Vidyalankar

S.Y. Diploma : Sem. IV [CO/CD/CM/CW]

Computer Network

Prelim Question Paper Solution

1. (a) (i) There are two modes for propagating light along optical channels, multimode and singlemode.

- **Multimode:** Multiple beams from a light source move through the core in different paths.
- **Single mode:** Fiber with extremely small diameter that limits beams to a few angles, resulting in an almost horizontal beam.

1. (a) (ii) Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer are taken.

1. (a) (iii) In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

1. (a) (iv) The Guided Media differing from Unguided Transmission Media

	Guided Transmission Media	Unguided Transmission Media
1)	Guided indicate, medium is contained have any within physical boundary	Unguided medium does not Physical boundary
2)	Transmission takes place through wire.	It is a wireless transmission.

1. (a) (v) Specific responsibilities of data link layer include the following.

1) Framing
2) Physical addressing
3) Flow control
4) Error control
5) Access control

1. (a) (vi) The four internetworking devices are,

- Repeaters
- Bridges
- Routers
- Gateway

Vidyalankar

1. (a) (vii)IP address is the 32-bit number for representing a host or system in the network. One portion of the IP address indicates a networking and the other represents the host in a network.

1. (a) (viii) Segmentation

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation

1. (b) (i) Difference between Network Layer Delivery and the Transport Layer Delivery

- The network layer is responsible for the source-to-destination delivery of packet.
- The transport layer is responsible for source-to-destination delivery of the entire message.
- Transport layer delivery across multiple network links.
- The transport layer is responsible for source-to-destination delivery of the entire message.

1. (b) (ii) Coaxial Cable

Coaxial cable is a common transmission medium. It has better shielding than twisted pairs, so it can pan longer distances at higher speeds. Two kinds of coaxial cable are widely used. One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start. The other kind, 75-ohm cable, is commonly used for analog transmission and cable television but is becoming more important with the advent of Internet over cable. This distinction is based on historical, rather than technical, factors (e.g., early dipole antennas had an impedance of 300 ohms, and it was easy to use existing 4:1 impedance matching transformers).

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh. The outer conductor is covered in a protective plastic sheath. A cutaway view of a coaxial cable is shown in Figure.

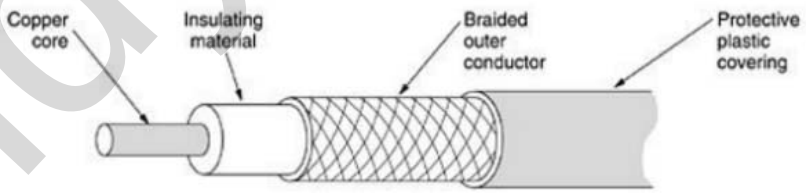


Fig. : A coaxial cable.

The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable quality, length, and signal-to-noise ratio of the data signal. Modern cables have a andwidth of close to 1 GHz. Coaxial cables used to be widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on long-haul routes. Coax is still widely used for cable television and metropolitan area networks.

Vidyalankar

1. (b) (iii) Circuit switching and packet switching differ in many respects. Circuit switching requires that a circuit be set up end to end before communication begins. Packet switching does not require any advance setup. The first packet can just be sent as soon as it is available.

The result of the connection setup with circuit switching is the reservation of bandwidth all the way from the sender to the receiver. All packets follow this path. Among other properties, having all packets follow the same path means that they cannot arrive out of order. With packet switching there is no path, so different packets can follow different paths, depending on network conditions at the time they are sent. They may arrive out of order.

Another difference is that circuit switching is completely transparent. The sender and receiver can use any bit rate, format, or framing method they want to. The carrier does not know or care. With packet switching, the carrier determines the basic parameters. A rough analogy is a road versus a railroad. In the former, the user determines the size, speed, and nature of the vehicle; in the latter, the carrier does. It is this transparency that allows voice, data, and fax to coexist within the phone system.

Item	Circuit switched	Packet switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
Time of possible congestion	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

2. (a) The problems in OSI Model and Protocols.

- Bad timing.
- Bad technology.
- Bad implementations.
- Bad politics.

- **Bad Timing:** The time at which a standard is established is absolutely critical to its success. David Clark of M.I.T. has a theory of standards that he calls the apocalypse of the two elephants.
  This figure shows the amount of activity surrounding a new subject. When the subject is first discovered, there is a burst of research activity in the form of discussions, papers, and meetings. After a while this activity subsides, corporations discover the subject, and the billion-dollar wave of investment hits.

- **Bad Technology:** The second reason that OSI never caught on is that both the model and the protocols are flawed. The choice of seven layers was more

Vidyalankar

political than technical, and two of the layers (session and presentation) are nearly empty, whereas two other ones (data link and network) are overfull.
The OSI model, along with the associated service definitions and protocols, is extraordinarily complex. When piled up, the printed standards occupy a significant fraction of a meter of paper. They are also difficult to implement and inefficient in operation. In addition to being incomprehensible, another problem with OSI is that some functions, such as addressing, flow control, and error control, reappear again and again in each layer.

- **Bad Implementations:** Given the enormous complexity of the model and the protocols, it will come as no surprise that the initial implementations were huge, unwieldy, and slow. Everyone who tried them got burned. It did not take long for people to associate "OSI" with "poor quality."
  Although the products improved in the course of time, the image stuck.

- **Bad Politics:** On account of the initial implementation, many people, especially in academia, thought of TCP/IP as part of UNIX, and UNIX in the 1980s in academia was not unlike parenthood (then incorrectly called motherhood) and apple pie.
  OSI, on the other hand, was widely thought to be the creature of the European telecommunication ministries, the European Community, and later the U.S. Government. This belief was only partly true, but the very idea of a bunch of government bureaucrats trying to shove a technically inferior standard down the throats of the poor researchers and programmers down in the trenches actually developing computer networks did not help much.

