Syllabus

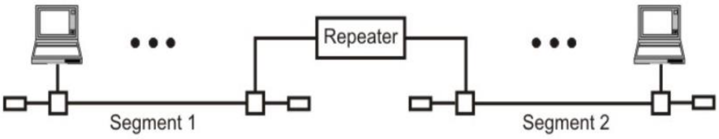
Network Layer: Repeaters, Bridges, Hubs, Switches, Routers, Gateways, Routing algorithms - Shortest path routing, Distance vector routing, Link state routing; X.25 layers and protocols, Congestion control - Leaky bucket algorithm, TCP/IP Protocol Suite- IP protocol, IP addresses, Subnetting, ARP, RARP; ICMP, ISDN Services and channels, Broadband ISDN, ATM- Design goals, architecture and layers.

Repeaters

A single Ethernet segment can have a maximum length of 500 meters with a maximum of 100 stations. To extend the length of the network, a repeater may be used. Functionally, a repeater can be considered as two transceivers joined together and connected to two different segments of coaxial cable. The repeater passes the digital signal bit-by-bit in both directions between the two segments. As the signal passes through a repeater, it is amplified and regenerated at the other end. The repeater does not isolate one segment from the other, if there is a collision on one segment, it is regenerated on the other segment. Therefore, the two segments form a single LAN and it is transparent to rest of the system.

Ethernet allows five segments to be used in cascade to have a maximum network span of 2.5 km. With reference of the ISO model, a repeater is considered as a level-1 relay. It simply repeats, retimes and amplifies the bits it receives. The repeater is merely used to extend the span of a single LAN. Important features of a repeater are as follows:

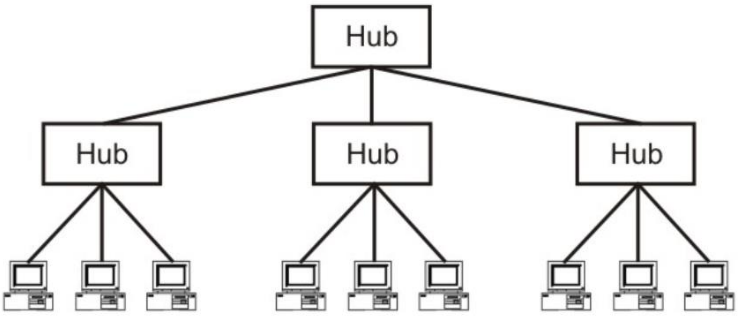
- A repeater connects different segments of a LAN.
- A repeater forwards every frame it receives.
- A repeater is a regenerator, not an amplifier.
- It can be used to create a single extended LAN



Hubs

Hub is a generic term, but commonly refers to a multiport repeater. It can be used to create multiple levels of hierarchy of stations. The stations connect to the hub with RJ-45 connector having maximum segment length is 100 meters. This type of interconnected set of stations is easy to maintain and diagnose. Figure next page shows how several hubs can be connected in a hierarchical manner to realize a single LAN of bigger size with a large number of nodes.

Hub as a multi-port repeater can be connected in a hierarchical manner to form a single LAN with many nodes.

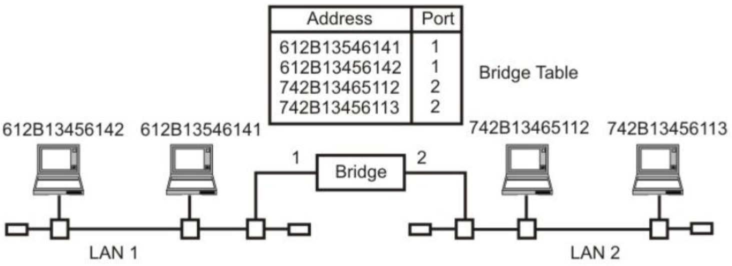


Bridges

The device that can be used to interconnect two separate LANs is known as a bridge. It is commonly used to connect two similar or dissimilar LANs. The bridge operates in layer 2, that is data-link layer and that is why it is called level-2 relay with reference to the OSI model. It links similar or dissimilar LANs, designed to store and forward frames, it is protocol independent and transparent to the end stations.

Use of bridges offer a number of advantages, such as higher reliability, performance, security, convenience and larger geographic coverage. But, it is desirable that the quality of service (QOS) offered by a bridge should match that of a single LAN. The parameters that define the QOS include availability, frame mishaps, transit delay, frame lifetime, undetected bit errors, frame size and priority. Key features of a bridge are mentioned below:

- A bridge operates both in physical and data-link layer.
- A bridge uses a table for filtering/routing.
- A bridge does not change the physical (MAC) addresses in a frame.
- Types of bridges:
    - Transparent Bridges.
    - Source routing Bridges.



Address	Port
612B13546141	1
612B13456142	1
742B13465112	2
742B13456113	2

Switches

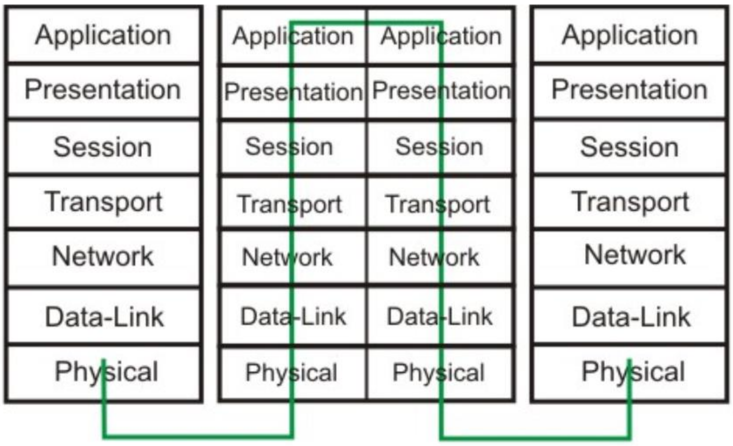
Switch is a device that connects devices together on a computer network. When it receives a frame, it checks its destination address and forwards the frame from matching port. In OSI model switch works on layer 2. Cisco makes more advance switches those works on layer 2, layer 3 and layer 4. These switches are known as multilayer switches.

