INTRODUCTION TO DATA COMMUNICATIONS AND COMPUTER NETWORKS

iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN

SCHOOL OF COMPUTING
MITCH M. ANDAYA

BASIC INFORMATION

- Professor's Name: Mitch M. Andaya
- Title: Vice President for Institutional Planning and Accreditation, Dean Emeritus, and Dean of the School of Computing
- Office: 8th Floor (Faculty Room)
- Email: mitch.andaya@iacademy.edu.ph

BASIC INFORMATION

Attendance will not be checked!

BASIC INFORMATION

- **But if you do decide to attend classes, the following rules will be strictly enforced:**
  - **Cell phones, tablets, and other gadgets are not allowed while class is in session. They must be kept hidden.**
  - **100% attention is required from you. Direct questions to the instructor, not the seatmate.**
  - **No sleeping in class.**
- **You may eat and drink while in class but observe cleanliness.**

BASIC INFORMATION

- Class Requirements : 4 Major Exams. Final grade is just the average of the major exams.
- Cancel the lowest major exam.
- A difficulty factor is given for each exam (to raise the score).

BASIC INFORMATION

- If you missed an exam:
  - you have one (1) week to take it (except for the last exam where no make-up exam will be given)
  - send me an email to schedule your make-up exam
  - no advanced exams will be given
  - there will be no difficulty factor for missed exams.
- Passing is 70%. Absolutely no extra work will be given for those who will fail or those who want a higher grade.

FUNDAMENTAL DEFINITIONS

- ***Data*** refers to the unorganized and unprocessed collection of instructions, concepts, facts, or figures.

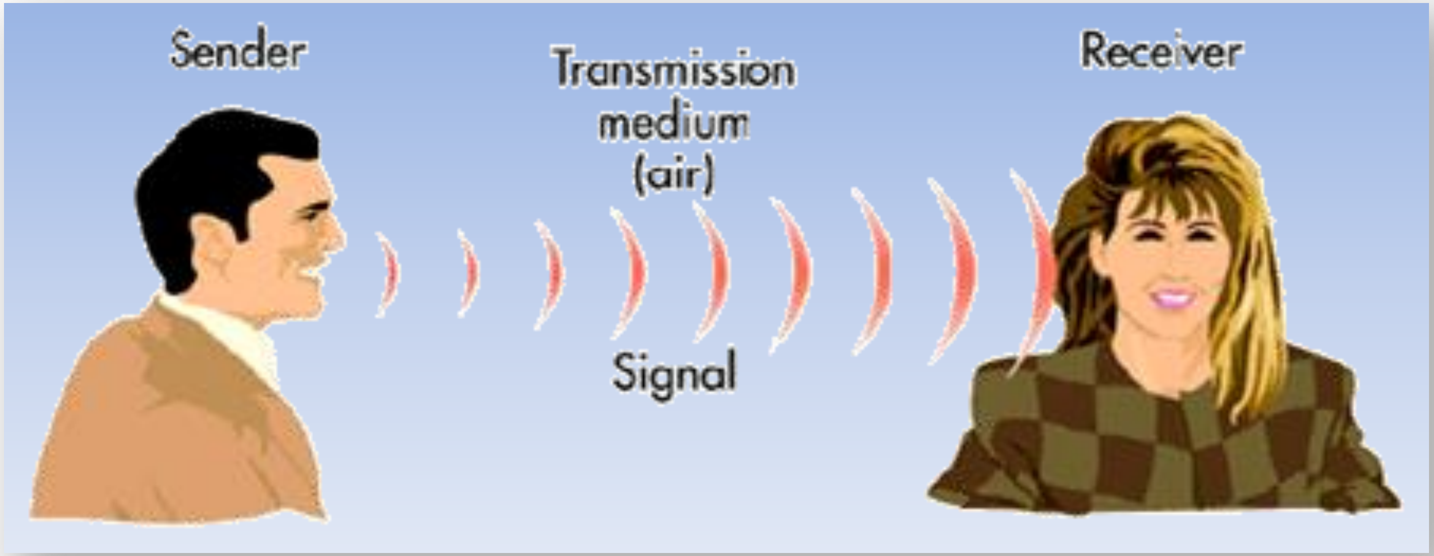
- ***Information*** refers to organized and processed data. It provides context to data.

Examples of Data:
21, 1998, 5, 3, 2,15

Example of Information:

FUNDAMENTAL DEFINITIONS

- ***Communication*** is the process of transferring ideas and information from a sender to a receiver with the use of a medium or channel.



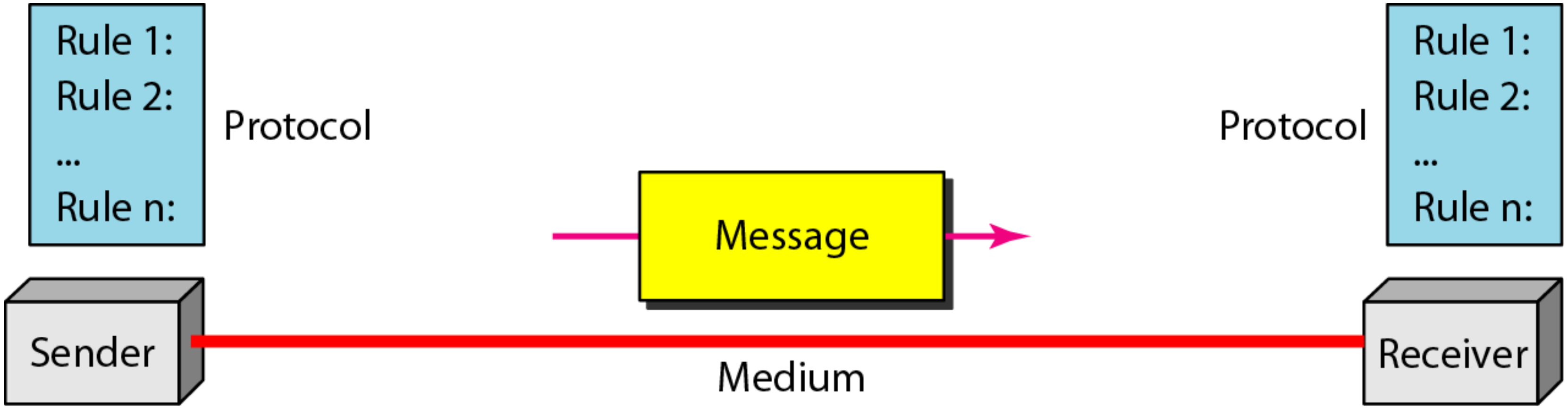
FUNDAMENTAL DEFINITIONS

- ***Data Communication*** is the act of relaying a message (in digital form) between two devices via some form of transmission medium (such as a wire cable).

  For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software.

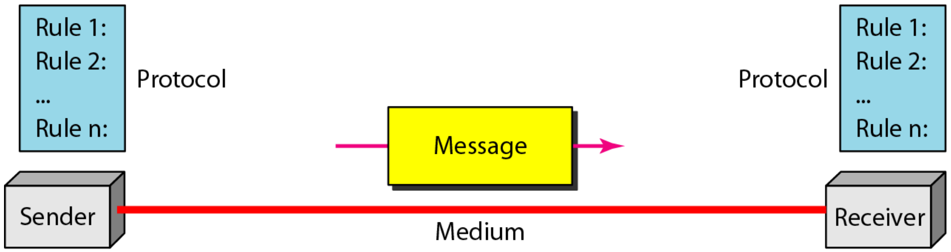
DATA COMMUNICATION SYSTEM

- A data communication system is made up of five elements: ***message***, ***sender***, ***receiver***, ***medium***, and ***protocol***.



DATA COMMUNICATION SYSTEM

– ***Message***. Information to be communicated (text, numbers, images, audio, and/or video)



– ***Sender***. The device that sends the message.

– ***Receiver***. The device that receives the message.

– ***Medium*** (or ***channel***). The physical (or non physical) path by which a message travels from sender to receiver.

– ***Protocol***. The set of rules that govern data communications.

DATA COMMUNICATION SYSTEM

- The effectiveness of a data communication system depends on three fundamental characteristics:

1. ***Delivery***. The system must deliver data to the correct destination.

2. ***Accuracy***. The system must deliver the data accurately (no alterations).

3. ***Timeliness***. The system must deliver data in a timely manner (not late).

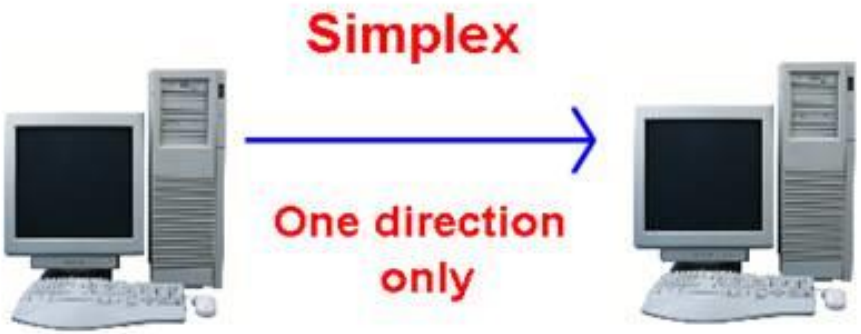
DATA FLOW

- ***Data flow*** refers to the direction of data transmission. There are three modes of transmission based on data flow: simplex, half-duplex, and full-duplex.

- In ***simplex*** mode, the communication is unidirectional, as on a one-way street.

  Only one of the two devices on a link can transmit; the other can only receive.

  Examples are keyboards and monitors.



DATA FLOW

- In ***half-duplex*** mode, each station can both transmit and receive, but not at the same time.

  When one device is sending, the other can only receive, and vice versa.

  Examples are walkie-talkies and CB radios.

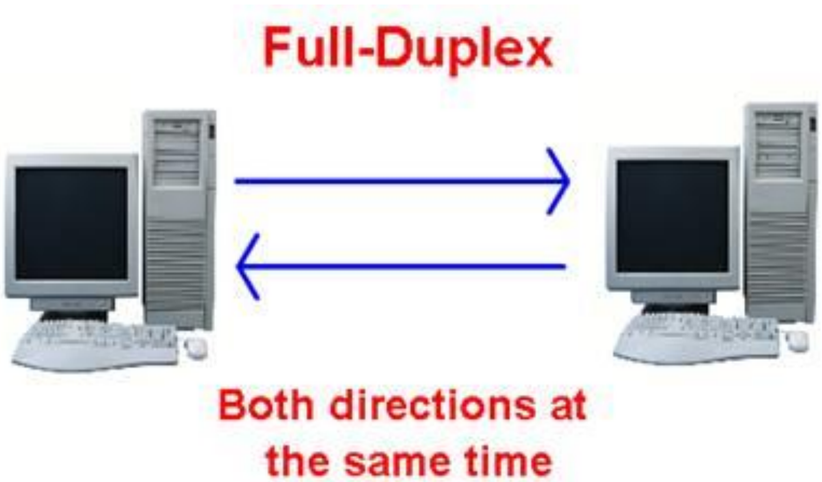
  There is a problem with turnaround time (the time it takes for the transmission circuits to change direction).

DATA FLOW

- In ***full-duplex*** mode (also called ***duplex***), both stations can transmit and receive simultaneously.

  Examples are telephones.

  This usually requires one set of transmission circuits each for transmission and reception.

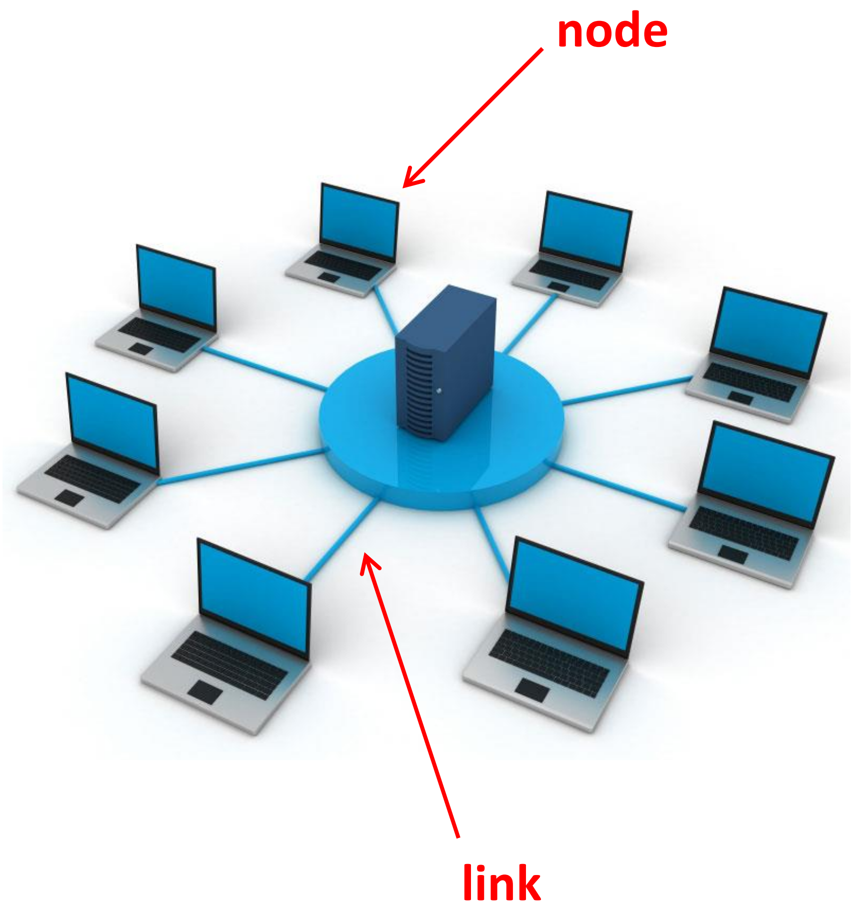


COMPUTER NETWORKS

- A network is a set of devices (often referred to as ***nodes***) connected by communication ***links***.

- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

- The connecting link may be physical (copper or fiber optic type) or non-physical (radio waves).



- A network must be able to meet a certain number of criteria. Most important of these are ***performance***, ***reliability***, and ***security***.

- ***Performance***. Performance can be measured using transit time and response time.

  Transit time is the amount of time required for a message to travel from one device to another.

  Response time is the elapsed time between an inquiry and a response.

- A network must be able to meet a certain number of criteria. Most important of these are ***performance***, ***reliability***, and ***security***.

Performance is often evaluated by two networking metrics: ***throughput*** and ***delay***. However, these two criteria are often contradictory.

Sending more data to the network increases throughput but the delay is also increased because of traffic congestion in the network.

- A network must be able to meet a certain number of criteria. Most important of these are ***performance***, ***reliability***, and ***security***.

- Network ***reliability*** is measured by the:

  1. frequency of failure,
  2. the time it takes a link to recover from a failure,
  3. and the network's robustness in a catastrophe.

COMPUTER NETWORKS

- A network must be able to meet a certain number of criteria. Most important of these are ***performance***, ***reliability***, and ***security***.

- Network ***security*** issues include:

    1. protecting data from unauthorized access,

    2. protecting data from damage,

    3. and implementing policies and procedures for recovery from breaches and data losses.

PHYSICAL STRUCTURES

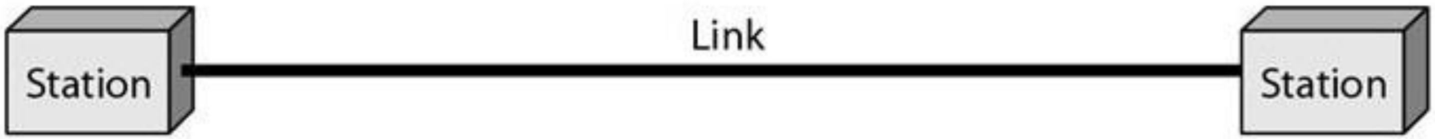
- A network is two or more devices connected through links.
- A link is a communications pathway that transfers data from one device to another.
- For communication to occur, two devices must be connected in some way to the same link at the same time.

PHYSICAL STRUCTURES

- There are two possible types of connections: ***point-to-point*** and ***multipoint***.

