6/3/2014

COMPUTER NETWORKS

CSE-2012 B.Sc. (Honours) Question Solution

S M TALHA JUBAED
DEPT. OF COMPUTER SCIENCE & ENGINEERING (CSE)
UNIVERSITY OF RAJSHAHI (RU)
HOTLINE# +088-01911-088 706

Question-01: What is computer network? What are the applications of computer networks? Classify network by transmission technology and by size and then briefly describe each type. 10 Marks CSE-2012 (Engg) CSE-2012

__Computer Network:__

A computer network or data network is a telecommunications network that allows computers to exchange data. In other words, computer networks means a collection of "autonomous" computers interconnected by a single technology.
In computer networks, networked computing devices pass data to each other along data connections. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

Network computer devices that originate, route and terminate the data are called network nodes.[1] Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices are said to be networked together when one device is able to exchange information with the other device, whether or not they have a direct connection to each other.

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications. Computer networks differ in the physical media used to transmit their signals, the communications protocols to organize network traffic, the network's size, topology and organizational intent.

The Internet is a network that connects users from all parts of the world. Educational institutions, government agencies, health care facilities, banking and other financial institutions, and residential applications use computer networking to send and receive data and share resources.

__Applications of Computer Network:__
There are many applications of computer networks. Following are some important applications of computer networks:

1. Business Applications
2. Home Applications
3. Mobile Users
4. Social Issues
5.
6. __Communication and Access to Information__
   (i) The primary purpose of computer networking is to facilitate communication. A network allows a user to instantly connect with another user, or network, and send and receive data. It allows remote users to connect with one other via videoconferencing, virtual meetings and digital emails.

   (ii) Computer networks provide access to online libraries, journals, electronic newspapers, chat rooms, social networking websites, email clients and the World Wide Web. Users can benefit from making online bookings for theaters, restaurants, hotels, trains and airplanes. They can shop and carry out banking transactions from the comfort of their homes.

   (iii) Computer networks allow users to access interactive entertainment channels, such as video on demand, interactive films, interactive and live television, multiperson real-time games and virtual-reality models.

7. __Resource Sharing__
   (i) Computer networks allow users to share files and resources. They are popularly used in organizations to cut costs and streamline resource sharing. A single printer attached to a small local area network (LAN) can effectively service the printing requests of all computer users on the same network. Users can similarly share other network hardware devices, such as modems, fax machines, hard drives and removable storage drives.
   (ii) Networks allow users to share software applications, programs and files. They can share documents (such as invoices, spreadsheets and memos), word processing software, videos,

photographs, audio files, project tracking software and other similar programs. Users can also access, retrieve and save data on the hard drive of the main network server.

8. **Centralized Support and Administration**

   Computer networking centralizes support, administration and network support tasks. Technical personnel manage all the nodes of the network, provide assistance, and troubleshoot network hardware and software errors. Network administrators ensure data integrity and devise systems to maintain the reliability of information through the network. They are responsible for providing high-end antivirus, anti-spyware and firewall software to the network users. Unlike a stand-alone system, a networked computer is fully managed and administered by a centralized server, which accepts all user requests and services them as required.

Classification of Network by Transmission Technology:

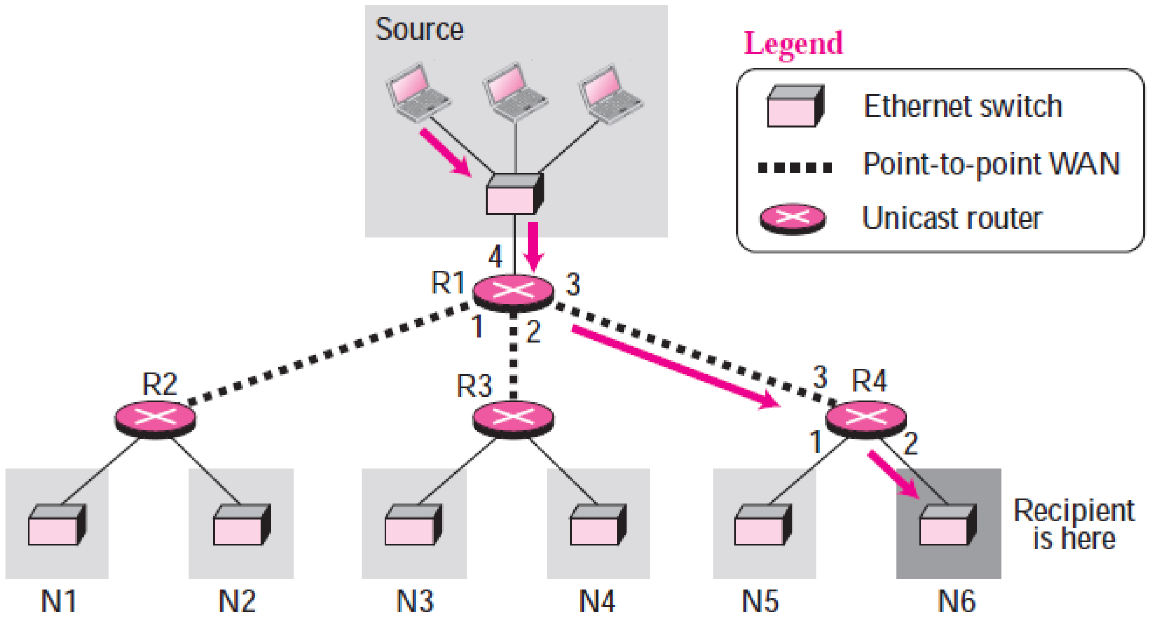
By transmission technology, network can be classified in following categories:

1. Unicasting network
2. Multicasting Network
3. Broadcasting Network
4. Point to Point Network

Unicasting Network:

In unicasting, there is one source and one destination network. The relationship between the source and the destination network is one to one. Each router in the path of the datagram tries to forward the packet to one and only one of its interfaces. Figure 12.1 shows a small internet in which a unicast packet needs to be delivered from a source computer to a destination computer attached to N6. Router R1 is responsible to forward the packet only through interface 3; router R4 is responsible to forward the packet only through interface 2. When the packet arrives to N6, the delivery to the destination host is the responsibility of the network; it is either broadcast to all hosts or the smart Ethernet switch delivers it only to the destination host. In unicasting, the routing table that defines the only output port for each datagram, is based on the optimum path .In unicasting, the router forwards the received datagram through only one of its interfaces.

Figure 12.1 *Unicasting*

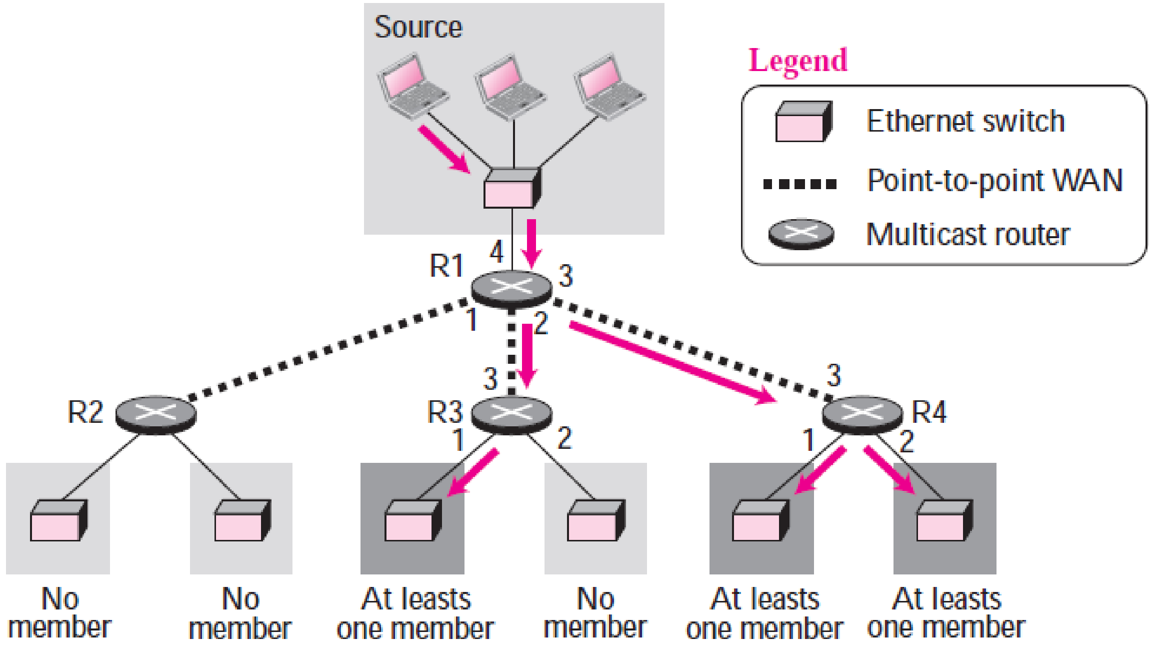


Multicasting

In multicasting, there is one source and a group of destinations. The relationship is one to many. In this type of communication, the source address is a unicast address, but the destination address is a group address, a group of one or more destination networks in which there is at least one member of the group that is interested in receiving the multicast datagram. The group address defines the members of the group. Figure 12.2 shows the same small internet in Figure 12.1, but the routers have been changed to multicast routers (or previous routers have been configured to do both types of job).

In multicasting, a multicast router may have to send out copies of the same datagram through more than one interface. In Figure 12.2, router R1 needs to send out the datagram through interfaces 2 and 3. Similarly, router R4 needs to send out the datagram through both its interfaces. Router R3, however, knows that there is no member belonging to this group in the area reached by interface 2; it only sends out the datagram through interface 1. In multicasting, the router may forward the received datagram through several of its interfaces.

Figure 12.2 *Multicasting*



Broadcasting

In broadcast communication, the relationship between the source and the destination is one to all. There is only one source, but all of the other hosts are the destinations. The Internet does not explicitly support broadcasting because of the huge amount of traffic it would create and because of the bandwidth it would need. Imagine the traffic generated in the Internet if one person wanted to send a message to everyone else connected to the Internet.