Routers

Router is used to connect the two different networks. When it receives a data packet in its interface, it reads the destination network information and forward the data packet from its port that is associated with destination network. Router makes this decision based on its routing table and security policy. On internet routers perform traffic directing function, by directing the packet to next network on its journey. Data packet would be forwarded from one router to another router until it reaches its destination network. DSL router is an example of router that connects PC to internet.

Gateways

A gateway works above the network layer, such as application layer as shown in Fig. As a consequence, it is known as a Layer-7 relay. The application level gateways can look into the content application layer packets such as email before forwarding it to the other side. This property has made it suitable for use in Firewalls discussed in the next module.



IP Addressing System.

Addressing:- Two possible approaches used for addressing are:-

i) Flat Addressing.

ii) Hierarchical Addressing.

i) FLAT ADDRESSING:- In flat addressing every possible node is assigned a unique number. When a node is added to the network, it must be given an address within the allowed address range.

↑ 48 BITS.

Addressing used in Ethernet is an example of flat addressing, where addresses (48 bits Long) are allocated centrally blocks of addresses are apportioned to manufactures, so that no two devices in the world will have same address.

Flat addressing has the advantage that if a node is moved from one Location to another, it can retain its Unique address

ii) HIERARCHICAL ADDRESSING:-

In Hierarchical addressing, each address consists of a number of fields; as each field is inspected, the packet is taken nearer to the destination. This Scheme has disadvantage that if a host moves from one Location to another, new address needs to be allocated to it.

IP ADDRESS

↳ Every Host and Router on the internet is provided with a Unique standard form of network address; which encodes its network number and host number.

The Combination is Unique; no two nodes have same Ip address.

Ip Address = Internet Address = 32 Bits

Ip Address is 32 bit binary address implemented in Software that uniquely & Universally defines Host or Router on the Internet.

IP Address ⇒ 4 Octets {8 bits} Consisting of Network ID (NID) and Host ID (HID)

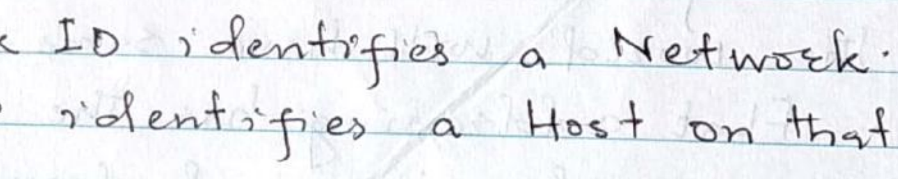
# Network ID identifies a Network.

# Host ID identifies a Host on that Network

CLASSIFICATION OF IP ADDRESSES :-

[Ip addresses are divided into Five different classes: Class A, Class B, class C, class D class E.] ⇒ known as Classful addressing.

Class A:



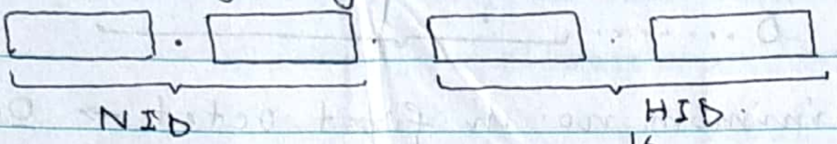
↓

[Defence networks]

$2^8 \rightarrow 256$ [Networks]

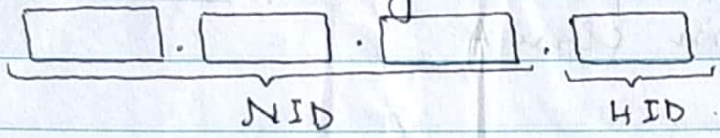
2^{24} Hosts. (16 millions)

Class B :- Big Organizations like Stock Exchange, University etc



2^{16}- (65.536) 2^{16} (65,536)

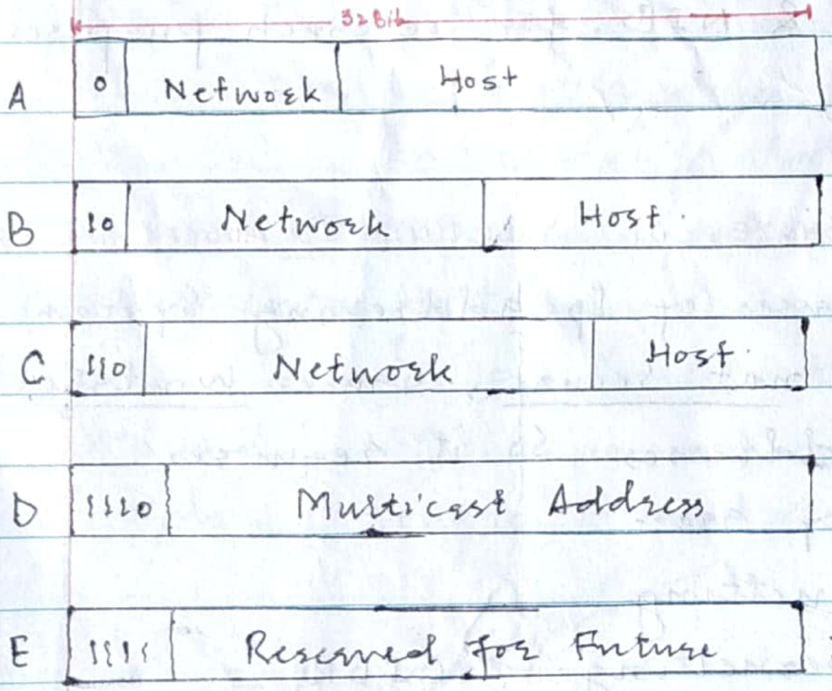
Class C :- Small organizations. Colleges etc.