2. (b) Bluetooth

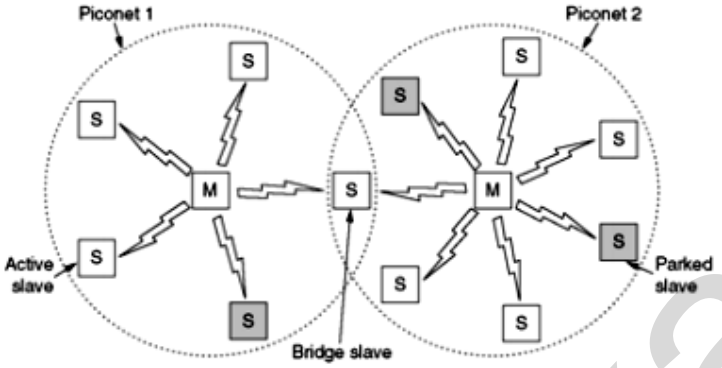
A wireless standard for interconnecting computing and communication devices and accessories using short-range, low-power, inexpensive wireless radios Bluetooth SIG: formed by Ericsson, IBM, Intel, Nokia and Toshiba Named after Harald Blaatand (Bluetooth) II (940-981) A Viking king who unified Denmark and Norway, also without cables Bluetooth SIG issued a 1500- page spec v1.0, in 1999 IEEE 802.15 standardizes only the physical and data link layers As a personal area network (PAN) standard.

- **Piconet :** basic unit of a Bluetooth system Consists of a master node and up to seven active slave nodes within a distance of 10 meters, and up to 255 parked nodes Master node controls the clock and de termines which device gets to communicate in which time slot, using TDM Slave nodes are fairly dumb, just doing whatever the master tells them to do

- **Parked nodes :** devices that the master has switched to a low-power state, they respond only to an activation or beacon signal from the master All communication is between the master and a slave; direct slave-slave communication is not possible

Bluetooth Architecture

Scatternet : an interconnected collection of piconets
Connected via a bridge node



2. (c)

- **Connection-oriented service :** Connection-oriented service is modelled after the telephone system. To talk to someone, pick up the phone, dial the number, talk, and then hang up. Similarly, to use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. The essential aspect of a connection is that it acts like a tube: the sender pushes objects (bits) in at one end, and the receiver takes them out at the other end. In most cases the order is preserved so that the bits arrive in the order they were sent.

  In some cases when a connection is established, the sender, receiver, and subnet conduct a negotiation about parameters to be used, such as maximum message size, quality of service required, and other issues. Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal. A typical situation in which a reliable connection-oriented service is appropriate is file transfer. The owner of the file wants to be sure that all the bits arrive correctly and in the same order they were sent.

- **Connectionless service :** In contrast, connectionless service is modelled after the postal system. Each message (letter) carries the full destination address, and each one is routed through the systemindependent of all the others. Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive. However, it is possible that the first one sent can be delayed so that the second one arrives first.

  Not all applications require connections. For example, as electronic mail becomes more common, electronic junk is becoming more common too. The electronic junk-mail sender probably does not want to go to the trouble of setting up and later tearing down a connection just to send one item. Nor is 100 percent reliable delivery essential, especially if it costs more All that is needed is a way to send a single message that has a high probability of arrival, but no guarantee. Unreliable (meaning not acknowledged) connectionless service is often called datagram service, in analogy with telegram service, which also does not return an acknowledgement to the sender.

Vivek Ghankar

2. (d) Satellites are specifically made for telecommunication purpose. They are used for mobile applications such as communication to ships, vehicles, planes, hand-held terminals and for TV and radio broadcasting.

Satellites orbit around the earth. Depending on the application, these orbits can be circular or elliptical. Satellites in circular orbits always keep the same distance to the earth‟s surface following a simple law.

Types of Satellites (based on orbits)

- **Geostationary or geosynchronous earth orbit (GEO):** GEO satellites are synchronous with respect to earth. Looking from a fixed point from Earth, these satellites appear to be stationary. These satellites are placed in the space in such a way that only three satellites are sufficient to provide connection throughout the surface of the Earth (that is; their footprint is covering almost 1/3rd of the Earth). The orbit of these satellites is circular.

- **Low Earth Orbit (LEO) satellites:** These satellites are placed 500-1500 kms above the surface of the earth. As LEOs circulate on a lower orbit, hence they exhibit a much shorter period that is 95 to 120 minutes. LEO systems try to ensure a high elevation for every spot on earth to provide a high quality communication link. Each LEO satellite will only be visible from the earth for around ten minutes.

- **Medium Earth Orbit (MEO) satellites:** MEOs can be positioned somewhere between LEOs and GEOs, both in terms of their orbit and due to their advantages and disadvantages. Using orbits around 10,000 km, the system only requires a dozen satellites which is more than a GEO system, but much less than a LEO system. These satellites move more slowly relative to the earth‟s rotation allowing a simpler system design (satellite periods are about six hours). Depending on the inclination, a MEO can cover larger populations, so requiring fewer handovers.

Applications of Satellites

Weather Forecasting Radio and TV Broadcast Military Satellites Navigation Satellites.

2. (e) The network layer provides services to the transport layer at the network layer/transport layer interface. The network layer services have been designed with the following goals in mind.

