1. *What is data communication? List and explain the characteristics of a data communication system. (June 2010 / Dec 2009 / 2010 /2011)*

*Solution:* Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

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

1. *Delivery*: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. *Accuracy*: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. *Timeliness*: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. *Jitter*: Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30ms. If some of the packets arrive with 30ms delay and others with 40ms delay, an uneven quality in the video is the result of transmission medium such as a wire cable.
5. *What are the five important components of data communications? (June 2011)*

*Solution:* A data communications system has five components



* 1. *Message*: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
	2. *Sender:* The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
	3. *Receiver:* The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
	4. *Transmission medium*: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
	5. *Protocol*: A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.
1. *Explain different transmission modes. (June 2011)*

*Solution:*Communication between two devices can be simplex, half-duplex, or full-duplex.



*Simplex*

* In simplex mode, the communication is unidirectional, as on a one-way street.
* Only one of the two devices on a link can transmit; the other can only receive.
* Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
* The simplex mode can use the entire capacity of the channel to send data in one direction.

*Half-Duplex*

* In half-duplex mode, each station can both transmit and receive, but not at the same time.
* When one device is sending, the other can only receive, and vice versa.
* The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait.
* In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
* Walkie-talkies and CB (citizens band) radios are both half-duplex systems.
* The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

*Full-Duplex*

* In full-duplex mode, both stations can transmit and receive simultaneously.
* The full-duplex mode is like a two-way street with traffic flowing in both directions at the same time.
* In full-duplex mode, signals going in one direction share the capacity of the link: with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate transmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.
* One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.
* The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.
1. *Explain Criteria of a computer network.*

*Solution:*The most important criteria of a network are performance, reliability, and security.

*Performance*

* Performance can be measured in many ways, including transit time and response time.
* Transit time is the amount of time required for a message to travel from one device to another. Response time is the elapsed time between an inquiry and a response.
* The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software.
* Performance is often evaluated by two networking metrics: throughput and delay. We often need more throughput and less delay.

*Reliability*

* Network reliability is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network's robustness in a catastrophe.

*Security*

* Network security issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.
1. *With neat diagram explain different type’s connections.*

*Solution:*A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.



*Point-to-Point:*

* A point-to-point connection provides a dedicated link between two devices.
* The entire capacity of the link is reserved for transmission between those two devices.
* Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible
* When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

*Multipoint:*

* A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.
* In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.
1. *With neat diagram explain mesh topology with applications of each. (June 2009)*

*OR*

*Name and explain four topologies of computer networks. (June 2011 / Dec 2012)*

*Solution:* The term *physical topology* refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. There are four basic topologies possible: mesh, star, bus, and ring.



*Mesh Topology:*

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To connect *n* devices $\frac{n\left(n+1\right)}{2}$ duplex links are required.

Example: Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.



Advantages:

* The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems.
* A mesh topology is robust.
* There is the advantage of privacy or security.
* Point-to-point links make fault identification and fault isolation easy.

Disadvantages:

* Because every device must be connected to every other device, installation and reconnection are difficult.
* The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
* The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

*Star Topology:*

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Advantages:

* Less expensive compared to mesh topology.
* In a star, each device needs only one link and one I/O port to connect it to any number of others.
* This factor also makes it easy to install and reconfigure.
* Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
* A star topology is robust.
* Easy fault identification and fault isolation.

Disadvantages:

* A star topology is less expensive than a mesh topology.
* Single point of failure, if hub goes down, then full system is dead.

*Bus Topology:*

A bus topology, is multipoint. One long cable acts as a backbone to link all the devices in a network. Nodes are connected to the bus cable by drop lines and taps. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



Advantages:

* Ease of installation.
* Bus uses less cabling than mesh or star topologies.

Disadvantages:

* Difficult reconnection and fault isolation.
* A bus is usually designed to be optimally efficient at installation.
* Signal reflection at the taps can cause degradation in quality.
* A fault or break in the bus cable stops all transmission.

*Ring Topology:*

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.



Advantages:

* A ring is relatively easy to install and reconfigure.
* To add or delete a device requires changing only two connections.
* Fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages:

* Unidirectional traffic can be a disadvantage.
* In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break.
1. *Give the comparison between LAN, MAN and WAN with an example. (June 2010)*

*OR*

Explain categories of network and differentiate between them. (June 2013)

