Vidyalankar

S.Y. Diploma : Sem. IV [IF]

Data Communication Networking

Prelim Question Paper Solution

1. (a) (i) Advantages:

- Easy to implement
- It is very cost effective because only a single segment required
- It is very flexible
- Moderate reliability.
- Can add new station or delete any station easily (scalable)

Disadvantages:

- Required suitable medium access control technique.
- Maximum cable length restriction imposed due to delay and signal unbalancing problem

1. (a) (ii) Yes, medium should be selected based on the topology. For example, for bus topology coaxial cable medium is suitable, and for ring/star topology twisted-pair or optical fiber can be used.

1. (a) (iii) Bit Rate: The speed of the data is expressed in bits per second (bits/s or bps). The data rate R is a function of the duration of the bit or bit time (T_B) Bit rate is typically seen in terms of the actual data rate.

Baud Rate: The term "baud" originates from the French engineer Emile Baudot, who invented the 5-bit teletype code. Baud rate refers to the number of signal or symbol changes that occur per second. A symbol is one of several voltage, frequency, or phase changes NRZ binary has two symbols, one for each bit 0 or 1, that represent voltage levels. In this case, the baud or symbol rate is the same as the bit rate. However, it's possible to have more than two symbols per transmission interval, whereby each symbol represents multiple bits. With more than two symbols, data is transmitted using modulation techniques.

1. (a) (iv) Types of cabling are:

- 10 BASE 5 - Maximum cable length is 500 meters using 4" diameter coaxial cable.
- 10 BASE 2 - Maximum cable length is 185 meters using 0.25" diameter CATV cable.
- 10 BASE T - Maximum cable length is 100 meters using twisted-pair cable (CAT-3 UTP).
- 10 BASE FL - Maximum cable length is 2 Km using multimode fiber optic cable (125/62.5 micrometer).

1. (a) (v) 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) (vi) Difference between Guided and 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. Amplitude.

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) 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) TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing) are two methods of multiplexing multiple signals into a single carrier. Multiplexing is the process of combining multiple signals into one, in such a manner that each individual signal can be retrieved at the destination. Since multiple signals are occupying the channel, they need to share the resource in some manner. The primary difference between FDM and TDM is how they divide the channel. FDM divides the channel into two or more frequency ranges that do not overlap, while TDM divides and allocates certain time periods to each channel in an alternating manner. Due to this fact, we can say that for TDM, each signal uses all of the bandwidth some of the time, while for FDM, each signal uses a small portion of the bandwidth all of the time.

TDM provides greater flexibility and efficiency, by dynamically allocating more time periods to the signals that need more of the bandwidth, while reducing the time periods to those signals that do not need it. FDM lacks this type of flexibility, as it cannot dynamically change the width of the allocated frequency.

The advantage of FDM over TDM is in latency. Latency is the time it takes for the data to reach its destination. As TDM allocates time periods, only one channel can transmit at a given time, and some data would often be delayed, though it's often only in milliseconds. Since channels in FDM can transmit at any time, their latencies would be much lower compared to TDM. FDM is often used in applications where latency is of utmost priority, such as those that require real-time information.

FDM and TDM are often used in tandem, to create even more channels in a given frequency range. The common practice is to divide the channel with

FDM, so that you have a dedicated channel with a smaller frequency range. Each of the FDM channels is then occupied by multiple channels that are multiplexed using TDM. This is what telecoms do to allow a huge number of users to use a certain frequency band.

1. (b) (ii) 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.

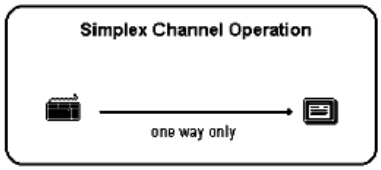
The result of the connection setup with circuit switching is the reservation of bandwidth all the way from the sender to the receiver. All packets follow this path. Among other properties, having all packets follow the same path means that they cannot arrive out of order. With packet switching there 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.

