

COMPUTER NETWORKS

Syllabus

UNIT-I

Introduction to computer Networks, direction of data flow (simplex, Half duplex, full duplex); Networks: distributed processing, network criteria, physical structure (type of connection, topology), categories of network (LAN, MAN, WAN); Internet: brief history, internet today; Protocols and standards; Reference models: OSI reference model, TCP/IP reference model, their comparative study.

UNIT-II

Physical Layer: Types of errors, framing (character and bit stuffing), error detection & correction methods; Flow control; Protocols: Stop &wait ARQ, Go-Back-N ARQ, Selective repeat ARQ, HDLC;

UNIT-III

Point to point protocol, LCP, NCP, FDDI, token bus, token ring; Reservation, polling, concentration; Multiple access protocols: Pure ALOHA, Slotted ALOHA, CSMA, CSMA/CD, FDMA, TDMA, CDMA; Traditional Ethernet, fast Ethernet;

UNIT-IV

Routing : techniques, static vs. dynamic routing , routing table for classful address; Routing algorithms: shortest path algorithm, flooding, distance vector routing, link state routing, Mobile routing basic algorithms.

UNIT-V

Protocols: ARP, RARP, IP, ICMP, IPV6; Unicast and multicast routing protocols. Congestion control algorithm: Leaky bucket algorithm, Token bucket algorithm, choke packets. Congestion control protocols.

UNIT-VI

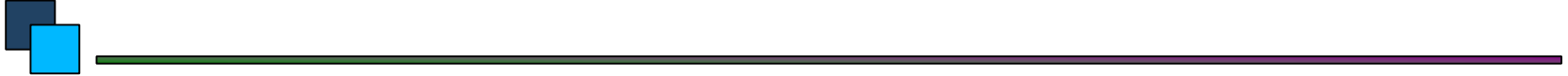
Process to process delivery; UDP; TCP; Quality of service: techniques to improve Qos. ISDN services & ATM; DSL technology, Cable modem, Sonet. Wireless LAN: IEEE 802.11; Introduction to blue-tooth, VLAN's, Cellular telephony & Satellite network.

Text Books:

1. B. A. Forouzan –“Data Communications and Networking (3rd Ed.) “ –TMH
2. A. S. Tanenbaum –“Computer Networks (4th Ed.)” –Pearson Education/PHI
3. W. Stallings –“Data and Computer Communications (8th Ed.)” –PHI/ Pearson Education

Reference Books:

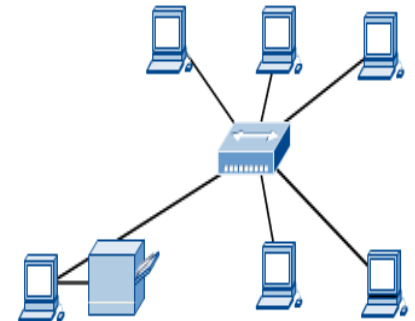
1. Kurose and Rose –“Computer Networking -A top down approach featuring the internet”
Pearson Education
2. Introduction to Data Communications and Networking by Wayne Tomasi-Pearson Edition
3. Comer –“Internetworking with TCP/IP, vol. 1, 2, 3(4th Ed.)” –Pearson Education/PHI



INTRODUCTION TO COMPUTER NETWORKS

Computer Networks

- ❏ "Computer network" means a collection of autonomous computers interconnected by a single technology.
- ❏ Two computers are said to be interconnected if they are able to exchange information.
- ❏ The connection need not be via a copper wire; fiber optics, microwaves, infrared, and communication satellites can also be used.
- ❏ The computers can be geographically located anywhere.



Computer Networks



- ❏ Neither the Internet nor the World Wide Web is a computer network.
- ❏ The Internet is not a single network but a network of networks and the Web is a distributed system that runs on top of the Internet.

Difference between Computer Network and Distributed System ???



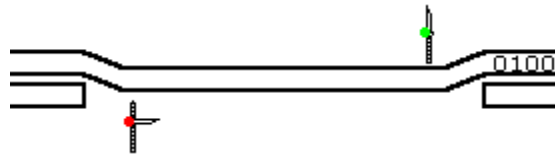
- ❑ The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system.
- ❑ Often a layer of software on top of the operating system, called middleware, is responsible for implementing this model. A well-known example of a distributed system is the World Wide Web, in which everything looks like a document (Web page).
- ❑ In a computer network, this coherence, model, and software are absent .
- ❑ Users are exposed to the actual machines, without any attempt by the system to make the machines look and act in a coherent way. If a user wants to run a program on a remote machine, he has to log onto that machine and run it there.
- ❑ Nevertheless, there is considerable overlap between the two subjects. For example, both distributed systems and computer networks need to move files around. The difference lies in who invokes the movement, the system or the user.

Direction of Data Flow

- A connection that allows traffic in both directions simultaneously is called **full duplex**. A two-lane road is full duplex.

```
010010010100010101000011
110000101010001010010010
```

- A connection that allows traffic either way, but only one way at a time is called **half duplex**. A single railroad track is half duplex.



- A connection that allows traffic only one way is called simplex. A one-way street is **simplex**. Another example of a simplex connection is an optical fiber with a laser on one end and a light detector on the other end.

```
010010010100010101000011
```

Uses of Computer Networks

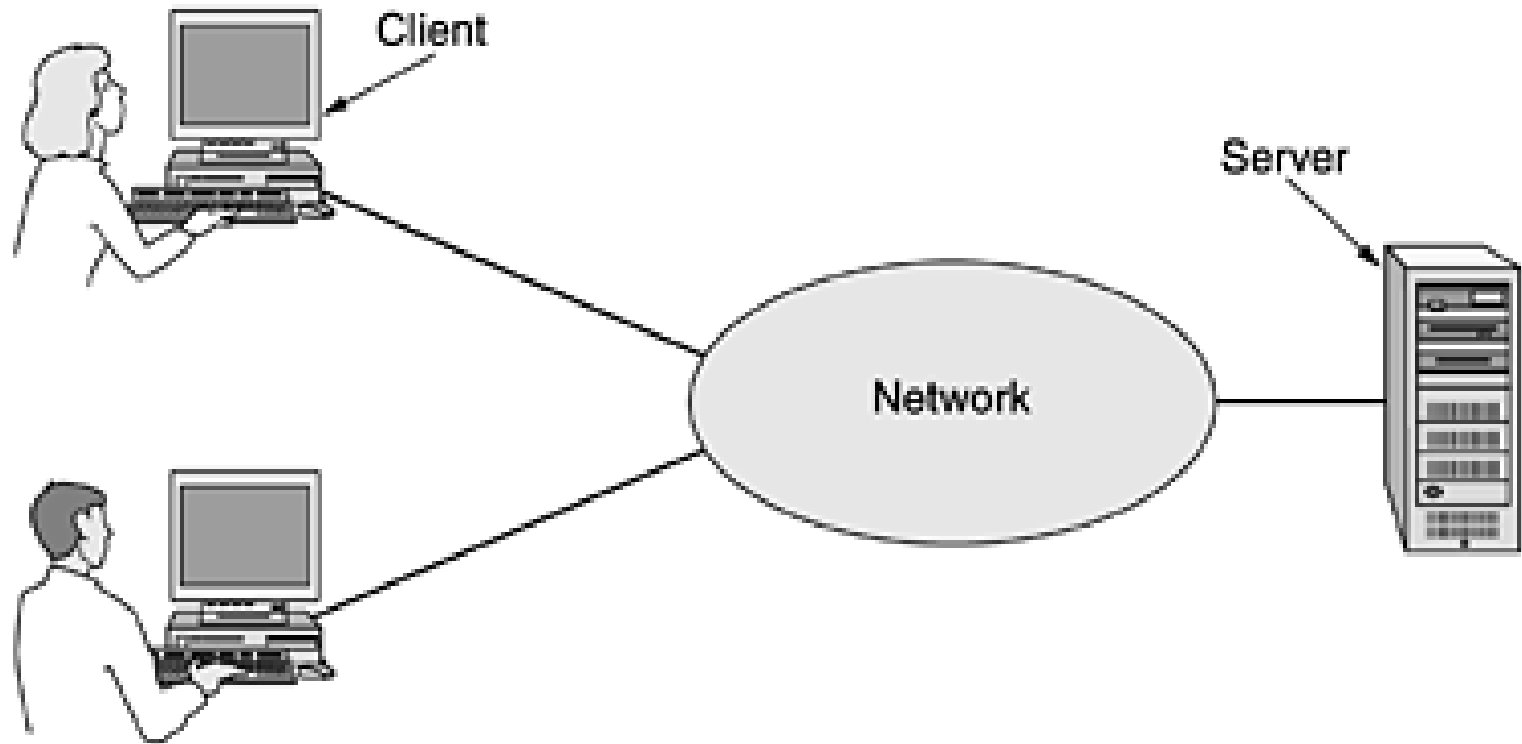


Resource sharing – The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user.