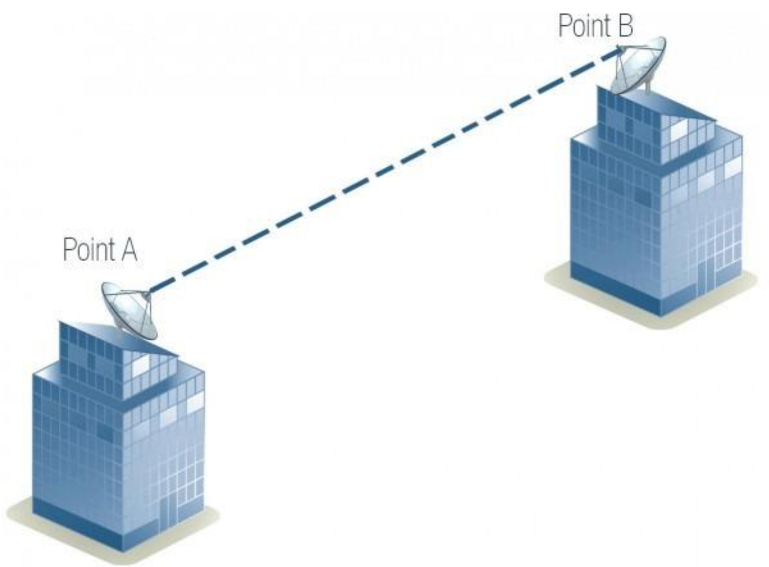
- A point-to-point connection provides a dedicated link between two devices.

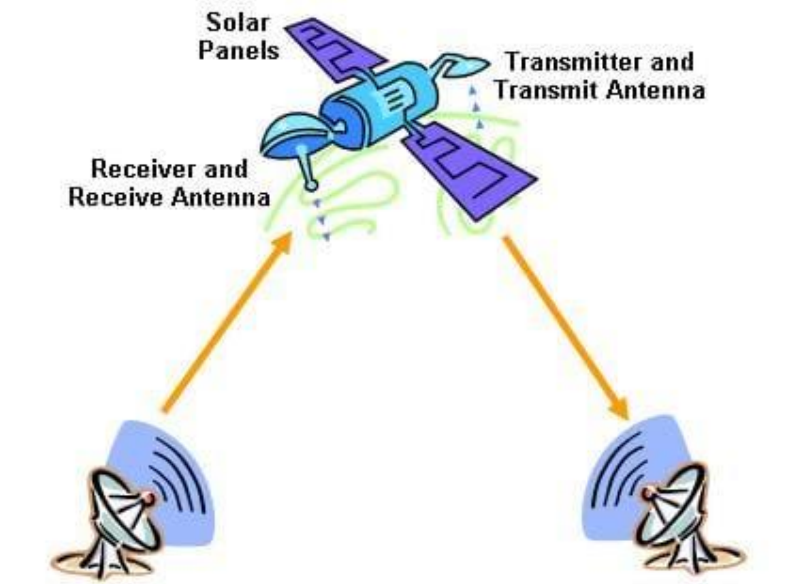
  The entire capacity of the link is reserved for transmission between those two devices.



PHYSICAL STRUCTURES

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.

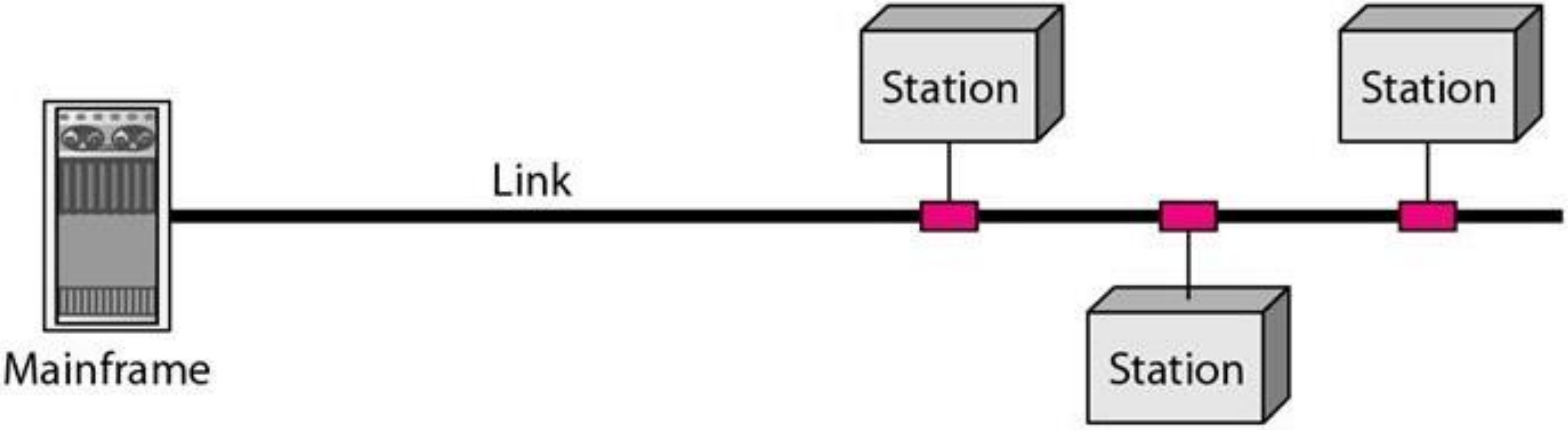




iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN

PHYSICAL STRUCTURES

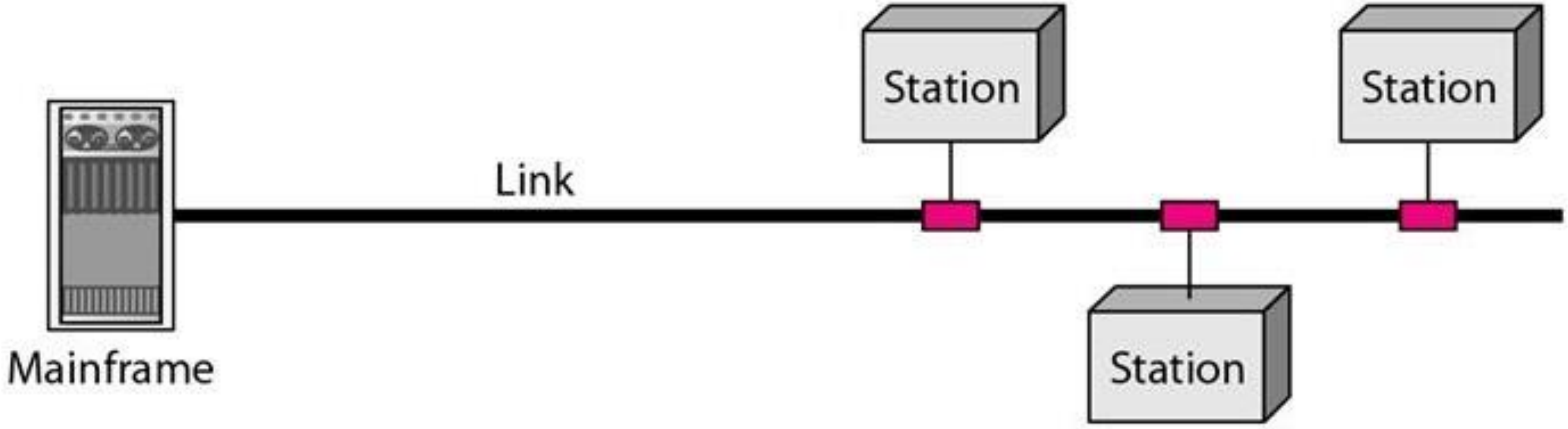
- A multipoint (also called ***multidrop***) connection is one in which more than two specific devices share a single link.



PHYSICAL STRUCTURES

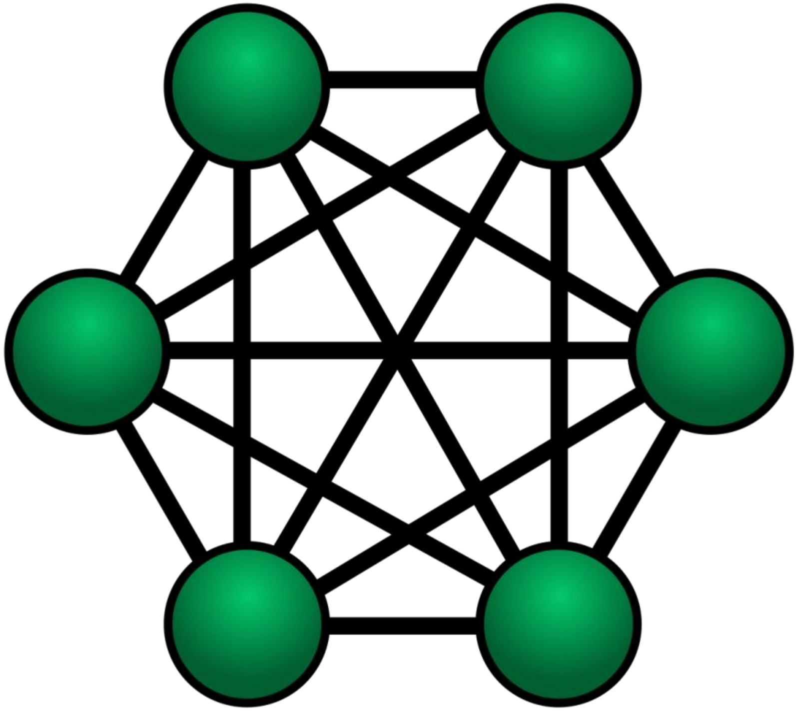
In a multipoint environment, the capacity of the channel is shared, either ***spatially*** (space) or ***temporally*** (time).

If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a temporally shared connection.

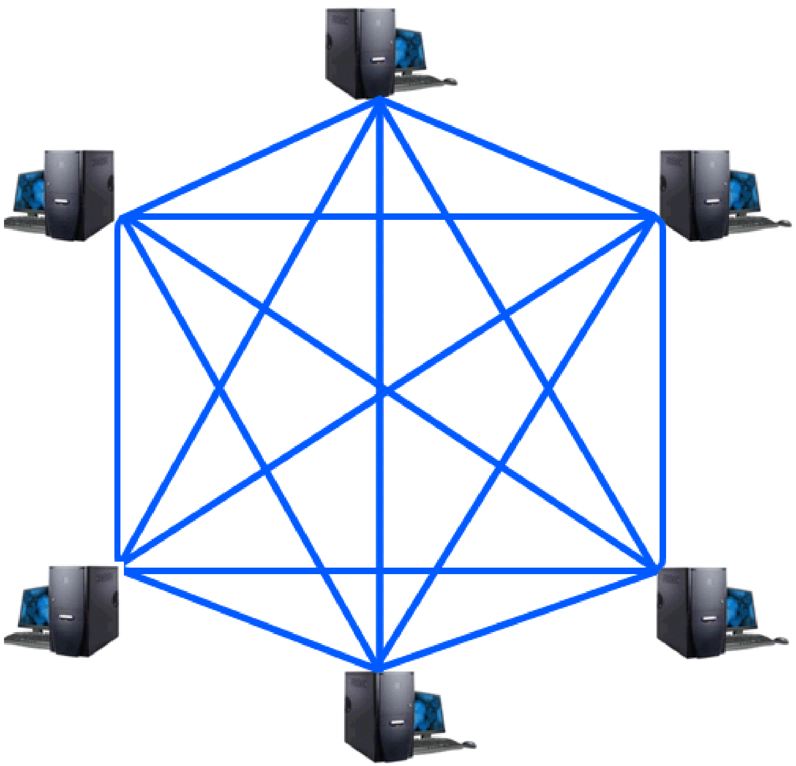


NETWORK TOPOLOGY

- ***Network topology*** defines the physical configuration brought about by the interconnection of devices.
- A network's topology is the cable pattern used to connect the clients with the servers.

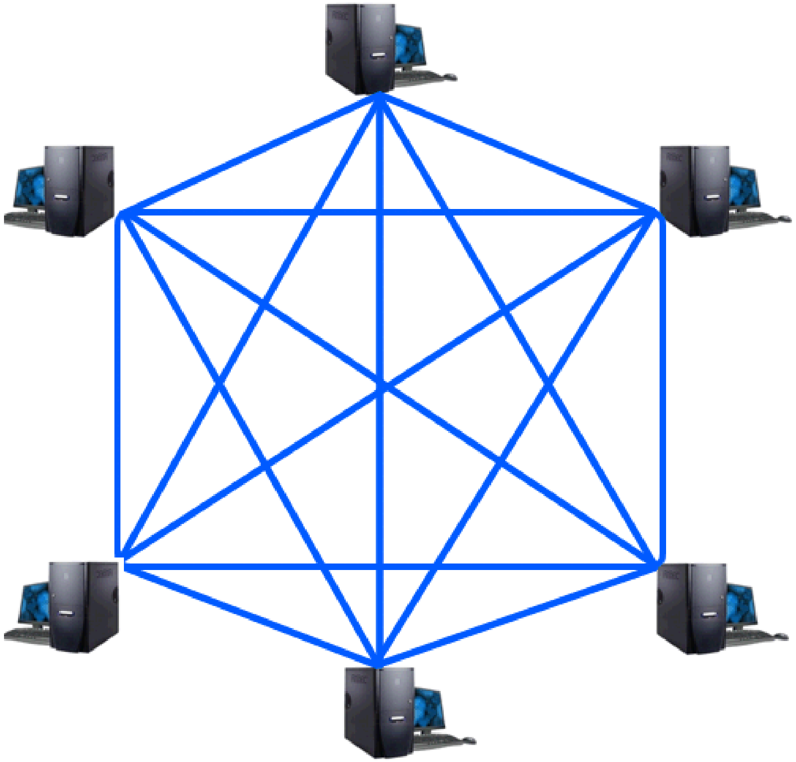


MESH TOPOLOGY



- 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

MESH TOPOLOGY

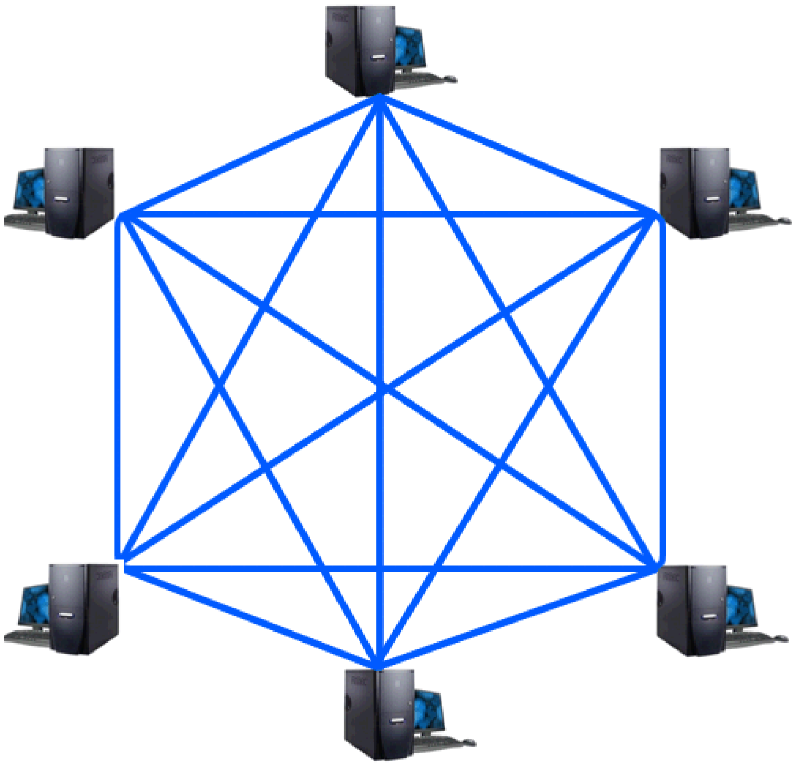


- The number of physical links required in a fully connected mesh network with *n* nodes is computed as:

$$\frac{n(n-1)}{2}$$

- For example, if there are 6 computers, there will be 6(5)/2 = 15 links.

