B. E.

Fifth Semester Examination, May-2007

COMPUTER NETWORKS (IT-305-E)

Note : Attempt any five questions.

Q. 1. What do you mean by computer network and Network topologies? Explain each with their advantage and disadvantage?

Ans. Computer Network : Mean an interconnected collection of autonomous computers. Two computers are said to be interconnected if they are able to exchange information. By requiring the computers to be autonomous, we wish to exclude from our definition system, in which there is a clear master/slave relation. If one computer can forcibly start, stop or control another one, the computers are not autonomous. A system with on control unit & many slaves is not a network, nor is a large computer with remote printers & terminals.

Network Topology : The topology of a network is the geometric representation of the relationship of all the links & linking devices to each other. There are five basic topologies possible; mesh, star, tree, bus & ring.

1. Mesh Topology : In a mesh topology, every device has a dedicated point-to-point link to every other device. The terms dedicated means that the link carries traffic only between the two devices it connects.

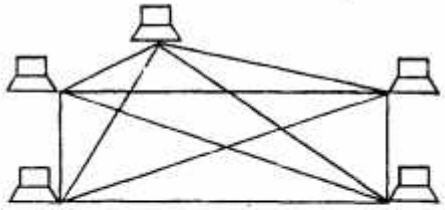


Fig. Mesh Topology

Advantages :

1. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. Second, a mesh topology is robust. If one link becomes unusable, it does not in capacitate the entire system.
3. Another advantage privacy or security.
4. Finally, point-to-point links make fault identification and fault isolation easy.

Disadvantages : The main disadvantages of a mesh are related to the amount of cabling and the number of input/output parts required. First, because every device must be connected to every other device, installation and reconfiguration are difficult. Second the sheer bulk of the wiring can be greater than the available space (in walls, or floors) can accommodate. And, finally the hardware required to connect each link (input/output ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

2. **Star Topology :** In a star topology, each device has a dedicated point to point link only to a central controller, usually called a hub. The devices are not directly linked to each other.

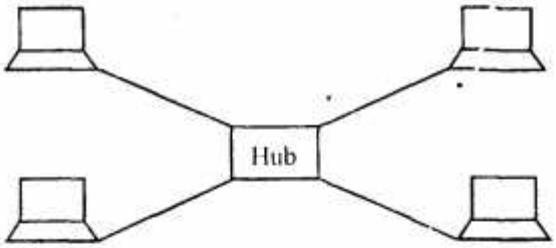


Fig. 2. Star topology

Advantages : Star topology is less expensive than a mesh topology. In a star, each device needs only one link & one input/output part to connect it to any no. of others. This factor also makes it easy to install & reconfigure.

Other advantages include robustness. If are link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification & fault isolation.

Tree Topology : A tree topology is a variation of a star. As in a star, nodes in a tree are linked to a central hub that controls the traffic to the network. However, not every device plugs directly into the central hub. The majority of devices connect to a secondary hub that in turn is connected to the central hub. The central hub in the tree is an active hub. The secondary hubs may be active or passive hubs. A passive hub provides a simple physical connection between the attached devices.

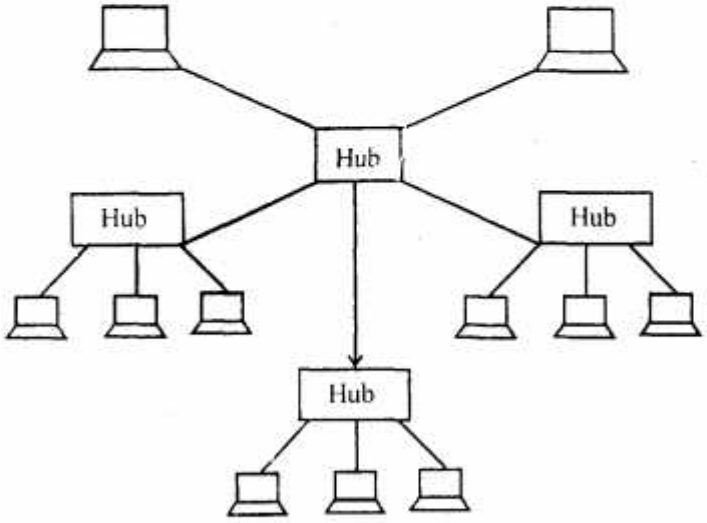


Fig. Tree topology

The advantages & disadvantages of a tree topology are generally the same as those of a star. The addition of secondary hubs, however, brings two further advantages. First, it allows more devices to be attached to a single central hub & can the refer increase the distance a signal can travel between devices. Second, it allows the network to isolate & prioritize communications from different computers.

Bus Topology : Instead of point to point configuration, A bus topology is midpoint. One long cable acts as a backbone to link all the devices in the network.

