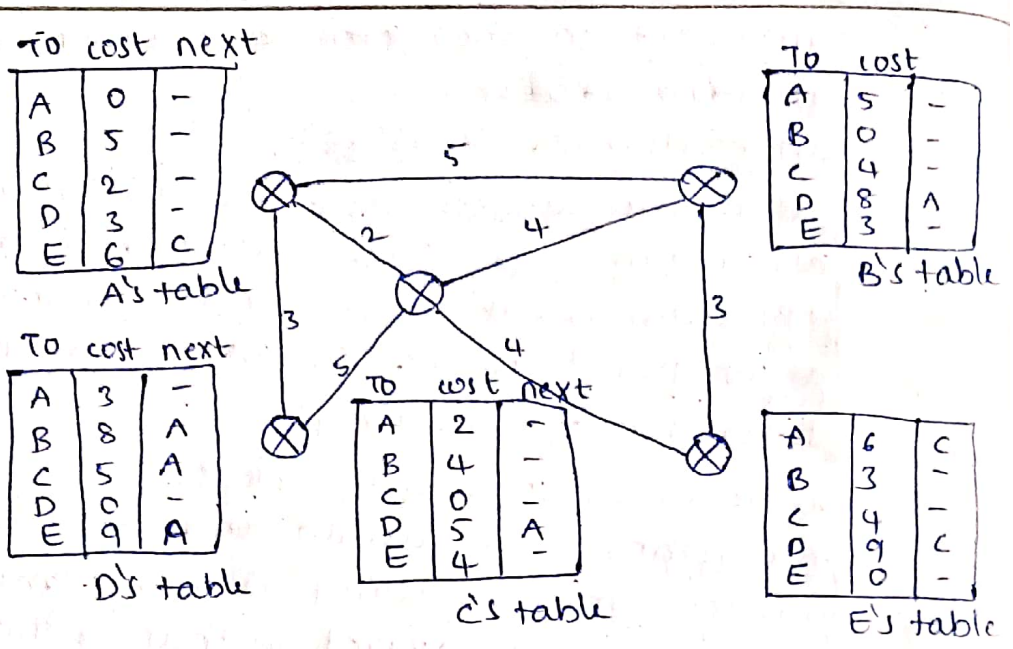


Distance vector routing :-

In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node.

Initialization :-

Each node can know only the distance between itself and its immediate neighbours, those directly connected to it. We assume that each node can send a message to the immediate neighbours and find the distance between itself and these neighbors. Below fig shows the initial tables for each node. The distance for any entry that is not a neighbour is marked as infinite (unreachable)



In distance vector routing, each node shares its routing table with its immediate neighbours periodically and when there is a change

sharing:-

The whole idea of distance vector routing is the sharing of information blw neighbours. Although node A does not know about node E, node C does. so if node C shares its routing table with A, node A can also know how to reach node E. on the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C and node C are also knows how to reach node D. In other words, nodes A and C, as immediate neighbours can improve their routing tables, if they help each other.

updating:-

when a node receives a two-column table from a neighbor, it needs to update its routing table. updating takes three steps:-

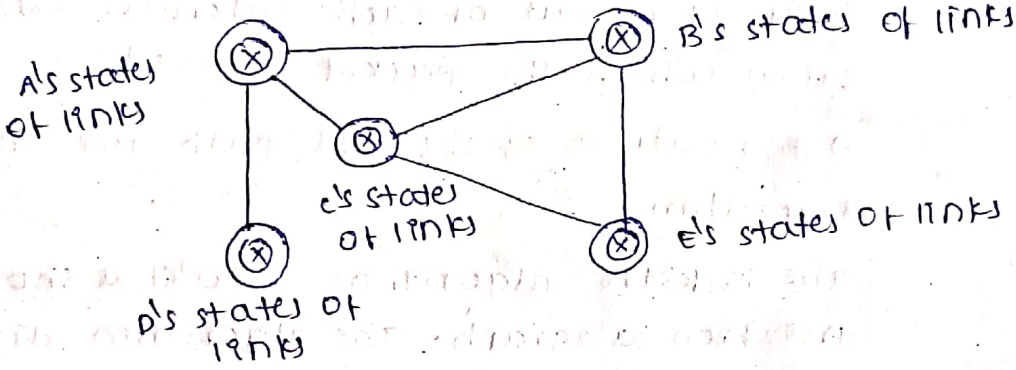
1) The receiving node needs to add the cost blw itself and the sending node to each value in the second colum (x+y)

2) If the receiving node uses information from any row. The sending node is the next node in the route.