MESH TOPOLOGY



- Advantages of mesh over other network topologies:

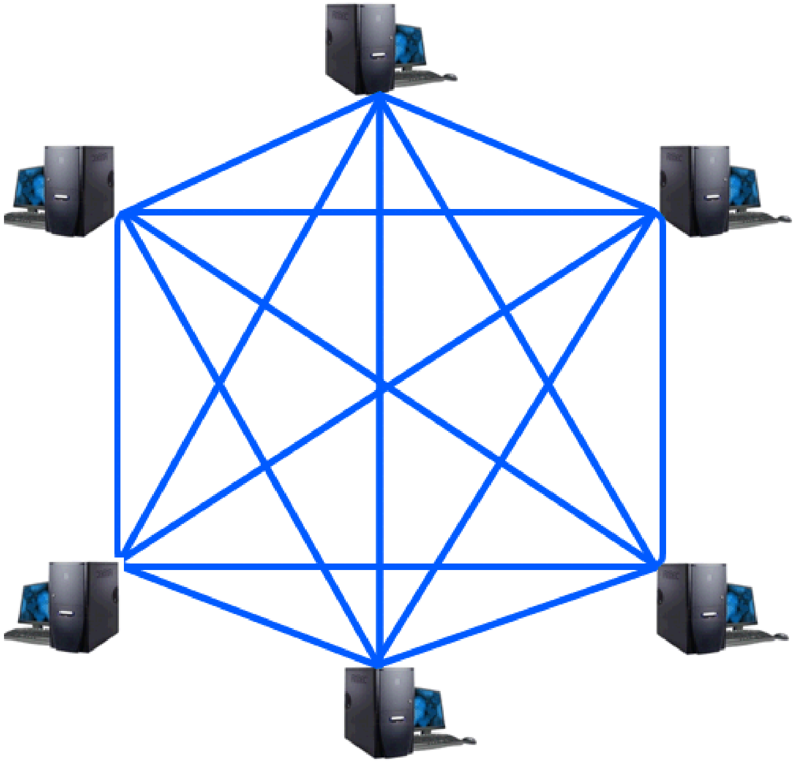
  1. The use of dedicated links guarantees that each connection can carry its own data load.

     This eliminates the traffic problems that can occur when links must be shared by multiple devices.

  2. A mesh topology is robust.

     If one link becomes unusable, it does not incapacitate the entire system.

MESH TOPOLOGY



3. There is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it.

4. Finally, point-to-point links make fault identification and fault isolation easy.

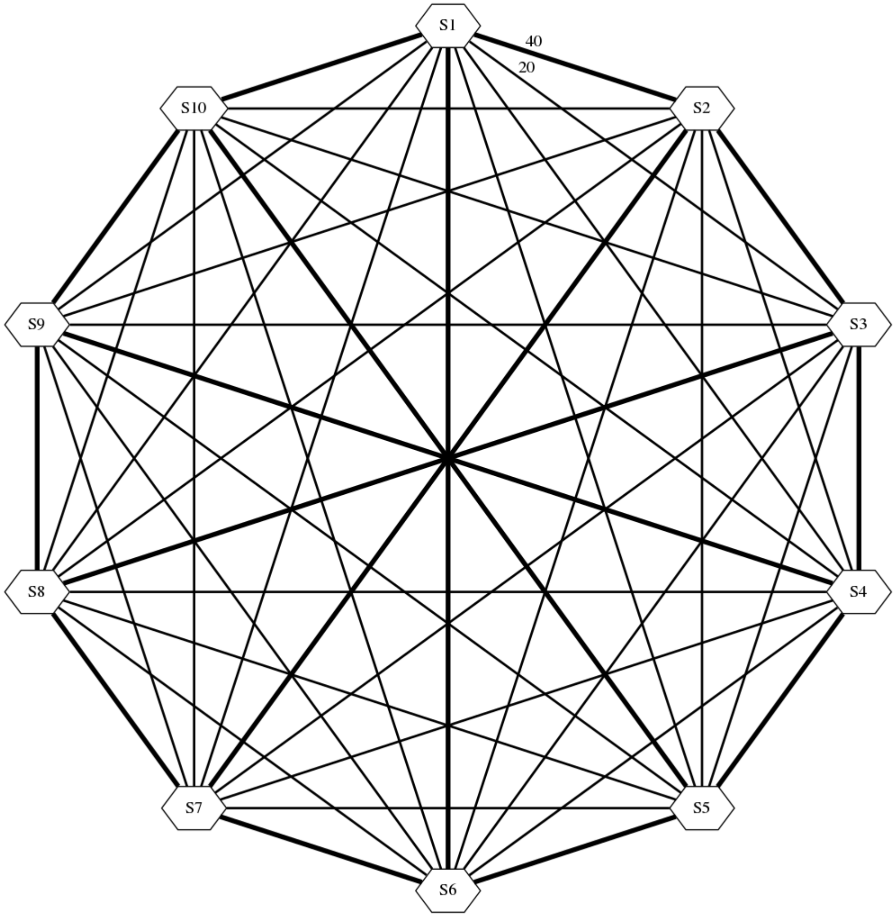
   This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN

MESH TOPOLOGY

- 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.

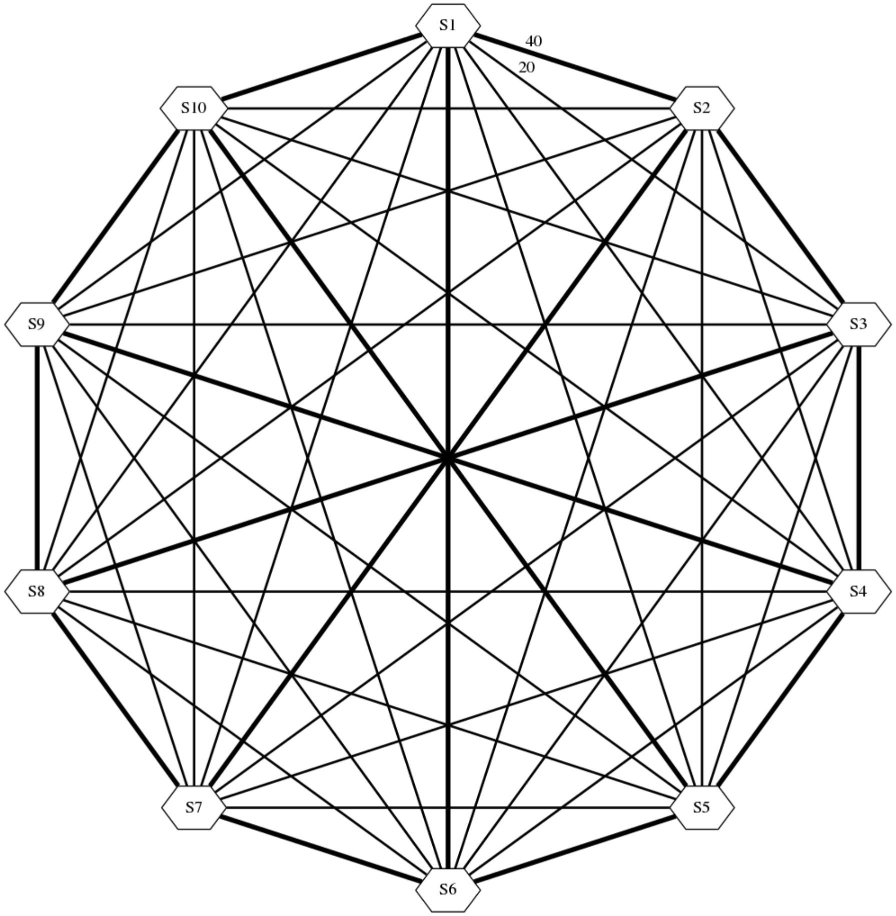


MESH TOPOLOGY

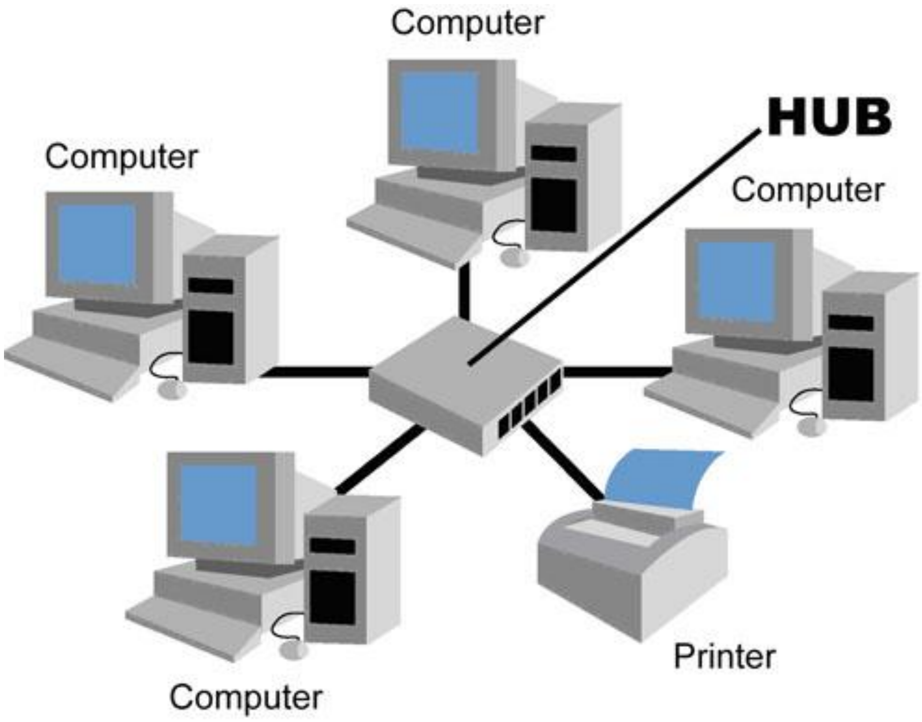
Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

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.

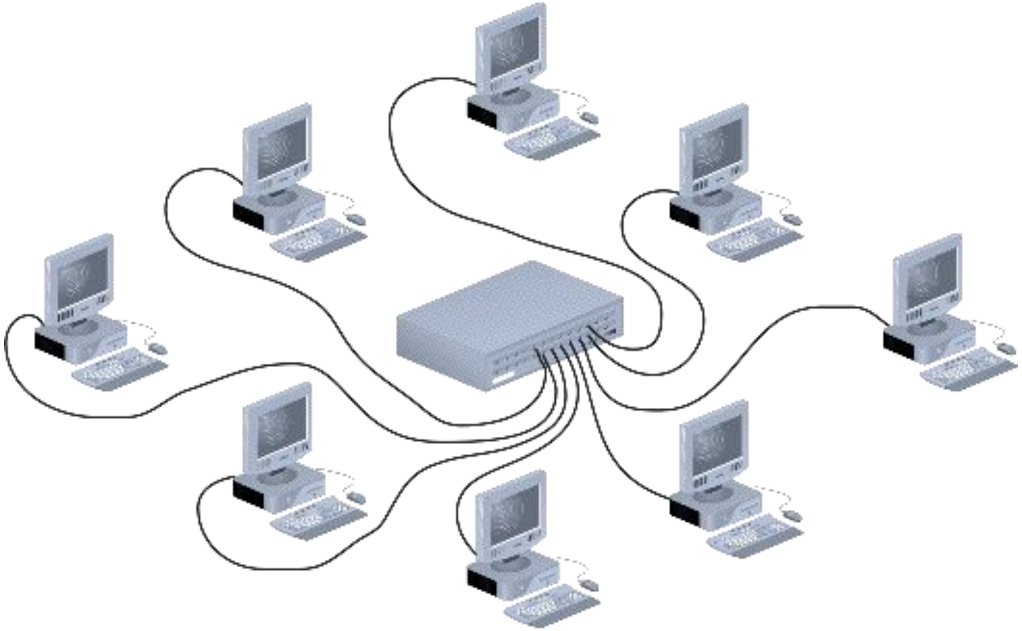


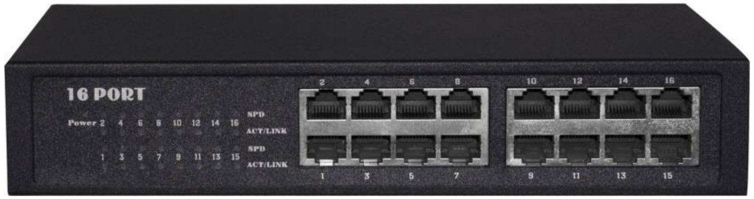
STAR TOPOLOGY

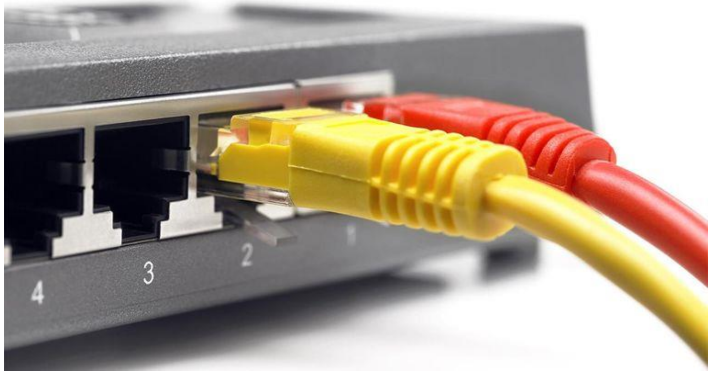


- In a ***star topology***, each device has a dedicated point-to-point link only to a central controller, usually called a ***hub***.
- The hub acts as an exchange: If one device wants to send data to another, it sends the data to the hub, which then relays the data to the other connected device.
- Actually, hubs broadcast all incoming data to all active ports but only the intended recipient accepts the data. All other devices will ignore the data.