- The services should be independent of the router technology.
- The transport layer should be shielded from the number, type, and topology of the routers present.
- The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.
- Given these goals, the designers of the network layer have a lot of freedom in writing detailed specifications of the services to be offered to the transport layer. This freedom often degenerates into a raging battle between two warring factions. The discussion centers on whether the network layer should provide connection-oriented service or connectionless service.

Vidyalankar

One camp (represented by the Internet community) argues that the routers' job is moving packets around and nothing else. In their view (based on 30 years of actual experience with a real, working computer network), the subnet is inherently unreliable, no matter how it is designed. Therefore, the hosts should accept the fact that the network is unreliable and do error control (i.e., error detection and correction) and flow control themselves.

This viewpoint leads quickly to the conclusion that the network service should be connectionless, with primitives SEND PACKET and RECEIVE PACKET and little else. In particular no packet ordering and flow control should be done, because the hosts are going to do that anyway, and there is usually little to be gained by doing it twice. Furthermore, each packet must carry the full destination address, because each packet sent is carried independently of its predecessors, if any.

The other camp (represented by the telephone companies) argues that the subnet should provide a reliable, connection-oriented service. They claim that 100 years of successful experience with the worldwide telephone system is an excellent guide. In this view, quality of service is the dominant factor, and without connections in the subnet, quality of service is very difficult to achieve, especially for real-time traffic such as voice and video.

These two camps are best exemplified by the Internet and ATM. The Internet offers connectionless network-layer service; ATM networks offer connection-oriented network layer service.

2. (f) Serial Transmission

In serial transmission all the bits are transrnitted in a serial manner over a single communication line. Serial transmission can be either asynchronous or synchronous.

- **Asynchronous Serial Transmission:** the timing constraints into consideration. Instead, both the communicating panics are agreed upon some specific patterns with which a receiver can retrieve information without considering the order in which the bits are transmitted. The agreed upon patterns are based on grouping of hits into bytes, each consisting of 8 bits.

  As time is not an important constraint in asynchronous transmission, a convention has been followed to alert the receiver about the arrival of a new group in which an extra '0' bit, called the start bit is added a the beginning of each byte and a bit 1, called the stop bit is inserted at the end of the byte being transmitted. As a result of which the size of the byte is increased to 10 bits, of which. 8 hits represent the actual information and 2 bits arc used to alert the receiver.

  A varying duration is maintained between the successive bytes. This can be represented either by an idle channel or by a stream of stop hits. This method is called Asynchronous because the sender and the receiver need not be synchronized with each other, but within each byte, synchronization is still maintained between the receiver and the incoming bit stream.

Vidyalankar

Advantages:
1) It is cheap and effective.
2) It is a preferred choice for low speed communication.

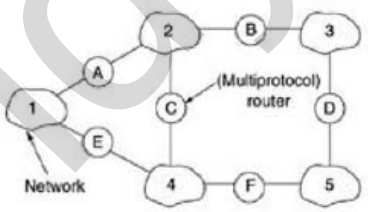
Disadvantage
The insertion of start and stop bits and gaps into the bit stream makes it slower than synchronous data transmission.

- **Synchronous Transmission :** In synchronous type of data transmission, the incoming bit stream is grouped to form longer frames containing multiple bytes with no spacing between the successive bytes. The bit streams arc then combined to form bytes by the receiver and are used for decoding purposes i.e., the incoming data is sent as an unbroken string of l's and 0's. These strings are separated into the bytes and characters for reconstructing the information. As no start and stop hits and the gap between bytes are available, timing between the successive bytes is critical. This is because the accuracy of the received information is entirely dependent on the ability of the receiver in maintaining the accurate count of the received bits.

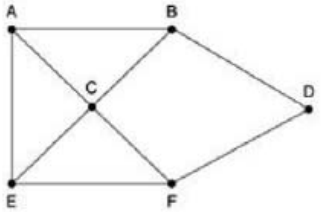
Advantages:
1) Synchronous data transmission is faster than the asynchronous data transmission because of the absence of start and stop bits and the non availability of the gaps between them. Hence, used for pc-to- pc communication.
2) Byte synchronization can be achieved in the data link layer.

3. (a) Internetworking Routing

Routing through an internetwork is similar to routing within a single subnet, but with some added complications. Consider, for example, the internetwork of Fig. (a) in which five networks are connected by six (possibly multiprotocol) routers. Making a graph model of this situation is complicated by the fact that every router can directly access (i.e., send packets to) every other router connected to any network to which it is connected. For example, B in Fig. (a) can directly access A and C via network 2 and also D via network 3.
This leads to the graph of Fig. (b).



(a) An internetwork.



(b) A graph of the internetwork.

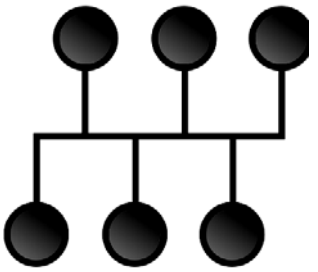
Once the graph has been constructed, known routing algorithms, such as the distance vector and link state algorithms, can be applied to the set of multiprotocol routers. This gives a two-level routing algorithm: within each network an interior gateway protocol is used, but between the networks, an exterior gateway protocol is used ("gateway" is an older term for "router"). In fact, since each network is independent, they may all use different algorithms.

Because each network in an internetwork is independent of all the others, it is often referred to as an Autonomous System (AS). A typical internet packet starts out on its LAN addressed to the local multiprotocol router (in the MAC layer header). After it gets there, the network layer code decides which multiprotocol router to forward the packet to, using its own routing tables. If that router can be reached using the packet's native network protocol, the packet is forwarded there directly. Otherwise it is tunneled there, encapsulated in the protocol required by the intervening network. This process is repeated until the packet reaches the destination network.