Items	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
Stored-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

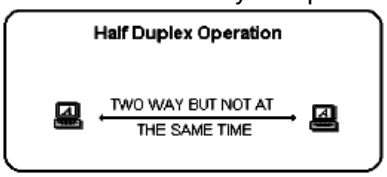
1. (b) (iii) Data in a simplex channel is always one way. Simplex channels are not often used because it is not possible to send back error or control signals to the transmit end.

It's like a one way street. An example of simplex is Television, or Radio. The simplex channel also corresponds directly to Shannon's model of communication discussed earlier.



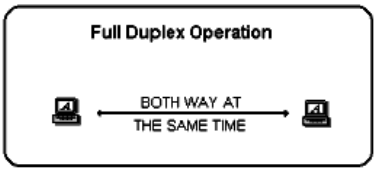
Half Duplex: A half-duplex channel can send and receive, but not at the same time. It's like a one-lane bridge where two way traffic must give way in order to cross. Only one end transmits at a time, the other end receives. In addition, it is possible to perform error detection and request the sender to retransmit information that arrived corrupted. In some aspects, you can think of Internet surfing as being half-duplex, as a user issues a request for a web document, then that document is downloaded and displayed before the user issues another request.

Another example of half-duplex is talk-back radio, and CB Radio (Citizens Band). You might have seen movies where truckies (drivers of very big trucks) communicate to each other, and when they want the other person to speak they say "over". This is because only one person can talk at a time.



Full Duplex : Data can travel in both directions simultaneously. There is no need to switch from transmit to receive mode like in half duplex. Its like a two lane bridge on a two-lane highway. Have you ever watched these television talk shows where the host has a number of people on the show, and they all try to talk at once. Well, that's full duplex!

Of course, in the world of data communications, full duplex allows both way communications simultaneously. An example can be a consumer which uses a cable connection to not only receive TV channels, but also the same cable to support their phone and Internet surfing. All these activities can occur simultaneously.



2. (a) Data communication is the transmission of electronic data over some media. The media may be cables, microwaves.

Elements of Data Communication

Four basic elements are needed for any communication system.

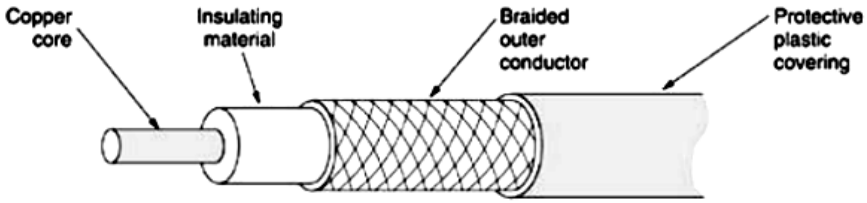
- **Sender** : The computer or device that is used for sending data is called sender, source or transmitter. In modern digital communication system, the source is usually a computer.

- **Medium**: The means through which data is sent from one location to another is called transmission medium. If the receiver and transmitter are within a building, a wire connects them. If they are located at different locations, they may be connected by telephone lines, fiber optics or microwaves.
- **Receiver**: The device or computer that receives the data is called receiver. The receiver can be a computer, printer or a fax machine.
- **Protocols**: There are rules under which data transmission takes place between sender and receiver. The data communication s/w are used to transfer data from one computer to another. The s/w follows same communication protocols can communicate and exchange data.

2. (b) 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.



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 bandwidth 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.

2. (c)

- 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.

2. (d) 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 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.

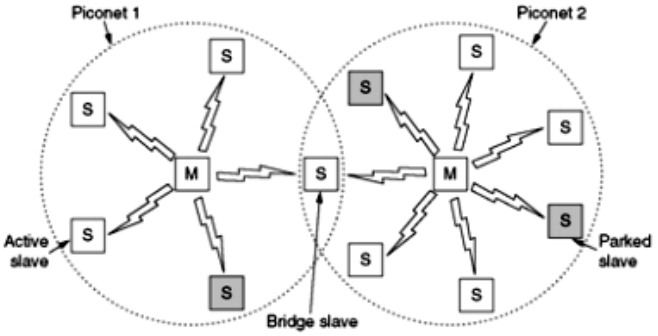
2. (e) **Bluetooth**

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 determines 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. (f) Serial Transmission

In serial transmission all the bits are transmitted 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.

