Subject: CN
Faculty: N.SHIRISHA
Topic:

Class Notes

Unit No: III
Lecture No: Lec 1
Link to Session
Planner (SP): S.No of SP
Book Reference: T1
Date Conducted: 30/4/21
Page No: 1

UNIT - III
The Network Layer

The N/w layer is concerned with getting packets from the source all the way to the destination.

To achieve its goal, the n/w layer must know about the topology of the comm. subnet & choose appropriate paths through it.

N/w Layer Design issues:

Store-and-forward Packet switching:

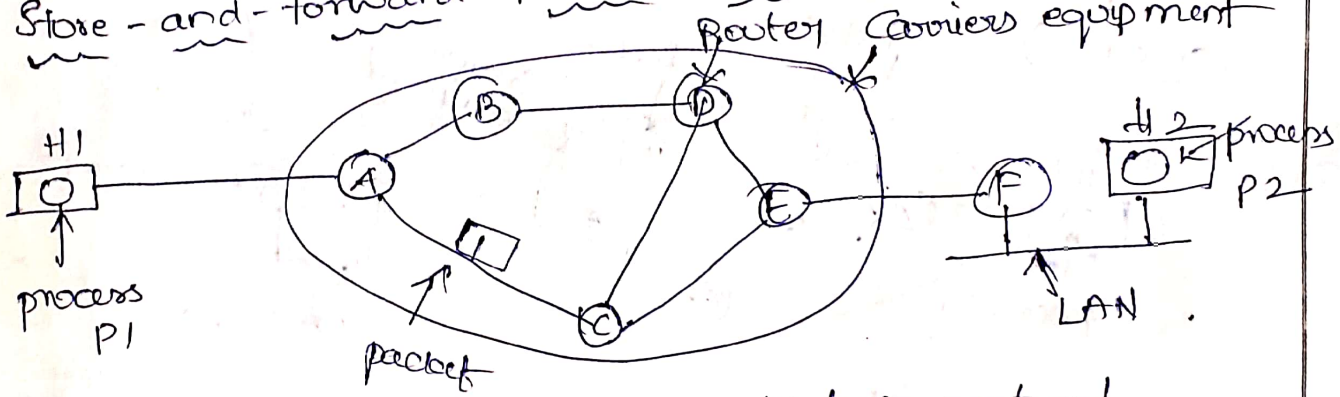


fig:- environment of n/w layer protocols.

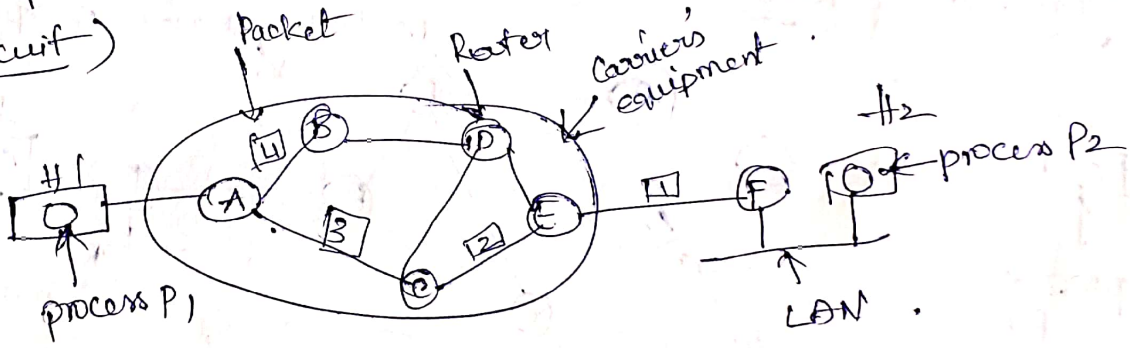
Services provided to the Transport layer:

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the no., type & topology of the routers present
3. The n/w addresses made available to the transport layer should use a uniform naming plan & even across LANs & WANs.

Implementation of Connectionless Service :

Here, Packets are injected into the subnet individually and routed independently of each other. Packets are frequently called datagrams & subnet is called datagram subnet.

If conn. oriented service is used, a path from the source router to the dest. must be established before any data packets can be sent. This conn. is called a VC (virtual circuit)



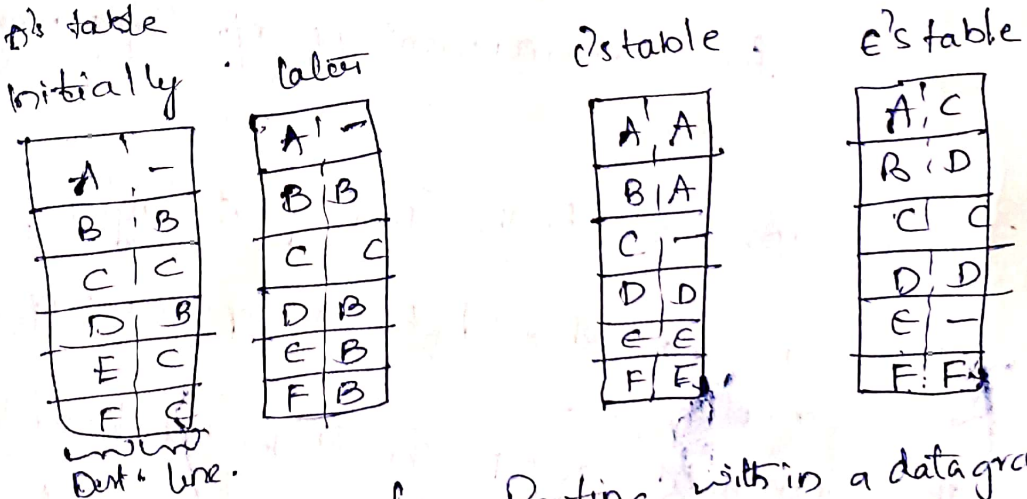


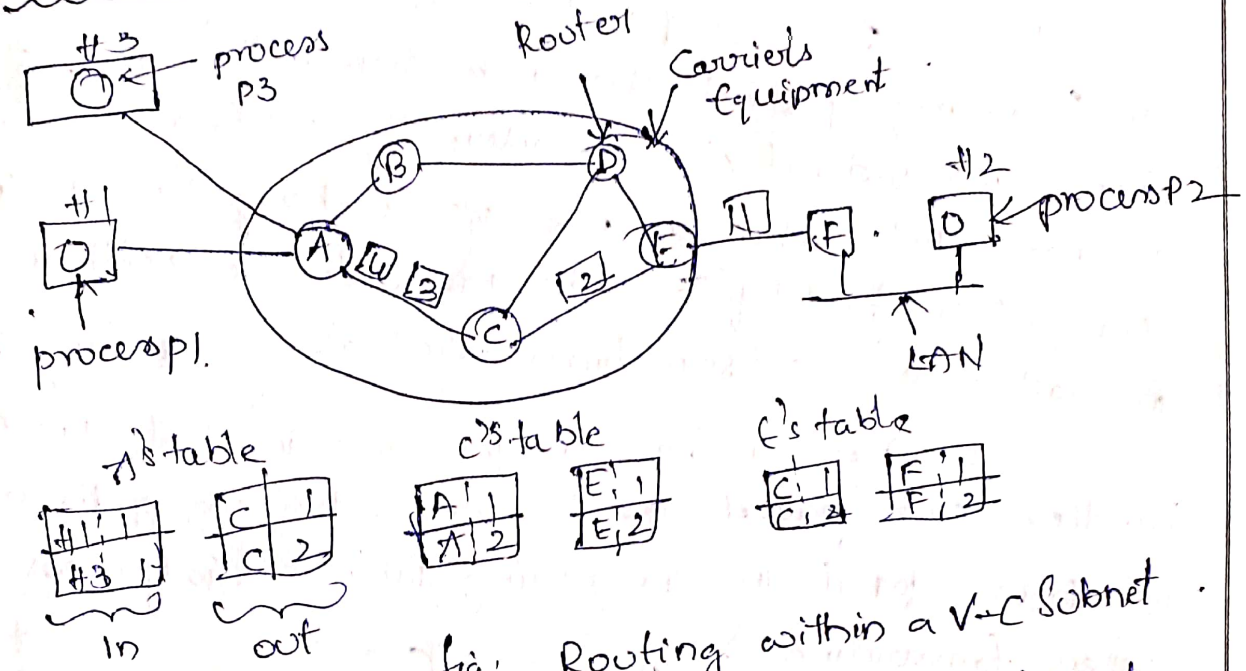
fig: Routing within a datagram subnet.

Subject:CN
Faculty: N.SHIRISHA
Topic: N/w layer design issues.

Class Notes

Unit No: III
Lecture No: 1 & 2
Link to Session
Planner (SP): S.No. of SP
Book Reference: T1
Date Conducted: 29/8/19
Page No: 2

Implementation of connection Oriented Service



A's table

In	Out
H1, 1	C, 1
H3, 1	C, 2

C's table

In	Out
A, 1	E, 1
A, 2	E, 2

E's table

In	Out
C, 1	F, 1
C, 2	F, 2

fig: Routing within a V-C Subnet.

Comparison of Virtual-Circuit and Datagram Subnet!

Issue	Datagram Subnet	Virtual-Circuit Subnet.
Circuit setup	not needed	Required
Addressing	Each packet contains the full source & dest. address	Each packet contains a short VC no.
State info.	Routers do not hold state info. about connections.	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is setup; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated.
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC.

Congestion Control	Difficult	Easy if enough resources can be allocated in advance for each VC.

Routing Algorithms :-

It is responsible for deciding which o/p line an incoming packet should be transmitted on. If the subnet uses virtual circuits internally, routing decisions are made only when a new VC is being set up thereafter, data packets just follow the previously established route. The latter case is sometimes called Session routing.

Router has two processes inside it. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables. This process is called forwarding.

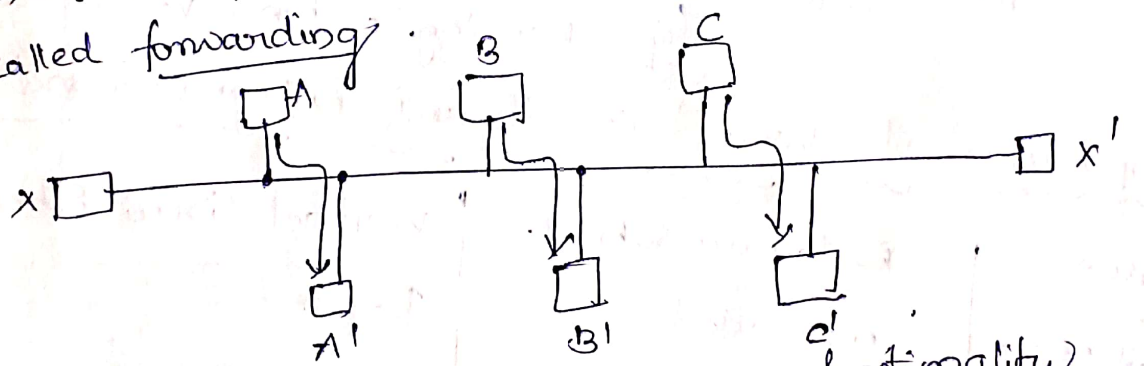


fig:- conflict b/w fairness & optimality.

Two types of Routing Algo. : ① Non Adaptive - static routing
② Adaptive.

Non-Adaptive Algo. do not base their routing decisions on measurements or estimates of the current traffic & topology.

