Networks

A Network is a set of devices (often referred to as nodes) connected by communication Links. A Node can be a computer, Printer, or any other device capable of sending and receiving data generated by other nodes on the network.

"Computer Network" to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information. The connection need not be via a copper wire, fiber optics, micro waves, infrared, and communication satellites can also be used.

Uses of Computer Networks

1. Business Applications
2. client-Server Model
3. Communication medium
4. Desktop sharing
5. Home Applications
   - Peer to peer communication
   - Person to person comm.
   - electronic commerce
   - entertainment (game playing)
6. Mobile users (Text messaging or texting, smart phones, GPS, m-Comm. NFC (Near Field comm.)
7. Social Issues.

Phishing Attack: Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.

BOTNET ATTACK: Botnet attack can be used to perform distributed denial-of-service attack (DDoS attacks), steal data, send spam, and allows the attacker to access the device and its connection.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

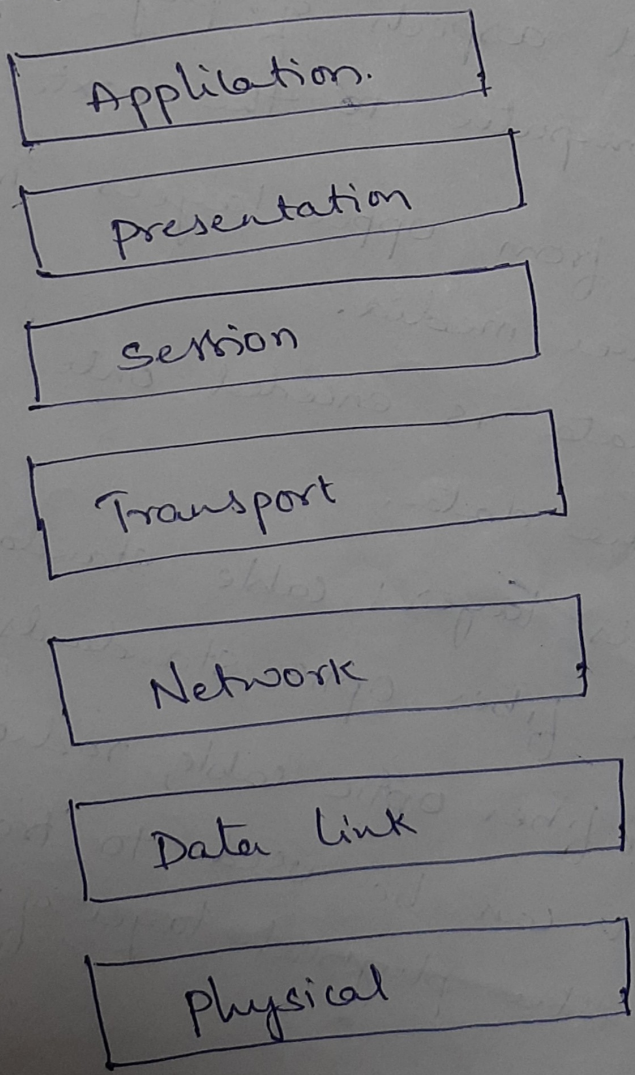
1. Delivery – The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.

2. Accuracy – The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.

3. Timeliness – The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

OSI

- OSI stands for open system Interconnection.
- Created by International standard organization (ISO)
- was created as a framework and reference model to explain how different networking technologies work together and interact.
- It is not a standard that networking protocols must follow.
- Each layer has specific functions it is responsible for
- All layers work together in the correct order to move data around a network.



How the data is referred to in the OSI Model.

Data	• Application, Presentation, and Session Layer.
Segment	• Transport layer
Packet	• Networking layer
Frame	• Data Link layer
Bits.	• physical layer

Functions of physical layer.

1. Bit Synchronization
2. Bit rate control - bit pe
3. physical topologies -
4. Transmission mode:
   - Simplex - half-duplex -
   - full-duplex

Physical Layer.

- Deals with all aspects of physically moving data from one computer to the next.
- Converts data from upper layers into 1s and 0s for transmission over media.
- Defines how data is encoded onto the media to transmit the data.
- Defined on this layer: cable standards, wireless standards, and fiber optic standards.
  Copper wiring, fiber optic cable, radio frequencies, anything that can be used to transmit data is defined on the physical layer of the OSI Model.
- Device Example Hub
- Used to transmit data.

Data Link layer:

- Is responsible for Moving frames from node to node or computer to computer.
- Can Move frames from one adjalent computer to another, cannot move frames across routers.
- Encapsulation = frame.
- Requires MAC Address or physical address.
- protocols defined include Ethernet Protocol and point-to-Point Protocol (PPP)
- Device Example : switch.
- Two Sub layers : Logic Link Control (LLC) and the Media Access Control (MAC)

Packet in Data Link Layer is referred as frame

DLL is handled by the NIC (Network Interface card) and device drivers of host machine.

Switch & Bridge are data link layer devices.

- Logic Link Control (LLC)
  Data Link layer addressing, flow control, address notification, error control.
- Media Access Control (MAC)
  Determines which computer has access to the network media at any given time.
  Determines where one frame ends and the next one starts, called frame synchronization.

functions of data link layer are

1. Framing
2. physical addressing
3. Error control
4. Flow control
5. Access control.

Network layer.

- Responsible for moving packets (data) from one end of the network to the other, called end-to-end communication
- Requires logical addresses such as IP addresses.
- Device example: Router.
  - Routing is the ability of various network devices and their related software to move Data packets from source to destination.

Segment in the Network layer is referred as packet.

functions of Network layer
- Routing
- Logical addressing.

header, IP address

Transport Layer.

Provides service to application layer by Taking service from Network layer

- Takes data from higher levels of OSI model and breaks it into segments that can be sent to lower-level layers for data transmission.
- Conversely, reassembles data segments into data that higher-level protocols and applications can use.
- Also puts segments in correct order (called Sequencing) so they can be reassembled in correct order at destination.

functions: Segmentation & Reassembly, Service point addressing

It also adds source & destination port no. in its header & forwards the segmented data to the N/w layer

- Concerned with the reliability of the transport of Sent data.

Services provided is connection oriented connection less.

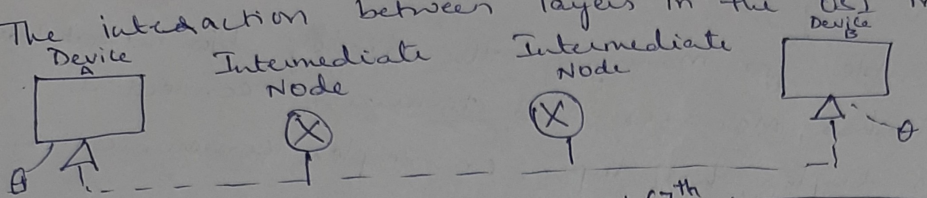
- May use a connection-oriented protocol such as TCP to ensure destination received segments.
- May use a connectionless protocol such as UDP to send segments without assurance of delivery.
- Uses Port addressing.