STAR TOPOLOGY



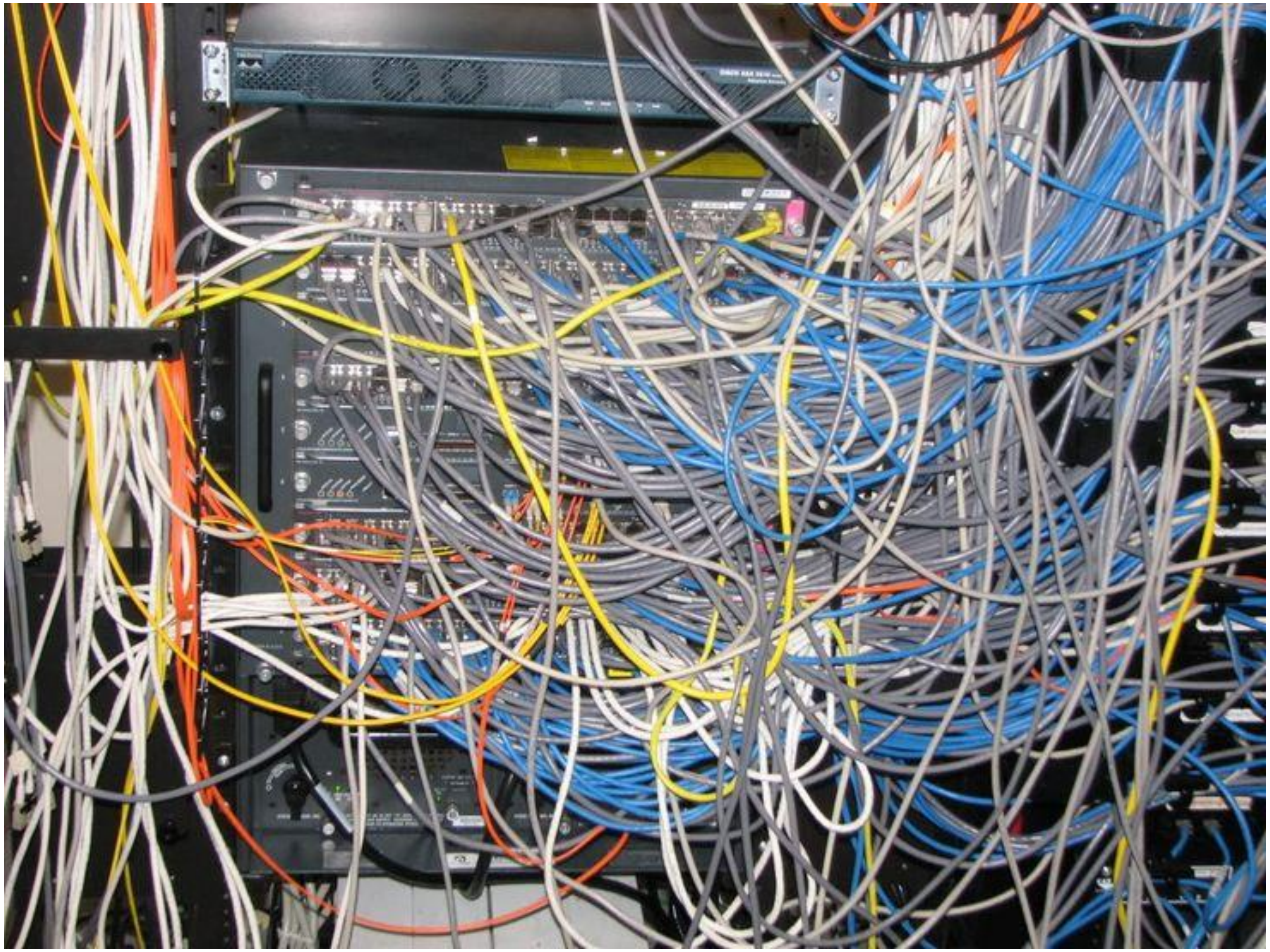




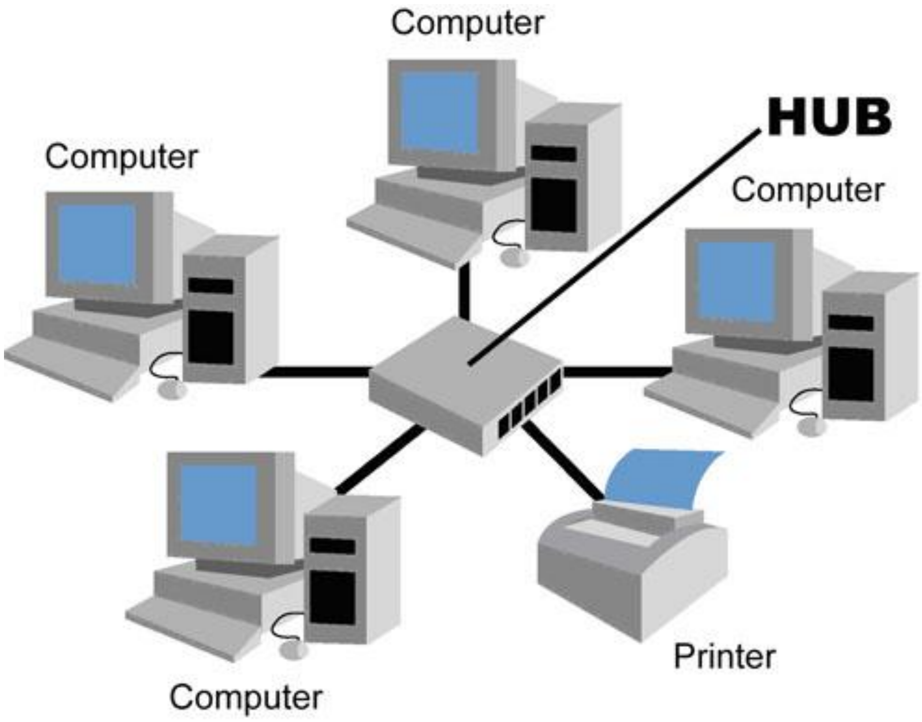
STAR TOPOLOGY

STAR TOPOLOGY

STAR TOPOLOGY



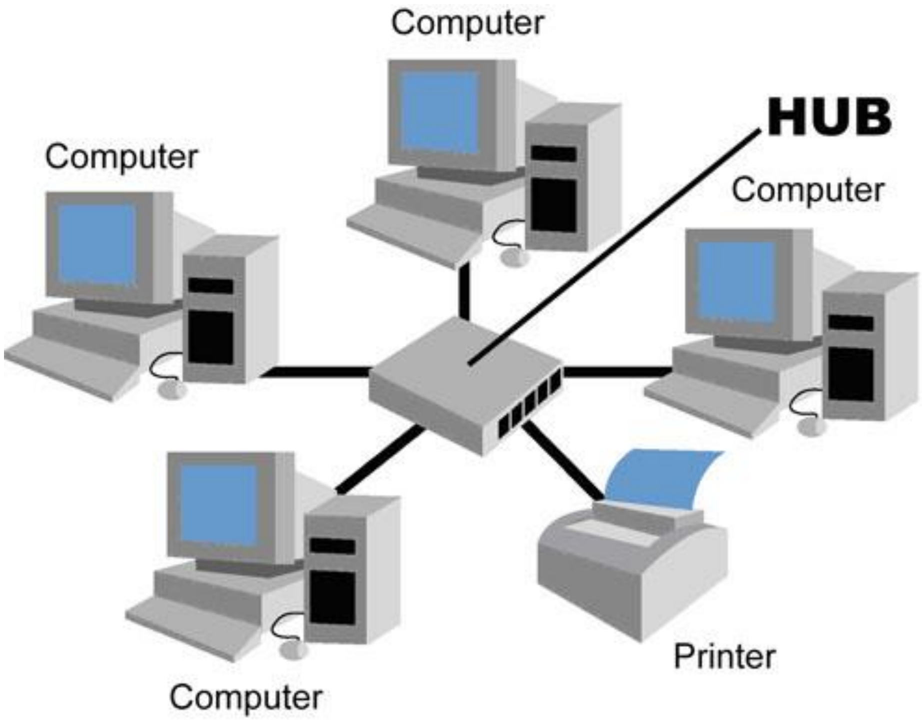
STAR TOPOLOGY



- A star topology is less expensive than a mesh topology.

  Each device needs only one link and one I/O port to connect it to any number of others.

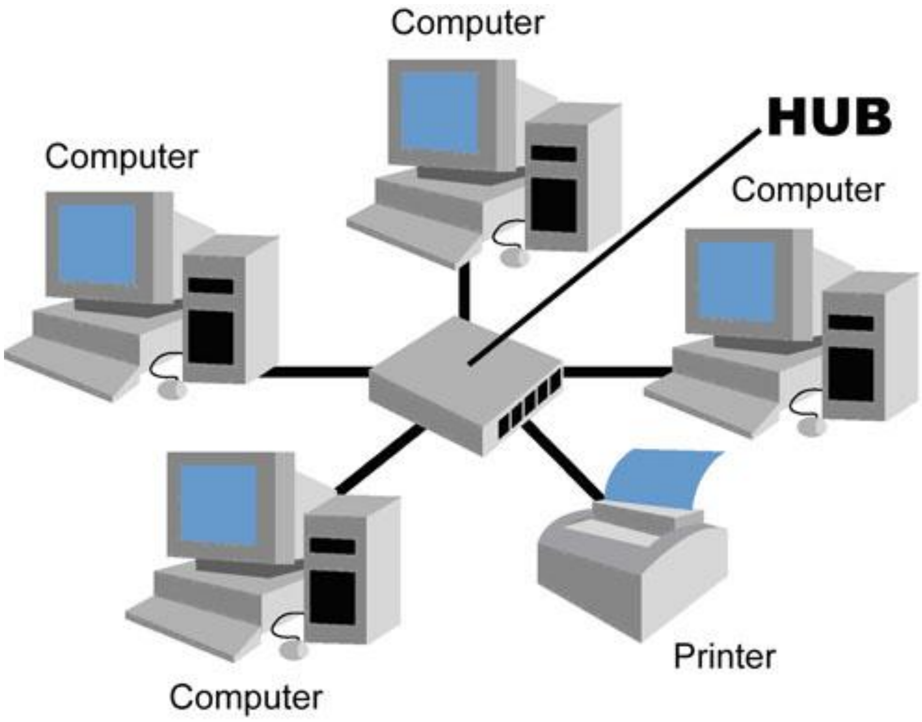
STAR TOPOLOGY



This factor also makes it easy to install and reconfigure.

Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

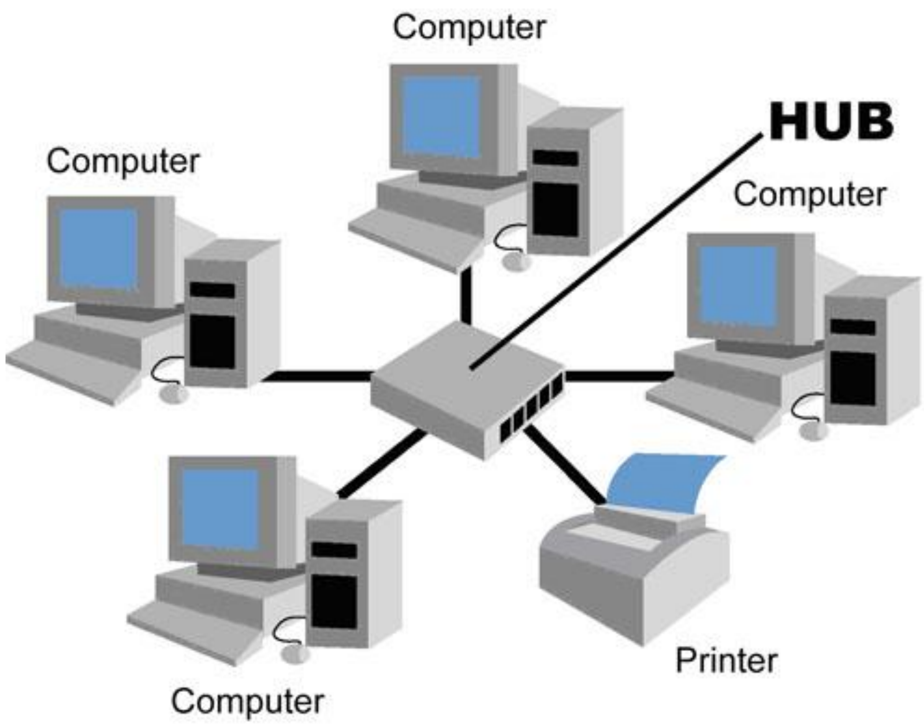
STAR TOPOLOGY



- 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.

STAR TOPOLOGY



- Although a star requires far less cable than a mesh, each node must be linked to a central hub.

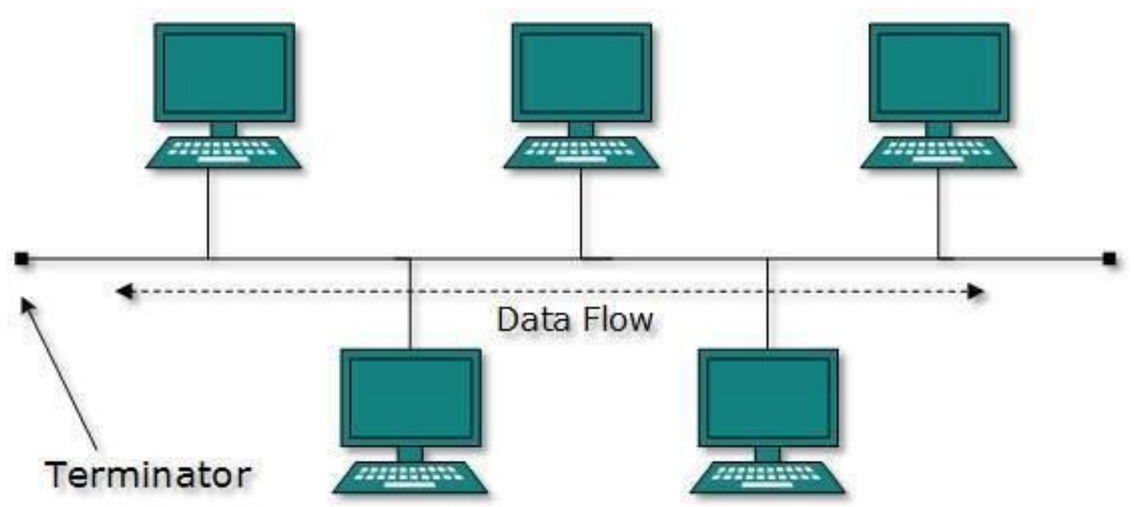
  For this reason, often more cabling is required in a star than in some other topologies (such as the ring or bus topology).

BUS TOPOLOGY

- The mesh and star topologies all describe point-to-point connections.

- A ***bus topology***, on the other hand, is multipoint. One long cable acts as a backbone or trunk line to link all the devices in a network.

- Only one workstation can transmit at any one time but there can be several receivers at any one time (multicasting or broadcasting).

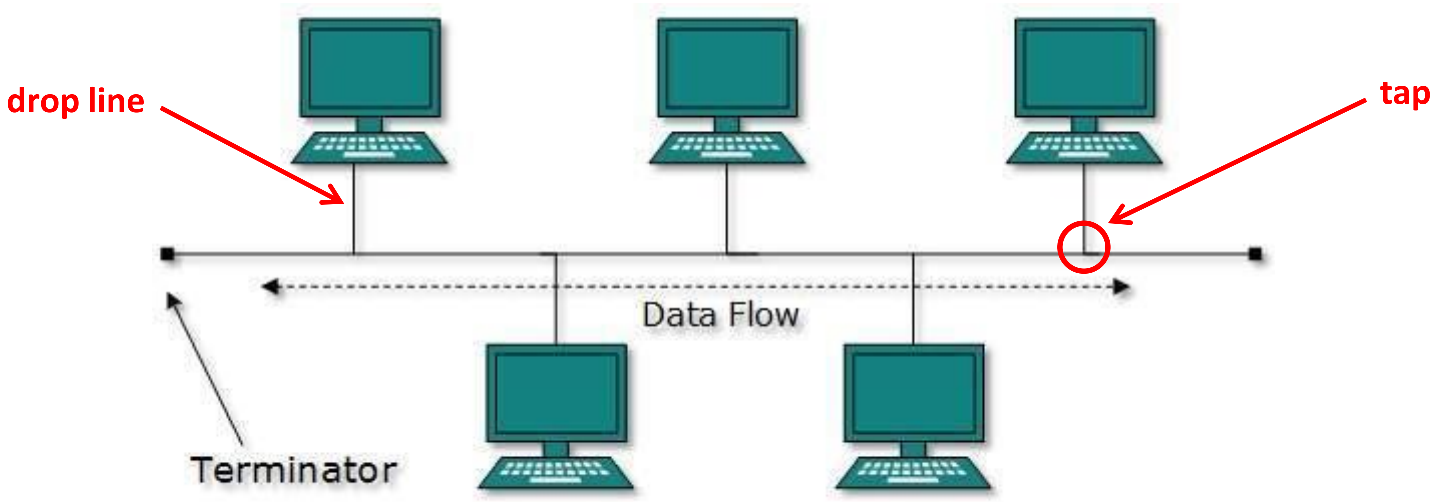


BUS TOPOLOGY

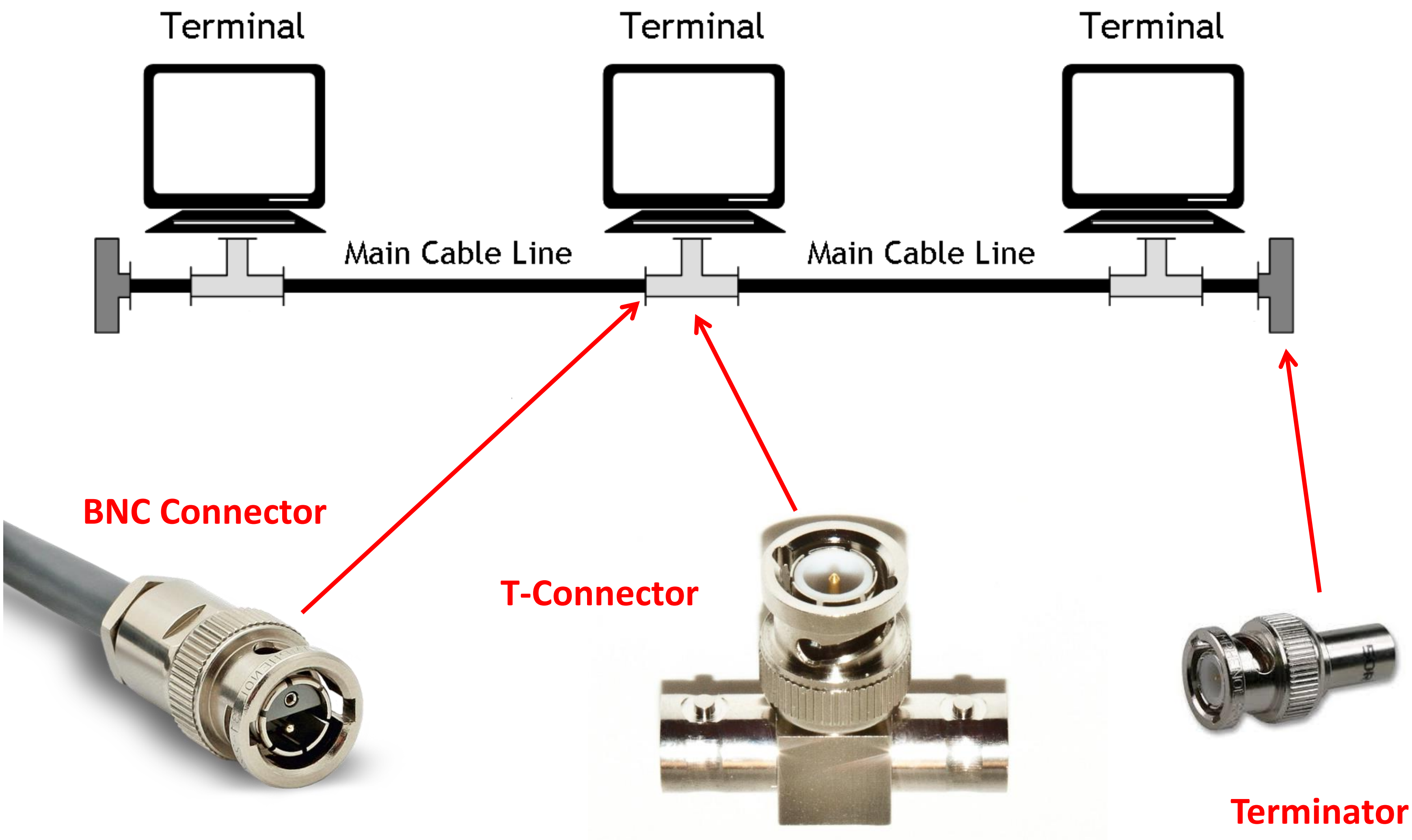
- Nodes are connected to the bus cable by ***drop lines*** and ***taps***.