3) The receiving node needs to compare each row of its old table with the corresponding row of the modified version of received table.

link state routing :-

The basic concept of link-state routing is that every node constructs a map of connectivity to the nlw, in the form of graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the nlw.



Building routing tables:-

1) creation of link state packet (LSP):-

A link state packet can carry a large amount of information. For the moment, we assume that it carries a minimum amount of data, the node identity, the list of links, a sequence number and age. The first two, node identity and the list of links are needed to make the topology. The third sequence number, facilitates flooding and distinguishes new LSPs from old ones. The 4th, age, prevents old LSPs from remaining in the domain for a long time.

LSP's are generated on two occassion

1) when there is a change in the topology of domain.

2) on a periodic basis :- The period in this case is much longer compared to distance vector.

2) Flooding of LSPs :-

After a node has prepared on LSP, it must be disseminated to all other nodes, not only to its neighbours. The process is called flooding and based on following

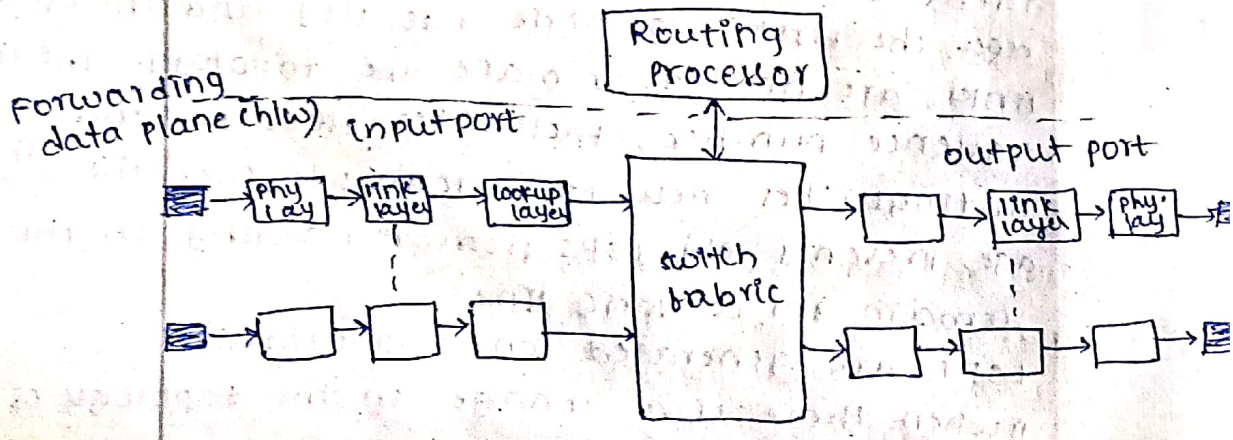
→ The creading node sends a copy of the LSP out of each interface.

→ A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has it discards the LSP, if it is newer, it sends a copy of it out of each interface except the one from which the packet arrived.

3) Formation of shortest path tree: Dijkstra Algorithm :-

The Dijkstra algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets :- tentative and permanent it finds the neighbours of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.

