Syllabus Content:

2.1 Network including the Internet

- Show understanding of the purpose and benefits of networking devices
- Show understanding of the characteristics of a LAN (local area network) and a WAN (wide area network) Explain the client-server and peer-to-peer models of networked computers
- Show understanding of thin-client and thick-client and the differences between them
- Show understanding of the bus, star, mesh and hybrid topologies
  Understand how packets are transmitted between two hosts for a given topology
  Justify the use of a topology for a given situation
- Show understanding of cloud computing, including the use of public and private clouds. Benefits and drawbacks of cloud computing
- Show understanding of the differences between and implications of the use of wireless and wired networks
- Describe the characteristics of copper cable, fibreoptic cable, radio waves (including WiFi), microwaves, satellites Describe the hardware that is used to support a LAN Including switch, server, Network Interface Card (NIC), Wireless Network Interface Card (WNIC), Wireless Access Points (WAP), cables, bridge, repeater
- Describe the hardware that is used to support a LAN
- Describe the role and function of a router in a network
- Show understanding of Ethernet and how collisions are detected and avoided Including Carrier Sense Multiple Access / Collision Detection (CSMA / CD
- Show understanding of bit streaming. Methods of bit streaming, i.e. real-time and on-demand Importance of bit rates / broadband speed on bit streaming
- Show understanding of the differences between the World Wide Web (WWW) and the internet Describe the hardware that is used to support the internet
- Including modems, PSTN (Public Switched Telephone Network), dedicated lines, cell phone network

Introduction:

The history of computing started off with centralized computers (in many cases mainframes) or servers performing all the calculations. Client computers were then attached to these centralised computers (servers) and if you wanted to calculate something, you would have to wait for the central computer to respond. As computing power got cheaper, client nodes became more powerful and the central computer less important.

Client server model:

The **client–server model** is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called **servers**, and service requesters, called **clients.**

Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system.

Client-server model

clients

internet
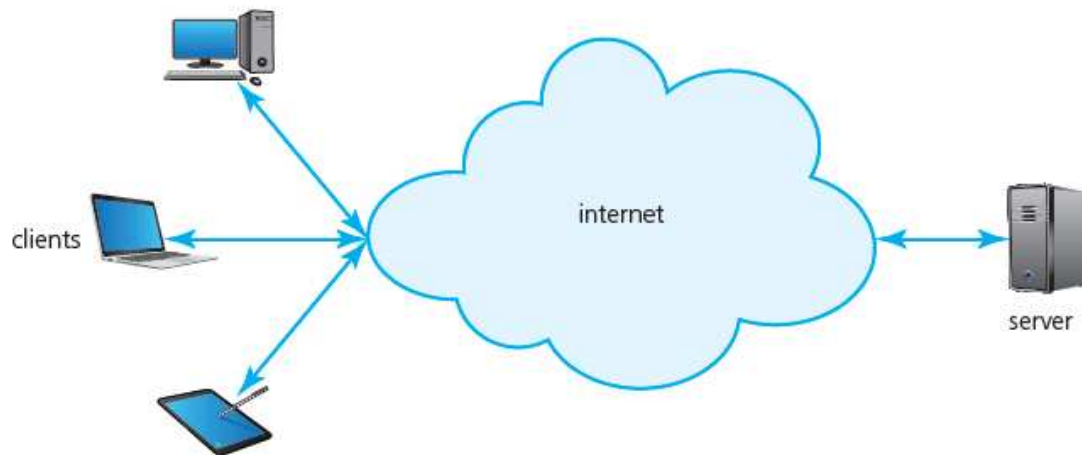
server

Client sends a request to the server and the server finds the requested data and sends it back to the client.

A system administrator manages the whole network; clients are connected through a network; allows data access even over large distances.

Server: a computer program running to serve the requests of other programs, the "clients"

Servers are software programs that in most cases run off normal computing hardware.
Server software includes:
- Printing
- File sharing
- Game hosting
- Websites
- Other web services

Client: an application or system that accesses a service made available by a server

Clients are software programs and processes that connect to servers, sending requests and receiving responses.