Remote Access to data - Suppose a company's information system as consisting of one or more databases and some number of employees who need to access them remotely. 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 have simpler machines, called clients, on their desks, with which they access remote data,

Introduction to Computer Networks



Introduction to Computer Networks

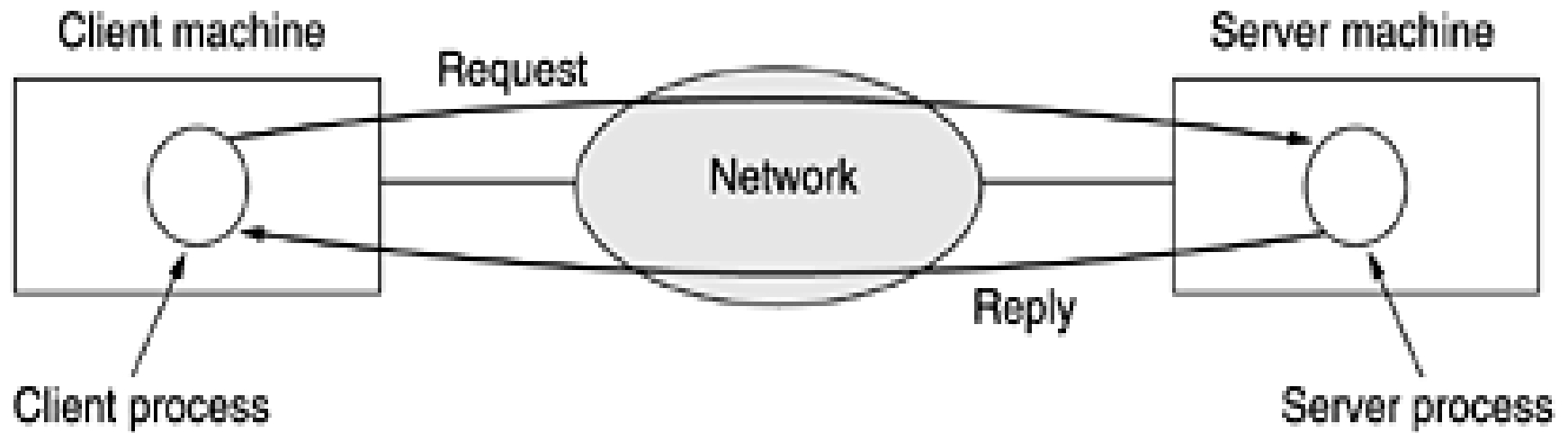






Figure . The client-server model involves requests and replies.

Uses of Computer Networks

Communication Medium

-  E-mails
-  Videoconferencing
-  doing business electronically
-  E-commerce

Networks



- ❖ A network consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.
- ❖ The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Network Speed

- ❑ A network's speed can be summed up with two values:
 - Bit rate:
 - How many bits can be placed on the network in a given time interval (e.g. 1 second)?
 - This is often called bandwidth, but this is a misnomer since bandwidth has to do with the range of frequencies to be used
 - Bit rate becomes the dominant factor when sending many packets (e.g. a large file)
 - Latency:
 - How long does it take a bit to be received by the destination node?
 - Latency becomes the dominant factor when sending individual packets, or alternating sending/receiving

Network topology

- A *topology* is a way of “laying out” the network. Topologies can be either physical or logical.
- *Physical topologies* describe how the cables are run.
- *Logical topologies* describe how the network messages travel

Network topology (cont.)

- Bus (can be both logical and physical)
- Star (physical only)
- Ring (can be both logical and physical)
- Mesh (can be both logical and physical)

Different Types of Networks

- ❖ Depending upon the geographical area covered by a network, it is classified as:
 - – Local Area Network (LAN)
 - – Metropolitan Area Network (MAN)
 - – Wide Area Network (WAN)

Types of Networks

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 1-6. Classification of interconnected processors by scale.

LAN, MAN & WAN

- ❏ Network in small geographical Area (Room, Building or a Campus) is called LAN (Local Area Network)
- ❏ Network in a City is call MAN (Metropolitan Area Network)
- ❏ Network spread geographically (Country or across Globe) is called WAN (Wide Area Network)


LAN (Local Area Network)

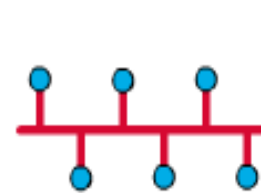
- *A LAN is a network that is used for communicating among computer devices, usually within an office building or home.*
- LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- Is limited in size, typically spanning a few hundred meters, and no more than a mile
- Is fast, with speeds from 10 Mbps to 10 Gbps
- Requires little wiring, typically a single cable connecting to each device
- Has lower cost compared to MAN's or WAN's.

LAN (Local Area Network)

- LAN's can be either wired or wireless. Twisted pair, coax or fiber optic cable can be used in wired LAN's.
- Every LAN uses a protocol – a set of rules that governs how packets are configured and transmitted.
- Nodes in a LAN are linked together with a certain topology. These topologies include:
 - Bus
 - Ring
 - Star
 - Mesh
- LANs are capable of very high transmission rates (100s Mb/s to G b/s).

Network Topology

 The network topology defines the way in which computers, printers, and other devices are connected. A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.



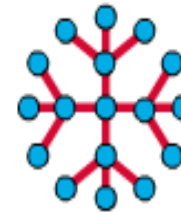
Bus Topology



Ring Topology



Star Topology



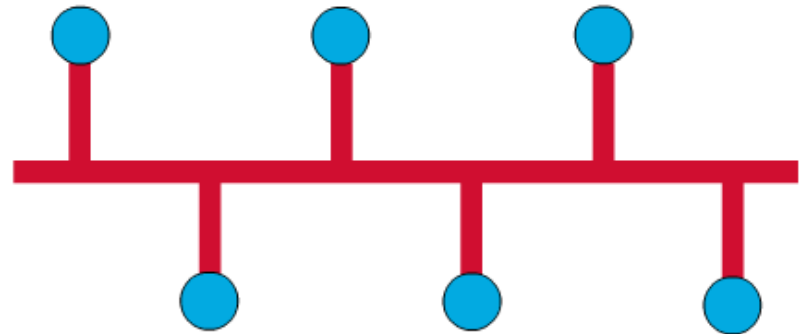
Extended Star Topology



Mesh Topology

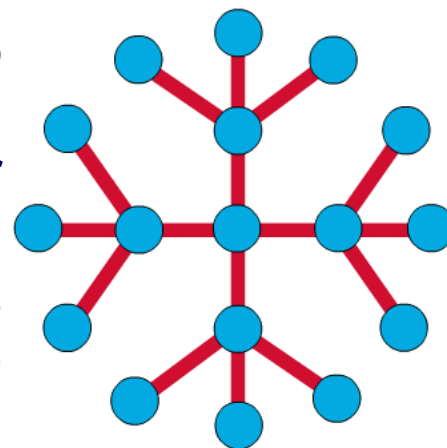
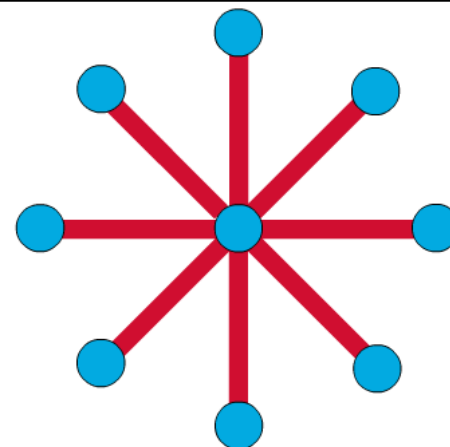
Bus Topology

Commonly referred to as a linear bus, all the devices on a bus topology are connected by one single cable.



Star & Tree Topology

- ❏ The star topology is the most commonly used architecture in Ethernet LANs.
- ❏ When installed, the star topology resembles spokes in a bicycle wheel.
- ❏ Larger networks use the extended star topology also called tree topology. When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



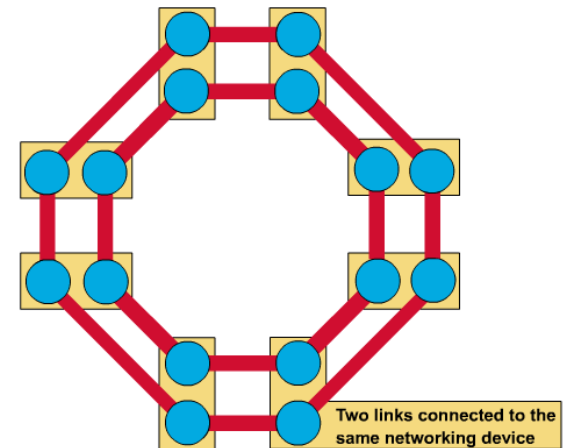
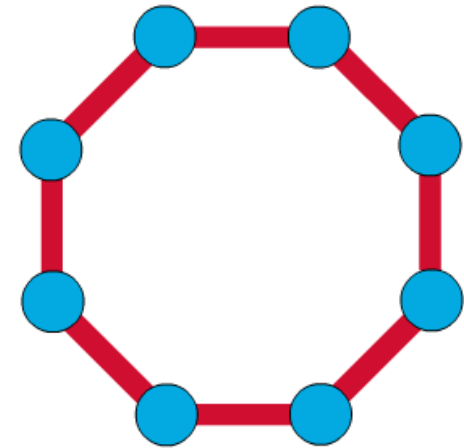
Ring Topology

■ A frame travels around the ring, stopping at each node. If a node wants to transmit data, it adds the data as well as the destination address to the frame.

■ The frame then continues around the ring until it finds the destination node, which takes the data out of the frame.

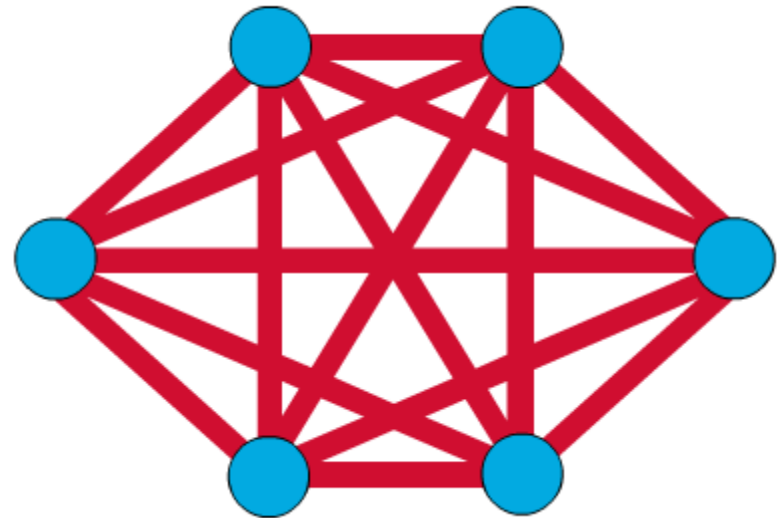
■ Single ring – All the devices on the network share a single cable

■ Dual ring – The dual ring topology allows data to be sent in both directions.



Mesh Topology

- ❏ The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- ❏ It is used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- ❏ Implementing the mesh topology is expensive and difficult.



Network topology (cont.)