** Router Architecture :-

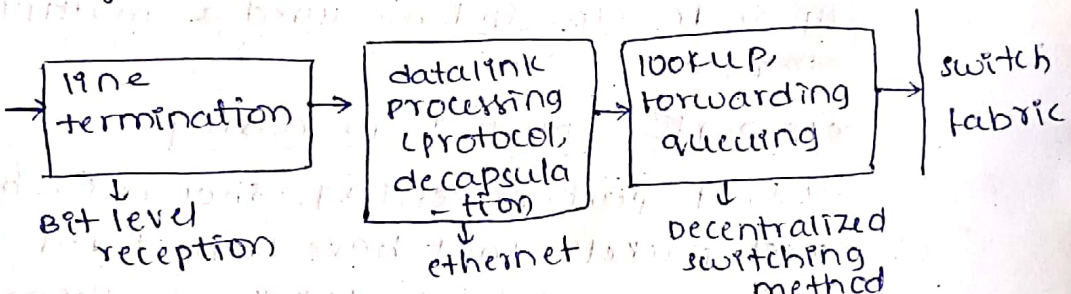


* Two key router functions
* run routing algorithm protocol
* forwarding datagram, from incoming to outgoing link.

1) Ip port :- (input processing).

An ip port performs several key functions. It performs the physical layer function of termi-nating an incoming physical link at a router, this is shown in the leftmost box of the ip port

An ip port performs link layer functions needed to interoperate with the link layer at other side of the incoming link. this is represented by the middle boxes in the ip and oip port. perhaps most crucially the lookup function is also performed at the ip port, this will occur in the rightmost box of the ip port.



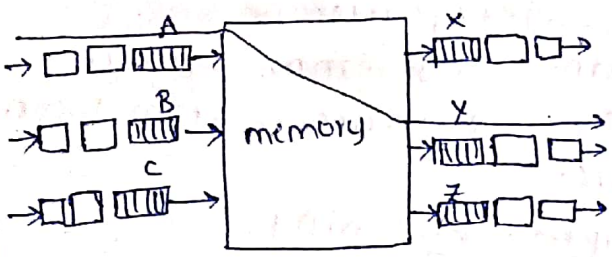
Queuing :- if datagram arrives faster than forwarding rate in to the switch fabric.

goal :- complete ip port processor at line speed.

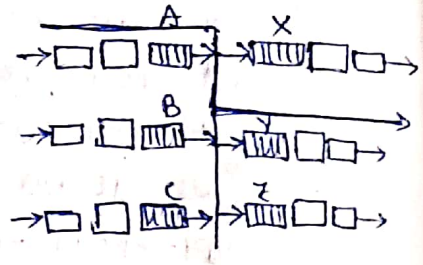
line speed :- the maximum speed a line can support

switching :-

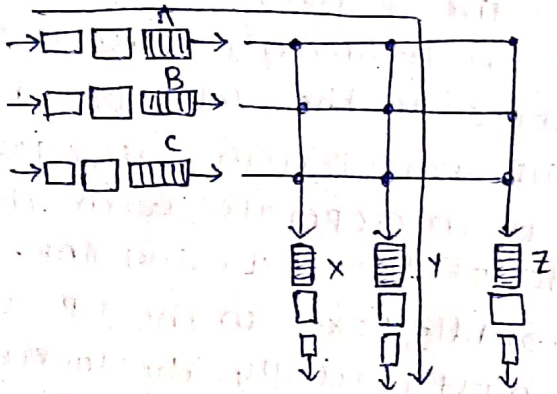
The switching fabric is at the very heart of a router, as it is through this fabric that the packets are actually switched from an ip port to an oip port. switching can be accomp-lished in a number of ways, as shown in below figure.



memory



BW



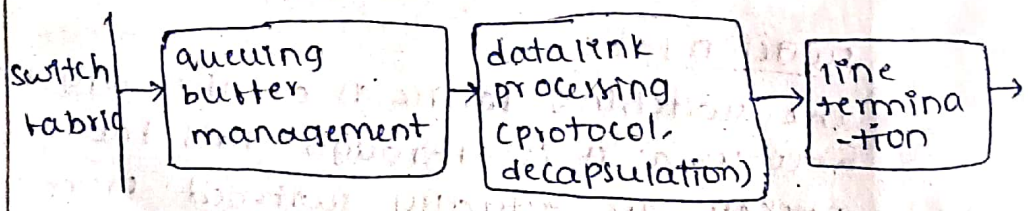
cross bar

* **switching rate:-**

A rate at which packets can transferred from ilp ~~or~~ to olp. and measured as multiple of ilp & olp rate.