*Solution:*

|  |  |  |
| --- | --- | --- |
| LAN | MAN | WAN |
| Local Area Network | Metropolitan Area Network | Wide Area network |
| LAN is privately owned and links the devices in a single office, building, or campus | MAN is privately owned and networks normally covers the area inside a town or a city. | Two types of WAN:switched WANpoint-to-point WAN |
| LAN size is limited to a few kilometers  | MAN is a network with a size between a LAN and a WAN.  | WAN size may comprise a country, a continent, or even the whole world. |
| LANs are designed to resource sharing between PC’s or workstations like hardware (e.g., printer) and software. | It is designed for customers who need a high-speed connectivity. | WAN provides long-distance transmission of data, image, audio, and video information. |
| Early LANs had data rates in the 4 to 16 Mbps range. Today, speeds are normally 100 or 1000 Mbps. | Speeds of MAN ranges in terms of Mbps. | Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). |
| Example of a LAN, found in many business environments, links a workgroup of task-related computers. | Example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network in a city. | Example of a switched WAN is the asynchronous transfer mode (ATM) network and point-to-point WAN is dial-up line that connects a home computer to the Internet |

1. *For n devices in n/w, what is the number of cable links required for a mesh, ring and star topologies?**(June 2011)*

*Solution:*

 Mesh Topology: Number of duplex links for *n* devices = $\frac{n\left(n-1\right)}{2}$

Ring Topology: Number of duplex links for *n* devices = *n*

Star Topology: Number of duplex links for *n* devices = *n*

1. *What is Internet? Explain hierarchical organization of internet. (Dec 2008)*

*Solution:*The Internet is a structured, organized interconnection of heterogeneous networks. The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time.

* We can sent electronic mail (e-mail) to a business associate, paid a utility bill, read a newspaper from a distant city, or looked up a local movie schedule-all by using the Internet.
* The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations.
* It is difficult to give an accurate representation of the Internet because it is continually changing-new networks are being added, existing networks are adding addresses, and networks of defunct companies are being removed. Today most end users who want Internet connection use the services of Internet service providers (ISPs).
* There are international service providers, national service providers, regional service providers, and local service providers.
* The Internet today is run by private companies, not the government.



*International Internet Service Providers*

* At the top of the hierarchy are the international service providers that connect nations together.

*National Internet Service Providers*

* The national Internet service providers are backbone networks created and maintained by specialized companies. There are many national ISPs operating in North America; some of the most well-known are SprintLink, PSINet, UUNet Technology, AGIS, and internet Mel.
* Some national ISP networks are also connected to one another by private switching stations called *peering points.* These normally operate at a high data rate (up to 600 Mbps).

*Regional Internet Service Providers*

* Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs. They are at the third level of the hierarchy with a smaller data rate.

*Local Internet Service Providers*

* Local Internet service providers provide direct service to the end users. The local ISPs can be connected to regional ISPs or directly to national ISPs.
* Most end users are connected to the local ISPs. A local ISP can be a company that just provides Internet services, a corporation with a network that supplies services to its own employees, or a nonprofit organization, such as a college or a university, that runs its own network.
* Each of these local ISPs can be connected to a regional or national service provider.
1. *What is Protocol? What are the key elements of a protocol? (Dec 2009 / 2010 / 2012)*

*Solution:* In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated.

The key elements of a protocol are syntax, semantics, and timing.

1. *Syntax*: The term syntaxrefers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
2. *Semantics:* The word semanticsrefers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
3. *Timing:* The term timingrefers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.
4. *What are standards? Name any four standard organizations. (June 2009)*

*Solution:*Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.

Data communication standards fall into two categories: *de facto* (meaning "by fact" or "by convention") and *de jure* (meaning "by law" or "by regulation").

* De facto: Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
* De jure: Those standards that have been legislated by an officially recognized body are de jure standards.

*Standard Organizations:*

* International Organization for Standardization (ISO)
* International Telecommunication Union-Telecommunication Standards Sector (ITU-T)
* American National Standards Institute (ANSI)
* Institute of Electrical and Electronics Engineers (IEEE)
* Electronic Industries Association (EIA)
1. *Explain following terms peer-to-peer process, interfaces between layers and encapsulation.*

*Solution:*

*Peer-to-peer processes:*

* An entity could be a software (process) or hardware circuit/chip. The entities in the same layer on different machines are called as peer entities. The interaction between peer entities is called peer-to-peer processes.



*Interfaces between layers:*

* The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers.
* Each interface defines the information and services a layer must provide for the layer above it. Well-defined interfaces and layer functions provide modularity to a network.
* As long as a layer provides the expected services to the layer above it, the specific implementation of its functions can be modified or replaced without requiring changes to the surrounding layers.

*Encapsulation:*

* Above figure reveals another aspect of data communications in the OSI model: encapsulation.
* A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on.
* In other words, the data portion of a packet at level *N* - 1 carries the whole packet (data and header and maybe trailer) from level *N.* The concept is called *encapsulation;* level *N* - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level *N* - 1, the whole packet coming from level *N* is treated as one integral unit.
1. *With a neat figure explain OSI reference model. (Dec 2008 / 2009 / 2010 / June 2010 /2013)*

*Solution:* The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.