In multicasting network, a single communications channel shared by all machines (addresses) on the network. Broadcast can be both a logical or a physical concept (e.g. Media Access Control (MAC) sublayer).

Point-to-point network:

In point to point networks, Connections made via links between pairs of nodes. 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.

Point-to-point networks consist of many connections between individual pairs of machines. To go from the source to the destination, a packet on this type of network may have to first visit one or more intermediate machines. Often multiple routes, of different lengths, are possible, so finding good ones is important in point-to-point networks. As a general rule (although there are many exceptions), smaller, geographically localized networks tend to use broadcasting, whereas larger networks usually are point-to-point. Point-to-point transmission with one sender and one receiver is sometimes called unicasting.

Classification by Size:

Network can be classified by size as follows:

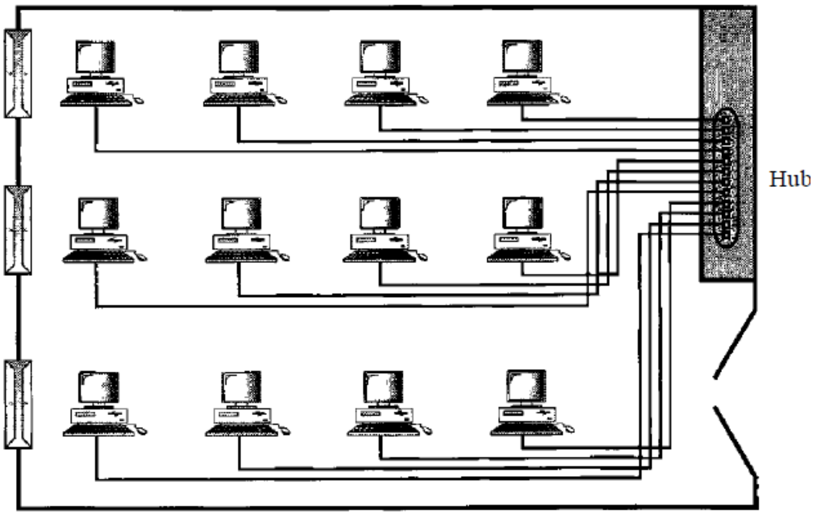
1. Local Area Networks (LAN)
2. Metropolitan Area Networks (MAN)
3. Wide Area Networks (WAN)

Local Area Networks:

A local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet. The LAN market has seen several technologies such as Ethernet, token ring, token bus, FDDI, and ATM LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology.
A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system. In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps.. Wireless LANs are the newest evolution in LAN technology. Wireless communication is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. **Wireless LANs** can be found on college campuses, in office buildings, and in many public areas. In this section, we concentrate on two wireless technologies for LANs: IEEE 802.11 wireless LANs, sometimes called wireless Ethernet, and Bluetooth, a technology for small wireless LANs.

Figure 1.10 *An isolated IAN connecting 12 computers to a hub in a closet*



Metropolitan Area Networks

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good 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 that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet.

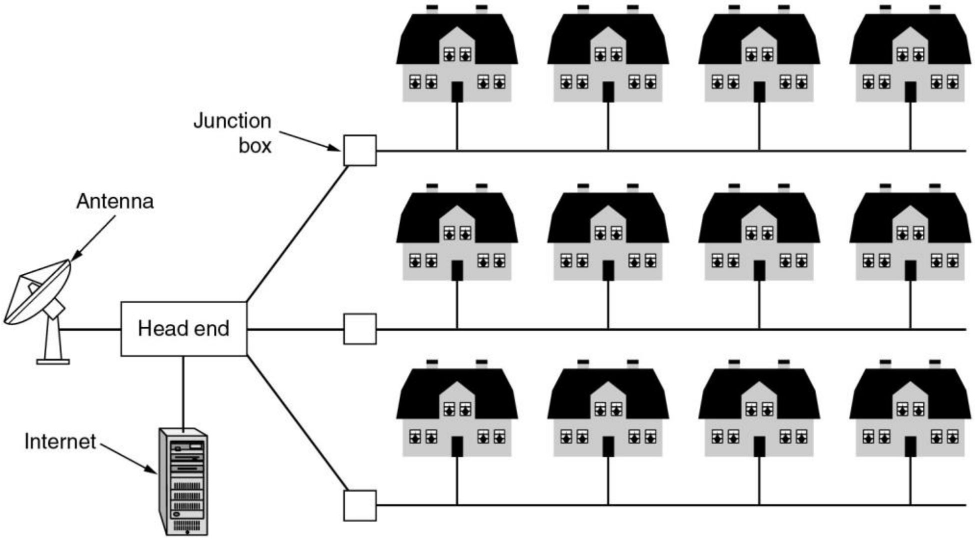


Figure 1-8. A metropolitan area network based on cable TV

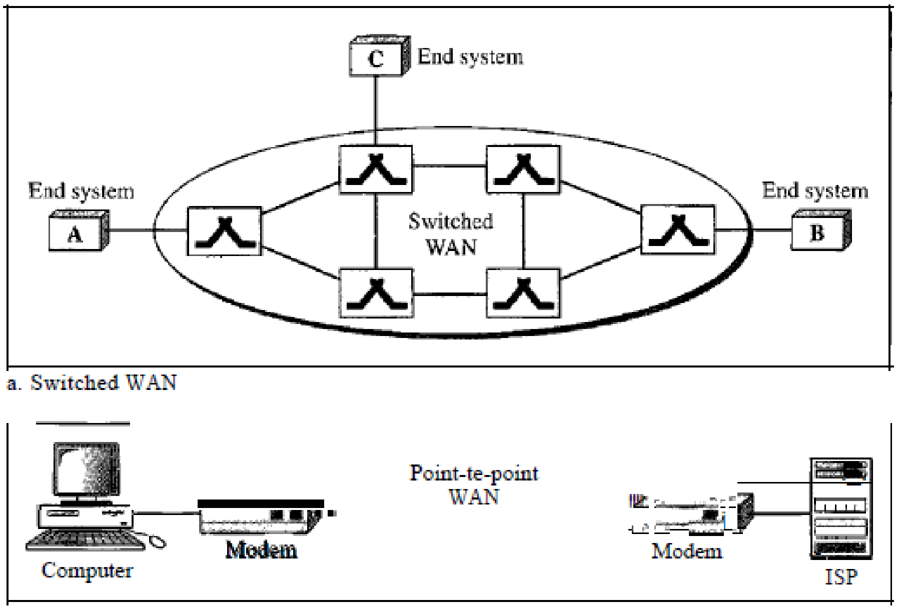
Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. In Chapters 17 and 18 we discuss wide-area networks in greater detail. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN (Figure 1.11). The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

An early example of a switched WAN is X.25, a network designed to provide connectivity between end users. X.25 is being gradually replaced by a high-speed, more efficient network called Frame

Relay. A good example of a switched WAN is the asynchronous transfer mode (ATM) network, which is a network with fixed-size data unit packets called cells.. Another example of WANs is the wireless WAN that is becoming more and more popular.

Figure 1.11 *WANs: a switched WAN and a point-to-point WAN*



a. Switched WAN

b. Point-to-point WAN

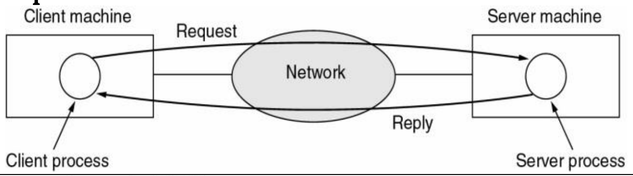
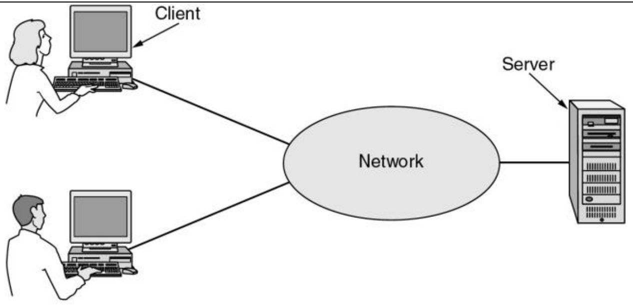
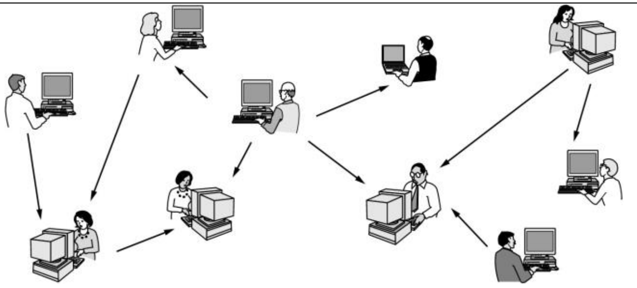
নির্দেশনাঃ এই প্রশ্নটি বিস্তারিত আকারে লেখার কারণ, এই তথ্যসমূহ জানা থাকলে, এই ধরণের অনেক প্রশ্নের উত্তর করা সম্ভব । পরীক্ষায় মার্কস এর উপর নির্ভর করে লিখতে হবে । ল্যান, ম্যান কিংবা ওয়ান সম্পর্কে বেশ ভাল এবং স্পষ্ট ধারনা থাকা প্রয়োজন ।

Question: differentiate between Client-Server model and Peer to Peer model of Computer Network. 4 Marks CSE-2012

Difference between Client-Server model and Peer to Peer model

Following are some important difference between client server model and peer to peer model of computer network:

Client Server model	Peer to Peer Model
In this model, the data are stored on powerful computers called **servers.** Often these are centrally housed and maintained by a system administrator. In contrast, the employees or users have simpler machines, called **clients,** on their desks, with which they access remote data. The client and server machines are connected by a network. This whole arrangement shown in **Fig 1.1** is called the **client-server model.**	Another type of person-to-person communication often goes by the name of peer-to-peer communication. In this form, individuals who form a loose group can communicate with others in the group, as shown in Fig. 1-3. Every person can, in principle, communicate with one or more other people; there is no fixed division into clients and servers.
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. Under most conditions, one server can handle a large number of clients.	peer-to-peer systems eliminates the central database by having each user maintain his own database locally, as well as providing a list of other nearby people who are members of the system.
In client-server model, two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the	In peer to peer model, A new user can go to any existing member to see what he has and get a list of other members to inspect for more music and

client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.	more names. This lookup process can be repeated indefinitely to build up a large local database of what is out there. It is an activity that would get tedious for people but is one at which computers excel.
The client-server model involves requests and replies.  Client machine Request Server machine Network Reply Client process Server process	**In a peer-to-peer system there are no fixed clients and servers.**
 **Figure 1.1 A network with two clients and one server.**	 Figure 1-3: Peer to Peer model of computer network.