Advantages:
- It is cheap and effective.
- 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:
  - 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.
  - Byte synchronization can be achieved in the data link layer.

3. (a) 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

i) Weather Forecasting Radio and TV Broadcast
ii) Military Satellites
iii) Navigation Satellites

3. (b) **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 system independent 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.

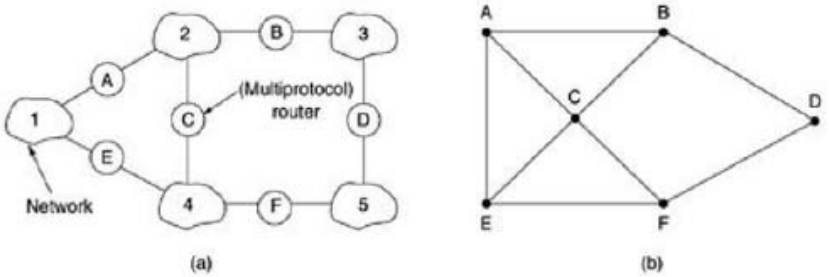
3. (c) Routing through an internetwork is similar to routing within a single subnet, but with some added complications. Consider, for example, the internetwork of Fig. (a) in which five networks are connected by six (possibly multiprotocol) routers. Making a graph model of this situation is complicated 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). 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 intranet work 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.



(a) An internetwork. (b) A graph of the internetwork

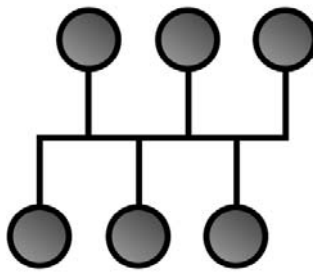
3. (d) • Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Summer is another name for error detection Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by re-computing the tag and comparing it with the one provided.

There exists a vast variety of different hash function designs. However, some are of particularly widespread use because of either their simplicity or their suitability for detecting certain kinds of errors (e.g., the cyclic redundancy check's performance in detecting burst errors).

- Error correction is the detection of errors and reconstruction of the original, error-free data.

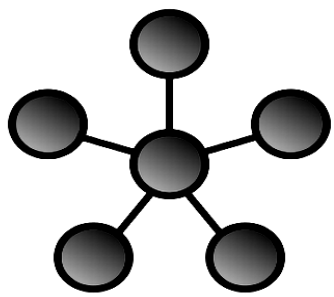
Error correction may generally be realized in two different ways: Automatic repeat request (ARQ) (sometimes also referred to as backward error correction): This is an error control technique whereby an error detection scheme is combined with requests for retransmission of erroneous data. Every block of data received is checked using the error detection code used, and if the check fails, retransmission of the data is requested – this may be done repeatedly, until the data can be verified.
Forward error correction (FEC): The sender encodes the data using an error-correcting code (ECC) prior to transmission. The additional information (redundancy) added by the code is used by the receiver to recover the original data. In general, the reconstructed data is what is deemed the "most likely" original data.

3. (e) **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.

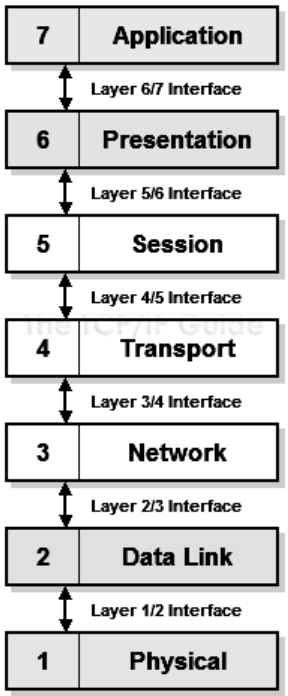
STAR Topology: In local area networks with a star topology, each network host is connected to a central hub with a point-to-point connection. In Star topology every node (computer workstation or any other peripheral) is connected to central node called hub or switch. The switch is the server and the 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 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. (f) 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