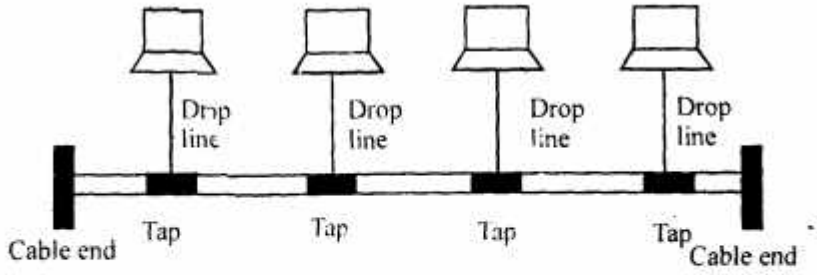


Fig. Bus Topology

Advantages : Of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh, star or tree topologies.

Disadvantage : Include difficult reconfiguration & fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices

Ring Topology : In a ring topology, each device has a dedicated point to point line configuration only with the two devices on either side of it.

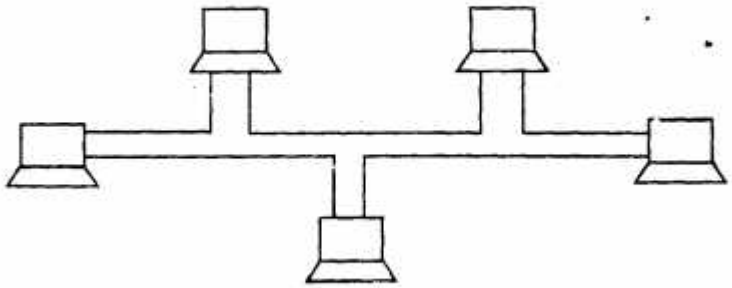


Fig. Ring Topology

A ring is relatively easy to install & reconfigure. Each device is linked only to tis immediate neighbours.

However,, unidirectional traffic can be a disadvantages. In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Q. 2. (a) Explain layed Architecture of Networks?

Ans. Layered Architecture of Networks : The OSI model is composed of seven ordered layers : Physical (Layer 1), Data ink (layer 2). network (Layer 3), Transport (Layer 4). Session (Layer 5), Presentation (Layer 6), and Application (Layer 7). The figure shows the layers involved when a message is sent from device A to device B. As the message travels from A to B. it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers. Within a single computer system, each layer calls upon the services of the layer just below it. For example, network layer (Layer 3) uses the services provided by the Layer 2 which is Data link and it provides services to layer 4 Transport layer. However, between computer systems, layer X on one system communicates only with layer X on other system. The processes on each system, that communicate at a given layer, are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process communicating to each other using protocols appropriate to the given layer.