Client examples include:

- Web browser page requests
- Chat systems on mobile phones
- Online games

A server **host** runs one or more server programs which share their resources with clients.

A client does not share any of its resources, but requests a server's content or service.

Clients therefore initiate communication sessions with servers which await incoming requests.

Examples of computer applications that use the client–server model are **Email**, **network**
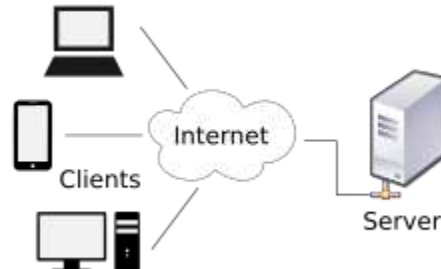
printing, and the **World Wide Web**.

Most networks are controlled by the use of servers. There are different types of servers, for example:

File servers: allows user to save and load data files.

Application server: deals with the distribution of applications software to each

client/node/computer

Print server: ensures that printing from devices on the network is done in queue

Proxy server: acts as a buffer between WAN (usually internet) and LAN.

Web Server: A web server provides access to a web application. The client is the web

browser software.

Peer to Peer model:

Point-to-point topology is the simplest of all the network topologies.

The network consists of a direct link between two computers. It does not have any central server. Nodes can share files with each other and each of the nodes will have its own data.

This is faster and more reliable than other types of connections since there is a direct connection. There is no need to authenticate users

The disadvantage is that it can only be used for small areas where computers are in close proximity. No more than 10 nodes are required (such as small business)

More than 10 nodes cause performance and node-management issues.
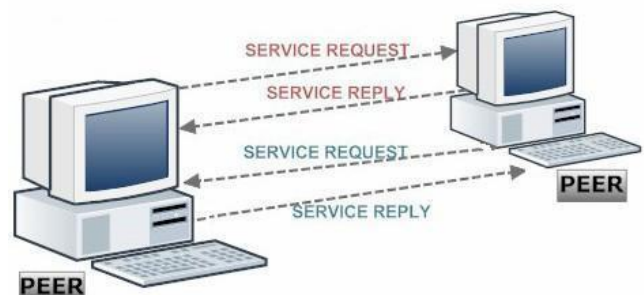
Thin Clients & Thick Clients:

Client server model offers thin-clients and thick-clients. These can offer refer both software and hardware.

Thin Client:

In computer networking, a thin client is a simple computer that has been optimized for establishing a remote connection with a server-based computing environment. The server does most of the work, which can include launching software programs, performing calculations, and storing data.

How thin-client works:

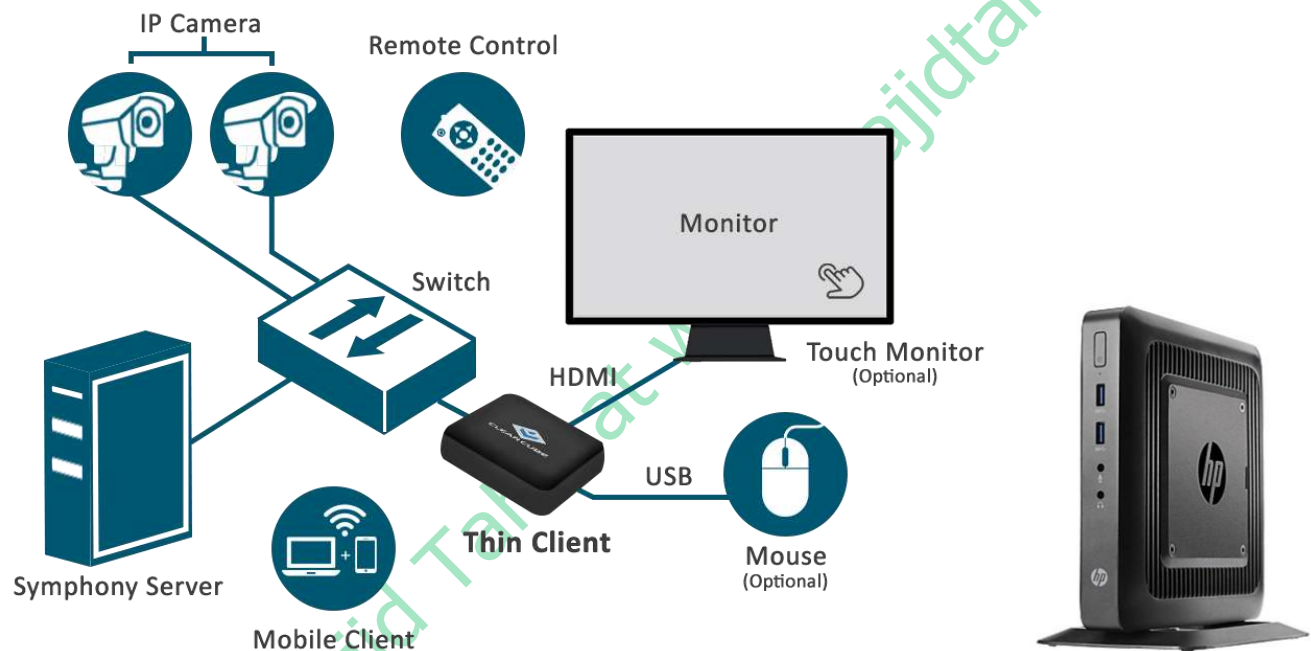- A thin client can't work stand-alone as PC. It must require one server. All thin client login as a user to the server by RDP protocol. Thin client is sharing computing and login server to share all resources of this server.
- Thin client need to connect with Monitor. Keyboard. Mouse. Cable.
- Thin client usually apply to Computer Lab/Smart Classroom/Library/Office/Real estate/ Call Center/Trainning Center this kind of group places. They are not suitable for home personal pc use.
- If can't thin client technology as a PC. It requires settings on Server. One connected, thin client can login on server for working.
- An HP Thin Client 574E is can be purchased from 800to 1000Rs.

Thick Client:

A **thick client** is a computer that does not require a connection to a server to run (unlike a thin **client**).

- However, they can benefit from being connected to a network and a server
- Thick clients are often found in the business environment, where <u>servers</u> provide some data and application support, but the thick client (office computer) is largely independent.
- Thick clients have an operating system and software applications and can be used offline (not connected to a network or server).
- Thick clients have several advantages. They can be used offline, have increased flexibility and higher server capacity.
- A hardware example is normal PC/Laptop since it has its own storage (HDD, SSD) RAM and OS. Its applications can run independently without a server. It can also be connected to server for different services.

Fat Clients

Thin Clients

- Thick clients are also known as **Fat Clients**

Thin client software	Thick client software
• always relies on a connection to a remote server or computer for it to work	• can run some of the features of the software even when not connected to a server
• requires very few local resources (such as SSD, RAM memory or computer processing time)	• relies heavily on local resources
• relies on a good, stable and fast network connection for it to work	• more tolerant of a slow network connection
• data is stored on a remote server or computer	• can store data on local resources such as HDD or SSD

Some Pros and Cons of Thick and Thin clients

	Pros	Cons
Thick clients	• more robust (device can carry out processing even when not connected to server) • clients have more control (they can store their own programs and data/files)	• less secure (relies on clients to keep their own data secure) • each client needs to update data and software individually • data integrity issues, since many clients access the same data which can lead to inconsistencies
Thin clients	• less expensive to expand (low-powered and cheap devices can be used) • all devices are linked to a server (data updates and new software installation done centrally) • server can offer protection against hacking and malware	• high reliance on the server; if the server goes down or there is a break in the communication link then the devices cannot work • despite cheaper hardware, the start-up costs are generally higher than for thick clients

Types of Network

Local Area Network (LAN)

A Local Area Network is a network confined to **one building or site**.

📖 Often a LAN is a **private network** belonging to an organization or business. Because LANs are geographically small, they usually use **cables** or low-power radio (**wireless**) for the connections.