OSI Reference Model Interfaces for Vertical Communication

4. (a) Compare FTP and TFTP

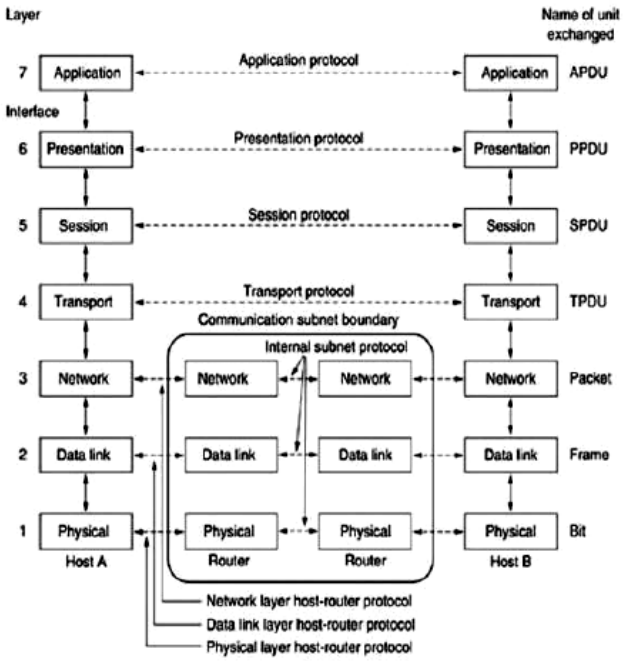
- FTP is a complete, session-oriented, general purpose file transfer protocol. TFTP is used as a bare-bones special purpose file transfer protocol.
- FTP can be used interactively. TFTP allows only unidirectional transfer of files.
- FTP depends on TCP, is connection oriented, and provides reliable control. TFTP depends on UDP, requires less overhead, and provides virtually no control.
- FTP provides user authentication. TFTP does not.
- FTP uses well-known TCP port numbers: 20 for data and 21 for connection dialog. TFTP uses UDP port number 69 for its file transfer activity.
- The Windows NT FTP server service does not support TFTP because TFTP does not support authentication.
- Windows 95 and TCP/IP-32 for Windows for Workgroups do not include a TFTP client program.

4. (b) 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.



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.

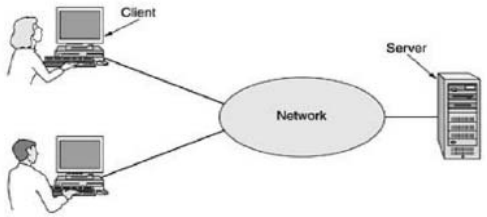
The Transport Layer: The basic function of the transport layer is to accept data from above, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. Furthermore, all this must be done efficiently and in a way that isolates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

4. (c) **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.)



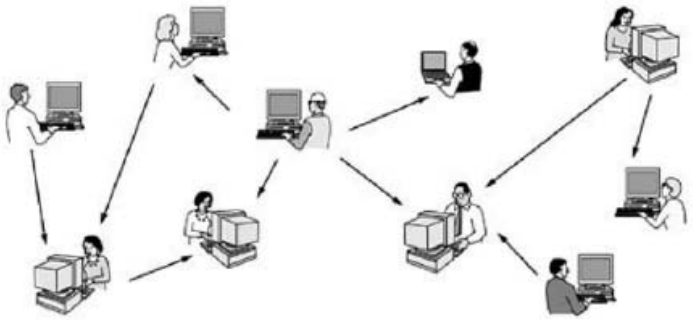
A network with two clients and one server

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.

4. (d) **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 Fig. 14. 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.



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

4. (e) 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.

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.

4. (f) **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.

5. (a) The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain namewww.example.com translates to the addresses 93.184.216.119 (IPv4) and 2606:2800:220:6d:26bf:1447:1097:aa7 (IPv6). Unlike a phone book, the DNS can be quickly updated, allowing a service's location on the network to change without affecting the end users, who continue to use the same host name. Users take advantage of this when they use meaningful Uniform Resource Locators (URLs), and e-mail addresses without having to know how the computer actually locates the services.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over subdomains to other

name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

The Domain Name System also specifies the technical functionality of this database service. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in DNS, as part of the Internet Protocol Suite.