Bus

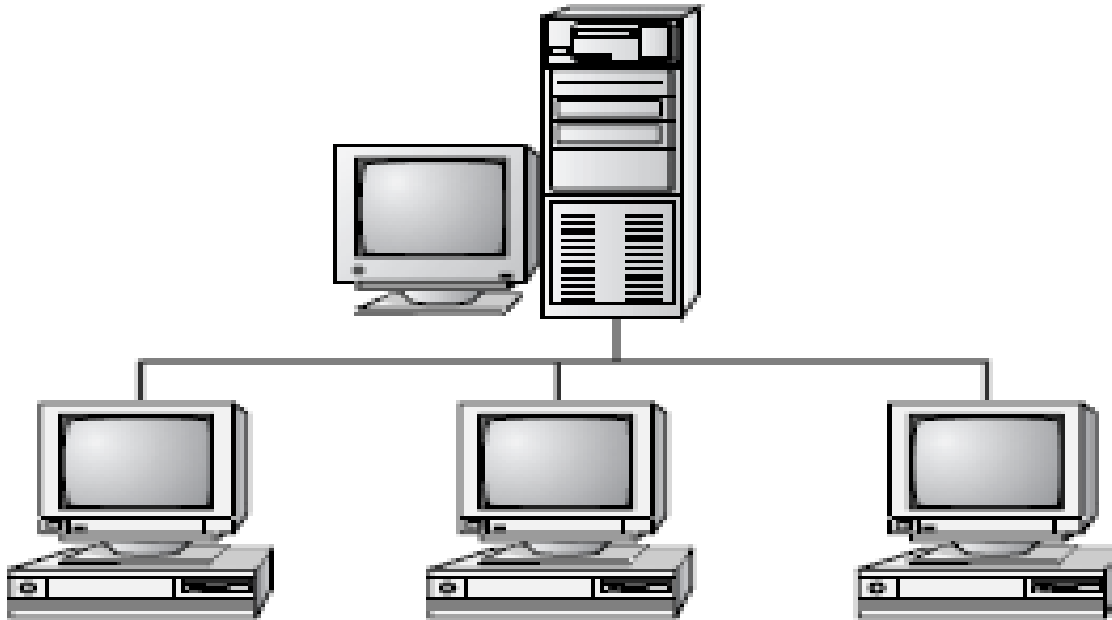
- A bus is the simplest physical topology. It consists of a single cable that runs to every workstation
- This topology uses the least amount of cabling, but also covers the shortest amount of distance.
- Each computer shares the same data and address path. With a logical bus topology, messages pass through the trunk, and each workstation checks to see if the message is addressed to itself. If the address of the message matches the workstation's address, the network adapter copies the message to the card's on-board memory.

Network topology (cont.)

- it is difficult to add a workstation
- have to completely reroute the cable and possibly run two additional lengths of it.
- if any one of the cables breaks, the entire network is disrupted. Therefore, it is very expensive to maintain.

Network topology (cont.)

- Bus topology



Network topology (cont.)

Star Topology

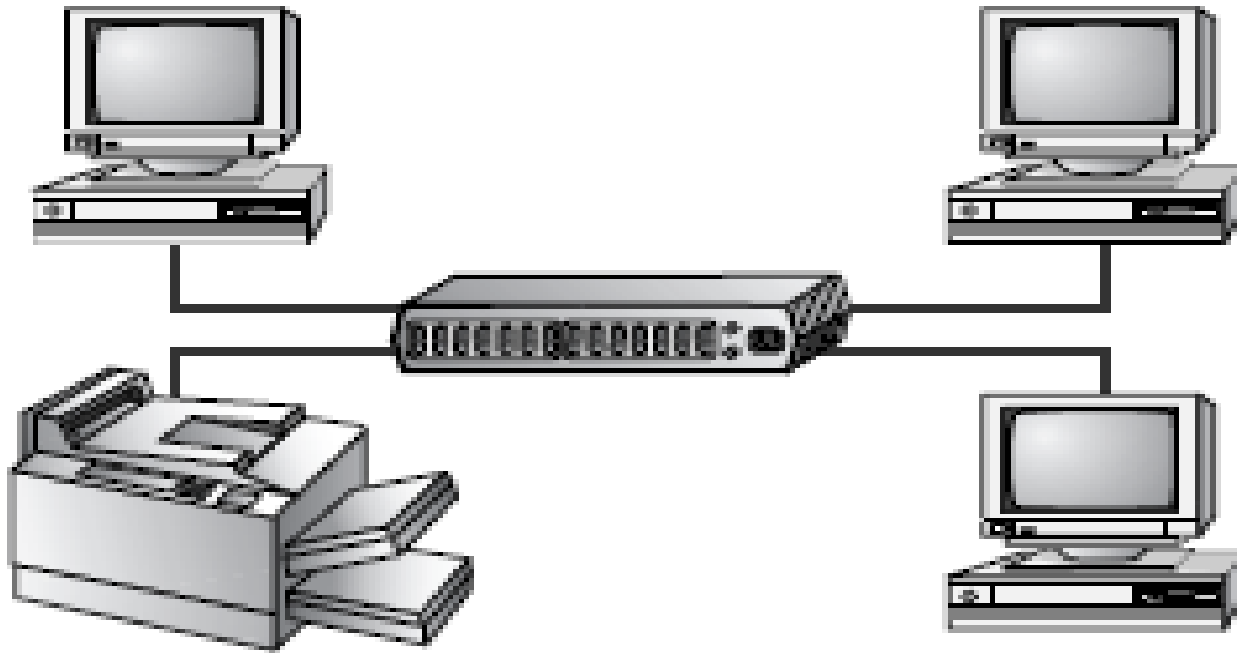
- A physical star topology branches each network device off a central device called a *hub*, making it very easy to add a new workstation.
- Also, if any workstation goes down it does not affect the entire network. (But, as you might expect, if the central device goes down, the entire network goes down.)
- Some types of Ethernet and ARCNet use a physical star topology. Figure gives an example of the organization of the star network.

Network topology (cont.)

- Star topologies are easy to install. A cable is run from each workstation to the hub. The hub is placed in a central location in the office.
- Star topologies are more expensive to install than bus networks, because there are several more cables that need to be installed, plus the cost of the hubs that are needed.

Network topology (cont.)

- Star Topology



Network topology (cont.)

Ring

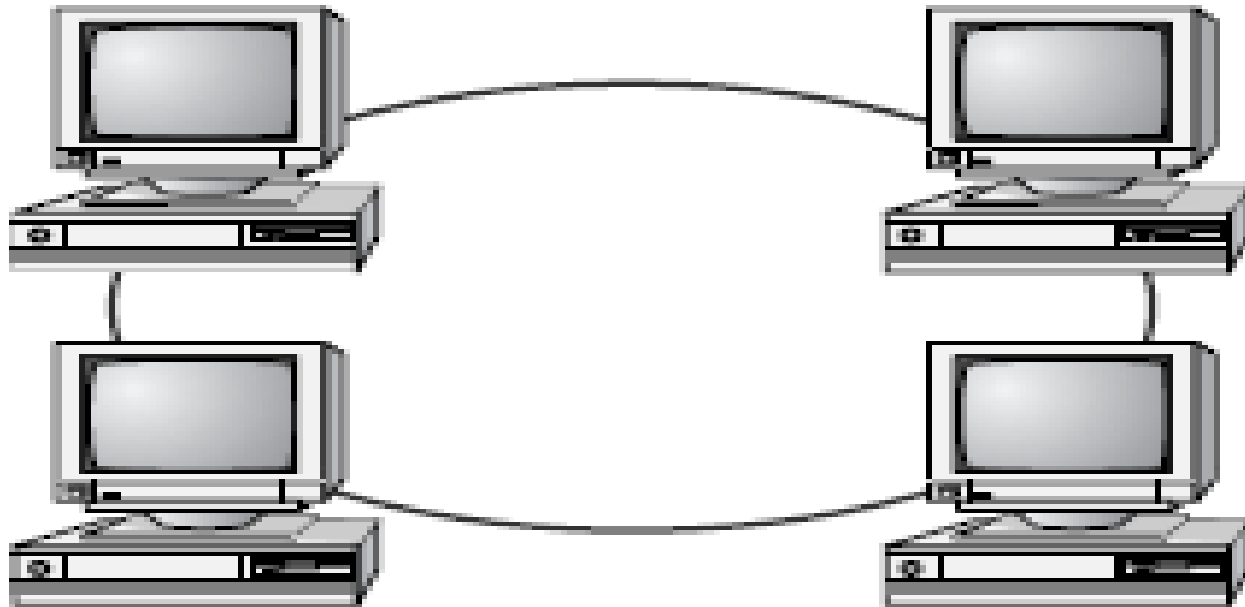
- Each computer connects to two other computers, joining them in a circle creating a unidirectional path where messages move workstation to workstation.
- Each entity participating in the ring reads a message, then regenerates it and hands it to its neighbor on a different network cable.

Network topology (cont.)

- The ring makes it difficult to add new computers.
- Unlike a star topology network, the ring topology network will go down if one entity is removed from the ring.
- Physical ring topology systems don't exist much anymore, mainly because the hardware involved was fairly expensive and the fault tolerance was very low.

Network topology (cont.)

- Ring Topology



Network topology (cont.)