  A drop line is a connection running between the device and the main cable.

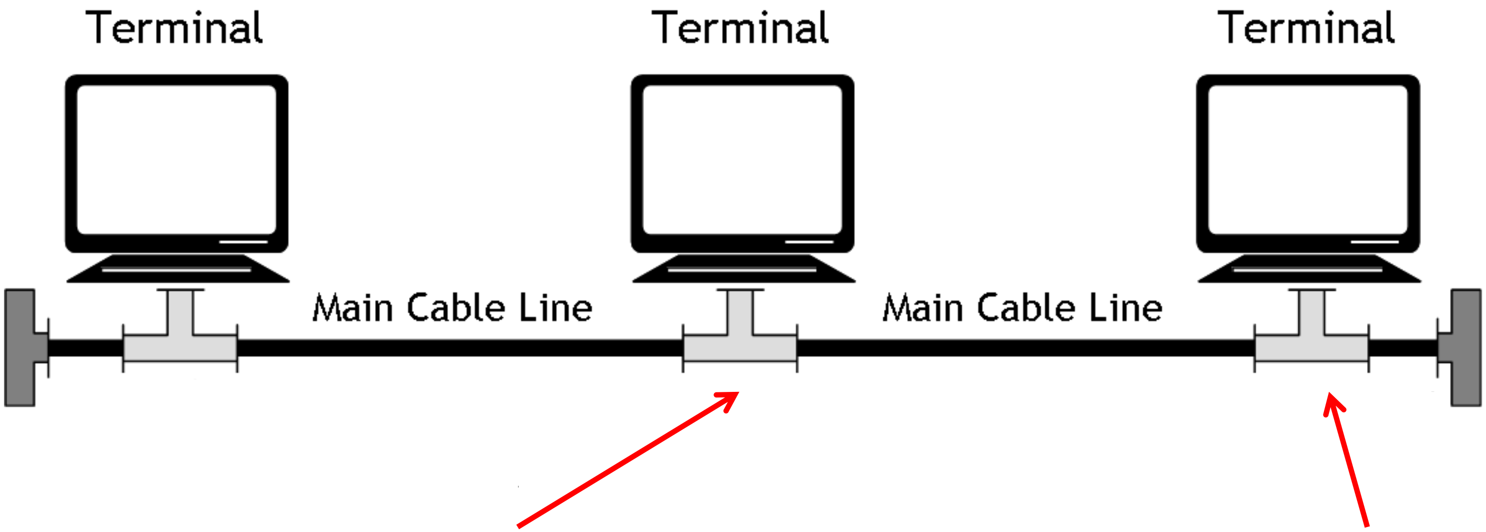
  A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.



BUS TOPOLOGY



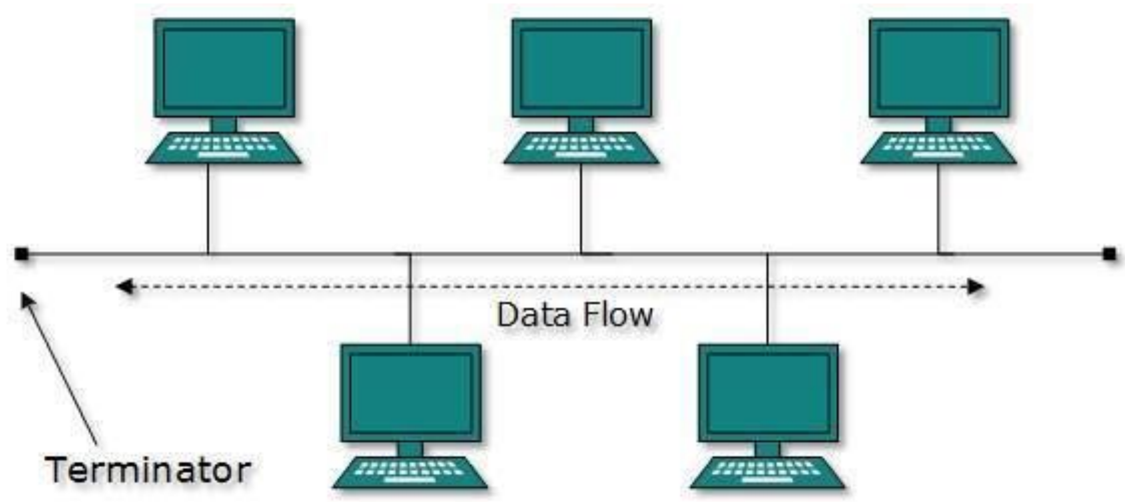
BUS TOPOLOGY



BUS TOPOLOGY

- 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. This is called ***attenuation*** (fading or weakening of a signal)

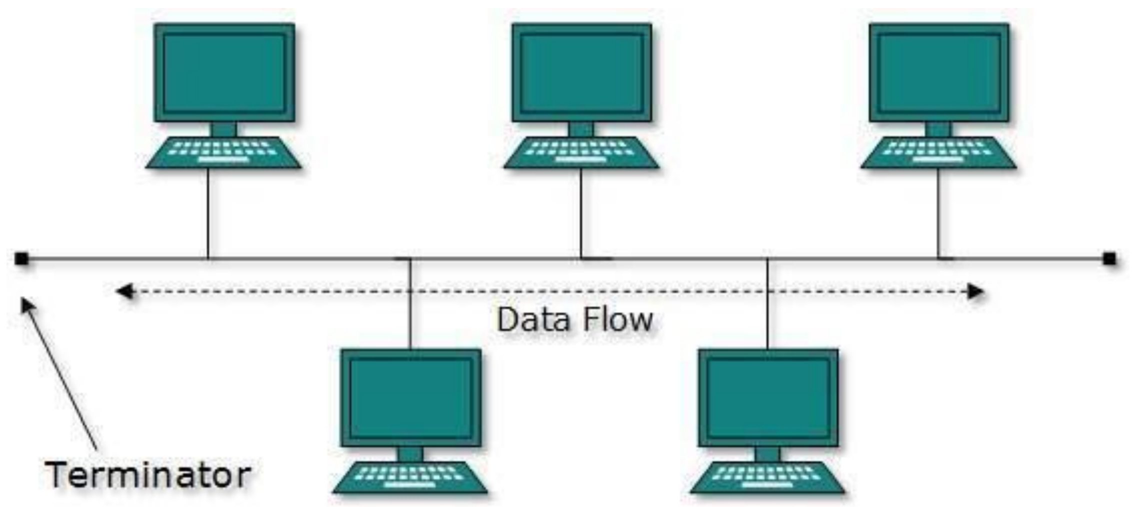
  For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



BUS TOPOLOGY

- 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.

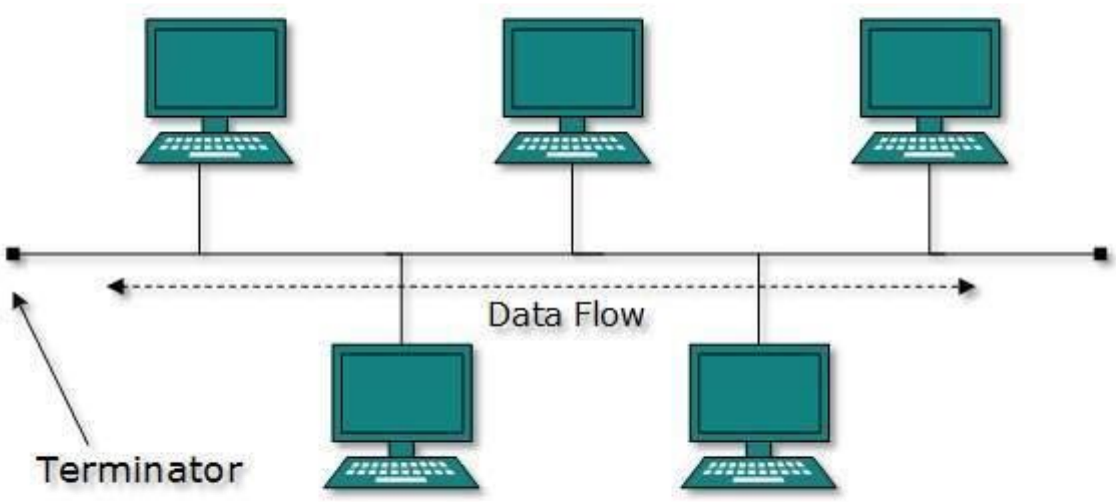


BUS TOPOLOGY

- In this way, bus networks make use of the least cable lengths resulting to relatively cheaper implementations.

  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.



BUS TOPOLOGY

- Disadvantages include difficult reconnection and fault isolation.

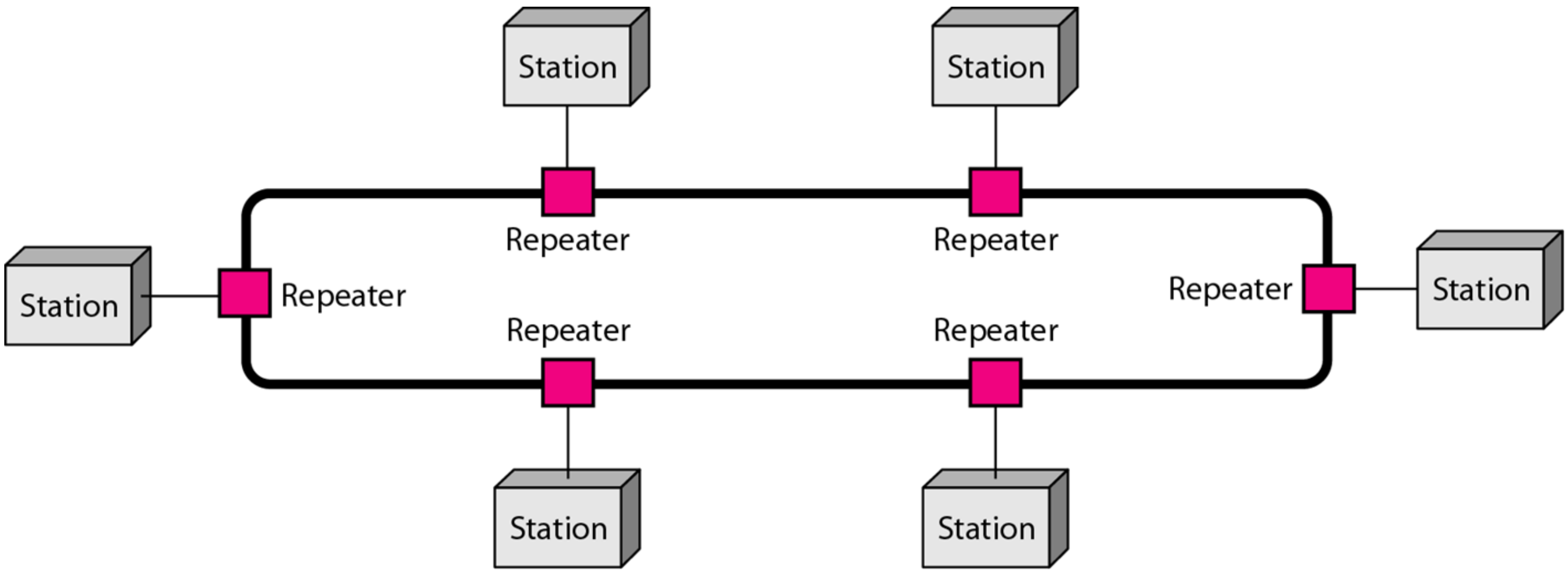
  A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Adding new devices may therefore require modification or replacement of the backbone.

  A break in the cabling anywhere on a bus layout will cause the entire network to fail and fault diagnosis and isolation are difficult.

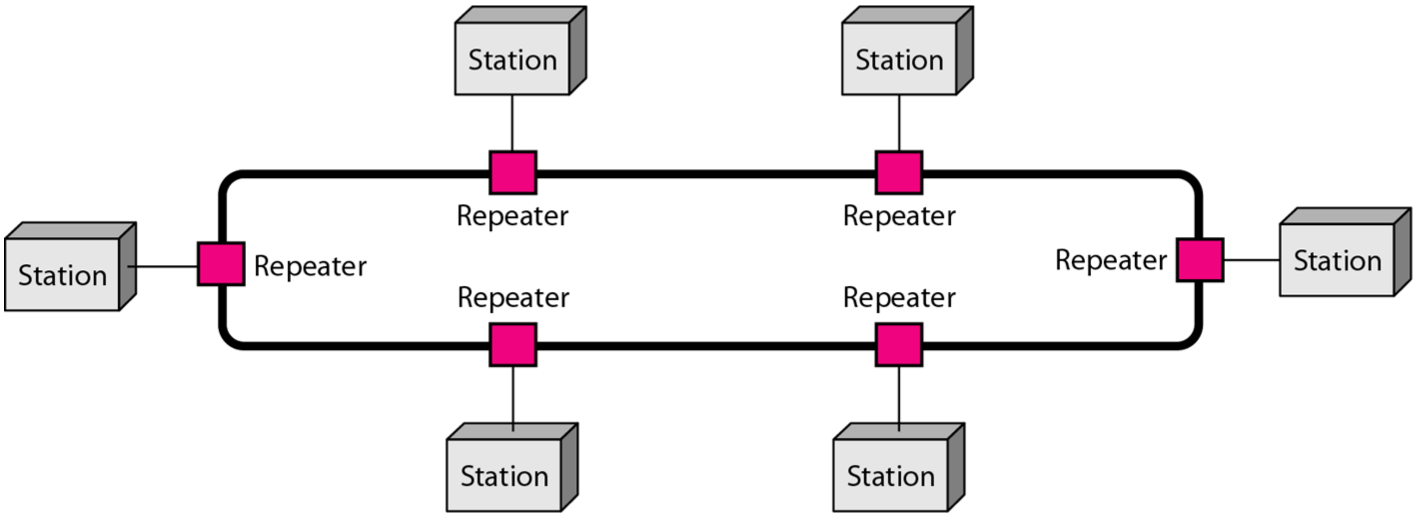
  And since the trunk is shared by several devices, it can also be a bottleneck when network traffic is heavy.

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.