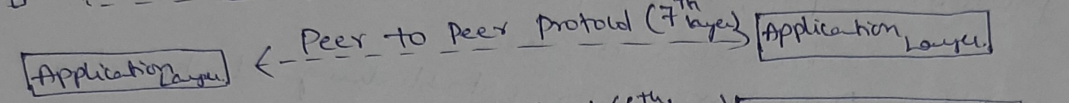
Data in Transport layer is called Segments

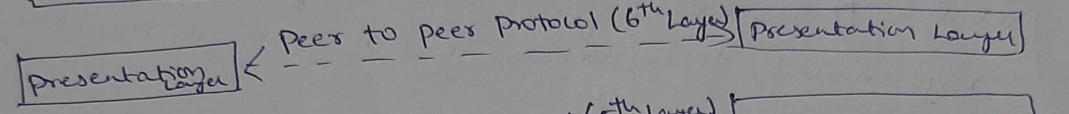
Transport layer is operated by O/S.

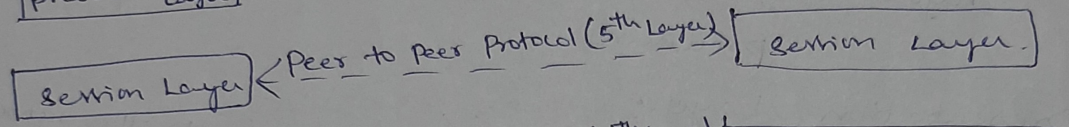
Transport layer is called heart of OSI model

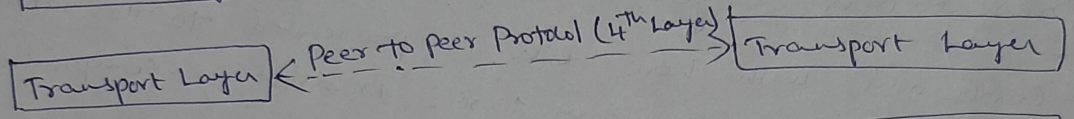
The interaction between layers in the OSI model.

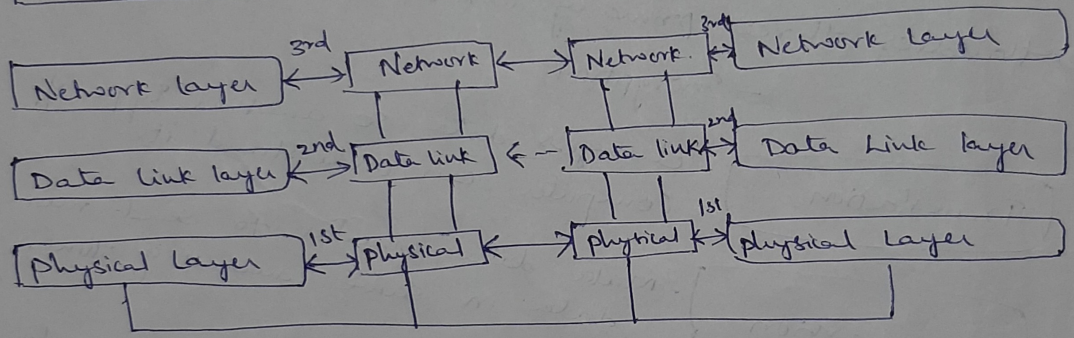




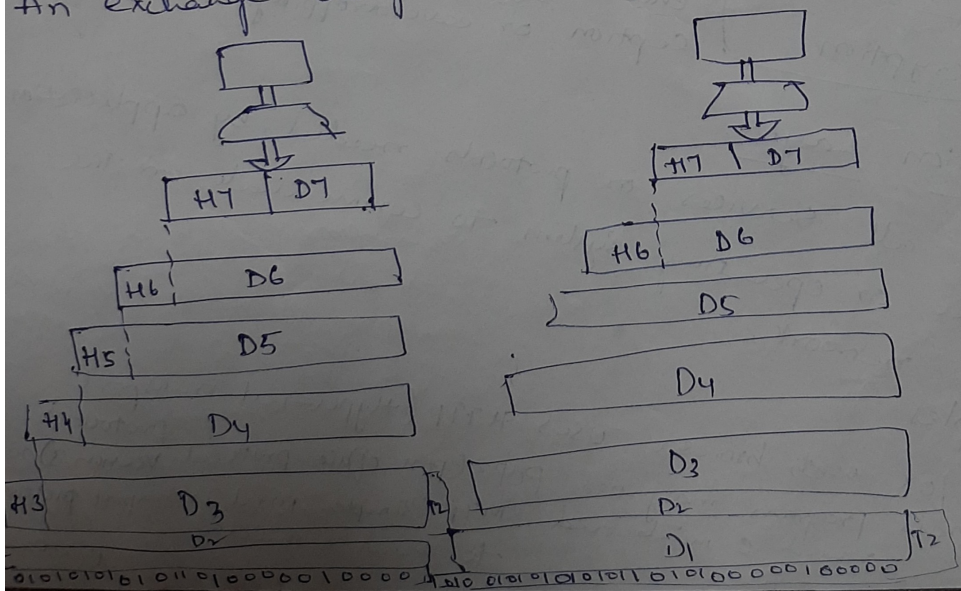








An exchange using the OSI model.



Session Layer:

This layer allows the two processes to establish, use and terminate a connection.

- Responsible for managing the dialog b/w networked devices.
- Establishes, manages, and terminates connections.
- provides duplex, half-duplex, or simplex communications between devices.
- provides procedures for establishing checkpoints, adjournment, termination, and restart or recovery procedures.

1. Session establishment, maintenance and termination
2. Synchronization
3. Dialog controller.

Presentation Layer:

- Concerned with how data is presented to the network.
- Handles three primary task :- Translation, - Compression, - Encryption.

Translation - changes data so another type of computer can understand it. (ASCII)

Compression - Make data similar to send more data in same amount of time.

Encryption - Encodes data to protect from interception or eavesdropping.

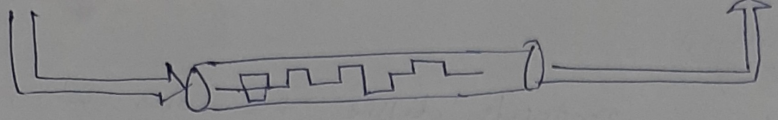
Application Layer.

- Contains all services or protocols needed by application software or operating system to communicate on the network.