Question: What is Topology? Briefly describe different types of topology with its advantages and disadvantages. 6 Marks CSE-2012 * CSE-2012 (Engg)**

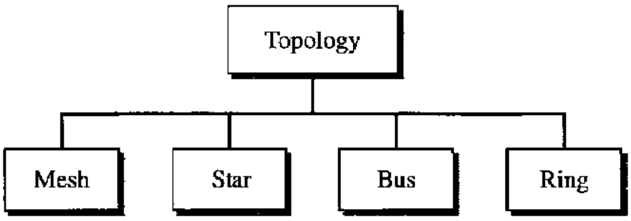
Topology:

The term @topology@ or 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. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. The physical topology of a network refers to the configuration of cables, computers, and other peripherals. There are four basic topologies possible: mesh, star, bus, and ring (see Figure 1.4).

Categories of Topology:

Following are the basic topologies used in computer networks:

Figure **1.4** *Categories oftopology*



Mesh Topology:

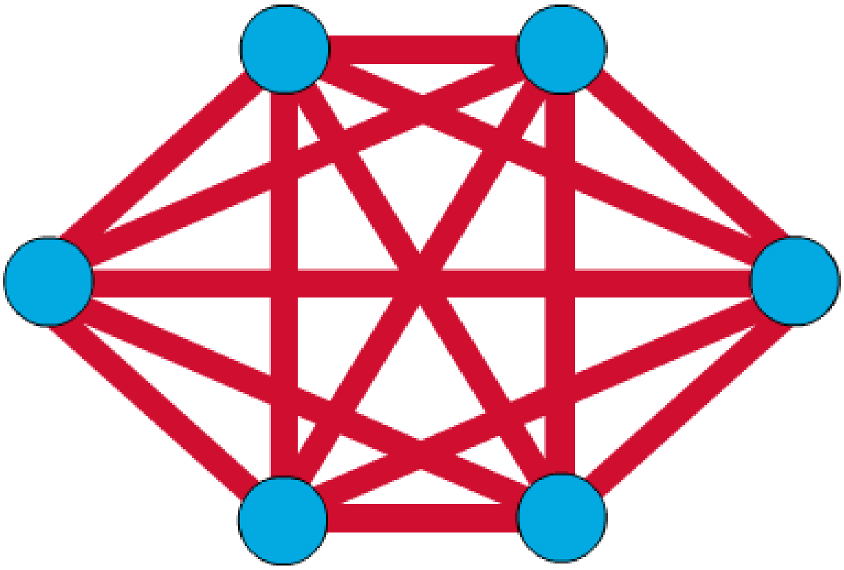
In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need

$$n(n-1)/2$$

duplex-mode links.

To accommodate that many links, every device on the network must have n – 1 input/output (VO) ports (see Figure 1.5) to be connected to the other n - 1 stations.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.



<u>**Advantages of Mesh Topology:**</u>

A mesh offers several advantages over other network topologies.

- **First,** the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

- **Second, a** mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

- **Finally,** point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.
- The arrangement of the network nodes is such that it is possible to transmit data from one node to many other nodes at the same time.
- The failure of a single node does not cause the entire network to fail as there are alternate paths for data transmission.
- It can handle heavy traffic, as there are dedicated paths between any two network nodes.
- Point-to-point contact between every pair of nodes, makes it easy to identify faults.

<u>**Disadvantages of Mesh Topology:**</u>

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

- First, because every device must be connected to every other device, installation and reconnection are difficult. Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive. For these reasons a mesh topology is usually implemented in a limited fashion, for

example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

- The arrangement wherein every network node is connected to every other node of the network, many connections serve no major purpose. This leads to redundancy of many network connections.
- A lot of cabling is required. Thus, the costs incurred in setup and maintenance are high.
- Owing to its complexity, the administration of a mesh network is difficult.

Star Topology:

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. Unlike a mesh topology, a star topology does not allow direct traffic between devices. 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 (see Figure 1.6) .

The star topology is used in local-area networks (LANs). High-speed LANs often use a star topology with a central hub.

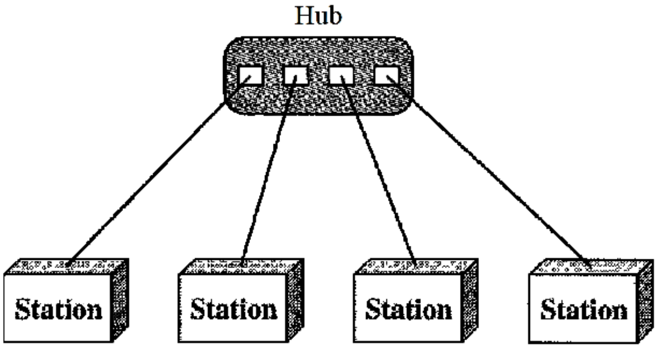


Figure 1.6 A star topology connecting four stations

Advantages of Star topology:

1. A star topology is less expensive than a 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.
2. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.
3. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.
4. Due to its centralized nature, the topology offers simplicity of operation.
5. It also achieves isolation of each device in the network.
6. Adding or removing network nodes is easy, and can be done without affecting the entire network.
7. Due to the centralized nature, it is easy to detect faults in the network devices.
8. As the analysis of traffic is easy, the topology poses lesser security risk.
9. Data packets do not have to pass through many nodes, like in the case of a ring network. Thus, with the use of a high-capacity central hub, traffic load can be handled at fairly decent speeds.
10. Easy to install and wire.
11. No disruptions to the network when connecting or removing devices.
12. Easy to detect faults and to remove parts.
13. The tree topology is useful in cases where a star or bus cannot be implemented individually.
14. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
15. The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.

16. Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
17. Fault identification is easy.
18. The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

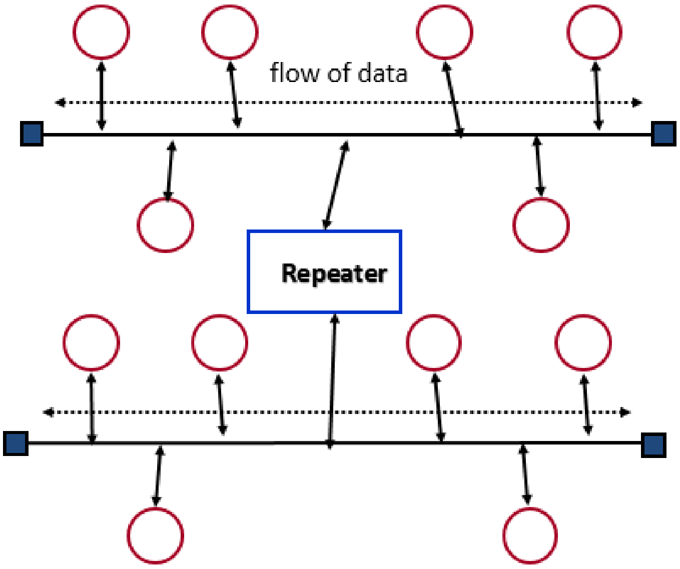
<u>**Disadvantages of Star topology:**</u>

1. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).
3. Network operation depends on the functioning of the central hub. Hence, central hub failure leads to failure of the entire network.
4. Also, the number of nodes that can be added, depends on the capacity of the central hub.
5. The setup cost is quite high.
6. Requires more cable length than a linear topology.
7. If the hub, switch, or concentrator fails, nodes attached are disabled.
8. More expensive than linear bus topologies because of the cost of the hubs, etc.
9. As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.
10. Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to that in other topologies.
11. Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

<u>**Bus topology:**</u>

A bus topology is multipoint. One long cable acts as a backbone to link all the devices in a network (see Figure 1.7). Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. 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.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology.



<u>***Bidirectional flow***</u>
Default is baseband cabling

Advantages of a Linear Bus Topology

1. Easy to connect a computer or peripheral to a linear bus.
2. Requires less cable length than a star topology.
3. It is easy to set up, handle, and implement.
4. It is best-suited for small networks.
5. It costs very less.
6. Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

