

Network Concepts and Communications



Introduction



- Communication is the desire of man. When human voice became inadequate, ancient civilizations devised drum codes and smoke signals to send information to far off distances.
- These primitive methods have given way to sending messages through electronic pulses. A stand alone computer communicates very efficiently by connecting it with other computers. Data in a computer is transmitted to another computer located across continents almost instantaneously using telephone, microwaves or radio links.
- The long distance communication link between a computer and a remote terminal was set up around 1965. Now networking has become a very important part of computing activity.

Network



- A large number of computers are interconnected by copper wire, fiber optic cable, microwave and infrared or through satellite.
- A system consisting of connected nodes made to share data, hardware and software is called a Computer Network.

Introduction: “Everything is Connected to Everything”



- Going online: Connecting to a collection of interconnected computers on a network.
 - Do banking.
 - Pay bills.
 - Buy groceries.
 - Book vacation travel.
 - Send messages.
 - Participate in discussions.
 - Do research.
 - Play games.
- **Network:** A collection of computers, display terminals, printers, and other devices linked either by physical or wireless means.

Introduction: “Everything is Connected to Everything”



■ Seeds of Networking

- 1966: ARPA (Advanced Research Projects Agency) State Defense Department’s research organization.
 - Focused major development effort on computer networking.
 - ARPA’s Goal: To promote research in advanced future technologies by funding university and industry research proposals.
 - Result: Thousands of databases became available to the public.

Introduction: “Everything is Connected to Everything”



■ Computer Networking

- **Internet:** A world wide network connecting millions of computer networks for the purpose of exchanging data and communications using special rules of communication.
- **internet:** (lower case i) The convention was generally to capitalize "Internet," because it is a proper noun. The word has become common and some may no longer treat it as a proper noun, and thus not capitalize it. Conventions vary. Originally, "internet" was more commonly used as a general term for interconnected networks of networks.

Introduction: “Everything is Connected to Everything”



■ Computer Networking

- The human need to communicate has motivated mankind’s creativity:
 - Cave dwellers drew pictures on walls.
 - Smoke signals, drum rhythms passed messages.
 - American pioneers: Pony express, Wells Fargo.
 - Alexander Graham Bell: invented the telephone.

Some Important Reasons for Networking



- **Sharing of resources:** Primary goal of a computer network is to share resources. For example several PCs can be connected to a single expensive line printer.
- **Sharing information:** Information on a single computer can be accessed by other computers in the network. Duplication of data file on separate PCs can be avoided.
- **Communication:** When several PCs are connected to each other, messages can be sent and received. From a remote location, a mobile salesman can relay important messages to the central office regarding orders. Relevant databases are updated and the business commitments are fulfilled.

Benefits of Network



- Effective handling of personal communications
- Allowing several users to access simultaneously Important programs and data:
- Making it easy for the users to keep all critical data on shared storage shdevice and safeguard the data.
- Allowing people to are costly equipment

The computer communication



The computer communication should ensure safe, secure and reliable data transfer.

Safe : The data received is the same as the data sent

Secure : The data being transferred cannot be damaged either will fully or accidentally.

Reliable: Both the sender and the receiver knows the status of the data sent. Thus the sender knows whether the receiver got the correct data or not.

Networks Terminology



- **Network :** A network is a collection of computers and other devices that can send data to and receive data from each other. A network is often connected by wires. However, wireless networks transmit data through infrared light and microwaves.
- **Node :** Each machine on a network is called a node. Most nodes are computers, but printers, routers, bridges, gateways, dumb terminals, and Coca Cola™ machines can also be nodes. Nodes that are fully functional computers are also called hosts.
- **Address:** Every network node has an address, a series of bytes that uniquely identify it. The more bytes there are in each address, the more addresses there are available and the more devices that can be connected to the network simultaneously.

Networks Terminology



- **Packet :** All modern computer networks are packet switched networks: data traveling on the network is broken into chunks called packets and each packet is handled separately. Each packet contains information about who sent it and where it's going.
- **Protocol :** A protocol is a precise set of rules defining how computers communicate: the format of addresses, how data is split into packets, and so on. There are many different protocols defining different aspects of network communication.

Communication Basics of Networks

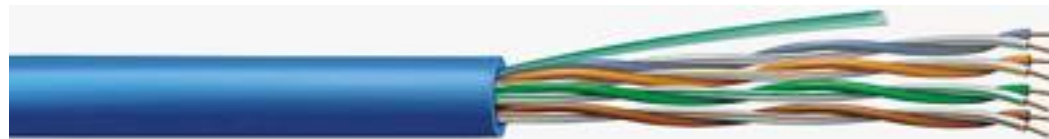


- Types of connections of computers into networks:
Physical versus Wireless connections
 - The first type: The Physical Connection.
 - Physically connect computers together.
 - Use of wires or optical cables.
 - The connections are called network links.
 - Three most common physical links:
 - Twisted pair
 - Coaxial cable
 - Fiber optic cable

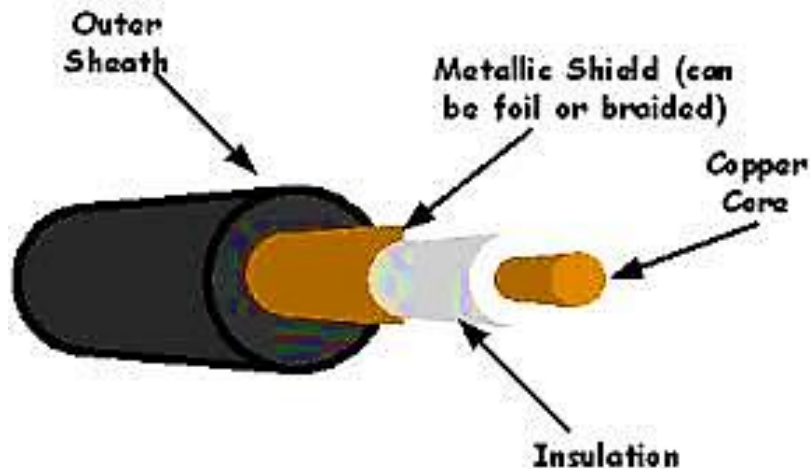
Communication Basics of Networks



- **Twisted pair**
 - Two wires twisted together.
 - Makes them less susceptible to acting like an antenna and picking up radio frequency information or appliance noise.
 - Telephone company uses twisted pair copper wires to link telephones.



Coaxial cable



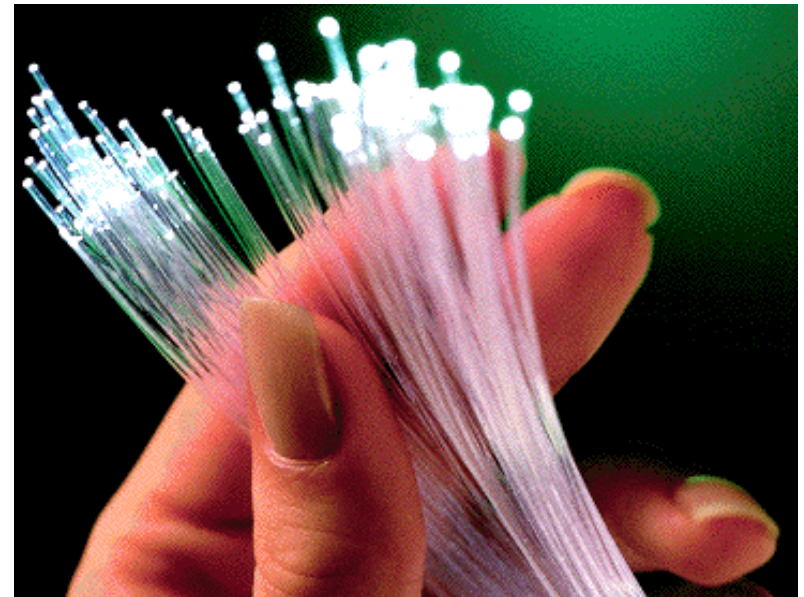
- Also two wires:
 - One of the wires is woven of fine strands of copper forming a tube.
 - The wire mesh surrounds a solid copper wire that runs down the center.
 - Space between has a non conducting material.
 - Makes them more impervious to outside noise.

Communication Basics of Networks



■ Fiber optic cable

- Light is electromagnetic.
- Can transmit more information down a single strand.
 - It can send a wider set of frequencies.
- Each cable can send several thousand phone conversations or computer communications.



Communication Basics of Networks



- Second type of connections of computers into networks: Wireless connections
 - The link is made using electromagnetic energy that goes through space instead of along wires or cables.
 - Three types of wireless communications commonly used in networking:
 - Infrared
 - Radio frequency
 - Microwave

Communication Basics of Networks



■ Infrared

- Commonly used in TV and VCR remote controls.
- Use infrared frequencies of electromagnetic radiation that behave much like visible light.
- Must be in the line of sight.
- Often used to connect keyboards, mice, and printers.



Communication Basics of Networks



■ Radio frequency

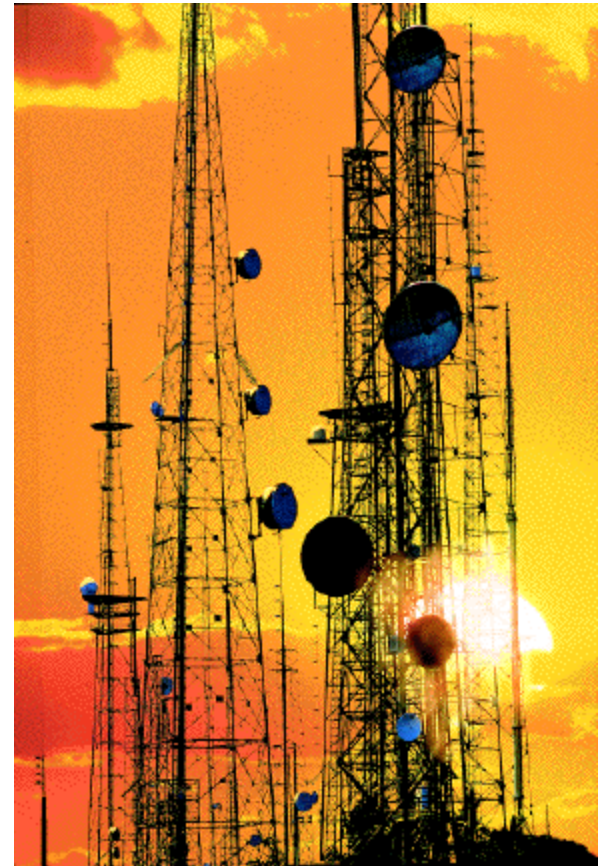
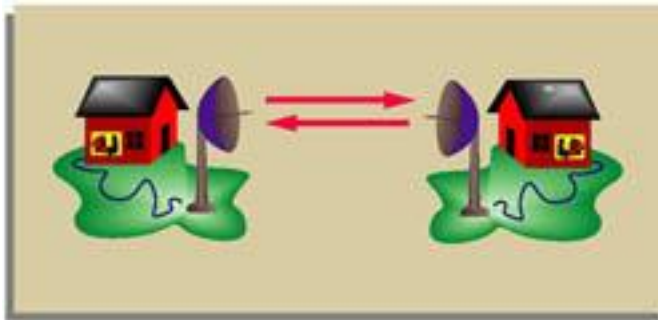
- Uses radio frequencies.
 - Function even though line of sight is interrupted.
- Not commonly used because of the possible interference from other sources of electromagnetic radiation such as old electric drills and furnace motors.