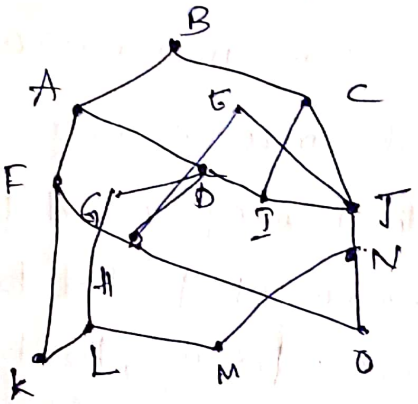
Adaptive Algo., change their routing decisions to reflect changes in the topology, usually the traffic as well.

Subject:CN
Faculty: N.SHIRISHA
Topic: Routing Algo:

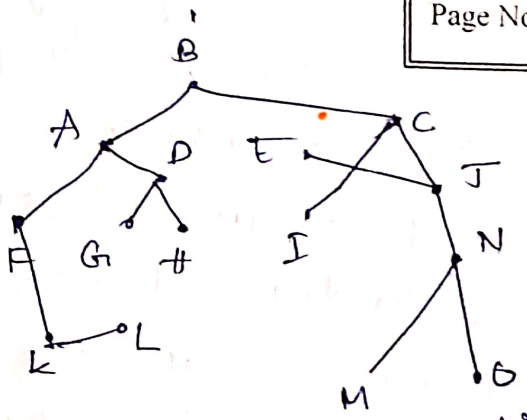
Class Notes

Unit No: V - III
Lecture No: 62
Link to Session
Planner (SP): S No. 03 of SP
Book Reference: T1
Date Conducted: 04/5/21
Page No: 3

Optimality principle :-



(a) A Subnet

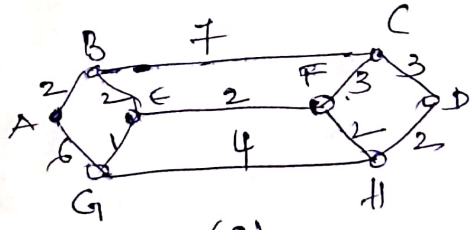


(b) A Sink tree for router B.

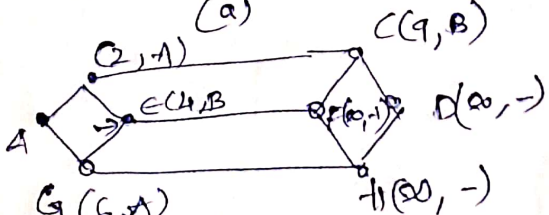
- One can make a general statement about optimal routes without regard to n/w topology or traffic. This statement is known as the optimality principle.

- The set of optimal routes from all sources to a given dest. form a tree rooted at the dest. such a tree is called a sink tree.

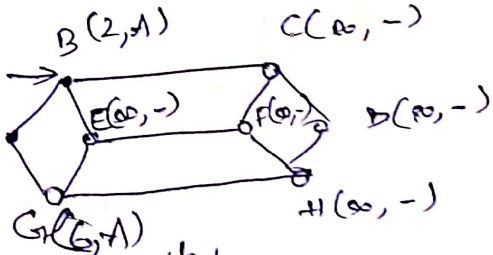
Shortest Path routing :

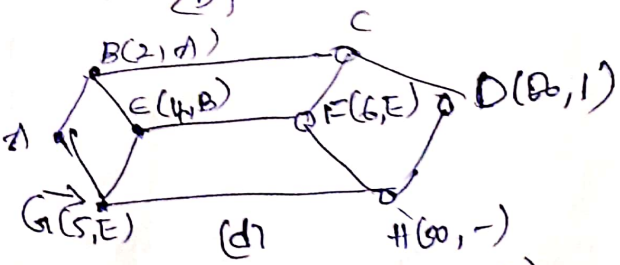


(a)

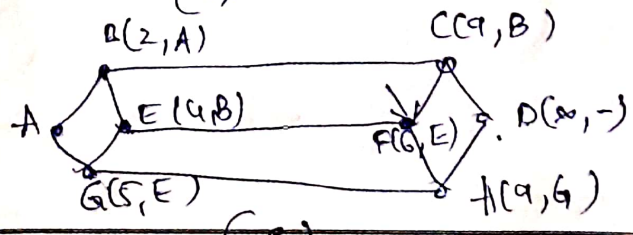


(b)

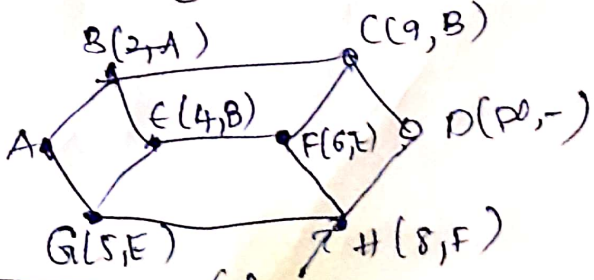




(c)



(d)



(e)

- Arrow indicates working node.

Flooding :

Another static algo. is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding obviously generates vast numbers of duplicate packets, an infinite no. 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 the packet being discarded when the counter reaches zero. Ideally, the hop counter should be initialized to the length of the path source to destination.

Subject: CN
Faculty: N.SHIRISHA
Topic: Routing Algorithms:

Class Notes

Unit No : III
Lecture No : 10.2
Link to Session:
Planner (SP) : 83
Book Reference : T1
Date Conducted : 29/8/19
Page No: 4

- Distance Vector Routing :

There are two dynamic algorithms.

① Distance Vector routing
② Link State routing.

Distance vector routing algorithms operate by having each router maintain a table (ie., a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging info. with the neighbors.

The other names for this algo. are Distributed Bellman-Ford algo. & the Ford-Fulkerson algo.

In DVR, each router maintains a routing table indexed by, containing one entry for, each router in the subnet. This entry contains two parts: the preferred outgoing line to use for that dest. and an estimate of the time or distance to that dest.

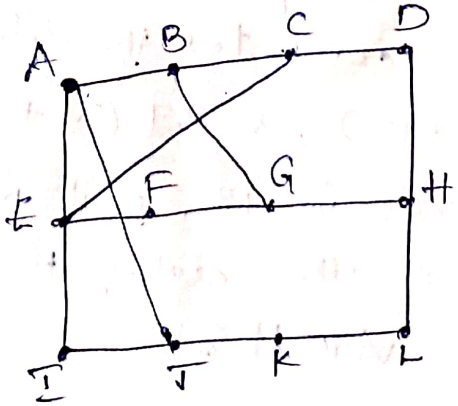


fig: A Subnet

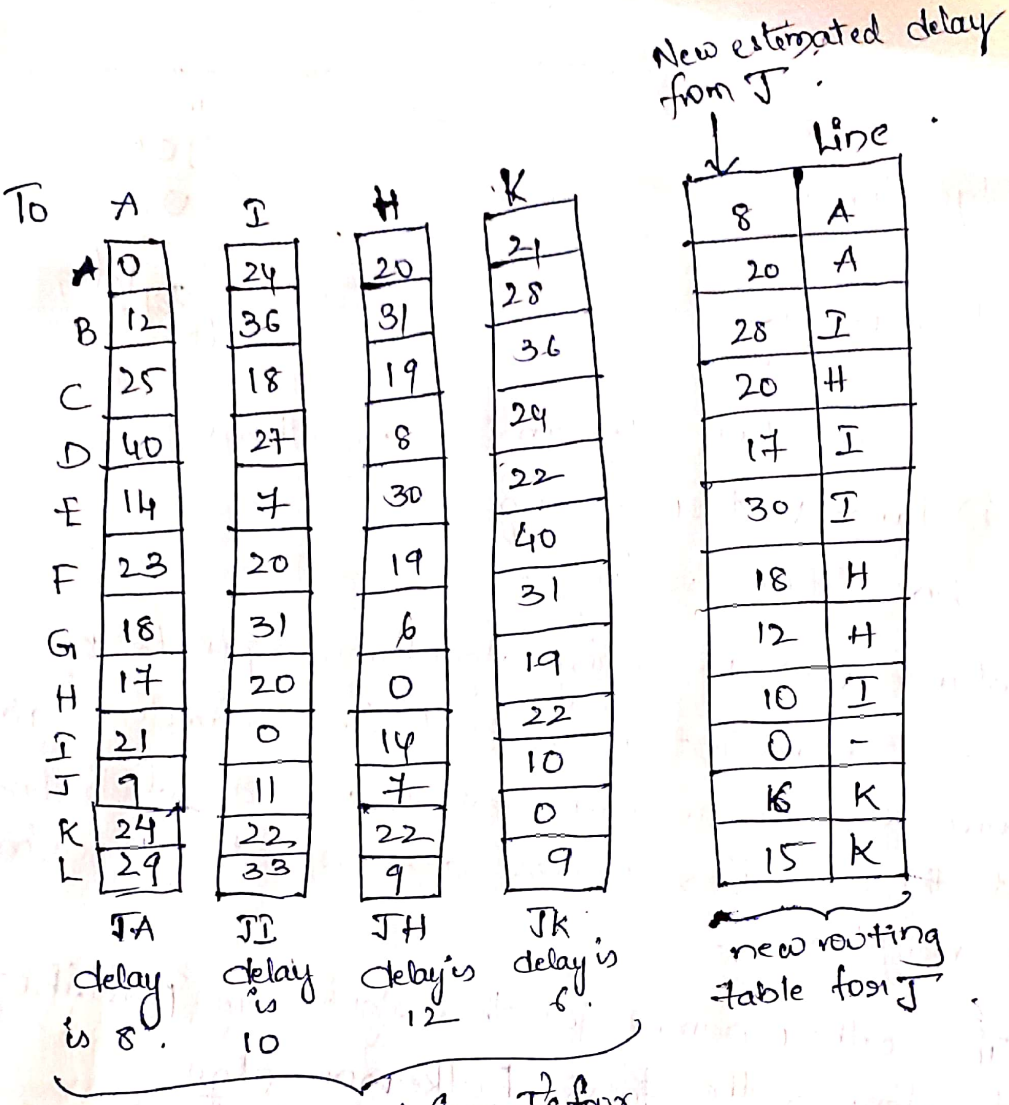


fig: I/P from A, I, H, K and the new routing table for J.

(b)

Consider how J computes its new route to router G. It knows that it can get to A in 8 msec, and A claims to be able to get to G in 18 msec, so J knows it can count on a delay of 26 msec to G if it forwards packets bound for G to A. Ily, it computes the delay to G via I, H, K as 41 (31+10), 18 (6+12), & 37 (31+6) msec, respectively. Best of these values is 18, so it makes an entry in its routing table that the delay to G is 18 msec. & that route to use is via H.

Subject: CN
Faculty: N.SHIRISHA
Topic: Routing Algorithms

Class Notes

Unit No : III
Lecture No : L01
Link to Session: 32
Planner (SP) :
Book Reference : T1
Date Conducted : 09/8/21
Page No: 5

The Count-to-Infinity Problem:

Consider the five-node (linear) subnet, where the delay metric is the no. of hops. Suppose A is down initially and all the other routers know this.

A	B	C	D	E	
•	•	•	•	•	Initially
1	•	•	•	•	After 1 exch.
1	2	•	•	•	After 2 exch.
1	2	3	•	•	After 3 exch.
1	2	3	4	•	After 4 exch.

(a)

A	B	C	D	E	
1	2	3	4		Initially
3	2	3	4		After 1 exch.
3	4	3	4		" 2 "
5	4	5	4		" 3 exc.
5	6	5	6		" 4 exc.
7	6	7	6		After 5 exch.
7	8	7	8		" 6 exch.
.	.	.	.		
.	.	.	.		
.	.	.	.		