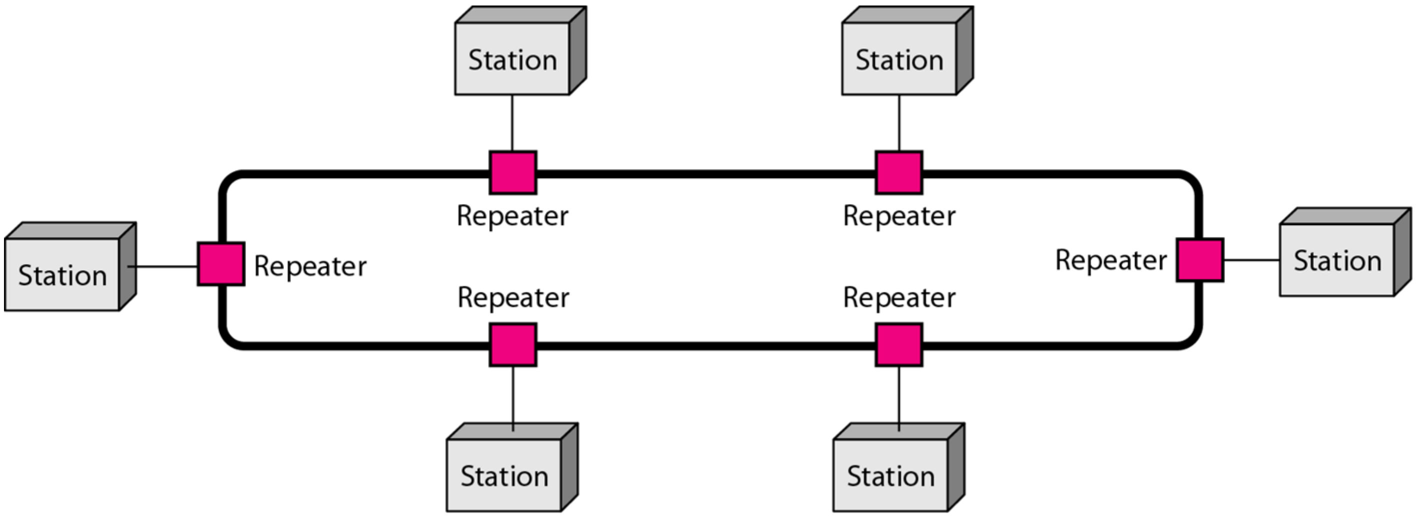
RING TOPOLOGY



- A signal is passed along the ring in one direction, from device to device, until it reaches its destination.

- Messages flow back to the sender (this permits verification that a message was received).

RING TOPOLOGY



- 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.

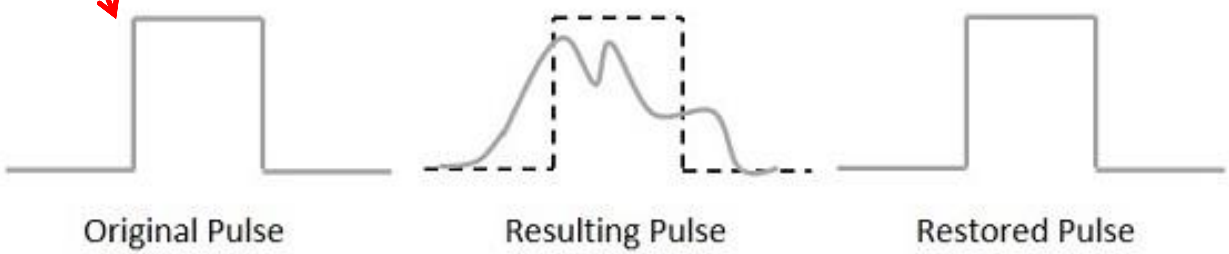
  Regenerating a signal means that the signal is received and rebuilt to its original strength and shape

RING TOPOLOGY

- How Repeaters Work

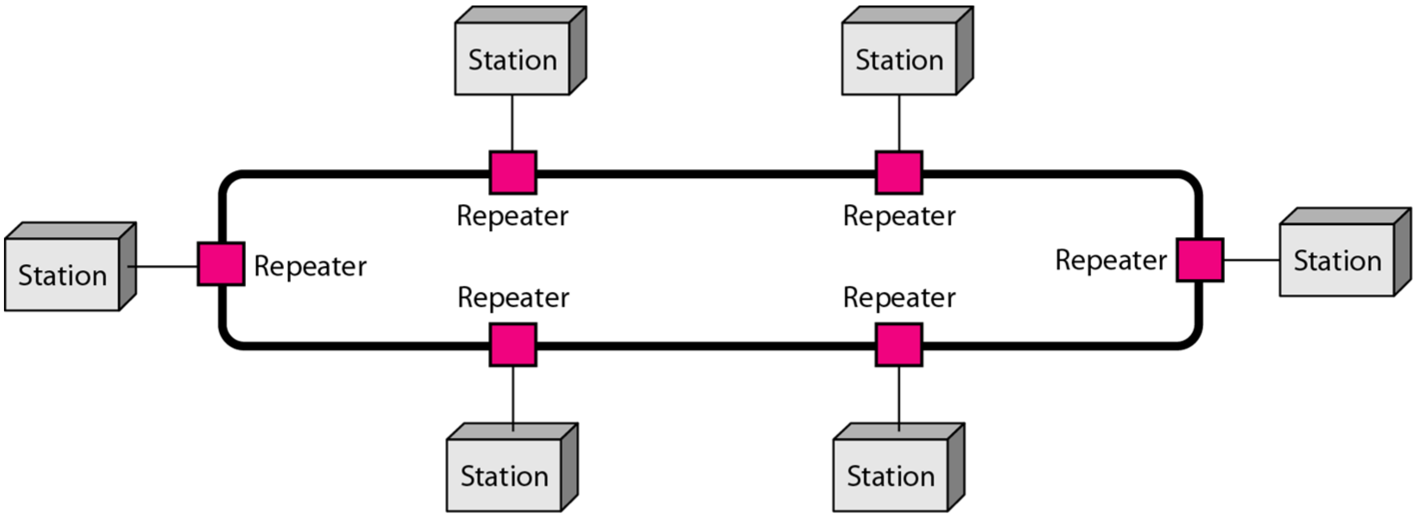
signal transmitted by the source device

signal after being regenerated by a repeater



signal after travelling some distance away from the source

RING TOPOLOGY

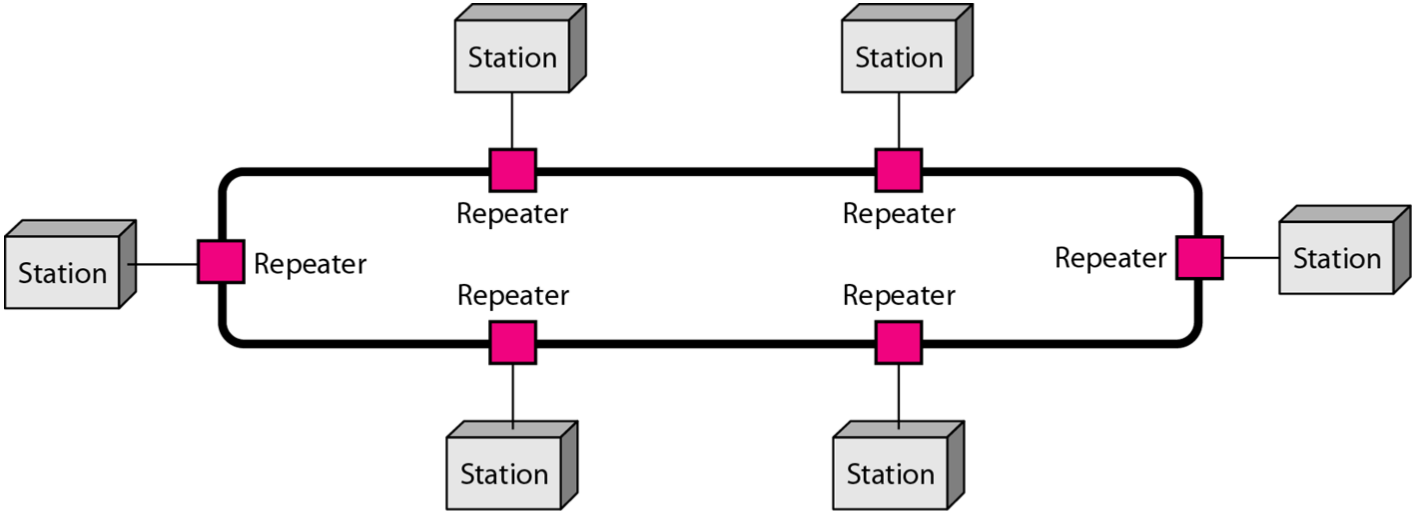


- A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically).

  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.

RING TOPOLOGY

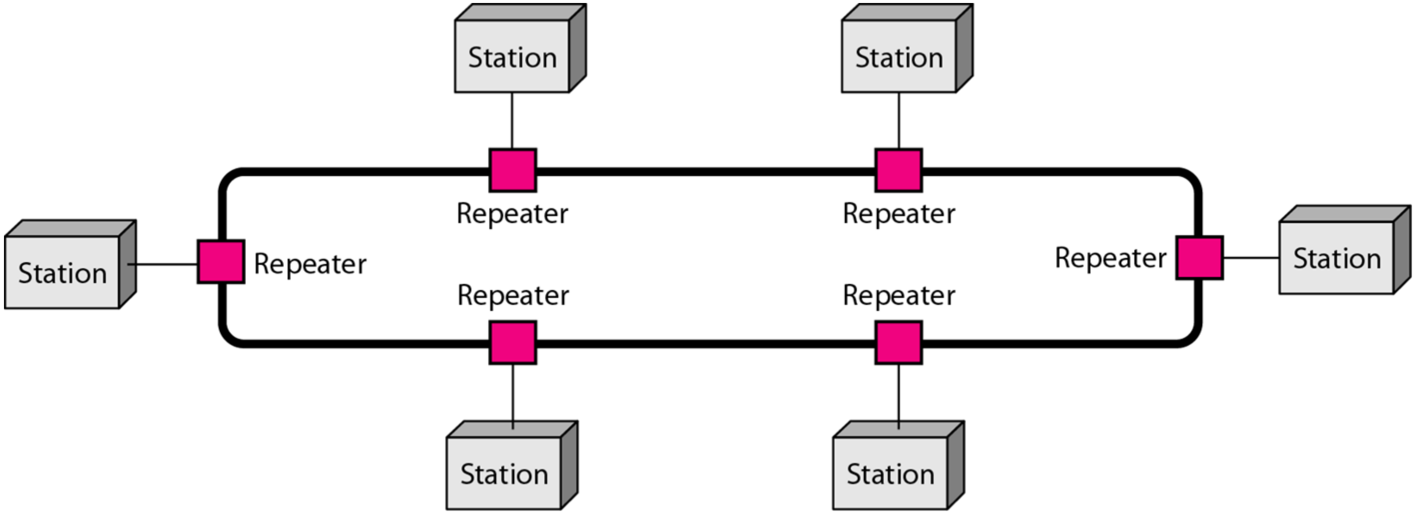


- Generally in a ring, a signal is circulating at all times.

  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.

RING TOPOLOGY



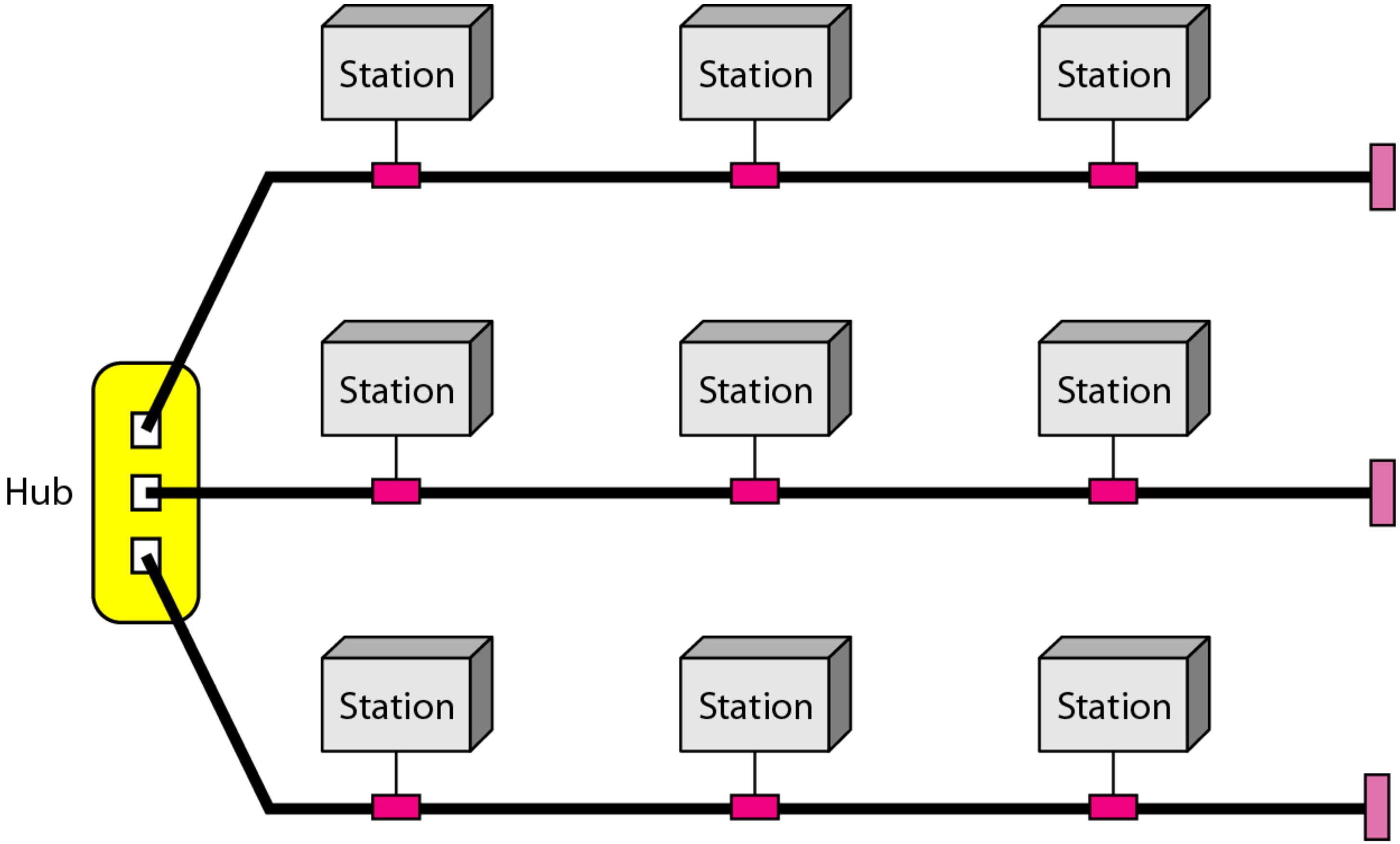
- However, unidirectional traffic can be a disadvantage.

  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.

HYBRID TOPOLOGY

- Example of a hybrid topology: a star backbone with three bus networks



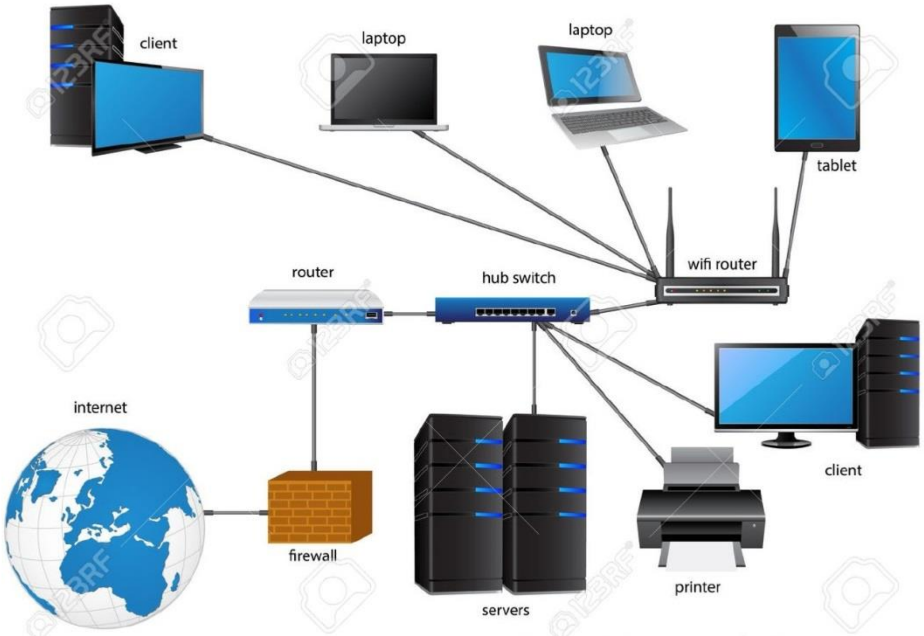
TYPES OF COMPUTER NETWORKS

- A ***Local Area Network*** (LAN) is a privately owned computer network covering a small geographical area, like a home, office, or campus.

  In other words, the size of LANs is usually small.

  The various devices in a LAN are connected to central devices called hubs or switches using cables.

  Many LANs today are even wireless.