Communication Basics of Networks



■ Microwave

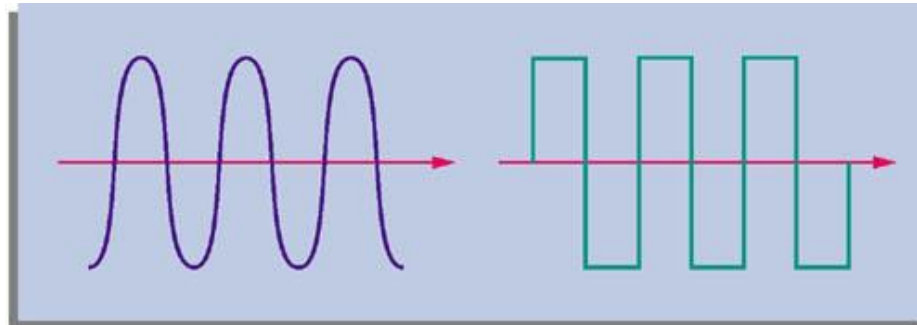
- Often used to communicate with distant locations.
- Must be line of sight.
- Satellite communications



1. Type of signal communicated (analog or digital).



- **Analog:** Those signals that vary with smooth continuous changes.
 - A continuously changing signal similar to that found on the speaker wires of a high fidelity stereo system.
- **Digital:** Those signals that vary in steps or jumps from value to value. They are usually in the form of pulses of electrical energy (represent 0s or 1s).



2. The speed at which the signal is transmitted (how fast the data travels).



- In digital systems: Speed is measured in...
 - **Bits per second** (bps).
 - The number of bits (0's and 1's) that travel down the channel per second.
 - **Baud rate**
 - The number of bits that travel down the channel in a given interval.
 - The number is given in signal changes per second, not necessarily bits per second.

Communication Basics of Networks



■ **MODEM** MOdulator DEModulator

- **Outgoing:** Converts binary data from computer (digital) into telephone compatible signals (analog).
- **Incoming:** Converts telephone signal (analog) into binary data for the computer (digital).
- Can be an external or internal device (usually a “Network Interface card”).



Communication Basics of Networks



- How is it possible to measure the capacity of communications links?
 - **Bandwidth:** Digital
 - Number of bits per second (bps) that can be sent over a link.
 - The wider the bandwidth, the more diverse kinds of information can be sent.
 - Simplest is voice, most sophisticated is moving videos.
 - **Bandwidth:** Analog
 - The difference between the highest and lowest frequencies that can be sent over an analog link (like phone lines).
 - Measurement is given in hertz (Hz).
 - For both: The wider the bandwidth, the more information can flow over the channel.

The Physical Organization of Networks



- Two parts to connect computers to networks
 - The hardware needed to connect the computer to the network.
 - The software needed to control the hardware.
 - (Software standards will be discussed in the next section.)

Types of Networks



- Categorizing networks according to size:
 - **LAN** (Local Area Network)
 - **MAN** (Metropolitan Area Network)
 - **WAN** (Wide Area Network)
 - **PAN** (Personal Area Network)

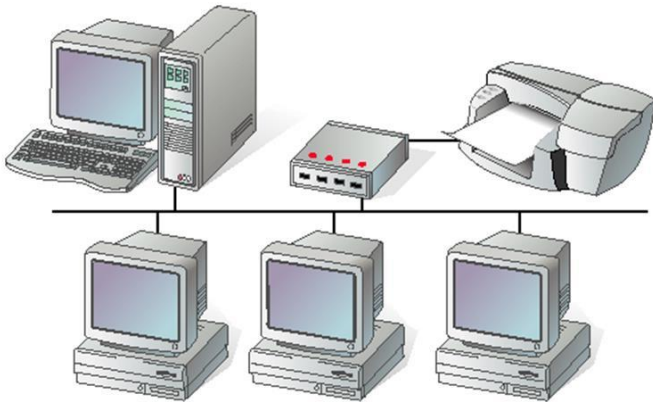
LAN (Local Area Network)



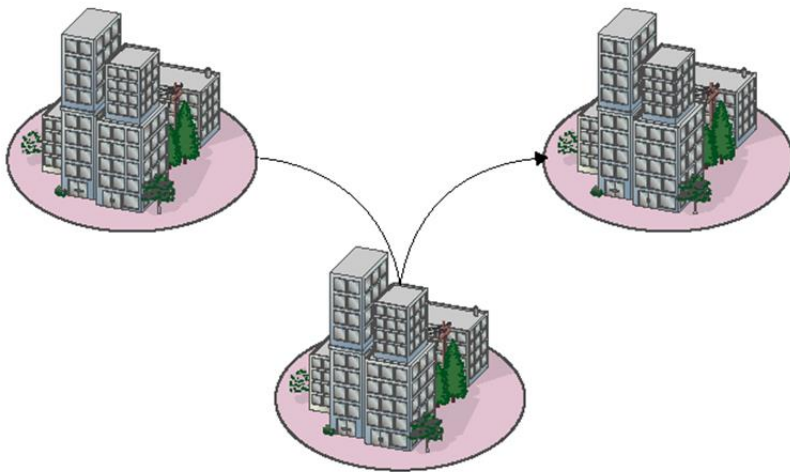
- A collection of nodes within a small area.
- The nodes are linked in a bus, ring, star, tree, or fully connected topology network configuration.

- Benefits of LANs:

- Sharing of hardware resources.
- Sharing of software and data.
- Consolidated wiring/cabling.
- Simultaneous distribution of information.
- More efficient person to person communication.



MAN (Metropolitan Area Network)

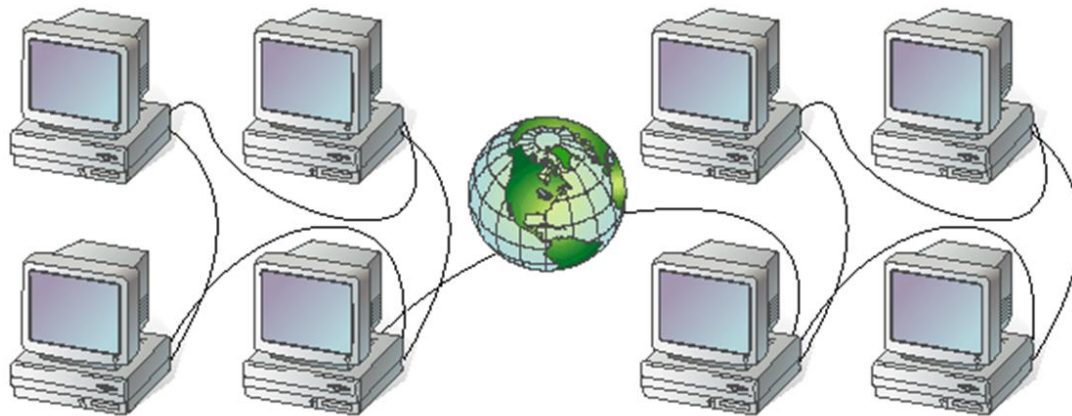


- A MAN spans the distance of a typical metropolitan city / Consists of many local area networks linked together.
- The cost of installation and operation is higher.
- MANs use high speed connections such as fiber optics to achieve higher speeds.

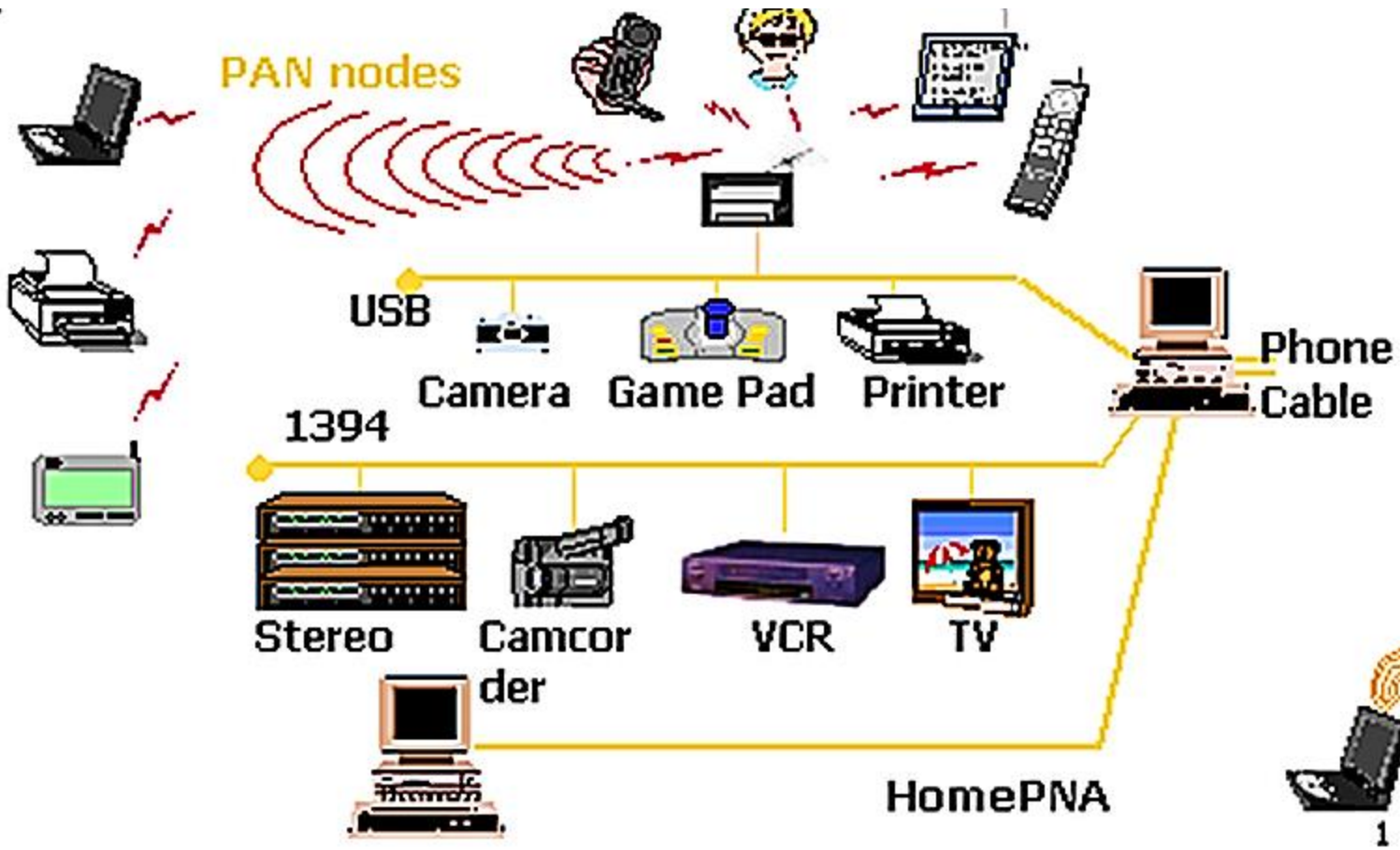
WAN (Wide Area Network)



- Consists of a number of computer networks including LANs. / WANs span a larger area than a single city.
- Connected by many types of links.
- These use long distance telecommunication networks for connection, thereby increasing the cost.
- The Internet is a good example of a WAN.



PAN(Personal Area Network)



Network topologies

Topology



- Topology refers to the **layout** of connected devices on a network.
- Here, some logical layout of topology.
 - Mesh
 - Star
 - Bus
 - Ring

Mesh Topology



- Here every device has a **point to point** link to every other device.
- Node 1 node must be connected with **$n - 1$** nodes.
- A fully connected mesh can have **$n(n - 1)/2$** physical channels to link **n** devices.
- It must have **$n - 1$** I/O ports.

