INDIAN SCHOOLMUSCAT

CLASS XI

INFORMATION TECHNOLOGY(802)

Chapter - 2 : Networking and Internet

Teacher: Saju Jagannath

Some points to keep in mind…..

- Please avoid login from multiple systems.
- Kindly logout at the end of the session.
- Please turn off your mic and webcam
- If you have any doubt, write in the chat box
- If there is any technical problem, hold on – we will be back
- Since it is a lockdown situation you can use rough notebook or notepad or sheets of paper to take down notes. You may take screenshots during the course of delivery of topics.

Evolution of Networks and Internet continued….

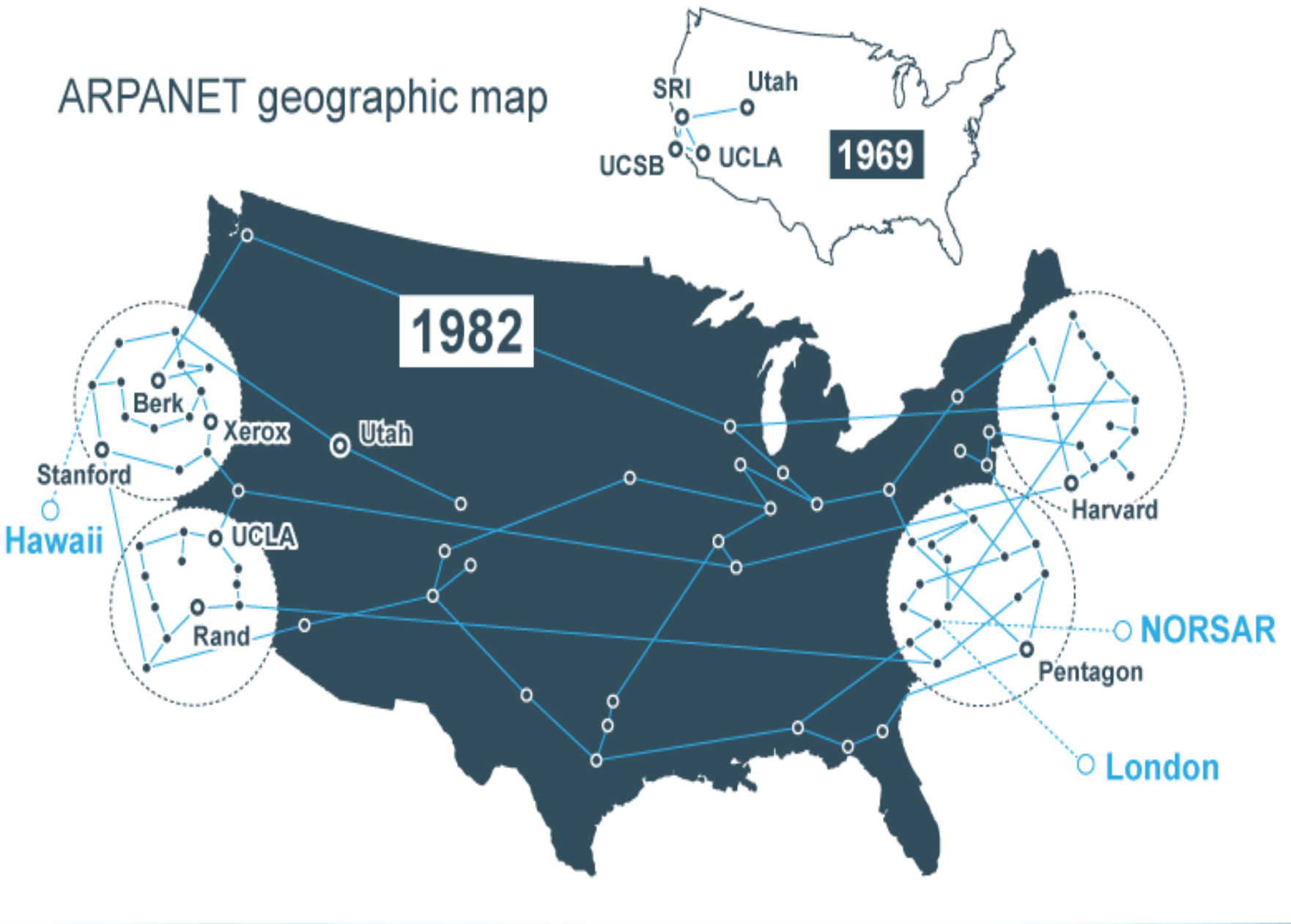
The connection comprised of several intermediary lines and switching offices enroute. They were vulnerable to danger of damage to the switching offices which may disrupt the entire network.

At the peak of cold war, US Department of Defense (DoD) realized the need to establish fault-tolerant network that would not fail at the time of nuclear war and could survive a single point failure in the network.

Evolution of Networks and Internet continued….

US Department of Defense realized the need to connect geographically separated research computers together to form a network. This led to the development of Advanced Research Projects Agency Network (ARPANET) in 1969. Along with several smaller networks, another large network called NSFNET was developed in 1984 by NSF,
U.S. National Science Foundation for research and education purpose.

ARPANET geographic map



Evolution of Networks and Internet continued….

When ARPANET and NSFNET were interconnected, the network growth increased tremendously. TC P/IP protocol (rules for communication) acted as a glue to connect various heterogeneous networks together into a single network. This wide network is an Internet (network of networks).
With the advent of Internet, the whole world got connected on a global level.

Evolution of Networks and Internet continued….

Several government and private organizations, collectively called Internet Service Providers (ISPs) joined hands to provide connectivity for Internet.

Internet made it possible to exchange information and communicate with remote nodes. There are several applications of Internet such as e-mail, file transfer, remote login, and World Wide Web (WWW).

Computer Networks

Nodes or stations are electronic devices such as computers, printers, Fax machines, and telephones which communicate with each other by sending and receiving data/message.

A one-way simple communication system that comprises the following components:

- Sender: The node that is responsible for sending the data.
- Receiver: The node that is responsible for receiving the data.
- Message: Message is the information or meaningful data that is being communicated in a structured form.

Computer Networks continued…..

Channel: Channel is the communication medium through which message is transmitted.

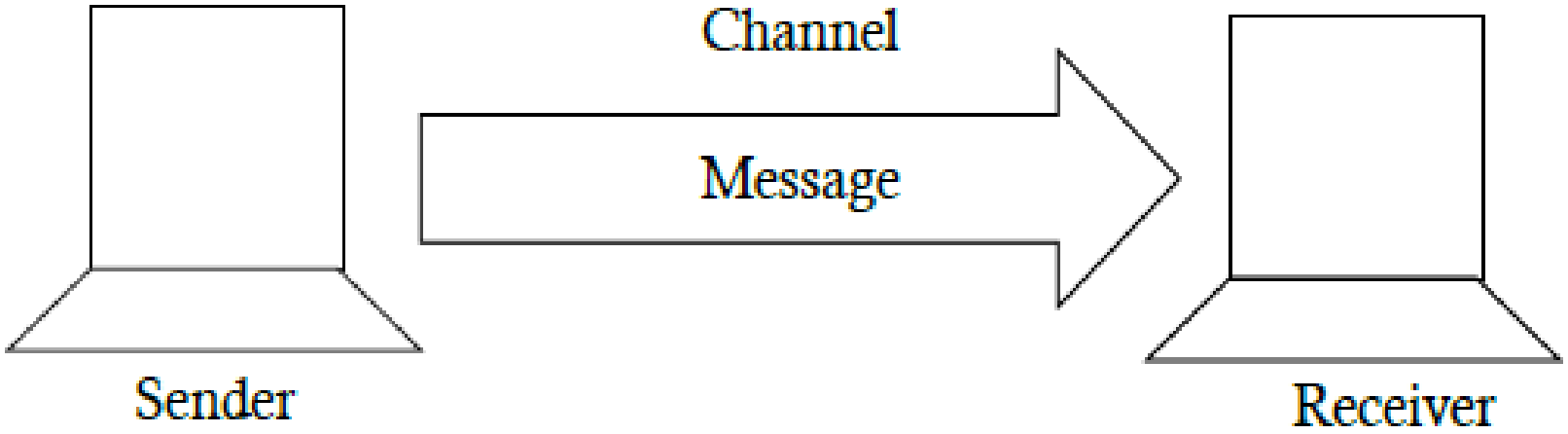


Figure 2.2: One-way Communication System

Computer Networks continued…..

A collection of interconnected nodes which communicate by means of some channel form computer network. The communication taking place in a computer network can be categorized as simplex, half-duplex, and full-duplex.

In simplex mode, information can be transferred only in one direction. This mode is termed unidirectional.

Computer Networks continued…..

In computer networks, the data transmitted using many fiber optics and satellites is simplex in nature. Half-duplex mode is a bidirectional communication between the two nodes, however, only one node at a time can transmit the data. This mode is generally used for transferring files between nodes in a low-bandwidth setting.

Computer Networks continued…..

In full-duplex mode, both communicating parties can send and receive at the same time.

The interactive applications use this mode of communication, thus speeding up the data transfer. NIC (Network Interface Card) on the systems for networking supports full-duplex mode.

Network Interface Card

Why we need a computer network?

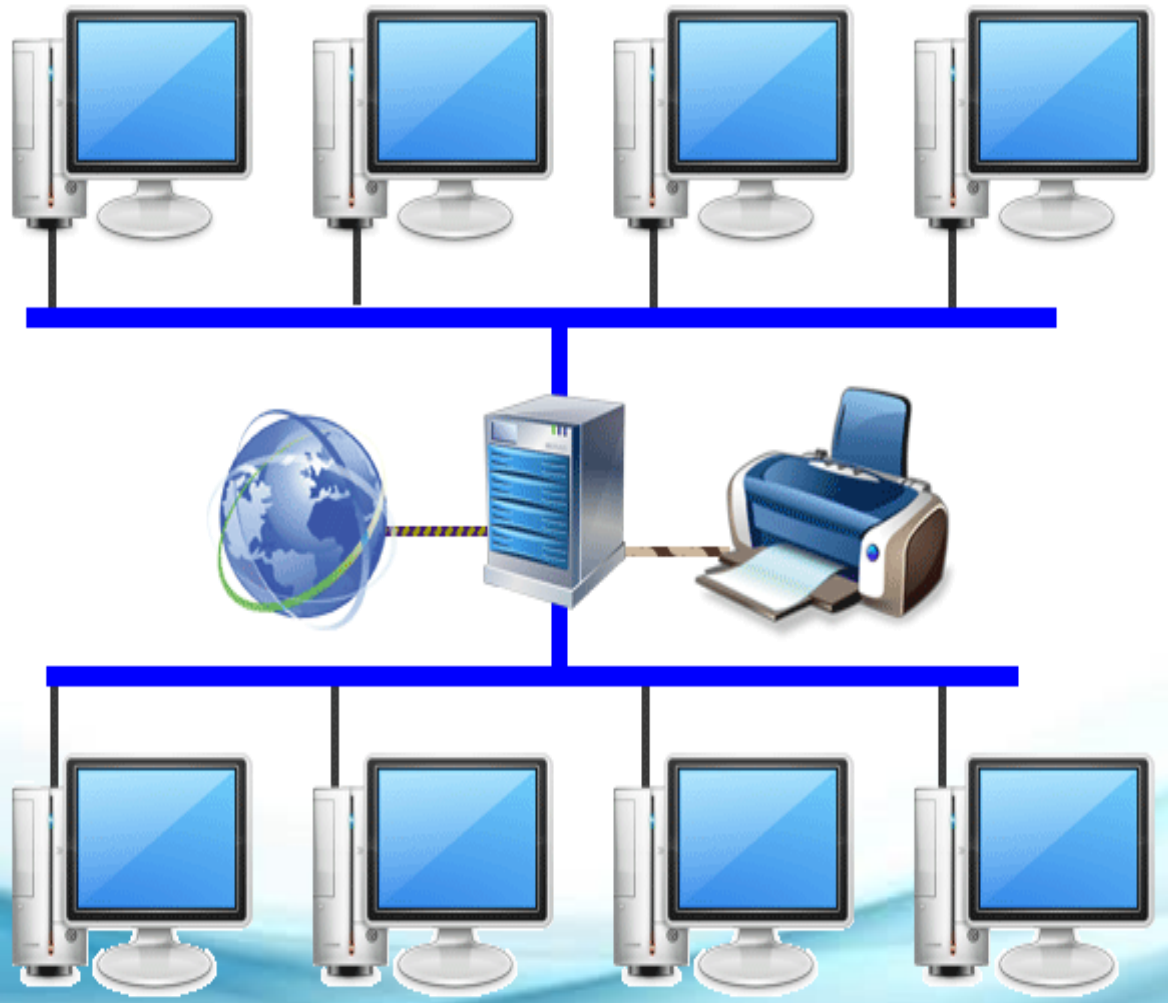
Computer networks can be used as means of resource sharing and communication.

Resource Sharing: Connecting computers through networking allows us to share hardware and software resources. Examples of hardware resources include peripherals (for example, printers and scanners), CPU, and memory. Examples of software resources include system and application software, and files that may include text, audio, and video content.

Need of network continued…..

Communication: Connecting computers through network facilitates exchange of information amongst the nodes in the network.

For example, any of the computer systems may send data to any of the computer systems in the network or the printer, as it is connected in the network.



COMPUTER NETWORK

Various network devices

Creation of a network requires various network devices such as modems, routers, switches and bridges, each of which plays a specific role in the network. Networks differ on the basis of transmission media used, arrangement of nodes in the network, their geographical span, and their purpose.

Transmission Medium

A transmission medium refers to the channel of transmission through which data can be transmitted from one node to another in the form of signal.

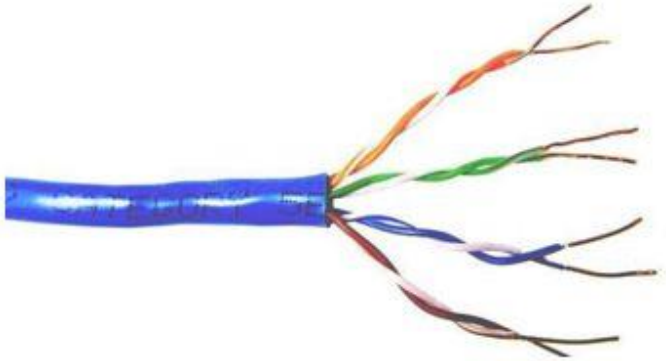
A signal encodes the data in a form suitable for transmission on the medium. A medium is characterized by its bandwidth defining the information carrying capacity of the medium.

A transmission medium may belong to one of the following two categories:

Guided Medium: The term refers to physical conductor such as twisted pair, coaxial cable, and fiber optics.
In twisted pair and coaxial cable, the signal travels as voltage and current signal whereas in optical fiber, the signal is in the form of light.