(b)

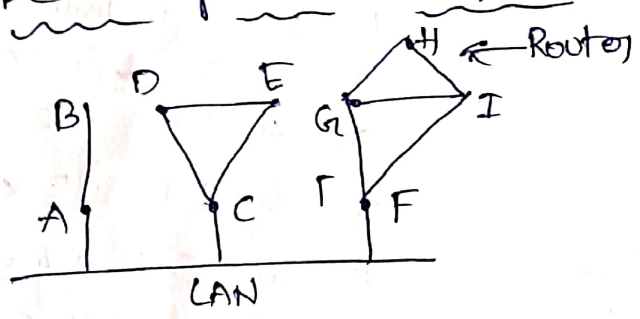
From this figure, it should be clear why bad news travels slowly: no router ever has a value more than one higher than the minimum of all its neighbours. Gradually, all routers work their way up to infinity, but the no. of exchanges required depends on the numerical value used for infinity. This problem is known as Count-to-Infinity problem.

Link State Routing:

Each router must do the following:

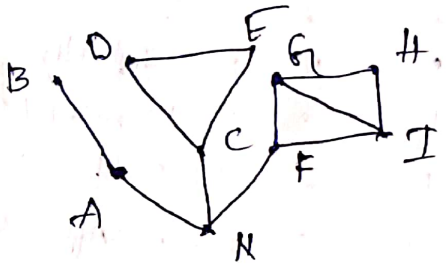
1. Discover its neighbors and learn their n/w addresses.
2. Measure the delay or cost to each of its neighbors.
3. Construct a packet telling all it has just learned.
4. Send this packet to all other routers.
5. Compute the shortest path to every other router.

Learning about Neighbors:



(a)

Nine routers & a LAN.

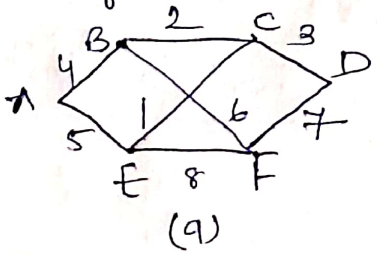


(b)

A graph model of (a).

Building Link state Packets

Once the info. needed for the exchange has been collected, the next step is for each router to build a packet containing all the data. The packet starts with the identity of the sender, followed by a sequence no. & age & a list of neighbors.



(a)

A Subnet

A
Seq.
Age
B 4
E 5

Link State Packets	
B	
Seq.	
Age	
A	4
C	2
F	6

C
Seq.
Age
B 2
D 3
E 1

D
Seq.
Age
C 3
F 7

E
Seq.
Age
A 5
C 1
E 8

F
Seq.
Age
B 6
D 4
E 8

(b)

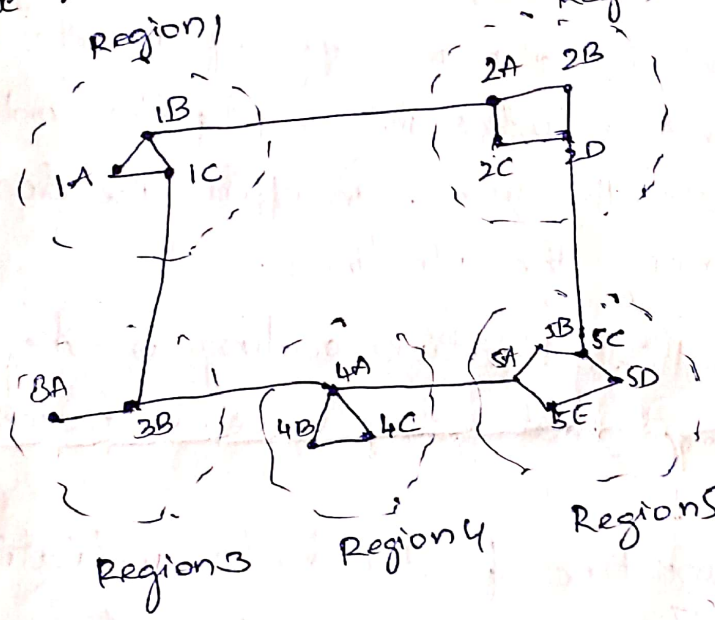
The link state packets for this Subnet.

Subject: CN
Faculty: N.SHIRISHA
Topic: Hierarchical Routing :

Class Notes

Unit No : II
Lecture No : 16
Link to Session:
Planner (SP) :
Book Reference : T1
Date Conducted : 13/09/13/5
Page No: 6

At a certain point the n/w may grow to the point where it is no longer feasible for every router to have an entry for every other router, so the routing will have to be done hierarchically. Here, the routers are divided into what we will call regions.



(a)

Full table for 1A.

Dest	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hiera. table for 1A

Dest.	line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	3
4	1C	3
5	1C	4

(c)

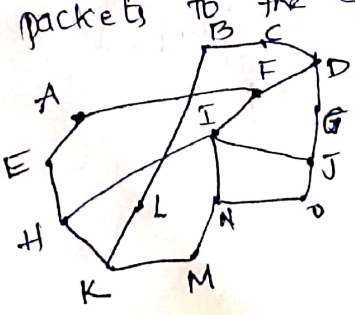
Broadcast Routing :

Sending a packet to all destinations simultaneously is called broadcasting.

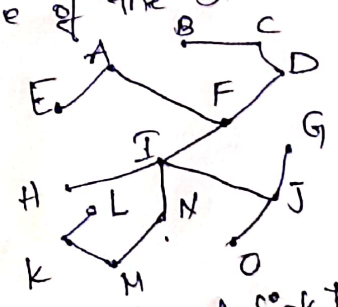
- ① Broadcasting – Least desirable of the methods.
- ② Flooding – It generates too many packets & consumes too much bandwidth.
- ③ Multidestination routing – Each packet contains either a list of destinations or a bitmap indicating the desired dest. The router generates a new copy of packets for each o/p line to be used and includes in each packet only those dest. that are to use the line. In effect, the destination set is partitioned among the o/p lines.

Multidestination routing is like separately addressed packets, except that when several packets must follow the same route.

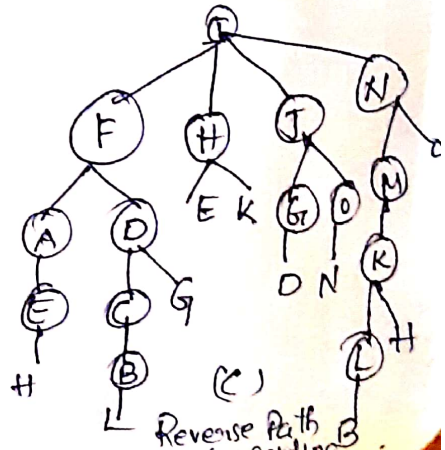
- ④ Explicit use of Sink tree for the router initiating the broadcast. The only problem that each router must have knowledge of some spanning tree for the method to be applicable.
- ⑤ Reverse path forwarding : When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast.



(a) A Subnet.



(b) A Sink tree



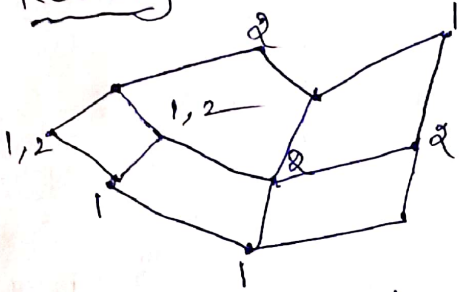
(c) Reverse path forwarding.

Subject: CN
Faculty: N.SHIRISHA
Topic: Multi Cast Routing :

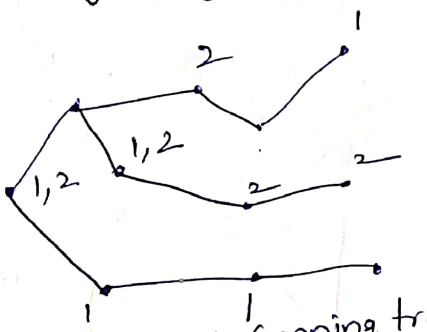
Class Notes

Unit No : III
Lecture No : L31
Link to Session: 33
Planner (SP) :
Book Reference : T1
Date Conducted : 2/8/19
Page No: 7

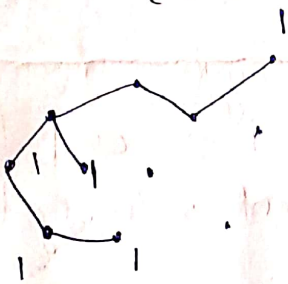
Sending a message to such a group is called where we need to send messages to well-defined groups that are numerically large in size but small compared to the n/w as a whole. is called Multicasting & its routing algo. is called Multicast Routing



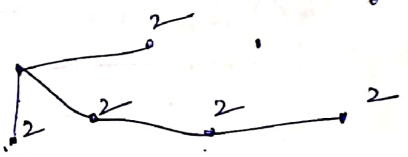
(a) A network



(b) A spanning tree for the leftmost router.



(c) A multicast tree for group 1



(d) A multicast tree for group 2

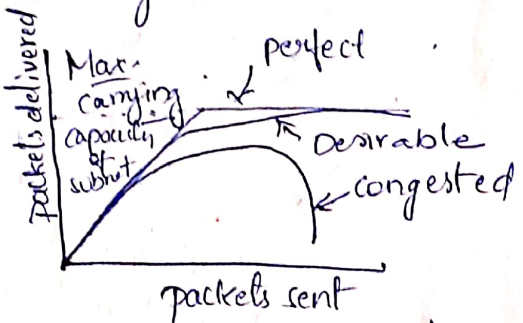
To do multicast routing, each router computes a spanning tree covering all other routers. (a) has two groups. 1 and 2. some routers are attached to hosts that belong to one or both of these groups. A spanning tree for the leftmost router is shown in (b).

When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group. Multicast packets are forwarded only along the appropriate spanning tree.

Various ways of pruning the spanning tree are possible. The simplest one can be used if link state routing is used.

Congestion Control Algorithms:

When too many packets are present in the subnet, performance degrades. This situation is called congestion.



Congestion can be brought on by several factors.

① If all of a sudden, streams of packets begin arriving on three or four input lines and all need the same output line, a queue will build up. If there is insufficient memory to hold all of them, packets will be lost.

② Slow processors can also cause congestion. If the routers' CPU are slow at performing the tasks, queues can build up, even though there is excess line capacity. Similarly, low bandwidth lines can also cause congestion.

General principles of congestion Control:

In Control theory pt. of view, this approach leads to dividing all solutions into two groups: open loop and closed loop.

Subject: CN
Faculty: N.SHIRISHA
Topic: Congestion Control

Class Notes

Unit No : III
Lecture No : 18
Link to Session:
Planner (SP) : 057
Book Reference : T1
Date Conducted : 3/5/21
Page No: 8

- In open loop, solutions to the problems are made by good design. They make decisions without regard to the current state of the network.
- In contrast, closed loop solns are based on the concept of a feedback loop.
  - → Monitor the system to detect when and where congestion occurs.
  - → pass this info. to places where action can be taken.
  - → Adjust system op. to correct the problem.

Congestion prevention policies:

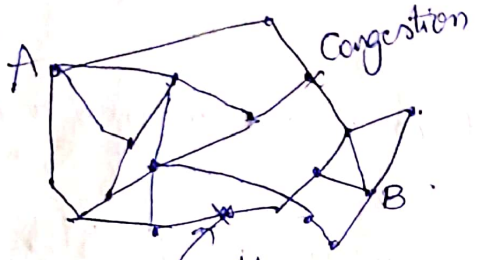
Layer	Policies
Transport	• Retransmission policy. • Out-of-order caching policy. • Acknowledgement policy. • Flow control policy. • Time out determination.
Network	• Virtual circuits Vs. datagram inside the Subnet. • packet queueing and service policy. • packet discard policy. • Routing algo. • Packet lifetime management.
Data link	• Retransmission policy. • Out-of-order caching policy. • Acknowledgement policy. • Flow control policy.