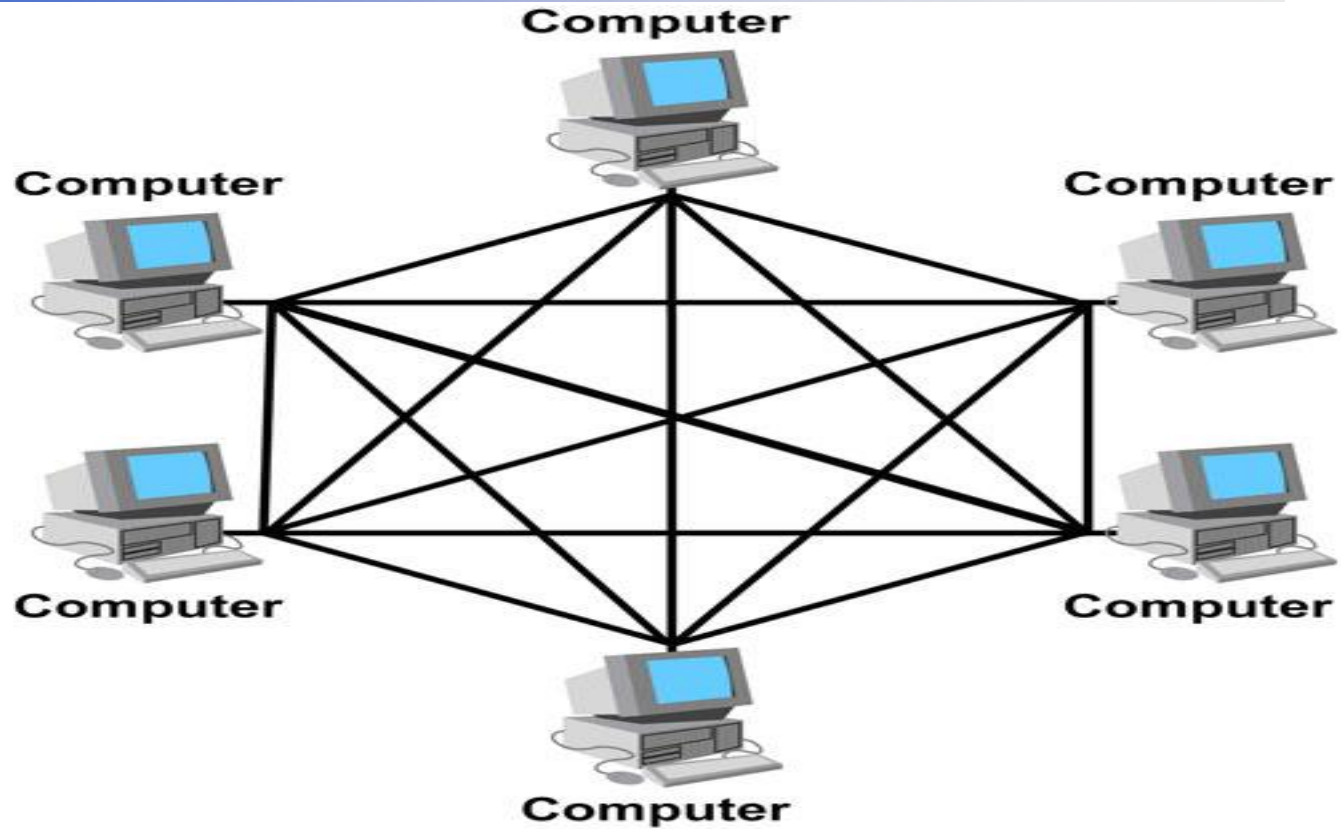
Mesh Topology



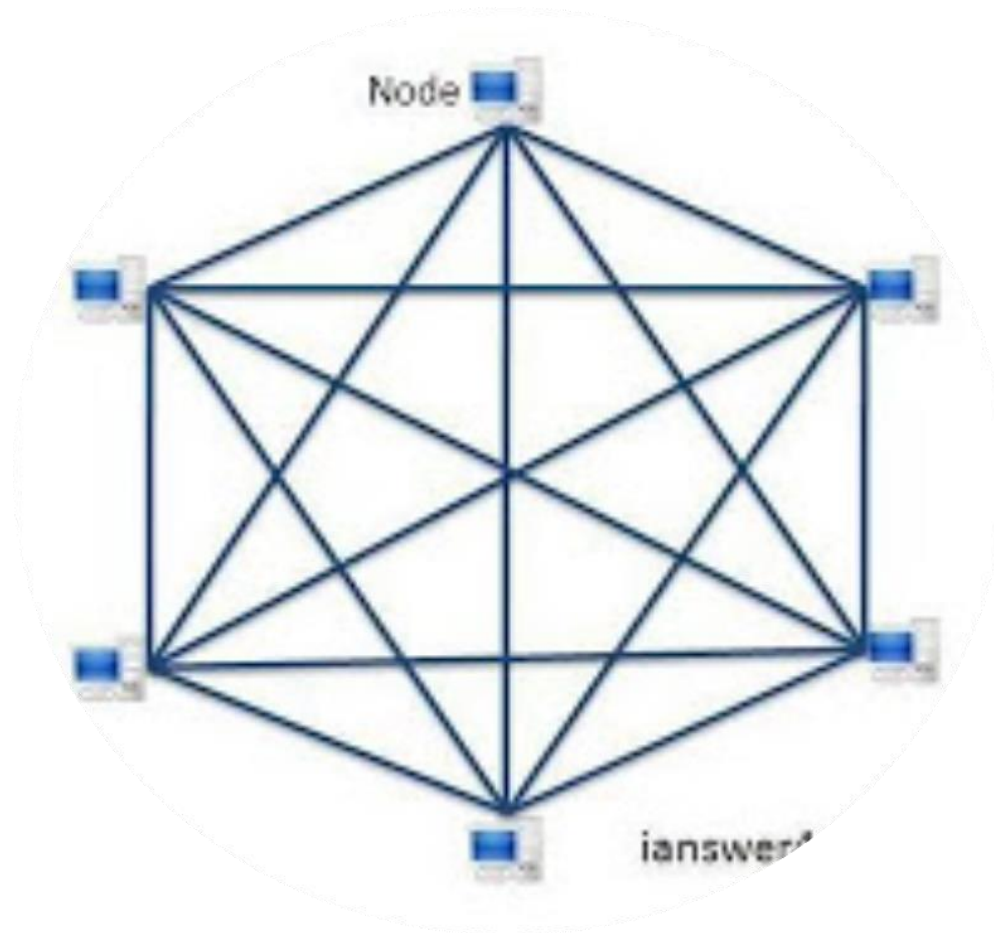
Advantages:

- 1.They use dedicated links so each link can only carry its own data load. So **traffic problem** can be avoided.
- 2.It is robust. If **any one link get damaged** it cannot affect others.
- 3.It gives privacy and security.(Message travels along a dedicated link)
- 4.Fault identification and fault isolation are easy.

Mesh Topology



Mesh Topology



Mesh Topology



- Disadvantages:
 1. The amount of **cabling** and the number of **I/O ports** required are very large. Since every device is connected to each devices through dedicated links.
 2. The sheer bulk of wiring is larger then the available space.
 3. Hardware required to connected each device is highly expensive.

Mesh Topology



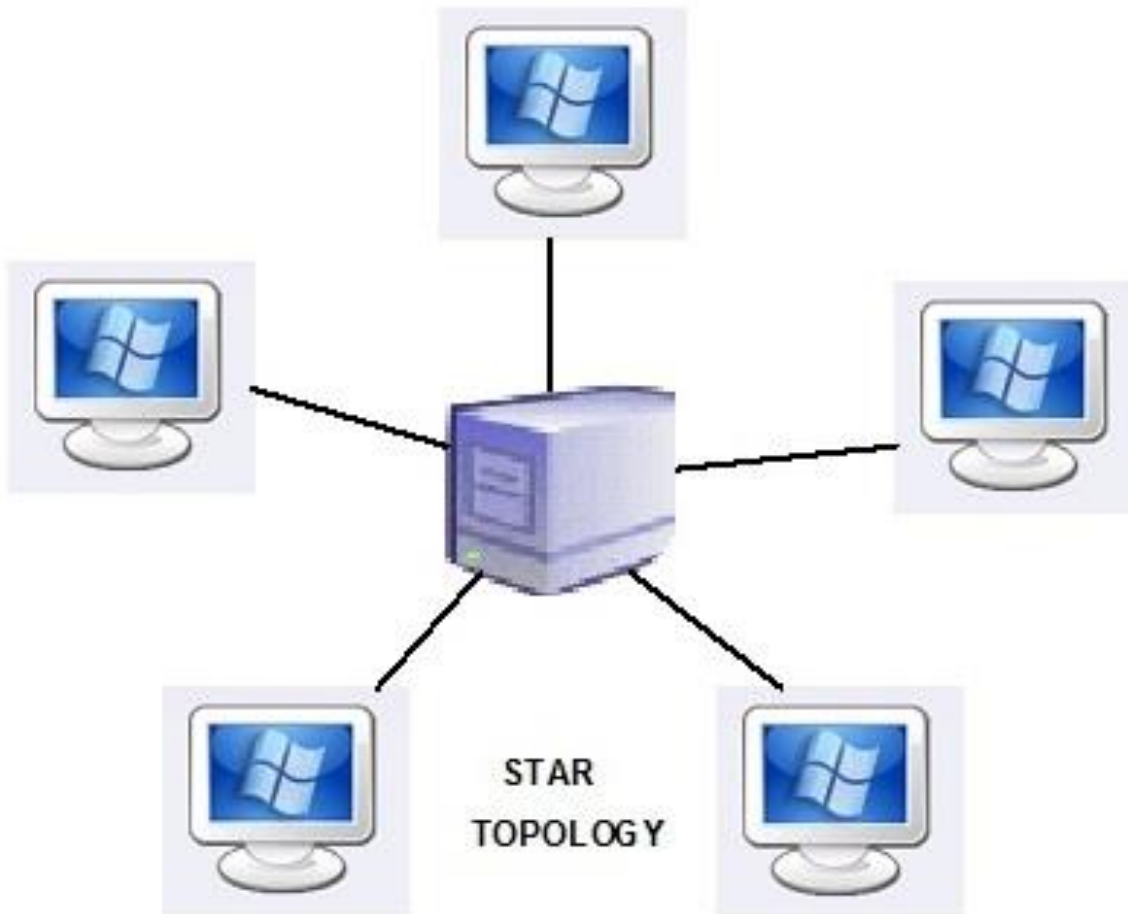
- Applications:
 1. Telephone Regional office.
 2. WAN.(Wide Area Network).

Star Topology

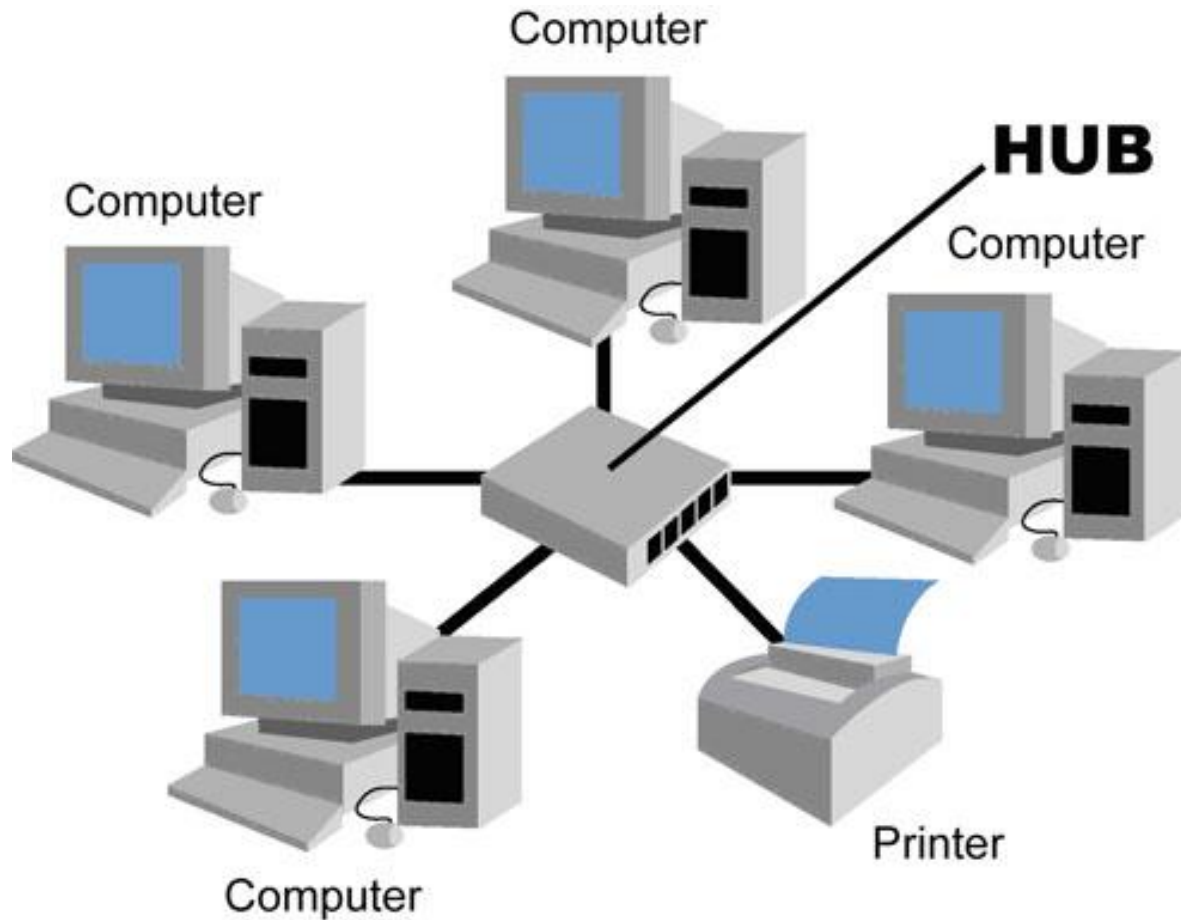


- Here each device has a dedicated point to point link to the central controller called “Hub”(Act as a Exchange).
- There is no direct traffic between devices.
- The transmission are occurred only through the central “hub”.
- When device 1 wants to send data to device 2; First sends the data to hub. Which then relays the data to the other connected device.