One of the differences between internetwork routing and intranetwork routing is that internetwork routing may require crossing international boundaries. Various laws suddenly come into play, such as Sweden's strict privacy laws about exporting personal data about Swedish citizens from Sweden. Another example is the Canadian law saying that data traffic originating in Canada and ending in Canada may not leave the country. This law means that traffic from Windsor, Ontario to Vancouver may not be routed via nearby Detroit, even if that route is the fastest and cheapest.

Another difference between interior and exterior routing is the cost. Within a single network, a single charging algorithm normally applies. However, different networks may be under different managements, and one route may be less expensive than another. Similarly, the quality of service offered by different networks may be different, and this may be a reason to choose one route over another.

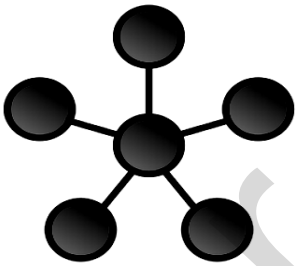
3. (b) **Bus topology :** In local area networks where bus topology is used, each node is connected to a single cable. Each computer or server is connected to the single bus cable. A signal from the source travels in both directions to all machines connected on the bus cable until it finds the intended recipient. If the machine address does not match the intended address for the data, the machine ignores the data. Alternatively, if the data matches the machine address, the data is accepted. Since the bus topology consists of only one wire, it is rather inexpensive to implement when compared to other topologies. However, the low cost of implementing the technology is offset by the high cost of managing the network. Additionally, since only one cable is utilized, it can be the single point of failure. If the network cable is terminated on both ends and when without termination data transfer stop and when cable breaks, the entire network will be down.



STAR Topology: In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the peripherals are the clients. The network does not necessarily have to resemble a star to be classified as a star network, but all of the nodes on the network must be

Vijayalakshmi

connected to one central device. All traffic that traverses the network passes through the central hub. The hub acts as a signal repeater. The star topology is considered the easiest topology to design and implement. An advantage of the star topology is the simplicity of adding additional nodes. The primary disadvantage of the star topology is that the hub represents a single point of failure.

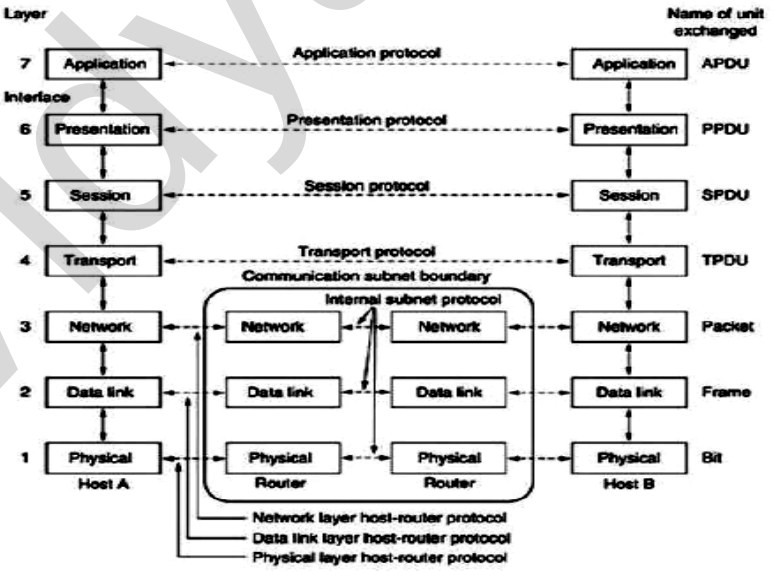


3. (c) The OSI Reference Model

The OSI model (minus the physical medium) is shown in Fig . This model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers (Day and Zimmermann, 1983). It was revised in 1995(Day, 1995). The model is called the ISO-OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.



Vidyalankar

OSI Reference model

The Physical Layer: The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit.

The Data Link Layer: The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

The Network Layer: The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

The Transport Layer: The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates the upper layers from the inevitable changes in the hardware technology.

The Session Layer: The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

The Presentation Layer: The presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

The Application Layer: The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for file transfer, electronic mail, and network news.

Vidyalankar

3. (d) Client-server model

In this model, the data is stored on powerful computers called servers. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simpler machines, called clients, on their desks, with which they access remote data, for example, to include in spreadsheets they are constructing. (Sometimes we will refer to the human user of the client machine as the "client," but it should be clear from the context whether we mean the computer or its user.)

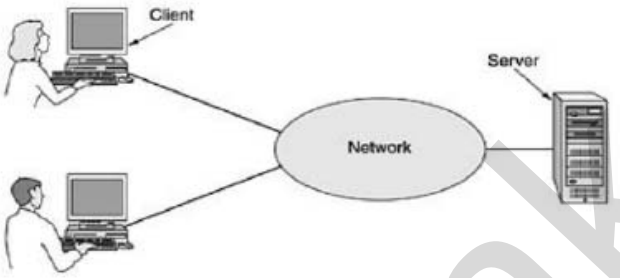


Fig. : A network with two clients and one server.

This whole arrangement is called the client-server model. It is widely used and forms the basis of much network usage. It is applicable when the client and server are both in the same building (e.g., belong to the same company), but also when they are far apart. For example, when a person at home accesses a page on the World Wide Web, the same model is employed, with the remote Web server being the server and the user's personal computer being the client. Under most conditions, one server can handle a large number of clients.

3. (e) Vertical Communication in OSI

In OSI Reference Model parlance, the mechanism for communication between adjacent layers in the model is called an *interface*. Of course, the term “interface” is also used widely in other contexts in the computer and networking worlds, since its generic meaning refers to connecting just about anything together. However, when someone talks about an interface between OSI model layers, that person typically refers to the process by which data is passed between layer N of the model and layer N-1 or layer N+1.