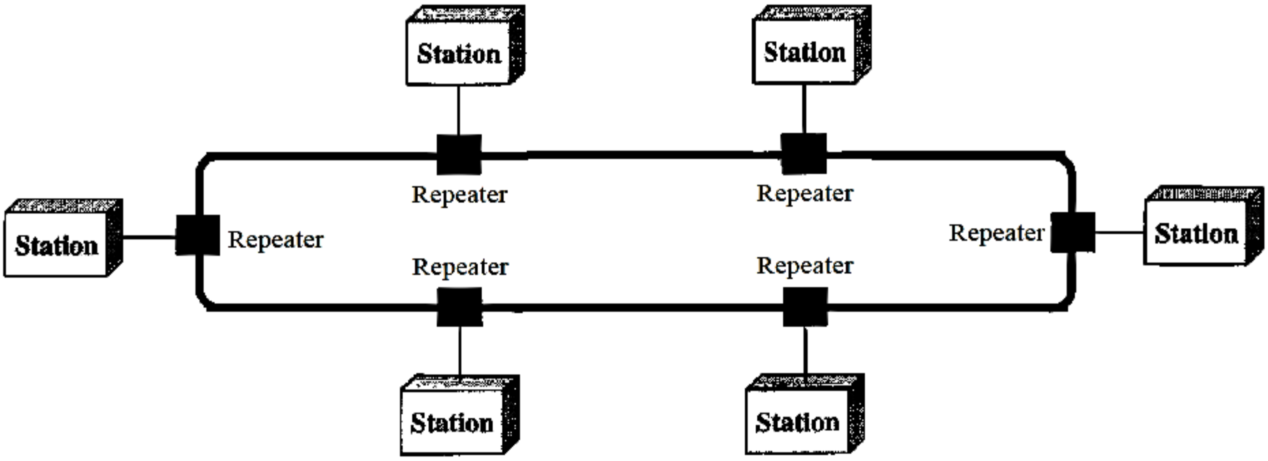
Disadvantages of a Linear Bus Topology

1. Entire network shuts down if there is a break in the main cable.
2. Terminators are required at both ends of the backbone cable.
3. Difficult to identify the problem if the entire network shuts down.
4. Not meant to be used as a stand-alone solution in a large building.
5. The cable length is limited. This limits the number of network nodes that can be connected. This network topology can perform well only for a limited number of nodes. When the number of devices connected to the bus increases, the efficiency decreases.
6. It is suitable for networks with low traffic. High traffic increases load on the bus, and the network efficiency drops.
7. It is heavily dependent on the central bus. A fault in the bus leads to network failure.
8. It is not easy to isolate faults in the network nodes.
9. Each device on the network "sees" all the data being transmitted, thus posing a security risk.
7. Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.
8. In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

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 (see Figure 1.8). A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbours (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, 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. However, 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. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

Figure 1.8 *A ring topology connecting six stations*



<u>**Advantages of Ring Topology:**</u>

1. The data being transmitted between two nodes passes through all the intermediate nodes. A central server is not required for the management of this topology.
2. The traffic is unidirectional and the data transmission is high-speed.
3. In comparison to a bus, a ring is better at handling load.
4. The adding or removing of network nodes is easy, as the process requires changing only two connections.
5. The configuration makes it easy to identify faults in network nodes.
6. In this topology, each node has the opportunity to transmit data. Thus, it is a very organized network topology.
7. It is less costly than a star topology.

<u>**Disadvantages of Ring Topology:**</u>

1. The failure of a single node in the network can cause the entire network to fail.
2. The movement or changes made to network nodes affect the entire network's performance.
3. Data sent from one node to another has to pass through all the intermediate nodes. This makes the transmission slower in comparison to that in a star topology. The transmission speed drops with an increase in the number of nodes.
4. There is heavy dependency on the wire connecting the network nodes in the ring.

<u>**Tree or Expanded Star**</u>

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star configured workstations connected to a linear bus backbone cable (See fig. 3). Tree topologies allow for the expansion of an existing network, and enable schools to configure a network to meet their needs.

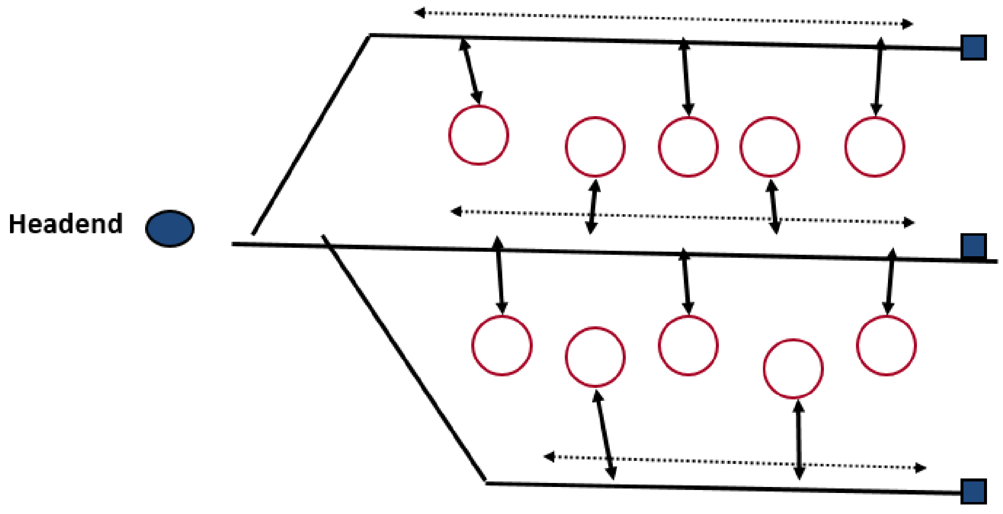


Figure: Tree topology

Advantages of a Tree Topology

1. Point-to-point wiring for individual segments.
2. Supported by several hardware and software venders.
3. The tree topology is useful in cases where a star or bus cannot be implemented individually. It is most-suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).
4. The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.
5. Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.
6. Fault identification is easy.
7. The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

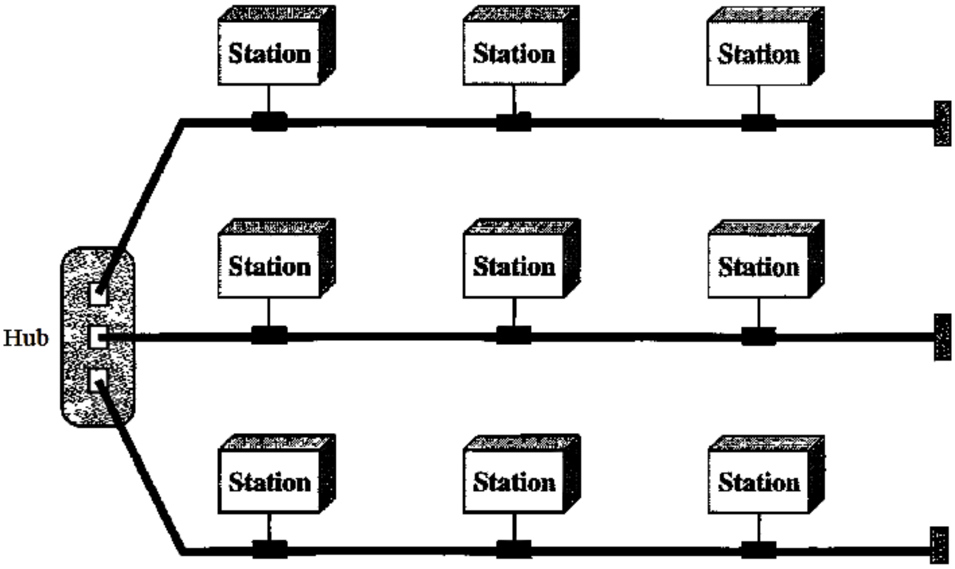
Disadvantages of a Tree Topology

1. Overall length of each segment is limited by the type of cabling used.
2. If the backbone line breaks, the entire segment goes down.
3. More difficult to configure and wire than other topologies.
4. As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.
5. Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to that in other topologies.
6. Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

Hybrid Topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure 1.9.

Figure 1.9 A *hybrid topology: a star backbone with three bus networks*



Question: Differentiate between Wired and Wireless Networks. 3 Marks CSE-2012

Difference between Wired and Wireless Network:

Following are some important difference between wired and wireless networks:

Wired Network	Wireless Network
Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables.	A wireless network is a network which uses high-frequency radio waves rather than wires to communicate between nodes. Wireless allows for devices to be shared without networking cable which increases mobility but decreases range. There are two main types of wireless networking; peer to peer or ad-hoc and infrastructure.
Wired network uses network cables.	Wireless network uses radio frequencies.
A wired network allows for a faster and more secure connection and can only be used for distances shorter than 2,000 feet.	A wireless network is a lot less secure and transmission speeds can suffer from outside interference.
Wired networking is less mobile than wired networking. Mobile computers need to be tied to an Ethernet cable and cannot roam freely within the wireless network range.	Wireless networking is a lot more mobile than wired networking. Mobile computers do not need to be tied to an Ethernet cable and can roam freely within the wireless network range.
Wired networks are invisible to other wired networks. The presence of one wired network has no effect on the performance of another wired network.	Wireless networks are often visible to other wireless networks. One wireless network can affect the performance of other wireless networks.
Wired network performance is not affected by the properties of the atmosphere.	Wireless network performance can be affected by the properties of the atmosphere.
Wired network performance is not affected by the properties of the earth's terrain.	Wireless network performance is strongly affected by the properties of the earth's terrain.
Connectivity is possible only to or from those physical locations where the network cabling extends.	Connectivity is possible beyond the bounds of physical network cabling.
The cost for wired networking has become rather inexpensive. Ethernet cables, hubs and switches are very inexpensive. Some connection sharing	Wireless gear costs somewhat more than the equivalent wired Ethernet products. At full retail prices, wireless adapters and access points may

software packages, like ICS, are free; some cost a nominal fee. Broadband routers cost more, but these are optional components of a wired network, and their higher cost is offset by the benefit of easier installation and built-in security features.	cost three or four times as much as Ethernet cable adapters and hubs/switches, respectively. 802.11b products have dropped in price considerably with the release of 802.11g.
Wired LANs offer superior performance. A traditional Ethernet connection offers only 10 Mbps bandwidth, but 100 Mbps Fast Ethernet technology costs a little more and is readily available. Fast Ethernet should be sufficient for file sharing, gaming, and high-speed Internet access for many years into the future. Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously. Use Ethernet switches instead of hubs to avoid this problem; a switch costs little more than a hub.	Wireless networks using 802.11b support a maximum bandwidth of 11 Mbps, roughly the same as that of old, traditional Ethernet. 802.11a and 802.11g LANs support 54 Mbps, that is approximately one-half the bandwidth of Fast Ethernet. As more wireless devices utilize the 802.11 LAN more heavily, performance degrades even further.
Wired networking performance is not distance sensitive, meaning that maximum performance will not degrade on computers farther away from the access point or other communication endpoint.	Wireless networking performance is distance sensitive, meaning that maximum performance will degrade on computers farther away from the access point or other communication endpoint.
In theory, wired LANs are more secure than wireless LANs.	In theory, wireless LANs are less secure than wired LANs, because wireless communication signals travel through the air and can easily be intercepted.