STAR TOPOLOGY:



Star Topology



Star Topology



■ Advantages:

1. Less expensive than mesh since each device is connected only to the hub.
2. Installation and configuration are easy.
3. Less cabling is needed than mesh.
4. Robustness. (if one link fails, only that link is affected. All other links remain active)
5. Easy to fault identification & to remove parts.
6. No disruptions to the network when connecting (or) removing devices.

Star Topology



■ Disadvantages:

1. Even it requires less cabling than mesh when compared with other topologies it still large. (Ring or bus).
2. Dependency (whole n/w dependent on one single point (hub)). When it goes down. The whole system is dead.

Applications



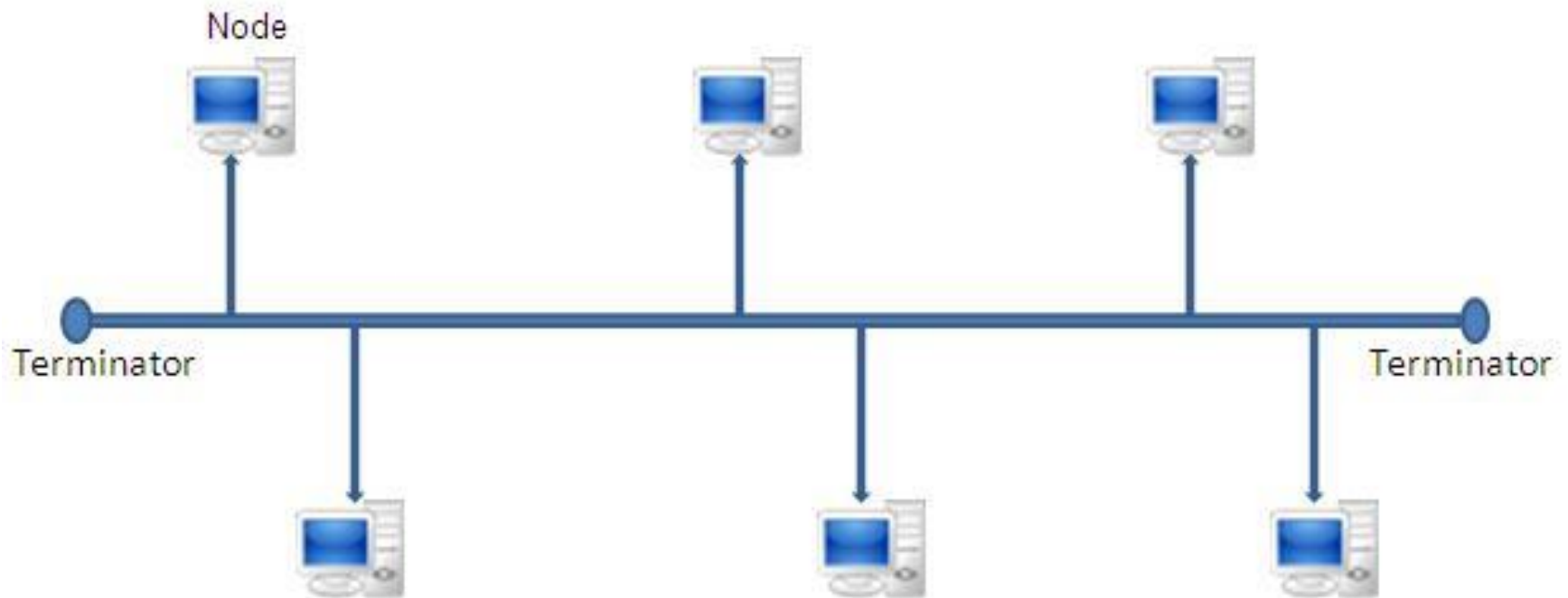
- Star topology used in Local Area Networks(LANs).
- High speed LAN often used STAR.

Bus Topology

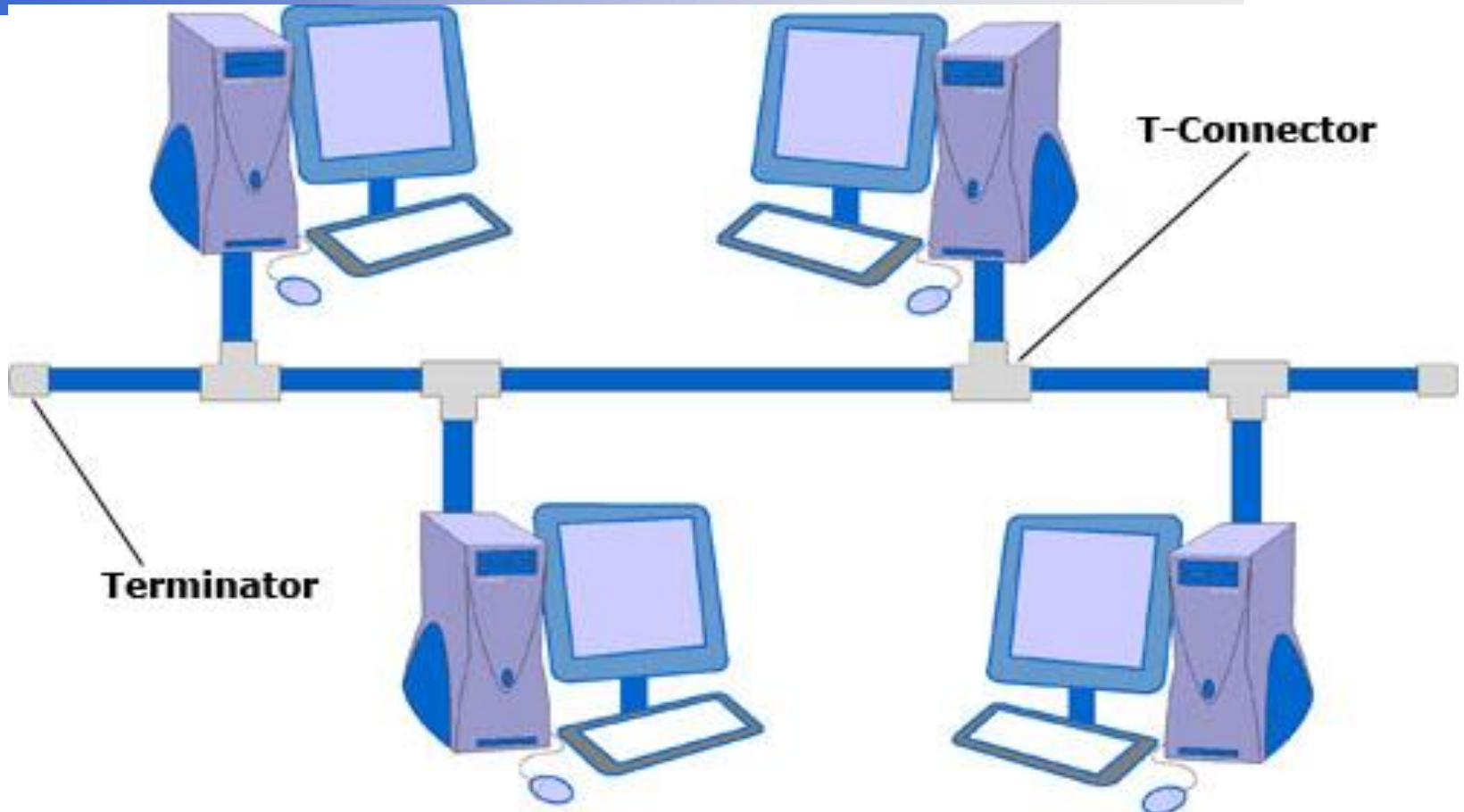


- A bus topology is multipoint.
- Here one long cable act as a backbone to link all the devices are connected to the backbone by drop lines and taps.
- **Drop line** is the connection b/w the devices and the cable.
- **Tap** is the splitter that cut the main link.
- This allows **only one device to transmit at a time.**