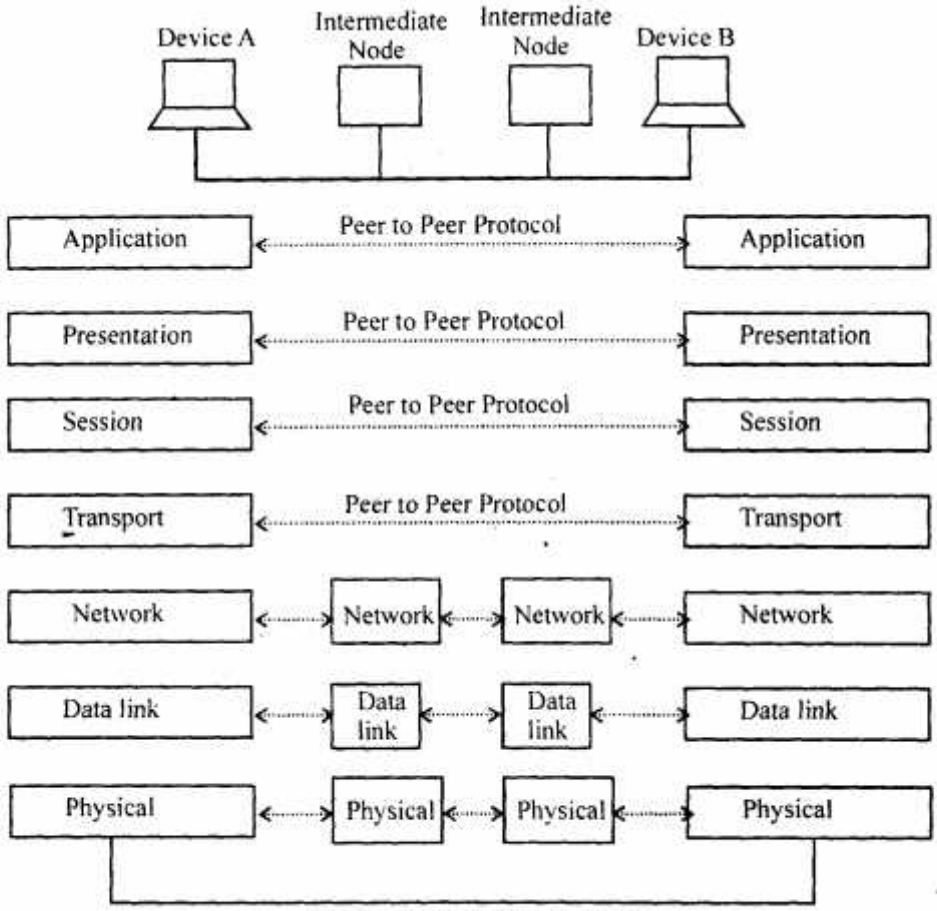


Fig. Physical Communication

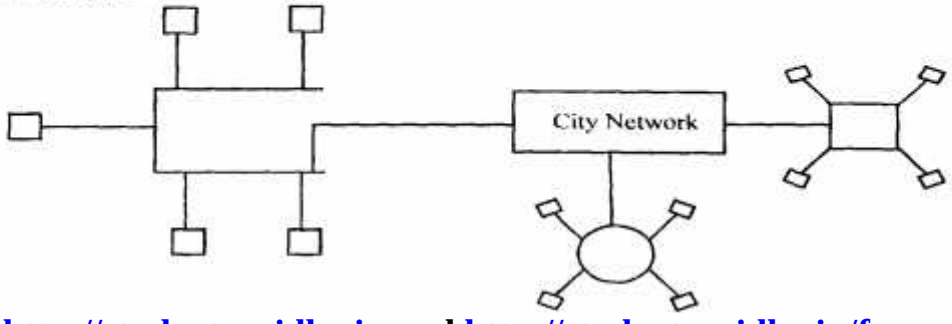
Q. 2. (b) Differentiate various types of Networks. (LAN, MAN & WAN).

Ans. Various Types of Networks :

1. LAN 2. MAN 3. WAN

1. LAN (Local Area Network) : It allows number of independent devices to communicate directly with each other in a limited geographical area.

2. MAN : Metropolitan Area Network covers an entire city. It may be connection of number of LANs or a single network fig. 1.



A MAN may be operated by a private company or may be owned.

3. WAN : Wide Area Network provides long distance transmission of data, voice, image and video information. WAN uses public leased or private communication devices.

Q. 3. What is TCP/IP model? Compare function of each layer? Also give protocol of each layer.

Ans. TCP/IP was developed prior to the OSI model. Therefore, layers in the TCP/IP protocol stack do not match exactly with those in the OSI model. The TCP/IP model is made up of five layers :

1. Physical layer
2. Data link layer
3. Network layer (IP)
4. Transport layer (TCP)
5. Application layer

The first four layers provide physical standards, network interface, internetworking and transport functions that correspond to the first four layers of the OSI model. The three top layers of the OSI model, however, are represented in the TCP/IP by a single layer called application layer. The figure illustrates how TCP/IP protocol stack fits itself in the OSI reference model.

Physical and Data Link Layer : At the physical and data link layers, TCP/IP does not define any specific protocol. It supports all of the standard and proprietary protocols.

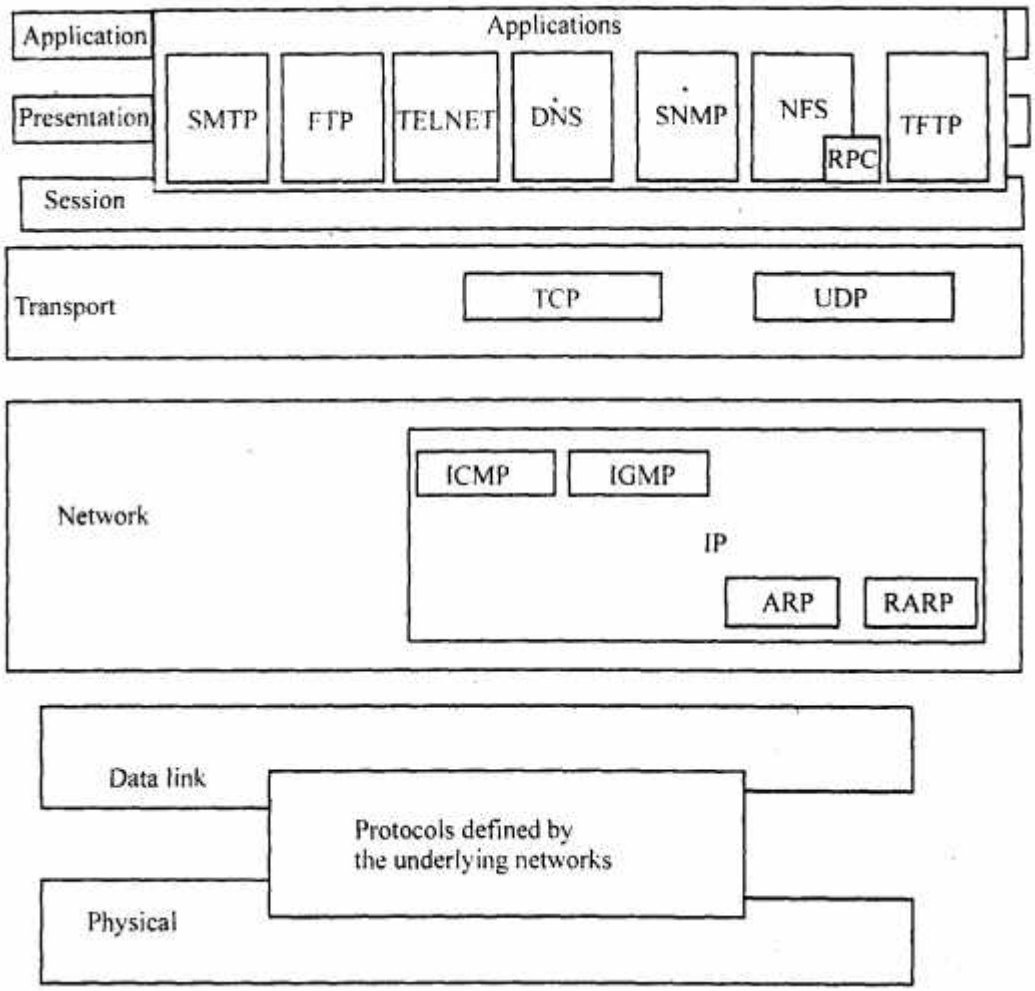
A network in a TCP/IP inter-network can be a Local Area Network (LAN), or a Metropolitan Area Network (MAN) or a Wide Area Network (WAN).