2) **olp port:- (output processing)**

output port processing, shown in below fig. takes packets that have been stored in the olp ports memory and transmits them over the olp link, this includes selecting and de-queing packets for transmission & performing the needed link-layer and physical-layer transmission functions.

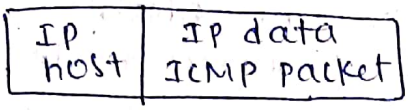


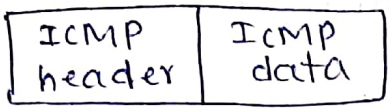
3) **switching fabric:-**

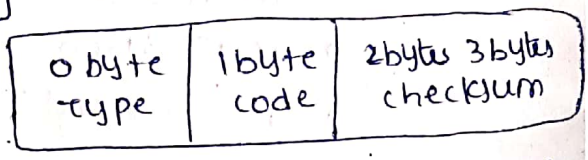
the switching fabric connects the router's ilp ports to its olp ports. The switching fabric is completely contained within the router- a nlw inside of a nlw router

4) Rotating processor- The routing processor executes the routing protocols, maintains routing tables and attached link state information & computes for forwarding table for the router. It also performs the nlw management functions.

ICMP :-







→ ICMP is network diagnostic and error reporting protocol. ICMP belongs to IP protocol suite and uses IP as carrier protocol.

→ After constructing ICMP packet, it is encapsulated in IP packet Because IP itself is a best-effort non reliable protocol, so is ICMP.

→ Any feedback about nlw is sent back to the originating host - if some error in the nlw occurs it is reported by means of ICMP, ICMP contains dozens of diagnostic and error reporting messages.

Internet control message protocol parameters

message type	Description
Destination unreachable	packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter prblm	invalid header field
Source quench	choke packet
Redirect	Teach a router about geography
Echo request	Ask a machine if it is alive
Echo reply	Yes, I am alive
Timestamp request	same as echo request, but with time stamp
Timestamp reply	same as echo reply, but with time stamp

Destination unreachable:-

It occurs when packet doesnot reach destination. suppose the sender sends the messages, but the message doesnot reach the destination, then intermediate router reports to sender that the destination is unreachable.

→ Destination nlw unreachable
→ Destination Host unreachable
→ Destination port unreachable.

Time exceeded :-

→ whenever a router decreases a datagram with a time-to-live value to zero, then the router discards a datagram and sends the time exceeded message to original source.
→ its depending upon time to live field if TTL=0 then the router can send an ICMP packet.

Parameter problem:-

→ The router and destination host can send a parameter problem message. This message conveys that some parameters are not properly set.
→ parameter prblms includes checksum, bad length of frame.

source quench:-

→ There is no flow control or congestion contro mechanism in the nlw layer. The sender is only concerned with only sending packets and the sender doesnot think whether receiver is ready to receive packets or is there any congestion occurs in the nlw layer, so that sender can send a lesser number of packets.

choke packet:-

it is a congestion control technique for both virtual circuit and data gram.

ping :- ping is the combination of echo request and echo reply

1) it works by sending ICMP echo request to interface on the nlw ~~for~~ wait for reply.
2) ping uses echo request and echo reply
3) we can hit any server on internet testing of the nlw can be done by ping command.

purpose of ICMP :-

1) To secure nlw traffic
2) To manage nlw traffic congestion.
3) To facilitate communication between nlw devices
4) To control nlw access
5) improve reliability

Network service models :-

The nlw service model defines the characteristics of end-to end transport of data between one "edge" of the nlw and the other i.e, blw sending & receiving end systems.

There are two service models

1) virtual circuit networks
2) Datagram networks.

Virtual circuit Networks :-

virtual circuit networks provide connection oriented.

→ A transport layer can offer applications connecti -onless service or connection oriented service blw two processes.

→ For example, the internets transport layer provi -des each application a choice blw two services; UDP, a connectionless service or TCP, a connection oriented service between two hosts.

→ A nlw layer connection service begins with handshaking blw source & destination host.

→ a nlw layer connectionless service does not have any handshaking.