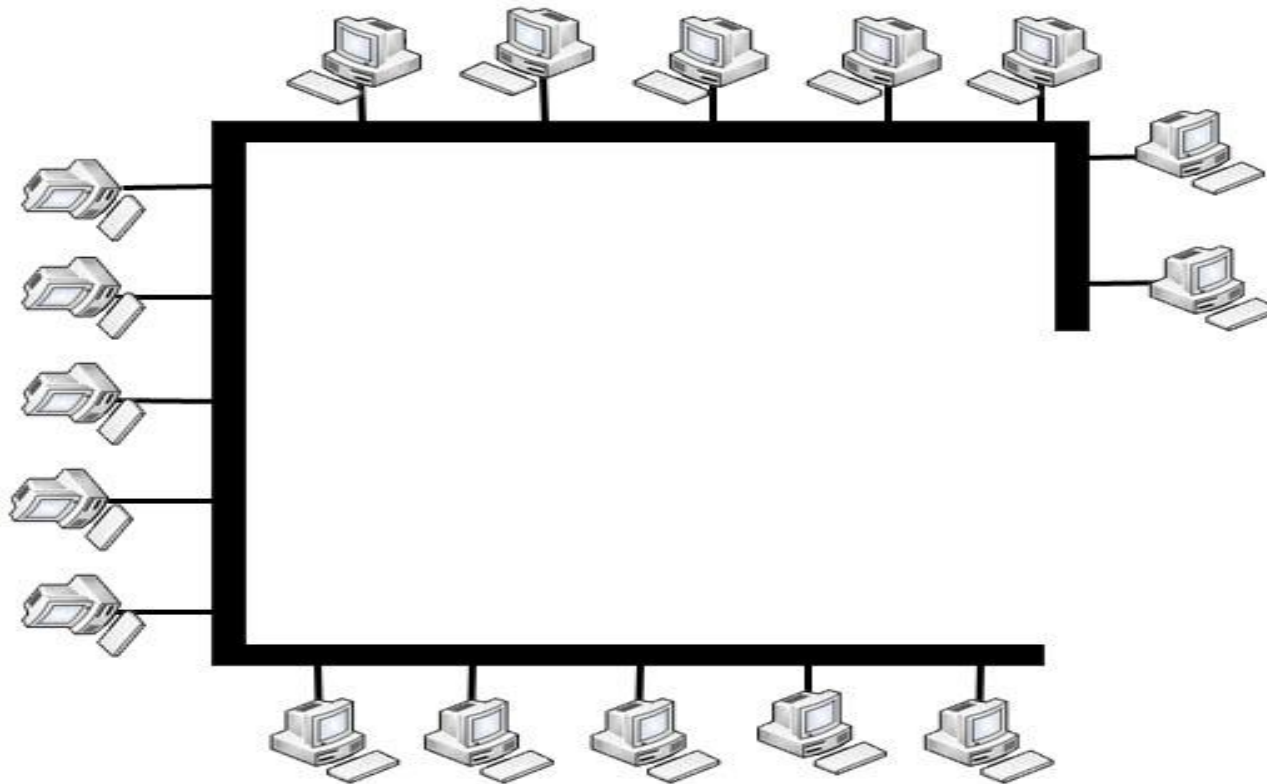
Bus Topology



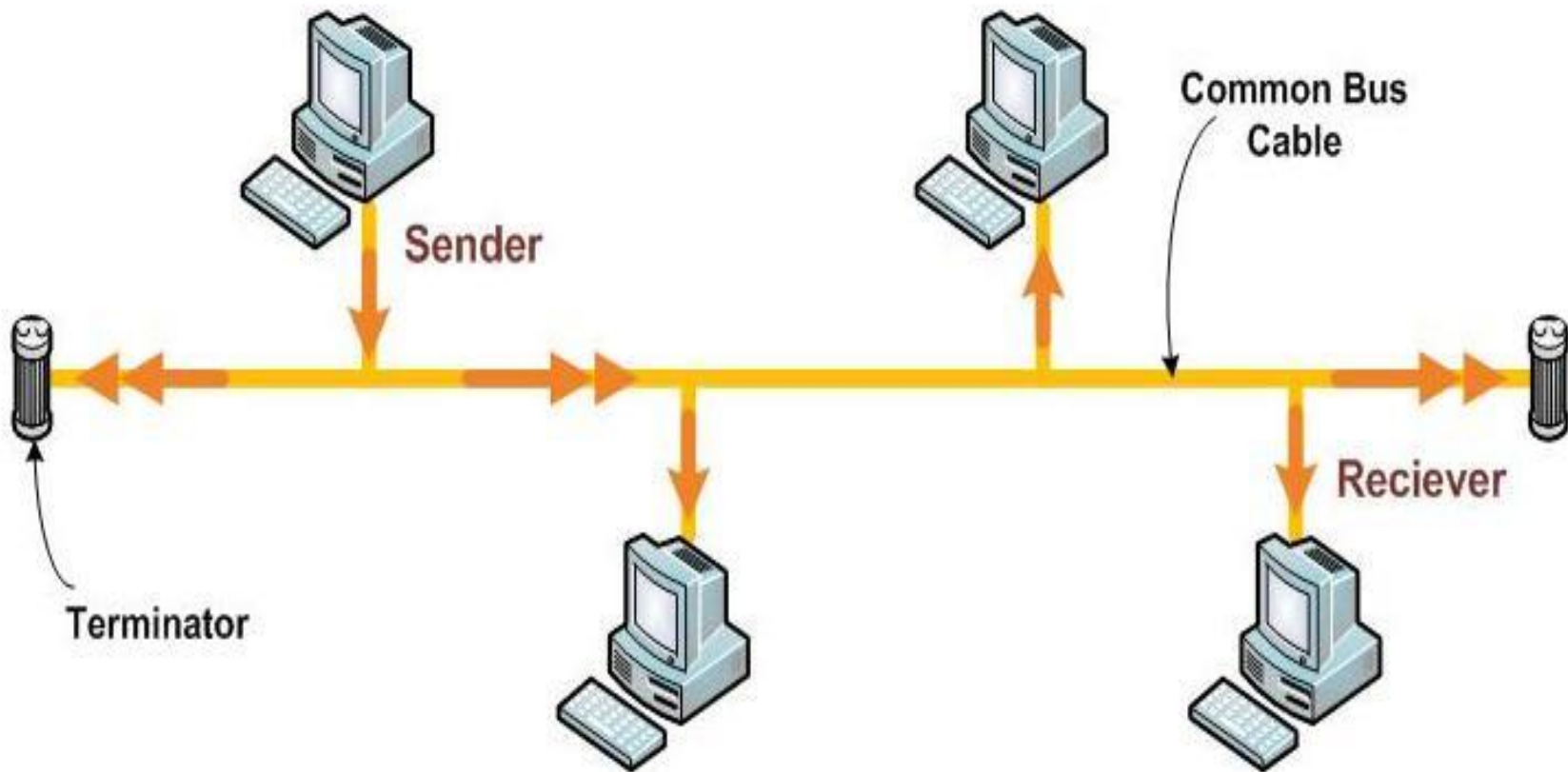
Bus Topology



Bus Topology



Bus Topology



Bus Topology



- A device want to communicate with other device on the n/ws sends a broadcast message onto the wire all other devices see.
- But only the intended devices accepts and process the message.

Bus Topology



Advantages:

1. Ease of installation
2. Less cabling

Disadvantages:

1. Difficult reconfiguration and fault isolation.
2. Difficult to add new devices.
3. Signal reflection at top can degradation in quality.
4. If any fault in backbone can stops all transmission.

Bus Topology



Applications:

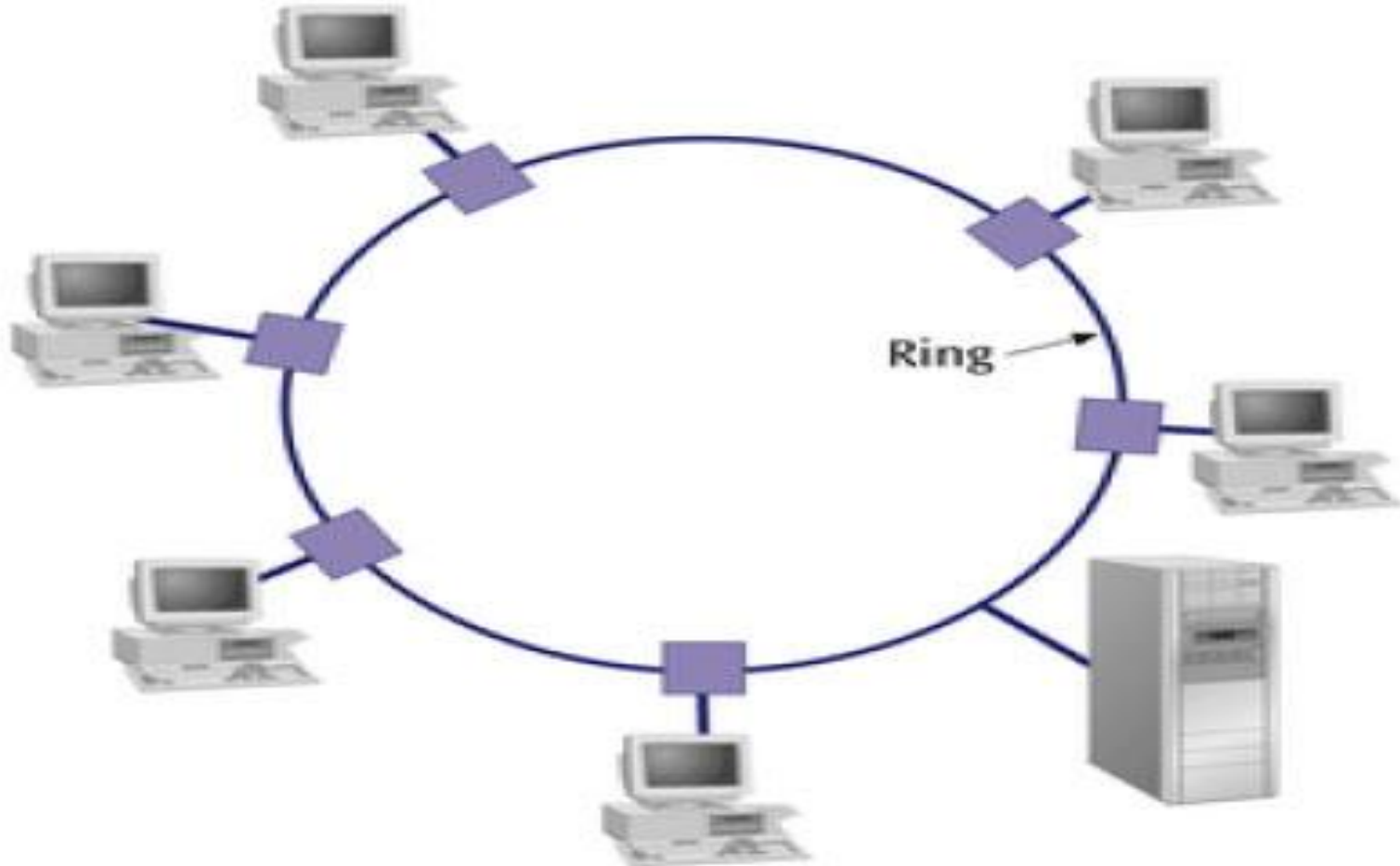
- Most computer's motherboard.

Ring Topology

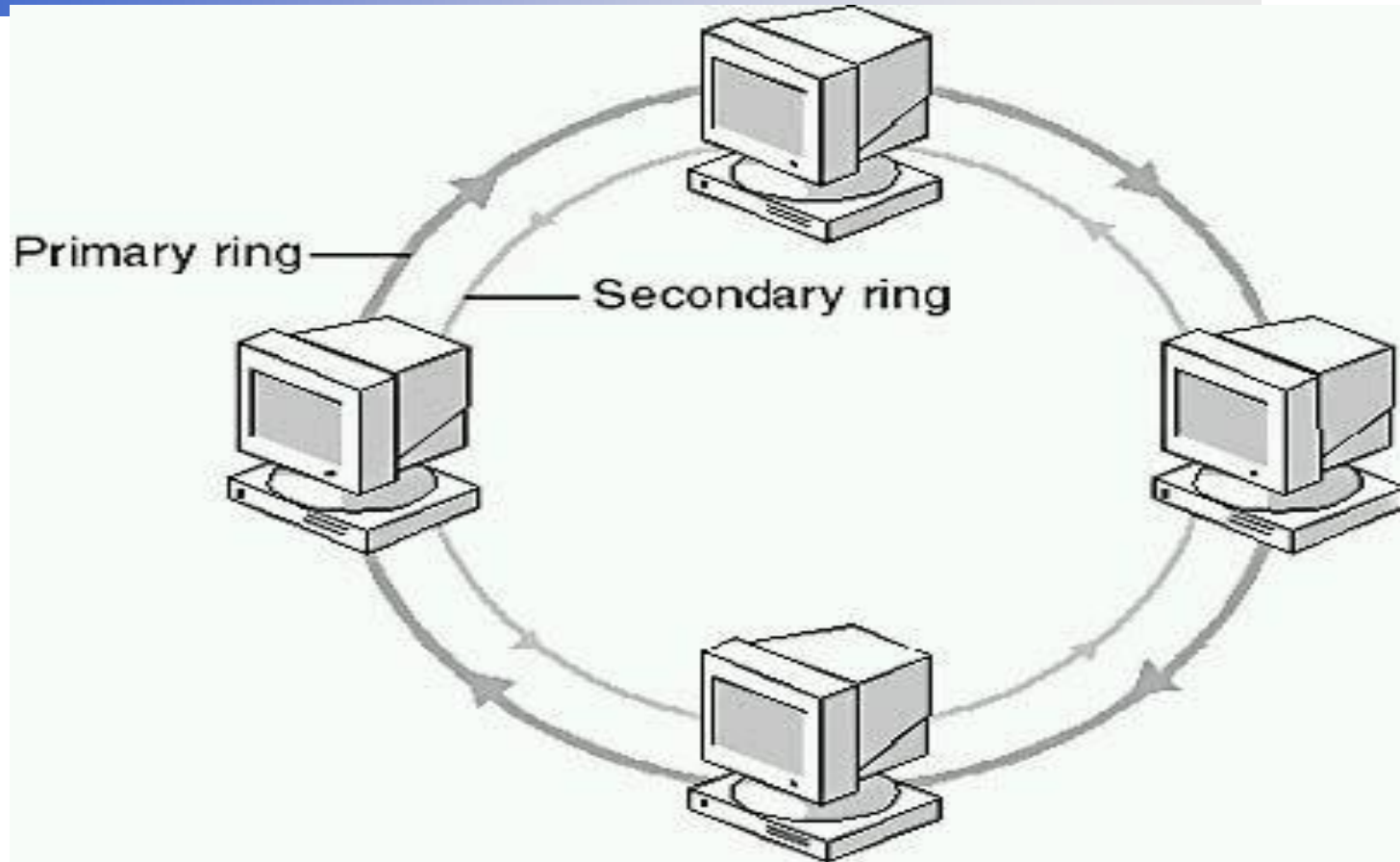


- Here each device has a dedicated connection with two devices on either side.
- The signal is passed in one direction from device to device until it reaches the destination and each device have **repeater**.
- When one device received signals instead of intended another device, its repeater then **regenerates** the data and passes them along.
- To add or delete a device requires changing only two connections.