*Physical Layer:* The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.

The physical layer is also concerned with the following responsibilities,

1. Physical characteristics of interfaces and medium
2. Representation of bits
3. Data rate
4. Synchronization of bits
5. Line configuration
6. Physical topology
7. Transmission mode



*Data Link Layer:* The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer).

Other responsibilities of the data link layer include the following:

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



*Network Layer:* The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

Other responsibilities of the network layer include the following:

1. Logical addressing.
2. Routing



*Transport Layer:* The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. The transport layer ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Other responsibilities of the transport layer include the following:

1. Service-point addressing.
2. Segmentation and Reassembly
3. Connection Control
4. Flow control
5. Error Control



*Session Layer:* The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

Other responsibilities of the session layer include the following:

1. Dialog Control
2. Synchronization



*Presentation Layer:* The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

Other responsibilities of the Presentation layer include the following:

1. Translation
2. Encryption
3. Compression



*Application Layer:* The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

1. Network virtual terminal
2. File transfer access and management
3. Mail Services
4. Directory Services



1. *Describe with a neat diagram. The functionalities of each layer in the TCP/IP model.*

*(June 2010)*

*Solution:* The TCP/IP protocol suite was developed prior to the OSI model.



TCP/IPis a hierarchical protocol made up of interactive modules, each upper-level protocol is supported by one or more lower-level protocols. The layers of the TCP/IPprotocol suite contain relatively independent protocols that can be mixed and matched depending on the needs of the system. Whereas the OSI model specifies which functions belong to each of its layers.

* 1. *Physical and Data Link Layer:*

At the physical and data link layers, TCP/IPdoes not define any specific protocol. It supports all the standard and proprietary protocols such as TDMA, FDMA, CSMA/CD, CSMA/CA etc. A network in a TCP/IPinternetwork can be a local-area network or a wide-area network.

* 1. *Network Layer:*

At the network layer TCP/IPsupports the Internetworking Protocol (IP), in turn, uses four supporting protocols: ARP, RARP, ICMP, and IGMP.

Interworking Protocol (IP):

* IP is the transmission mechanism used by the TCP/IP protocols.
* It is an unreliable and connectionless protocol, *a best effort* delivery service. The term *best effort* means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.
* IP transports data in packets called *datagrams,* each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated.
* IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

ARP (Address Resolution Protocol):

* ARP is used to associate a logical address with a physical address.
* The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver. Because the sender does not know the physical address of the receiver, the query is broadcast over the network.
* Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
* The response packet contains the recipient's IP and physical addresses. The packet is unicast directly to the inquirer by using the physical address received in the query packet.

RARP (Reverse Address Resolution Protocol):

* RARP finds the logical address for a machine that knows only its physical address.
* A RARP request is created and broadcast on the local network.
* Another machine on the local network that knows all the IP addresses will respond with a RARP reply.
* The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.

ICMP (Internet Control Message Protocol):

* ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. ICMP sends query and error reporting messages.

IGMP (Internet Group Message Protocol):

* IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients.
	1. *Transport Layer:*

Transport layer of TCP/IP *is* represented by two protocols: TCP and UDP. IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another. UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.

UDP (User Datagram Protocol):

* UDP is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.
* UDP is unreliable protocol which does not guarantee ordered delivery of packets.

TCP (Transmission Control Protocol):

* TCP is a reliable stream transport protocol (means connection-oriented).
* A connection must be established between both ends of a transmission before either can transmit data.
* At the sending end of each transmission, TCP divides a stream of data into smaller units called *segments.* Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received.
* Segments are carried across the internet inside of IP datagrams.
* At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

SCTP (Stream Control Transmission Protocol):

* SCTP provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP.
	1. *Application Layer:*

The application layerin TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer such as SMTP, FTP, DNS, HTTP, SNMP etc.

1. *Differentiate between: i) ARP and RARP ii) ICMP and IGMP iii) UDP and TCP. (Dec 2009)*

*Solution:*

|  |  |
| --- | --- |
| ARP | RARP |
| Address resolution Protocol | Reverse Address Resolution Protocol |
| Maps logical address to physical address | Maps physical address to logical address |
| ARP request (query) is created with its logical, physical address and destination logical address and broadcast on the local network. | RARP request is created and broadcast on the local network. |
| Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet. | The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program. |
| Request is broadcast and response is unicast | Request is broadcast and response is unicast |
|  |  |
| ICMP | IGMP |
| Internet Control Message Protocol | Internet Group Message Protocol |
| ICMP is a mechanism used by hosts and gateways to send notification of datagram problems back to the sender. | IGMP is used to facilitate the simultaneous transmission of a message to a group of recipients. |
| ICMP sends query and error reporting messages.  | Single copy is sent from sender, when router found more than one copy is required, it creates required number of packets and sends to recipients. |
|  |  |
| TCP | UDP |
| Transmission Control Protocol | User Datagram Protocol |
| Connection Oriented Service | Connectionless service |
| Reliable data communications | Unreliable data communications |
| Ordered delivery of data | Ordered delivery of data is not guaranteed |
| Duplication of data is not possible | Possibility of duplication |
| Connection overhead (Slow) | Fast |
| Acknowledgements are used to make sure that data is delivered efficiently | No acknowledgements in UDP |