Network Layer : The data link layer is concerned with access to and routing data across a network for two end systems attached to the same network. In those cases where two devices are attached to different networks, procedures are needed to allow data to traverse multiple interconnected networks. This is the function of the network layer. The Internet Protocol (IP) is used at this layer to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. At this network layer TCP/IP supports the Internet working protocol (IP). IP, in turn contains four supporting protocols :

1. ARP
2. RARP
3. ICMP
4. IGMP

Transport Layer : The IP is a host-to-host protocol. It delivers the packet from source device to destination derive. However, it does not provide any mechanism to identify the source process (programme) and the destination process to which the packet is meant. One of the essential features provided by the transport layer protocols are exactly this supporting delivery of messages from a process to another process. At this layer, TCP/IP suite defines two protocols–UDP (User Datagram Protocol) and TCP (Transmission Control Protocol).

Application Layer : Finally, the application layer contains the logic needed to support the various user applications. For each different type of application, such as file transfer, separate module is needed that is particular to that application. The application layer in TCP/IP is equivalent to the combined session, presentation and application layers in the OSI model.



Q. 4. Explain following terms :

(i) SMTP **(ii) ARP**
(iii) IMAP **(iv) POP**
(v) FTP **(vi) ICMP**
(vii) RARP **(viii) HTTP**
(ix) DNS **(x) SONET**

Ans. (i) SMTP : (Simple Mail Transfer Protocol) : It is the TCP/IP protocol defining electronic mail service on the internet.

(ii) ARP : (Address Resolution Protocol) : In TCP/IP, a protocol for obtaining the physical address of a node when the internet address is known.

(iii) IMAP : (Interactive Mail Access Protocol) : The basic idea behind IMAP is for the e-mail server to maintain a central repository that can be accessed from any machine.

(iv) POP : (Post Office Protocol) : A client server protocol that is used between a user work station & a

mail server.

(v) FTP : (File Transfers Protocol) : In TCP/IP, an application layer protocol that transfers files between two sites.

(vi) ICMP : (Internet Control Message Protocol) : A protocol in TCP/IP protocol suit that handles error & control messages.

(vii) RARP : (Reverse Address Resolution Protocol) : A TCP/IP protocol that allows a host to find its internet address given its physical address.

(viii) HTTP : (Hyper Text Transfer Protocol) : An application service for retrieving a web document.

(ix) DNS : (Domain Name System) : A TCP/IP application service that converts user friendly names to I/P addresses.

(x) SONET : (Synchronous Optical Network) : A standard developed by ANSI for fiber optic technology that can transmit high speed data. It can be used to deliver text, audio & video.

Q. 5. (a) What do you mean by IP addressing, IP address classes and subnet addressing? Explain.

Ans. IP Addressing : An address that identifiers the connection of a host to its network. Each Internet address consists of four bytes (32 bits), defining three fields : Class type, netid and hostid. These parts are of varying lengths, depending on the class of the address (see fig.).

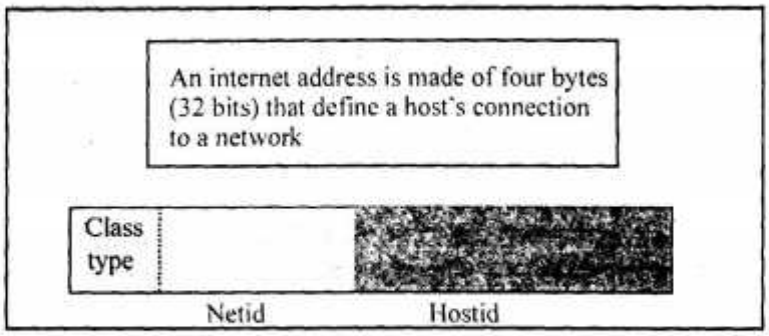


Fig. Internet Address

IP Address Classes : There are currently five different field-length patterns in use, each defining a class of address. The different classes are designed to cover the needs of different types of organizations. For example, class A addresses are numerically the lowest. They use only one byte to identify class type and netid and leave three bytes available for hostid numbers. This division means that class A networks can accommodate for more hosts than can class B or class C networks, which provide two and one byte hostid fields, respectively. Currently both class A and class B are full. Addresses are available in class C only. Class D is reserved for multicast addresses. Multicasting allows copies of a datagram to be passed to a select group of hosts rather than to an individual host. It is similar to broadcasting, but, where broad-casting requires that a packet be passed to all possible destinations, multicasting allows transmission to a selected subset. Class E addresses are reserved for future use.