Mesh

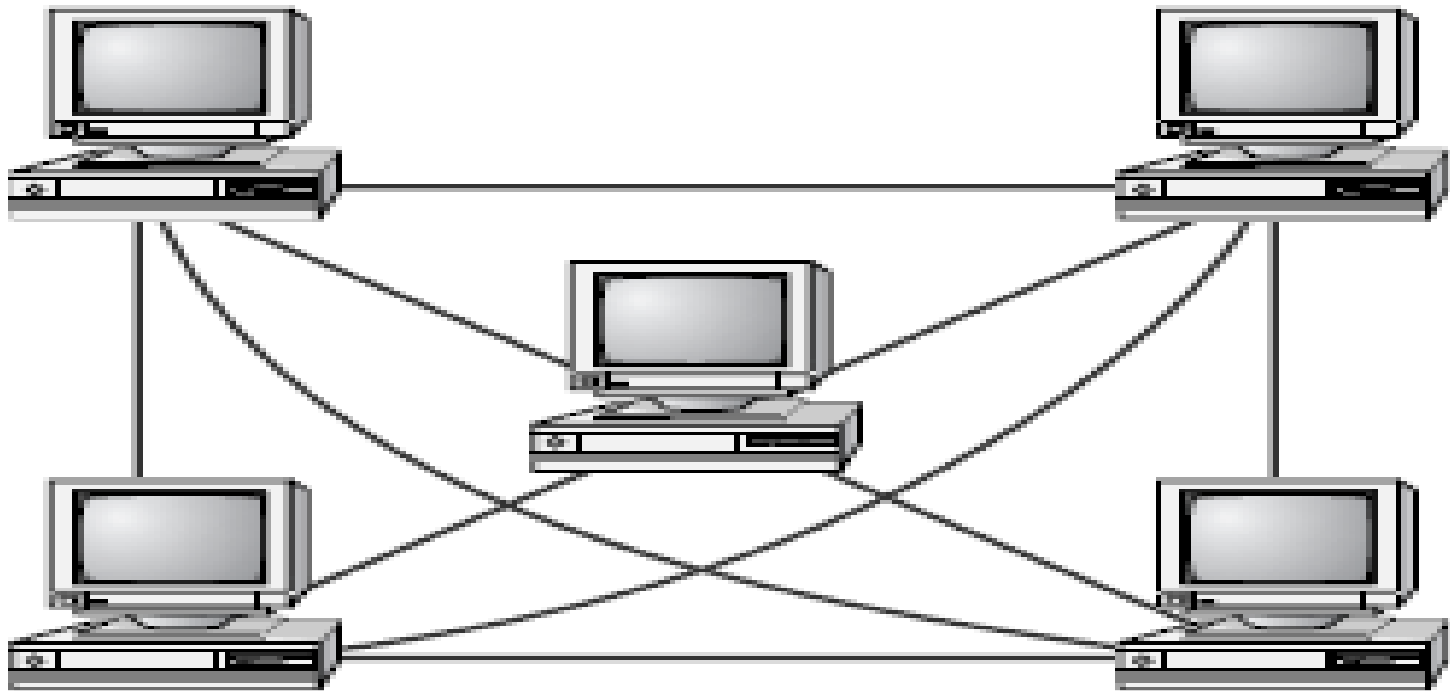
- The *mesh topology* is the simplest logical topology in terms of data flow, but it is the most complex in terms of physical design.
- In this physical topology, each device is connected to every other device
- This topology is rarely found in LANs, mainly because of the complexity of the cabling.
- If there are x computers, there will be $(x \times (x-1)) \div 2$ cables in the network. For example, if you have five computers in a mesh network, it will use $5 \times (5 - 1) \div 2$, which equals 10 cables. This complexity is compounded when you add another workstation.
- If a network contains n machines then there are n^2 maximum connections possible so that each machine becomes accessible from other.

Network topology (cont.)

- Because of its design, the physical mesh topology is very expensive to install and maintain.
- Cables must be run from each device to every other device. The advantage you gain from it is its high fault tolerance.
- With a logical mesh topology, however, there will always be a way of getting the data from source to destination.
- It may not be able to take the direct route, but it can take an alternate, indirect route. It is for this reason that the mesh topology is still found in WANs to connect multiple sites across WAN links. It uses devices called *routers* to search multiple routes through the mesh and determine the best path.
- However, the mesh topology does become inefficient with five or more entities.

Network topology (cont.)

- Mesh Topology



Network topology (cont.)

- Advantages and Disadvantages of Network Topologies

Topology	Advantages	Disadvantages
Bus	Cheap. Easy to install.	Difficult to reconfigure. Break in bus disables entire network.
Star	Cheap. Easy to install. Easy to reconfigure. Fault tolerant.	More expensive than bus.
Ring	Efficient. Easy to install.	Reconfiguration difficult. Very expensive.
Mesh	Simplest. Most fault tolerant.	Reconfiguration extremely difficult. Extremely expensive. Very complex.

Advantages of LAN



- Speed
- Cost
- Security
- E-mail
- Resource Sharing

Disadvantages of LAN

- Expensive To Install
- Requires Administrative Time
- File Server May Fail
- Cables May Break



MAN (Metropolitan Area Network)

- A **metropolitan area network (MAN)** is a **large** computer network that usually covers a city or a large campus.
- The best-known example of a MAN is the cable television network available in many cities
- A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities.
- A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations.
- A MAN often acts as a high speed network to allow sharing of regional resources.
- A MAN typically covers an area of between 5 and 50 km diameter.

MAN (Metropolitan Area Network)

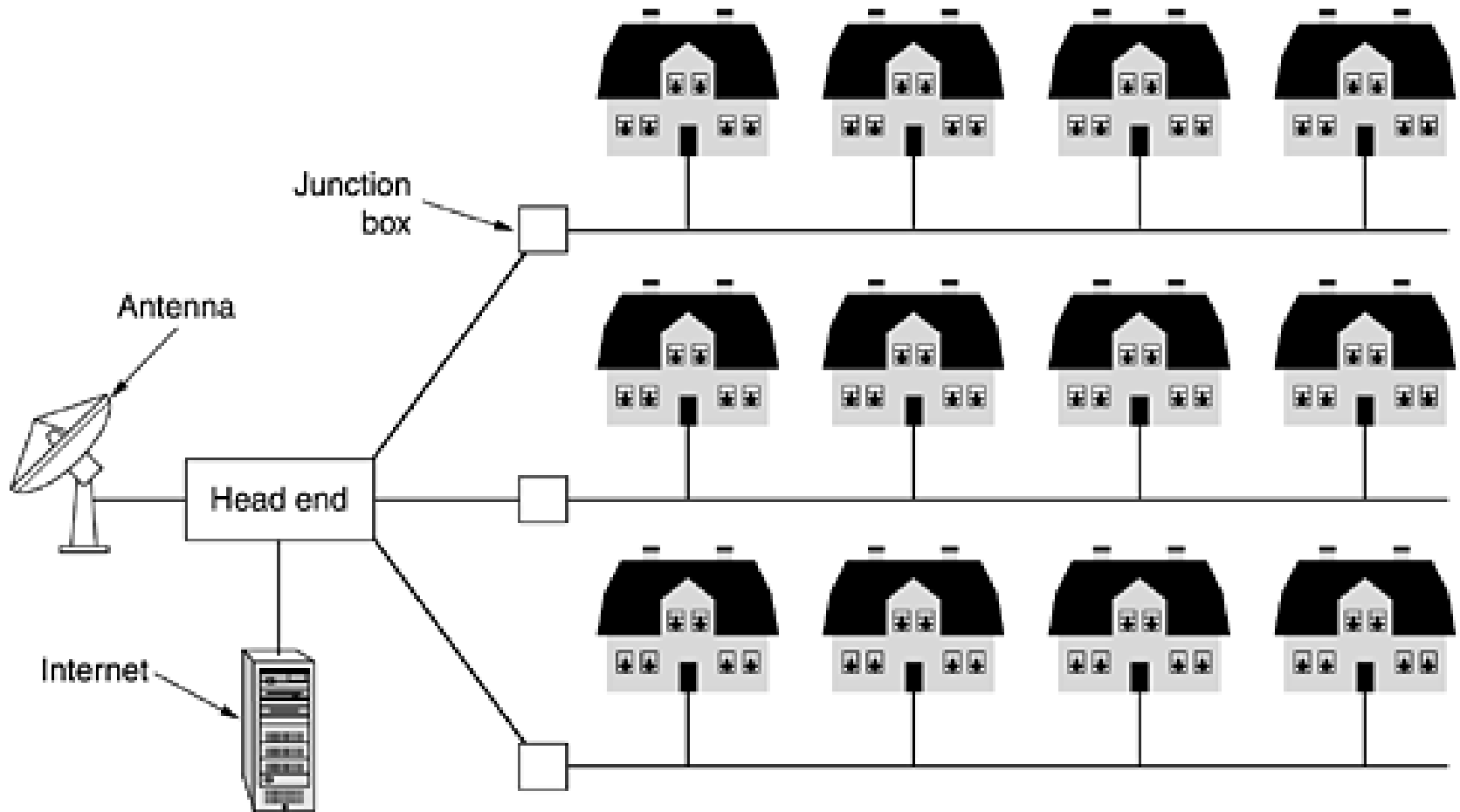


Figure . A metropolitan area network based on cable TV

WAN (Wide Area Network)

- WAN covers a large geographic area such as country, continent or even whole of the world.
- A WAN is two or more LANs connected together. The LANs can be many miles apart.
- To cover great distances, WANs may transmit data over leased high-speed phone lines or wireless links such as satellites.
- Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data.
- The world's most popular WAN is the Internet.