2^{24}- (167,77216) 2^{8} → 256

Class D :- It is designed for multicastings. There is no NID or HID. whole address is designed /used for multicasting.

Class E :- Reserved by Internet for special use such as research etc.



A 1.0.0.0 to 127.255.255.255.

B 128.0.0.0 to 191.255.255.255.

C 192.0.0.0 to 223.255.255.255.

D 224.0.0.0 to 239.255.255.255

E 240.0.0.0 to 255.255.255.255.

For class A:

0 .... $\underbrace{\quad . \qquad . \qquad . \quad}$

Minimum no. in first octet → <u>0</u>0000000 - 0.

Maximum no. in first octet → <u>0</u>1111111 - 127

But 0 and 127 are reserved for special purpose, so only <u>126 (2^7-2)</u> are possible in class A.

Class →	Class B	Class C	Class D	Class E
first Octet	↓ 10	↓ 110	1110	1111

$\underbrace{\hspace{12em}}_{\text{Reserved Bits.}}$

Class ~~A~~	No. of Networks.	No. of Hosts.
- CLASS A	$2^7-2 = 126$ Networks	$2^{24}-2 = 16777214$ Hosts
- CLASS B	$2^{14} = 16,384$ Networks	$2^{16}-2 = 65534$ Hosts
- CLASS C	$2^{21} = 20,97,152$ Network	$2^8-2 = 254$ Hosts.
- CLASS D	No HID & NID, all 28 bits are used for Multi	
- CLASS E	No HID & NID, for research purposes.	

INEFFICIENCIES OF EXISTING IP ADDRESSING SYSTEM.

Existing classes of Ip addressing System isn't <u>Flexible</u>, <u>not Secure</u>, Causes <u>Wastage</u> of so many addresses. So it requires extensions, they are:-

1. Subnetting.
2. Supernetting or CIDR.
3. Public and Private Hosts.

In order to ~~mad~~ reduce the need for new Ip addresses, following three blocks of Ip address space are reserved for Private networks and Hosts.

10.0.0.0 to 10.255.255.255 - 1 Class A N/w

172.16.0.0 to 172.31.255.255 - 16 Class B N/w.

192.168.0.0 to 192.168.255.255 - 256 Class C N/w.

SUBNETTING :-

Subnetting is the process of dividing Large network into the smaller networks based on Layer 3 Ip addresses.

Subnet Mask :- Subnet mask is a 32 bits Long address used To distinguish between network address and host address in Ip address. Subnet mask has only one purpose To identify which part of Ip address is network address and which part is host address.

- In binary notation Subnet mask on bit [1] represents network address while bit [0] represents Host address.

- In decimal notation Subnet mask value 1 To 255 represent network address & value 0 represent host address.

- In Subnetting we borrow host bits To Create networks.

Advantages of Subnetting:-

- Subnetting breaks Large n/w into smaller networks and smaller networks are easy to manage.
- Subnetting reduces network traffic by removing Collision & broadcast traffic, that overall improves performance.
- Subnetting allows to apply network security policies at interconnection b/w Subnets.
- Subnetting allows To Save money

Subnetting Class B Address Space:-

NUMBER OF BITS IN NETWORK ADDRESS PREFIX	SUBNET MASK	NUMBER OF USABLE SUBNET.	NUMBER OF USABLE HOST ADDRESSES / SUBNET
2 = N	255.255.192.0	$4 = 2^2 = 2^N$.	$2^H - 2 = 2^{14} - 2 = 16382$
3	255.255.224.0	$2^3 = 8$	$2^H - 2 = 2^{13} - 2 = 8190$
4	255.255.240.0	$2^4 = 16$	$2^{12} - 2 = 4096 - 2 = 4094$
5	255.255.248.0	$2^5 = 32$.	$2^{11} - 2 = 2046$.
6	255.255.252.0	$2^6 = 64$	$2^{10} - 2 = 1022$.
7	255.255.254.0	$2^7 = 128$	$2^9 - 2 = 510$.
8	255.255.255.0	$2^8 = 256$.	$2^8 - 2 = 254$.
9.	255.255.255.128	$2^9 = 512$	$2^7 - 2 = 126$
10	255.255.255.192	$2^{10} = 1024$.	$2^6 - 2 = 62$
11	255.255.255.224	$2^{11} = 2048$.	$2^5 - 2 = 30$
12	255.255.255.240	$2^{12} = 4096$.	$2^4 - 2 = 14$
13	255.255.255.248	$2^{13} = 8192$.	$2^3 - 2 = 6$
14	255.255.255.252	$2^{14} = 16384$	$2^2 - 2 = 2$.

SUBNETTING CLASS C ADDRESS SPACE:

No. of Bits in Network Prefix.	SUBNET MASK	No. of USABLE SUBNET ADDRESSES	No. of USABLE HOSTS ADDRESSES / SUBNET.
2	255.255.255.192	$2^2 = 4$.	$2^{8-2} - 2 = 62$.
3	255.255.255.224	$2^3 = 8$.	$2^5 - 2 = 32$.
4	255.255.255.240	$2^4 = 16$	$2^4 - 2 = 14$.
5	255.255.255.248	$2^8 = 32$	$2^3 - 2 = 6$.
6	255.255.255.252	$2^6 = 64$.	$2^2 - 2 = 2$.

QUESTIONS

1). Address of System is 24.31.13.26.

a). Calculate Network-Id.

Clearly 24.31.13.26 is class A address having Subnet mask ⇒ 255.0.0.0.