📖 LANs normally consist of computers and devices such as **printer**, **scanner** connected to **hub/switch.**
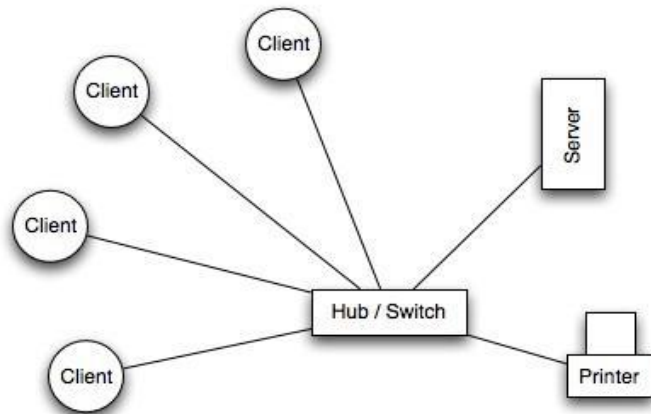
Wireless Local Area Network (WLAN)

A wireless LAN (WLAN) is a LAN that uses **radio signals** (**WiFi**) to connect computers instead of cables. At the centre of the WLAN is a **wireless switch or router** - a small box with one or two antennas sticking out the back - used for **sending and receiving data** to the computers. (Most laptops have a wireless antenna built into the case.)

📖 It is much more **convenient** to use wireless connections instead of running long wires all over a building.

📖 However, WLANs are more **difficult to**
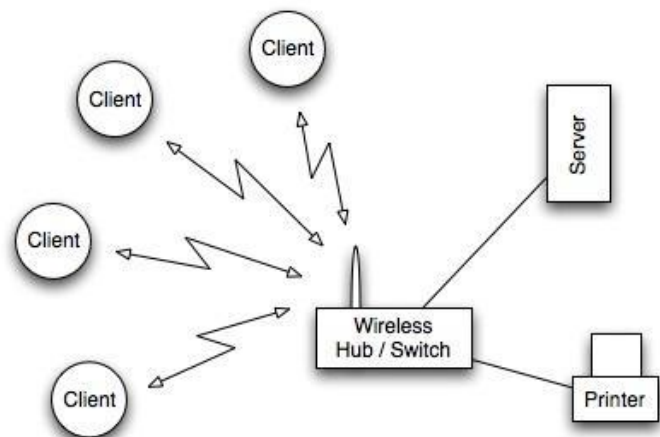
make secure since other people can also try to connect to the wireless network. So, it is very important to have a good, hard-to-guess **password** for the WLAN connections.

Typically, the **range** of a wireless connection is about **50m**, but it depends how many walls, etc. are in the way.

Wide Area Network (WAN)

A Wide Area Network is a network that extends over a **large area**.

A WAN is often created by **joining several LANs** together, such as when a business that has offices in different countries links the office LANs together.

Because WANs are often geographically spread over large areas and **links** between computers are over **long distances**, they often use quite exotic connections technologies: **optical fibre** cables, **satellite** radio links, **microwave** radio links, etc.
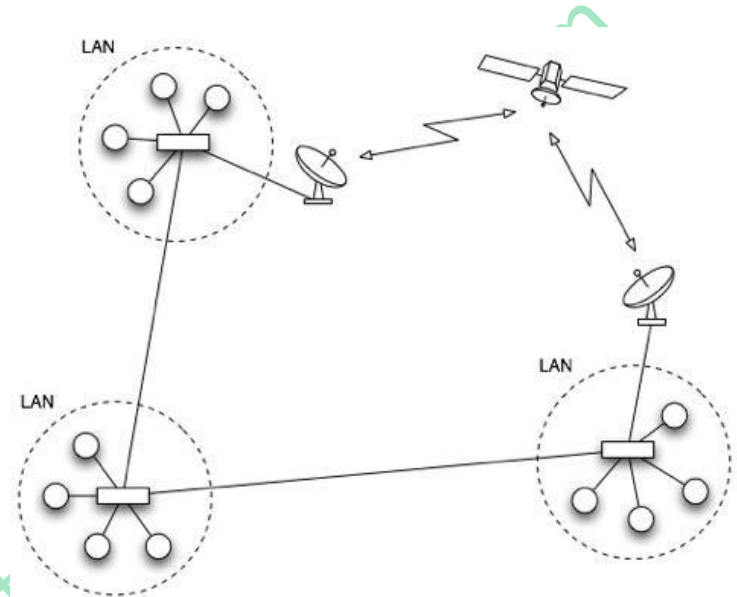
Network Topology

Computers in a network have to be connected in some logical manner. The layout pattern of the interconnections between computers in a network is called network topology. You can think of topology as the virtual shape or structure of the network. Network topology is also referred to as 'network architecture.'