Question: What is OSI Reference Model? Why it is called layered architecture? 3 Marks CSE-2012

OSI Reference Model:

The OSI reference 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 (see Figure 2.3).

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s. **An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.** The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. The OSI model was intended to be the basis for the creation of the protocols in the OSI stack.

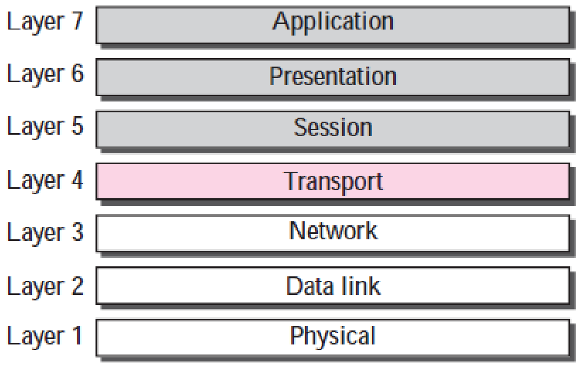


Figure 2.3 *The OSI model*

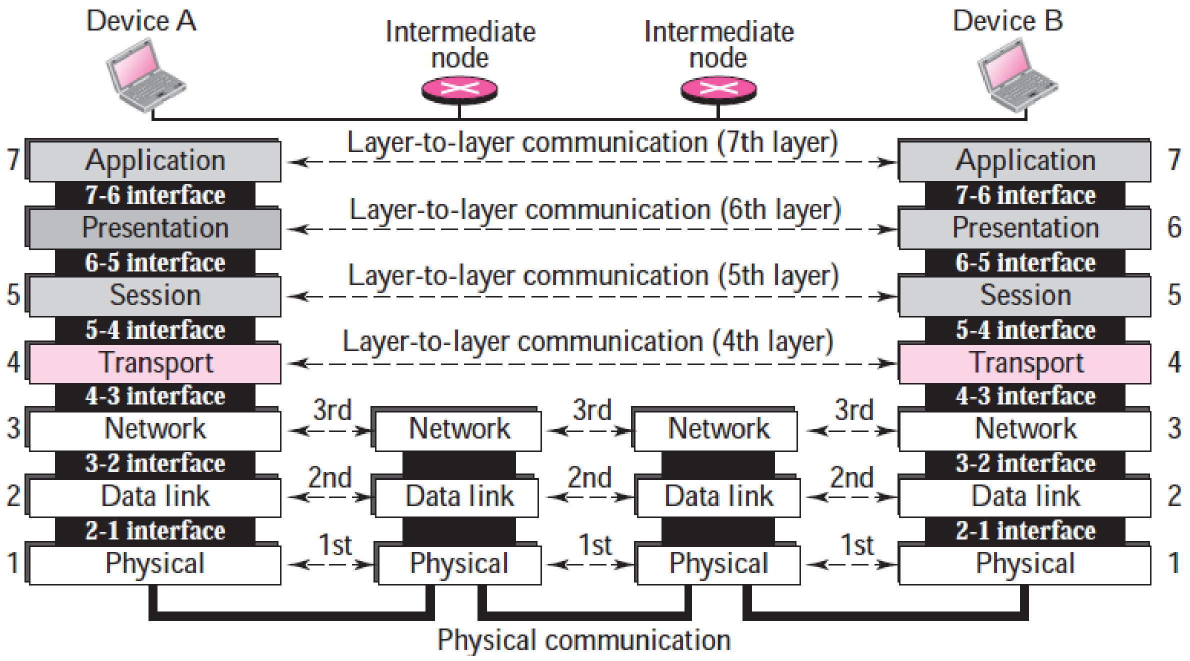
<u>Why it is called layered architecture:</u>

The OSI model is composed of seven ordered layers: physical (layer 1), data link (layer 2), network (layer 3), transport (layer 4), session (layer 5), presentation (layer 6), and application (layer 7). Figure 2.4 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

In developing the model, the designers distilled the process of transmitting data to its most fundamental elements. They identified which networking functions had related uses and collected those functions into discrete groups that became the layers. Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible. Within a single machine, each layer calls upon the services of the layer just below it.

Since OSI model is composed of seven order layers and the process of transmitting data is distilled to discrete groups that became the layers, that's why OSI model is called Layered Architecture.

Figure 2.4 *OSI layers*



Question: Briefly describe the functionalities of each OSI layer and also show the diagram of how data is encapsulated by each layer at the sender and dencapsulated at the receiver end. 7 Marks CSE-2012

Functionalities of OSI layers:

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 media. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. The physical layer is responsible for moving individual bits from one (node) to the next. The physical layer is also concerned with the following:

❑ **Physical characteristics of interfaces and media.** The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.

❑ **Representation of bits.** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals—electrical or optical. The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

❑ **Data rate.** The transmission rate—the number of bits sent each second—is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

❑ **Synchronization of bits.** The sender and receiver must not only use the same bit rate but must also be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

❑ **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected together through a dedicated link. In a multipoint configuration, a link is shared between several devices.

❑ **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected using a mesh topology (every device connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), or a bus topology (every device on a common link).

❑ **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In the simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

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:

❑ **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

❑ **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the connecting device that connects the network to the next one.

❑ **Flow control.** If the rate at which the data is absorbed by the receiver is less than the rate produced at the sender, the data link layer imposes a flow control mechanism to prevent overwhelming the receiver.

❑ **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

❑ **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

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 (link), the network layer ensures that each packet gets from its point of origin to its final destination.
If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Other responsibilities of the network layer include the following:

❑ **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

❑ **Routing.** When independent networks or links are connected together to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

Transport Layer:

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on the host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, 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:

❑ **Service-point addressing.** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

❑ **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

❑ **Connection control.** The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

❑ **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

❑ **Error control.** Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Session Layer:

The services provided by the first four layers (physical, data link, network and transport) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction between communicating systems. Specific responsibilities of the session layer include the following:

❑ **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.

❑ **Synchronization.** The session layer allows a process to add checkpoints (synchronization points) into a stream of data. For example, if a system is sending a file of 2,000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Specific responsibilities of the presentation layer include the following:

❑ **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information should be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

❑ **Encryption.** To carry sensitive information a system must be able to assure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

❑ **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

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. Specific services provided by the application layer include the following:

❑ **Network virtual terminal. A** network virtual terminal is a software version of a physical terminal and allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal, which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows you to log on.

❑ **File transfer, access, and management (FTAM).** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

❑ **E-mail services.** This application provides the basis for e-mail forwarding and storage.

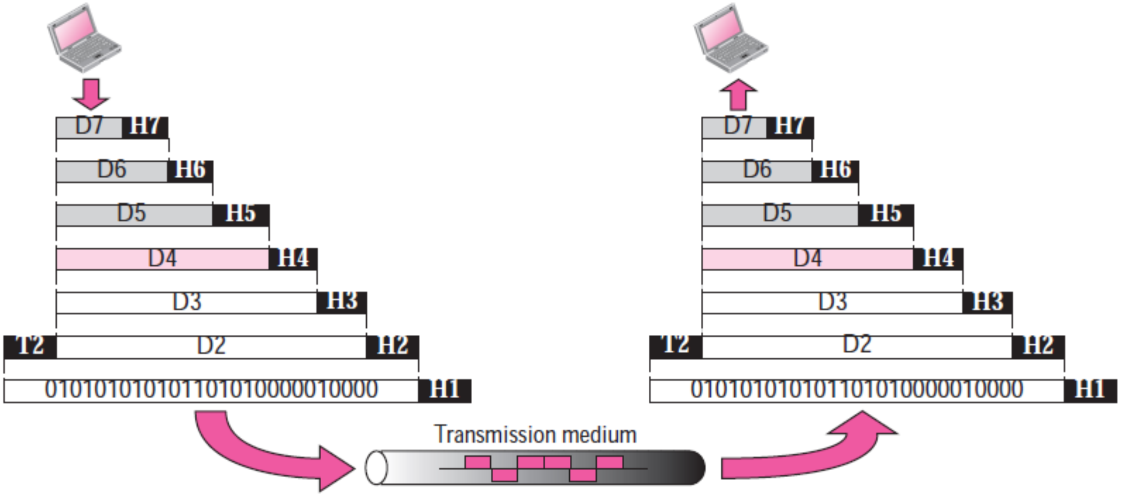
❑ **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

Encapsulation and dencapsulation:

Figure 2.5 reveals encapsulation and dencapsulation aspects of data communications in the OSI model. A packet at level 7 is encapsulated in the 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 part of a packet at level N is carrying the whole packet (data and overhead) from level N + 1. The concept is called encapsulation because level N is not aware what part of the encapsulated packet is data and what part is the header or trailer. For level N, the whole packet coming from level N + 1 is treated as one integral unit.

Similarly,
At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on. A packet at level 7 is unwrapped then passes the rest to layer 6, a packet at level 6 is unwrapped then passes the rest to layer 5 and so on. A packet at level 1 is dencapsulated in the packet at level 2. The whole packet at level 2 is dencapsulated in a packet at level 3, and so on. In other words, the data part of a packet at level N is carrying the partial packet (only data) from level N - 1. The concept is called dencapsulation.

Figure 2.5 *An exchange using the OSI model*



Question: What is TCP/IP? Differentiate between OSI model and TCP/IP model. 4 Marks CSE-2012

TCP/IP:

TCP/IP stands for Transmission Control Protocol/Internet Protocol. Transmission Control Protocol/Internet Protocol, TCP/IP is the suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

The TCP/IP protocol suite was developed prior to the OSI model. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model with the layers named similarly to the ones in the OSI model.