∴ Network Id = 24.0.0.0.

b). What will be the address of 1st Host?

Address of first Host = 24.0.0.1

24.0.0.0 assigned for network id.

c). What will be the address of Last Host?

Address of Last Host = 24.255.255.254

While 24.255.255.255 will be assigned for broadcasting purpose and is known as Directed Broadcast Address.

Hence Hosts dont use two addresses because one is assigned for Net-Id & other for Directed broadcast.

- For a Net-id, host bits should be all 0's.
- For a Directed broadcast Address, host bits will all be 1's.

Q:- If Ip Address of a System is 36.11.119.14. Find Net-id, Directed Broadcast Address, 1st Host & Last Host address.

Ip Address = 36.11.119.14.
Net Id = 36.0.0.0.
Directed Broadcast Address = 36.255.255.255.
First Host = 36.0.0.1.
Last Host = 36.255.255.254.

Q:- If Ip Address is 199.83.44.12. Calculate Net-id, Directed Broadcast Address, 1st Host & Last Address and number of hosts in network.

Ip = 199.83.44.12. [CLASS C Address].
Net Id = 199.83.44.0.
Direct Broadcast Address = 199.83.44.255.
1st Host = 199.83.44.1.
Last Host = 199.83.44.254.
No. of Hosts in a Nw = $2^8 - 2 = \underline{254}$.

How Data is transferred between two different LAN networks of different CLASSES:-

- When network wants to transfer data, it designs a packet.

- This packet Contains data, Source Ip, and Destination Ip. This packet is transferred to Local Router.

- Local Router routes this packet to destination Systems Local Router.

- Whether to transfer data to one System or to broadcast the data, it is decided by Destination Router.

• If destination Ip is Directed Broadcast Address, then this packet is broadcasted.

1) Packet from 16.0.0.1 to 197.15.21.16.

DATA	16.0.0.1	197.15.21.16
	↓ Source Ip	↓ Destination Ip

2) If packet transmitted to every System of 197.15.21, then packet will be.

DATA	16.0.0.1	197.15.21.255
	↓ Source Ip	↓ Destination Ip.

• How Data is transferred within Same LAN Network.

We have two networks, connected via LAN.

- Let one network is of Class A of Net Id = 16.
- If Source Ip & Destination Ip have same Net-Id, then router will filter packet i,e it willn't allow packet to go outside.
- If we want to transfer data to every system in network Ip 64, then

DATA	SOURCE Ip	DESTINATION IP
	16.0.0.1	64.255.255.255

LIMITED BROADCAST ADDRESS:-

In this all bits are set to 1 & is used for broadcasting to every system in the same network.

A Special Type of Ip Address is the Limited Broadcast Address 255.255.255.255. A broadcast involves delivering a message from one Sender to many recipients. Senders direct an Ip broadcast to 255.255.255.255. to indicate all nodes on the Local network should pick up that message. This broadcast is limited in the way that it doesn't reach every node on Internet, but to only nodes on LAN.

ROUTING:

· Routing is an act of moring information across an inter-network from a Source To destination.

- Routing is process of choosing a path over which to send the packets.

· Routing occurs at Layer 3. [Network Layer].

→ · Routing ALgorithm is a part of network Layer Software responsible for deciding which output Line an incoming packet should be transmitted on i.e. what should be the next intermediate node for the packet.

Routing protocols use metrics to evaluate what path will be the best for packet to travel.

- A metric is standard of measurement; such as path bandwidth, reliability, delay, Current Load on that path. that is used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize and mantain routing tables, which contain route information.

Desirable properties of a router are:-

i) Correctness and simplicity:- Packets are to be delivered Correctly. Simpler the routing algorithms, better it is.

ii) Robustness:-

Ability of network to deliver packets via some route even in face of failures.

iii) Stability:-

Algorithm should converge to equilibrium fast in the face of changing conditions in the network.

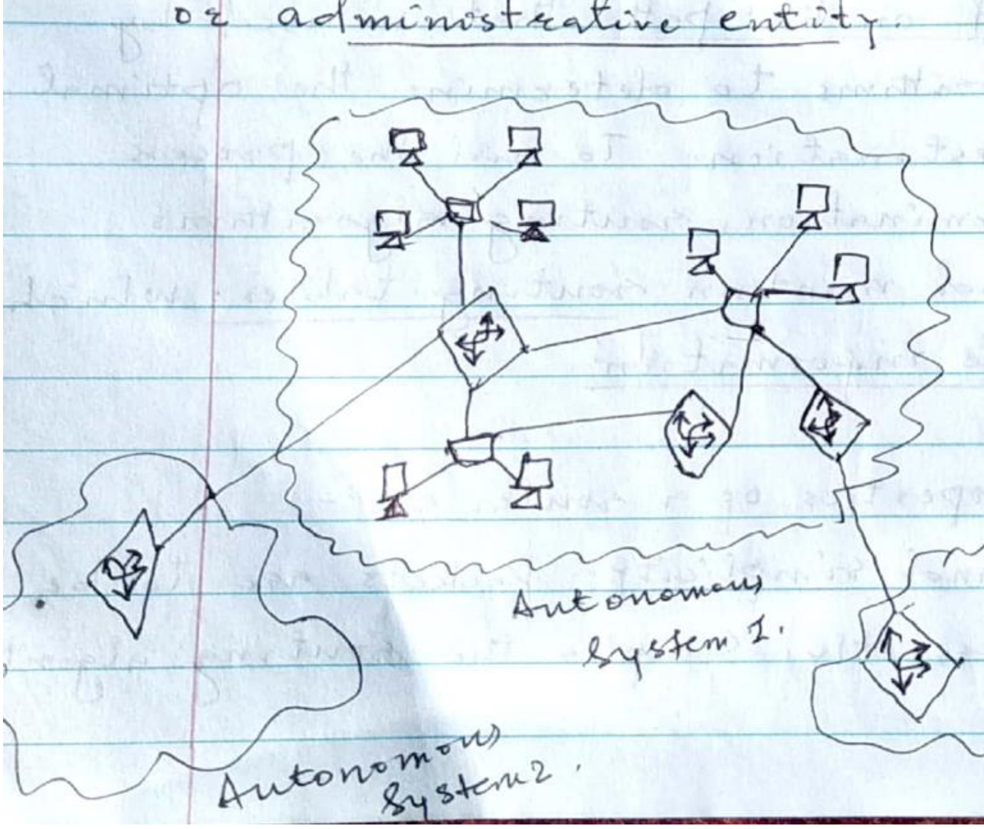
iv) Fairness and Optimality:-

v) Efficiency:- Minimum Overhead.