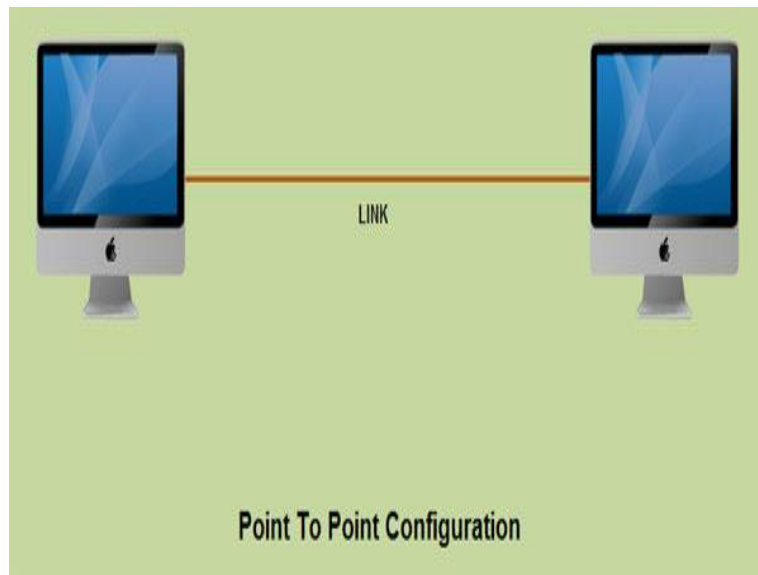
Intranet and Internet Specifications

- **Intranet:** *An intranet is a private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network.*
- An intranet uses [TCP/IP](#), [HTTP](#), and other Internet protocols and in general looks like a private version of the Internet. With [tunneling](#), companies can send private messages through the public network, using the public network with special encryption/decryption and other security safeguards to connect one part of their intranet to another.
- **Internet:** *is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer (and sometimes talk directly to users at other computers).*

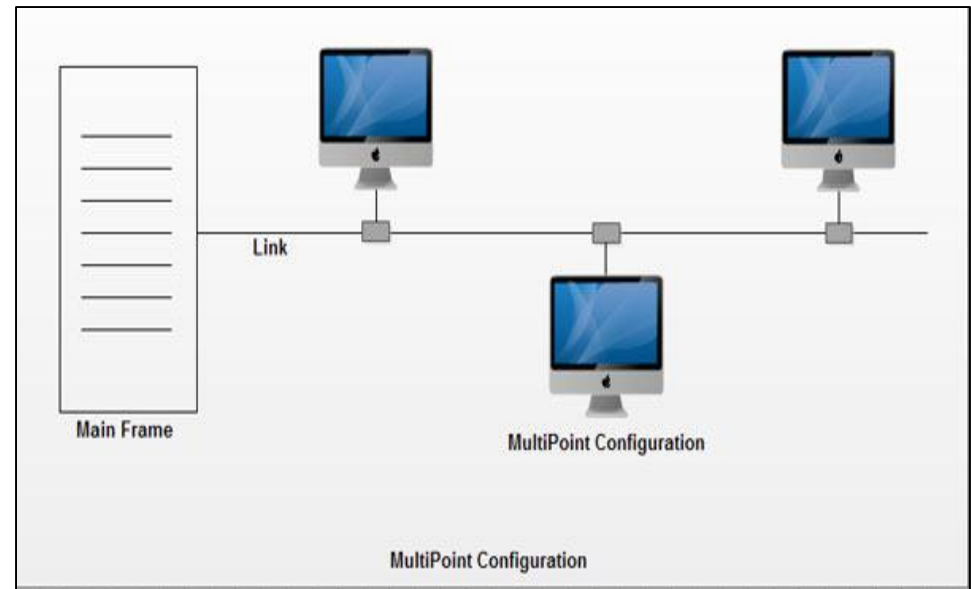
Types of Connections

➤ The two different computer network connection types are

- **Point –to–Point Connection**



- **Multipoint Connection**



Point –to–Point Connections

- A **point-to-point connection** is a direct link between two devices such as a computer and a printer. It uses dedicated link between the devices.
- The entire capacity of the link is used for the transmission between those two devices.
- In point to point networks, there exist many connections between individual pairs of machines.
- To move from sources to destination, a packet (short message) may follow different routes. In networking, the Point-to-Point Protocol (PPP) is a data link protocol commonly used in establishing a direct connection between two networking nodes.

Multipoint Connections

- A multipoint connection is a link between three or more devices. It is also known as Multi-drop configuration.
- The networks having multipoint configuration are called **Broadcast Networks**. In broadcast network, a message or a packet sent by any machine is received by all other machines in a network.
- The packet contains address field that specifies the receiver. Upon receiving a packet, every machine checks the address field of the packet. If the transmitted packet is for that particular machine, it processes it; otherwise it just ignores the packet.


PP and MP Connections

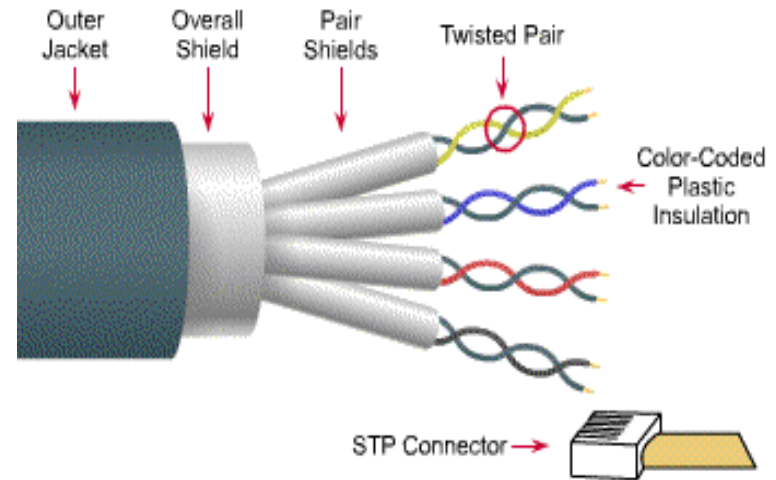
- **Unicast** is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.
- **Broadcast** is the term used to describe communication where a piece of information is sent from one point to all other points. In this case there is just one sender, but the information is sent to all connected receivers.
- **Multicast** is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers, or any other number of receivers).

Network Components

- Physical Media
- Interconnecting Devices
- Computers
- Networking Software
- Applications

Networking Media

 Networking media can be defined simply as the means by which signals (data) are sent from one computer to another (either by cable or wireless means).




- Speed and throughput: 10-100 Mbps
- Cost per node: Moderately expensive
- Media and connector size: Medium to Large
- Maximum cable length: 100m (short)


Networking Devices

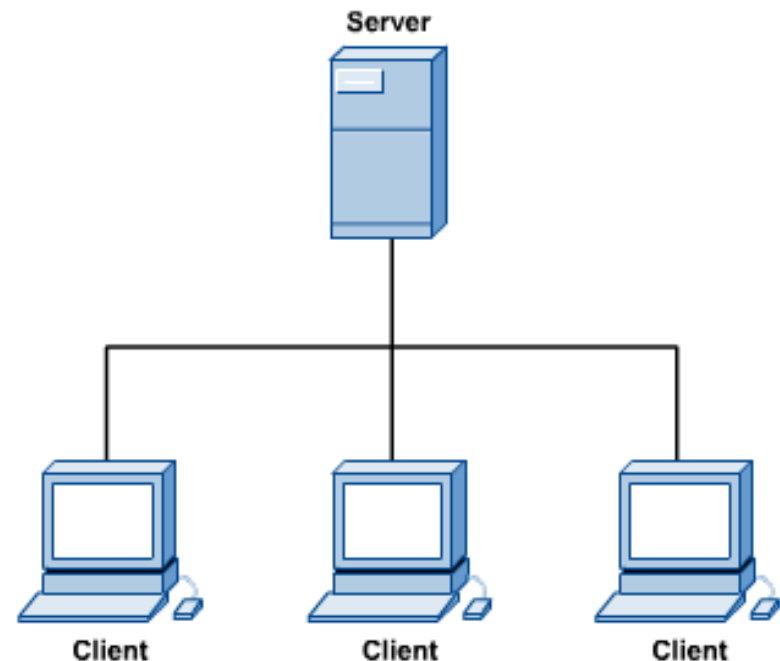
■ HUB, Switches, Routers, Wireless Access Points, Modems etc.



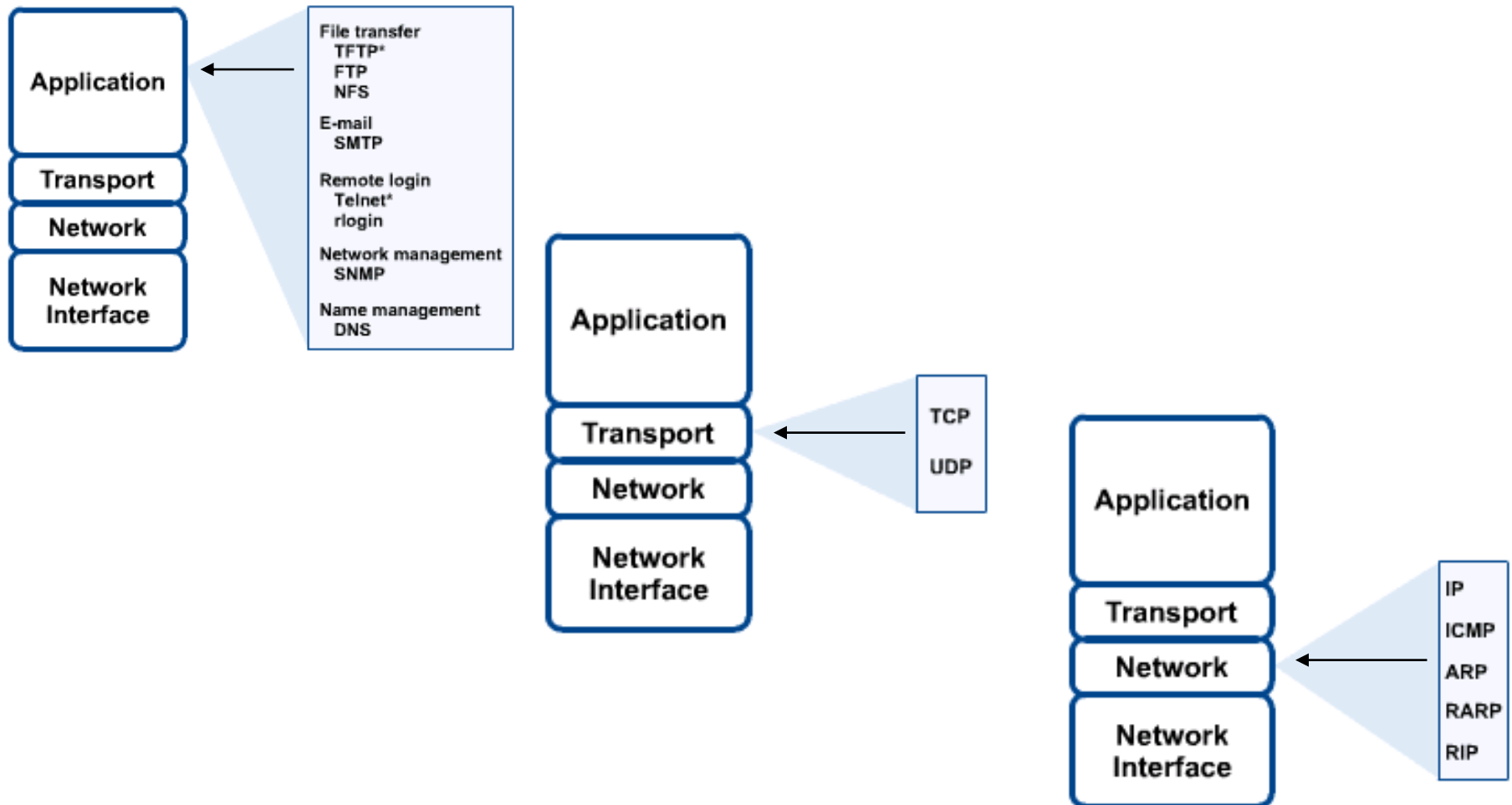
Computers: Clients and Servers

 In a client/server network arrangement, network services are located in a dedicated computer whose only function is to respond to the requests of clients.