Fig: Policies that affect congestion.

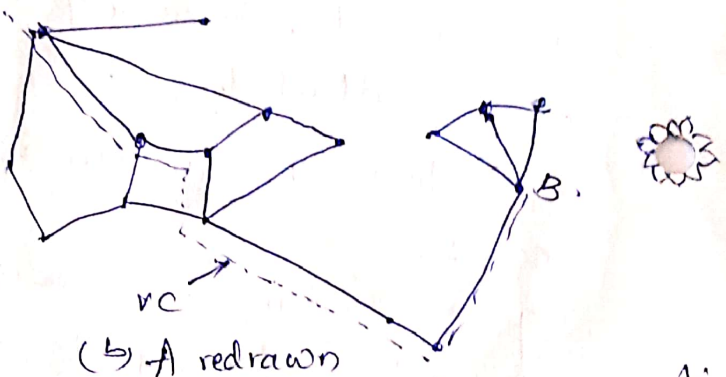
Congestion-control in Virtual-circuit Subnet:

① Congestion can be prevented by admission control: once congestion has been signaled, no more virtual circuits are setup until the problem has gone away.

② An alternative approach is to allow new VC to sail carefully route all new VC's around problem areas.



(a) A congested Subnet



(b) A redrawn Subnet that eliminates the congestion. A new VC from A to B is shown.

Congestion Control in Datagram Subnet:

Each routers can easily monitor the utilization of its o/p lines and other resources. For Eg., it can associate with each line a real variable, u, whose value, b/w 0.0 and 1.0, reflects the recent utilization of that line, a sample of inst. line f is 0 & 1.

$$u_{new} = au_{old} + (1-a)f$$

where the constant a determines how fast the routers forgets recent history.

Choke Packets: The router sends a choke packet back to the source host, giving it the dest. found in the packet.

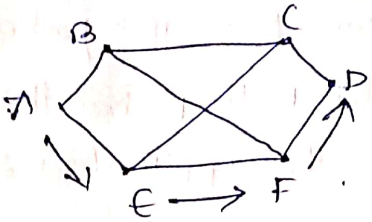
- When the source host gets the choke pack., it is required to reduce the traffic sent to the specified destination by X percent.

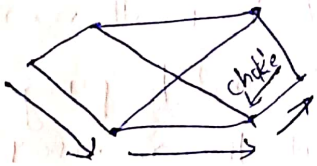
Subject: CN
Faculty: N.SHIRISHA
Topic: Congestion control (contd..)

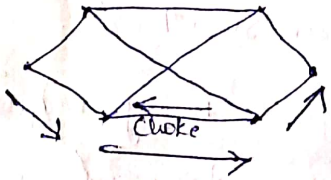
Class Notes

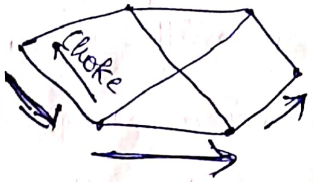
Unit No : III
Lecture No : L04
Link to Session:
Planner (SP) : 05
Book Reference : T1
Date Conducted : 03/09/21
Page No: 9

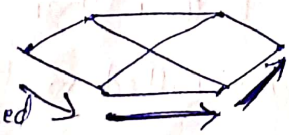
Hop-by-Hop Choke packets :



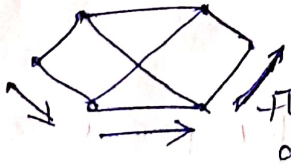




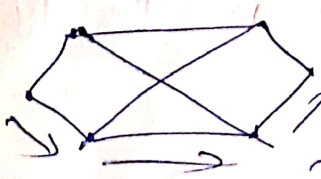




Reduced flow.



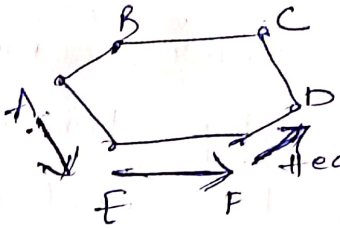
Flow is still at max. rate



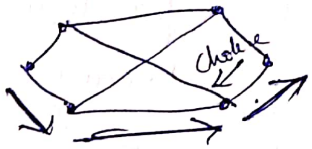
flow is reduced

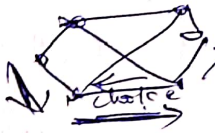
(a)

A choke pack. that effects only the source.

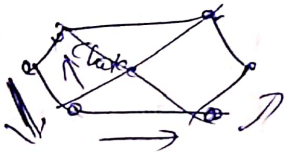


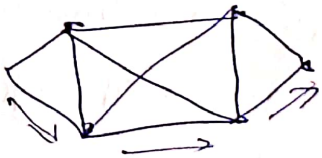
Heavy flow.





Reduced flow





(b)

A choke packet that effects each hop it passes through.

Load Shedding :

Load shedding is a fancy way of saying that when routers are being inundated by packets that they cannot handle, they just throw them away.

A router drowning in packets can just pick packets at random to drop, but usually it can do better that that. Which packet to discard may depend on the applications running. For file transfer, an old packet is worth more than a new one because dropping packet 6 and keeping packets 7 through 10 will cause a gap at the receiver that may force packets 6 through 10 to be retransmitted.

In a 12-packet file, dropping 6 may require 7 through 12 to be retransmitted, where as dropping 10 may require only 10 through 12 to be retransmitted. In Contrast, for multimedia, a new packet is more important than a old one. The former policy ('old is better than new') is often called wine & the latter is often called milk.

Random Early Detection :

Discarding packets before all the buffer space is really exhausted. A popular algo. for doing this is called RED (Random Early Detection).

Subject: CN
Faculty: N.SHIRISHA
Topic: Congestion Control Algorithms: (contd.)

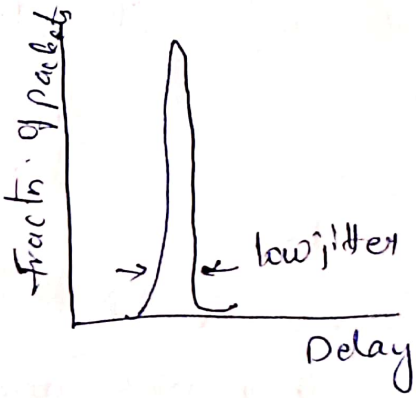
Class Notes

Unit No : IV
Lecture No : 104
Link to Session:
Planner (SP) : 084
Book Reference : T1
Date Conducted : ~~29.09.21~~ 15.01
Page No: 10

Jitter Control:

For applications such as audio and video streaming, it does not matter much if the packets take 20msec or 30msec to be delivered, as long as the transit time is constant. The variation in the packet arrival time is called the Jitter.

(a) High Jitter.



The jitter can be bounded by computing the expected transit time for each hop along the path. When a packet arrives at a router, the router checks to see how much the packet is behind or ahead of its schedule. This info is stored in the packet and updated at each hop.

Internetworking :

Two or more networks are connected to form an internet.

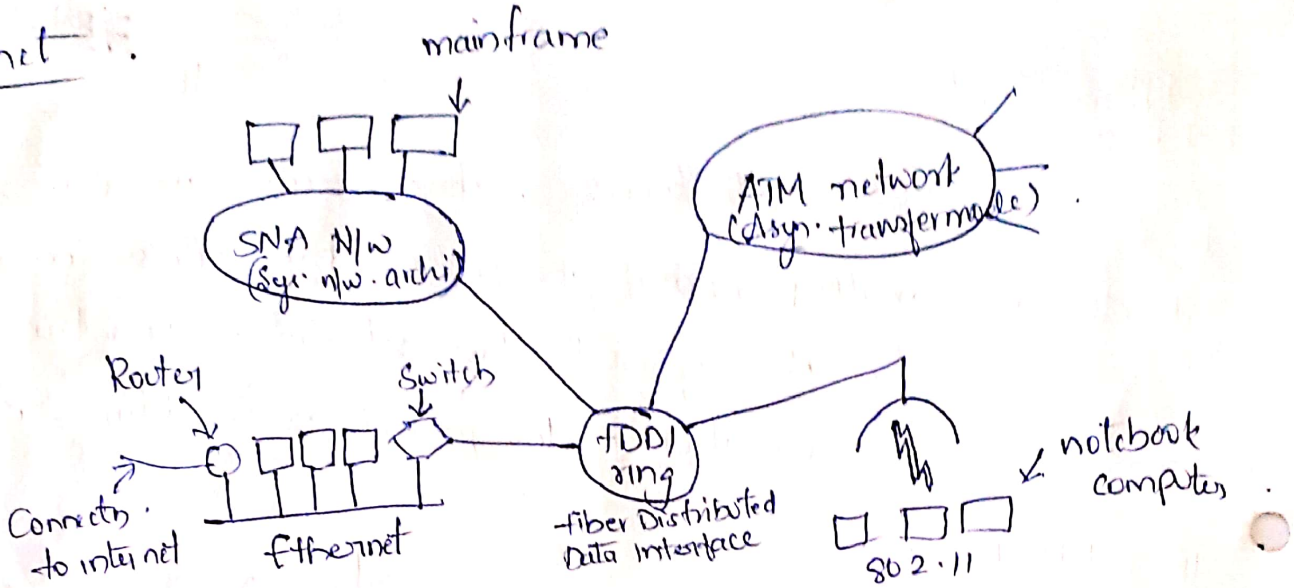


fig: A collection of interconnected n/w's.

The purpose of interconnecting all these networks is to allow users on any of them to communicate with users on all the other ones and also to allow users on any of them to access data on any of them. Accomplishing this goal means sending packets from one network to another. Since n/w often differ in important ways, getting packets from one network to another is not always so easy.

How N/w Differs: Item	Some Possibilities
Service offered	- Conn. oriented versus connectionless
Protocols	- IP, IPX, SNA, ATM, MPLS, AppleTalk etc.,
Addressing	- Flat (802) versus hierarchical (IP)
Multicasting	- Present or absent (also broadcasting)
Packet size	- Every n/w has its own maximum
Quality of Service	- Present or absent; many diff. kinds
Error handling	- Reliable, ordered, and unordered delivery
Flow control	- Sliding window, rate control, other
Congestion control	- Leaky bucket, token bucket, RED, Choke etc.

Subject: CN
Faculty: N.SHIRISHA
Topic: Internetworking :

Class Notes

Unit No : II
Lecture No : L07
Link to Session: ~~08~~ 7
Planner (SP) :
Book Reference : T1
Date Conducted : 16/09/21
Page No: 11

How Networks can be connected :

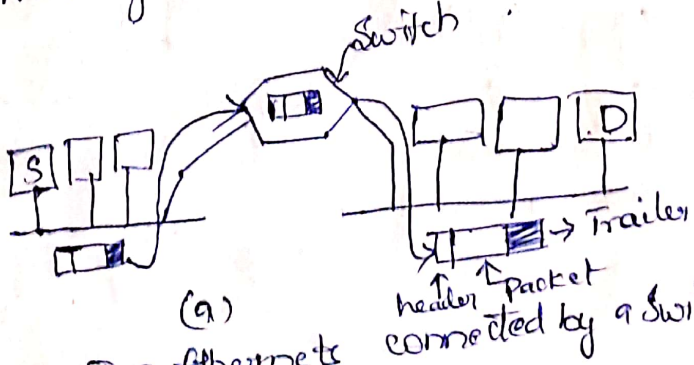
In physical layer, n/w's can be connected by repeaters or hubs, which move the bits from one n/w to an identical n/w.