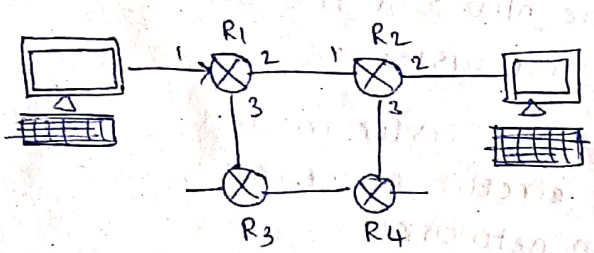
Let's now consider how a vc service can be implemented in a computer nlw.

A vc consists of

1) a path (series of links & routers)
2) vc number (one number for each link)
3) entries in the forwarding table

A packet belonging to a virtual circuit will carry a vc number in its header. Because a virtual ckt may have a different vc number on each link, each router must replace the vc numb of each traversing packet with a new vc numb the new vc number is obtained from the forwarding table.

To illustrate the concept, consider the nlw shown in the figure.



The numbers next to links of R1 in the above figure are the link interface numbers. Suppose now that host A requests that the nlw establish a vc between itself and host B. Suppose also that the nlw chooses the path A-R1-R2-B and assigns vc numbers 12, 22 and 32 to the three links in this path for the virtual ckt, when a packet in the vc leaves host A, the value in the vc number field in the packet header R1, the value is 22, and when it leaves R2, the value is 32.

There are three identifiable phases in the virtual circuit

i) VC setup:- During this setup phase, the sending transport layer contacts the nlw layer, specifies the receiver's address, and waits for the nlw to set up the vc. The nlw layer determines the path blw sender and receiver, that is, the series of links and routers through which all packets of the vc will travel.

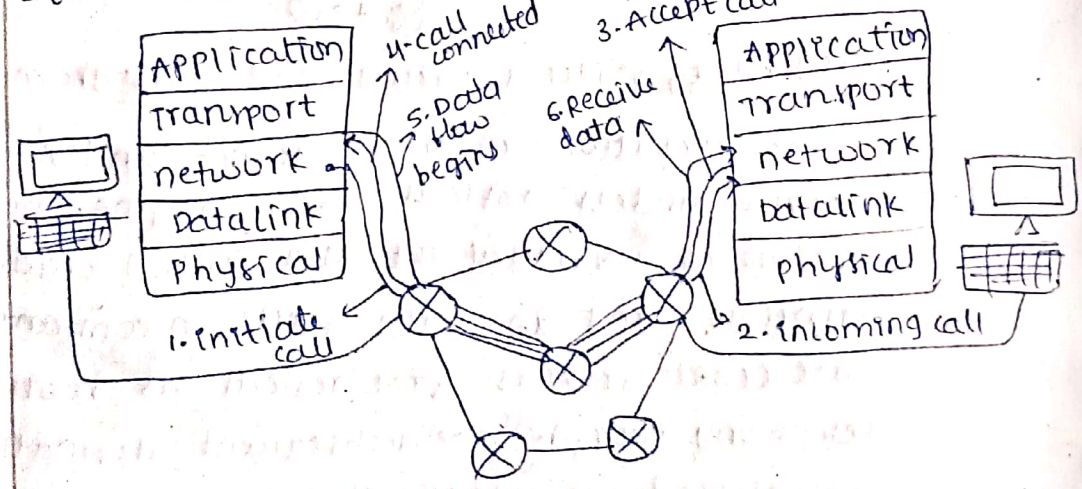
The nlw layer also determines the vc number for each link along the path. Finally the nlw layer adds an entry in the forwarding table in each router along the path. During vc setup, the nlw layer may also reserve resources along the path of the vc.

ii) Data transfer:-

once the vc has been established, packets can begin to flow along the path vc.

iii) VC teardown:-

This is initiated when the sender informs nlw layer of its desire to terminate the vc. The nlw layer will then typically inform the end system on the other side of the nlw of the call termination and update the forwarding table.