Devices on the network are referred to as 'nodes.' The most common nodes are computers and peripheral devices. Network topology is illustrated by showing these nodes and their connections using cables. There are a number of different types of network topologies, including point-to-point, bus, star, ring, mesh, tree and hybrid. Let's review these main types.

Bus Topology

Bus topology uses one main cable to which all nodes are directly connected. The main cable acts as a **backbone** for the network. One of the computers in the network typically acts as the computer server. The first advantage of bus topology is that it is easy to connect a computer or peripheral device. The second advantage is that the cable requirements are relatively small, resulting in lower cost.

One of the disadvantages is that if the main cable breaks, the entire network goes down. This type of network is also difficult to troubleshoot. For these reasons, this type of topology is not used for large networks, such as those covering an entire building.
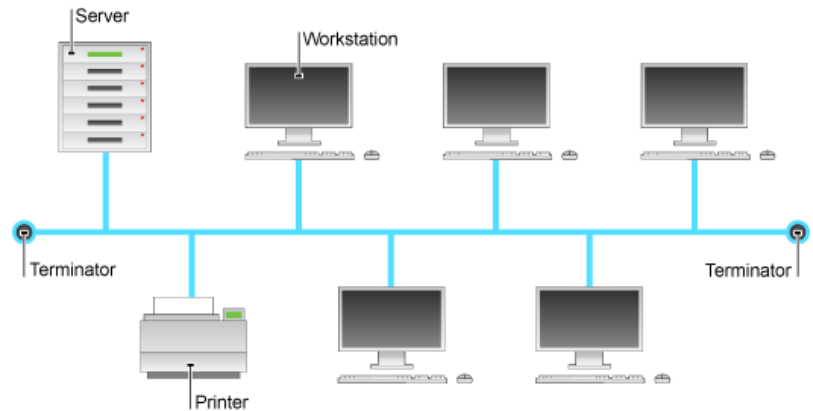
Star Topology:

In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible.
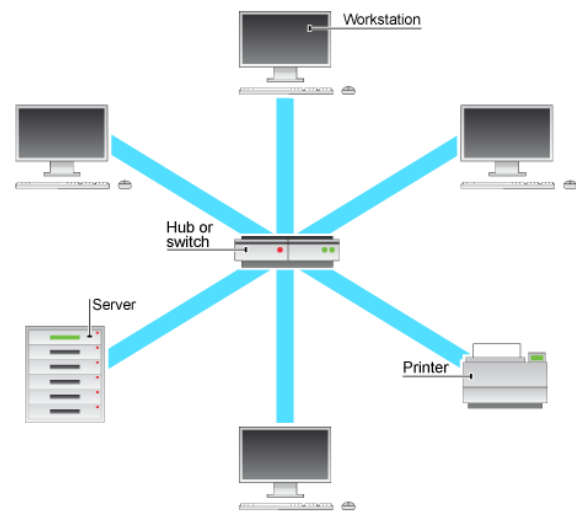
Star topology is very popular because the startup costs are low. It is also easy to add new nodes to the network. The network is robust in the sense that if one connection between a computer and the hub fails, the other connections remain intact. If the

central hub fails, however, the entire network goes down. It also requires more cable than bus topology and is, therefore, more expensive.