The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol(IP) address spaces The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the Domain Name System. A DNS name server is a server that stores the DNS records for a domain name, such as address (A or AAAA) records, name server (NS) records, and mail exchanger (MX) records (see also list of DNS record types); a DNS name server responds with answers to queries against its database.

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

Issue	Datagram subnet	Virtual-circuit subnet
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 it.
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated.
Quality of service	Difficult	Easy if enough resources can be allocated in advance
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC.

5. (c) 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. (d) **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.

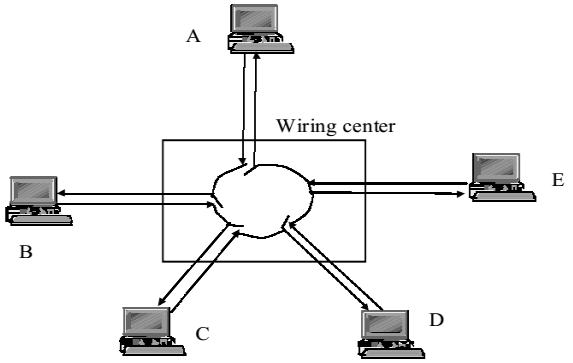
UDP : Provides a comparatively simpler but unreliable service by sending packets from one host to another. UDP does not take any extra measures to ensure that the data sent is received by the target host or not. The term 'unreliable connection' are used where loss of some information does not hamper 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.

5. (e) Fiber Distributed Data Interface (FDDI) is a standard fordata transmission in a local area network. It uses optical fiberas its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called CDDI (Copper Distributed Data Interface), standardized as TP-PMD (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).

Designers normally constructed FDDI rings in a network topology such as a "dual ring of trees". A small number of devices, typically infrastructure devices such as routers and concentrators rather than host computers, were "dual-attached" to both rings. Host computers then connect as single-attached devices to the routers or concentrators. The dual ring in its most degenerate form simply collapses into a single device. Typically, a computer-room contained the whole dual ring, although some implementations deployed FDDI as a metropolitan area network.

FDDI requires this network topology because the dual ring actually passes through each connected device and requires each such device to remain continuously operational. The standard actually allows for optical bypasses, but

network engineers consider these unreliable and error-prone. Devices such as workstations and minicomputers that might not come under the control of the network managers are not suitable for connection to the dual ring.



As an alternative to using a dual-attached connection, a workstation can obtain the same degree of resilience through a dual-homed connection made simultaneously to two separate devices in the same FDDI ring. One of the connections becomes active while the other one is automatically blocked. If the first connection fails, the backup link takes over with no perceptible delay.

5. (f) Multimode and single mode 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 take different paths and hits boundary at different angles. Each angle defines a new path or mode.

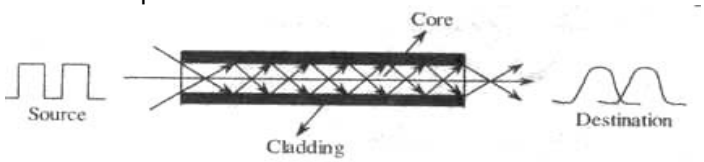


Fig. : Stepindex Multimode Fiber

- **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 beamtravels 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

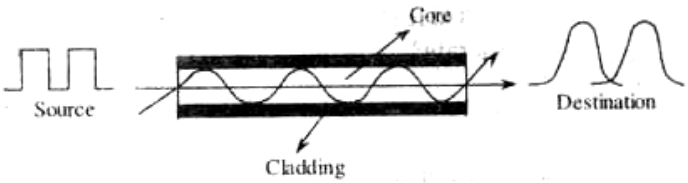


Fig. : Graded index multimode Fiber

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.

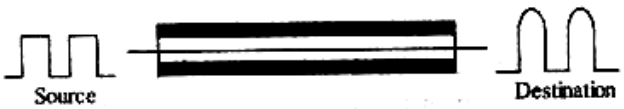
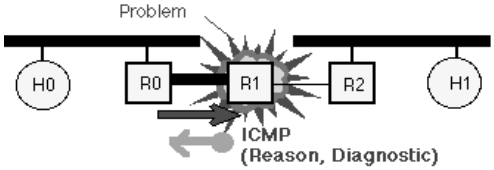


Fig. : Singlemode Fiber.