Vertical Communication: Vertical communication is done up and down the protocol stack every time anything is sent across the network, and of course, whenever anything is received. This occurs because the higher levels are implemented as logical functions, in software; there is no actual physical connection. The higher layers package data and send it down to the lower layers for it to be sent across the network. At the very lowest level, the data is sent over the network. On the receiving end, the process is reversed, with the data traveling back up to the higher layers on the receiving device. The next topic dealing with horizontal communication explains more about this logical interaction between corresponding layers

Vidyalankar

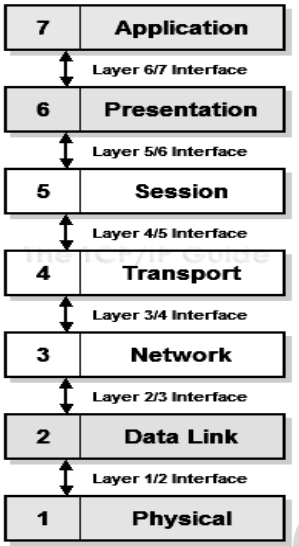


Fig. : OSI Reference model interfaces for Vertical Communication.

3. (f) Peer-to-peer

The peer-to-peer Communication is a type of person-to-person communication. In this form, individuals who form a loose group can communicate with others in the group, as shown in Figure. Every person can, in principle, communicate with one or more other people; there is no fixed division into clients and servers.

Peer-to-peer communication really hit the big time around 2000 with a service called Napster, which at its peak had over 50 million music fans swapping music, in what was probably the biggest copyright infringement in all of recorded history. The idea was fairly simple. Members registered the music they had on their hard disks in a central database maintained on the Napster server. If a member wanted a song, he checked the database to see who had it and went directly there to get it. By not actually keeping any music on its machines, Napster argued that it was not infringing anyone's copyright. The courts did not agree and shut it down.

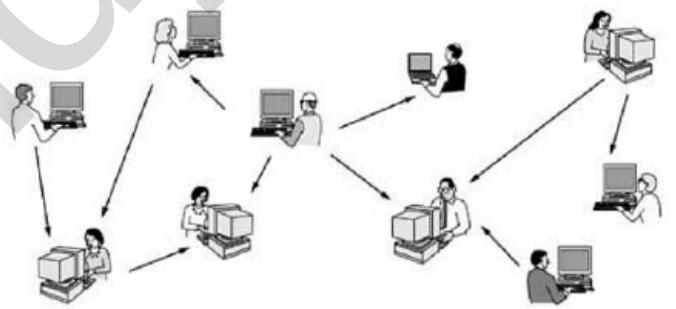


Fig. : In a peer-to-peer system there are no fixed clients and servers.

vidyalankar

4. (a) Compare IPV4 and IPV6

	IPV4	IPV6
1)	Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length. For more information, see IPv6 addressing.
2)	Uses broadcast addresses to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, multicast scoped addresses are used. For more information, see Multicast scope.
3)	Fragmentation is supported at originating hosts and intermediate routers.	Fragmentation is not supported at routers. It is only supported at the originating host. For more information, see Fragmentation in an IPv6 network.
4)	IP header includes a checksum.	IP header does not include a checksum.
5)	IP header includes options.	All optional data is moved to IPv6 extension headers. For more information, see Extension headers.
6)	IPSec support is optional.	IPSec support is required in a full IPv6 implementation.
7)	No identification of payload for QoS handling by routers is present within the IPv4 header.	Payload identification for QoS handling by routers is included in the IPv6 header using the Flow Labelfield. For more information, see Option to provide QoS classification data.

4. (b) Subnet Masking

An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>). It is called a subnet mask because it is used to identify network address of an IP address by perfoming bitwise AND operation on the netmask.

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to a host.

Subnetting an IP network is to separate a big network into smaller multiple networks for reorganization and security purposes. All nodes (hosts) in a subnetwork see all packets transmitted by any node in a network. Performance of a network is adversely affected under heavy traffic load due to collisions and retransmissions.

Vidyalankar

Applying a subnet mask to an IP address separates network address from host address. The network bits are represented by the 1's in the mask, and the host bits are represented by 0's. Performing a bitwise logical AND operation on the IP address with the subnet mask produces the network address. For example, applying the Class C subnet mask to our IP address 216.3.128.12 produces the following network address:

```
IP:     1101 1000 . 0000 0011 . 1000 0000 . 0000 1100  (216.003.128.012)
Mask:   1111 1111 . 1111 1111 . 1111 1111 . 0000 0000  (255.255.255.000)
        ---------------------------------------------
        1101 1000 . 0000 0011 . 1000 0000 . 0000 0000  (216.003.128.000)
```

4. (c) **Dual cable**

Dual cable systems have two identical cables, cablel1 is used to transmit data (inbound communication) and cable2 is used to receive (outbound communication). A computer that wants to transmit data, it will sent data to cabel1 which is received by a device called the head-end at the root of the cable tree. The head-end then send this data down the tree on to cable2 which is received by the receiver.

Single cable system

Single cable system has only a single cable but they use different frequency bands to different inbound and outbound communication. Inbound communication from the computers to the head-end uses low-frequency band.

In the subsplit system, it ranges from 5 to 30MHz and in the midsplit system it is 5 to 116MHz. The head-end receives the inbound signals, shift them to high-frequency band and transmit over the network. Outbound communication from the head-end to the computer uses high-frequency band.

4. (d) Multimode and singlemode are the two modes of propagation of light along optical channels. They differ in physical characteristics of the fiber and the light source.