DECENTRALIZED ARCHITECTURE

↓

Decentralized Architecture treats the Internet as a Set of independent groups, which each group called an autonomous System (AS). An autonomous System consists of Routers and networks controlled by a particular Organization or administrative entity.



INTERNAL ROUTERS:-

Some routers in an Autonomous System (AS) Connect only to other routers in the Same (AS). These are internal routers and run interior routing protocols.

BORDER ROUTERS:-

Some routers in an Autonomous System Connect both to routers within the Autonomous System & to routers in one or more other Autonomous Systems. These routers are responsible for passing traffic between the AS & the rest of internetwork. They run both interior and exterior routing protocols.

ROUTING PROTOCOL:-

A routing protocol is a protocol that specifies how routers communicate with each other disseminating information that enables them to Select routes between any two nodes on a Computer network; the Choice of route being done by routing algorithms.

Routing Algorithm Classification:-

Routing Algorithms Can be Classified based on following Criteria:-

- Static versus Adaptive.
- Single-path versus Multi-path.
- Intra-domain versus Inter-domain.
- Flat versus Hierarchical.
- Link State versus Distance vector.
- Host-intelligent versus Router-Intelligent.

i) Static versus Adaptive.

Static routing or Non-adaptive routing algos are hardly algorithms at all; the table mappings are established by the network administrator before the begining of routing. These mappings don't change unless the network ~~a~~ administrator alters them. Routing ~~algorithms~~ decisions in these algorithms are in no way based on current topology or traffic.

Static routing systems can't react to network changes

Adaptive or Dynamic Routing:-

↳ Adjust to changing network circumstances by analyzing incomming traffic messages

If the message indicates a network change, routing algorithm recalculates routes & Sends out new routing update messages.

2) SINGLE-PATH versus MULTI-PATH.

This division is based upon the number of paths a router stores for a single destination.

- Single Path algorithms are where only a single path is stored in the routing table.
- Some sophisticated routing tables support multiple paths to the same destination; these are known as multiple path algorithms.

Multi-path algorithms provide Substantially

- Better <u>Throughput</u> and <u>Reliability</u>.

known as LOAD SHARING.

3). INTERDOMAIN versus INTRADOMAIN.

Some routing algorithms work only within domains; [others work with and between domains] → <u>INTRADOMAIN</u>

4). LINK STATE versus DISTANCE VECTOR.

This category is based on the way the routing tables are updated.

Distance vector algorithms also known as <u>Bellman-Ford</u> algorithm. key features of distance vector routing are:-

- Routers share the knowledge of the entire autonomous system
- Sharing of information takes place only with neighbours.

- Sharing of information takes place where at fixed regular intervals - every 30 Secs.

Link State algorithms - (Shortest path first algorithms) have following key features:

- Routers share knowledge only about their neighbours compared to all routers in autonomous System.
- Sharing of information takes place only with all routers in internet, by sending small updates using Flooding
- Sharing of information takes place only when there is Change, when there is a Change, which leads to lesser internet traffic Compared to distance vector routing.
- Convergence takes place more quickly in Link-state algorithms, these are less prone to routing Loops than distance vector algos.
- But Link-State algorithms require more processing power & memory than distance vector algorithms.
- Link State algorithms are more expensive to implement & support.
- Link State protocols are generally more scalable than distance vector protocols

Host Intelligent versus Router Intelligent

↳ The division is based on whether the Source knows about the entire route or just about the next-hop where to forward the packet. [Some routing algorithms assume that the Source end node will determine the entire route] ⇒ SOURCE ROUTING.

In Source-routing Systems, routers merely act as Store-and-Forward devices. These algorithms are referred as Host Intelligent Routing, as entire route is determined by Source.

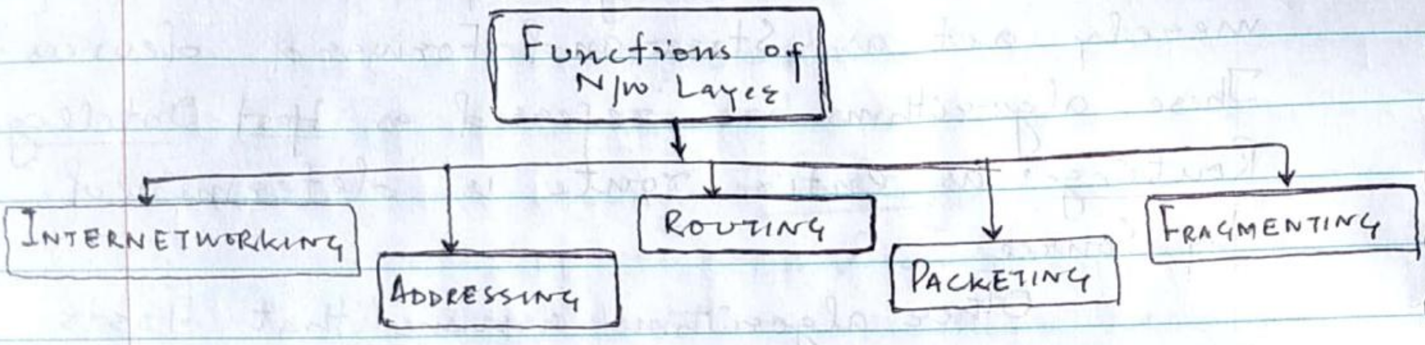
Other algorithms assume that Hosts know nothing about routes, routers determine the path through the internet based on their own strategy. Hence Router Intelligence.