Mesh Topology:

In mesh topology, every node has a direct point-to-point connection to every other node. Because all connections are direct, the network can handle very high-volume traffic. It is also robust because if one connection fails, the others remain intact. Security is also high since data travels along a dedicated connection.
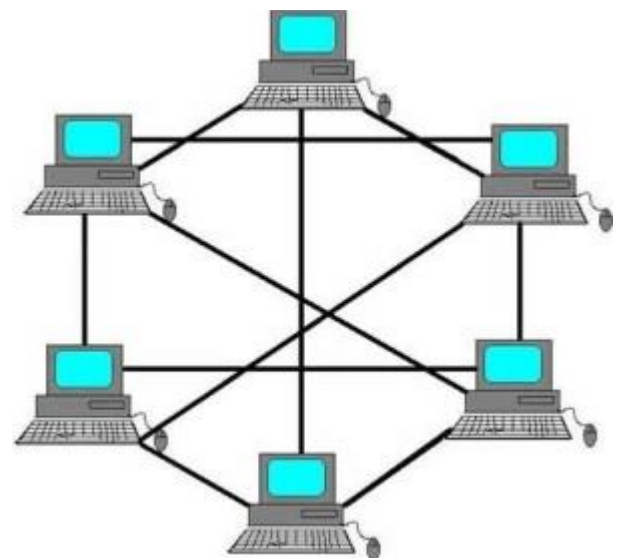
This type of topology requires a lot of cables and is, therefore, expensive. Many of the connections are

also redundant since there are several different paths for data to travel from one node to another.

Tree Topology:

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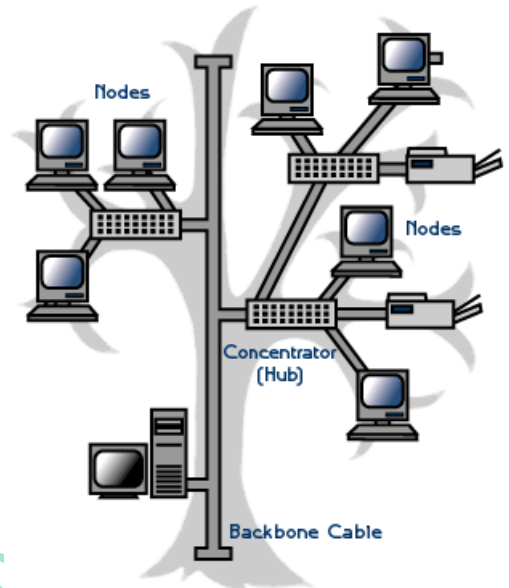
HYBRID Topology:

Hybrid topology is combination of two or more different topologies (e.g., bus, star, ring, etc.).
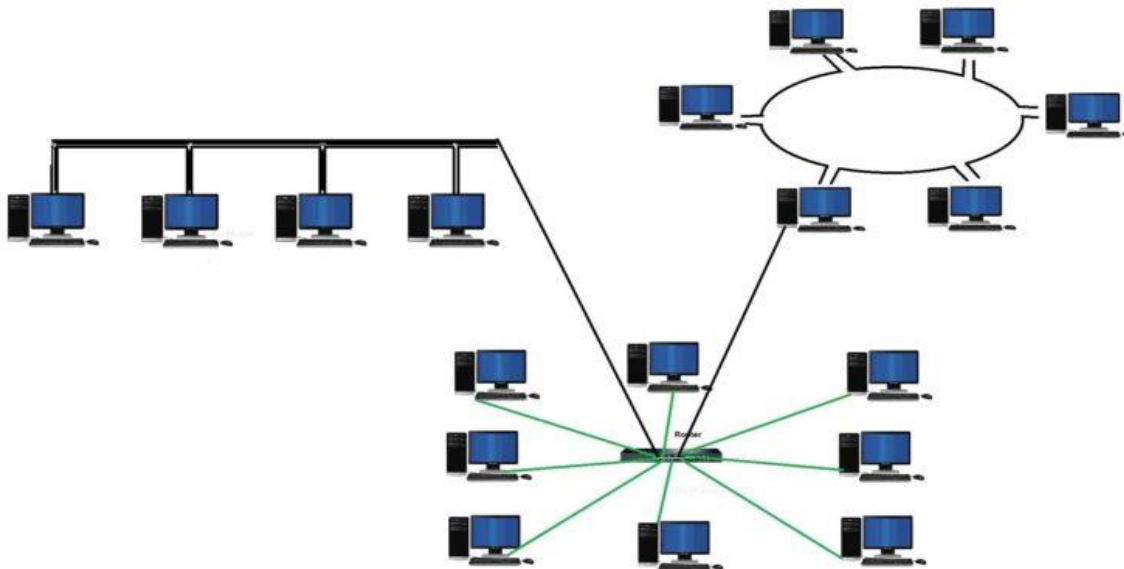
The Hybrid network is based on both peer-to-peer and; client-server relationship.