There is subtle but important distinction blw vc setup at the nlw layer and connection setup at the transport layer. connection setup at the transport layer [illegible] the two end systems.

during setup, systems also determine the parameters (like sequence number, windowsize) of their transport-layer connection.

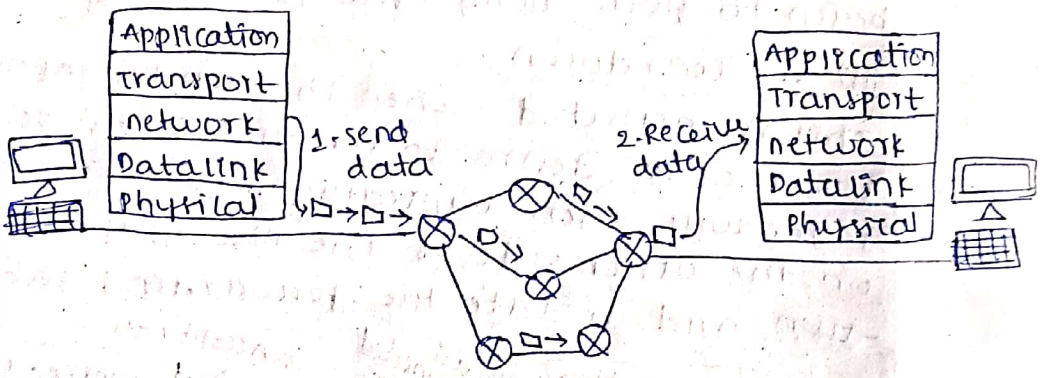
Handshaking:-

It is the process that establishes communication between two networking devices.

Datagram networks:-

Datagram nlw's are computer nlw's that provide connectionless services.

→ In a datagram nlw, each time an end system wants to send a packet, it stamp the packet with address of destination end system and then pops the packet into the nlw. As shown in the below figure, there is no VC setup and routers do not maintain any VC state information.



Origins of virtual circuit and Datagram nlw's:-

The evolution of the internet and ATM nlw service models reflects their origins. With the notion of a virtual ckt as a central organizing principle, and an early focus on constant bit rate (CBR) services, ATM reflects its roots in the telephony world. The subsequent definition of a unspecified bit rate (UBR) and available bit rate (ABR) services classes acknowledges the importance of data applications developed in the data networking community.

→ The internet, on the other hand, grew out of need to connect computers together. With sophis-ticated endsystem devices, the internet architec-ts choose to make the nlw-service model as simple as possible and to implement any addition-al functionality, as well as any new application level nlw services at a higher-layer, at the end system.

Internet protocols forwarding and addressing in the internet:-

Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces. when a router receives a packet from one of its attached nlws, it needs to forward the packet to another attached nlw or to some attached nlws

→ The third layer of communication protocol hierarchy is the nlw layer which specifies the networking aspects of a communcation transaction. This IP layer handles networking aspects and establi-shes routes for packets.

→ The IP produces a header for packets. An IP header contains the IP addresses of a source node and a destination node respectively.

→ An IP packet can be encapsulated in the layer 2 frames when the packet enters a LAN.

→ Ip layer provides a best-effort service. IP is inherently unreliable

→ Ip provides seamless internet connectivity and scalability. This layer is based on the connection-less or called datagram switching.

→ The advantage of this kind of service are

1) flexibility to allow interconnection blw nlw topologies

2) robustness to node failure.

IP Addresses:-

In order to provide computer to computer communication via internet, we need a global addressing scheme. such an addressing is provided by internet protocol (IP) at the nlw layer.

→ It is a 32-bit address. This called IP address or logical address which is made up of the nlw ID & unique host ID

→ It is represented in decimal value of each octet separated by a period (.)

→ Every host and router have IP address. which is unique and no two devices have same address at same time.