NETWORK LAYER.

Network Layer in Internet model is responsible for carrying a packet from one computer to another.

Network Layer is responsible for Host-to-Host delivery.

Functions of Network Layer.



1) INTERNETWORKING:-

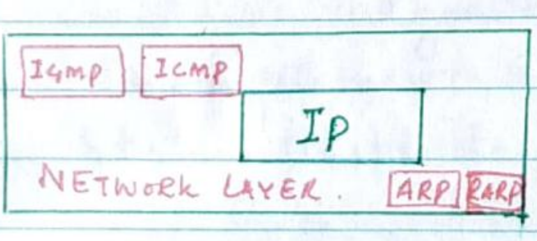
Main duty of network layer is to provide internetworking.

NETWORK LAYER PROTOCOLS:

ARP, Ipv4, ICMP, IPv6. ICMPv6.

In the Internet model, or TCP/IP suite, there are five network layer protocols:

ARP, ICMP, IP, RARP, IGMP.



- The main protocol in Network Layer is Ip. which is responsible for Host-to-Host delivery of datagrams from a Source to Destination.

- Ip needs a protocol called ARP [Address Resolution Protocol] to find the MAC address (Physical Address) of the next hop. This address must be passed to the data Link layer, with the Ip datagram to be inserted into encapsulating frame.

- During datagram delivery, Ip needs services of ICMP to handle unusual situations such as occurroence of an error.

- Ip is designed for unicast delivery, one Source to one Destination. Multimedia and other new applications in the Internet need multicasting delivery, one Source to many destinations. For multicasting, ~~of~~ Ip uses the services of another protocol called IGMP.

ARP ⇒ ADDRESS RESOLUTION PROTOCOL.

The Internet is made of a combination of Physical networks connected by devices such as routers. A packet starting from a Source host may pass through several different Physical networks, finally reaching the destination host.

The hosts and routers are recognized at the network Layer by their Ip addresses. Ip address is an internetwork address. An Ip address is universally Unique.

However, packets pass through Physical networks to reach these Hosts & Routers At Physical network, the Hosts and Routers are recognized by their MAC addresses.

MAC address should be Locally Unique.

Delivery of a packet to a Host or a Router requires two Levels of addressing.

1) IP } Need mapping b/w
2) MAC. } these two.

We have two types of address mapping:

- STATIC Mapping.
- DYNAMIC Mapping.

→ Static Mapping:-

Static Mapping means creating a table that associates an Ip address with a MAC. This table is stored in each machine on the network.

→ Dynamic Mappings:-

In dynamic mapping each time a machine knows one of the two addresses

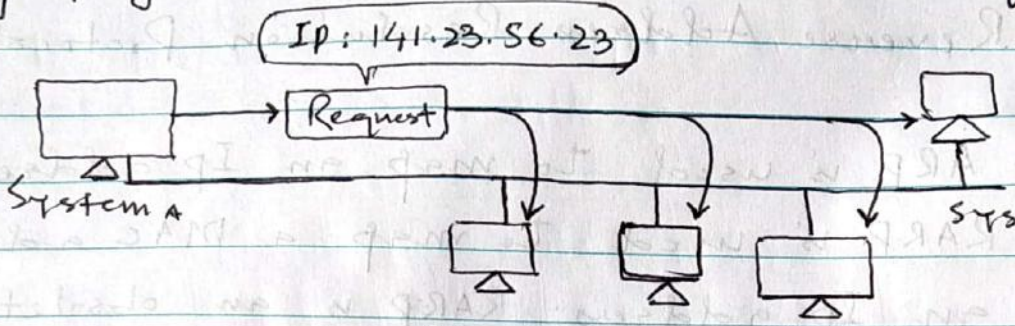
; it can use a protocol to find the other one
Two protocols have been designed to perform dynamic mapping ; Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).

- ARP is used to map an Ip address to a MAC.
- RARP is used to map a MAC address to an Ip address. RARP is an obsolete now and is replaced by DHCP.

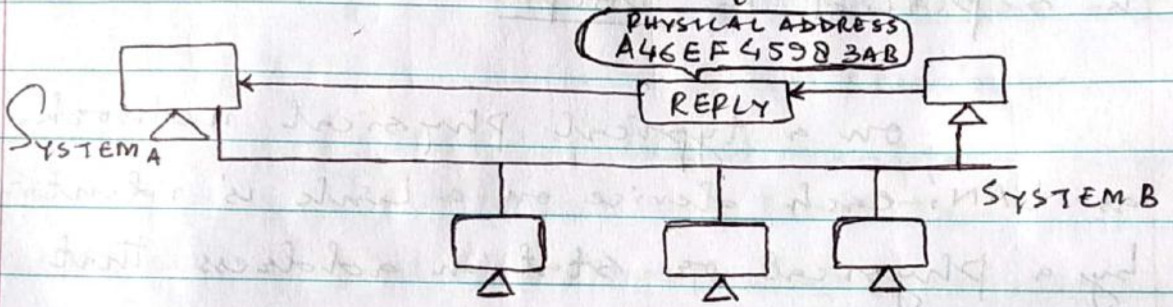
On a typical physical network, such as LAN, each device on a link is identified by a physical or station address that is usually imprinted on the NIC.