Common network cable types

- Unshielded twisted pair (UTP)



- Shielded twisted pair (STP)

- Coaxial cable

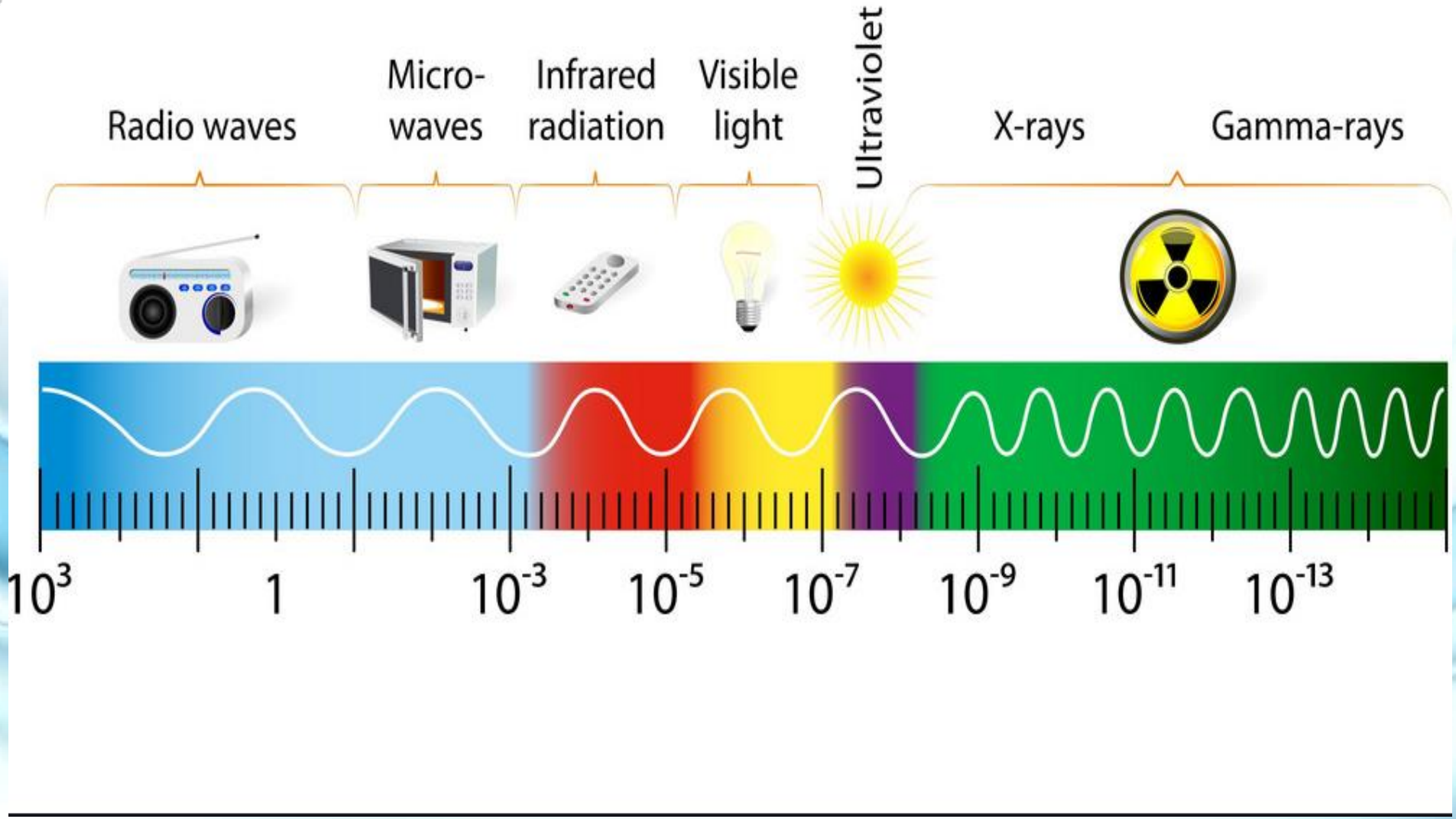
- Fiber optic

Transmission medium continued……

Unguided Medium: The unguided medium uses electro-magnetic waves that do not require a physical conductor.

Examples of unguided medium include infrared, radio, and microwave.

THE ELECTROMAGNETIC SPECTRUM



Topology

The arrangement (also called layout) of nodes in a network is called network topology.

There are broadly two types of topologies – broadcast and point to point.

In broadcast topology, all nodes share the same physical link. When one node transmits, all nodes receive. Collision may occur when more than one node simultaneously transmits,

Topology continued….

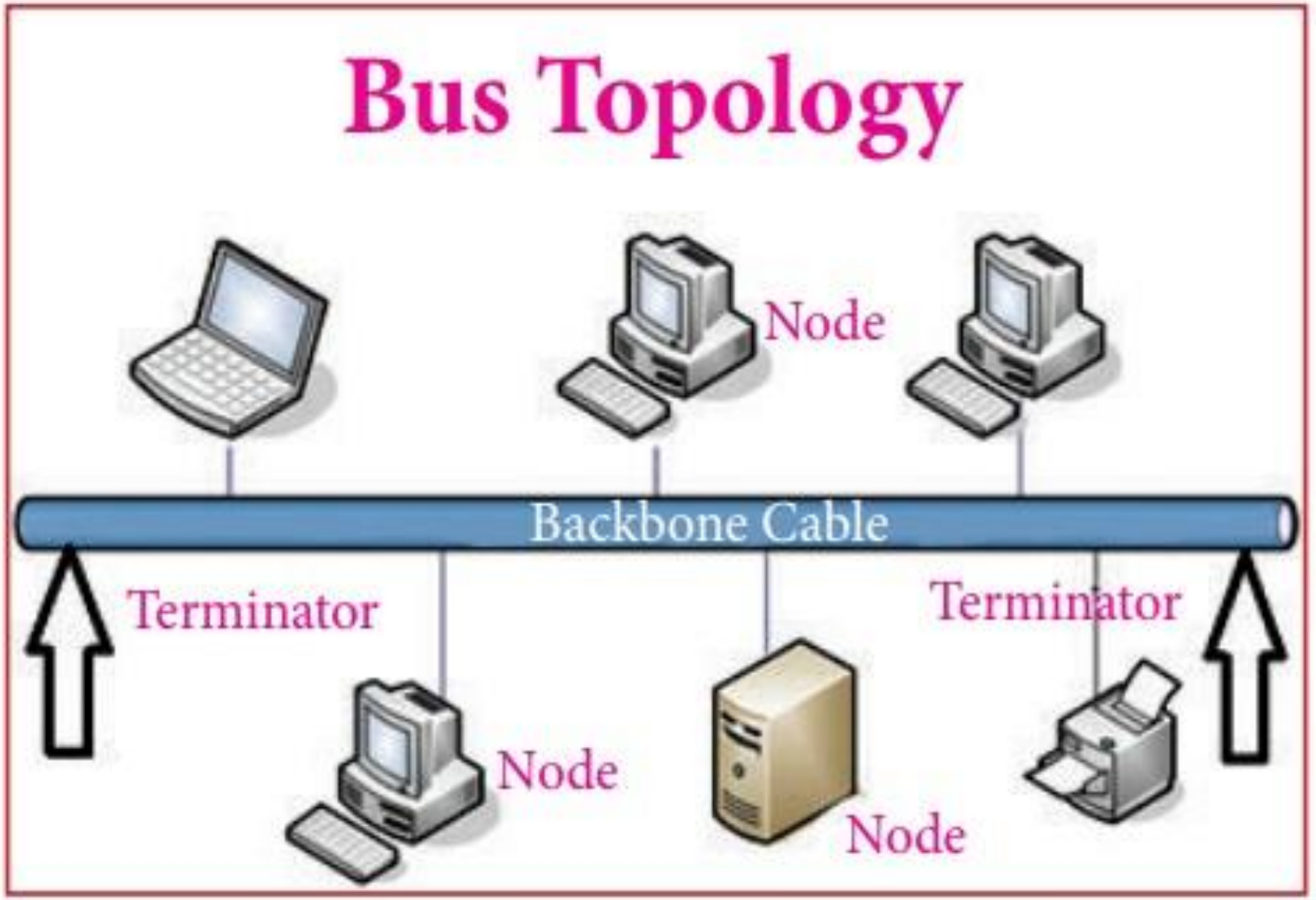
and there is collision resolution mechanism for handling it. Broadcast topologies are mainly bus and ring.

In point to point topology, every pair of nodes has a dedicated link. Popular point to point topologies are star and mesh.

Bus Topology

In bus topology, there is a long cable, called backbone cable (or simply backbone), that connects various nodes through connector called tap.

In this, a message sent by one is received by all devices connected to backbone cable. This topology requires less cabling and is easy to install and extend the network laid using it. However,fault detection and isolation is difficult.


Bus Topology
Node
Backbone Cable
Terminator
Terminator
Node
Node

Ring Topology

In this, a message sent by one is received by all devices connected to backbone cable. This topology requires less cabling and is easy to install and extend the network laid using it. However, fault detection and isolation is difficult.

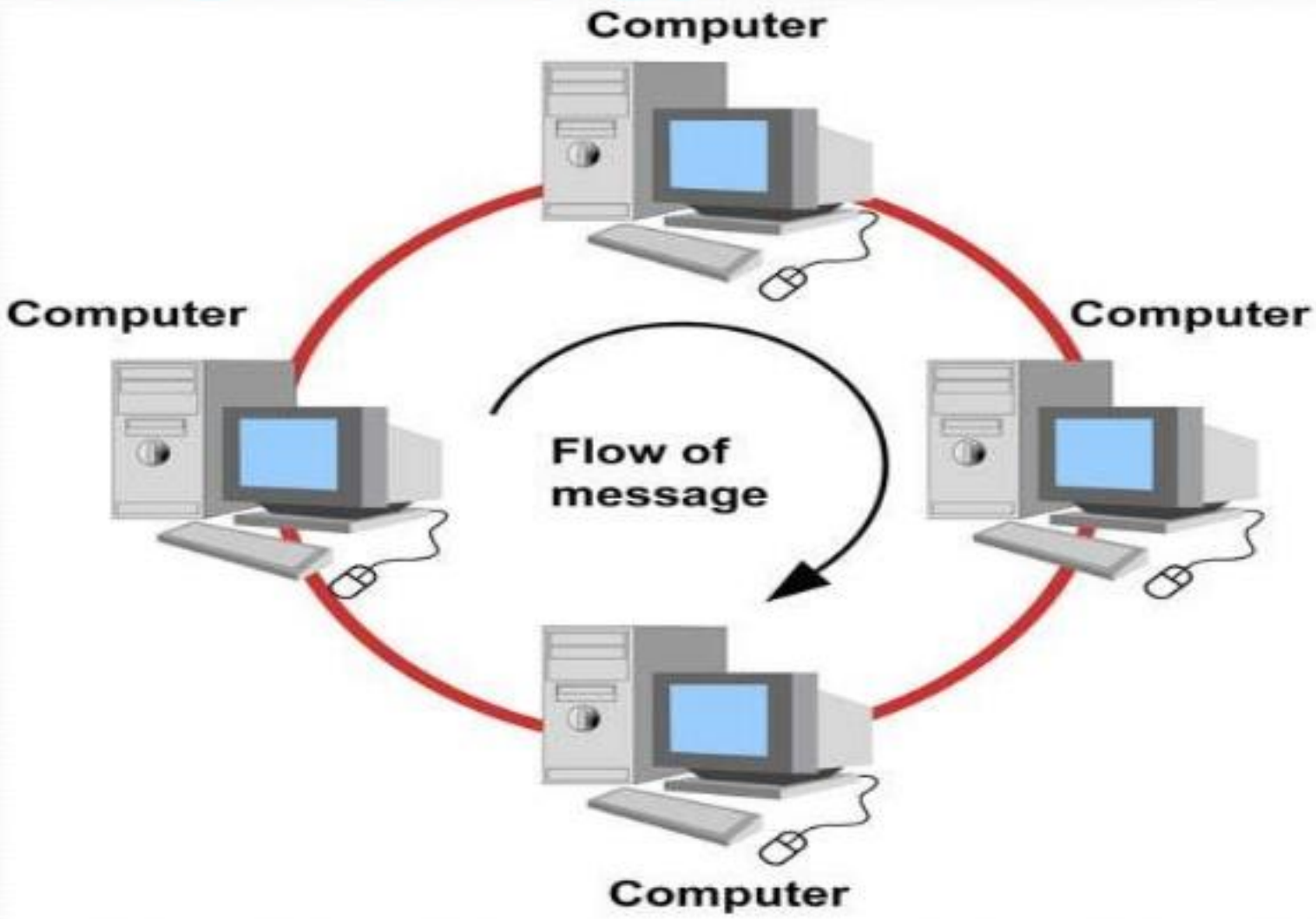
The message to be communicated is transmitted in one direction, thereby, relaying the message to the intended recipient.

Ring Topology continued….

Addition and deletion of devices, and fault detection and isolation is easy.

However, the topology suffers from the limitation of single point failure leading to disruption of entire network. Sending a message from one node to another node may take more time

Ring Topology



Star Topology

In star topology, all the devices are connected to the central controller called hub.