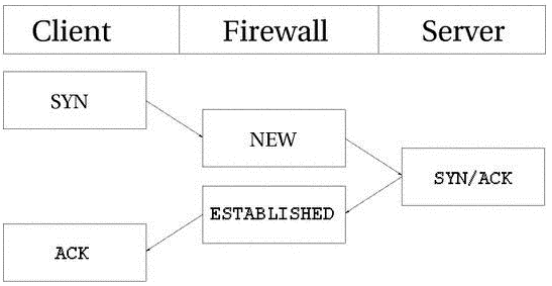
6. (a) **Internet Control Message Protocol (ICMP):** The Internet Control Message Protocol (ICMP) [RFC792] protocol is classic example of a client server application. The ICMP server executes on all IP end system computers and all IP intermediate systems (i.e routers). The protocol is used to report problems with delivery of IP datagrams within an IP network. It can be sued to show when a particular End System (ES) is not responding, when an IP network is not reachable, when a node is overloaded, when an error occurs in the IP header information, etc. The protocol is also frequently used by Internet managers to verify correct operations of End Systems (ES) and to check that routers are correctly routing packets to the specified destination address.



ICMP messages generated by router R1, in response to message sent by H0 to H1 and forwarded by R0. This message could, for instance be generated if the MTU of the link between R0 and R1 was smaller than size of the IP packet, and the packet had the Don't Fragment (DF) bit set in the IP packet header. The ICMP message is returned to H0, since this is the source address specified in the IP packet that suffered the problem. A modern version of Path MTU Discovery provides a mechanism to verify the Path MTU [RFC4821].

It is the responsibility of the network layer (IP) protocol to ensure that the ICMP message is sent to the correct destination. This is achieved by setting the destination address of the IP packet carrying the ICMP message. The source address is set to the address of the computer that generated the IP packet (carried in the IP source address field) and the IP protocol type is set to "ICMP" to indicate that the packet is to be handled by the remote end system's ICMP client interface.

6. (b) A TCP connection is always initiated with the 3-way handshake, which establishes and negotiates the actual connection over which data will be sent. The whole session is begun with a SYN packet, then a SYN/ACK packet and finally an ACK packet to acknowledge the whole session establishment. At this point the connection is established and able to start sending data. The big problem is, how does connection tracking hook up into this? Quite simply really.
As far as the user is concerned, connection tracking works basically the same for all connection types. Have a look at the picture below to see exactly what state the stream enters during the different stages of the connection. As you can see, the connection tracking code does not really follow the flow of the TCP connection, from the users viewpoint. Once it has seen one packet(the SYN), it considers the connection as NEW. Once it sees the return packet(SYN/ACK), it considers the connection as ESTABLISHED. If you think about this a second, you will understand why. With this particular implementation, you can allow NEW andESTABLISHED packets to leave your local network, only allow ESTABLISHED connections back, and that will work perfectly. Conversely, if the connection tracking machine were to consider the whole connection establishment as NEW, we would never really be able to stop outside connections to our local network, since we would have to allow NEW packets back in again. To make things more complicated, there is a number of other internal states that are used for TCP connections inside the kernel, but which are not available for us in User-land. Roughly, they follow the state standards specified within RFC 793 - Transmission Control Protocolat page 21-23. We will consider these in more detail further along in this section.



6. (c) DSL modems works over telephone lines, specifically the copper wire they contain. Because phone and voice data is transmitted at low frequencies while the Internet data uses higher frequencies, the same line can handle both tasks without one interfering with the other. However, DSL users will have to install a filter, or a device that separates the signals. This is as simple as plugging the device into the phone jack.

Cable modems operate on the same premise, but use the coaxial cables that carry television signals rather than phone lines. The cable uses a separate signal for each channel and treats Internet signals in the same way it does other channel information. Users may need to pay for a special installation if they do not already have cable service, or may be required to purchase a splitter to connect their modems to their existing cable connection.

Ultimately, there are three factors that come into play when choosing between DSL and cable modems: speed, reliability, and location. The differences in the ways cable and DSL modems transmit data mean that a cable modem is faster, but a DSL modem is more consistent.