 The server contains the file, print, application, security, and other services in a central computer that is continuously available to respond to client requests.



Networking Protocol: TCP/IP



Applications

- E-mail
- Searchable Data (Web Sites)
- E-Commerce
- News Groups
- Internet Telephony (VoIP)
- Video Conferencing
- Chat Groups
- Instant Messengers
- Internet Radio



Protocol Hierarchies

- ❏ To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- ❏ The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- ❏ The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
- ❏ Layer n on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the ***layer n protocol***.
- ❏ Basically, “***Protocol*** is an agreement between the communicating parties on how communication is to proceed”.

Protocol Hierarchies

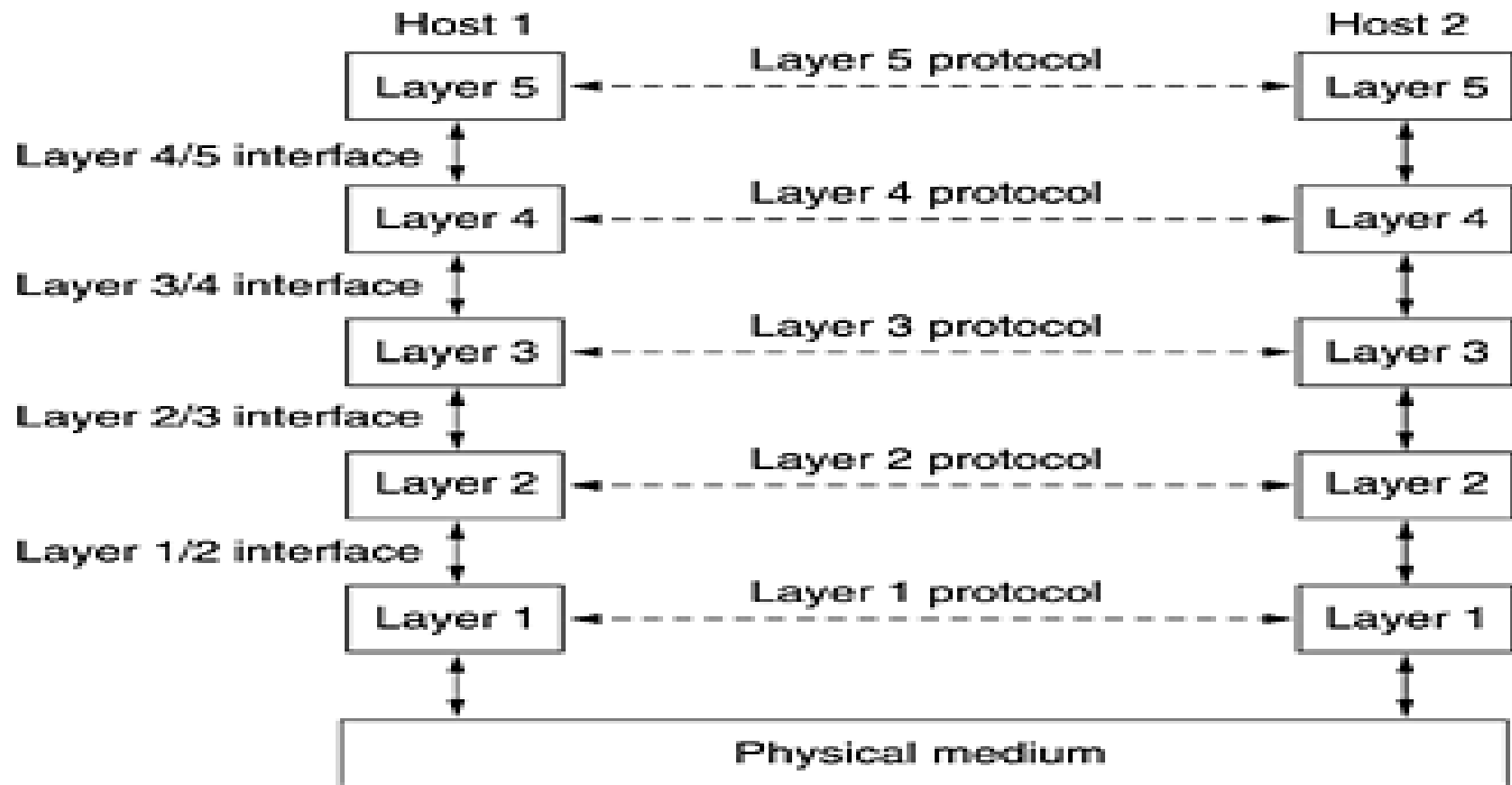





Figure. Layers, protocols, and interfaces.





Protocol Hierarchies

- ❏ In reality, no data are directly transferred from layer n on one machine to layer n on another machine.
- ❏ Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs.
- ❏ virtual communication is shown by dotted lines and physical communication by solid lines.
- ❏ **Interface defines-> Primitive operations and services - Lower to upper**
- ❏ **Layer + protocol -> Network architecture**
- ❏ **List of protocols used by system 1 Protocol/ Layer -> Protocol Stack**

Design Issues for the layers







-  **Data Transfer Rules-** The protocol used must determine the number of channels needed and the priorities to be used. This is based on the mode of communication (simplex, half-duplex and full-duplex)
-  **The protocol** that the layers use must be able to correct the sequence of the packets received if they are not in correct order.
-  Another major issue is the **maximum size of data** that can be sent and received at one go. This leads to the need for segmentation at the sending end and re assembly at the receiving end. The problem is that if the sending packets are too small in size, then the process becomes inefficient.

Design Issues for the layers

-  The sender and receiver identification must be made possible for each layers. This can be achieved by some form of **addressing**.
-  A common form of **error control and error correction** on both the sending and receiving ends.
-  Rate of sending and rate of receiving must match. If the rate of sending is too high that the receiver cant cope up, it leads to congestion and packet loss. **Flow control** can be used in these cases.
-  Choosing the best possible route between the sender and the receiver when more than one path is available for data traversal. This is called **Routing**.








Connection Oriented and Connectionless Services

Connection Oriented Services

-  It is reliable because never lose data .
-  To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection. In most cases the order is preserved so that the bits arrive in the order they were sent.
-  In some cases when a connection is established, the sender, receiver, and subnet conduct a negotiation about parameters to be used, such as maximum message size, quality of service required, and other issues.
-  Typically, one side makes a proposal and the other side can accept it, reject it, or make a counterproposal.
-  Guaranteed of Service by providing acknowledgment.
-  have higher overhead and place greater demands on bandwidth.

Connection Oriented and Connectionless Services

Connectionless Services

-  Non reliable because packets may loss.
-  No Guarantee of Service
-  In contrast, connectionless service is modeled after the postal system.
-  Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others.
-  Normally, when two messages are sent to the same destination, the first one sent will be the first one to arrive.
-  However, it is possible that the first one sent can be delayed so that the second one arrives first.
-  less overhead than connection-oriented communication.

Connection Oriented and Connectionless Services

Connection-oriented		Service	Example
		Reliable message stream	Sequence of pages
		Reliable byte stream	Remote login
Connection-less		Unreliable connection	Digitized voice
		Unreliable datagram	Electronic junk mail
		Acknowledged datagram	Registered mail
		Request-reply	Database query

Figure. Six different types of service.

Service Primitives

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Figure : Five service primitives for implementing a simple connection-oriented service.