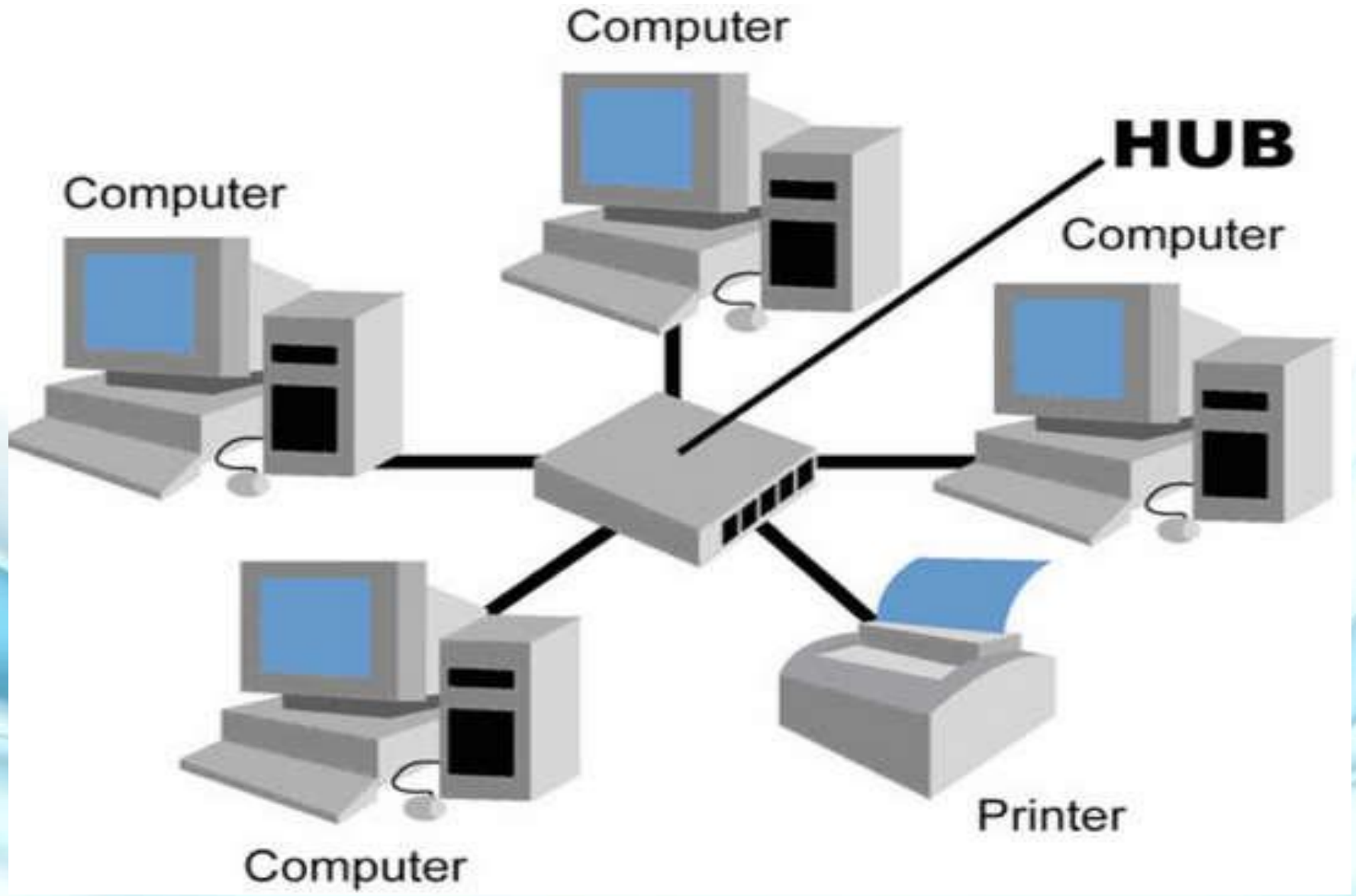
Communication between any two devices takes place through the hub responsible for relaying messages.

Star network can be easily installed and configured.

Also, fault detection and isolation is easy.

However, it requires more cabling as compared to bus and ring topology. Also, hub failure will lead to network failure.

Star Topology

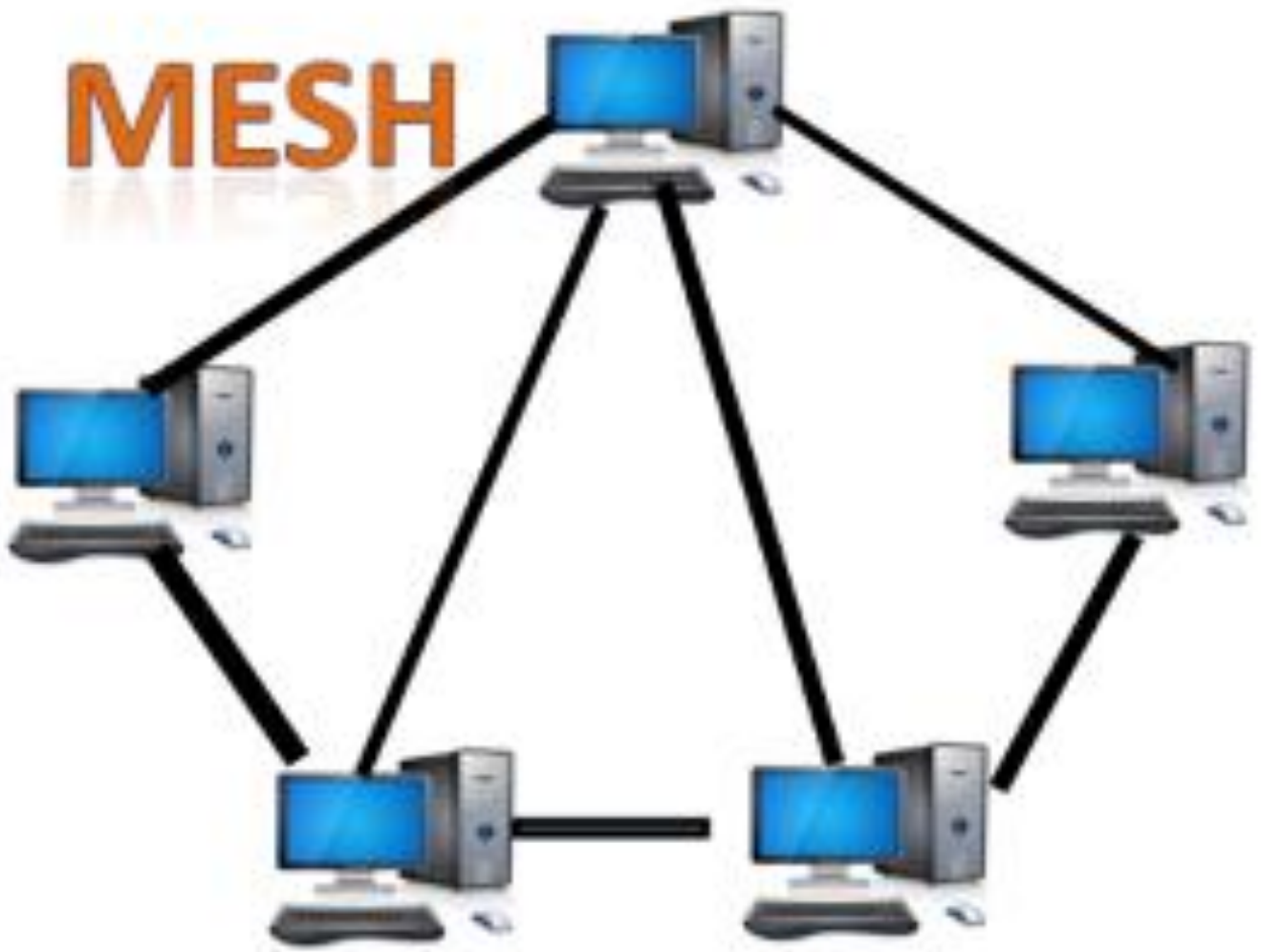


Mesh Topology

In mesh topology, every node is connected with every other node in the network.

Because of dedicated point to point connection between every possible pair of nodes, the topology provides secure data transfer without any traffic problem. It requires a large number of connections establish the topology. This leads to difficulty in installation as the number of nodes grow as the network grows.

Mesh Topology



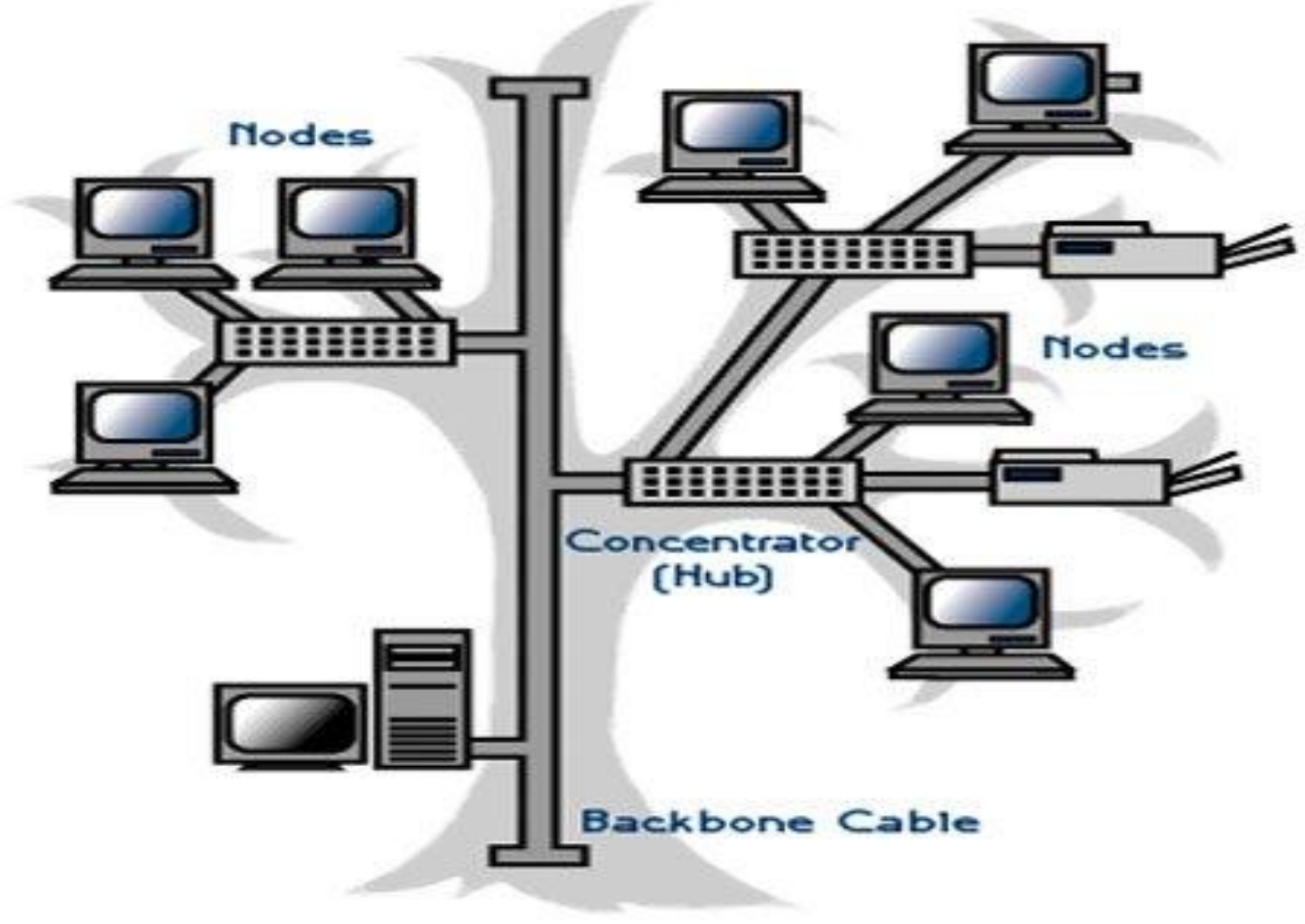
Tree Topology

Tree topology is a hybrid topology using combination of star and bus topology. Backbone cable in a bus topology acts like the stem of the tree, and star networks (and even individual nodes) are connected to the main backbone cable like the branches of tree. Damage to a segment of a network laid using tree topology will not affect other segments.

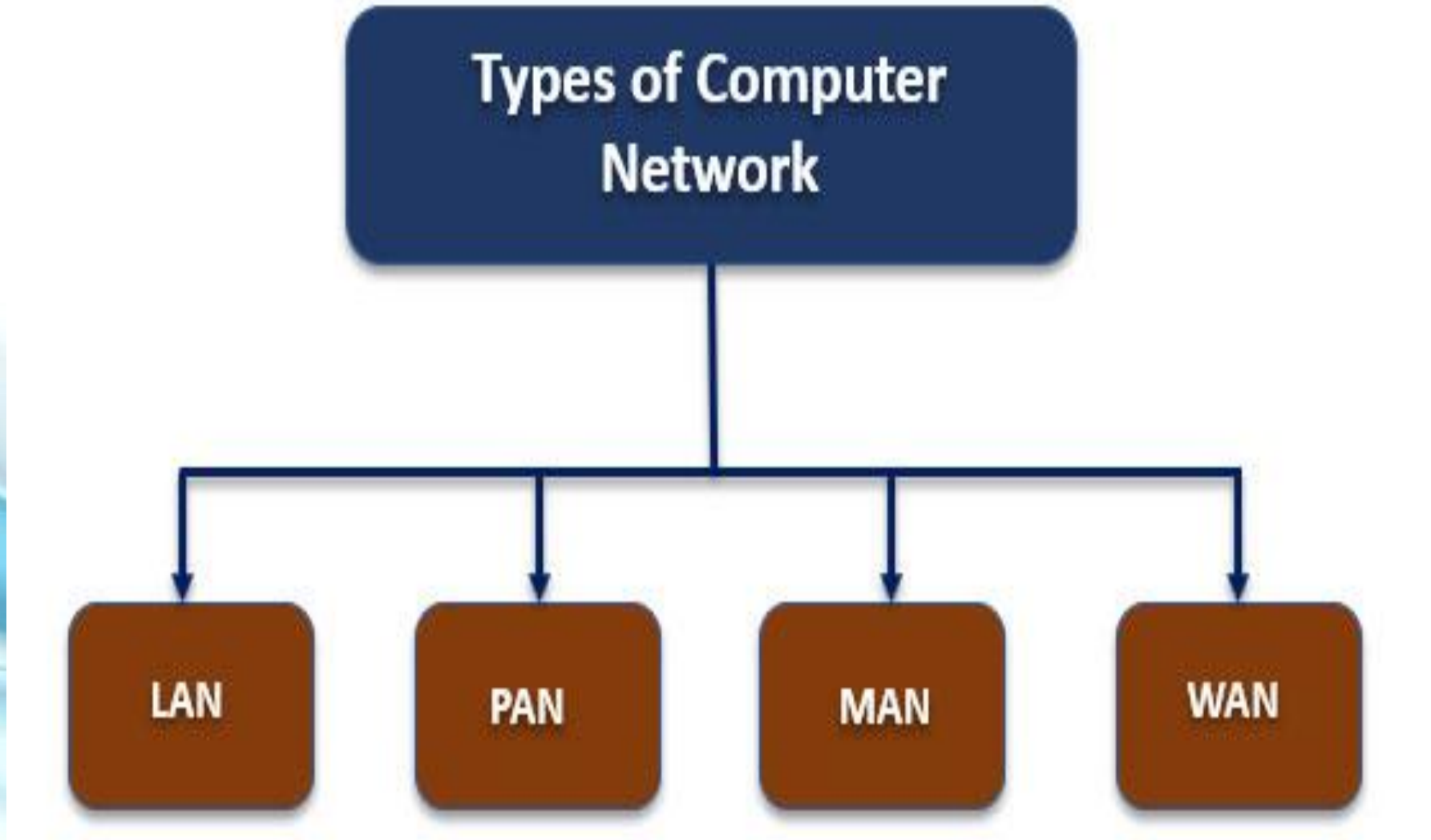
Tree Topology continued…

Installation and configuration is difficult as compared to other topologies. Also, if the backbone cable is damaged, the entire network communication is disrupted.