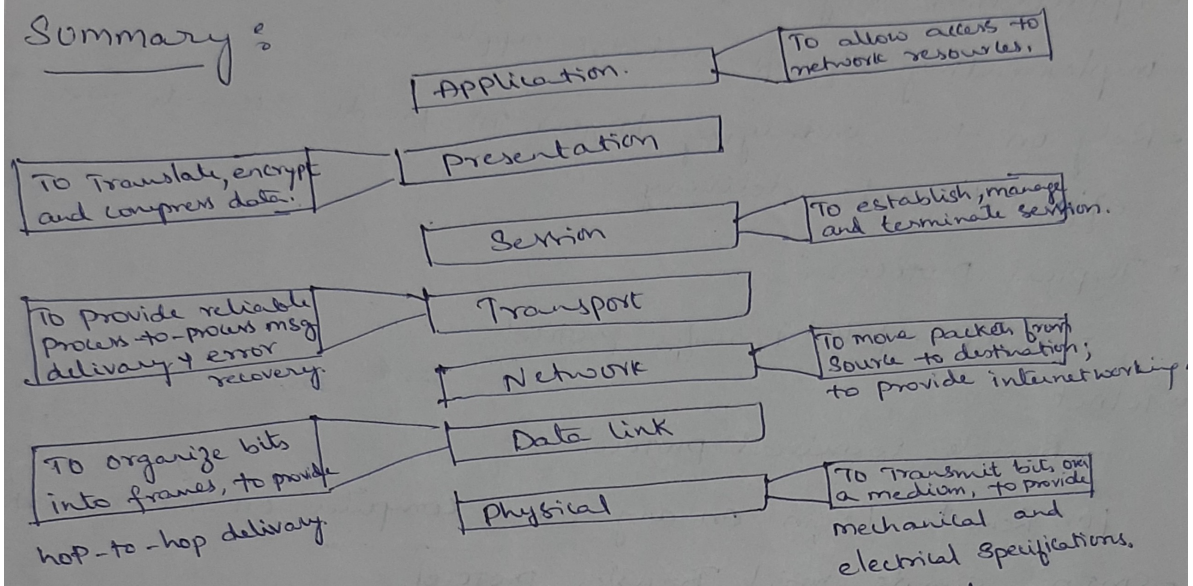
functions -
1. Network virtual Terminal
2. FTAM - File transfer access & mgt.
3. mail services
4. Directory services

- Examples.
  - Firefox web browser uses HTTP (Hyper-Text Transport Protocol)
  - E-mail program may use POP3 (Post office protocol version 3) to read e-mails and SMTP (Simple mail Transport protocol) to send e-mails.

P.T.O.

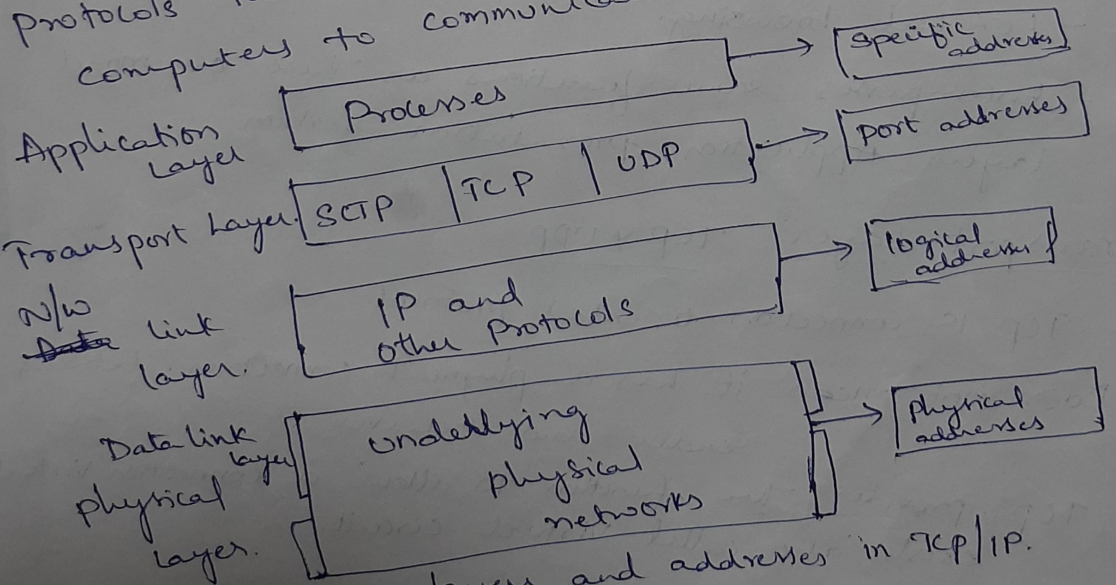


Summary:



TCP/IP Model (Transmission Control Protocol/Internet protocol)

- A protocol suite is a large number of related protocols that work together to allow networked computers to communicate.



Relationship of layers and addresses in TCP/IP.

Application Layer.

- Application layer protocols define the rules when implementing specific network applications.
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
  - FTP - File Transfer Protocol.

Telnet
  - Remote terminal protocol.

For Remote Login on any other computer on the network.

SMTP - Simple mail Transfer protocol.

~~For Remote login on any other computer on the network~~

For Mail Transfer

HTTP - Hypertext Transfer Protocol.
  - For web browsing.
  - Encompasses same functions as their OSI model layers Application presentation section.

Transport Layer. TCP & UDP

- TCP is connection oriented protocol

Does not mean it has a physical connection between sender and receiver.

- TCP provides the function to allow a connection virtually exists - also called virtual circuit.

- UDP provides the functions:
  - Dividing the chunks of data into segments
  - Reassembly segments into the original chunk
  - Provide further the functions such as reordering and data resend.
- Offering a reliable byte-stream delivary servie
  - Functions the same as the Transport layer in OSI
  - Synchronize source and destination computer to set up the session between the respective computer

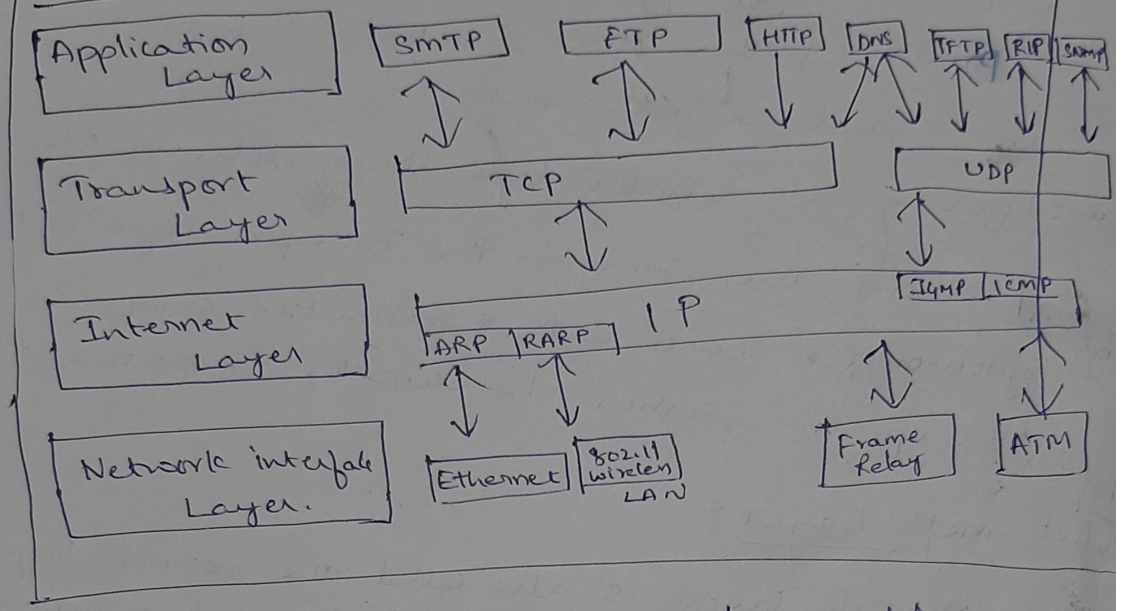
Internet Layer:

The Network layer is also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control message protocol (ICMP), which is used for error reporting.

Host-to-Network Layer:

The Host-to-network layer is the lowest layer of the TCP/IP reference model. It combines the link layer and the physical Layer of the ISO/OSI model. At this Layer, data is transferred between network nodes in a WAN or between nodes on the same LAN.

TCP/IP model and its Relation to protocols of the TCP/IP suite.



OSI Model

- Contains 7 Layers
- Uses strict Layering resulting in vertical layers
- Supports both connection less & connection-oriented comm. in the network layer, but only connection oriented comm. in Transport layer.
- It distinguishes between service, interface and protocol.
- Protocols are better hidden and can be replaced relatively easily as technology changes (No Transparency)
- OSI reference model was devised before the corresponding protocols were designed.

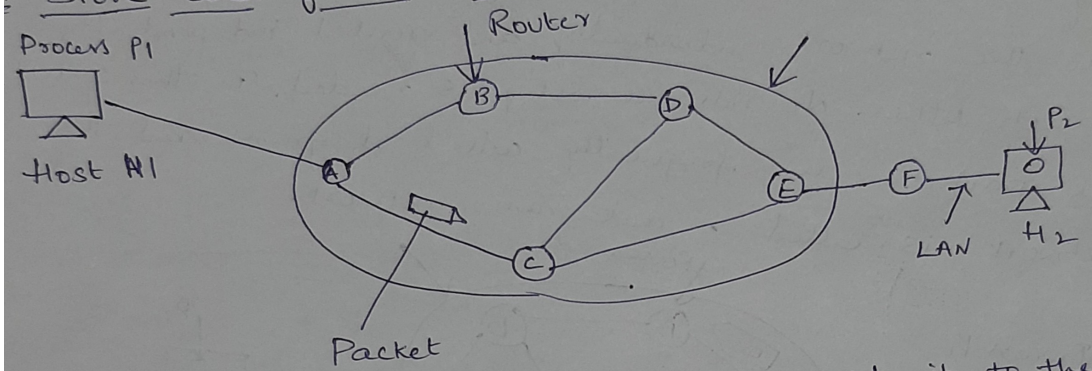
TCP/IP Model.

- Contains 4 Layers
- Uses Loose Layering resulting in horizontal layers.
- Supports only connectionless communication in the network layer, but both connectionless & connection oriented communication in Transport layer.
- Does not clearly distinguish between service, interface and protocol.
- protocols are not hidden and thus cannot be replaced easily. (Transparency)
  Replacing IP by a substantially different protocol would be virtually impossible
- The protocols came first and the model was a description of the existing protocols.

Network Layer: Design Issues.

1. Store-and-forward packet switching
2. Services provided to transport layer
3. Implementation of connectionless service
4. Implementation of connection-oriented service
5. Comparision of virtual-circuit and ~~dag~~ datagram networks.

1. Store-and-forward packet switching.



A Host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the ISP. The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum. Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered. This mechanism is store-and-forward packet switching.

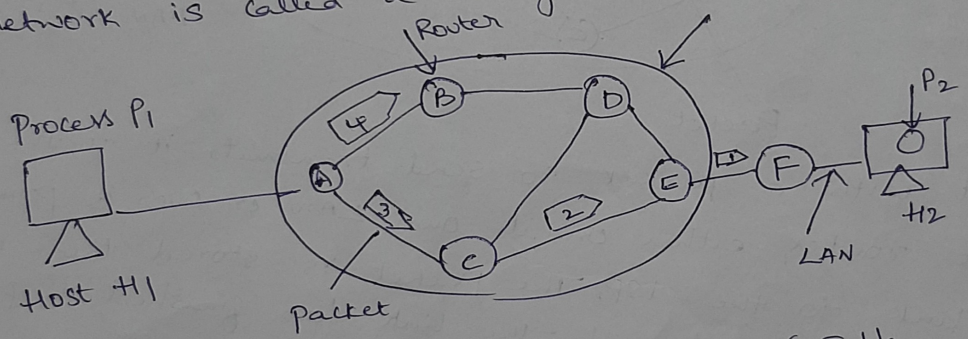
2. Services provided to Transport Layer.

The network Layer provides services to the transport Layer at the network layer/transport layer interface. The servile need to be carefully designed with the following goals in mind:

1. Service independent of router technology.
2. Transport layer shielded from number, type, topology of routers.
3. Network addresses available to transport layer use uniform numbering plan even across LANs and WANs.

3. Implementation of Connectionless Services.

If connectionless service is offered, packets are injected into the network individually and routed independently of each other. No advance setup is needed. In this context, the packets are frequently called datagrams and the network is called a datagram network.



A's table (initially)

A	☒
B	B
C	C
D	B
E	C
F	C

Dest. Line

A's table (later)

A	☒
B	B
C	C
D	B
E	D
F	D

C's Table

A	A
B	A
C	☒
D	E
E	E
F	E

E's table

A	C
B	D
C	C
D	D
E	☒
F	F

Let us assume for this example that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets 1, 2, 3, & 4 and

Send each of them in turn to router A.
Every router has an internal table telling it where to send packets for each of the possible destinations. Each table entry is a pair (destination and the outgoing line). Only directly connected lines can be used.