In data link layer, we find bridges, switches, which operate at the data link layer. They can accept frames, examine the MAC addresses, & forward the frames to a different n/w while doing minor protocol translation in the process, from Ethernet to FDDI or to 802.11.

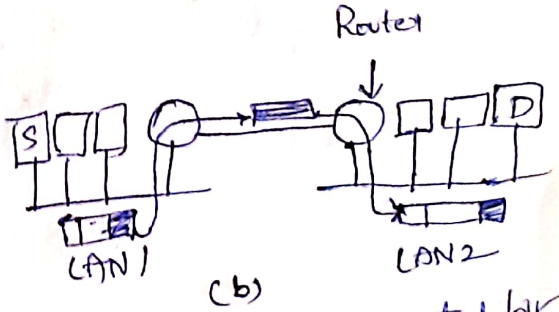
In n/w layer, routers can connect two n/w's. A router that can handle multiple protocols is called a multiprotocol router.

In transport layer we find transport gateways, which can interface b/w two transport connections.

Finally, in application layer, appl gateways translate message semantics.



(a) Two Ethernets connected by a switch



(b) Two Ethernets connected by routers.

Concatenated Virtual Circuits :

Two styles of internetworking are possible :

① a Connection-oriented concatenation of V-C subnets,

② a datagram internet style.

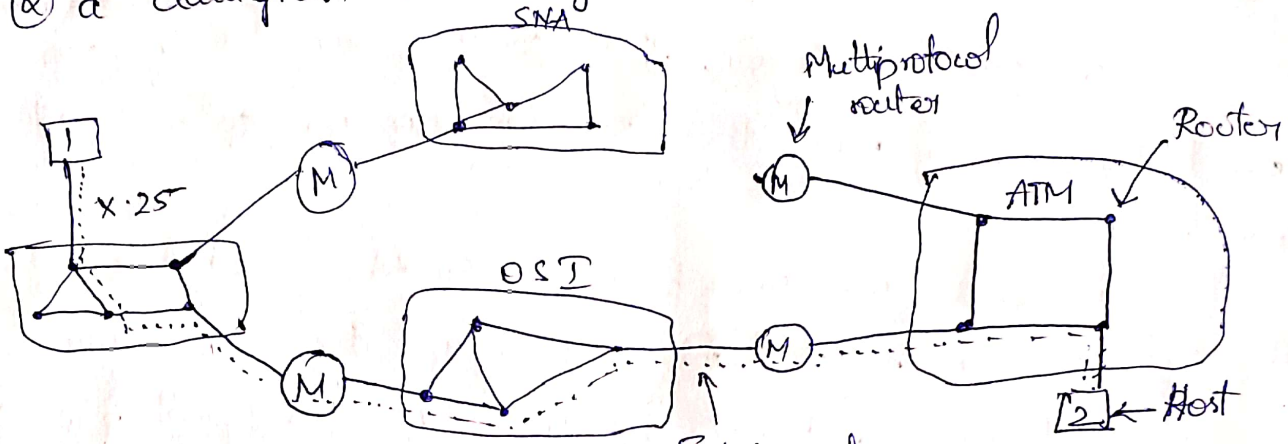


fig: Internetworking using concatenated VC.

Connectionless Internetworking :

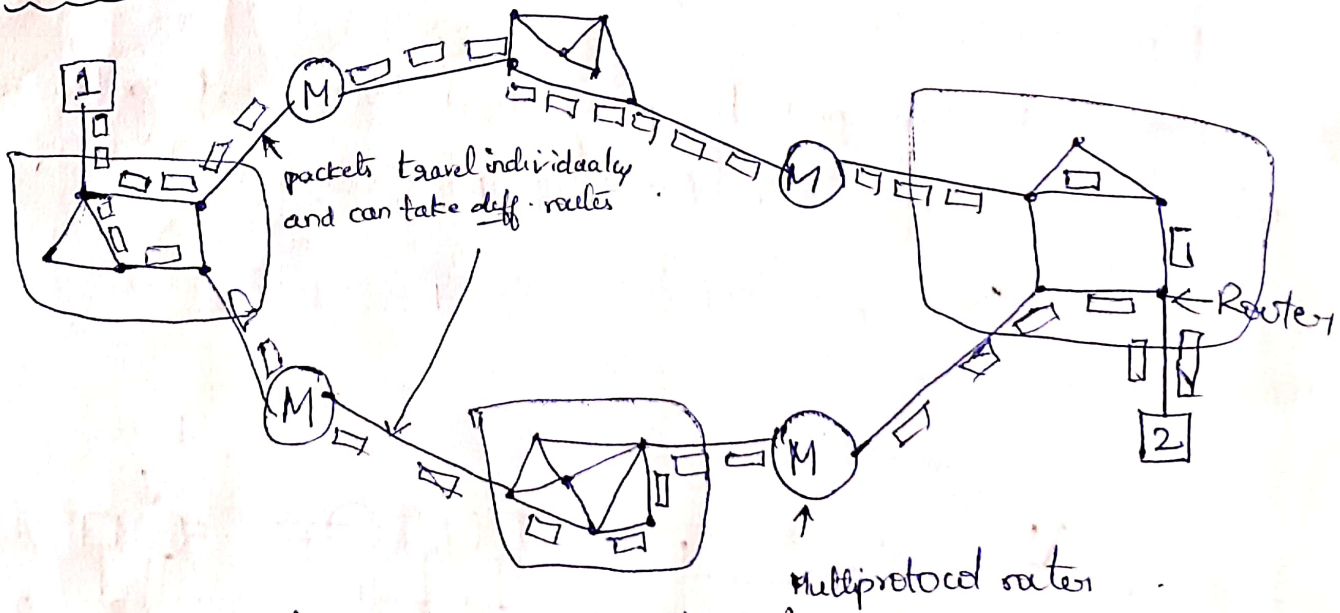


fig: A Connectionless internet.

Subject: CN
Faculty: N.SHIRISHA
Topic: Internetworking

Class Notes

Unit No: IV
Lecture No: L37
Link to Session
Planner (SP): S.No.... of SP
Book Reference: T1
Date Conducted: 14/5/21
Page No: 12

Tunneling :

Handling the general case of making two diff. n/w's internetwork is exceedingly difficult. The source and destination are on the same type of n/w, but there is a diff. n/w in b/w.

Eg: International bank with a TCP/IP based Ethernet in paris,
a TCP/IP based Ethernet in london,
a non-IP wide area n/w in bw.

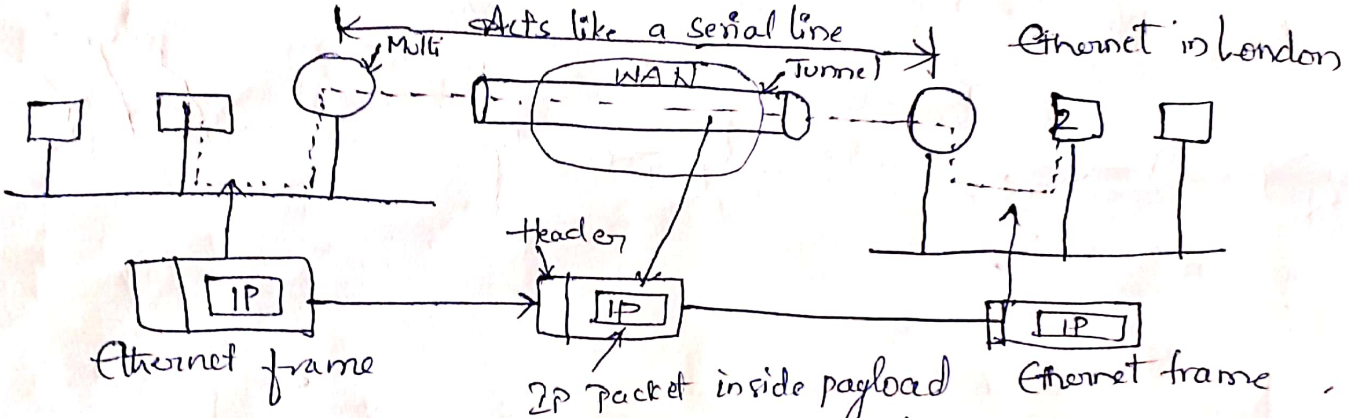


fig: Tunneling a packet from paris to london.

Solution to this problem is a technique called tunneling

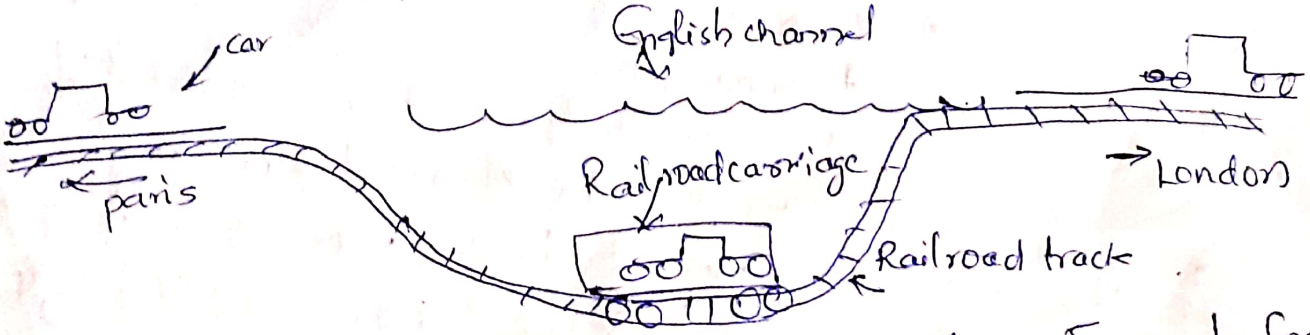
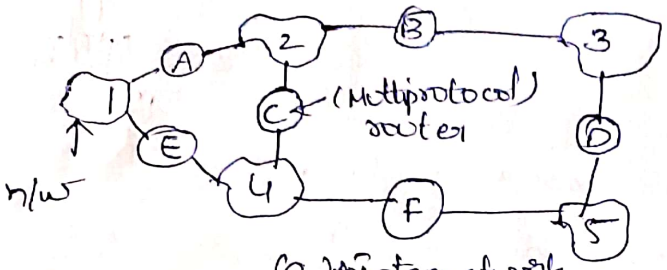
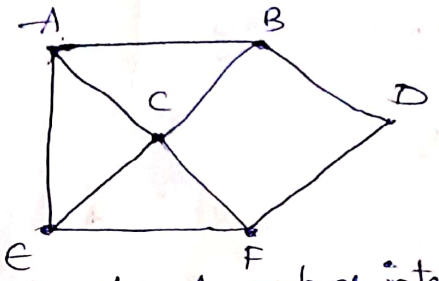


fig:- Tunneling a car from France to England

Internetwork routing :



(a) An internetwork



(b) A graph of intern/w.

Once the graph has been constructed, such as distance vector and link state algo., can be applied to the set of multiprotocol routers. This gives a two-level routing algo; within each n/w an interior gateway protocol is used, but btw the n/ws, an exterior gateway protocol is used.

Because each n/w in an intern/w is independent of all the others, it is often referred to as an Autonomous system (AS).

Fragmentation :

Each n/w imposes some max. size on its packets. These limits have various causes :

1. Hardware
2. OS
3. protocols
4. Compliance with some (International) standard.
5. Desire to reduce ckt-induced retransmissions to some level.
6. Desire to prevent one packet from occupying the channel too long.