Multimode: Multimode mostly use LED (Light Emitting Diode) as a light source. LED produces unfocused light that enters core at many different places and at many different angles. It is appropriate for short distances as it diffuses over distance. Therefore, in multimode the multiple beam of light from a light source follows different paths in the core. Travelling of beam in the cable depends on the structure of the core.

There are two forms of multimode,

- Step-index multimode fiber
- Graded-index multimode fiber.

- **Step-index Multimode Fiber:** In step-index multimode fiber the core and the cladding have different densities.
  Further, the density of the core is constant from the center to the edges. The beam travels through the constant density in a straight direction. When it reaches at the interface of the core and the cladding, its direction suddenly changes due to a lower density. This sudden change (refraction) leads to the distortion of the signal and hence multiple beams takedifferent paths and hits boundary at different angles. Each angle defines a new path or mode.

Vidyalankar

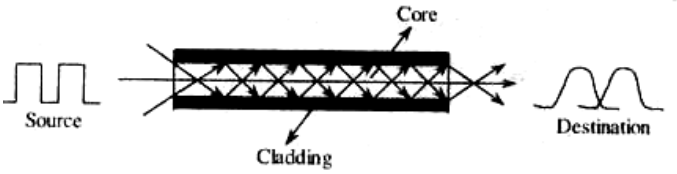


Fig. : Stepindex Multimode Fiber

- Graded-index multimode fiber : In graded-index multimode fiber, the core has varying densities. The center of the core has the highest density and it gradually decreases towards the edge. When the beam travels through the fiber it touches the boundary of the core at different places and at different angles thus giving rise to a curve. However, only the beam travelling through the center of the core travels unchanged. Hence multiple beams give rise to different curves or waveforms as shown in figure

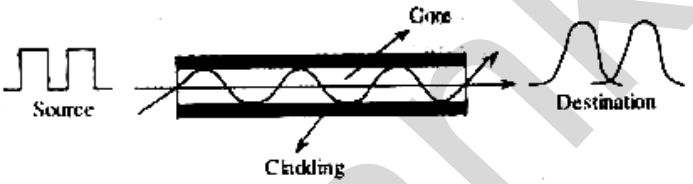


Fig. : Graded index multimode Fiber

Singlemode: A singlemode fiber uses an ILD (Injection Laser Diode) as a light source. The laser produces a focused beam of light that enters the core at small range of angles which is almost close to the horizontal line. Further, the radius of core in singlemode fiber is less than that of multimode fibers. By reducing the radius of core, only a single angle or mode can pass through the core. Thus, the beam of light propagates almost horizontally.

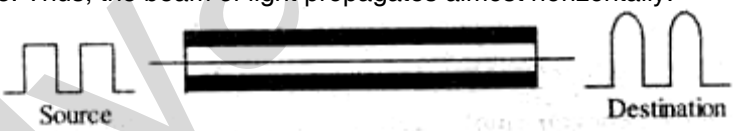


Fig. : Singtemode fiber

4. (e) **Protocol Hierarchies:** To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

This concept is actually a familiar one and used throughout computer science, where it is variously known as information hiding, abstract data types, data encapsulation, and object-oriented programming. The fundamental idea is that a particular piece of software (or hardware) provides a service to its users but keeps the details of its internal state and algorithms hidden from them.

Interfaces: Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one. When network designers decide how many layers to include in a network and what each one should do, one of the most important considerations is defining clean interfaces between the layers. Doing so, in turn, requires that each layer perform a specific collection of well-understood functions

Services: Layers can offer two different types of service to the layers above them are,

- Connection-oriented and
- Connectionless.

Request-reply is commonly used to implement communication in the client-server model: the client issues a request and the server responds to it.

4. (f) Data Link Layer Design Issues

The data link layer has a number of specific functions it can carry out. These functions include.

- Providing a well-defined service interface to the network layer.
- Dealing with transmission errors.
- Regulating the flow of data so that slow receivers are not swamped by fast senders.

To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer, as illustrated in Figure. Frame management forms the heart of what the data link layer does.

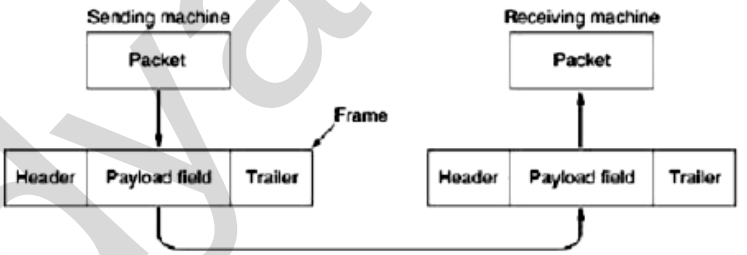


Fig. : Relationship between packets and frames.

In fact, in many networks, these functions are found only in the upper layers and not in the data link layer. However, no matter where they are found, the principles are pretty much the same, so it does not really matter where we study them. In the data link layer they often show up in their simplest and purest forms, making this a good place to examine them.

5. (a) Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a protocol used by Internet Protocol (IP), specifically IPV4, to map IP network address to the hardware addresses used by a datalink protocol. The protocol operates below the network layer as a part of the interface between OSI network and OSI link layer.

Vidyalankar

The term address resolution refers to the process of finding an address of a computer in a network. The address is resolved using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore it provides the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address. Thus, learning of 48-hit Ethernet

Working of ARP: When an incoming packet destined for a host machine on a particular Local Area Network (LAN) which arrives at gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and if it finds the IP address, provides it and sends it to the machine. If IP address is not found, ARP broadcasts a request packet in a special format to all machines on the LAN to see if any machine knows this LP address. If a machine recognizes the IP address as its own, it sends a reply. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

5. (b) **Hub:** A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability. What a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network.