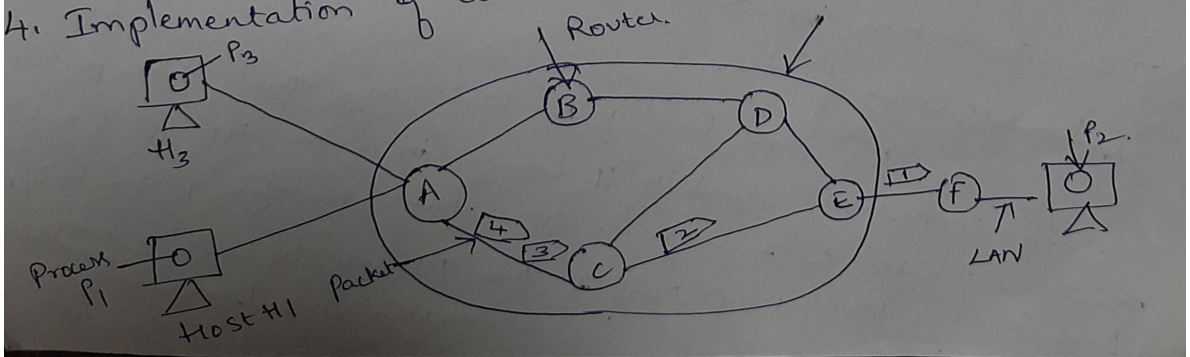
A's initial routing table is shown in the fig. Under the Label "initially".

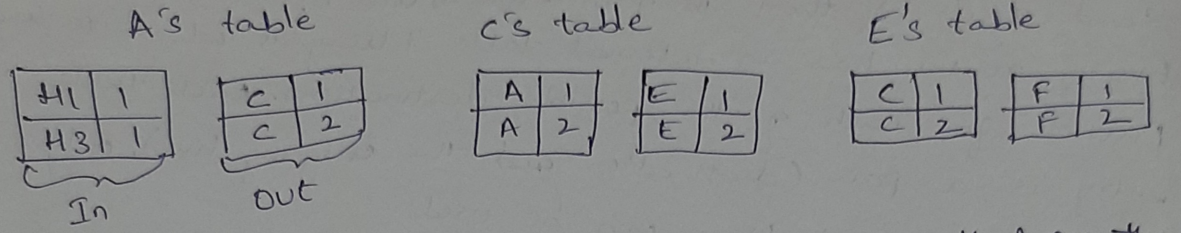
At A, packet 1, 2 and 3 are stored briefly having arrived on the incoming link. Then each packet is forwarded according to A's table, onto the outgoing link to C within a new frame. Packet 1 is then forwarded to E and then to F.

However, something different happens to packet 4. When it gets to A it is sent to router B, even though it is also destined for F. For some reason (traffic jam along ACE path), A decided to send packet 4 via a different route than that of the first three packets. Router A updated its routing table, shown under the label "later".

The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

4. Implementation of connection-oriented service





If Connection-oriented service is used, a path from the source router all the way to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit) and the network is called a virtual-circuit network.

When a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the telephone system works. When the connection is released the virtual circuit is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit is belong to.

As an example, consider the situation shown in fig. Here, host H1 has established connection 1 with HostH2. This connection is remembered as the first entry in each of the routing tables.

The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier 1.

Jitter: Jitter refers to the [illegible] time. It is the uneven delay in the delivery of audio or video packets. Video packets are sent every 30ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

A data communications system has five components.

1. Message: The message is the information to be communicated popular forms of information include text, numbers, pictures, audio, & video.

2. Sender: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.

3. Receiver: The Receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

4. Transmission medium: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio wave

5. Protocol: A protocol is a set of rules that govern data comm. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Adaptive Algorithm: in contrast, change their routing decisions to reflect changes in the topology, and usually the traffic as well.

Adaptive algorithms differ in

1. where they get their information (e.g. locally, from adjacent routers, or from all routers)
2. when they change the routes (e.g. every ΔT sec, when the load changes or when the topology changes), and
3. what metric is used for optimization (e.g. distance, number of hops, or estimated transit time).

This Procedure is called dynamic routing.

Different Routing Algorithms

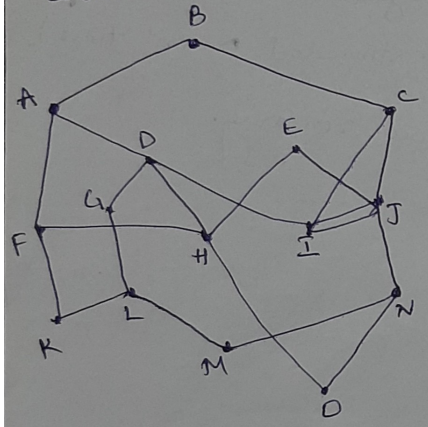
- Optimality Principle
- Shortest path algorithm
- Flooding
- Distance vector routing
- Link state routing
- Hierarchical Routing

The Optimality Principle

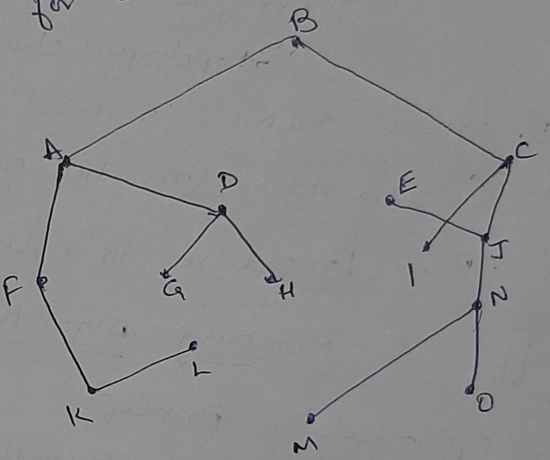
One can make a general statement about optimal routes without regard to network topology or traffic. This statement is known as the optimality principle.

It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same.

As a directed consequences of the Optimality Principle, we can see that the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such a tree is called a sink tree. The goal of all routing algorithm is to discover and use the sink trees for all routers.



(a) A network

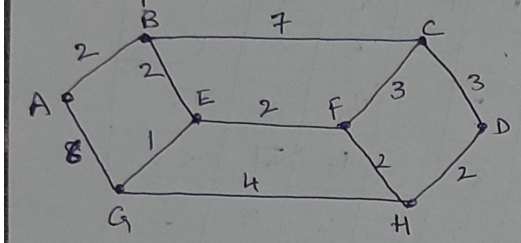


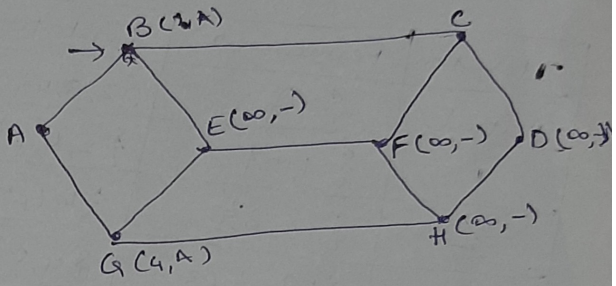
(b) A sink tree for router B.