Anytime a host or a router, needs to find the MAC address of another host or router on its network, such as LAN, each device it sends an ARP query packet. The packet includes the physical and Ip addresses of the sender and Ip address of the reciever. Because the sender doesn't know the physical address of the reciever, the query is broadcasted over the network.

Every host or router on the network recieves and processes the ARP query packet, but only intended reciepient recognizes its Ip address and sends back an ARP response packet. ~~but~~ The packet is unicast directly to the inquirer using Physical address recieved in query packet



a). ARP request is broadcasted.



b) ARP reply is unicast.

ICMP- INTERNET CONTROL MESSAGE PROTOCOL.

To make efficient use of network resources, Ip was designed to provide unreliable and connectionless best.effort datagram delivery Service. As a Consequence, Ip has no Error-Control mechanism and Lacks mechanism for host & management queries. A Companion protocol known as Internet Control Message Protocol (ICMP) has been designed to Compensate these two deficiencies.

ICMP messages Can be broadly divided into two broad Categories-

- Error Reporting Messages.
- Query Messages.

i) Error Reporting Messages:-
Destination Unreachable, Time Exceeded, Parameter problems, Redirect.

ii) Query Messages:-
Echo, Echo request & reply, Timestamp request and reply, Address mask request and reply.

i) Echo Request and Reply:-

The echo-request and echo-reply messages are designed for diagnostic purposes. Network managers & users utilize this pair of messages to identify network problems.

Combination of Echo-Request and Echo-Reply determine whether Two systems (hosts or router) can communicate with each other.

ii) Time-Stamp Request and Reply:-

Two machines (Hosts or Routers) can use the Time-Stamp request and reply to determine the roundtriptime (RTT) needed for Ip datagram to travel between them.

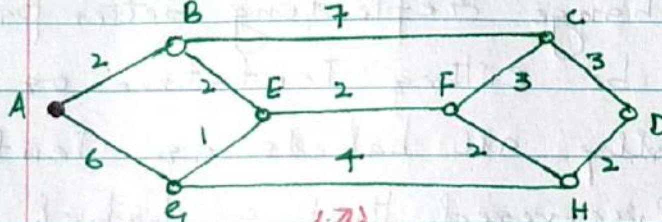
Also used to synchronize clocks in two machines.

iii) Router Address Mask Request and Reply:-

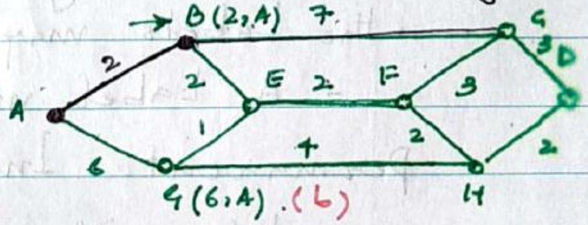
Ip address of a host contains a network address, Subnet address, and host identifier. A host may know its full Ip address, but it mayn't know which part of address defines n/w or Sub-n/w address. In this case, host can send an Address mask request message to router. The router sends a mask in Address mask reply message.

- Shortest Path Rooting:-

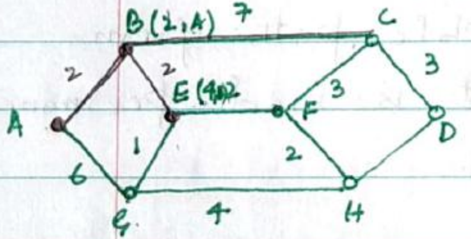
Lets build a graph ~~of~~ representing a network with each node representing a router and each arc of graph representing a Communication Line or Link. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

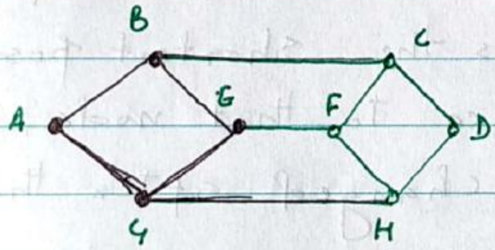


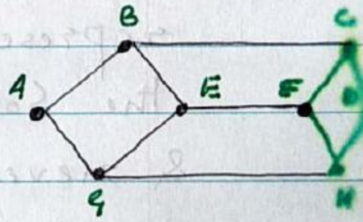
(a)

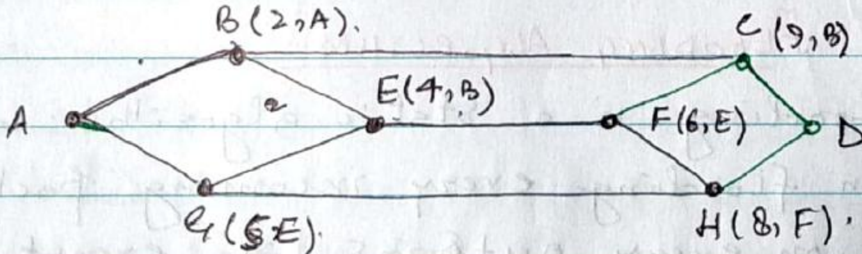


(b)









DIJKSTRA ALGORITHM.

- In Dijkstra algorithm, each node is Labelled in parenthesis with distance from the Source node along the best known path.

- Initially, no paths are known, So all nodes are Labelled with infinity

- As algorithm proceeds & paths are found, the Labels may change reflecting better paths.

- A Label may be either Tentative or permanent. Initially all Labels are Tentative

- When it is discovered that a Label represents the shortest possible path from the Source to that node, it is made permanent & never changed after that.

FLOODING ALGORITHM:

- Flooding is a Static algorithm.