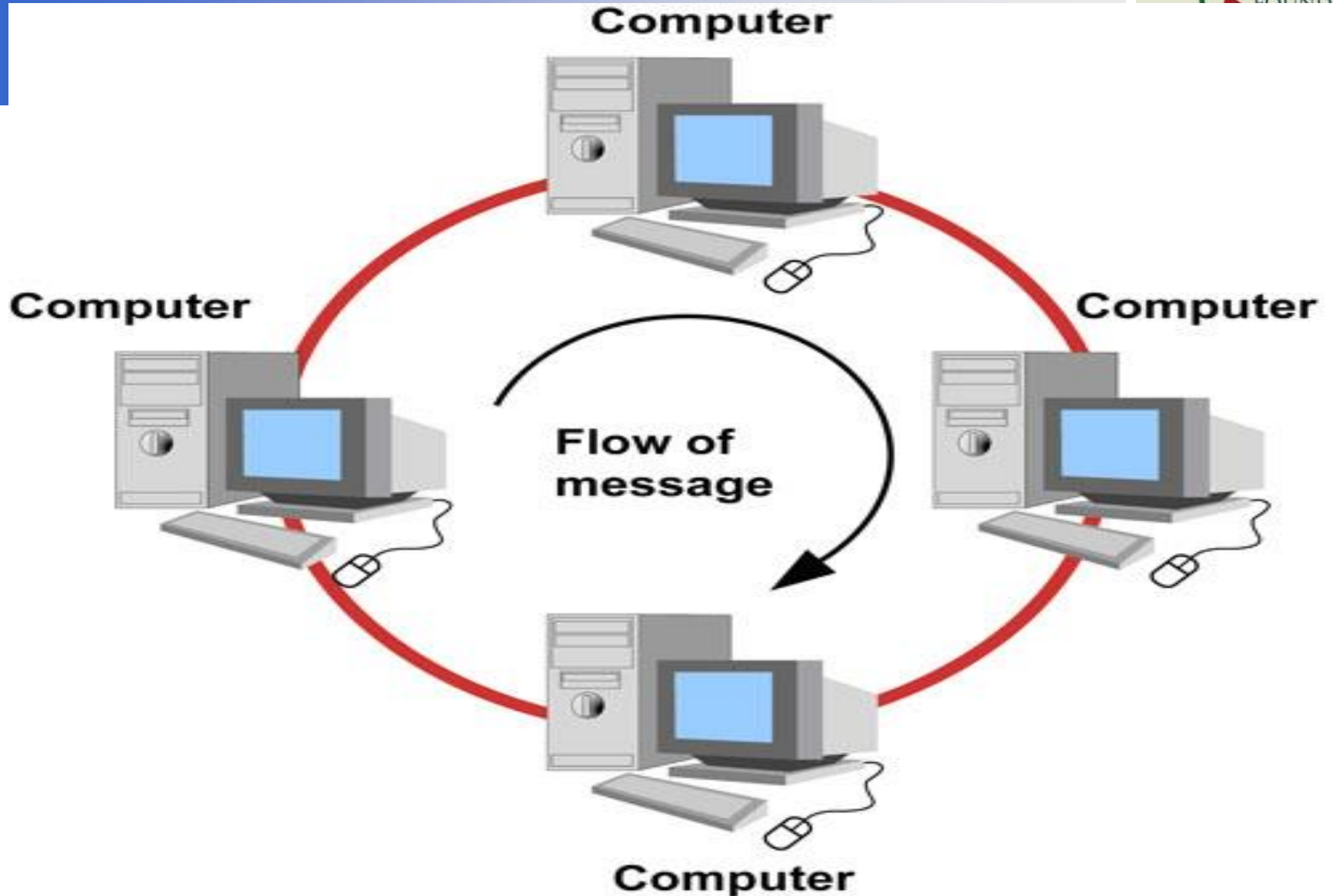
Ring Topology



Ring Topology



Ring Topology



Ring Topology



Advantages:

1. Easy to install.
2. Easy to reconfigure.
3. Fault identification is easy.

Disadvantages:

1. Unidirectional traffic.
2. Break in a single ring can break entire network.

Ring Topology



Applications:

- Ring topologies are found in some office buildings or school campuses.
- Today high speed LANs made this topology **less popular.**

Considerations for choosing topology



- **Money** Bus n/w may be the least expensive way to install a n/w.
- **Length** of cable needed the linear bus n/w uses shorter lengths of cable.
- **Future growth** with star topology, expanding a n/w is easily done by adding another devices.
- **Cable type** most common used cable in commercial organization is twisted pair. Which often used with star topologies.

Full **mesh topology** is theoretically the best since every device is connected to every other device.(thus maximizing speed and security. however, it quite expensive to install)

Software Architecture of Networks



- Types of nodes important to networks.

| | |
|---------|--|
| Hub | A device that repeats or broadcasts the network stream of information to individual nodes (usually personal computers) |
| Switch | A device that receives packets from its input link, and then sorts them and transmits them over the proper link that connects to the node addressed. |
| Bridge | A link between two networks that have identical rules of communication. |
| Gateway | A link between two different networks that have different rules of communication. |
| Router | A node that sends network packets in one of many possible directions to get them to their destination. |

Protocol



- A protocol is a precise set of rules defining how computers communicate: the format of addresses, how data is split into packets, and so on.
- There are many different protocols defining different aspects of network communication.

IP



- IP was designed to allow multiple routes between any two points and to route packets of data around damaged routers.

TCP



- Since there are multiple routes between two points, and since the quickest path between two points may change over time as a function of network traffic and other factors), the packets that make up a particular data stream may not all take the same route.
- Furthermore, they may not arrive in the order they were sent, if they even arrive at all.

IP Addresses and Domain Names



- Every computer on an IPv4 network is identified by a four byte number.
- When data is transmitted across the network, the packet's header includes the address of the machine for which the packet is intended (the destination address) and the address of the machine that sent the packet (the source address).

Domain Name System



- to translate hostnames that humans can remember (like `www.math.hcmuns.edu.vn`) into numeric Internet addresses (like `203.162.44.3`).

Ports



- Each computer with an IP address has several thousand logical ports.
- Each port is identified by a number between 1 and 65,535. Each port can be allocated to a particular service.

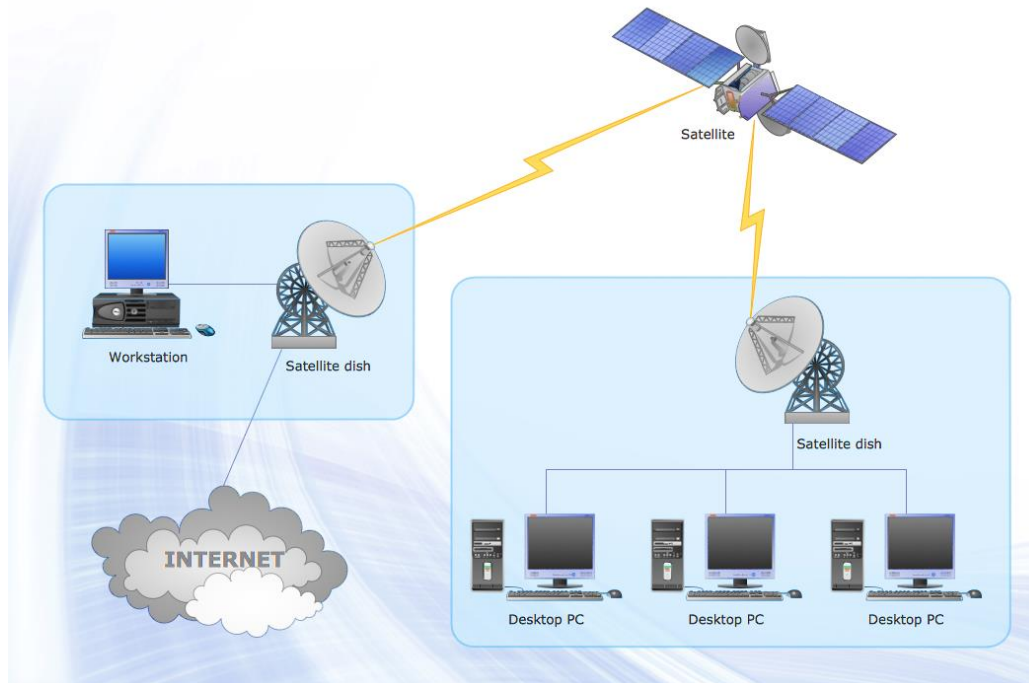
Well known port assignments



| | | |
|----------|-----|-----|
| ■ FTP | 21 | TCP |
| ■ SSH | 22 | TCP |
| ■ telnet | 23 | TCP |
| ■ SMTP | 25 | TCP |
| ■ HTTP | 80 | TCP |
| ■ POP3 | 110 | TCP |
| ■ IMAP | 143 | TCP |

The Internet

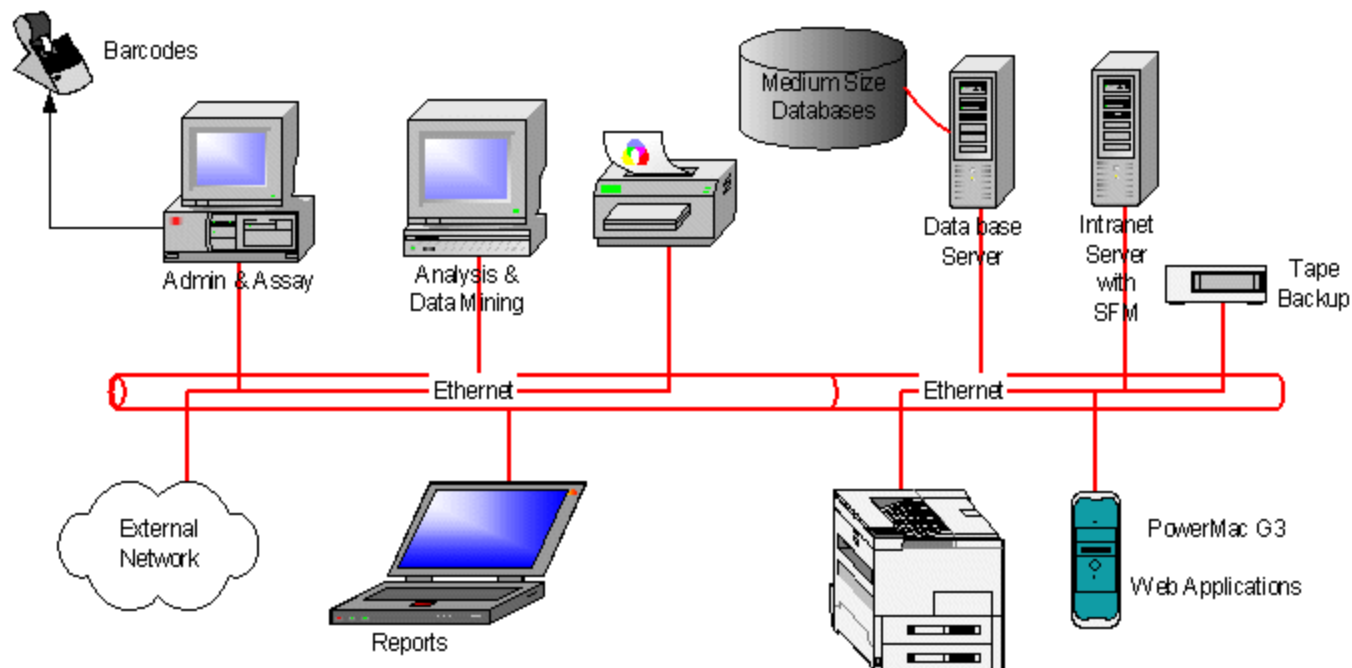
- The Internet is the world's largest IP based network.
- Intranet is a current buzzword that loosely describes corporate practices of putting lots of data on internal web servers.