Tree Topology



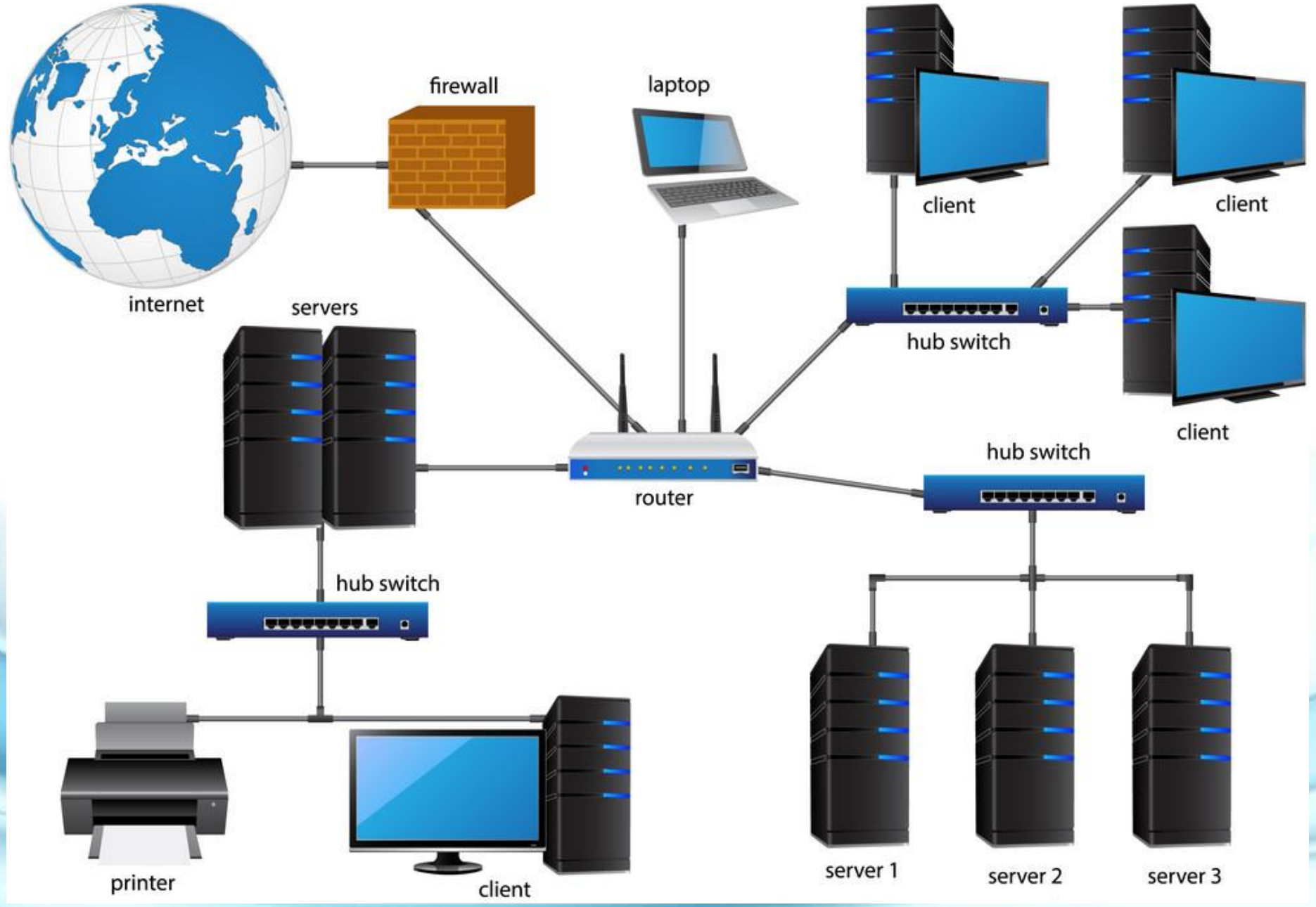
On the basis of geographical span, network can be broadly categorized as LAN, PAN,MAN & WAN.



LAN (Local Area Network)

LAN stands for **Local Area Network**. Local Area networks are private networks and can span a radius of up to 1 Km.

They are generally established within a building or campus. **LAN**s operate at a speed in the range 10 Mbps to 1 Gbps.



Local Area Network(LAN)

PAN (Personal Area Network)

A personal area **network** (**PAN**) is a **computer network** for interconnecting electronic devices centered on an individual person's workspace.

A **PAN** provides data transmission among devices such as **computers**, smartphones, tablets and personal digital assistants.

PAN (Personal Area Network)

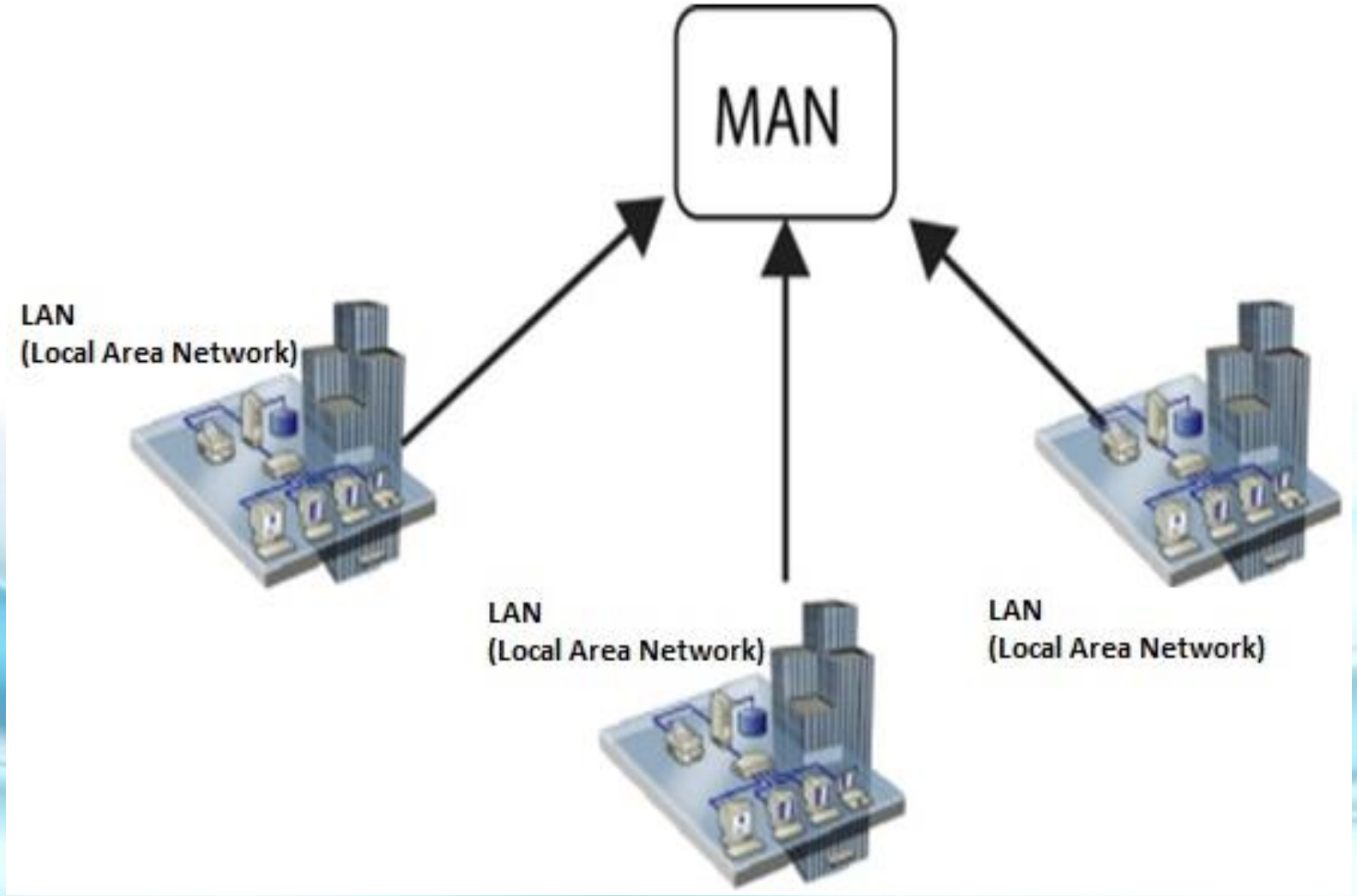
MAN (Metropolitan Area Network)

MAN stands for **Metropolitan Area Network**. It may be owned by a single organization or by many individuals or organizations.

These networks are used to establish link within a city, and span an area of radius up to 50 Km. **MAN**s facilitate sharing of resources by connecting various local area networks.

For example, a cable television network within a city.

MAN (Metropolitan Area Network)



WAN (Wide Area Network)

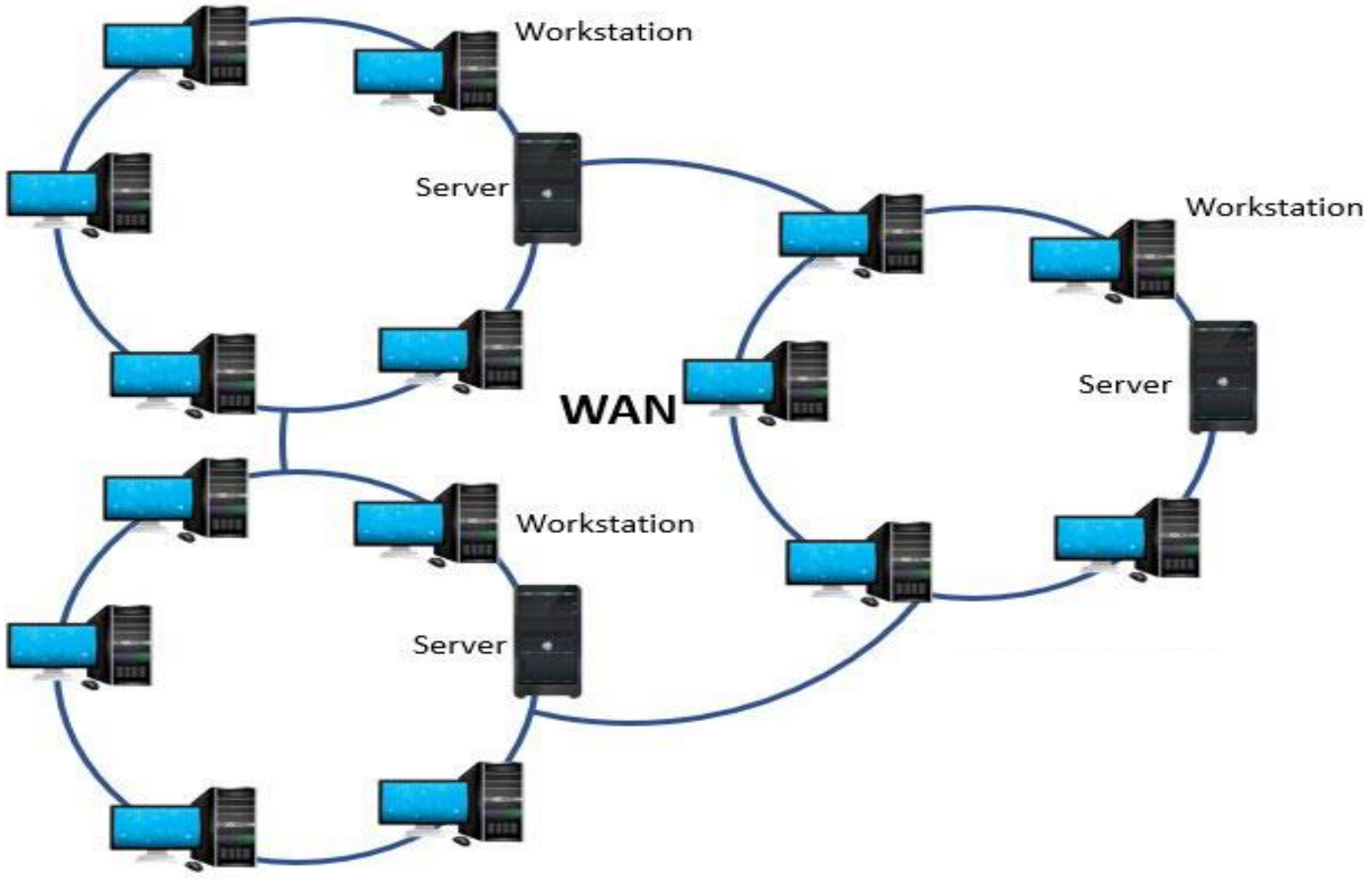
WAN stands for **Wide Area Network**. Typically a **WAN** spans a segment of about 1000 Km.

They are used for long distance communication and are well suited for connecting remote areas.

They establish link within a country or continent.

A **WAN** may be owned and managed by several organizations. It connects various local and metropolitan area networks.

WAN (Wide Area Network)



WLAN (Wireless LAN)

WLAN. Stands for "Wireless Local Area **Network**." A **WLAN**, or **wireless LAN**, is a **network** that allows devices to connect and communicate wirelessly.

Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a **WLAN** communicate via Wi-Fi (Wireless Fidelity – It describes a technology for radio wireless local area networking of devices based on the IEEE 802.11 standards).