Repeater: A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers. The regular amplifies everything fed into it. That means, if the input signal has noise induced into it, both the desired signal and noise signal are together amplified. But, in the case of a repeater, it regenerates the input signal, and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.

Switch: A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network. if data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses.

Bridge: A bridge is also a device which works in the Data Link Layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.

Vidyalankar

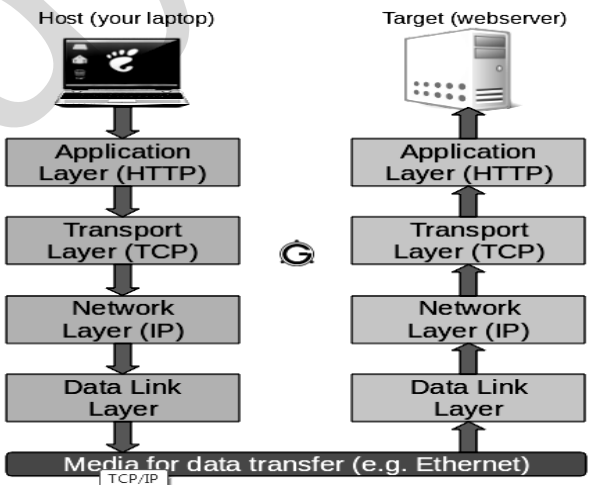
5. (c) Compare Virtual-Circuit and Datagram Subnets

	Issue	Datagram subnet	Virtual-circuit subnet
1)	Circuit setup	Not needed	Required
2)	Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number.
3)	State information	Routers do not hold state information about connections	Each VC requires router table space per connection
4)	Routing	Each packet is routed independently.	Route chosen when VC is set up; all packets follow it.
5)	Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated.
6)	Quality of service	Difficult	Easy in enough resources can be allocated in advance for each VC.
7)	Congestion control	Difficult	Easy in enough resources can be allocated in advance for each VC.

5. (d) TCP/IP Protocol Suite

Communications between computers on a network is done through protocol suits. The most widely used and most widely available protocol suite is TCP/IP protocol suite. A protocol suit consists of a layered architecture where each layer depicts some functionality which can be carried out by a protocol. Each layer usually has more than one protocol options to carry out the responsibility that the layer adheres to. TCP/IP is normally considered to be a 4 layer system. The 4 layers are as follows:

- Application layer
- Transport layer
- Network layer
- Data link layer



Vidyalankar

- **Application layer:** This is the top layer of TCP/IP protocol suite. This layer includes applications or processes that use transport layer protocols to deliver the data to destination computers.
  At each layer there are certain protocol options to carry out the task designated to that particular layer. So, application layer also has various protocols that applications use to communicate with the second layer, the transport layer. Some of the popular application layer protocols are:
  - HTTP (Hypertext transfer protocol)
  - FTP (File transfer protocol)
  - SMTP (Simple mail transfer protocol)
  - SNMP (Simple network management protocol) etc

- **Transport Layer:** This layer provides backbone to data flow between two hosts. This layer receives data from the application layer above it. There are many protocols that work at this layer but the two most commonly used protocols at transport layer are TCP and UDP.
  TCP is used where a reliable connection is required while UDP is used in case of unreliable connections.

- **Network Layer:** This layer is also known as Internet layer. The main purpose of this layer is to organize or handle the movement of data on network. By movement of data, we generally mean routing of data over the network. The main protocol used at this layer is IP. While ICMP(used by popular 'ping' command) and IGMP are also used at this layer.

- **Data Link Layer:** This layer is also known as network interface layer. This layer normally consists of device drivers in the OS and the network interface card attached to the system. Both the device drivers and the network interface card take care of the communication details with the media being used to transfer the data over the network. In most of the cases, this media is in the form of cables. Some of the famous protocols that are used at this layer include ARP(Address resolution protocol), PPP(Point to point protocol) etc.

5. (e) WiMAX and Wi-Fi are both wireless technologies but Wi-Fi can only be operated in short ranges (Max 250 m) and WiMAX could be operated in long ranges (around 30 Km). WiMAX has fixed and mobile version which could be used for several applications with higher bandwidth (around 40 Mbps). Like DSL or Cable internet in cities, WiMAX could be a cable broadband replacement in rural areas where most providers don't have copper network to offer DSL services. And 40 Mbps is much faster than even ADSL2+. Triple play services like voice, video and data could be easily offered over WiMAX. The new version of WiMAX 802.16m is expected to deliver 1 Gbps which is equivalent to Fibre to Home and it's very useful for backhauling of remote offices or provider access stations.

Difference between WiMAX and Wi-Fi

- Both operates in Microwave frequency range to offer wireless access
- Wi-Fi a short range technology mostly used in, in-house applications whereas WiMAX is a long range technology to deliver wireless broadband to far end.

- Wi-Fi is mostly an end user technology where users can purchase Wi-Fi devices and configure them by themselves and WiMAX is mostly deployed by service providers.
- Wi-Fi uses CSMA/CA protocol which could be connection based or connection less whereas WiMAX uses connection oriented MAC protocol.
- Wi-Fi is a wireless LAN technology and WiMAX is a wireless LAN technology (WLAN)

5. (f) **TCP** divides the data (coming from the application layer) into proper sized chunks and then passes these chunks onto the network. It acknowledges received packets, waits for the acknowledgments of the packets it sent and sets timeout to resend the packets if acknowledgements are not received in time. The term 'reliable connection' is used where it is not desired to loose any information that is being transferred over the network through this connection. So, the protocol used for this type of connection must provide the mechanism to achieve this desired characteristic. For example, while downloading a file, it is not desired to loose any information(bytes) as it may lead to corruption of downloaded content.