A hybrid topology is always produced when two different basic network topologies are connected.

This network topology can be wired or wireless. Hybrid network topology allows the network.

Public and Private Cloud Computing

Cloud storage

The Cloud Storage is method of data storage where data is stored on off-site servers. The physical storage covers hundreds of servers in many locations.
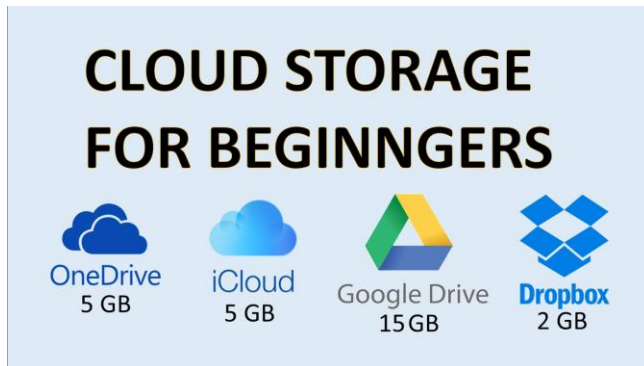
- **Cloud storage** is a model of computer data storage in which the digital data is stored in logical pools.

- The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically owned and managed by a hosting company.

- These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running.

- People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Public Cloud: is a storage environment where the customer/client and cloud storage provider are different companies

Private Cloud: is storage provided by dedicated environment behind a company firewall. Customer/Client and cloud storage provider are integrated and operate on a single entity.

Hybrid Cloud: is a combination of public and private clouds. Some data resides at private cloud and less commercial or less sensitive data is on Public cloud.Instead of saving data on local hard disk or other storage devices, user can save data on cloud storage. The Pros and Cons are given in table below:

Pros of using cloud storage	Cons of using cloud storage
• customer/client files stored on the cloud can be accessed at any time from any device anywhere in the world provided internet access is available • no need for a customer/client to carry an external storage device with them, or use the same computer to store and retrieve information • provides the user with remote back-up of data to aid data loss and disaster recovery • recovers data if a customer/client has a hard disk or back-up device failure • offers almost unlimited storage capacity	• if the customer/client has a slow or unstable internet connection, they would have problems accessing or downloading their data/files • costs can be high if large storage capacity is required • expensive to pay for high download/upload data transfer limits with the customer/client internet service provider (ISP) • potential failure of the cloud storage company is possible – this poses a risk of loss of all back-up data

Internet

The **Internet** is an example of a **global WAN** .In fact it is the world's largest WAN. Computers on the International Space Station are linked to the Internet, so then you could say that the Internet is now the first off-planet WAN!

Bluetooth (Personal Area Network) WPAN

Bluetooth is a wireless networking technology designed for very **short-range** connections (typically just a few meters). The idea of Bluetooth is to get rid of the need for all of those cables (e.g. USB cables) that connect our computer to peripheral devices such as printers, mice, keyboards, etc. Bluetooth devices contain small, **low-power** radio transmitters and receivers. When devices are in range of other Bluetooth devices, they detect each other and can be **'paired'** (connected)