Subnetting Addressing : It is the further division of a network into smaller networks called subnetworks. For example, Fig. 2. shows the network in fig. 1 divided into three subnetworks. In this example, the rest of the Internet is not aware that the network is divided into three physical subnetworks. The three subnetworks still appear as a single network to the rest of the Internet. A packet destined for host 141.14.2.21 still reaches router R1. The destination address of the IP datagram is still a class B address where 141.14 defines the netid and 2.21 defines hostid. However, when the packet arrivs at router R1 the interpretation of the I/P address changes. Router R1 knows that the network 141.14 is physically divided into three subnetworks. It knows that the last

two octets define two things : Subnetid and hostid. Therefore, 2.21 must be interpretel as subnetid 2 and host 21. The router R1 uses the first two octets (141.14) as the netid, the third octet (2) a: the subnetid and four octet (21) as the hostid.

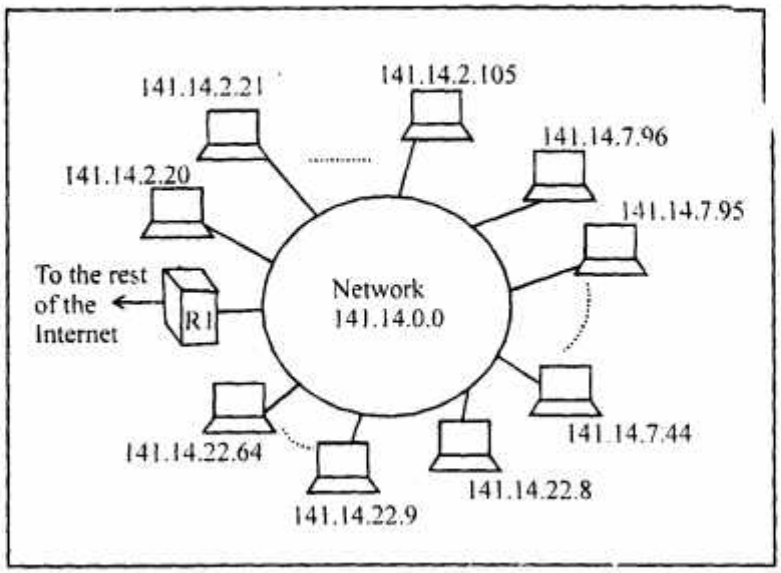


Fig. A network with two levels of hierarchy (not subnetted)

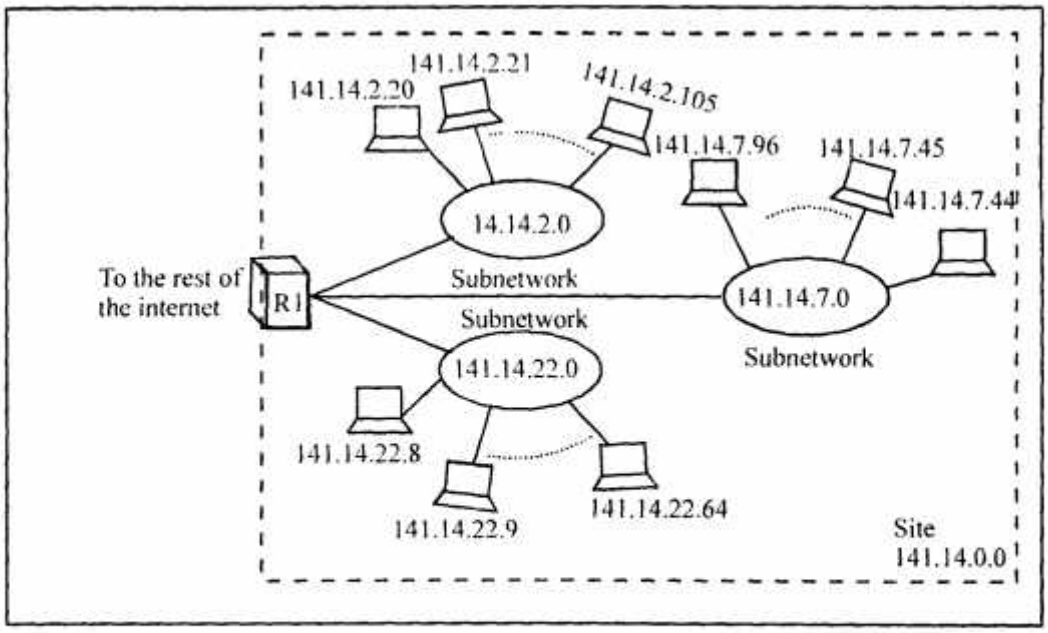


Fig. A network with three levels of hierarchy (subnetted)

Q. 5. (b) Differentiated the following :

(i) IPV6 to IPV4 **(ii) Bridge, Router and Gateway.**

Note that a sink tree is not necessarily unique: other trees with the same path lengths may exist. The goal of all routing algorithms is to discover and use the sink trees for all routers.