The Intranet



- Intranet is a current buzzword that loosely describes corporate practices of putting lots of data on internal web servers.



Network Address Translation



- translates the internal addresses into the external addresses.

Software Architecture of Networks



- Problem: If someone wants his own WWW site, he must find a home for it.
- Solution: Find a **Server** willing to store your homepage.
 - **Server**: A dedicated computer that is part of a network.
 - The hard drive contains files that are “served” to whatever requests them.
 - Could be data, programs, or home pages for the WWW.
 - The server normally runs the networking software.
 - **Client/server** model: One computer, the client, requests information from another computer, the server.
 - Client computers can run any type of operating system as long as they have the ability to use Internet protocols.

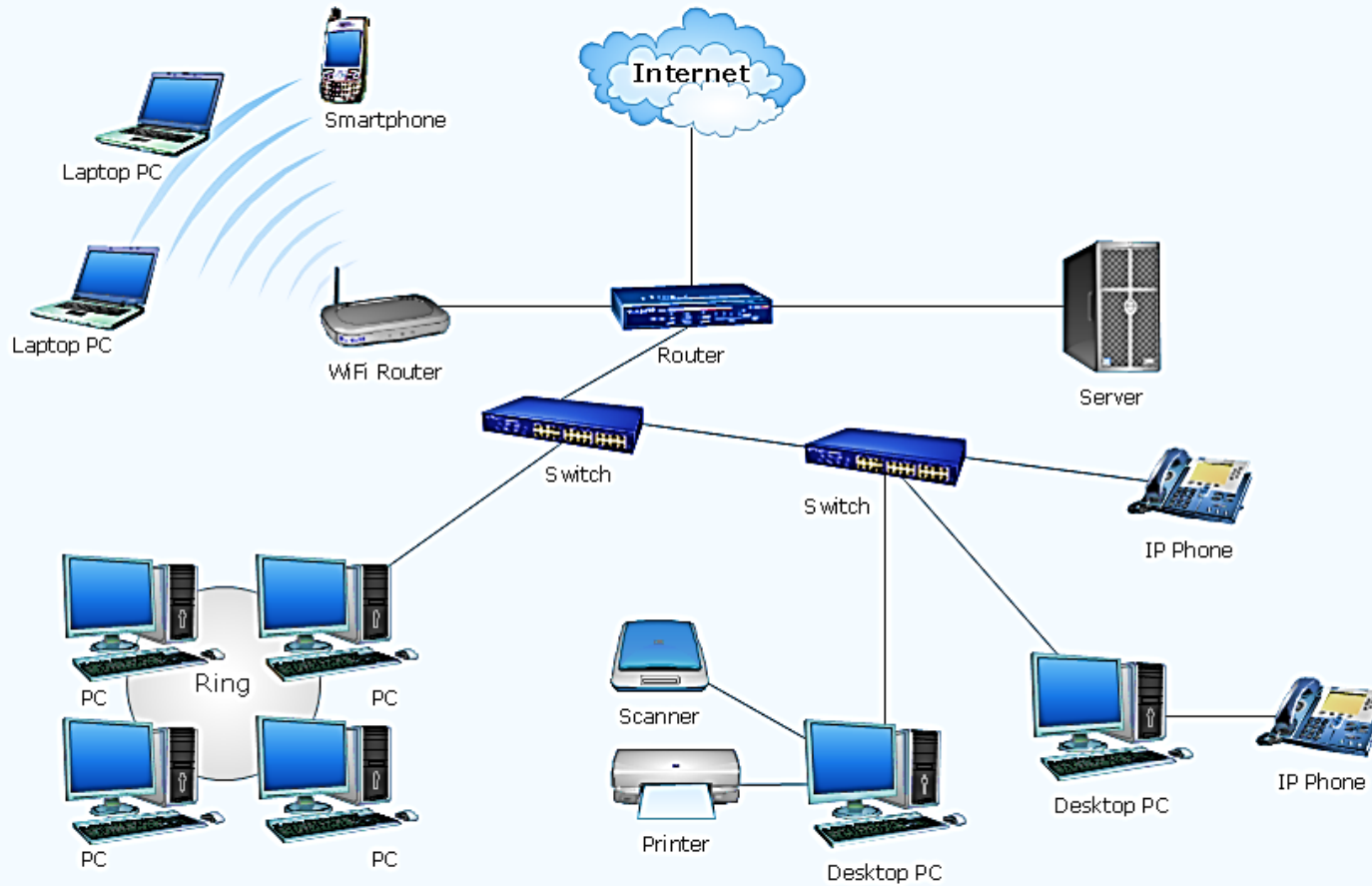
Security of a Network Firewall



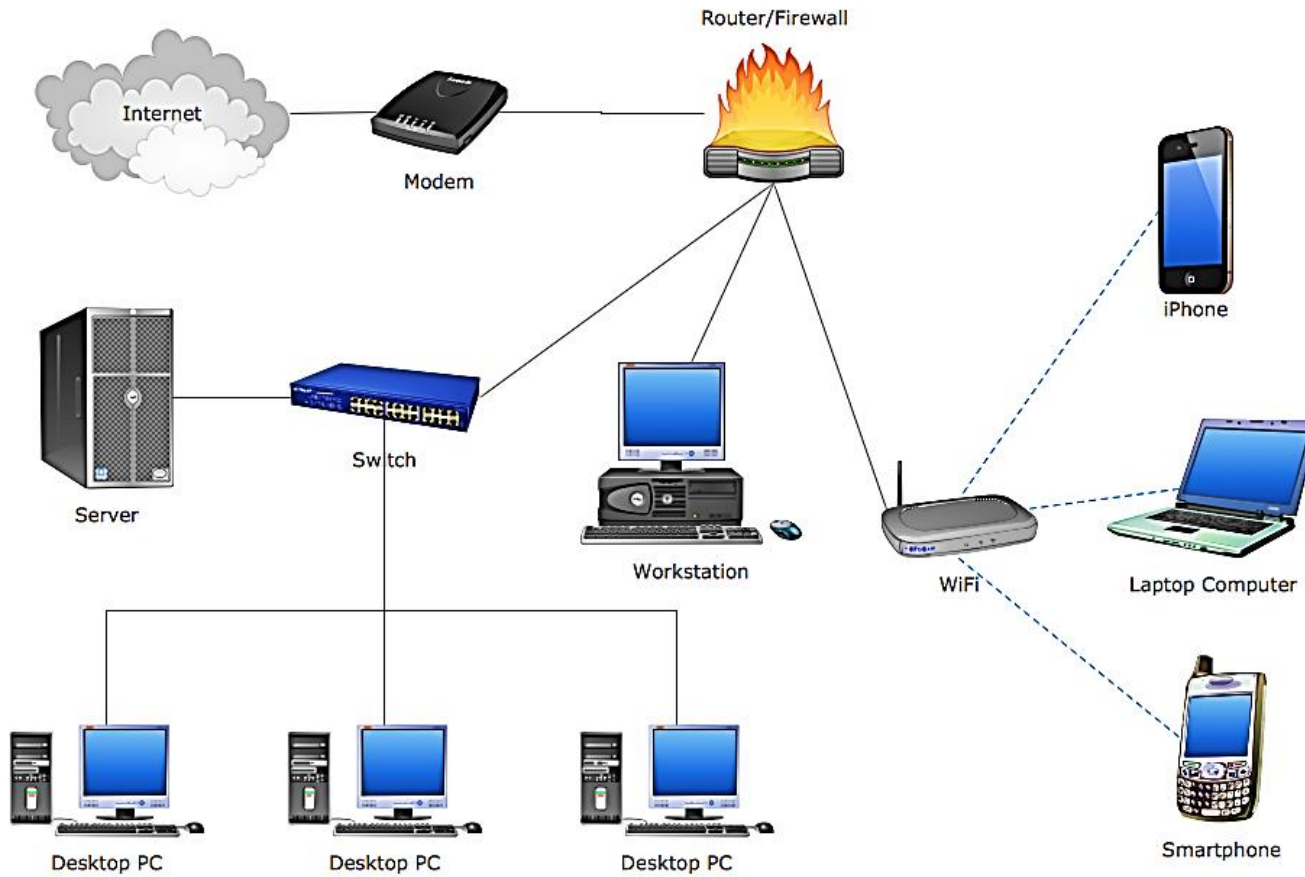
- **Firewall:** A set of programs that monitor all communication passing into and out of a corporation's intranet.
 - Helps prevent, but doesn't eliminate, unauthorized access.