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

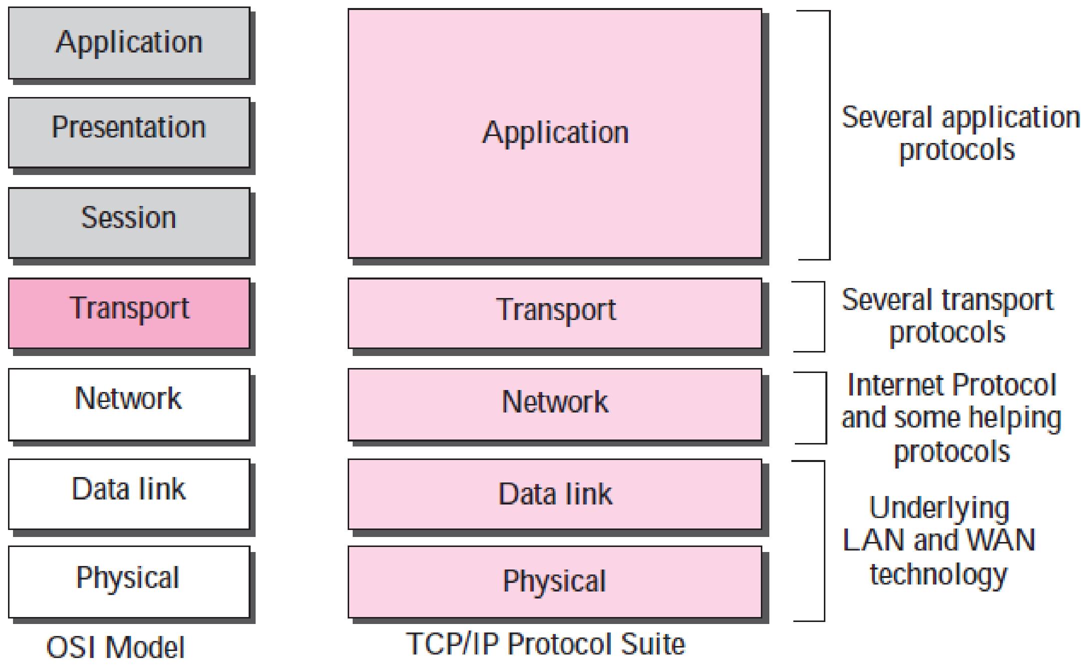
TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination. TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network.

Difference between OSI model and TCP/IP model:

Following are some important differences between OSI reference model and TCP/IP Model.

OSI Reference Model	TCP/IP Model
OSI provides layer functioning and also defines functions of all the layers.	**TCP/IP is** more based on protocols and protocols are not flexible with other layers.
TCP/IP is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality, but the modules are not necessarily interdependent.	OSI model specifies which functions belong to each of its layers, the layers of the TCP/IP protocol suite contain relatively independent protocols that can be mixed and matched, depending on the needs of the system.
In OSI model, the transport layer guarantees the delivery of packets.	**In TCP/IP model,** transport layer does not guarantees delivery of packets.
OSI model follows horizontal approach.	**TCP/IP** Model follows vertical approach.
OSI is a general model.	**TCP/IP model** cannot be used in any other application.
Network layer of OSI model provide both connection oriented and connectionless service.	The network layer in TCP/IP model provides connectionless service.
OSI model has session layer.	In TCP/ IP, No session layer, characteristics are provided by transport layer
OSI model has presentation layer.	In TCP/IP, No presentation layer, characteristics are provided by application layer
OSI model has a problem of fitting the protocols in the model.	TCP/IP model does not fit any protocol.
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP, replacing model is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	In TCP/IP, it is not clearly separated its services, interfaces and protocols.
It has seven layers.	It has 4 layers.
OSI model Supports connectionless and connection-oriented communication in the network layer	TCP/IP Supports only connectionless communication in the network layer
OSI model, Model was developed before the development of protocols.	In TCP/IP, Protocols were developed first and then the model was developed.
OSI model is Protocol independent standard.	TCP/IP is a Protocol dependent standard.
OSI is a a theoretical model.	TCP/IP is a model around which Internet is developed.

Figure 2.8 *TCP/IP and OSI model*



Question: What is meant by connection less and connection oriented protocol? Briefly describe three way handshaking technique of TCP/IP. 6 Marks CSE-2012

Connectionless Protocol

A connectionless protocol describes the communication between two network end points where a message is sent from one end point to another without a prior arrangement. At one end, the device transmits data to the other before ensuring that the device on the other end is ready to use. This describes most transmissions on the open internet. Some protocols allow for error correction by requesting a retransmission if necessary.

The internet uses a variety of connectionless protocols to function. Among the supported protocols are HTTP (hypertext transfer), IP, UDP, ICMP, IPX and TIPC. A connectionless protocol is different from a connection-oriented system. A connection-oriented system requires both devices to be able to communicate with each other.

Connectionless protocols, in contrast, allow data to be exchanged without setting up a link between processes. Each unit of data, with all the necessary information to route it to the intended destination, is transferred independent of other data packets and can travel over different paths to reach the final destination. Some data packets might be lost in transmission or might arrive out of sequence to other data packets.
UDP is a connectionless protocol. It is known as a datagram protocol because it is analogous to sending a letter where you don't acknowledge receipt.
Examples of applications that use connectionless transport services are broadcasting and tftp. Early implementations of NFS used UDP, whereas newer implementations prefer to use TCP.

Connection-Oriented Protocols

A Connection-Oriented Protocol (COP) is a networking protocol used to establish a data communication session in which endpoint devices use preliminary protocols to establish end-to-end connections and then the subsequent data stream is delivered in sequential transfer mode.

COPs guarantee sequential data delivery but are classed as an unreliable network service because there is no process to ensure that total data received is the same as what was sent.

COPs provide circuit-switched connections or virtual circuit connections in packet-switched networks (PSN).

Well-known COPs include:

1. Transmission Control Protocol
2. Connection-Oriented Ethernet
3. Asynchronous Transfer Mode
4. Frame Relay
5. Stream Control Transmission Protocol
6. Internetwork Packet Exchange/Sequenced Packet Exchange
7. Transparent Interprocess Communication
8. Datagram Congestion Control Protocol

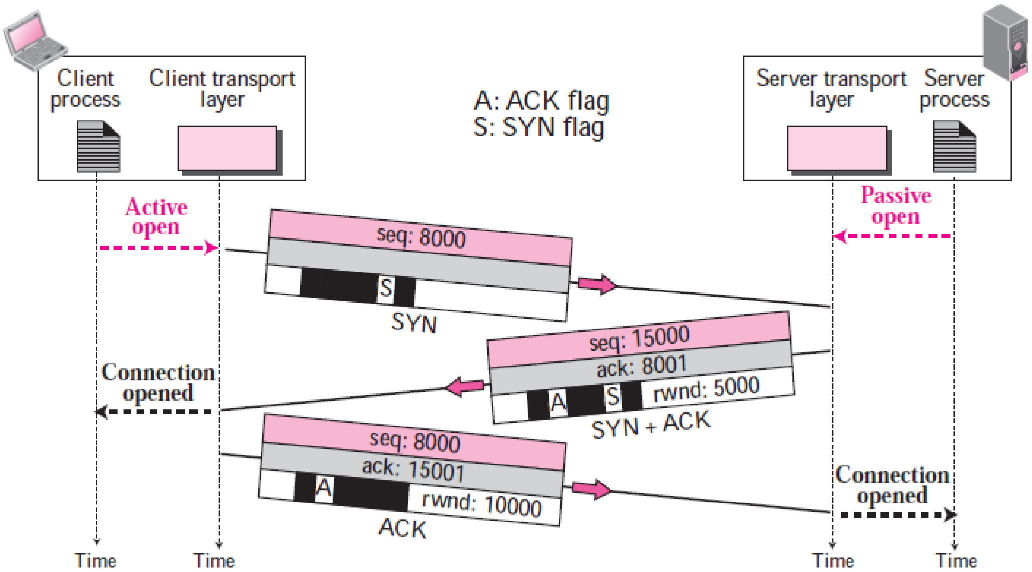
Three way handshaking technique of TCP/IP:

The connection establishment in TCP is called three-way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol. The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This request is called a passive open. Although the server TCP is ready to accept a connection from any machine in the world, it cannot make the connection itself.
The client program issues a request for an active open. A client that wishes to connect to an open server tells its TCP to connect to a particular server. TCP can now start the three-way handshaking process as shown in Figure 15.9.

The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. The client in our example chooses a random number as the first sequence number and sends this number to the server. This sequence number is called the initial sequence number (ISN). Note that this segment does not contain an acknowledgment number. It does not define the window size either; a window size definition makes sense only when a segment includes an acknowledgment. The segment can also include some options that we discuss later in the chapter. Note that the SYN segment is a control segment and carries no data. However, it consumes one sequence number. When the data transfer starts, the ISN is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing one imaginary byte.

Figure 15.9 *Connection establishment using three-way handshaking*



2. The server sends the second segment, a SYN + ACK segment with two flag bits set: SYN and ACK. This segment has a dual purpose. First, it is a SYN segment for communication in the other

direction. The server uses this segment to initialize a sequence number for numbering the bytes sent from the server to the client. The server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client. Because it contains an acknowledgment, it also needs to define the receive window size, rwnd (to be used by the client), as we will see in the flow control section.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers. The client must also define the server window size. Some implementations allow this third segment in the connection phase to carry the first chunk of data from the client. In this case, the third segment must have a new sequence number showing the byte number of the first byte in the data. In general, the third segment usually does not carry data and consumes no sequence numbers.