Speed: Cable modems have outpaced DSL modems, providing substantially higher speeds. DSL is capable of providing maximum downstream speeds of 1.5 Mbps to 15 Mbps, with an upstream speed of 128 kbps to 1 Mbps. Cable Internet yields maximum downstream speeds of 25 Mbps to 100 Mbps and upstream speeds of 2 Mbps to 8 Mbps. However, cable modems rarely reach the maximum speeds they are capable of. In fact, one study of broadband Internet service across the US found that the average speed for all types combined was just 3.9 Mbps.

Consistency: DSL Internet transfers data directly between the ISP and the home over the phone line, so bandwidth is never shared with anyone else. This means that users will see overall consistent performance. Cable Internet, on the other hand, delivers a block of bandwidth to an entire neighborhood and then shares it among the homes. This means that during peak hours, when many homes in the neighborhood are online, Internet speeds may be drastically reduced, especially if others in the neighborhood use their connections heavily.

Location: Whether consumers can obtain cable or DSL service will depend on their location, and providers may not service all areas. Beyond that, though, DSL modems are distance-sensitive; that is, their performance is limited by how close they are to the DSL provider's central office, or hub. DSL signals degrade the farther they travel along wiring, giving DSL modems a range of about 18,000 feet, or 3.4 miles. However, there is still a drop-off in performance after about 9,000 to 10,000 feet, or 1.7 to 1.9 miles. Cable modems do not have this problem because the materials that transmit the data do not degrade signals over long distances.

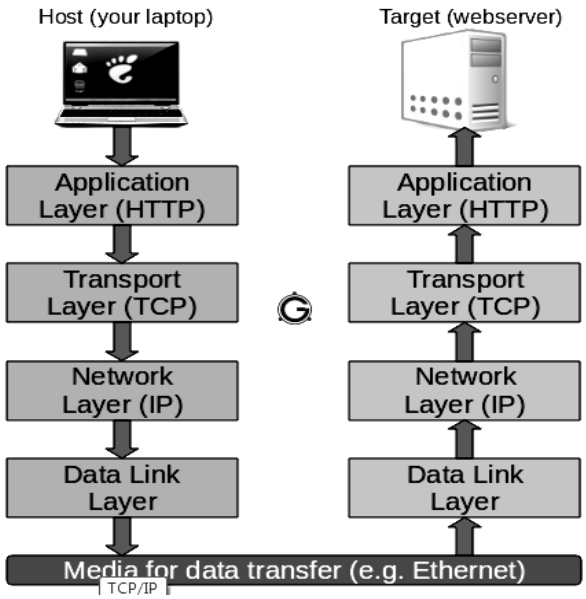
6. (d) **(i)** 1024 subnets and 62 hosts

(ii) 172.24.43.0

6. (e) **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



- **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.

6. (f) There are practical limits to the size of our Ethernet network. A primary concern is the length of the shared cable. Electrical signals propagate along a cable very quickly, but they weaken as they travel, and electrical interference from neighboring devices (fluorescent lights, for example) can scramble the signal. A network cable must be short enough that devices at opposite ends can receive each other's signals clearly and with minimal delay. This places a distance limitation on the maximum separation between two devices on an Ethernet network.

Additionally, since in CSMA/CD only a single device can transmit at a given time, there are practical limits to the number of devices that can coexist in a single network.

Ethernet networks face congestion problems as they increased in size. If a large number of stations connected to the same segment and each generated a sizable amount of traffic, many stations may attempt to transmit whenever there was an opportunity. Under these circumstances, collisions would become more frequent and could begin to choke out successful transmissions, which could take inordinately large amounts of time to complete. One way to reduce congestion would be to split a single segment into multiple segments, thus creating multiple collision domains. This solution creates a different problem, as now these now separate segments are not able to share information with each other.

To alleviate these problems, Ethernet networks implemented bridges. Bridges connect two or more network segments, increasing the network diameter as a repeater does, but bridges also help regulate traffic. They can send and receive transmissions just like any other node, but they do not function the same as a normal node. The bridge does not originate any traffic of its own; like a repeater, it only echoes what it hears from other stations.

❑ ❑ ❑ ❑ ❑