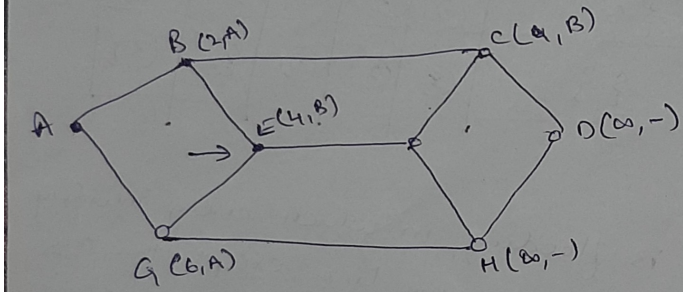
Shortest Path Routing (Dijkstra's)

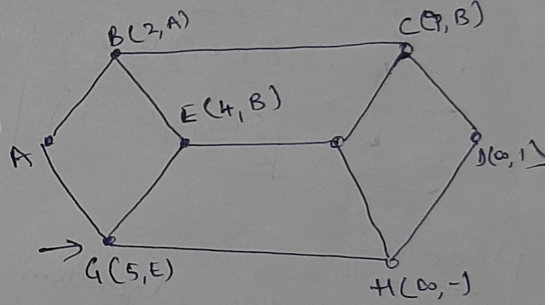
The idea is to build a graph of the subnet, with each node of the graph representing a router and each arc of the graph representing a communication line or link. To choose a route between a given pair of routers, the algorithm just finds the shortest path between them on the graph.

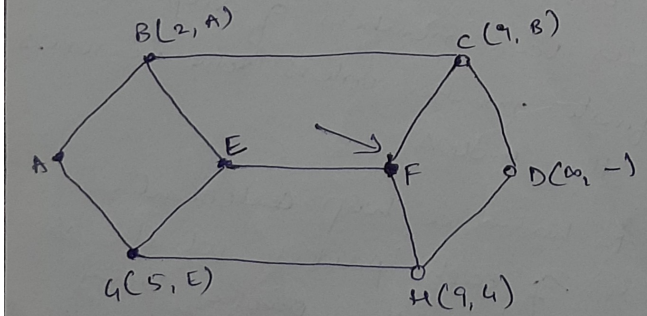
1. Start with the local node (router) as the root of the tree. Assign a cost of 0 to this node and make it the first permanent node.
2. Examine each neighbor of the node that was the last permanent node.
3. Assign a cumulative cost to each node and make it tentative.
4. Among the list of tentative nodes.
5. Repeat step 2 to 4 until every node becomes permanent.

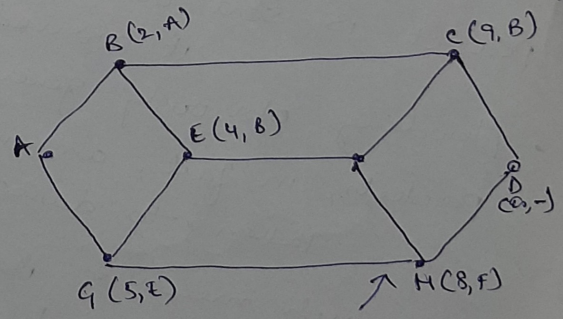




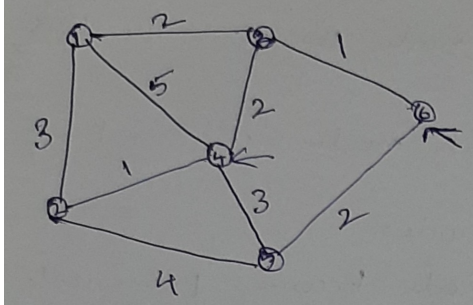


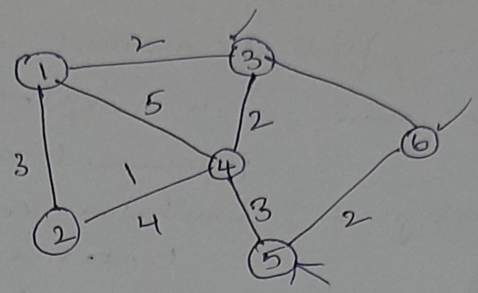






Execution of Dijkstra's algorithm.





Iteration	Permanent	tentative	D_2	D_3	D_4	D_5	D_6
Initial	{1}	{2,3,4}	3	2 ✓	5	∞	∞
1	{1,3}	{2,4,6}	3 ✓	(2)	4 ✓	∞	5
2	{1,2,3}	{4,6,5}	(3)	(2)	4	∞	3 ✓
3	{1,2,3,6}	{4,5}	(3)	(2)	4 ✓	5	(3)
4	{1,2,3,4,6}	{5}	(3)	(2)	(4)	5 ✓	(3)
5	{1,2,3,4,5,6}	{}	(3)	(2)	(4)	(5)	(3)

Flooding

Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on.

- flooding obviously generates vast number of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.
- one such measure is to have a hop ~~count~~ 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 from source to destination.

Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. 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, node C also knows how to reach node D.

In other words, nodes A and C, as immediate neighbors, can improve their routing table if they help each other.

Note: In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

Updating

When a node receive a two-column table from a neighbor, it needs to update its routing table. Updating takes three steps.

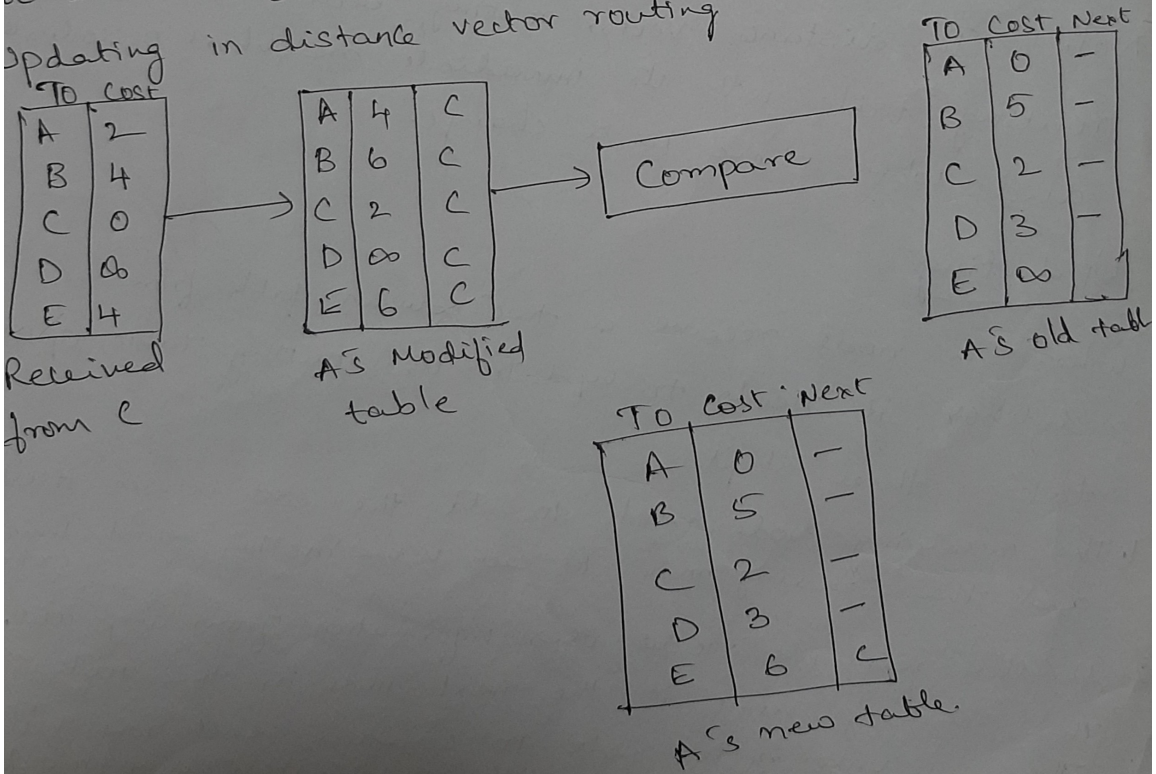
1. The receiving node needs to add the cost between itself and the sending node to each value in the second column (x+y)
2. If the receiving node uses information from any row. The sending node is the next node in the route.
3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of received table.