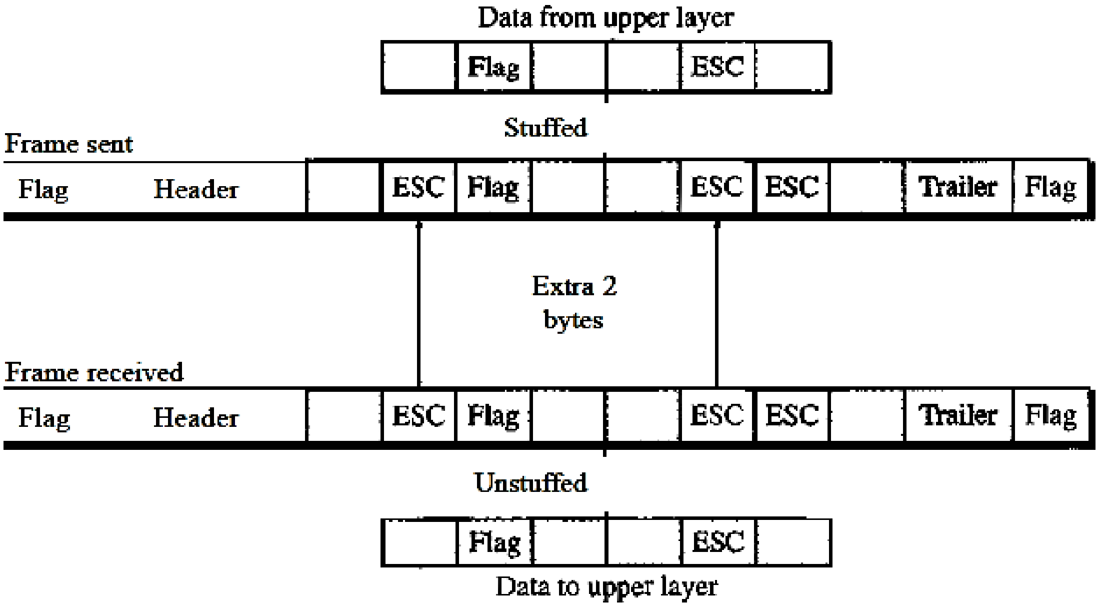
Question: Describe Flag bytes with byte stuffing technique for framing? 5 Marks CSE-2012

Flag bytes with byte stuffing technique:

Byte stuffing is the process of adding 1 extra byte whenever there is a flag or escape character in the text. In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Byte stuffing by the escape character allows the presence of the flag in the data section of the frame, but it creates another problem. What happens if the text contains one or more escape characters followed by a flag? The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame. To solve this problem, the escape characters that are part of the text must also be marked by another escape character. In other words, if the escape character is part of the text, an extra one is added to show that the second one is part of the text. Figure 11.2 shows the situation.

Figure 11.2 *Byte stuffing and unstuffing*



Question: What is Error control? Why it is necessary? 4 Marks CSE-2012

Error Control:

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ). Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame. Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

Why it is necessary:

Question: Describe Hamming Coding technique for error detection and correction. 7 Marks CSE-2012

Hamming Coding Technique:

When data is transmitted from one location to another there is always the possibility that an error may occur. There are a number of reliable techniques that can be used to encode data so that the error can be detected and corrected. With this assignment you will explore a simple error detection-correction technique called a Hamming Code. A Hamming Code can be use to detect and correct a one-bit change in an encoded sequence. This approach can be useful as a change in a single bit is more probable than a change in two bits or more bits.

Here is an example of how this process works. Consider the table below which has 15 positions. Data is represented (stored) in every position except 1, 2, 4 and 8. These positions (which, note, are powers of 2) are used to store the parity (error correction) bits.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		1		2	3	4		5	6	7	8	9	10	11

Using the four parity (error correction bits) positions we can represent 15 values (1- 15). These values and their corresponding binary representation are shown in the table below. Notice that the least significant place is on the left not the right.

Value	$2^0=1$	$2^1=2$	$2^2=4$	$2^3=8$
1	1	0	0	0
2	0	1	0	0
3	1	1	0	0
4	0	0	1	0
5	1	0	1	0
6	0	1	1	0
7	1	1	1	0
8	0	0	0	1
9	1	0	0	1
10	0	1	0	1
11	1	1	0	1
12	0	0	1	1
13	1	0	1	1
14	0	1	1	1
15	1	1	1	1

Using the format given, data is represented by the 11 non-parity bits. Say for example we have the following data item to be encoded:

After placing the data in the table

10101101011

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
		1		0	1	0		1	1	0	1	0	1	1

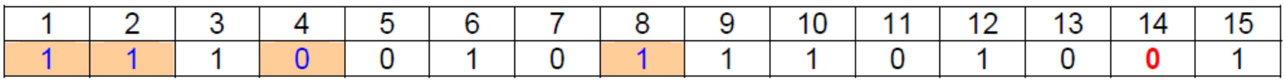
We find that in positions 3, 6, 9, 10, 12, 14 and 15 we have a '1'. Using our previous conversion table we obtain the binary representation for each of these values. We then exclusive OR the resulting values (essentially setting the parity bit to 1 if an odd # of 1's else setting it to 0). The results of this activity are shown below:

```
      1   1   0   0   3
      0   1   1   0   6
      1   0   0   1   9
      0   1   0   1   10
      0   0   1   1   12
      0   1   1   1   14
      1   1   1   1   15
     ---------------
XOR   1   1   0   1   (11)
```

The parity bits are then put in the proper locations in the table providing the following end result:

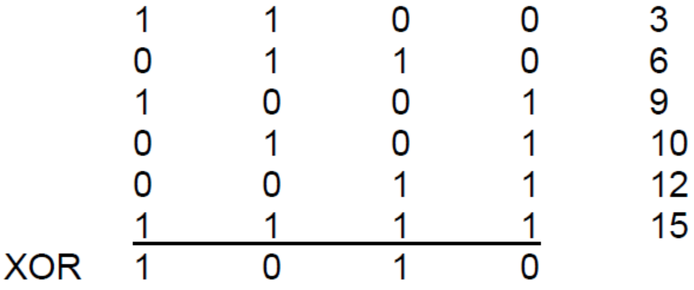
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	0	0	1	0	1	1	1	0	1	0	1	1

This is the encoded sequence that would be sent. The receiving side would re-compute the parity bits and compare what it calculated to the ones received. If they were the same no error occurred – if they were different the location of the flipped bit is determined. For example, let's say that the bit in position 14 was flipped during transmission. The receiving end would see the following encoded sequence:



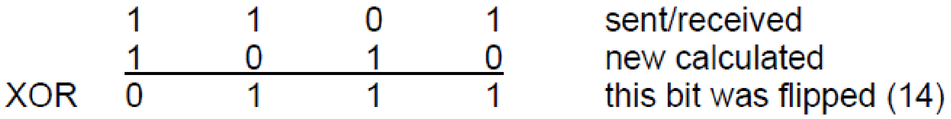
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	1	0	0	1	0	1	1	1	0	1	0	0	1

Below is the re-calculation done at the receiving end (notice the information for position 14 has been left out as it was flipped from 1 to 0).



```
       1    1    0    0    3
       0    1    1    0    6
       1    0    0    1    9
       0    1    0    1    10
       0    0    1    1    12
       1    1    1    1    15
       ------------------
XOR    1    0    1    0
```

The re-calculated parity information is then compared to the parity information sent/received. If they are both the same the result (again using an XOR – even parity) will be all 0's. If a single bit was flipped the resulting number will the position of the errant bit (check back into table). For example:



```
       1    1    0    1      sent/received
       1    0    1    0      new calculated
       ------------------
XOR    0    1    1    1      this bit was flipped (14)
```

Question: Describe the lost frame detection and resend process of Go-Back-N ARQ. 4 Marks CSE-2012

Lost Frame Detection And Resend Process Of Go-Back-N ARQ:

Lost frame detection and resend process of Go-Back-N ARQ is described below:

Acknowledgment and Lost frame Detection:

Although there can be a timer for each frame that is sent, in our protocol we use only one. The reason is that the timer for the first outstanding frame always expires first; we send all outstanding frames when this timer expires. The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting. The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire.

This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer. The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgment for several frames.

Resending a Frame

When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4,5, and 6 again. That is why the protocol is called Go-Back-N ARQ.

Example:

Figure 11.17 shows what happens when a frame is lost. Frames 0, 1, 2, and 3 are sent. However, frame 1 is lost. The receiver receives frames 2 and 3, but they are discarded because they are received out of order (frame 1 is expected). The sender receives no acknowledgment about frames 1, 2, or 3. Its timer finally expires. The sender sends all outstanding frames (1, 2, and 3) because it does not know what is wrong. Note that the resending of frames l, 2, and 3 is the response to one single event. When the sender is responding to this event, it cannot accept the triggering of other events. This means that when ACK 2 arrives, the sender is still busy with sending frame 3. The physica1layer must wait until this event is completed and the data link layer goes back to its sleeping state. We have shown a vertical line to indicate the delay. It is the same story with ACK 3; but when ACK 3 arrives, the sender is busy responding to ACK 2. It happens again when ACK 4 arrives. Note that before the second timer expires, all outstanding frames have been sent and the timer is stopped.