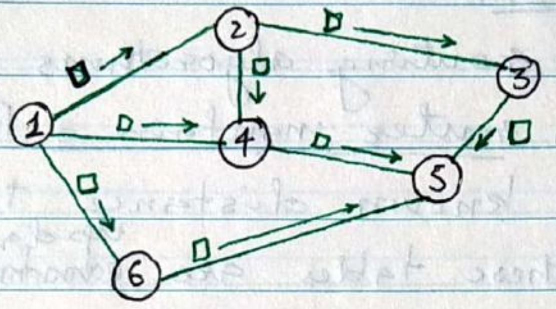
- In flooding every incoming packet is sent out on every outgoing line except the one it arrived on.

- Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite unless some measures are taken to damp the process.

- One such measure is to have a Hop Counter contained in the Header of each packet, which is decremented at each Hop.

with packet being discarded when counter reaches Zero.

Metric → No. of Hops.
Assume max hops = 3.



- The major disadvantage of flooding is. Redundant packets are created in the network.
- Flooding Creates Unnecessary packets which leads to Congestion at routers in the network.
- Flooding is used in the Military Operations.

SELECTIVE FLOODING:- A variation of flooding that is more practical is Selective Flooding In this algorithm the routers don't send every incomming packet out on every Line, only on those Lines that are going approximately in the right direction.

-Flooding always chooses Shortest path because it chooses every possible path in parallel.

DISTANCE VECTOR ROUTING ALGO :-

- Distance Vector routing is a dynamic routing algorithm.
- Distance vector routing algorithms operate by having each router mantain a Routing Table giving the best known distance to each destination. These tables are ~~exchanged~~ updated by exchanging info. with neighbours.
- Distance vector routing algorithms are also known as Bellman-Ford routing algorithm and Ford-Fulkerson algorithm.

- In distance vector routing, each router mantains a routing table indexed by & contaning one entry for each router in the Subnet.

Imp:- In distance vector, routing, protocol uses a routing algorithm in which routers periodically send routing updates to all neighbours by broadcasting their entire route tables.

LINK STATE ROUTING PROTOCOLS.

If distance vector routing protocols are road signs, then Link State routing protocols are Like a road maps.

In Link state routing protocols, each router originates information about itself, its directly connected Links and state of those Links. This information is passed around from router to router, each router making a copy of it, but never changing it,

Ultimate objective is that every router has identical information about the internw and each router will ~~identi~~ independently calculate its own best paths.

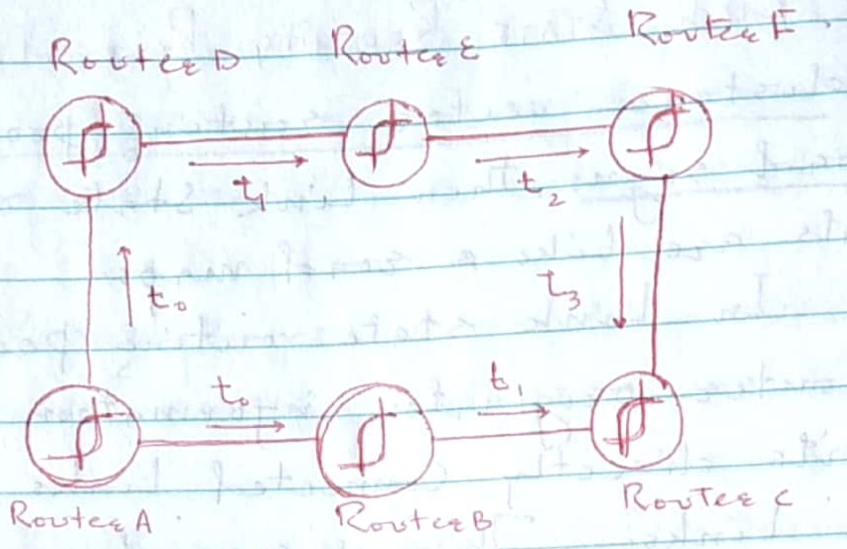
Link State protocols are more complex than distance vector protocols, but basic functionality includes 4 steps:

1). Each router establishes a relationship - an adjacency with each of its neighbours.

2). Each router sends Link state advertisements (LSAs), some

3) Each ~~LSA~~ router stores a copy of all LSAs it has seen in a database.

4). The completed topological database, also called the Link State database describes graph of internetwork.



1) Neighbours.

2) Link State Flooding.

3) Sequence Numbers:- [When LSAs are flooded all are tagged with same sequence no. at one time.]

ROUTER C

CASE 1:-

LSA from Router B at t_1 is entered into Router C's topological database.

At some time t_3, another copy of the same LSA arrives from A-D-E-F-C. Router C sees that it already has LSA in database with same Sequence number.

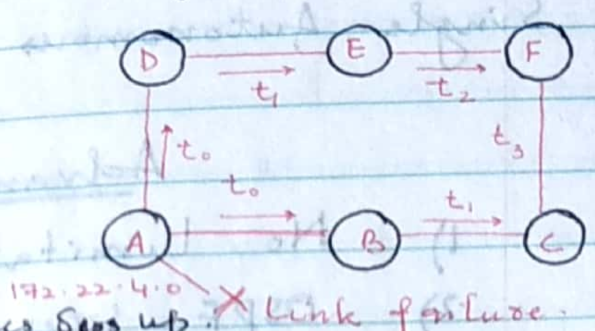
So if a router gets LSA of Same Sequence number, with same information as already stored in Link State databse, incomming LSA is discarded.

CASE 2:-

If an incomming LSA has Same information but Sequence number is greater then recieved information & new Sequence no. is entered into database and LSA is flooded.

CASE 3:-

[Link Failure]



Network 172.22.4.0 goes down & then after few Secs goes up.

So router A will send LSA [down LSA] with Sequence no. 166. & then will send LSA [up LSA] with Sequence no. 167.

Router C will recieve the two LSAs along A-B-C while with some delay other LSAs will be routed along A-D-E-F-C path & are discarded.

Without Sequence numbers, Router C couldn't have entertained the correct Info.