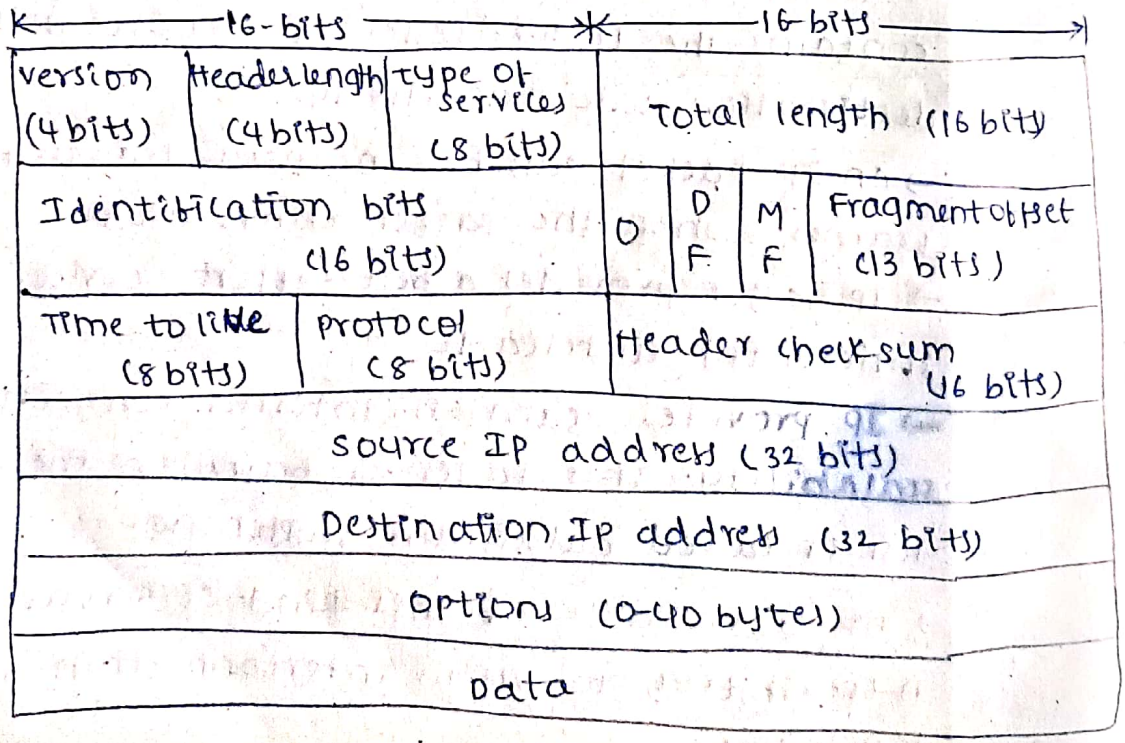
→ IP address can be static or dynamic

→ These numbers are assigned by ISP (internet service provider)

→ IP are of 2 types
IPV4 & IPV6

IPV4 (internet protocol version 4):-

→ The packet format of IP version 4 is shown below figure.

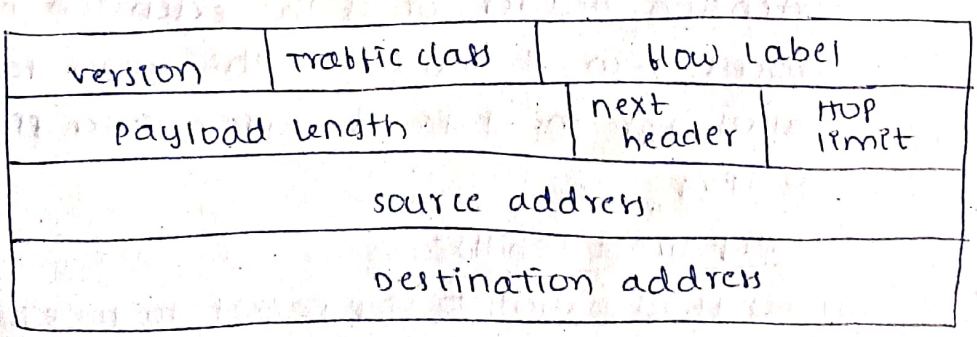


IPV4 header format

→ each packet comprises the header and data.
→ the size of header is variable with 20 bytes of fixed length header and an options field whose size is variable up to 40 bytes.
→ In the figure
1) version specifies IP version
2) Header length specifies length of the header
3) Type of service specifies quality of service such as priority level, delay, reliability and cost.
4) Total length specifies the total length of the packet in bytes.
5) Identification, flags and fragment offset are used for packet fragmentation and reassembly.
6) Time to live specifies the maximum no. of hops after which a packet must be discarded.
7) protocol specifies the protocol used at destination
8) Header checksum is method of error detection and correction.
9) source and destination IP addresses are 32-bit fields.
10) options is rarely used variable-length field to specify security level, timestamp and type of route.