WLAN (Wireless LAN)

Internet Working Devices

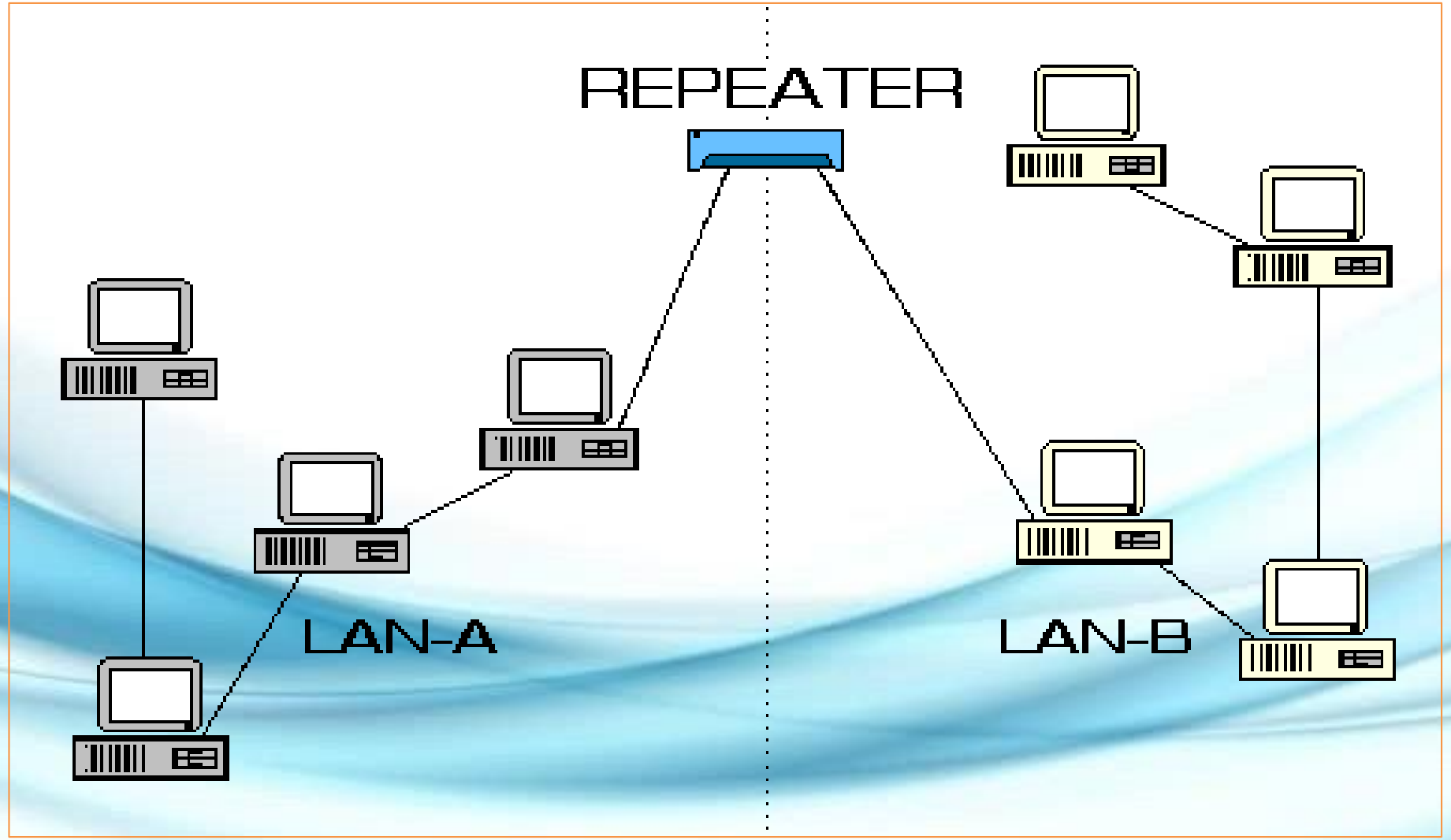
Repeater :

With increase in distance, a signal may become weak and distorted. A repeater is used to restore the input signal to its original form, so that it can travel a larger distance.

Thus, it is placed between two cable segments. It is also known as digital regenerator which reshapes and amplifies the digital signal.

Repeater

Repeater in a network



WLAN (Wireless LAN)

WLAN. Stands for "Wireless Local Area **Network**." A **WLAN**, or **wireless LAN**, is a **network** that allows devices to connect and communicate wirelessly.

Unlike a traditional wired LAN, in which devices communicate over Ethernet cables, devices on a **WLAN** communicate via Wi-Fi (Wireless Fidelity – It describes a technology for radio wireless local area networking of devices based on the IEEE 802.11 standards).

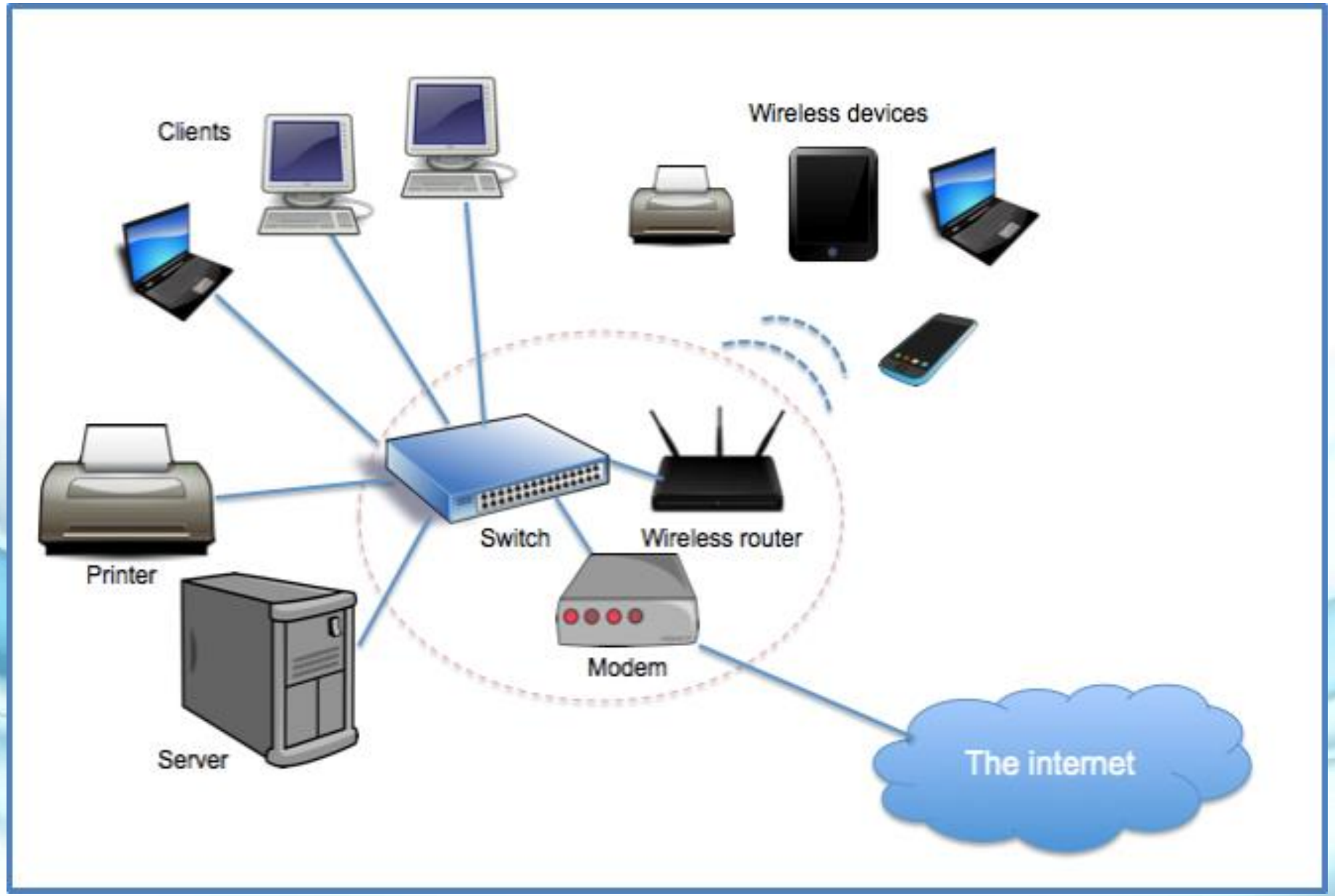
WLAN (Wireless LAN)

Internet Working Devices

MODEM: The word "**modem**" stands for modulator-demodulator. A **modem** is typically **used** to send digital data over a phone line.

The sending **modem** modulates the data into a signal that is compatible with the phone line, and the receiving **modem** demodulates the signal back into digital data.

MODEM continued……



Internet Working Devices

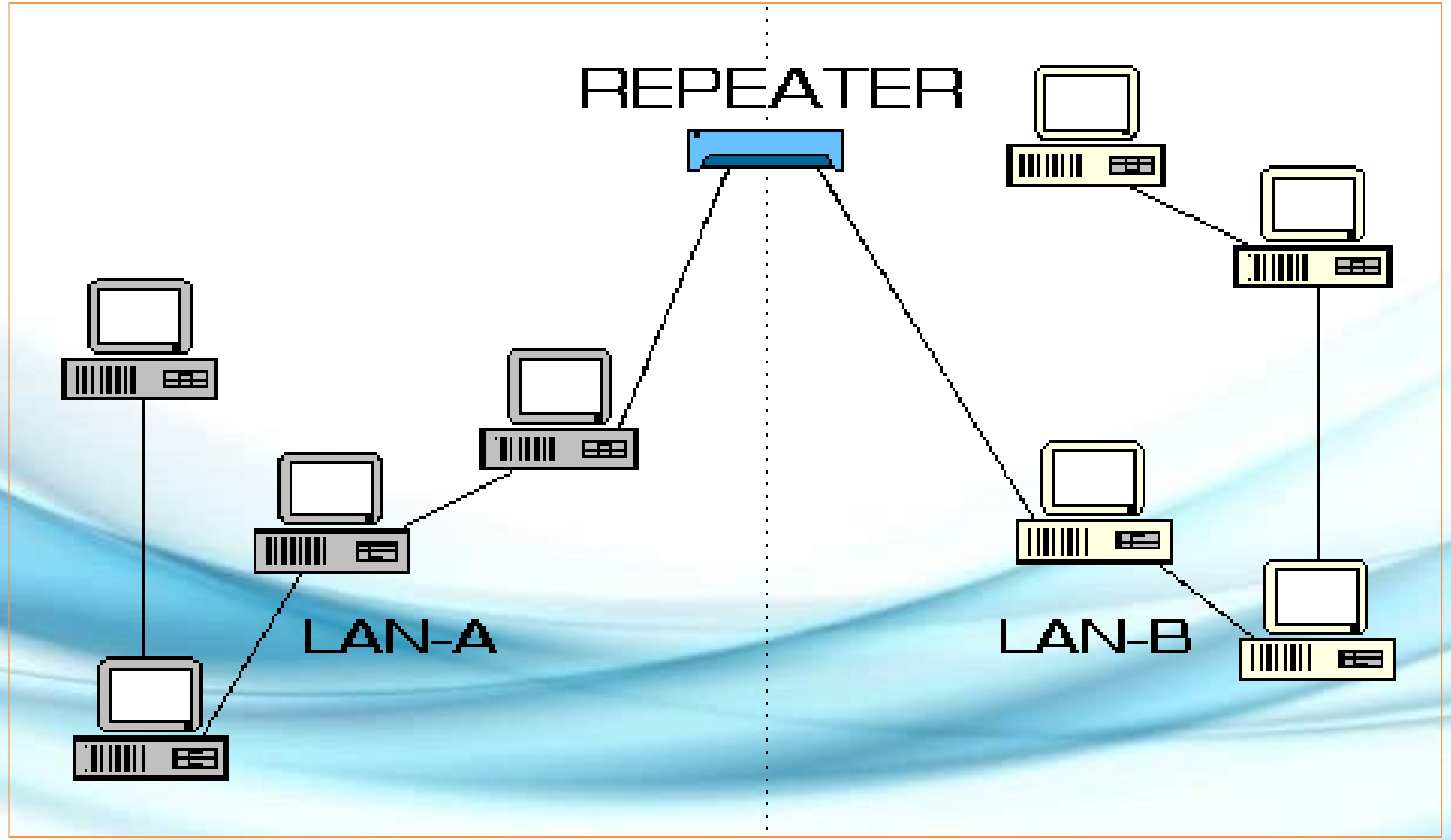
Repeater :

With increase in distance, a signal may become weak and distorted. A repeater is used to restore the input signal to its original form, so that it can travel a larger distance.

Thus, it is placed between two cable segments. It is also known as digital regenerator which reshapes and amplifies the digital signal.

Repeater

Repeater in a network



Hub

Unlike a repeater which connects two cables, a hub connects several lines, also called, cable segments.
A hub comprises several input/output (I/O) ports, each of which connects to a single cable.
Data arriving on an incoming line is output to all lines except the line on which the hub receives the data.

HUB

Hub

Bridge

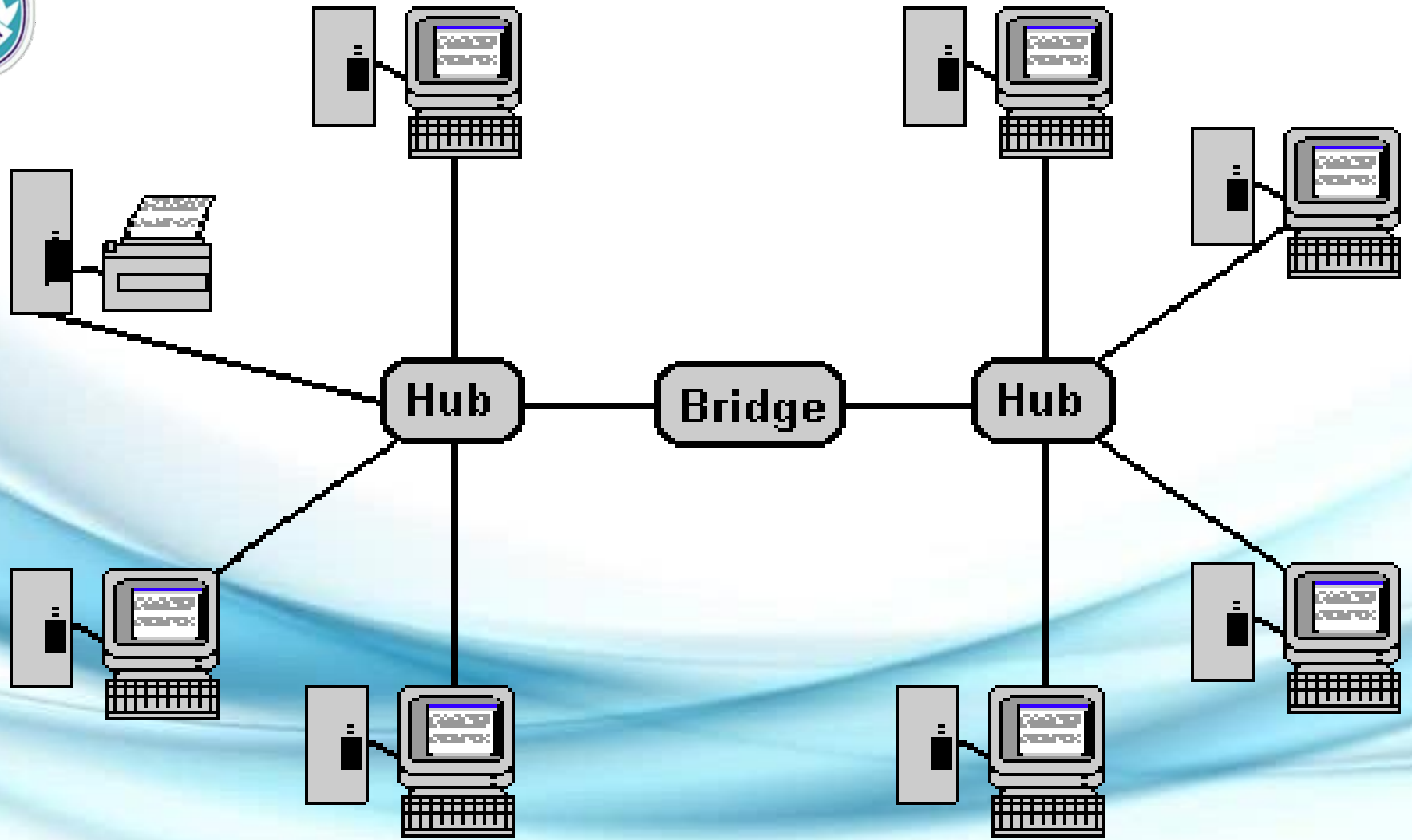
A bridge is a multiport device used for connecting two or more local area networks (LAN), possibly operating at different speeds.