a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

b. If the next-node entry is the same the receiving node chooses the new row.

Eg: Suppose node C has previously advertised a route to node X with distance 3. Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity. Node A must not ignore this value even though its old entry is smaller the old route does not exist anymore. The new route has a distance of infinity.

Updating in distance vector routing



Distance Vector Routing:

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

Mainly 3 things in this

Initialization

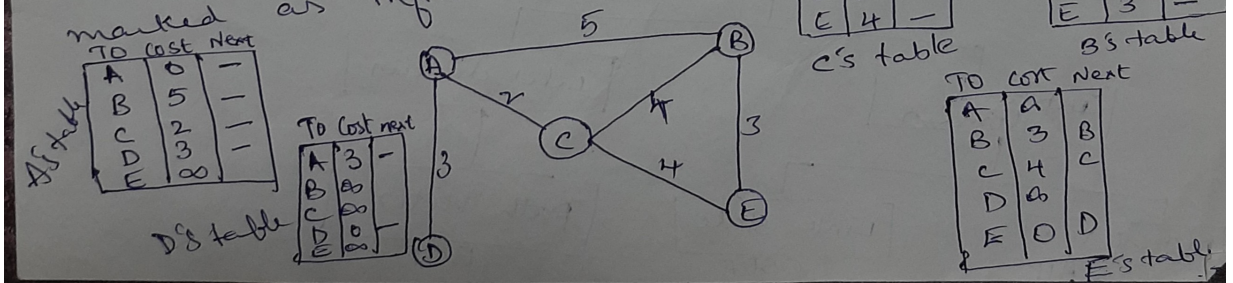
sharing

Updating.

Initialization:

Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors 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 neighbor is marked as infinite (Unreachable).



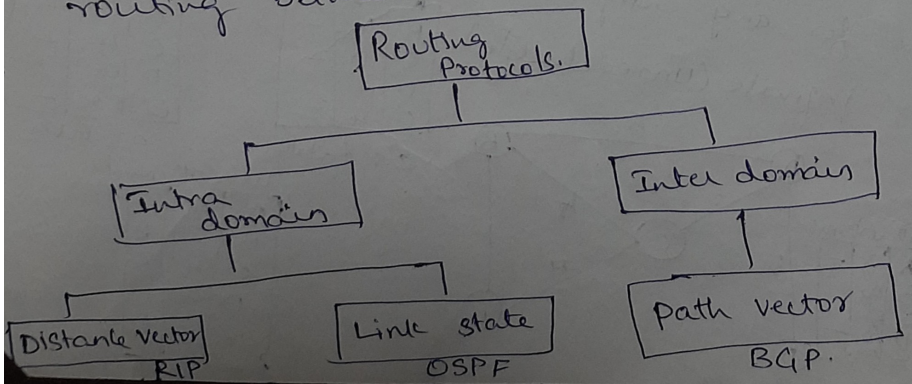
- A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.
- flooding is not practical in most applications.

Intra- and- Inter domain Routing.

An Autonomous System (AS) is a group of networks and routers under the authority of a single administration.

Routing inside an autonomous system is referred to as intra domain routing (Distance Vector, Link state).

Routing between autonomous system is referred to as inter domain routing. (PATH VECTOR) Each autonomous system can choose one or more intra domain routing protocols to handle routing inside the autonomous system. however only one inter domain routing protocol handles routing between autonomous system.



Routing Algorithms

The main function of NL (Network Layer) is routing packet from the source machine to the destination machine.

There are two processes inside router;

a) one of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing table. This process is forwarding.

b) The other process is responsible for filling in and updating the routing tables. That is where the routing algorithm comes into play. This process is routing.

Regardless of whether routes are chosen independently for each packet or only when new connections are established, certain properties are desirable in a routing algorithm correctness, simplicity, robustness, stability, fairness, optimality.

Routing algorithms can be grouped into two major classes;

1. Non-adaptive (Static Routing)
2. adaptive (Dynamic Routing)

Non-adaptive algorithm do not base their routing decisions on measurements or estimate of the current traffic and topology. Instead, the choice of the route to use to get from I to J is computed in advance, offline and downloaded to the routers when the network is booted. This procedure is sometimes called static routing.

Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 and tells the network to establish to establish the virtual circuit.

This leads to the second row in the tables. Note that we have a conflict here because although A can easily distinguish connection 1 packets from H1 from connection 1 packets from H3, C cannot do this.

For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection. Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets.

In some contexts, this process is called Label switching. An example of a connection-oriented network service is MPLS (Multi-Protocol Label Switching).

Comparison of Virtual-circuit and datagram networks

Issue	Datagram Network	Virtual-Circuit Network
Circuit Setup	Not Needed	Required
Addressing	Each packet contains the full source and destination address.	Each packet contains a short VC number.
State information	Routers do not hold state information about connections	Each VC requires router table space per connection.
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed route 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

Random Early Discard (RED)

1. This is a proactive approach in which the router discards one or more packets before the buffer becomes completely full.
2. Each time a packet arrives, the RED algorithm computes the average queue length, avg.
3. If avg is lower than some lower threshold congestion is assumed to be minimal or non-existent and the packet is queued.
4. If avg is greater than some upper threshold, congestion is assumed to be serious and the packet is discarded.
5. If avg is between the two thresholds, this might indicate the ~~ones~~ onset of congestion. The probability of congestion is then calculated.