IPV6 (Internet protocol version 6) :-

→ The IPV6 protocol defines a set of headers including the basic IPV6 header and IPV6 extension headers.
Below fig shows IPV6 header



IPV6 header format

The following list describes the function of each Header field

1) Version (4 bits) :-

It represents the version of IP i.e, 0110

2) Traffic class :- (8-bits)

These 8 bits are divided into two parts. The most significant 6 bits are used for type of service and 2 least significant bits are used for explicit congestion notification (ECN)

3) Flow label (20-bits) :-

This label is used to maintain the flow of the packets belonging to communication. It helps router to identify that a particular packet belongs to a specific flow of informations. This field helps avoid re-ordering of data packets

4) payload length (16-bits) :-

This field is used to tell the routers how much information a particular packet contains in its payload. payload is composed of extension Headers and upper layer data. With 16 bits, upto 65535 bytes can be indicated but if the extension headers contains Hop by hop extension header then the payload may exceed 65535 bytes and this field is set to 0

5) next Header (8 bits) :-

This field is used to indicate either the type of extension Header or if the extension header is not present then it indicates the upper layer PDU. The values for the type of upper layer PDU are same as IPv4

6) Hop limit (8bits) :-

This field is used to stop packet to loop in nlw infinitely

7) source address (128 bits) :-

Indicates address of the originator of the packet.

8) Destination address (128-bits):-
provides address of recipient of the packet.

IPV6 extension Headers:-
The following IPV6 extension headers are currently defined.

1) Routing - extended routing, such as IPV4 loose source route
2) Fragmentation - Fragmentation and reassembly
3) Authentication - integrity and authentication & security.
4) encapsulating security payload - confidentiality.
5) Hop by Hop options - special options that require hop by hop processing
6) Destination options - optional information to be examined by the destination node

Differences between routing & forwarding table:-

Routing table	Forwarding table
1) Routing is used for routing the traffic	1) It is used for forwarding data to appropriate destination port.
2) stores the destination address for nlws	2) responsible for storing the next hop & each nlw, frame type.
3) It is process of findingpath blw two nlws based on their nlw addresses	3) process of collecting data from one device & sending to another device
4) operates an nlw layer	4) operates on nlw layer
5) concentrates on calculating changes in topology & works based on IP address	5) checks forwarding tables and forwarding packets accordingly.
6) It follow different protocol such as routing internet protocol.	6) It follow different protocol such as UDP. security payloads

Difference b/w IPV4 & IPV6 :-

IPV4	IPV6
1) IPV4 address are 32-bit address which means there can be about 4 billion different IPV4 address.	1) IPV6 are 128 bit address that provides around 340 billion of IPV6 address
2) IPV4 have 5 classes class A 1 to 127 class B 128 - 191 class C 192 - 223 class D 224 - 239. class E 239 - 255	2) IPV6 Doesn't have any class
3) IPV4 is a numeric address.	3). IPV6 is a alphanume -ric address
4) they are separated by periods (.) /dot Ex:- 192.112.255.250	4) they are separated by colon (:) Ex:- 6d1c:18yf:byef:830a:350:6742:946f:6960
5) 2^{32} = 4,294,967,296	5) 2^{128} - 340,282,3669--
6) It supports manual & DHCP address	6) It supports auto & renumbering configuration
7) It can generate 4.29×10^9 address space	7) It can generate 3.9×10^{38} address space
8) Fragmentation is performed by sender & forwarding routers.	8) Fragmentation is performed by sender
9) In IPV4 packet flow identification is not available	9) In IPV6 packet flow identification is availa -ble.
10) checksum field is available	10) checksum field is not available