Thus, a bridge may be used to produce bigger LAN by combining smaller LANs. A bridge enables devices on one LAN segment to communicate with the devices on another LAN segment.

Bridge continued…..

Unlike hubs, they are intelligent devices which exercise discretion while forwarding data to the outgoing line leading to destination.

Bridge continued….



Switch

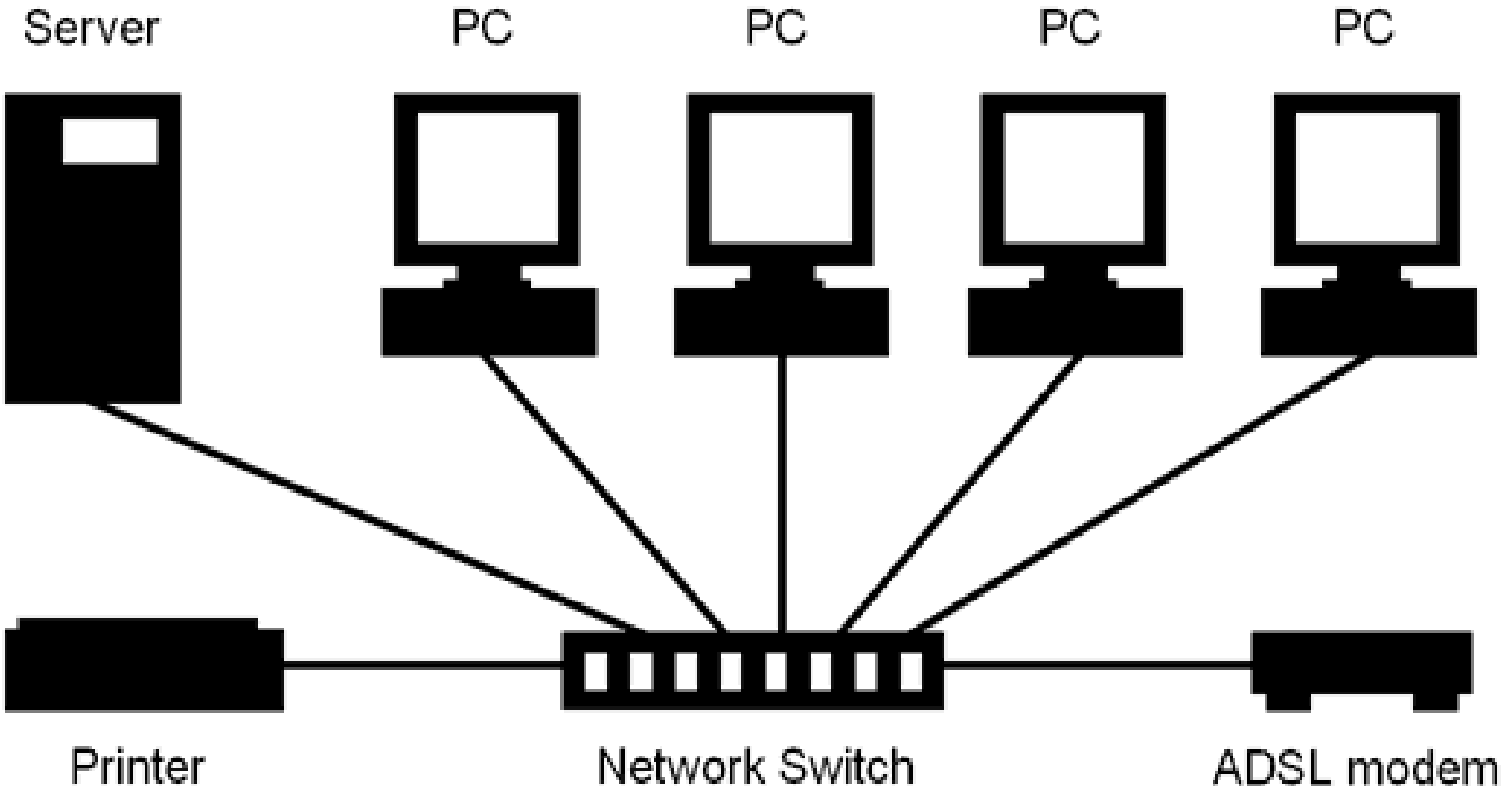
Unlike bridges which connect two or more LAN segments, switches are used to connect individual nodes in the network with each other.

Each node within network is connected to a unique port in the switch.

On receiving the incoming data frame, it forwards it to only single line connecting to the destination node.

All the nodes connected through switch forms only one LAN.

Switch continued….

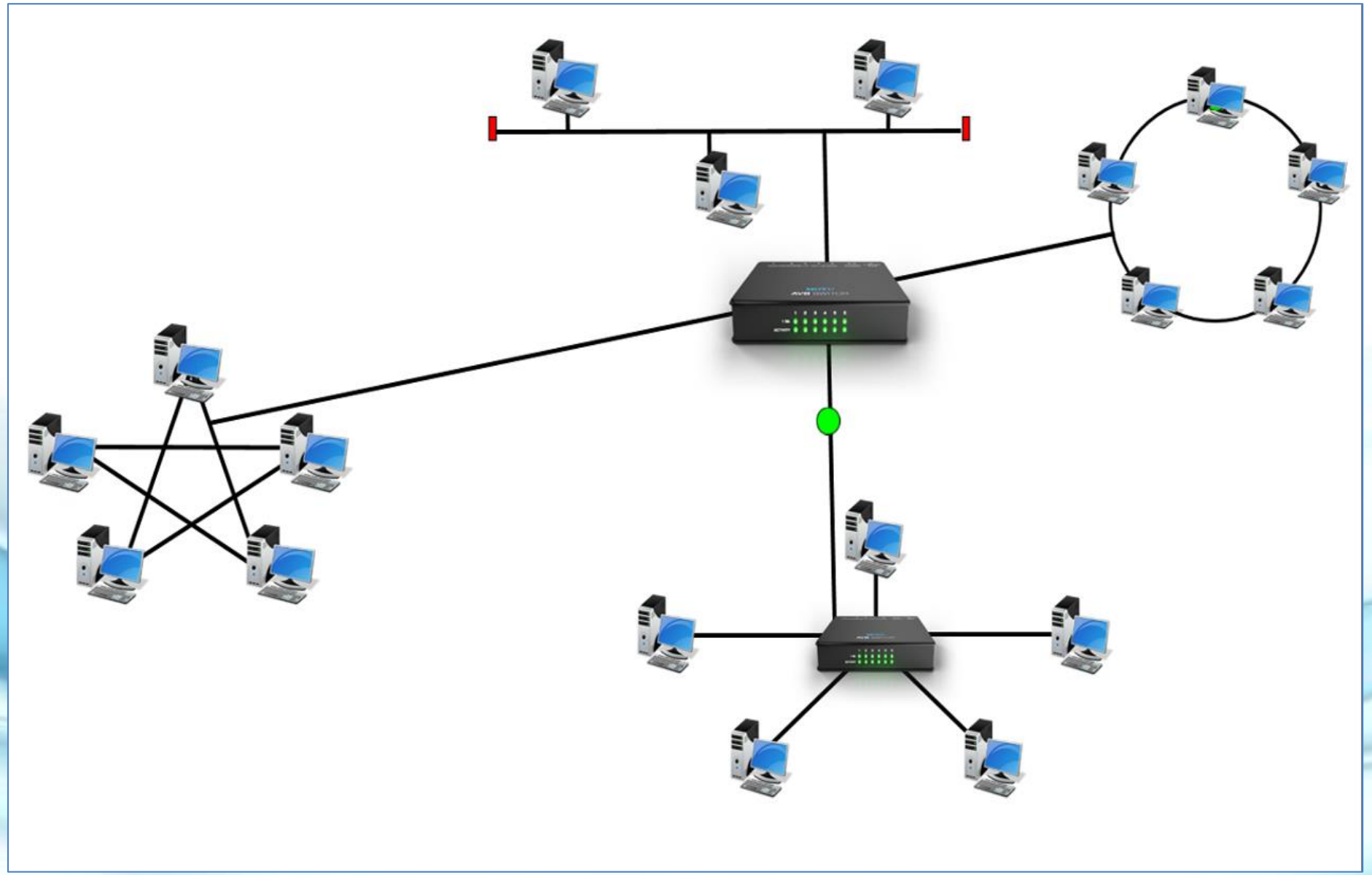


Router

Routers are used for connecting various networks (LAN or WAN) with each other. A router transmits data from incoming network to another network.

A router maintains a routing table of various networks. Based on the destination address, the router determines to which network the incoming packet should be transmitted.

Router continued….