1. *Explain the different level of addressing used in an internet with a suitable example for each level of addressing in TCP/IP? (Dec 2012)*

*Solution:*Four levels of addresses are used in an internet employing the *TCP/IP* protocols: physical (link) addresses, logical (IP) addresses, port addresses, and specific addresses.



*Physical Addresses:*

* The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
* It is included in the frame used by the data link layer. It is the lowest-level address.
* The size and format of these addresses vary depending on the network.
* For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC) looks like: 07:01:02:01:2C:4B.
* LocalTalk (Apple), however, has a 1-byte dynamic address that changes each time the station comes up.

*Example:*



* In Figure node with physical address 10 sends a frame to a node with physical address 87.
* The two nodes are connected by a link (bus topology LAN). At the data link layer, this frame contains physical (link) addresses in the header. These are the only addresses needed. The rest of the header contains other information needed at this level. The trailer usually contains extra bits needed for error detection.
* As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver. The data link layer at the sender receives data from an upper layer. It encapsulates the data in a frame, adding a header and a trailer. The header, among other pieces of information, carries the receiver and the sender physical (link) addresses. Note that in most data link protocols, the destination address, 87 in this case, comes before the source address (10 in this case). In a bus topology, the frame is propagated in both directions (left and right).
* The frame propagated to the right is sent to every station on the network. Each station with a physical addresses other than 87 drops the frame because the destination address in the frame does not match its own physical address.
* The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is de-capsulated and delivered to the upper layer.

*Logical Addresses:*

* Logical addresses are necessary for universal communications that are independent of underlying physical networks.
* Physical addresses are not adequate in an internetwork environment where different networks can have different address formats.
* A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network.
* The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet.
* No two publicly addressed and visible hosts on the Internet can have the same IP address.

Example:



* Figure shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. Each router has three pairs of addresses, one for each connection.
* The computer with logical address A and physical address 10 needs to send a packet to the computer with logical address P and physical address 95.
* The sender encapsulates its data in a packet at the network layer and adds two logical addresses (A and P). The network layer, however, needs to find the physical address of the next hop before the packet can be delivered.
* The ARP protocol finds the physical address of router 1 that corresponds to the logical address of 20. Now the network layer passes this address to the data link layer, which in tum, encapsulates the packet with physical destination address 20 and physical source address 10.
* The frame is received by every device on LAN 1, but is discarded by all except router 1, which finds that the destination physical address in the frame matches with its own physical address.
* The router de-capsulate the packet from the frame to read the logical destination address P. Since the logical destination address does not match the router's logical address, the router knows that the packet needs to be forwarded.
* The router consults its routing table and ARP to find the physical destination address of the next hop (router 2), creates a new frame, encapsulates the packet, and sends it to router 2. The source physical address changes from 10 to 99. The destination physical address changes from 20 (router 1 physical address) to 33 (router 2 physical address). The logical source and destination addresses must remain the same; otherwise the packet will be lost.
* At router 2 we have a similar scenario.

*Port Addresses:*

* The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet.
* Today, computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process.
* For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP).
* For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCPIIP architecture, the label assigned to a process is called a port address.
* A port address in TCP/IP is 16 bits in length. Example 753.

*Example:*



* Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses *a, b,* and *c*. The receiving computer is running two processes at this time with port addresses *j* and *k*.
* Process *a* in the sending computer needs to communicate with process *j* in the receiving computer.
* To show that data from process *a* need to be delivered to process *j*, and not *k*, the transport layer encapsulates data from the application layer in a packet and adds two port addresses (*a* and *j*), source and destination. The packet from the transport layer is then encapsulated in another packet at the network layer with logical source and destination addresses (A, P).
* Finally, this packet is encapsulated in a frame with the physical source and destination addresses of the next hop. We have not shown the physical addresses because they change from hop to hop inside the cloud designated as the Internet.
* Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Specific Addresses:

* Some applications have user-friendly addresses that are designed for that specific address.
* Examples include the e-mail address (for example, forouzan@fhda.edu) the recipient of an e-mail and the Universal Resource Locator (URL) (for example, [www.mhhe.com](http://www.mhhe.com/)) is used to find a document on the World Wide Web.