UDP provides a comparatively simpler but unreliable service by sending packets from one host to another. UDP does not take any extra measures to ensure that the data sent is received by the target host or not. The term 'unreliable connection' are used where loss of some information does not hamper the task being fulfilled through this connection. For example while streaming a video, loss of few bytes of information due to some reason is acceptable as this does not harm the user experience much.

6. (a) **SLIP and PPP**

- SLIP is obsolete and has been replaced by PPP in most applications.
- PPP can auto-configure settings while SLIP cannot.
- PPP provides error detection and recovery while SLIP doesn't.
- SLIP has very minimal overhead compared to PPP.

SLIP (Serial Line Internet Protocol) and PPP (Point-to-Point Protocol) are two protocols that are used in interconnecting two points in order to facilitate the transmission of data to and fro. Although they can be used with different types of media, the most typical use is with telephone lines for an Internet connection; used to establish digital communication between the user and the ISP. The main difference between SLIP and PPP is in their current use. SLIP is the older of the two and had a very minimal feature set. This eventually led to the creation of PPP and its more advanced features, thus rendering SLIP obsolete.

One of the key features in PPP is its ability to auto-configure its connection settings during initialization. The client and host communicate during initialization and negotiate on the best settings to be used. This is unlike SLIP which needs the settings coded beforehand in order to establish a successful connection. Auto-configuration significantly simplifies setup since most settings do not need to be entered manually.

Another essential feature added into PPP is error detection and recovery. In the process of transmitting data, it is very possible that a packet or two gets lost

Vijayalakshmi

along the way. PPP is able to detect errors and automatically initiate the recovery of the lost packets. SLIP does not have any provisions for error detection so it needs to be implemented on a higher level. Not only does this add complexity, it also increases the processing needed.

Although SLIP is obsolete and is no longer used in most computer systems, it still enjoys some use in certain systems like microcontrollers. This is because of the relatively small amount of overhead that it adds. In order to transmit a packet, PPP adds a header as well as padding information in the end. In comparison, SLIP simply adds an end character at the end of each packet. In applications where the features of PPP are not really needed, using it is just a waste of bandwidth as the header and padding would always be there. In this case, using SLIP is actually more advantageous than PPP.

6. (b) IPv6 Overview

IPv6 was designed to take an evolutionary step from IPv4. It was not a design goal to take a radical step away from IPv4. Functions that work in IPv4 were kept in IPv6.

Functions that didn't work were removed. The changes from IPv4 to IPv6 fall primarily into the following categories:

- Header Format Simplification
- Improved Support for Options
- Expanded Routing and Addressing Capabilities
- Quality-of-Service Capabilities
- Authentication and Privacy Capabilities

IPv6 Header Format : The most important changes introduced in IPv6 are evident in the header format:

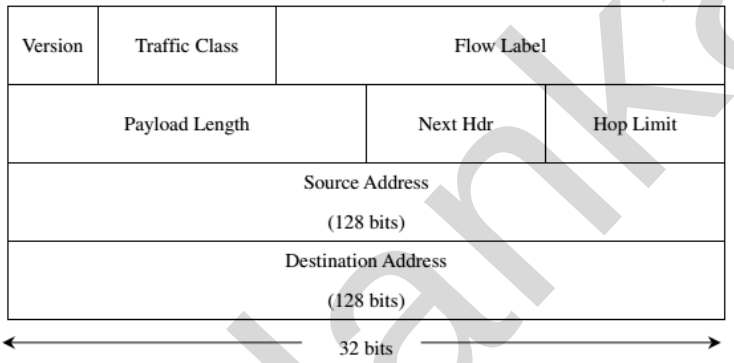
Expanded addressing capabilities. IPv6 increases the size of the IP address from 32 to 128 bits. This ensures that the world won't run out of IP addresses. In addition to unicast and multicast addresses, a new type of address, called an any cast address, has also been introduced.

A streamlined 40-byte header. As discussed below, a number of IPv4 fields have been dropped or made optional. The resulting 40-byte fixed-length header allows for faster processing of the IP datagram. A new encoding of options allows for more flexible options processing.

Flow labeling and priority. IPv6 has an elusive definition of a "flow". This new idea allows the labeling of packets belonging to particular flows. The IPv6 header also has an eight-bit Traffic Class field. This field, like the TOS field in IPv4, can be used to give priority to certain packets within a flow, or it can be used to give priority to datagrams from certain applications over datagrams from other applications.

Vidyalankar

Fields defined in the IPv6 header are: Version. This 4-bit field identifies the IP version number. For IPv6, it is 6. Traffic class. This 8-bit field is similar in spirit to the ToS field in IPv4. Flow label. This 20-bit field is used to identify a "flow" of datagrams. Payload length. This 16-bit value is treated as an unsigned integer giving the number of bytes in the IPv6 datagram following the 40-byte packet header. Next header. 8-bit selector. Identifies the type of header immediately following the IPv6 header. Uses the same values as the IPv4 Protocol field. Hop limit. 8-bit unsigned integer. Decremented by 1 by each node that forwards the packet. The packet is discarded if Hop Limit is decremented to zero. Source Address. 128-bit address of the originator of the packet Destination Address. 128-bit address of the intended recipient of the packet.



IPv6 header format

6. (c) **(i)** 1024 subnets and 62 hosts

(ii) 172.24.43.0

(iii) 10.33.207.254

(iv) 192.168.51.64

❑ ❑ ❑ ❑ ❑

Vidyalanka