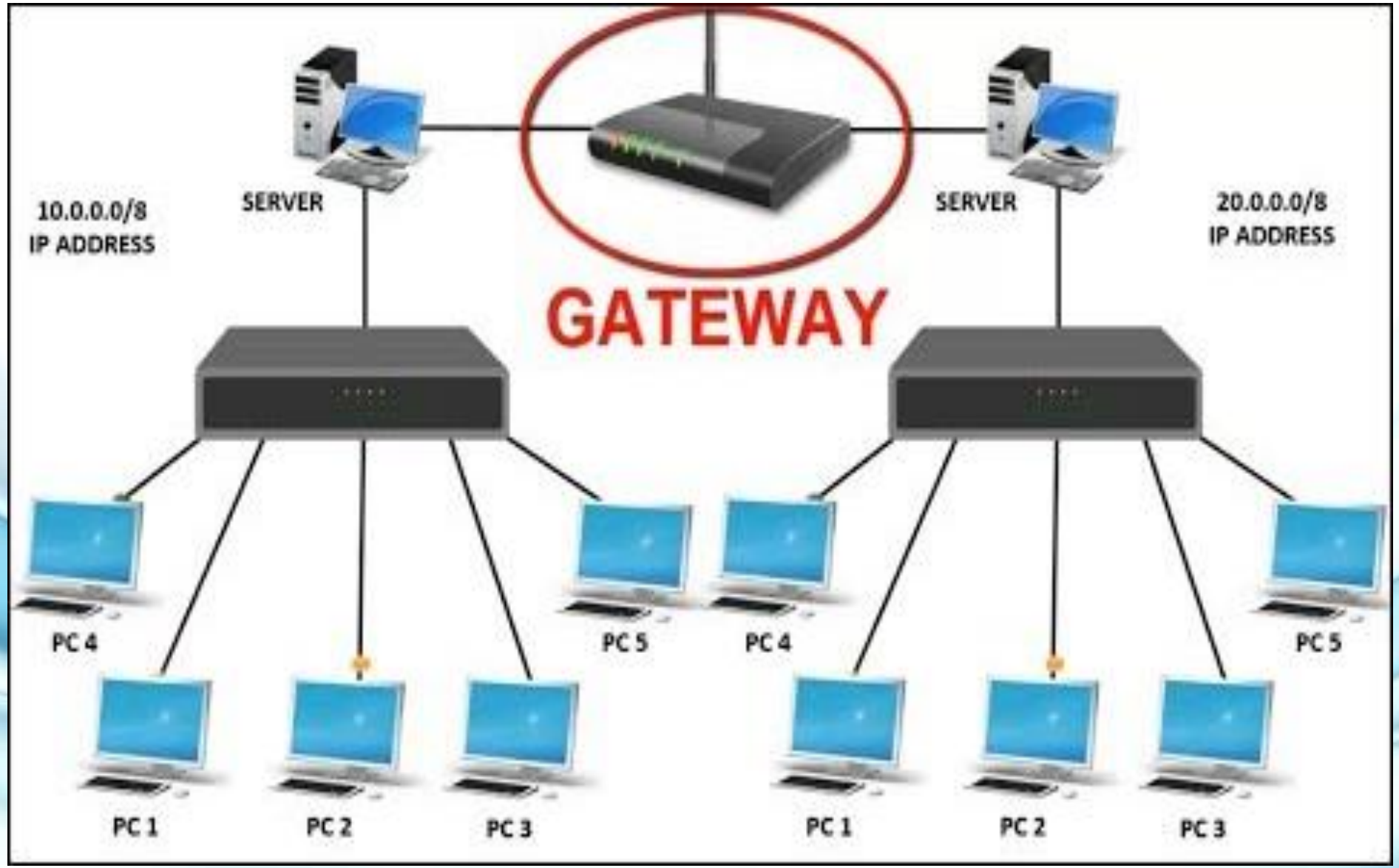
Gateway

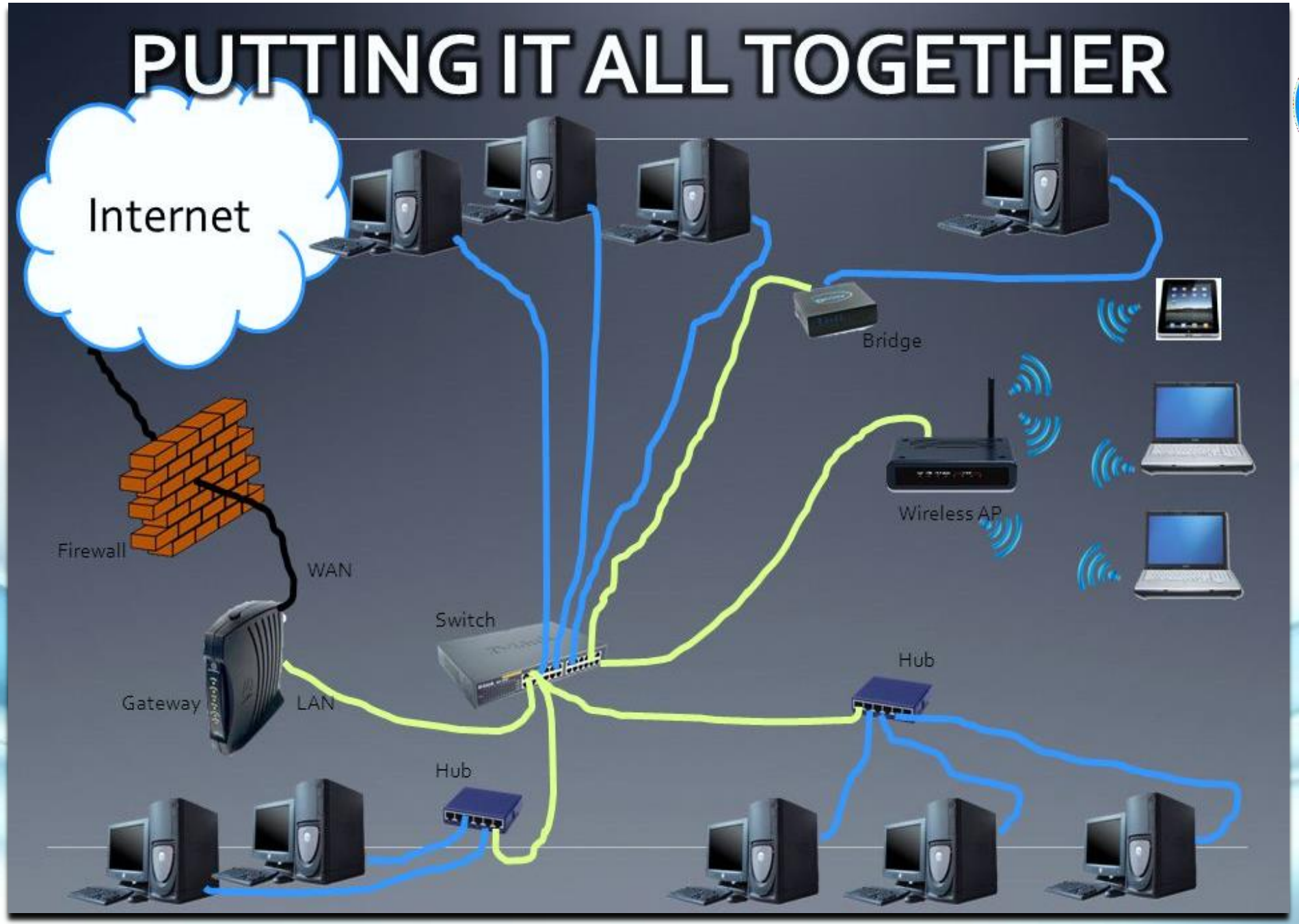
A gateway connects networks based on different protocol technologies to communicate with each other.

Data coming from one network operating on one protocol is converted according to the protocol of outgoing network, and then forwarded.

Thus a gateway may be thought of as a router equipped with software for protocol conversion.

Gateway continued…




PUTTING IT ALL TOGETHER
Internet
Bridge
Wireless AP
Firewall
WAN
Switch
Gateway
LAN
Hub
Hub

Internet

A wide network of networks i.e. interconnection of WANS form the global Internet. It is neither owned by any single individual nor by any single organization.

It has made it possible to exchange information and communicate with remote nodes.

Internet continued….

One can access the Internet using several means such as leased line, dial-up access, and wireless connectivity. The machines on the Internet are known as hosts. The machine that initiates a request is called client and the machine that processes a client request is called server.

Applications of Internet

There are several applications of Internet such as e-mail, file transfer, remote login, and World Wide Web (WWW).

Electronic Mail (E-Mail):

An email may be a written text and may include multimedia attachment consisting of text, audio, image, or video. Sender of the e-mail may send it to one or more intended recipients.

Electronic Mail (E-Mail): continued…

Sending and receiving of mails can take place through web based e-mail application also called webmail application, (such as, Gmail, Windows Live Hotmail, and *Yahoo*), or a desktop based e-mail applications (such as, Microsoft outlook, Thunderbird, mail application on mobile phone).

Electronic Mail (E-Mail): continued…

Transferring mail over the Internet is governed by a set of rules known as email protocols such as SMTP (Simple Mail Transfer Protocol) and POP3 (Post Office Protocol).

Applications of Internet

File Transfer:

Transferring files from one machine to another through a TC P based network is done using FTP (File Transfer Protocol).

File Transfer Protocol is based on client server architecture.Using FTP, local host (client) can download or upload files to and from remote host (server).

Applications of Internet

Remote Login (TELNET):

TELNET stands for TErminaL NETwork. It is a client server based application that allows the user working on one system to access a remote system. For initiating remote login, the user (client) should specify the address of remote system, and should authenticate himself/herself using username and password mechanism.

Remote Login (TELNET): continued…

On successful login, the client can access the remote system.

TELNET service is often used for accessing data on the remote host, or executing on the server the applications installed on it (server).

Applications of Internet

World Wide Web (WWW):

World Wide Web (WWW), commonly known as web, is a repository of information on machines spread all over the Internet and linked to each other. The information is organized in the form of documents called web pages.

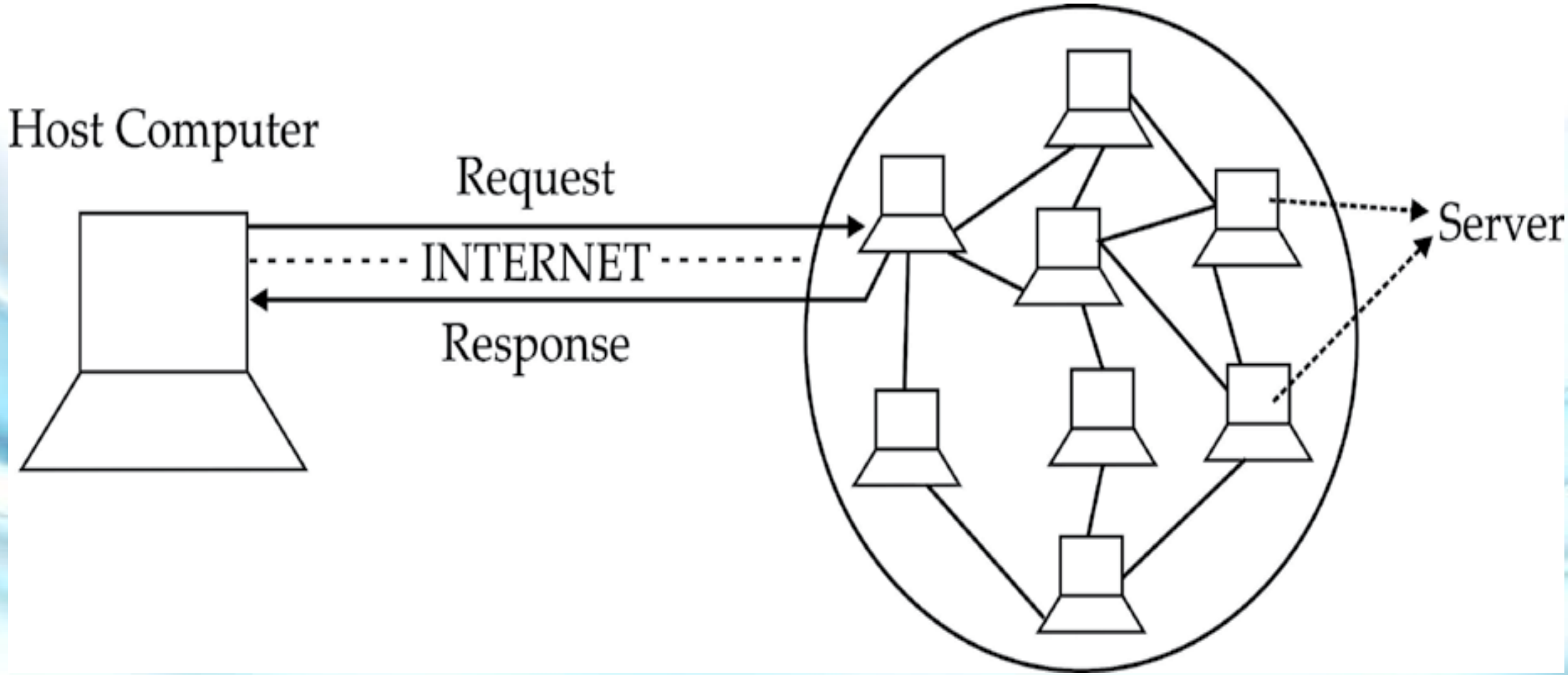
World Wide Web (WWW): Continued…

A web page may contain text, images, audio, videos, and information for linking the web pages in the form of hyperlinks.

WWW uses distributed client server architecture based on HTTP (Hyper Text Transfer Protocol).

The client request is relayed through Internet to the appropriate server, which sends back the reply through Internet to the host system.

WWW and Internet



TCP/IP Model

The TC P/IP (Transmission Control Protocol/Internet Protocol) is often called the glue which holds Internet and WWW (collection of servers where information is stored)together.

When we are dealing with the Internet, we are essentially dealing with the TC P/IP model.

TCP/IP Model continued…

The simple task of sending the data from one place to another through network requires several sub-tasks such as specifying sender and receiver's network and physical address, dividing the message into smaller fragments so that they can be easily transmitted over Internet, taking appropriate measures for error and flow control, and taking necessary action on receiving the message.

TCP/IP Model (4 – Layers)

APPLICATION LAYER (HTTP, FTP, SMTP, …)
TRANSPORT LAYER (TCP, UDP, …)
INTERNET LAYER (IP,ICMP,ARP,…)
LINK LAYER (Ethernet, Wifi, …)

APPLICATION LAYER

APPLICATION LAYER: Data/message is created at the sender's end at Application layer. At the receiving end it is examined and processed (possibly displayed) at Application layer. This layer is also responsible for enveloping the message to be sent with the header. Several protocols such as HTTP, SMTP, POP3, and TELNET (remote login) operate on this layer.

TRANSPORT LAYER

TRANSPORT LAYER: Application layer passes the message to the Transport layer which appends the information about the source and destination ports of the processes at two ends. At the ends, the ports process the message. Mainly two end-to end protocols operate at this layer, namely TCP and UDP.

TRANSPORT LAYER Continued…

TCP (Transmission Control Protocol) is a reliable connection-oriented protocol needed when timely and error free delivery of data is important.

UDP (User Datagram Protocol) is an unreliable connectionless protocol needed in a scenario such as exchange of short messages and client server request-reply messages, where immediate response is more important rather than assured delivery.

TRANSPORT LAYER Continued…

Further, transport layer divides the message into a number of fragments, called segments, depending upon the maximum transmission size permitted.
In TCP, each segment will carry the sequence number denoting its relative position in the message, so that, the message can be assembled at the receiver end by the transport layer at recipient's end.

TCP/IP Model (4 – Layers)

APPLICATION LAYER (HTTP, FTP, SMTP, …)
TRANSPORT LAYER (TCP, UDP, …)
INTERNET LAYER (IP,ICMP,ARP,…)
LINK LAYER (Ethernet, Wifi, …)

APPLICATION LAYER

APPLICATION LAYER: Data/message is created at the sender's end at Application layer. At the receiving end it is examined and processed (possibly displayed) at Application layer. This layer is also responsible for enveloping the message to be sent with the header. Several protocols such as HTTP, SMTP, POP3, and TELNET (remote login) operate on this layer.

TRANSPORT LAYER

TRANSPORT LAYER: Application layer passes the message to the Transport layer which appends the information about the source and destination ports of the processes at two ends. At the ends, the ports process the message. Mainly two end-to end protocols operate at this layer, namely TCP and UDP.

TRANSPORT LAYER Continued…

TCP (Transmission Control Protocol) is a reliable connection-oriented protocol needed when timely and error free delivery of data is important.

UDP (User Datagram Protocol) is an unreliable connectionless protocol needed in a scenario such as exchange of short messages and client server request-reply messages, where immediate response is more important rather than assured delivery.

TRANSPORT LAYER Continued…

Further, transport layer divides the message into a number of fragments, called segments, depending upon the maximum transmission size permitted.
In TCP, each segment will carry the sequence number denoting its relative position in the message, so that, the message can be assembled at the receiver end by the transport layer at recipient's end.

INTERNET LAYER

INTERNET LAYER: Transport layer hands over the segments to the Internet layer which adds source and destination machine network address (also termed IP address). Internet layer is mainly responsible for packet routing and injects packets into the network that may take independent path to the destination, and thus may arrive out of order at the destination.

INTERNET LAYER Continued…

At the receiving layer, message is reassembled in the correct order. In the Internet layer, Internet Protocol (IP) is used. IP defines the format of packets exchanged over the Internet. This protocol is usually accompanied by three other protocols, namely, Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Dynamic Host Configuration Protocol (DHCP).

LINK LAYER

LINK LAYER is also called Host to Internet layer. This layer is responsible for adding the header containing sender and receiver physical address to the packet received from Internet layer.

The resulting message is called frame. It may be noted that recipient's physical address corresponds to the physical address of the next host on the network to which message is to be relayed, and not (necessarily) the physical address of the destination machine.

Suppose host 1 wishes to send a message Hello to host 2. Diagram in Figure 2.19 illustrates how layer by layer message is processed at the host 1 and host 2.