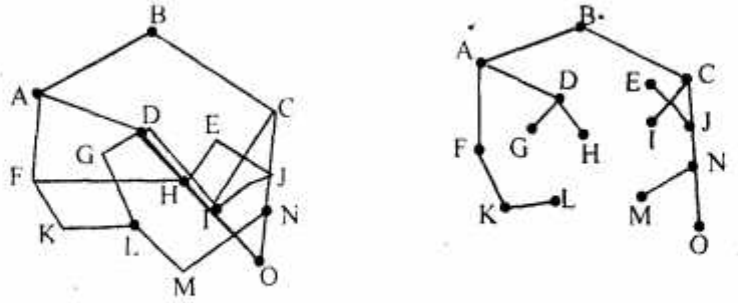


Fig. A subnet (b) A sink tree for router B

Q. 6. (b) What do you mean by Congestion Control? On which principle it work? Explain by example.

Ans. Congestion Control : Congestion in a network may occur if users send data into the network at a rate greater than that allowed by network resources. For example, congestion may occur because the switches in a network have a limited buffer size to store arrived packets before processing. Congestion in a frame relay network is a problem that must be avoided because it decreases throughput and increases delay. A high throughput and low delay are the main goals of the frame relay protocol. A packet-switched network such as X.25 uses flow control at both the data link layer and the network layer. Flow control at the network layer is end-to-end. Flow control at the data link layer is node-to-node. Both mechanisms prevent users from sending excessive traffic into the network. Frame relay protocol does not have a network layer. Even at the data link layer, frame relay does not use flow control. In addition, frame relay allows the user to transmit bursty data. This means that a frame relay network has the potential to be really congested with traffic, thus requiring congestion control.

General Principles of Congestion Control : Many problems in complex systems, such as computer networks, can be viewed from a control theory point of view. This approach leads to dividing all solutions into two groups : open loop and closed loop. Open loop solutions attempt to solve the problem by good design, in essence, to make sure it does not occur in the first place. Once the system is up and running, midcourse corrections are not mode. Tools for doing open-loop control include deciding when to accept new traffic, deciding when to discard packets and which ones and making scheduling decisions at various points in the network. All of these have in common the fact that they make decisions without regard to the current state of the network. In contrast, closed loop solutions are based on the concept of a feedback loop. This approach has three parts when applied to congestion control :

1. Monitor the system to detect when and where congestion occurs.
2. Pass this information to places where action can be taken.
3. Adjust system operation to correct the problem.

Various metrics can be used to monitor the subnet for congestion. Chief among these are the percentage of all packets discarded for lack of buffer space, the average queue lengths, the number of packets that time out and are retransmited, the average packet delay and the standard deviation of packet delay. In all cases, rising numbers indicate growing congestion.

Q. 7. Explain the following :

(i) Quality of services,

(ii) Remote Monitoring Techniques,

(iii) Firewalls.

Ans. (i) Quality of Service : Quality of service is an important issue for ATM networks, in part because they are used for real-time traffic, such as audio and video. When a virtual circuit is established, both the transport layer and the ATM network layer must agree on a contract defining the service. In the case of a public network, this contract may have legal implications. The contract between the customer and the network has three parts :

1. The traffic to be offered.
2. The service agreed upon.
3. The compliance requirements.

It is work noting that the contract may be different for each direction. The first part of the contract is the traffic descriptor. It characterizes the load to be offered. The second part of the contract specifies the quality of service desired by the customer and accepted by the carrier. Both the load and the service must be formulated in terms of measurable quantities, so compliance can be objectivity determined. Merely saying "moderate load" or "good service" will not do. To make it possible to have concrete traffic contracts, the ATM standard defines a number of QoS (Quality of Service) parameters whose values the customer and carrier can negotiate. For each quality of service parameters, the worst case performance for each parameter is specified and the carrier is required to meet or exceed it. In some cases, the parameter is a minimum; in other it is a maximum. Again here, the quality of service is specified separately for each direction. Some of the more important ones are listed in fig., but not all of them are applicable to all service categories.