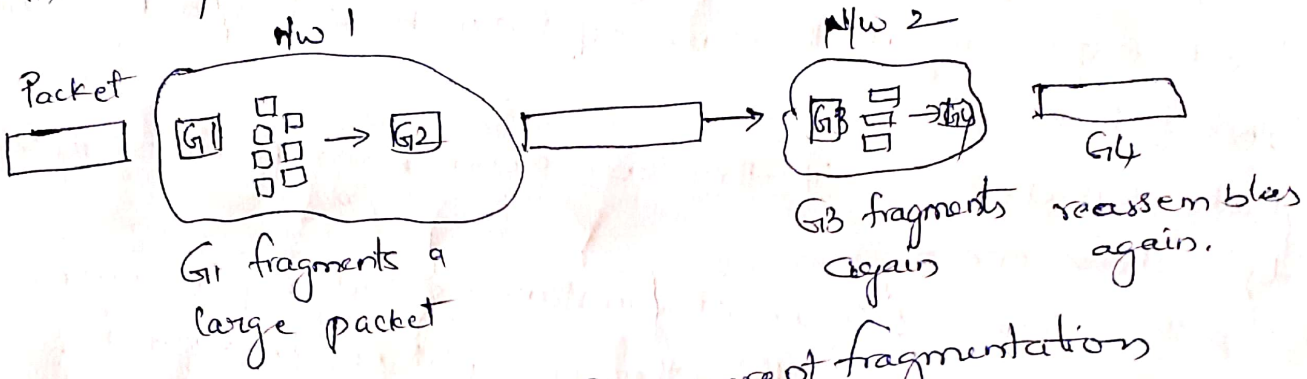
So, Ntw designers cannot choose max. size of packet. Max. payloads range from 48 bytes (ATM cells) to 65,515 bytes (IP packets), although the payload size in higher layers is often larger.

Subject: CN
Faculty: N.SHIRISHA
Topic: Internetworking (Contd..)

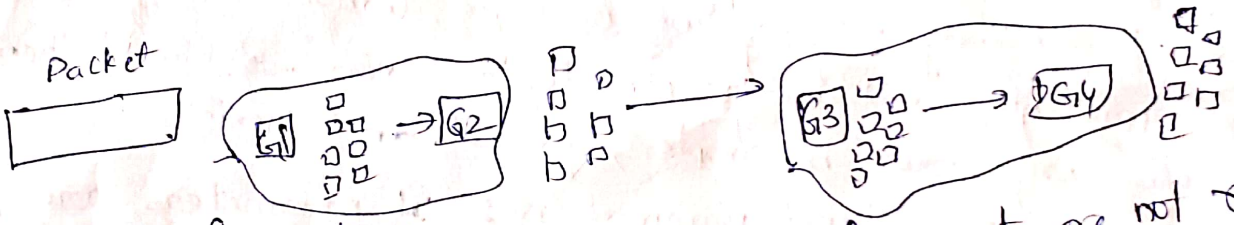
Class Notes

Unit No: II
Lecture No: L36 & 37
Link to Session: 36 & 37
Planner (SP): S.No.... of SP
Book Reference: T1
Date Conducted: 14/9/21
Page No: 13

Basically, the only solution to the problem is to allow gateways to breakup packets into fragments, sending each fragment as a separate internet packet.



(a) Transparent fragmentation



(b)
Non-transparent fragmentation.

The network Layer in the internet :

The Principles that drove its design in the past and made it the success today.

① Make sure it works : Do not finalize the design or standard until multiple prototypes have successfully communicated with each other.

② keep it simple : If a feature is not absolutely essential, leave it out, especially if the same effect can be achieved by combining other feature.

③ Make clear choices : If there are several ways of doing the same thing, choose one.

④ Exploit modularity : If the circumstances that require one module or layer to be changed, the other ones will not be affected.

⑤ Expect heterogenity : Diff types of h/w's, transmission facilities, and applications will occur on any large n/w. To handle them, the n/w design must be simple, general and flexible.

⑥ Avoid static options and parameters : If parameters are unavoidable, it is best to have the sender and receiver negotiate a value than defining fixed choices.

⑦ Look for a good design ; it need not be perfect : Rather than messing up the design, the designers should go with the good design and put the burden of working around it on the people with the strange requirements.

⑧ Be strict when sending and tolerant when receiving : Only send packets that rigorously comply with the standards, but expect incoming packets that may not be fully conformant and try to deal with them.

⑨ Think about Salability :- If the system is to handle millions of hosts and billions of users effectively, no centralized databases of any kind are tolerable & load must be spread as evenly as possible over the available resources.

⑩ consider performance and cost : If a ntw has poor performance, no one will use it.

Subject: CN
Faculty: N.SHIRISHA
Topic: The Network layer in the Internet;

Class Notes

Unit No: III
Lecture No: L8
Link to Session 38
Planner (SP): S.No.... of SP
Book Reference: T1
Date Conducted: 18/3/21
Page No: 14

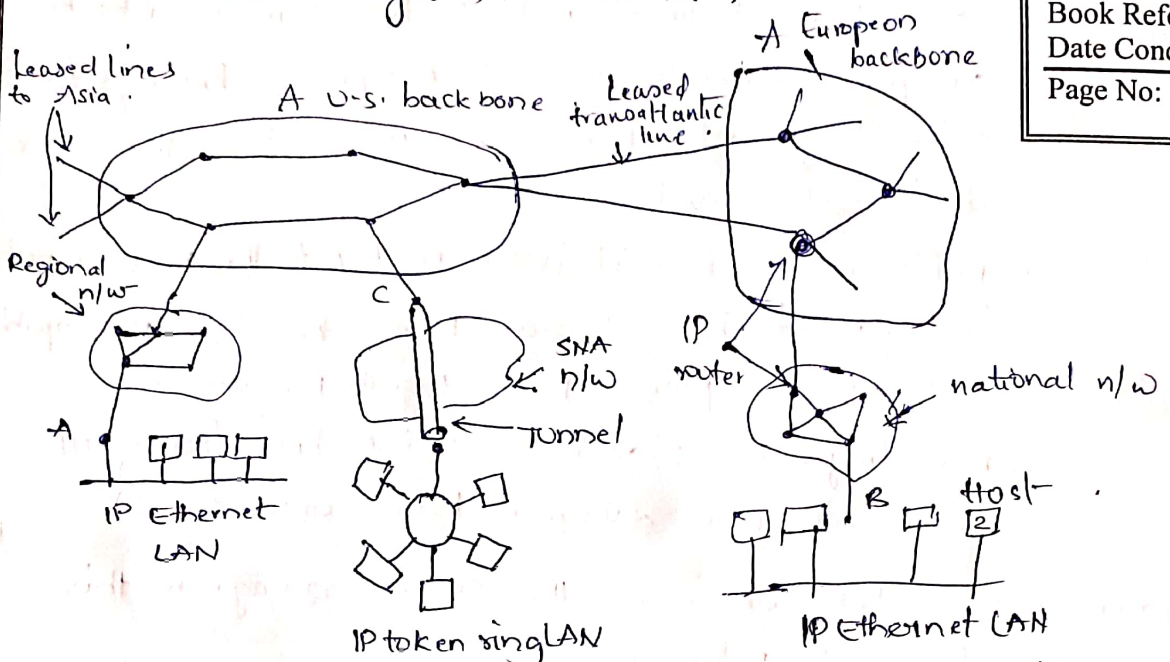


fig: The internet is an interconnected collection of many n/w's.

The IP Protocol:

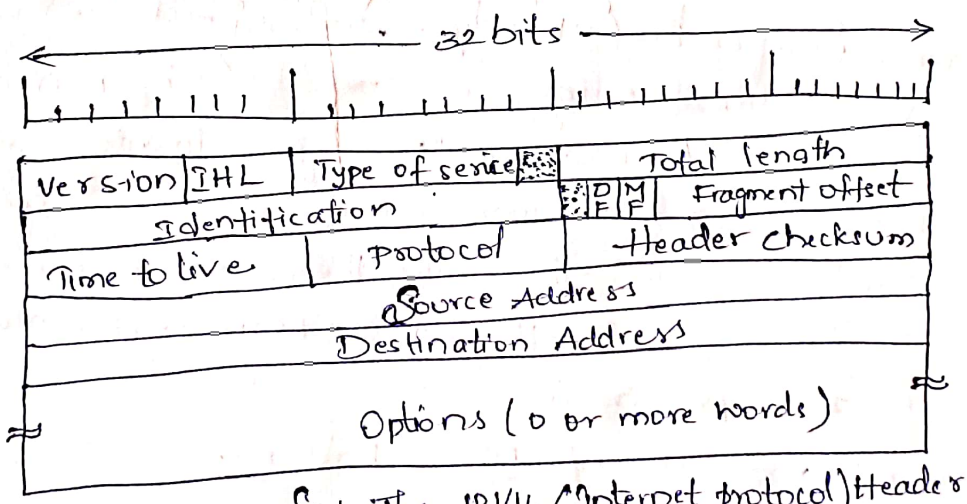


fig: The IPV4 (Internet protocol) Header.

Version : keeps track of which version of the protocol the datagram belongs to.

IHL : header length; to tell how long the header is, in 32-bit words
Min. is 5, which applies when no options are present.
Max. value of this 4-bit field is 15, which limits the header to 60 bytes, thus options field to 40 bytes.

Type of Service: To distinguish diff' classes of service.
Originally, a 6 bit field contained, a three bit precedence & three flags, D, T, R - Delay, Throughput, Reliability.

- Total length : Includes - both header and data max. length is 65,535 bytes.

- Identification : To Allow destination host to determine which datagram a newly arrived fragment belongs to. All the fragments of a datagram contain the same identification value.

- DF : Don't fragment ; It is an order to the routers not to fragment the datagram b'coz the dest. is incapable of putting the pieces back together again.

- MF : More fragments ; It is needed to know when all fragments of a datagram have arrived.

- The fragment offset : tells where in the current datagram this fragment belongs.

- Time to live : It is a counter used to limit packet lifetimes.

- Protocol : Which transport process to give it to ; TCP or UDP.

- Header checksum : Verifies header only. Such a checksum is useful for detecting errors generated by bad memory words inside a router. The algo. is to add up all the 16-bit halfwords as they arrive, using one's complement arithmetic and then take the one's complement of the result. So, Header checksum is assumed to be zero upon arrival.

- Source & Dest. addr. ; indicate n/w no. & host no.

- Option :-

Option	Security :
Security	specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed.
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address & timestamp.

The Network layer in the Internet (contd..)

IPV6 :

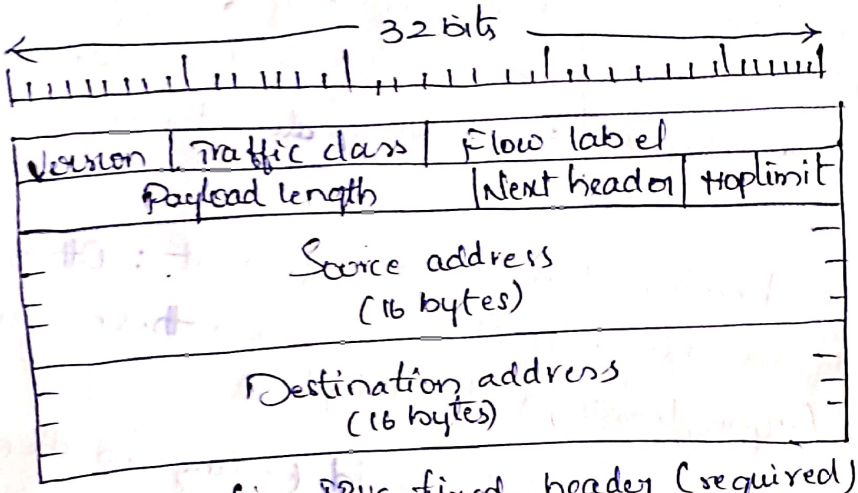


fig: IPV6 fixed header (required).