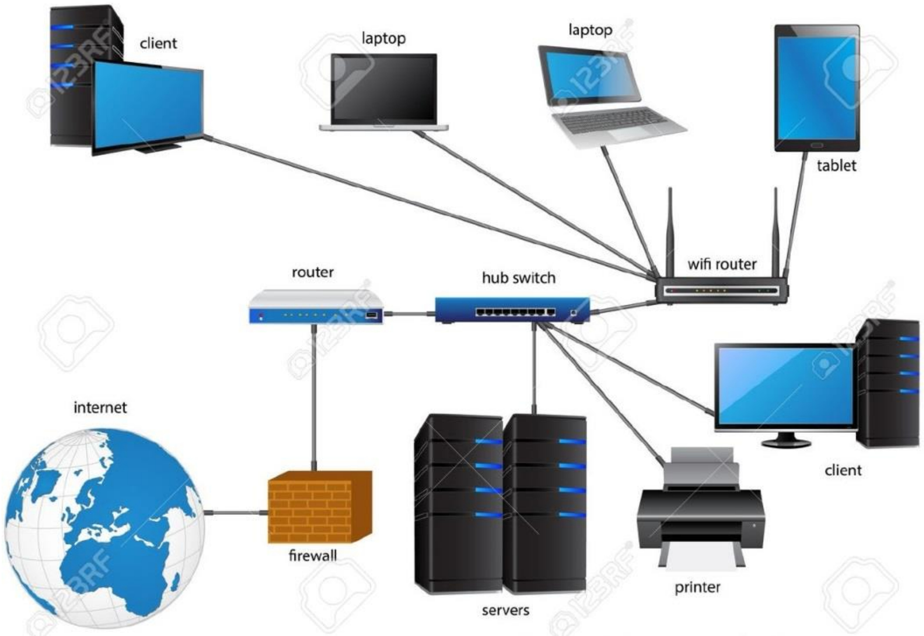


TYPES OF COMPUTER NETWORKS

LAN offers high speed communication of data rates of 10 to 1,000 megabits per second (Mbps).

The current IEEE standard for Ethernet LANs can reach speeds up to 2.5 Gbps and 5 Gbps.

They also have projects investigating the standardization of 10 Gbps and even 40 Gbps.



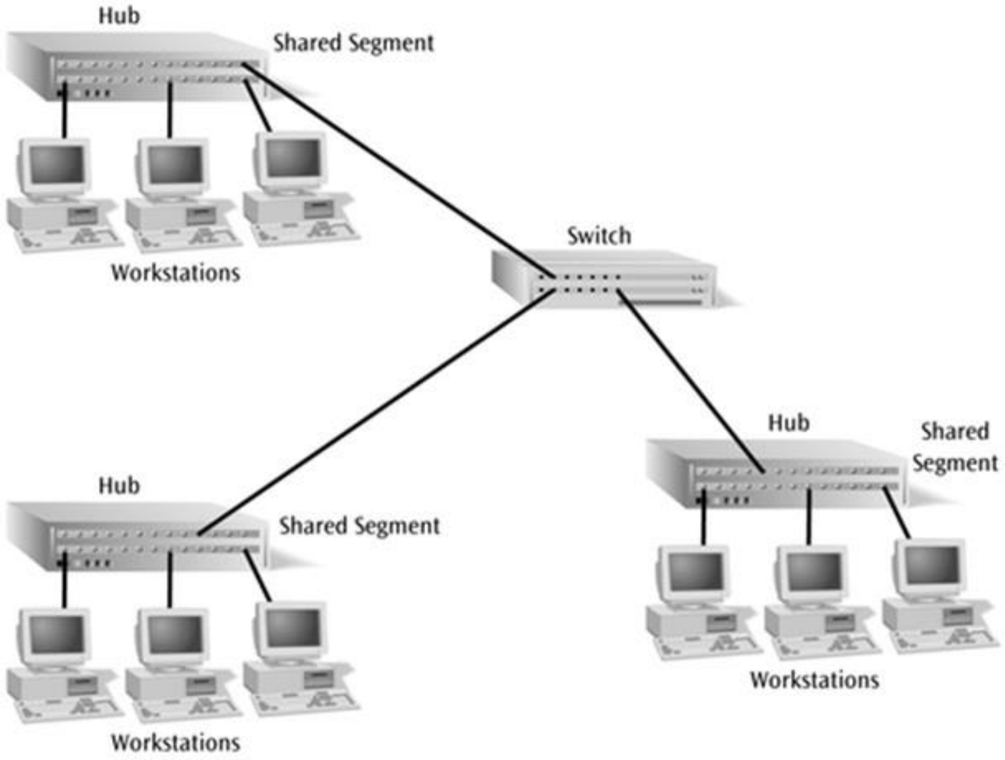
TYPES OF COMPUTER NETWORKS

Several LANs can be connected to one another. This is called ***internetworking***. When two or more networks are connected, they make an ***internetwork***, or ***internet***.

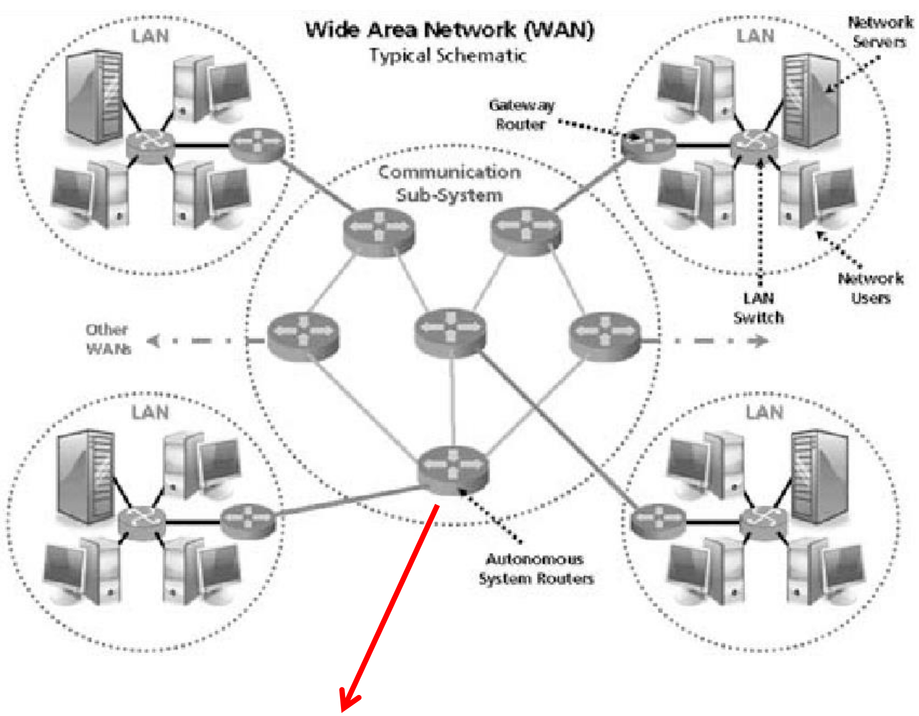
This is done by using network connectivity devices such as a ***switch***.

A switch is able to handle the data and knows the specific addresses to send the message.

It can decide which computer is the message intended for and send the message directly to the right computer.



TYPES OF COMPUTER NETWORKS



Router – an internetworking device that routes data to other networks until that data ultimately reaches its destination.

- A ***wide area network*** (WAN) is also an interconnection of devices capable of communication.

  A WAN has a wider geographical span, spanning a town, a state, a country, or even the world.

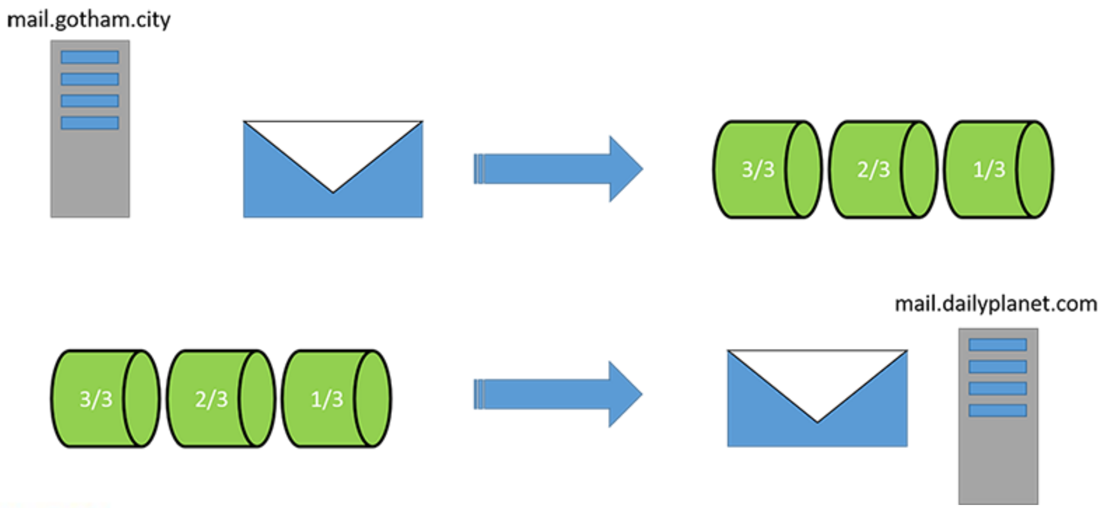
  A LAN interconnects hosts; a WAN interconnects connecting devices such as switches or routers.

  A LAN is normally privately owned by the organization that uses it; a WAN is normally created and run by communication companies and leased by an organization that uses it.

TYPES OF COMPUTER NETWORKS

- In a WAN, a message is divided into parts of a certain size in bytes (typically 1,000 or 1,500 bytes). These are called the ***packets***. Such a network is called a ***packet-switched network***.

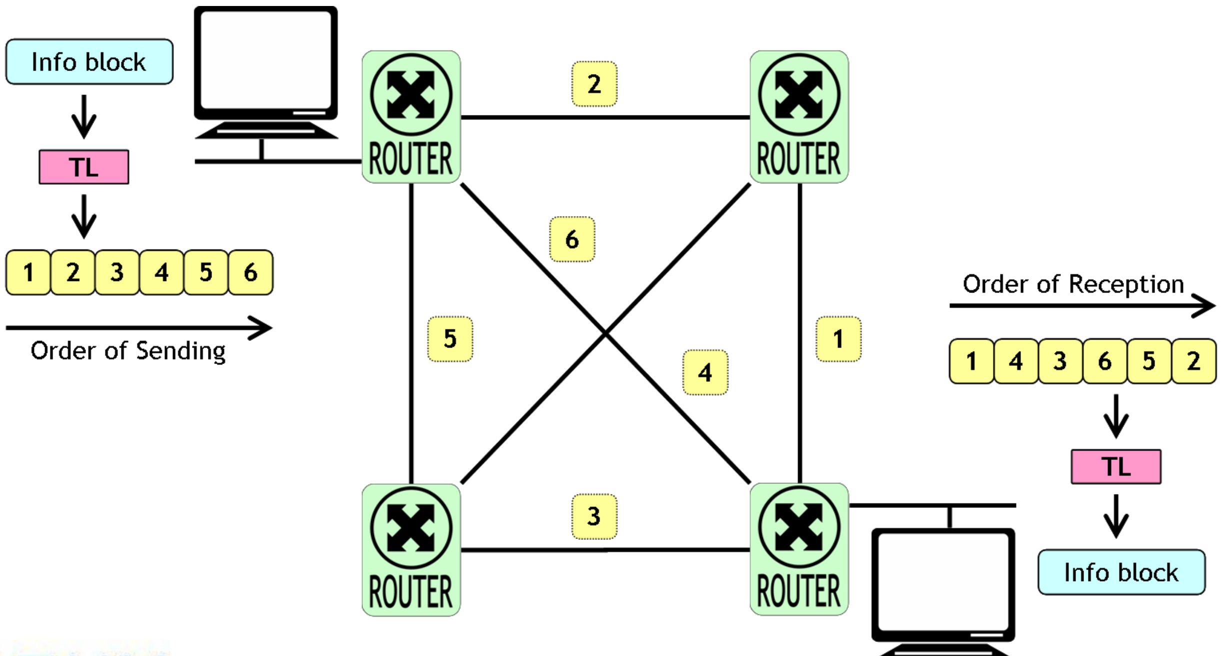
  Each packet carries the information that will help it get to its destination – (1) the sender's address, (2) the intended receiver's address, (3) something that tells the network how many packets this message has been broken into and (4) the number of this particular packet.



TYPES OF COMPUTER NETWORKS

- The packets are then sent off to their destination.

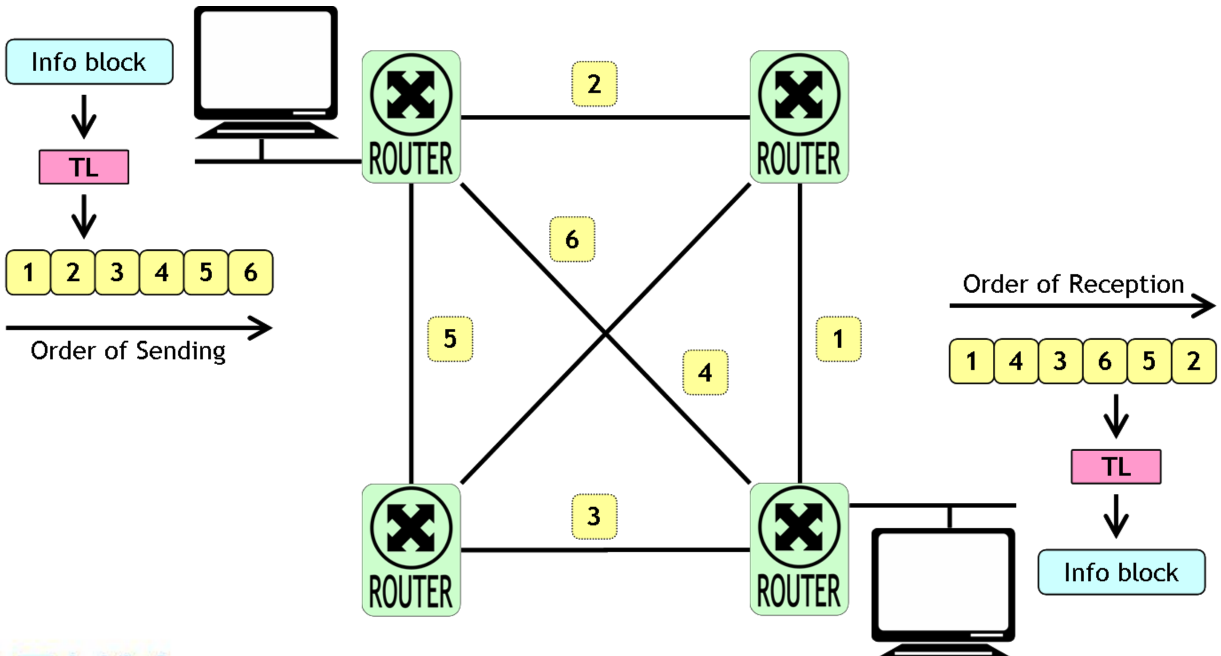
  However, each packet may follow different routes to the destination.



TYPES OF COMPUTER NETWORKS

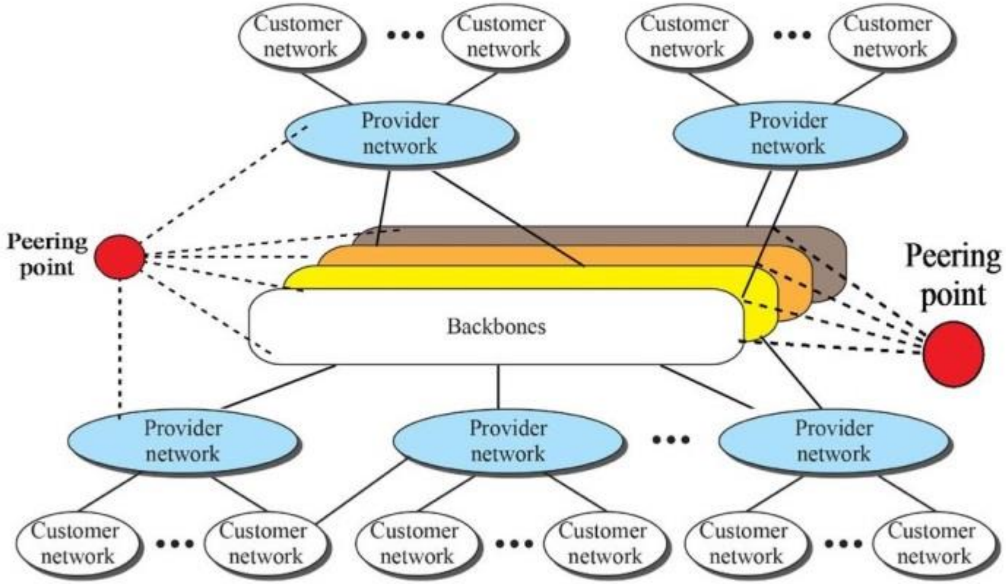
- This makes the network more efficient. The network can balance the load across various pieces of equipment on a millisecond-by-millisecond basis.