Parameter	Acryonym	Meaning
Peak cell rate	PCR	Maximum rate at which cells will be sent.
Sustained cell rate	SCR	The long-term average cell rate
Minimum cell rate	MCR	The minimum acceptable cell rate
Cell delay variation tolerance	CDVT	The maximum acceptable cell jitter
Cell loss ratio	CLR	Fraction of cells lost or delivered too late
Cell transfer delay	CTD	How long delivery takes (mean and maximum)
Cell delay variation	CDV	The variance in cell delivery times
Cell error rate	CER	Fraction of cells delivered without error
Severely-errored cell block ratio	SECBR	Fraction of blocks garbled
Cell misinsertion rate	CMR	Fraction of cells delivered to wrong destination

Fig. Some of the quality of service parameters

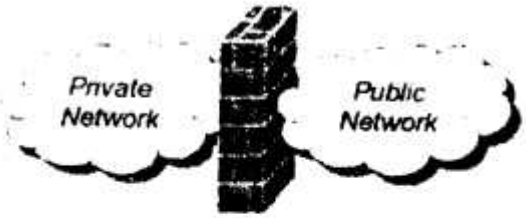
(ii) Remote Monitoring Techniques : CSMA/CD (Carrier Sense Multiple Access/with Collision Detection) is the result of an evolution from multiple access (MA) to carrier sense multiple access with collision detection (CSMA/CD).

Whenever multiple users have unregulated access to a single line, there is a danger of signals overlapping & destroying each other. Such overlaps, which turn the signals into unusable noise, are called collisions.

As traffic increases on a multiple access link, so do collisions. A Lan, therefore, needs a mechanism to coordinate traffic, minimize the no. of collisions that occur, & maximize the no. of frames that are delivered successfully. The access mechanism used is CSMA/CD

In a CSMA system, any workstation wishing to transmit must first listen for existing traffic on the line. A device listens by checking for a voltage. If no voltage is detected, the line is considered idle & the transmission is initiated. CSMA cuts down on the no. of collisions but does not eliminate them. Collisions can still occur. If another station has transmitted too recently for its signal to have reached the listening station, the listener assumes the line is idle & introduces its own signal onto the line. The final step is the addition of collision detection (CD). In CSMA/CD the station wishing to transmit first listens to make certain the link is free, then transmits its data, then listens again. During the data transmission the station checks the line for the extremely high voltages that indicate a collision. If a collision is detected, the station quite the current transmission & waits & predetermined amount of time for the line to clear, then sends its data again.

(iii) Firewalls : A firewall is a hardware or software device which is configured to permit, deny or proxy data through a computer network which has different levels of trust.



Firewall separating zones of trust

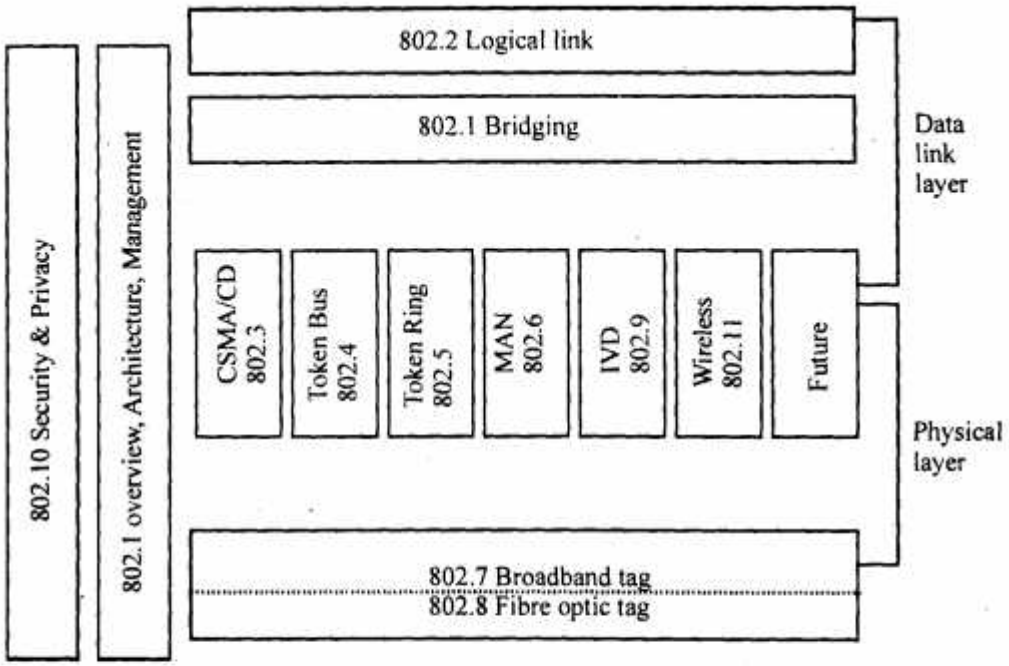
Function : A firewall's basic task is to transfer traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone (DMZ).

A firewall's function within a network is similar to firewalls in building construction, because in both cases they are intended to isolate one "network" or "compartment" from another. However, network firewalls, unlike physical farewells, are designed to allow some traffic to flow.

Without proper configuration, a firewall can often become worthless. Standard security practices dictate a "default-deny" firewall ruleset, in which the only network connections which are allowed are the ones that have been explicitly allowed. Unfortunately, such a configuration requires detailed understanding of the network applications and endpoints required for the organization's day-to-day operation. Many businesses lack such understanding and therefore implement a "defualt-allow" ruleset, in which all traffic is allowed unless it has been specifically blocked. This configuration makes inadvertent network connections and system compromise much more likely.