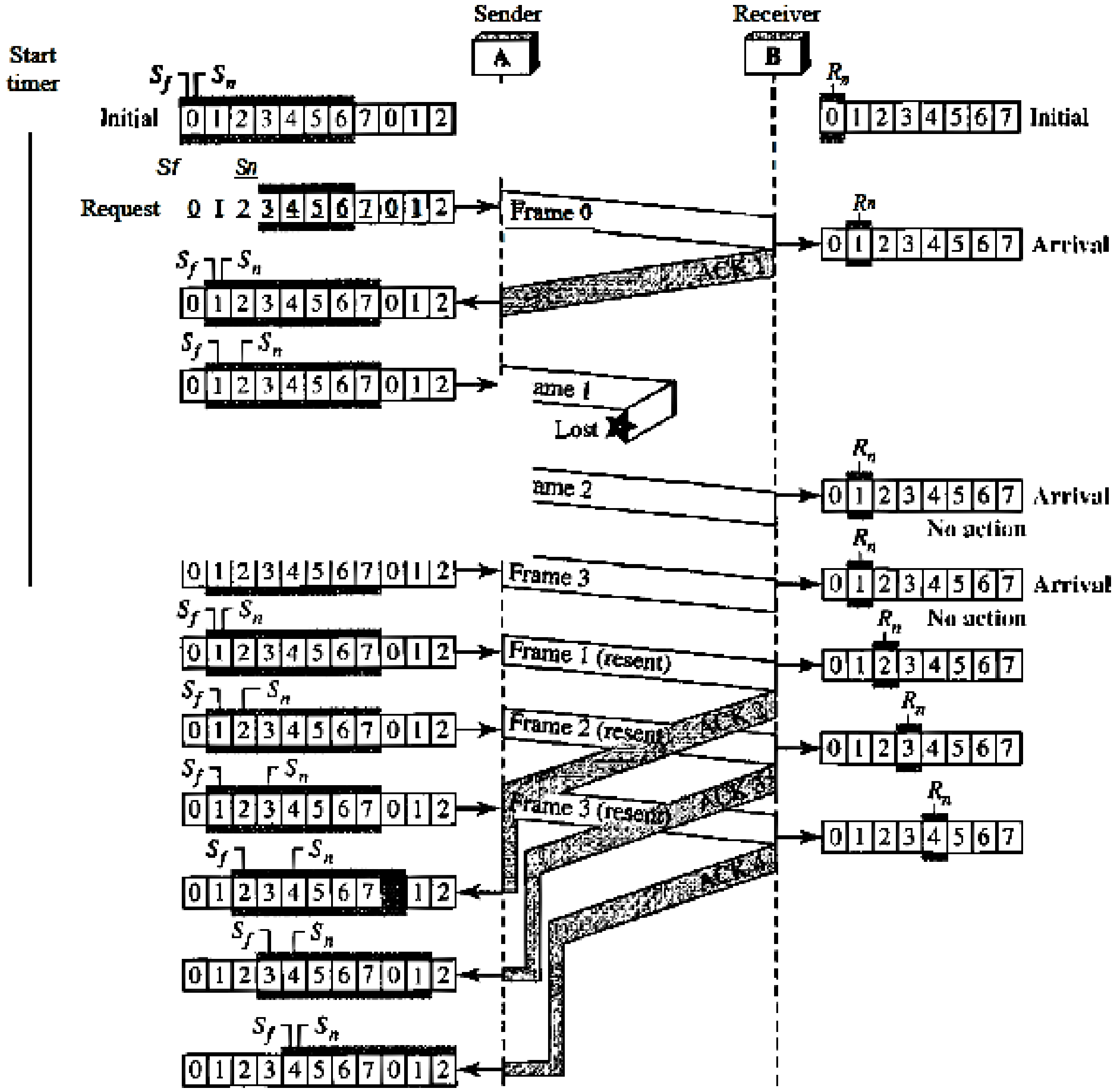


Figure 11.7 Flow diagram for Example

Question: Differentiate between subnetting and super netting. Briefly describe the concept of class less IP addressing. 6 Marks CSE-2012

<u>Difference between subnetting and super netting:</u>

Following are some important differences between subnetting and supernetting:

Subnetting	Supernetting
Subnetting is the process of dividing an IP network in to sub divisions called subnets	Supernetting is the process of combining several IP networks with a common network prefix
Subnetting will increase the number of entries in a routing table and also will complex the routing process	Supernetting will reduce the number of entries in a routing table and also will simplify the routing process
In subnetting, host ID bits (for IP addresses from a single network ID) are borrowed to be used as a subnet ID	in supernetting, bits from the network ID are borrowed to be used as the host ID
The network mask is used when a network is not subnetted. When we divide a network to several subnetworks, we need to create a subnetwork mask (or subnet mask) for each subnetwork. A subnetwork has subnetid and hosted.	When we combine several network into a supernet, we need to create a supernetwork mask (or supernet mask).
A subnet mask that divides a block into eight subblocks has three more 1s ($2^3 = 8$) than the default mask.	A supernet mask that combines eight blocks into one superblock has three less 1s than the default mask.

<u>Classless IP Addressing:</u>

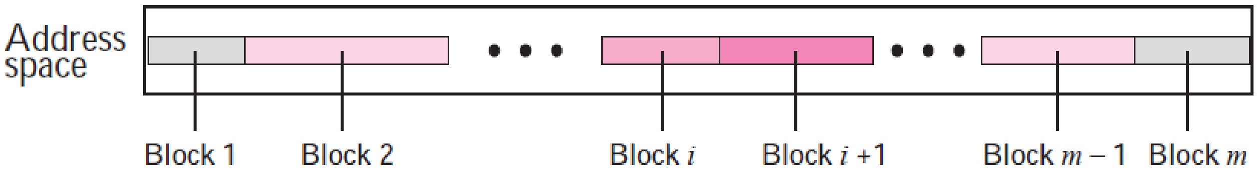
A scheme of IP Addressing to overcome address depletion and give more organizations access to the Internet where there are no classes, but the addresses are still granted in blocks is called Classless IP Addressing.
Subnetting and supernetting in classful addressing did not really solve the address depletion problem and made the distribution of addresses and the routing process more difficult. With the growth of the Internet, it was clear that a larger address space was needed as a long-term solution. The larger address space, however, requires that the length of IP addresses to be increased, which means the format of the IP packets needs to be changed. Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization. The short-term solution still uses IPv4 addresses, but it is called classless addressing. In other words, the class privilege was removed from the distribution to compensate for the address depletion.

In classless addressing, variable-length blocks are used that belong to no classes. We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.

<u>Variable-Length Blocks</u>

In classless addressing, the whole address space is divided into variable length blocks. Theoretically, we can have a block of $2^0, 2^1, 2^2, \ldots, 2^{32}$ addresses. The only restriction, as we discuss later, is that the number of addresses in a block needs to be a power of 2. An organization can be granted one block of addresses. Figure 5.27 shows the division of the whole address space into non-overlapping blocks.

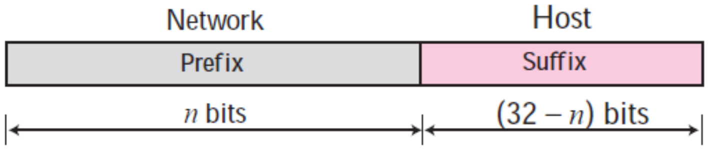
Figure 5.27 *Variable-length blocks in classless addressing*



<u>Two-Level Addressing</u>

In classless addressing. When an organization is granted a block of addresses, the block is actually divided into two parts, the prefix and the suffix. The prefix plays the same role as the netid; the suffix plays the same role as the hosted used in classfull addressing. All addresses in the block have the same prefix; each address has a different suffix. Figure 5.28 shows the prefix and suffix in a classless block. In classless addressing, the prefix defines the network and the suffix defines the host. In classless addressing, the length of the prefix, n, depends on the size of the block; it can be 0, 1, 2, 3, . . . , 32. In classless addressing, the value of n is referred to as prefix length; the value of 32 − n is referred to as suffix length. The prefix length in classless addressing can be 1 to 32.

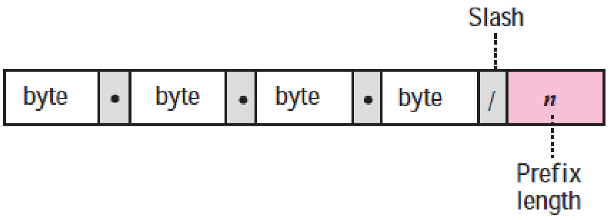
Figure 5.28 *Prefix and suffix*



Slash Notation

The prefix length in classless addressing play a very important role when we need to extract the information about the block from a given address in the block. In classless addressing, the prefix length cannot be found if we are given only an address in the block. The given address can belong to a block with any prefix length. In classless addressing, we need to include the prefix length to each address if we need to find the block of the address. In this case, the prefix length, n, is added to the address separated by a slash. The notation is informally referred to as slash notation. An address in classless addressing can then be represented as shown in Figure 5.29. The slash notation is formally referred to as **classless interdomain routing** or **CIDR** (pronounced cider) notation. **In classless addressing, we need to know one of the addresses in the block and the prefix length to define the block.**

Figure 5.29 *Slash notation*



Network Mask

The idea of network mask in classless addressing is the same as the one in classful addressing. A network mask is a 32-bit number with the n leftmost bits all set to 0s and the rest of the bits all set to 1s.

Extracting Block Information

An address in slash notation (CIDR) contains all information we need about the block: the first address (network address), the number of addresses, and the last address. These three pieces of information can be found as follows:

❑ The number of addresses in the block can be found as:

$$N = 2^{32} - n$$

in which n is the prefix length and N is the number of addresses in the block.

❑ The first address (network address) in the block can be found by ANDing the address with the network mask:

First address = (any address) AND (network mask)

Alternatively, we can keep the n leftmost bits of any address in the block and set the 32− n bits to 0s to find the first address.

❑ The last address in the block can be found by either adding the first address with the number of addresses or, directly, by ORing the address with the complement (NOTing) of the network mask:

Last address = (any address) OR [NOT (network mask)]

Alternatively, we can keep the n leftmost bits of any address in the block and set the 32 − n bits to 1s to find the last address.

Block Allocation

The next issue in classless addressing is block allocation. The ultimate responsibility of block allocation is given to a global authority called the Internet Corporation for Assigned Names and Addresses (ICANN). However, ICANN does not normally allocate addresses to individual Internet users. It assigns a large block of addresses to an ISP (or a larger organization that is considered an ISP in this case). For the proper operation of the CIDR, three restrictions need to be applied to the allocated block.

1. The number of requested addresses, N, needs to be a power of 2. This is needed to provide an integer value for the prefix length, n (see the second restriction). The number of addresses can be 1, 2, 4, 8, 16, and so on.
2. The value of prefix length can be found from the number of addresses in the block. Since N = 232 - n, then n = log2 (232/N) = 32 - log2N. That is the reason why N needs to be a power of 2.
3. The requested block needs to be allocated where there are a contiguous number of unallocated addresses in the address space. However, there is a restriction on choosing the beginning addresses of the block. The beginning address needs to be divisible by the number of addresses in the block. To see this restriction, we can show that the beginning address can be calculated as X × 2n - 32 in which X is the decimal value of the prefix. In other words, the beginning address is X × N.