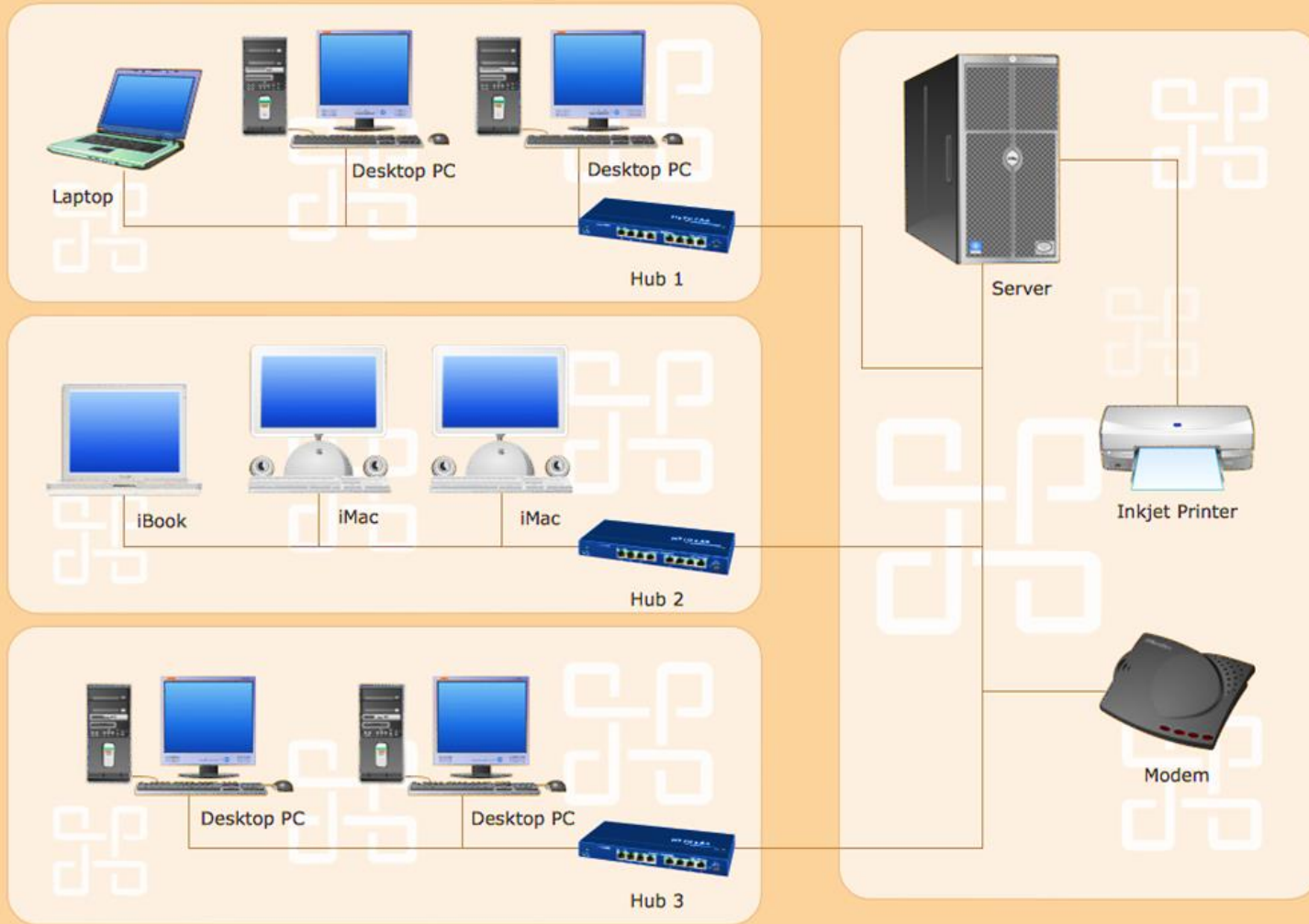
WEB Studio Network



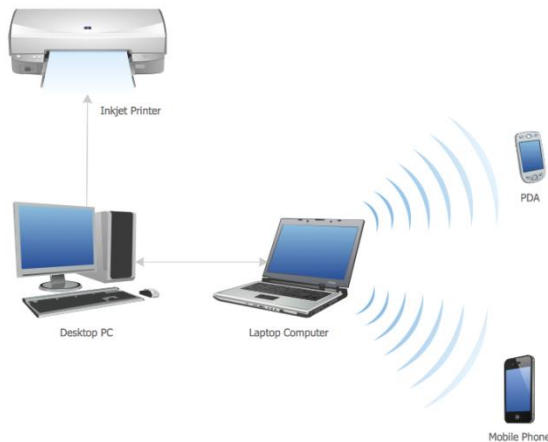
Network Diagram



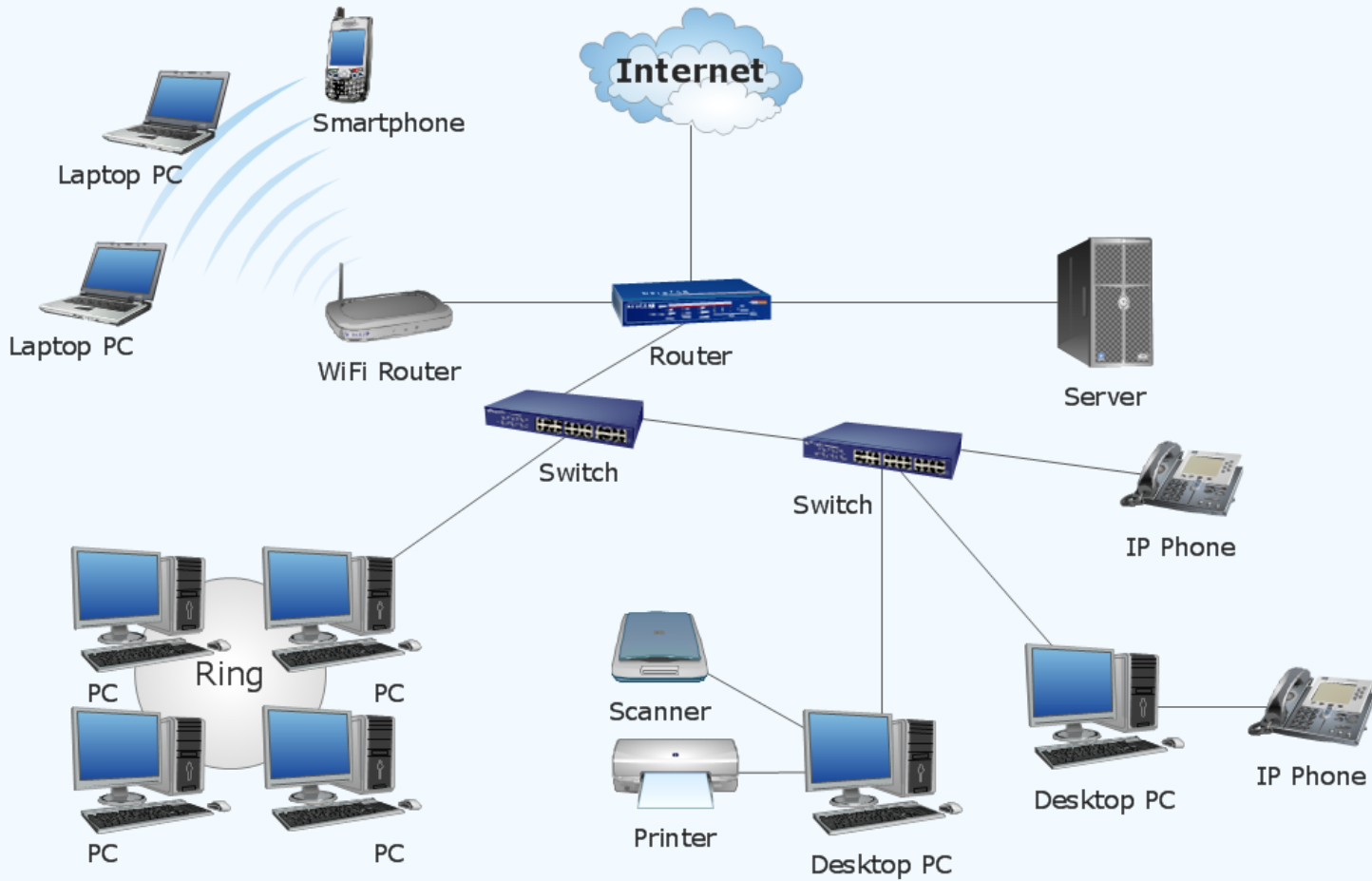
Simple LAN



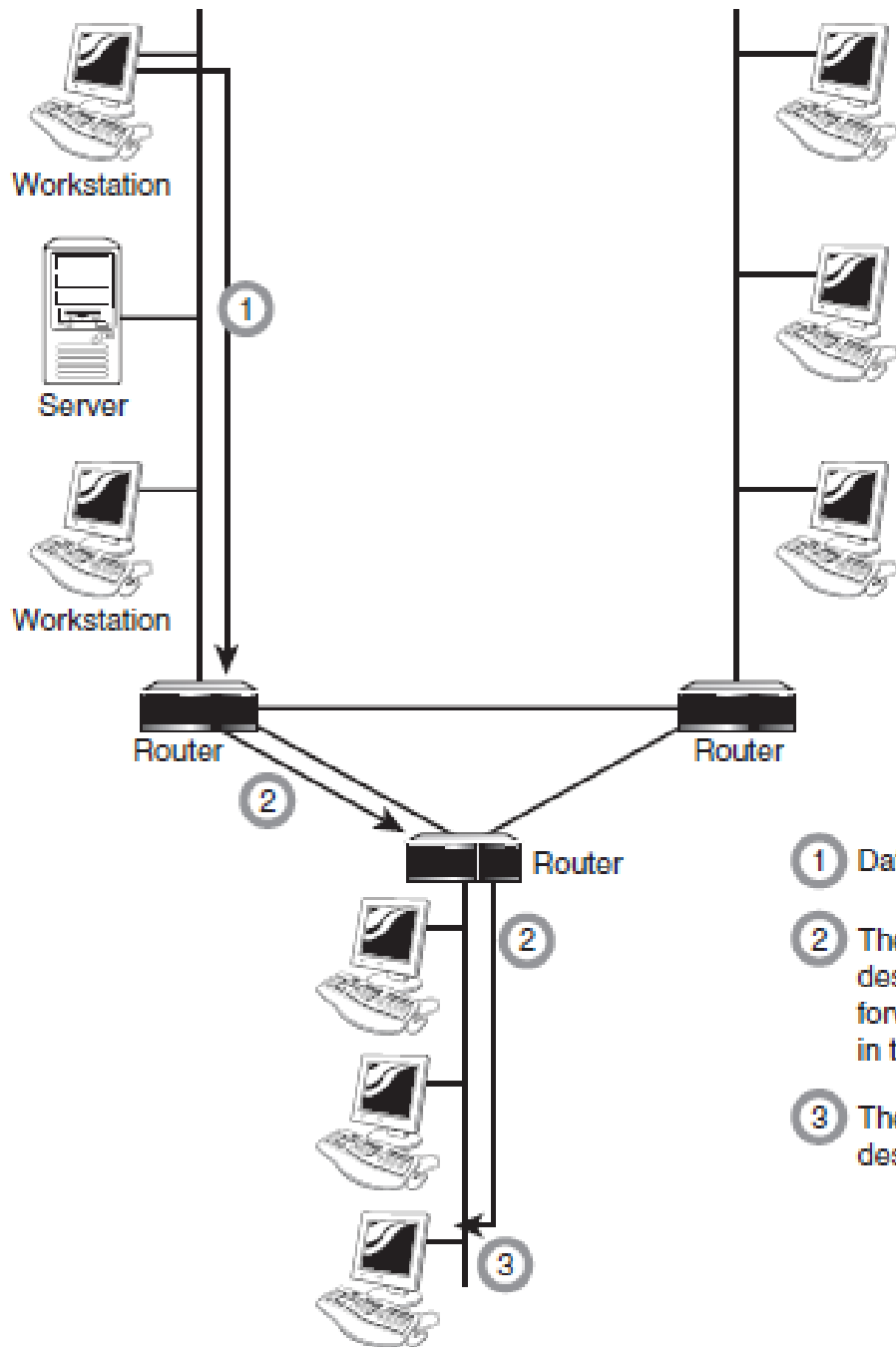
PAN and Bluetooth



A Personal area network (PAN) is a computer network that is used for data transmission between different personal devices (computers, telephones, digital devices, etc.) and for connecting to the higher level network and Internet. PANs can be wired with computer buses (USB and FireWire). A wireless personal area network (WPAN) can be made using the network technologies such as Bluetooth, IrDa, UWB, Z Wave, ZigBee, Body Area Network.



Router



- 1 Data is sent to the router
- 2 The router determines the destination address and forwards it to the next step in the journey
- 3 The data reaches its destination

Malware



What is Malware?

Malware is short for malicious software.

Malware is the name given to any software that could harm a computer system, interfere with a user's data, or make the computer perform actions without the owner's knowledge or permission.

Malware



Basically malware is software that you really don't want to have on your computer!

People can end up with malware installed on their computer system in a variety of ways:

- Having their computer hacked, and the software installed by the hacker.
- Visiting dodgy websites and clicking on infected links
- The computer being infected by a computer virus
- Installing software that seems ok, but has malware hidden inside (known as a 'Trojan Horse').

Computer Virus



So, What is a Computer Virus?

A computer virus is a piece of software that can **'infect'** a computer (install itself) and **copy itself** to **other computers**, without the users knowledge or permission.

Most computer viruses come with some kind of **'payload'** - the **malware** that does something to your computer.

Computer Virus



For example, the virus might install some **spyware** (software that watches what you do with your computer), it might search your computer for **credit card information**, or it might install software that gives someone **remote control** of your computer (turning it into a 'zombie').



Protection from Viruses



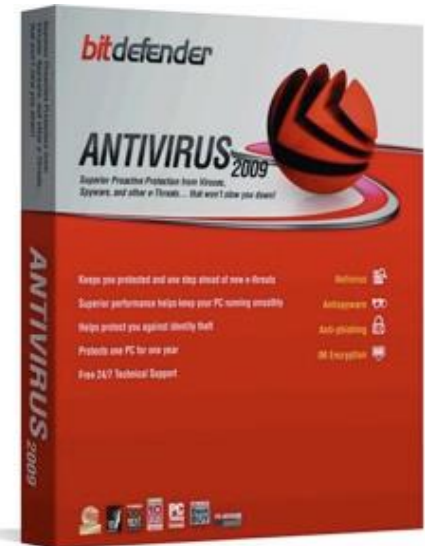
How Can a Computer Be Protected from Viruses?

There are some simple things you can do to help prevent a virus infecting your computer:

Install anti-virus software and keep it up-to-date
(this is the most important thing you can do!)

Install anti-malware software (stops software installing without your knowledge)

Never download and install software from the Internet unless you are certain it is from a source you can **trust**



Protection from Viruses



Don't open e-mail attachments unless you have scanned them (even a file that seems to be a picture can contain a virus)

Don't click links in websites that seem suspicious (if a site is offering prizes / free stuff / etc. be suspicious!)

If someone gives you a **memory stick or CD-ROM**, run a **virus scan** on it before opening any files.

Don't trust cracked versions of software from file-sharing sites (often these have viruses and other malware added to them - a Trojan horse). So use Open source or buy a genuine software.