Q. 8. (a) Differentiate various types of LAN standards.

Ans. Various Types of LAN Standards : The Institute of Electric and Electronics Engineers (IEEE) publishes several widely accepted LAN recommended standards. These standards are very important because they encourage the use of common approaches for LAN protocols and interfaces. The IEEE LAN committes are organised as follows :



Where CSMA/CD = Carrier sense multiple access/collision detection.

MAN = Metropolitan Area Network

IVD = Integrated Voice Date.

Fig. IEEE 802 standards

IEEE 802.1 : High level Interface (and Medium Access Control, MAC, bridges).

IEEE 802.2 : Logical Link Control (LLC).

IEEE 802.3 : Carrier Sense Multiple Access/Collision Detection (CSMA/CD)

IEEE 802.4 : Token Bus

IEEE 802.5 : Token ring

IEEE 802.6 : Metropolitan Area Networks

IEEE 802.7 : Broadband LANs

IEEE 802.8 : Fibre optic LANs

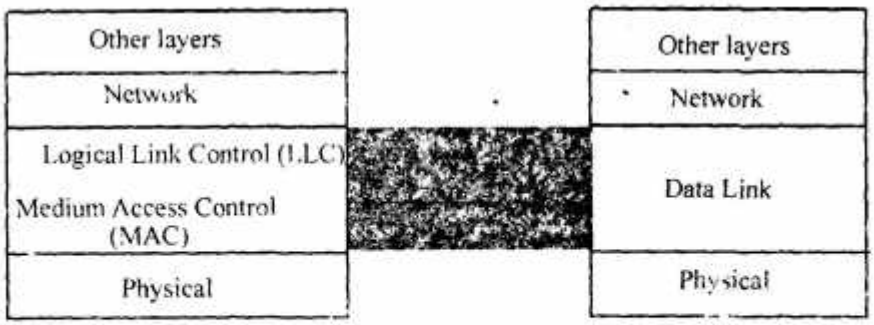
IEEE 802.9 : Integrated data and voice networks

IEEE 802.10 : Security

IEEE 802.11 : Wireless Networks

IEEE 802 Standards : The IEEE has sub-divided the data link layer into two sub-layers : Logical Link Control (LLC) and medium Access Control (MAC).

LLC is a non-architecture specific, that is, it is the same for all IEEE defined LANs. MAC sub-layer contains a number of distinct modules; each carrier proprietary information specific to the LAN product being used.



Q. 8. (b) Explain ATM in detail.

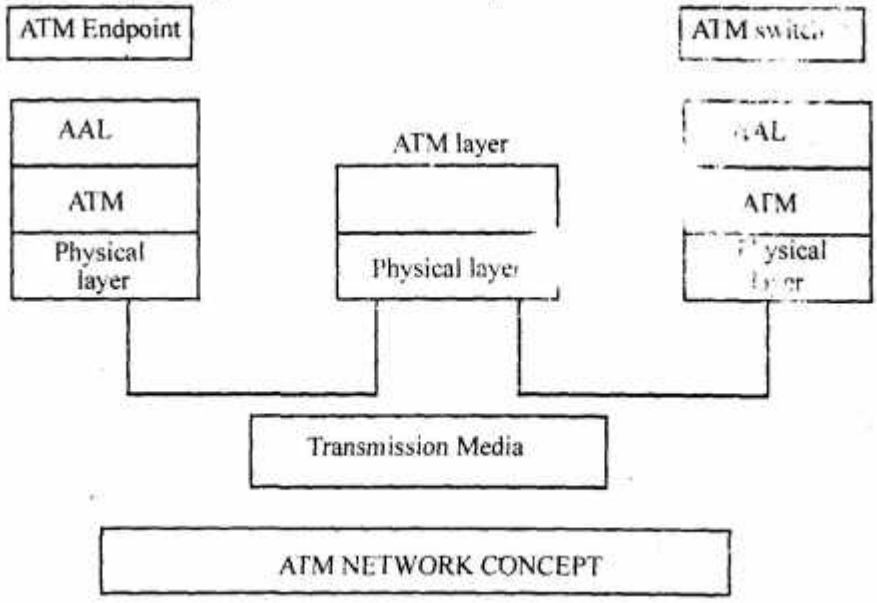
Ans. ATM : Asynchronous Transfer Mode (ATM) is the cell relay protocol designed by ATM forum and adopted by ITU-T. The combination of ATM and B-ISDN will allow high speed interconnection of all the world's networks. ATM can be thought of as the "highway" for the information superhighway.

ATM Operation : ATM represents cell-switching technology that can operate at speeds ranging from T1 1.544 MBPS to gigabit speeds of SONET. The ATM components are :

1. ATM network interface cards.
2. ATM LAN switches.
3. ATM Routers.
4. ATM WAN switches.
5. ATM services processors.

ATM Network :

1. It is a network of end point and switches.
2. The ATM layer can reside at either location.
3. The physical layer is requested at both ATM end-points and ATM switches.



ATM NETWORK CONCEPT