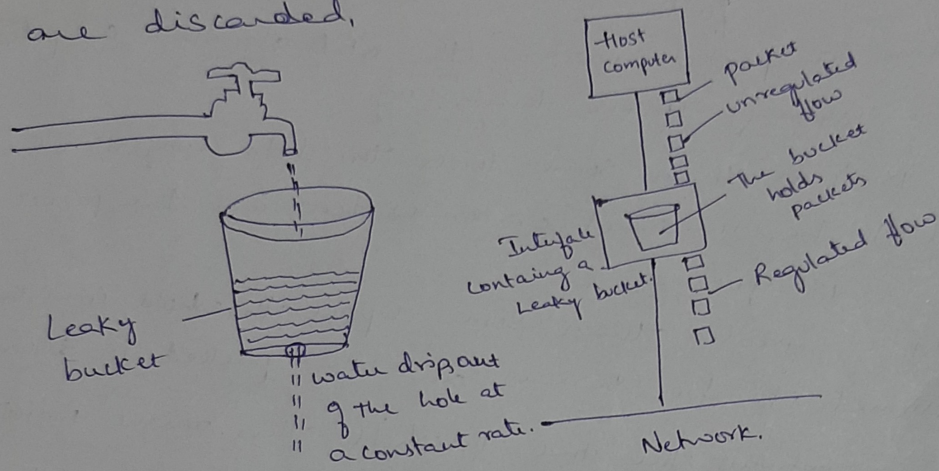
Traffic Shaping

1. Another method of congestion control is to "shape" the traffic before it enters the network.
2. Traffic shaping controls the rate at which packets are sent (not just how many) used in ATM and Integrated Service Networks.
3. At connection set-up time, the sender and carrier negotiate a traffic pattern (shape).

Two traffic shaping algorithms are

1. Leaky Bucket
2. TOKen Bucket.

The Leaky Bucket Algorithm used to control rate in a network. It is implemented as a single server queue with constant service time. if the bucket over flows then packets are discarded.

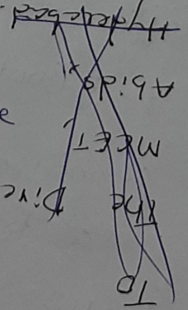


a) a leaky bucket with water (b) a leaky bucket with packets.

. The leaky bucket enforces a constant output rate regardless of the burstiness of the input. Does nothing when input is idle.

The host injects one packet per clock tick onto the network. This results in a uniform flow of packets, smoothing out burst and reducing congestion.

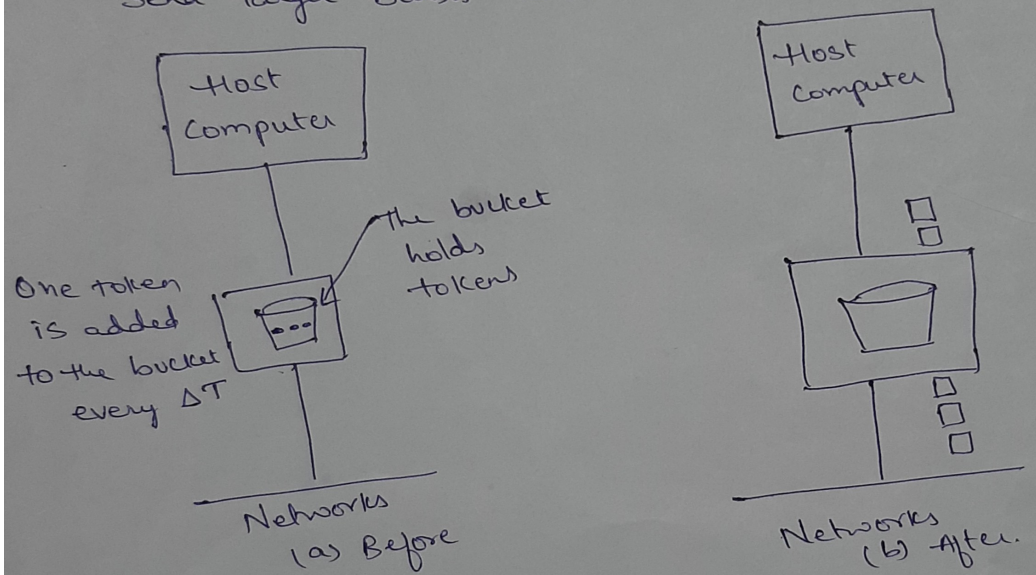
When packets are the same size, the one packet per ticket is okay. For variable length packets though, it is better to allow a fixed number bytes per tick.



e.g. 1024 bytes per tick will allow one 1024 byte packet or two 512-byte packets or four 256 byte packets on 1 tick.

Token Bucket Algorithm

1. In contrast to the LB, the Token Bucket Algorithm, allows the output rate to vary, depending on the size of the burst.
2. In the TB algorithm, the bucket holds tokens. To transmit a packet, the host must capture and destroy one token.
3. Tokens are generated by a clock at the rate of one token every Δt sec.
4. Idle hosts can capture and save up tokens in order to send larger bursts later.



1. LB discards packet; TB does not; TB discards tokens.
2. With TB, a packet can only be transmitted if there are enough tokens to cover its length in bytes.
3. LB sends packets at an average rate. TB allows for larger bursts to be sent faster by speeding up the output.
4. TB allows savings up tokens (permissions) to send large bursts. LB does not allow saving.

The reason congestion control and flow control are often confused is that best way to handle both problems is to get the host to slow down. Thus, a host can get a "slow down" message either because the receiver cannot handle the load or because the network cannot handle it. Several techniques can be employed. These include;

1. Warning bit
2. Choke packets
3. Load shedding
4. Random early discard
5. Traffic shaping.

The first 3 deal with congestion detection and recovery. The last two deal with congestion avoidance.

Warning Bit

A special bit in the packet header is set by the router to warn the source when congestion is detected.

. The bit is copied and piggy-backed on the ACK and sent to the sender.

. The sender monitors the number of ACK packets it receives with the warning bit set and adjusts its transmission rate accordingly.

Choke Packets

A more direct way of telling the source to slow down.

2. A choke packet is a control packet generated at a congested node and transmitted to restrict traffic flow.
3. The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.
4. An example of a choke packet is the ICMP source Quench packet.

Hop-by-Hop choke packets

1. Over long distances or at high speeds choke packets are not very effective.
2. A more ~~effective~~ efficient method is to send to choke packets hop-by-hop.
3. The source, on receiving the choke packet must reduce its transmission rate by a certain percentage.
4. A example of a choke packet is the ICMP source Quench packet
5. This requires each hop to reduce its transmission even before the choke packets arrive at the source.

Load Shedding.

When buffer becomes full, routers simply discard packets. Which packet is chosen to be the victim depends on the application and on the error strategy used in the data link layer.
For a file transfer, for e.g. cannot discard older packets Since this will cause a gap in the received data.
For real-time voice or video it is probably better to throw away old data and keep new packets.
Get the application to mark packets with discard priority.