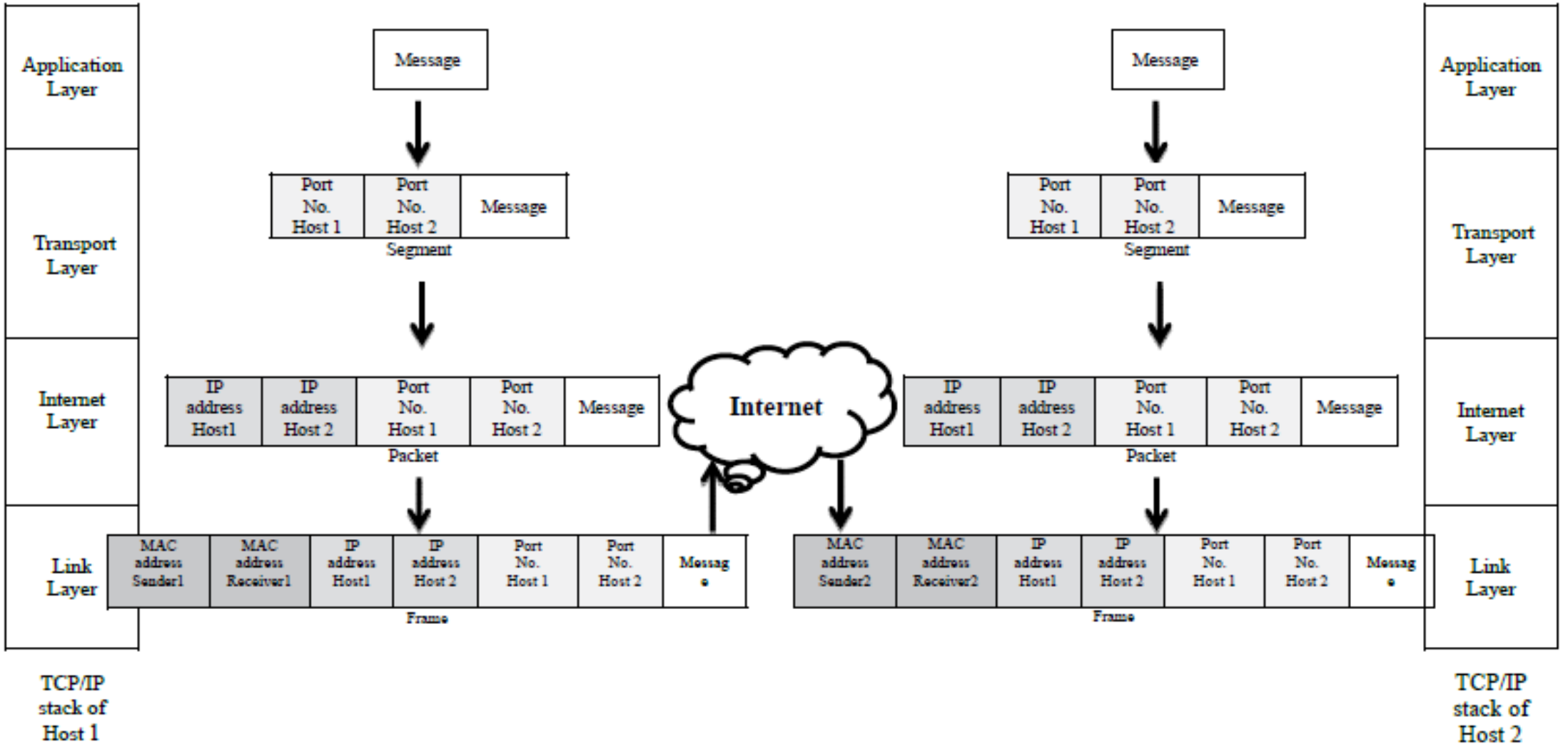


Figure 2.19: Message transfer illustrated through TCP/IP Model

Network Safety Concerns

With increase in use of network for accessing data and resource sharing, security is becoming a prime concern. Large amount of data placed on the Internet and substantially increasing number of users are leading to security issues such as misuse of data, hacking, copyright issues and many more.

Network Safety Concerns Continued….

Malwares: The term malware refers to malicious software (programs) designed with the intension to affect the normal functionality by causing harm to the system, or with the intension of getting unauthorized access to the system, or denying access to legitimate users of computing resources.

A malware may be virus, worm, Trojan horse, or spam.

Network Safety Concerns Continued….

Virus: A virus is a software code that may harm your system by overwriting or corrupting the system files. A computer virus is similar in action to viruses in our body which replicate themselves and affect body cells. The affected part is called infected area.

Network Safety Concerns Continued….

A computer virus may make several copies of it by inserting its code onto the system programs, files or boot sector of hard drives and thereby may corrupt them. This causes the system to slow down or even stop functioning.

The viruses are mainly categorized as boot sector virus, file infector virus, and macro virus.

Network Safety Concerns Continued….

Boot sector viruses affect boot record of the disks. These are the memory resident viruses that embed themselves into the disk area and are activated when the drive is started (booted up),
for example, Michelangelo virus.

Network Safety Concerns Continued….

File Infectors are the viruses that attach themselves to executable files either by overwriting a part of their code or by appending their code to the files, for example, Romeo and Juliet virus.

Network Safety Concerns Continued….

Macro viruses embed themselves into the documents.
These viruses are executable files which are often received as email attachments.
When attachment is opened, viruses starts functioning by affecting the system programs (by deleting, creating or overwriting other files), and may get forwarded to others whose email id appears in the address book.
Melissa is an example of such a virus, which got spread through a Microsoft word document sent as an email attachment.

Network Safety Concerns Continued….

Worm: A worm is often received via network, and it automatically keeps on creating several copies of itself on the hard disk thereby flooding the hard disk.
When worm is received as an email attachment, it is automatically forwarded to the recipients leading to network congestion.

Network Safety Concerns Continued….

Thus a **worm** may crash the system and entire network. No host application is required for worms to replicate themselves.

For example, Code Red Worm which makes more than2,50,000 copies of itself in approximately 9 hours.

Network Safety Concerns Continued….

Trojan Horse: Trojan Horse is a code that appears to be desirable and useful but ends up harming the system. Trojan horse can attach itself with a safe application. **For example**, it may be attached to any game downloaded over Internet. Such an application when executed creates a backdoor in the system through which a hacker can access the system. The hacker can monitor all the activity performed on the system.

Network Safety Concerns Continued….

Eg:Trojan Horse named Sub7 was created which took advantage of security flaw of earlier version browsers such as Internet Explorer andChrome to illegally access the host computer.

Network Safety Concerns Continued….

Spam: Spams are the unwanted electronic mails, generally sent in bulk over the Internet to recipients. Such undesirable mails are generally commercial mails sent for advertisement purpose.

However, they may contain link to phishing sites that attempts to steal user information or link to sites that contain malware or infected files. Spam mail filters used by e-mail software can be used to prevent spam mails.

Network Safety Concerns Continued….

Phishing: Phishing refers to the act of stealing user's personal information through fraud mails.
These mails either entail personal information through embedded forms, or contain links to the web page that may prompt you to provide this information. Information attempted to be stolen may include bank account number, debit/credit card number, passwords or any other valuable data.

Network Safety Concerns Continued….

Few main causes that make end users victims of phishing include:

Lack of awareness: Many a times we end up providing our account information in the mails received from our bank. Such mails though appear to be legitimate but are fraudulent.

Lack of awareness that bank will never ask for account PIN and password either through mail or message make us prey of these targeted attacks.

Network Safety Concerns Continued….

Misleading Mails : Often fraud mails received contains tempting information such as bag a lottery prize, or a warning indicating closing of account in case of failure in proving account details.

Lack of Security: Lack of inadequate security measures on computers is also a main cause that makes us fall prey to phishing.

Network Safety Concerns Continued….

IPR Issues: The intellectual property is the work produced by a person or an organization using the mind and creativity.

The intellectual property comprises of intangible assets such as literary work, artistic work, a work of music, and an engineering design. Intellectual Property Rights (IPR),are the rights of a person or an organization on intellectual property.

Network Safety Concerns Continued….

Commonly defined Intellectual Property Rights include patents, copyright, industrial design rights, trade marks, trade dress like visual appearance of a product or its packaging, and trade secrets.

There are various issues concerned with these rights such as piracy of software, plagiarism (presenting the literary work done by someone as own work), trademark violations, patent violations, and copyright violations.

Network Safety Concerns Continued….

Hacking: Hacking may be described as having unauthorized access to someone's computer or computer network for stealing resources such as password or confidential files, or causing harm to network or system.

A hacker identifies the vulnerabilities of the system in order to achieve this.

Network Safety Concerns Continued….

A hacker may be driven by several reasons for doing so such as his/ her own personal interest, as a means of fun, or protest. Hackers are also categorized as good hacker and bad hacker. Bad hacker hacks the system with bad intensions whereas good hacker tries to hack system in order to identify its weaknesses so that they can be isolated. These bad (unethical) hackers are termed crackers, as opposed to good (ethical) hackers.

Network Security Tools and Services

Since Internet has emerged as a prime tool for sharing resources and accessing data, exponentially growing number of users are using it with both good and bad intentions.

Everyone accessing the Internet needs to be aware of the security issues and take protective measures to address the same. Systems that are used as a tool for accessing Internet can be protected using anti-virus and firewall.

Network Security Tools and Services continued…

Protection using Anti-Virus: Anti-virus is software that aims to protect your system against malicious and potentially unwanted programs. It is responsible for detecting these malicious programs by searching or them, and removing them to keep the system protected. The software operates by maintaining a database of malware definitions, which are automatically updated.

Network Security Tools and Services continued…

It searches for any malicious program by scanning the files against the stored malware definitions for a match. In case of a match, they are declared as potentially harmful, and are disabled and removed depending upon anti-virus software settings.

Network Security Tools and Services continued…

Protection using Firewall : A firewall aims at protecting the internal network of an organization, home, or individual from malicious traffic from external networks. A router or a computer (often dedicated to serve as a firewall) may be installed between external network and internal network for this purpose. Firewall inspects the network traffic, and allows only that data to pass through the network that does not violate the security constraint.

Network Security Tools and Services continued…

Hardware firewall in form of router prevents malicious software from entering your network from outside network. However, software firewall installed on personal computer prevents unauthorized access or malwares from gaining access to personal computer. Network firewalls may also encrypt the incoming data by converting it to non readable format, thus, adding further protection.

Network Security Tools and Services continued…

Protective Measures while accessing Internet :

Never click on a suspicious link specified on a web page or send through a mail for which you are not sure about its authenticity.

Make sure that passwords are strong and are changed frequently. Passwords are the means for authenticating users, thereby allowing access to networked systems.

Network Security Tools and Services continued…

Weak passwords have smaller length and uses small subset of possible characters, and thus, are subjected to be cracked easily.

One should also avoid setting obvious passwords such as names, mobile numbers, or date of birth.

Passwords should be strong having long length and including characters such as numbers and punctuation signs.

Network Security Tools and Services continued…

Never disclose personal information such as account details, passwords, credit and debit card details, and other valuable information. Also, report phishing issues to the concerned authorities. In case of unsolicited mails, mark them as spam mails.

Network Security Tools and Services continued…

Security of the communication made over the Internet can be indicated by the security of protocol being used. Secured Hyper Text Transfer Protocol (HTTPs) is a secure version used for communication between client and host on the Internet. So, ensure that all communications are secure, especially online transactions.

Network Security Tools and Services continued…

The security of website can be ensured of there is padlock on the left side of address bar.
It indicates that website has a SSL (Secure Socket Layer) digital certificate issued by trusted party which ensures and proves identity of remote host.

Network Security Tools and Services continued…

Ensure that the web browser being used for accessing web is updated and is secure.

Make sure that the website address is properly spelled. Because there may be two websites with almost same name, one being a phishing website.

Network Security Tools and Services continued…

The anti-virus software should be up to date. Delete cookies periodically. A cookie is small piece of information about the client browsing a website. On receiving a request from a client, the server records the client information such as domain name and registration id on the server site in the form of a file or a string.

Network Security Tools and Services continued…

The server sends this cookie along with response requested by the client. At the client side, the browser stores this cookie received from the server in a directory called cookie directory.

By obtaining access to these cookies, hacker may gain unauthorized access to these websites. Thus, cookies should be deleted occasionally along with the temporary files stored on our system during web browsing.

Cyber Security

Cybercrimes are the crimes related to the misuse of computer or Internet such as theft,fraud, and forgery.
The IT act defines cybercrime as *an unlawful act where in the computer is either a tool or a target or both.*
Some of these crimes are mentioned below:

1. Sending spam mails to uninterested recipients.
2. Hacking someone's account or system.

Cyber Security

3. Stealing someone's personal information through phishing.
4. Hosting a site carrying lots of malwares or being a source for spreading them.
5. Harassing someone through mails, messages or social networking.
6. Posting offensive content on any site or sending it to anyone.
7. Defaming someone using Internet.

Cyber Security

8. Forging someone's digital signatures
9. Indulging in fraudulent financial transaction
10. Providing misleading information to clients/ general public through use of Internet resources
11. Intellectual Property theft

Cyber Security

Cyber laws are the laws for systematic use of e-resources, for example, e-business, and serve as a measure against illegal cyber-crime.

Various cyber laws have also been enacted to prevent cyber-crimes and take action against those involved in such crimes.

Cyber Security

These laws define the action that would be taken against people committing the offences. For cyber security, an amendment in IT Act 2000 named Information Technology Amendment Act,2008 was also introduced. The act also defines offences and penalties for cyber-crime. Cyber police is responsible for detecting such crimes and taking the necessary measure against it in accordance with IT Act.

Safe Practices on Social Networking

Social network refers to the network of people interacting and sharing information such as their views, photographs, videos and any other information.

Popular social networking sites include Facebook, LinkedIn, and Twitter. Facebook is social networking site with a purpose to connect with the world around you.

Safe Practices on Social Networking

LinkedIn is a business oriented social networking site that aims to connect people professionally. Twitter is a site where people share their views inform of short messages known as tweets limited to 140 characters.

Safe Practices on Social Networking

Social networking has emerged as an important platform where people bounded geographically by distance can communicate and share their views. Often, people interacting with each other share similar interest.

Safe Practices on Social Networking

It is also an important means for raising awareness about an issue. However, since information spread so quickly, it may be misused for spreading a rumor. Moreover, many users with fake identities get involve in unethical use of the information available on these sites. So, users need to be aware while posting or accessing any data as it may lead to data theft, data misuse or can be a source of malware.

Safe Practices on Social Networking

Social networking can also take place in discussion forum and chat room setting. Discussion forums allow people to share their queries and views by posting on them.

Anyone can initiate a discussion by placing a post on discussion board, and can also comment on the posts initiated by others.

Safe Practices on Social Networking

People participating in a discussion need not be online all the time. These forums are managed by a moderator, who control the content posted on it. Chat room setting is similar to discussion forums, where people can discuss their ideas and queries; however, they need to be present online in order to participate in the currently ongoing discussion.

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- Do not post any personal information and photos on the social networking site as it may be misused against you by some unethical user. Personal information even includes details such as date of birth, home address, personal phone number, and work history details.

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- Take accountability while posting anything on the social networking site as it will be permanent and can be used for making analysis about you.
- Do not post any offensive content on social networking site as it may lead to a criminal action against you.

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- It is always better to set your own privacy settings, rather than going for default settings. You should limit the access to your profile only to selected group of people.

Also, you can limit the people who can search you by your name.

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- Be selective while making friends on the social networking site. Do not send or accept friendship request from any unknown user.

  Also, trust the authenticity of a message only if you are sure about its origin (sender).

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- Beware before spreading any kind of a rumor as it may be treated as a cyber-crime.
- If someone is harassing or threatening you, take snapshot of it as a proof, and block the person. Also, report the incident to the site administrator.

Rules one need to follow below mentioned safe practices while getting involved in social networking:

- Also, take all protective measures while accessing Internet such as protecting the system using anti-virus and firewall, secure browsing, and password management.

Digital Literacy

Digital literacy refers to raising knowledge and awareness about technology such as desktop computers, smartphones, tablets, and other electronic gadgets.

It also includes familiarity with software tools and Internet.

This knowledge facilitates people to acquire, analyze, share, create, and deliver information in efficient and constructive way.

Digital Literacy

Digital literacy also aids people in several arenas such as education, social networking, e-commerce, healthcare, and tourism.

Especially in education, it provides learners with the digitally enhanced learning through use of technology.

Any Questions?