Version :- is always 6 for IPv6 & 4 for IPV4.

Traffic class : To distinguish packets with different real-time delivery requirements.

flowlabel : To allow a source and destination to setup a pseudoconnection with particular properties and requirements of them.

payload length : Tells how many bytes follow the 40-byte header. Name was changed from IPV4 total length field.

Next header field : Which of the (currently) six extension headers, if any, follow this one. If this is the last IP header, the Next header field tells which transport protocol handler to pass the packet to.

- The Hop limit field : To keep packets from living forever. Same as Time to live field in IPV4. , a field that is decremented on each hop.

Source & Dest address :- They are written as eight groups of four hexadecimal digits with colons b/w groups: 8000:0000:0000:0000:0123:4567:89AB:CDEF.

Extension Headers :

Extension header	Description
Hop-by-hop options	Miscellaneous info. for routers
Destination options	Additional info. for the dest.
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender's identity.
Encrypted security payload	Information about the encrypted contents.

Some of the headers have a fixed format : Others contain a variable no. of variable-length fields. For these, each item is encoded as a (type, length, value) tuple.

The type is a 1-bytes field telling which option this is. The type values have been chosen so that the first 2 bits tell routers that do not know how to process the option what to do. The choices are : skip the option; discard the packet; discard the packet and send back an ICMP packet;

The length is also a 1-byte field. It tells how long the value is (0-255 bytes). The value is any info. req., up to 255 bytes.

Quality of Service :

Requirements :

A stream of packets from a source to a destination is called a flow. In a connection-oriented n/w, all the packets belonging to a flow follow the same route;

In connectionless n/w, they may follow diff. routes.

The needs of each flow can be characterized by four primary parameters : ① reliability ② delay ③ jitter ④ bandwidth.

Subject: CN
Faculty: N.SHIRISHA
Topic: Network Layer in the internet

Class Notes

Unit No: III
Lecture No: L38
Link to Session 38
Planner (SP): S.No.... of SP
Book Reference: T1
Date Conducted: 18/4/21
Page No: 15

IP Adresses :

Every host and routers on the internet has an IP address, which encodes its n/w no. & host no. No two m/c's on the internet have the same IP address.

All IP addresses are 32 bits long and are used in the Source address and Destination address fields of IP packets.

IP addresses are divided into the five categories called classful addressing.

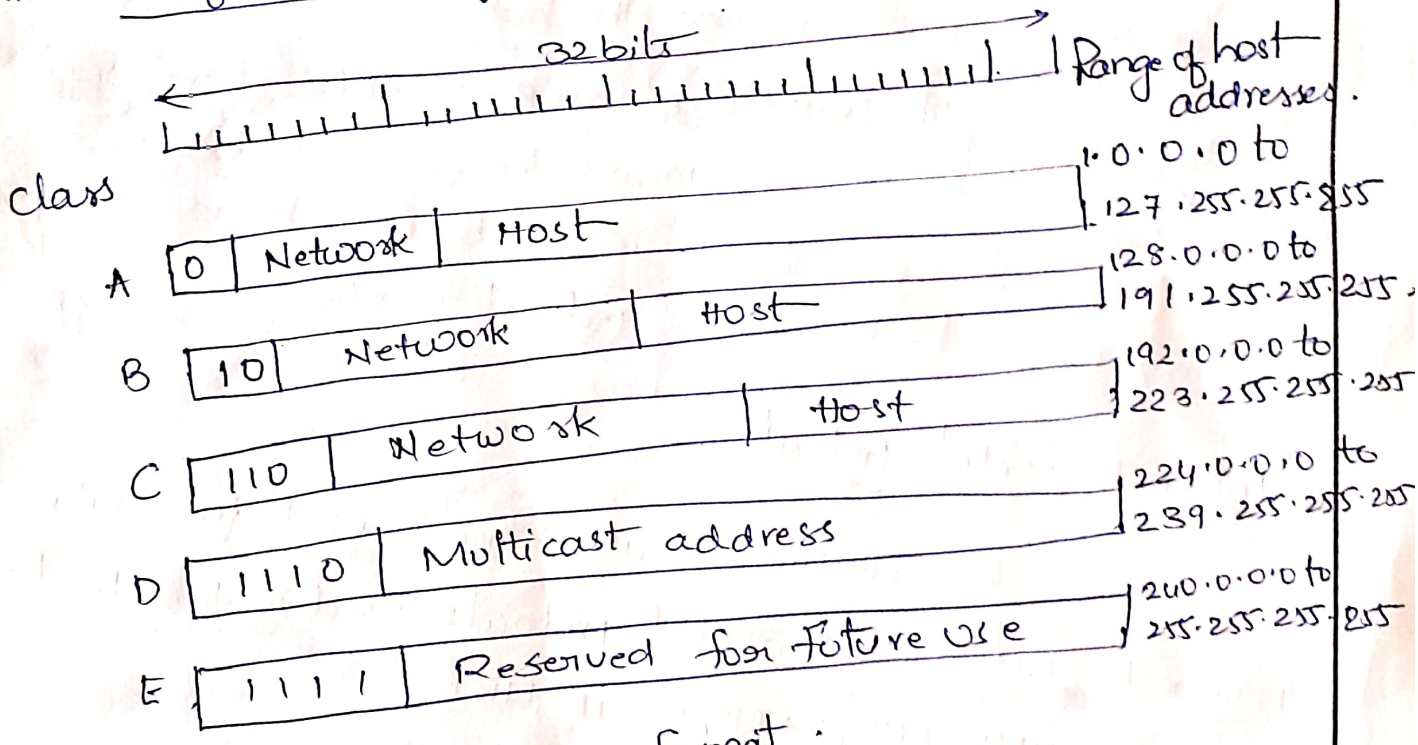


fig: IP address format.

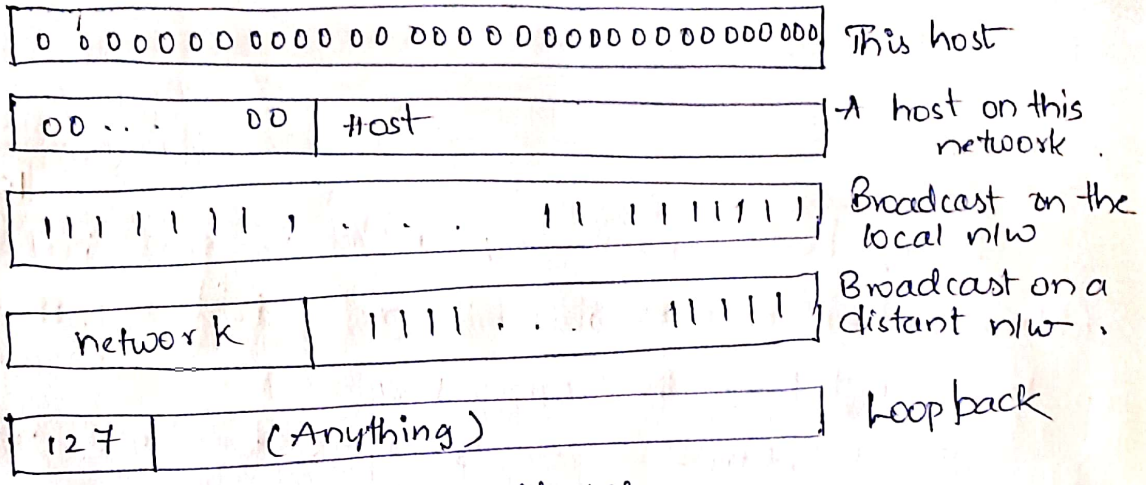


fig: Special IP addresses.

Network addresses, which are 32-bit numbers, are usually written in dotted decimal notation. Each of 4 bytes is written in decimal, from 0 to 255. The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255.

The values 0 and -1 (all 1s) have special meanings. The value 0 means this n/w or this host. The value -1 is used as a broad-cast address to mean all hosts on the indicated n/w.

Internet Control Protocols:

In addition to IP, which is used for data transfer, the internet has several control protocols used in the n/w layer, including ICMP, ARP, RARP, BOOTP, DHCP.

ICMP (Internet Control Message Protocol)

When some thing unexpected occurs, the event is reported by the ICMP, which is also used to test the Internet

Subject: CN
Faculty: N.SHIRISHA
Topic: ICMP (The n/w layer in the internet) cont'd..

Class Notes

Unit No: III
Lecture No: L38
Link to Session 38
Planner (SP): S.No.... of SP
Book Reference: T1
Date Conducted: 18/9/21
Page No: 16

Message type	Description
- Destination unreachable	Packet could not be delivered
- Time exceeded	Time to live field hit 0.
- Parameter problem	Invalid header field
- Source quench	Choke packet
- Redirect	Teach a router about geography
- Echo	Ask a m/c if it is alive
- Echo reply	Yes, I am alive
- Timestamp request	Same as Echo request, but with timestamp
- Timestamp reply	" reply, "

fig: The principal ICMP Msg types.

- Dest. Unreachable: It is used when the subnet or a router cannot locate the destination or when a packet with the DF bit cannot be delivered because a "small-packet" n/w stands in a way.

- The Time Exceeded: Message is sent when a packet is dropped b'coz its counter has reached zero. This event is a symptom that packets are looping, that there is enormous congestion, or that the timer values are being set too low.

- The Parameter Problem: - It indicates that an illegal value has been detected in the header field.

- The Source Quench - When a host received this message, it was expected to slow down.

The Redirect – It is used when a router notices that a packet seems to be routed wrong.

Echo and Echo reply – used to see if a given destination is reachable and alive.

ARP – The Address Resolution Protocol.

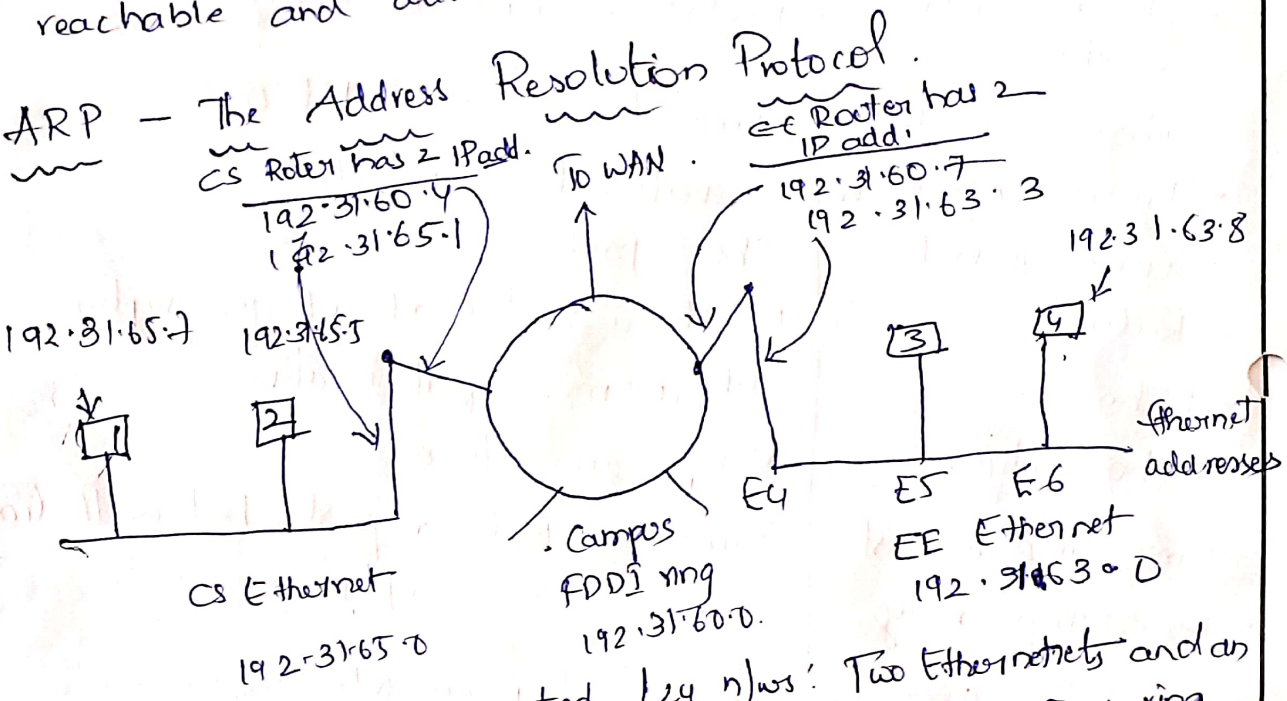


fig: three interconnected /24 n/ws: Two Ethernets and an FDDI ring.