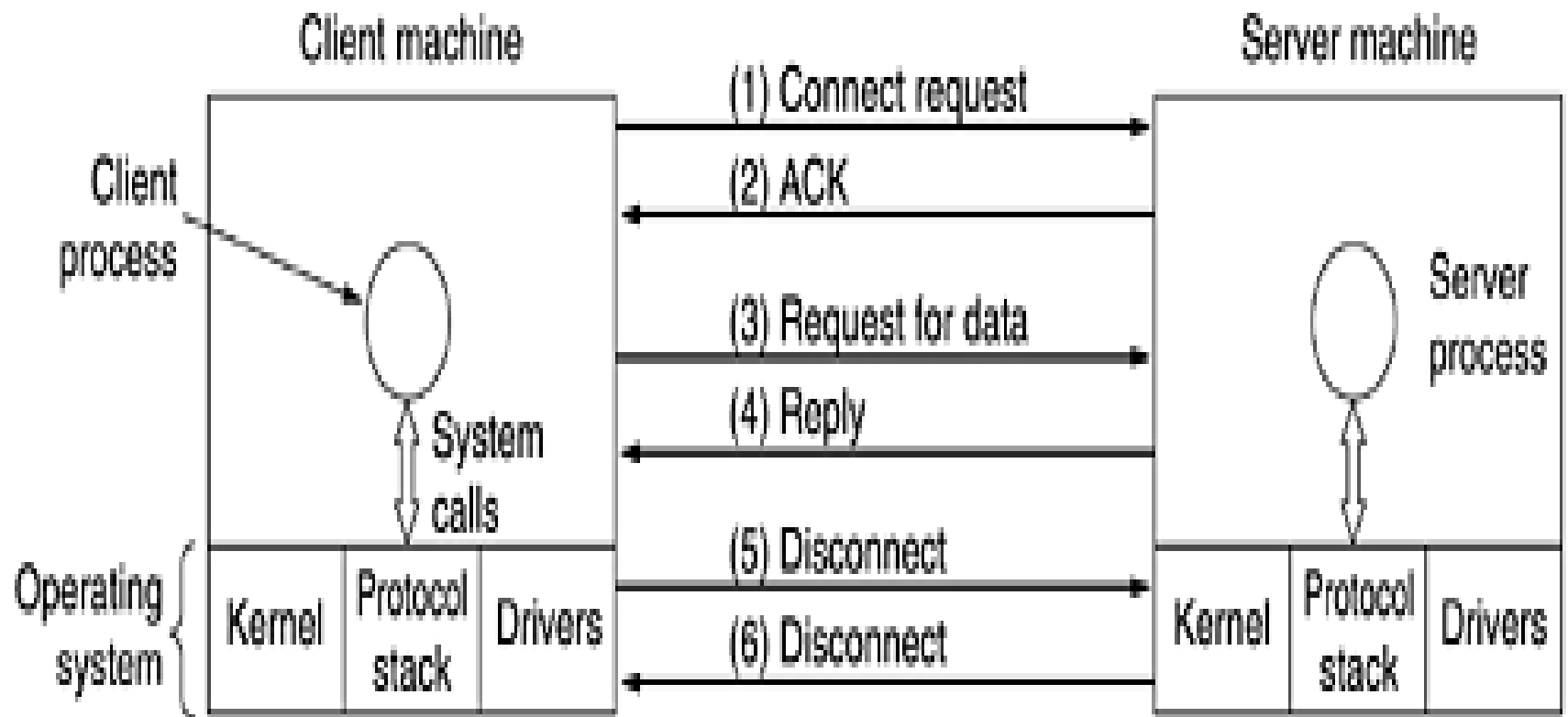


Figure . Packets sent in a simple client-server interaction on a connection-oriented network.

Hardware, Software and Networks Peripherals (device)



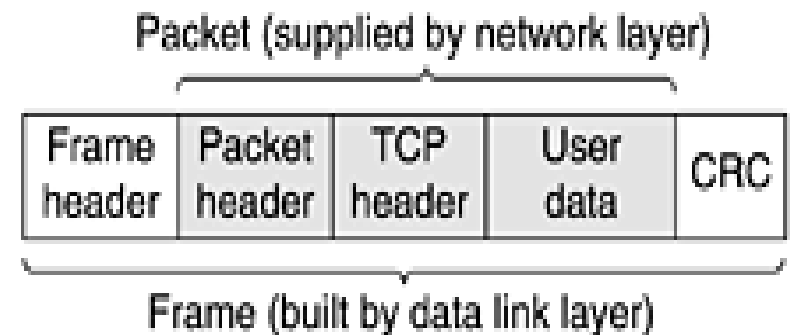
- Network Interface Card (NIC)
- Repeater
- Hub
- Bridge
- Routers
- Switch

Hardware, Software and Networks Peripherals (device)



Application layer	Application gateway
Transport layer	Transport gateway
Network layer	Router
Data link layer	Bridge, switch
Physical layer	Repeater, hub

(a)



(b)

Fig : (a) Which device is in which layer. (b) Frames, packets, and headers.

Hardware, Software and Networks Peripherals (cont.)

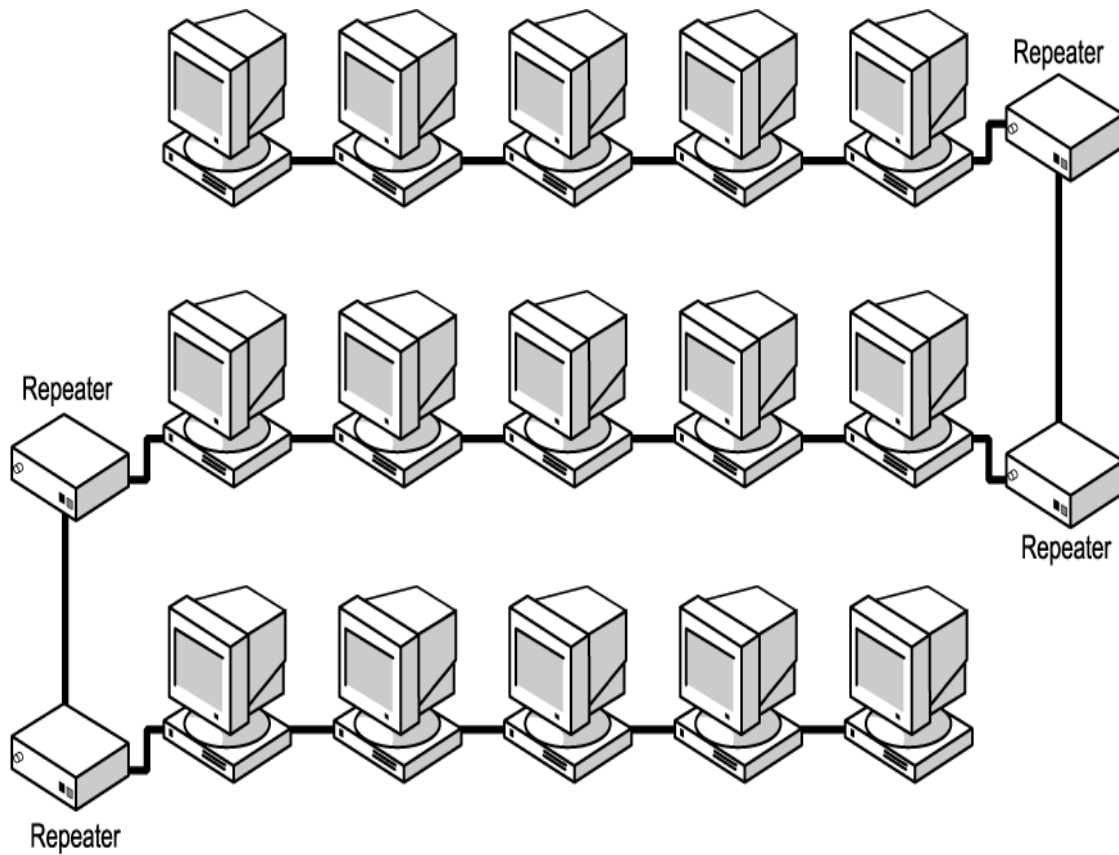
Network Interface Card (NIC)

- NIC provides the physical interface between computer and cabling.
- It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.
- The following factors should be taken into consideration when choosing a NIC:
 1. - Preparing data
 2. - Sending and controlling data
 3. - Configuration
 4. - Drivers
 5. - Compatibility
 6. - Performance

Repeaters

- Repeaters are very simple devices. They allow a cabling system to extend beyond its maximum allowed length by amplifying the network voltages so they travel farther.
- Repeaters are nothing more than amplifiers and, as such, are very inexpensive.
- Repeaters can only be used to regenerate signals between similar network segments.
- For example, we can extend an Ethernet 10Base2 network to 400 meters with a repeater. But can't connect an Ethernet and Token Ring network together with one.
- The main disadvantage to repeaters is that they just amplify signals. These signals not only include the network signals, but any noise on the wire as well.
- Eventually, if you use enough repeaters, you could possibly drown out the signal with the amplified noise. For this reason, repeaters are used only as a temporary fix.

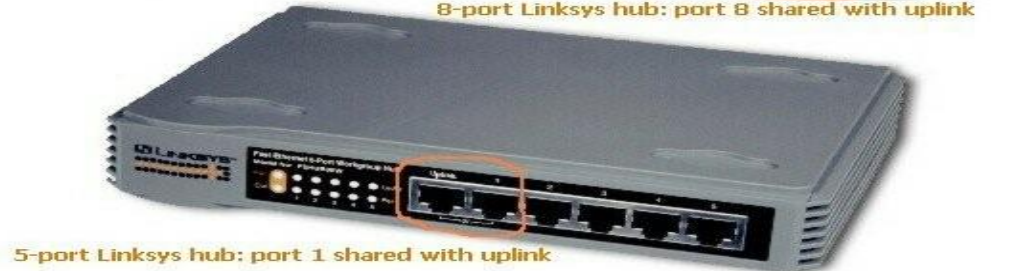
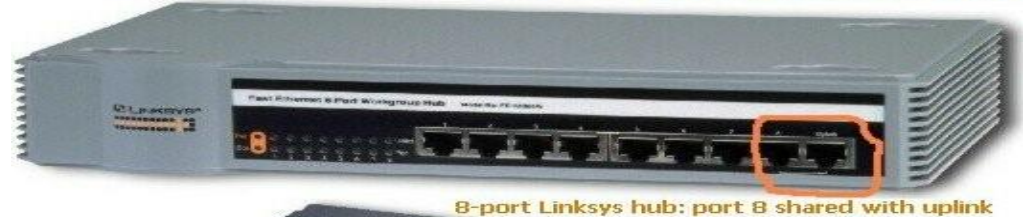
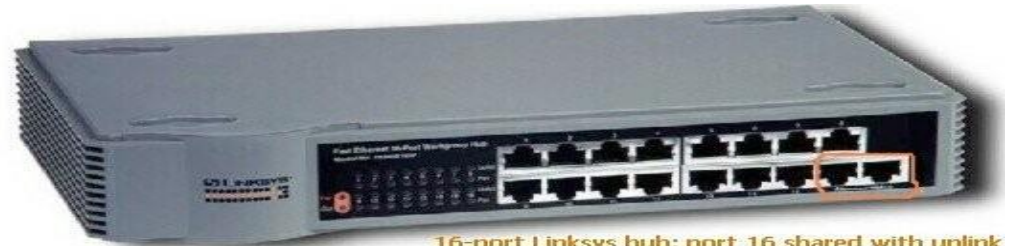
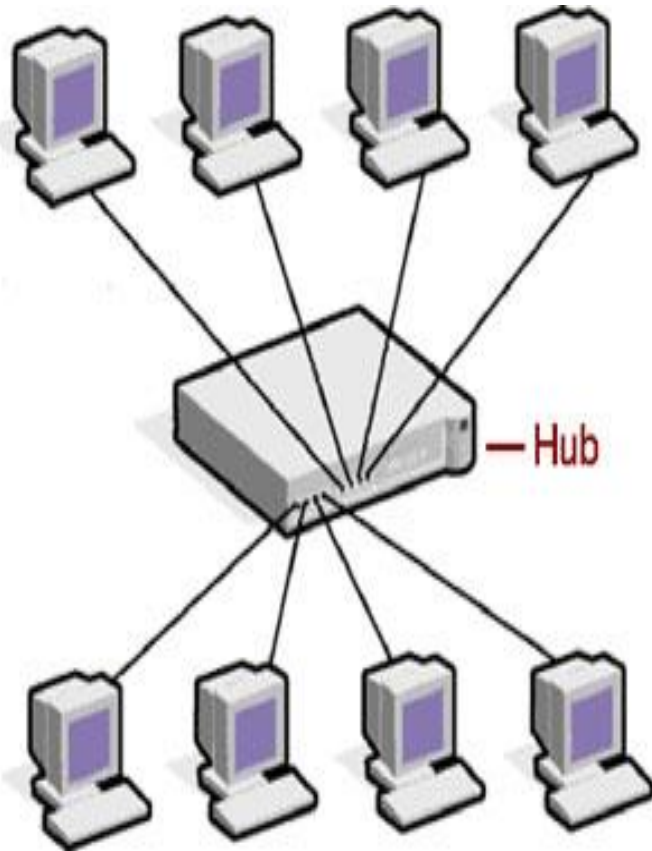
Repeaters