  And if there is an error in one of the packets, only that packet will have to retransmitted instead of the entire message.



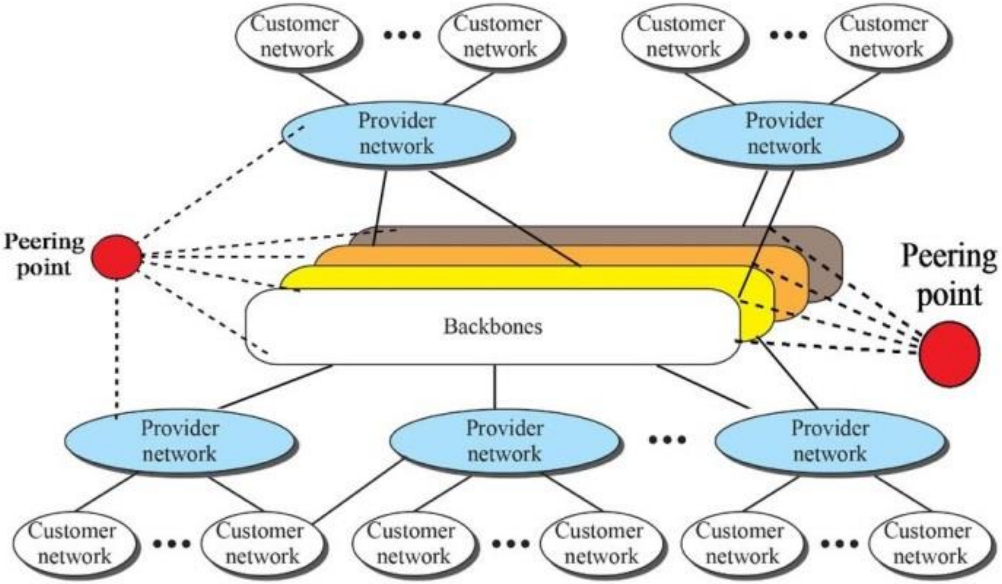
THE INTERNET

- As mentioned earlier, an internet (note the lowercase *i*) is two or more networks that can communicate with each other.
- The most notable internet is called the ***Internet*** (uppercase *I*), and is composed of thousands of interconnected networks.
- The Internet has several backbones, provider networks, and customer networks.



THE INTERNET

- At the top level, the backbones are large networks owned by some communication companies such as Sprint, Verizon (MCI), AT&T, and NTT.
- The backbone networks are connected through some complex switching systems, called ***peering points***.

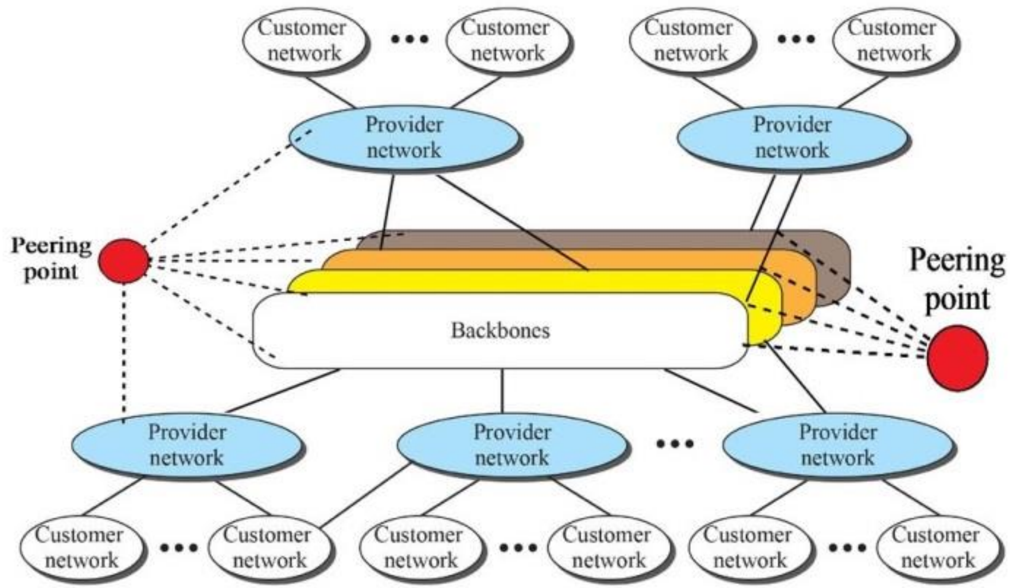


THE INTERNET

- At the second level, there are smaller networks, called ***provider networks***, that use the services of the backbones for a fee.

- The provider networks are connected to backbones and sometimes to other provider networks.

- The customer networks are networks at the edge of the Internet that actually use the services provided by the Internet. They pay fees to provider networks for receiving services.

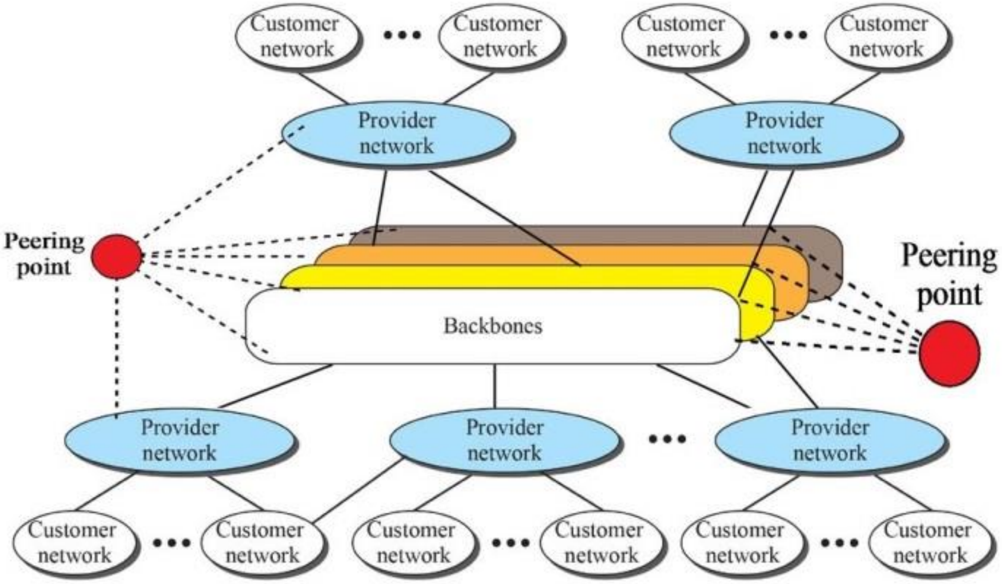


THE INTERNET

- Backbones and provider networks are also called ***Internet Service Providers*** (ISPs).

- The backbones are often referred to as ***International ISPs***.

- And the provider networks are often referred to as ***national*** or ***regional ISPs***.



THE HISTORY OF THE INTERNET

- In the mid-1960s, mainframe computers in research organizations were stand-alone devices.

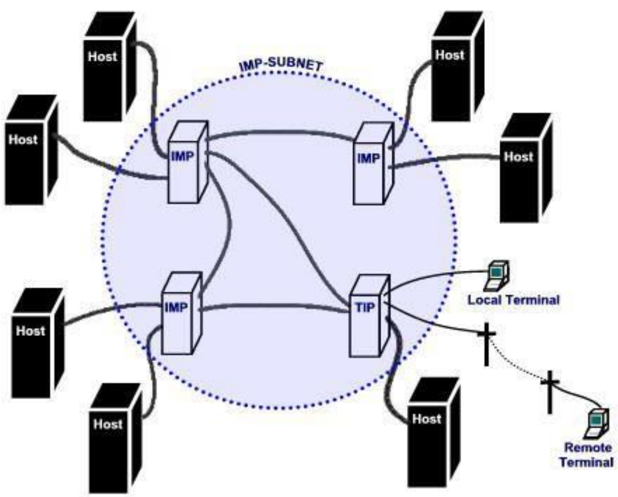
- Computers from different manufacturers were unable to communicate with one another.

- The Advanced Research Projects Agency (ARPA) in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.

ARPA

ADVANCED RESEARCH PROJECTS AGENCY

THE HISTORY OF THE INTERNET



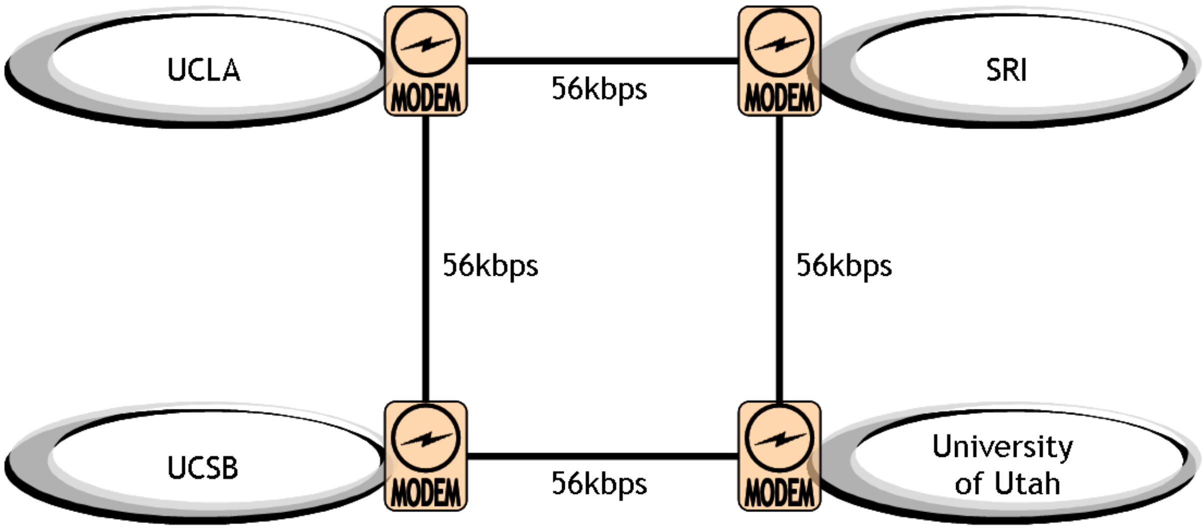
- In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for the Advanced Research Projects Agency Network (ARPANET), a small network of connected computers.
- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an ***interface message processor*** (IMP).
- The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN

THE HISTORY OF THE INTERNET

- By 1969, ARPANET was a reality. Four nodes, at the University of California at Los Angeles (UCLA), the University of California at Santa Barbara (UCSB), Stanford Research Institute (SRI), and the University of Utah, were connected via the IMPs to form a network.

- A software called the ***Network Control Protocol*** (NCP) provided communication between the hosts.

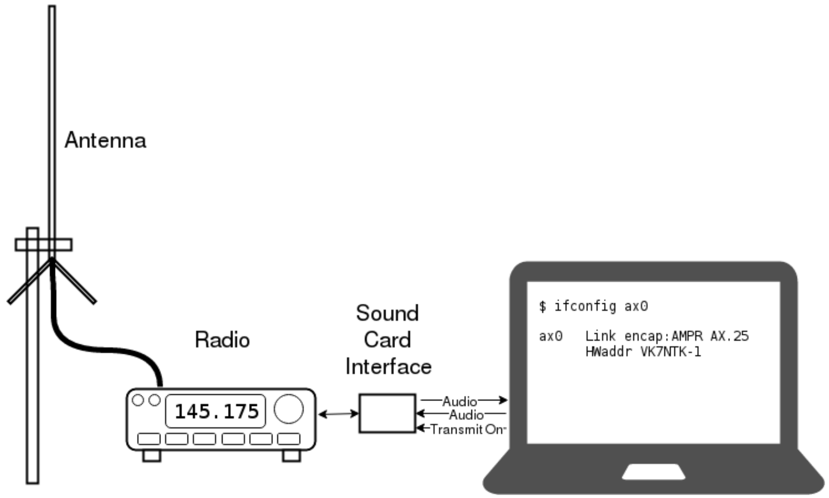


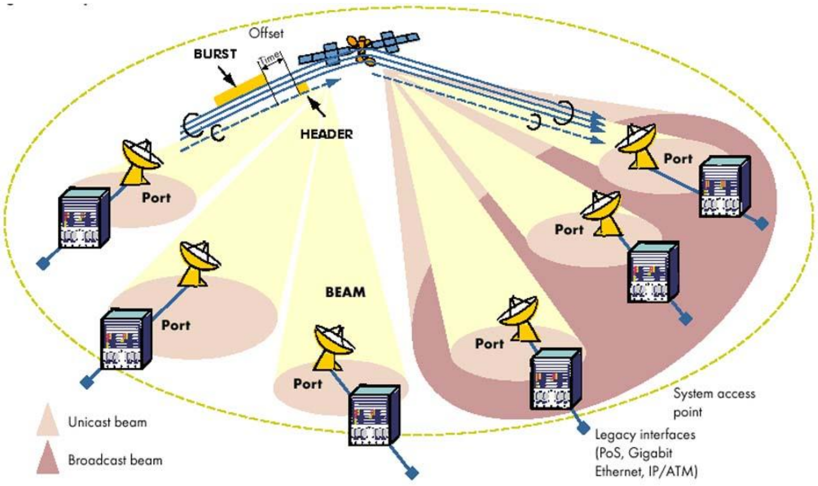
THE HISTORY OF THE INTERNET

- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the ***Internetting Project***.

- But since NCP has several limitations, both started working on a new communications protocol which would later be called TCP/IP (Transmission Control Protocol/Internet Protocol).

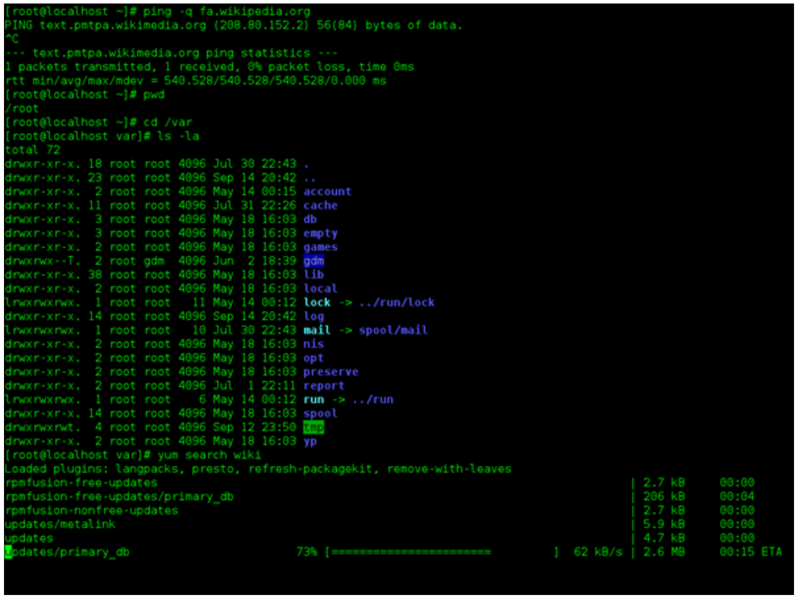
- In October 1977, an internet consisting of three different networks (ARPANET, packet radio, and packet satellite) was successfully demonstrated. Communication between networks was now possible.





iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN

THE HISTORY OF THE INTERNET



- In 1981, under a Defense Department contract, UC Berkeley modified the UNIX operating system to include TCP/IP. This inclusion of network software along with a popular operating system did much for the popularity of internetworking.
- The open (non-manufacturer-specific) implementation of the Berkeley UNIX gave every manufacturer a working code base on which they could build their products.
- In 1983, authorities abolished the original ARPANET protocols, and TCP/IP became the official protocol for the ARPANET.
- Those who wanted to use the Internet to access a computer on a different network had to be running TCP/IP.

iACADEMY
SCHOOL OF COMPUTING • SCHOOL OF BUSINESS • SCHOOL OF DESIGN