The IP addresses get mapped onto dll addresses, such as Ethernet.

For Eg: A Small University with several Class C n/ws. Here we have two Ethernets, one in the Computer Science Dept., with IP address 192.31.65.0 and one in Electrical Eng., with IP addr. 192.31.63.0. These are connected by a campus backbone ring with IP address 192.31.60.0. Each m/c on an Ethernet has a unique Ethernet address, labeled E1 through E6, and each m/c on the FDDI ring has an FDDI address, labeled F1 through F3.

Subject: CN
Faculty: N.SHIRISHA
Topic: ARP

Class Notes

Unit No: III
Lecture No: 27
Link to Session
Planner (SP): S No: 28 of SP
Book Reference: T1
Date Conducted: 12/5/21
Page No: 17

The host 1 sends a packet to a user on host 2. The sender knows the name of the intended receiver as mary@eagle.cs.uni.edu.
- The first step is to find the IP address for host 2, DNS returns for host 2 (192.31.65.5) in the Destination address field & gives it to the IP software to transmit. This is called Address resolution protocol.

RARP, BOOTP and DHCP

If we need to find IP address when Ethernet address is given. The first solution devised was to use RARP (Reverse Address Resolution protocol).

The disadvantages of RARP is that it uses a dest. address of all 1's (limited broadcasting) to reach RARP server. Such broadcasts are not frwarded by raters, so a RARP server is needed on each n/w. So, An alternative approach called BOOTP was invented.

But Bootp requires manual configuration of tables mapping IP add. to Ethernet address. When a new host is added to a LAN, it cannot use BOOTP until an admin. has assigned it an IP address and entered its Ethernet, IP address into the BOOTP conf.

To eliminate this error-prone setup, BOOTP was Extended to DHCP (Dynamic Host Configuration protocol.) allows automatic assignment.

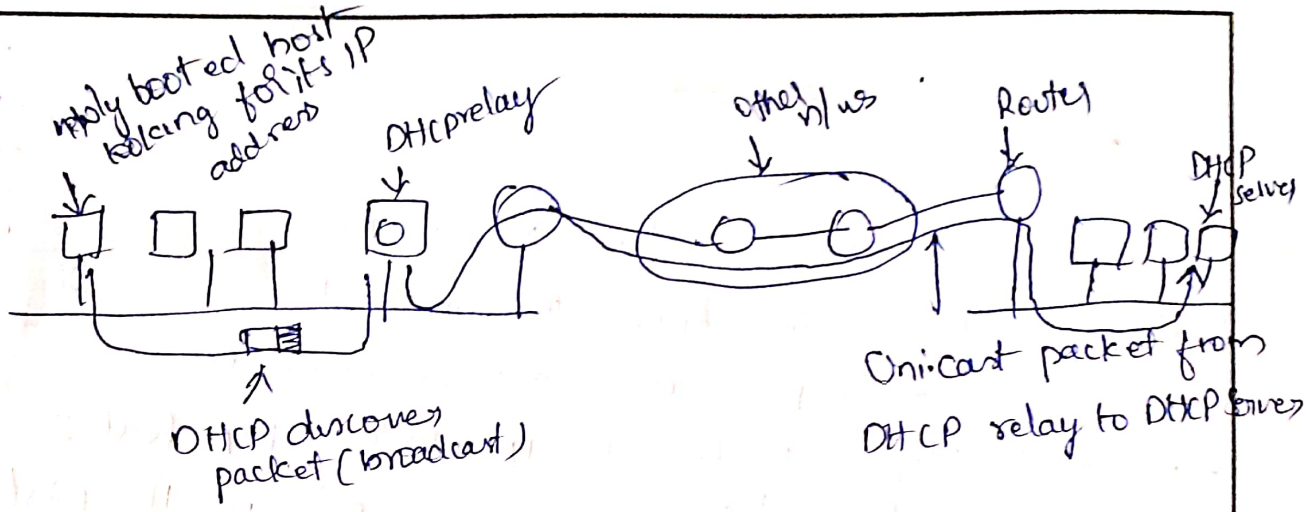
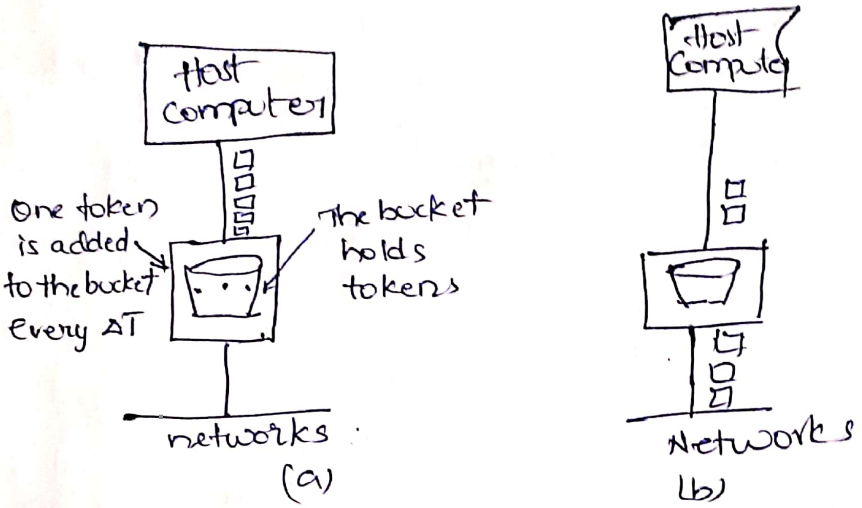


fig: operation of DHCP

22
8
T1
18/5/21

Token Bucket Algo:

In this algo., the leaky bucket holds tokens, generated by a clock at the rate of one token every ΔT sec.



The Token bucket algo. (a) Before (b) After.

(a) holds a bucket with three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token.

(b) we see that three of five packets have gotten through, but the other two are stuck waiting for two more tokens to be generated.

- Diff. b/w the two algo. is that the token bucket algo. throws away tokens when the bucket fills up but never discards packets. In contrast, the leaky bucket algo. discards packets when the bucket fills up.

Quality of service (contd..)

Together these determine the QoS (Quality of Service) the flow requires. Several common applications are:

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Video Conferencing	Low	High	High	High

Techniques for Achieving Good Quality of Service:

① Overprovisioning: Provides so much router capacity, buffer space & bandwidth that the packets just fly through easily.

② Buffering:

③

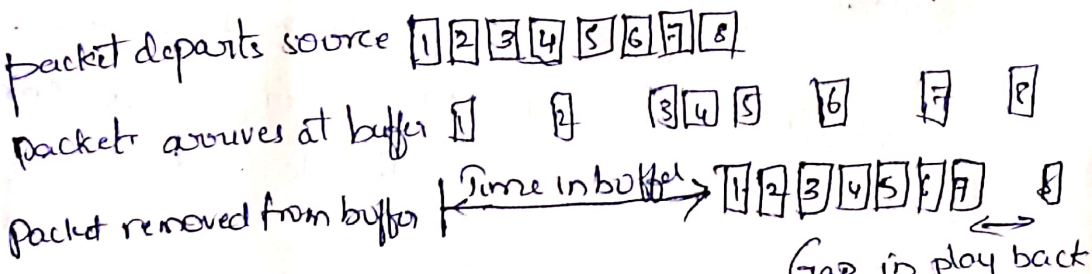
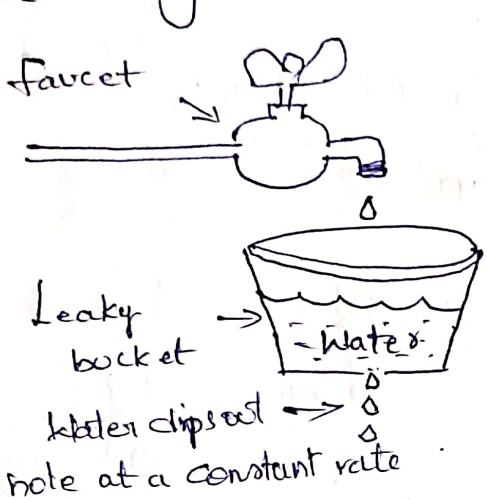


fig: Smoothing the o/p stream by buffering packets.

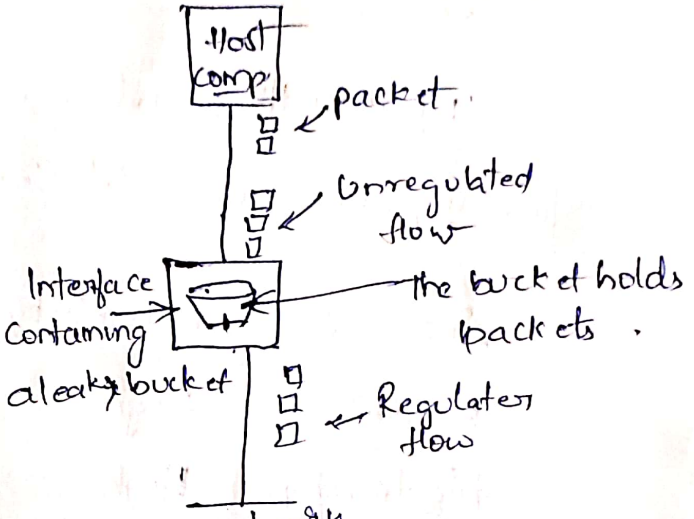
Traffic Shaping: Smooths out the traffic on the server side rather than on the client side.

- It regulates the average rate of data transmission.
- When a connection is setup, the user and the subnet agree on a certain traffic pattern for that circuit. Sometimes this is called a service level agreement.

The Leaky Bucket Algorithm :



(a) Leaky bucket with water.



(b) Leaky bucket with packets

Imagine a bucket with a small hole in the bottom, No matter the rate at which water enters the bucket, the outflow is at a constant rate, ρ, when there is any water in the bucket and zero when the bucket is empty. Also once the bucket is full, any additional water entering it spills over the sides is lost.

The same idea is applied to the packets :

Conceptually, each host is connected to the n/w by an interface containing a leaky bucket. If the packet arrives at the queue when it is full; the packet is discarded. This arrangement can be built into the h/w interface or simulated by the host OS. and is called the leaky bucket algorithm.