Hubs

- Hubs are devices used to link several computers together.
- They repeat any signal that comes in on one port and copy it to the other ports (a process that is also called *broadcasting*).
- There are two types of hubs: active and passive.
- *Passive hubs* simply connect all ports together electrically and are usually not powered.
- *Active hubs* use electronics to amplify and clean up the signal before it is broadcast to the other ports.
- In the category of active hubs, there is also a class called “intelligent” hubs, which are hubs that can be remotely managed on the network.

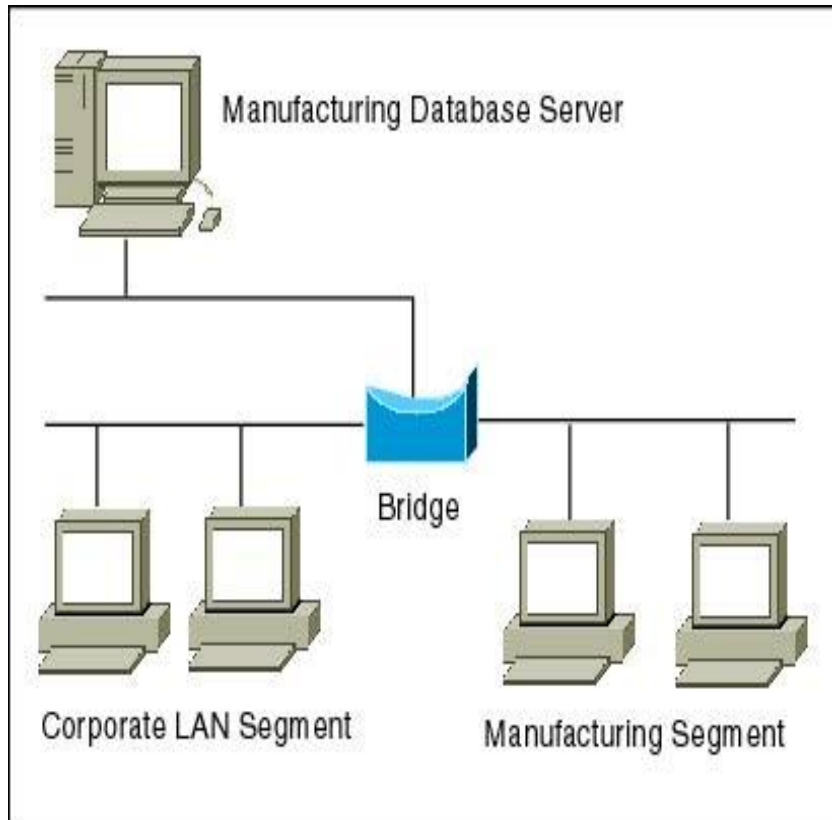
Hubs



Bridges

- They join similar topologies and are used to divide network segments.
- For example, with 200 people on one Ethernet segment, the performance will be ordinary, because of the design of Ethernet and the number of workstations that are fighting to transmit. If you divide the segment into two segments of 100 workstations each, the traffic will be much lower on either side and performance will increase.
- If it is aware of the destination address, it is able to forward packets; otherwise a bridge will forward the packets to all segments. They are more intelligent than repeaters but are unable to move data across multiple networks simultaneously.
- Unlike repeaters, bridges *can* filter out noise.
- The main disadvantage to bridges is that they can't connect dissimilar network types or perform intelligent path selection. For that function, you would need a router.

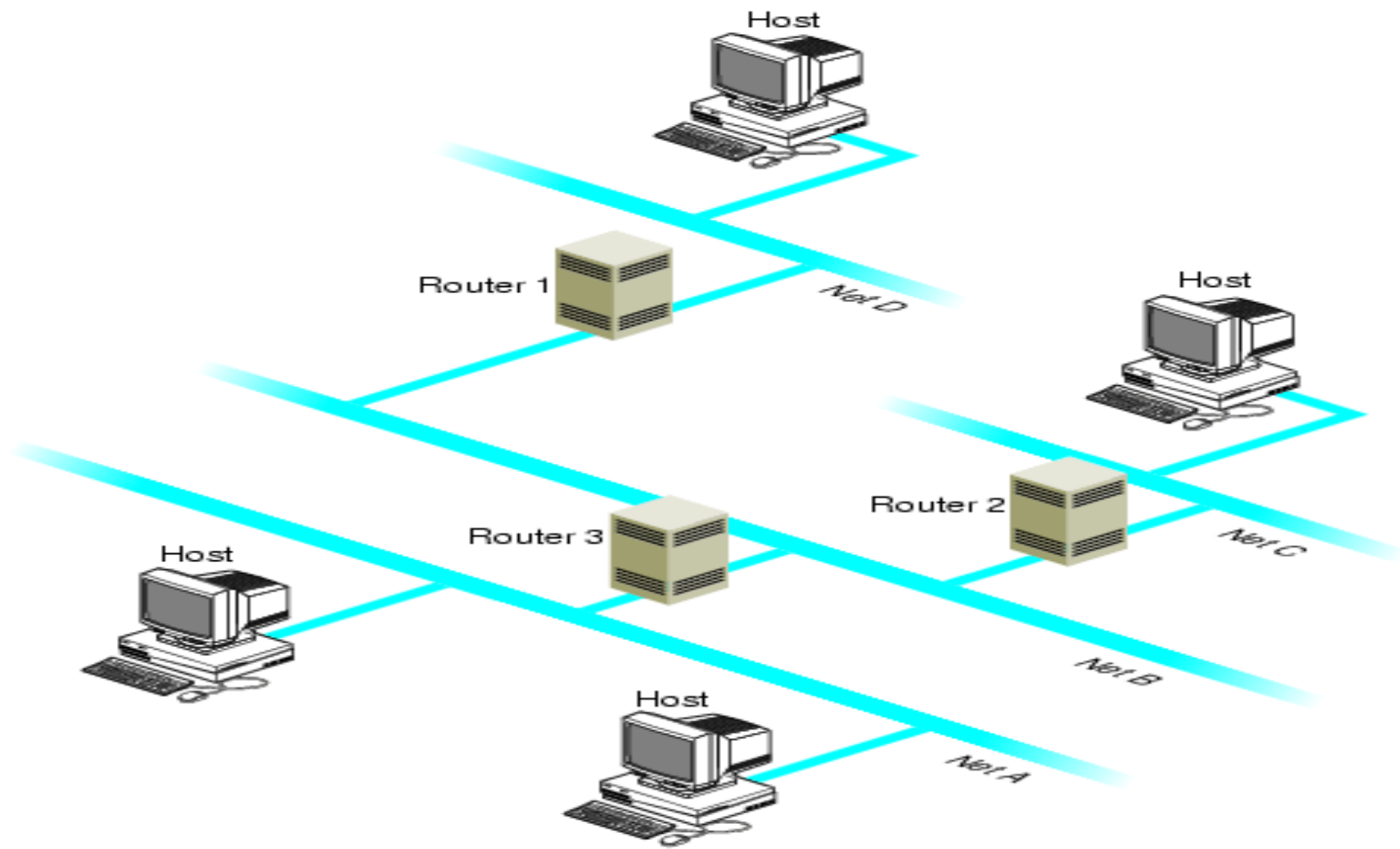
Bridges



Routers

- Routers are highly intelligent devices that connect multiple network types and determine the best path for sending data.
- The advantage of using a router over a bridge is that routers can determine the best path that data can take to get to its destination.
- Like bridges, they can segment large networks and can filter out noise.
- However, they are slower than bridges because they are more intelligent devices; as such, they analyze every packet, causing packet-forwarding delays. Because of this intelligence, they are also more expensive.
- Routers are normally used to connect one LAN to another.
- Typically, when a WAN is set up, there will be at least two routers used.

Routers



Switch

- A **network switch** is a computer networking device that connects network segments.
- Low-end network switches appear nearly identical to network hubs, but a switch contains more "intelligence" (and a slightly higher price tag) than a network hub.
- Network switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately.
- By delivering each message only to the connected device it was intended for, a network switch conserves network bandwidth and offers generally better performance than a hub.
- A **vital difference** between a **hub** and a **switch** is that all the nodes connected to a hub share the bandwidth among themselves, while a device connected to a switch port has the **full bandwidth** all to itself.
- For example, if 10 nodes are communicating using a hub on a 10-Mbps network, then each node may only get a portion of the 10 Mbps if other nodes on the hub want to communicate as well. .
- But with a switch, each node could possibly communicate at the full 10 Mbps.

Switch