Typical uses of Bluetooth:
- Connecting a **wireless keyboard** to a computer
- Connecting a **wireless mouse** to a computer
- Using a **wireless headset** with a mobile phone
- **Printing wirelessly** from a computer or PDA
- **Transferring data** / music from a computer to an MP3 player
- **transferring photos** from a phone / camera to another device
- **Synchronizing** calendars on a PDA and a computer
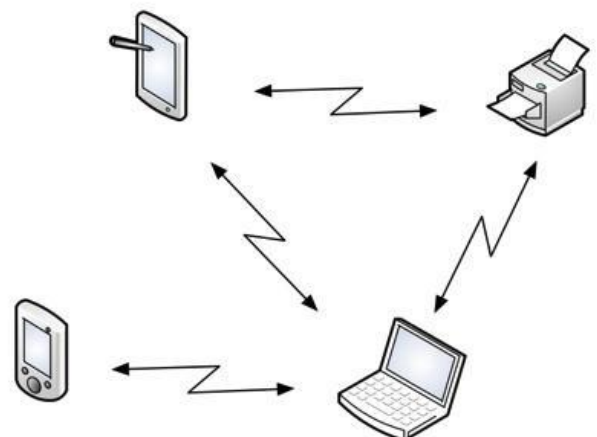
World Wide Web:

- The term "**WWW**" refers to the "**World Wide Web**" or simply the Web.
- The World Wide Web consists of all the public Web sites connected to the Internet worldwide, including the client devices (such as computers and cell phones) that access Web content.
- The WWW is just one of many applications of the Internet and computer networks.

Internet:

The Internet is named for "interconnection of computer networks". It is a massive hardware combination of millions of personal, business, and governmental computers, all connected like roads and highways.

The Internet started in the 1960's under the original name **"ARPAnet"**. ARPAnet was originally an experiment in how the US military could maintain communications in case of a possible nuclear strike. With time, ARPAnet became a civilian experiment, connecting university mainframe computers for academic purposes.
As personal computers became more mainstream in the 1980's and 1990's, the Internet grew exponentially as more users plugged their computers into the massive network. Today, the Internet has grown into a public spider web of millions of personal, government, and commercial computers, all connected by cables and by wireless signals.

No single person owns the Internet. No single government has authority over its operations. Some technical rules and hardware/software standards enforce how people plug into the Internet, but for the most part, the Internet is a free and open broadcast medium of hardware networking.

It is important to understand that the Internet is not a WAN; it is the biggest internetwork in existence. Furthermore, it has never been designed as a coherent entity; it has just evolved to reach its current form and is still evolving to whatever future form it will take. There is no agreed definition of its structure; however, there is a hierarchical aspect to the structure particularly with respect to the role of an Internet Service Provider (ISP).
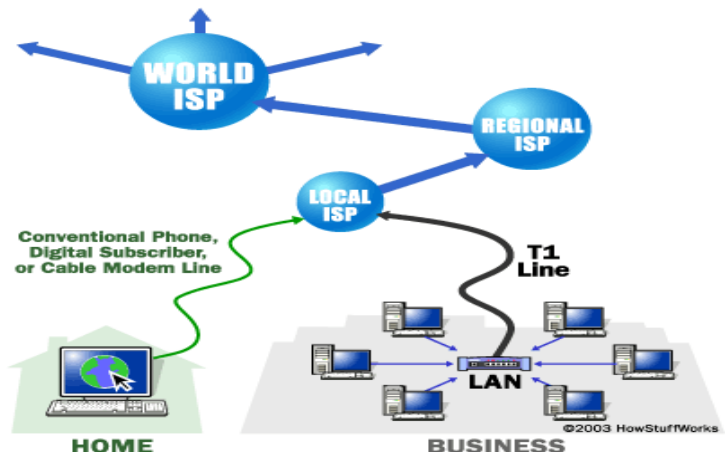
Access ISP's or Tier-3:

The initial function of the ISP was to give Internet access to an individual or company. This function is now performed by what may be described as an **'access ISP'**.

Regional ISPs or Tier-2:

Access ISPs might then connect to what might be called '**middle tier**' or **regional ISPs** which in turn are connected to **tier1 ISPs.**

Internet Backbone or Tier-1:

Tier-1 ISPs are also known as **Internet backbone ISPs**. An ISP is a network and connections between ISPs are handled **by Internet Exchange Points (IXPs)**. The other networks which can be considered to share the top of the hierarchy with **tier1** ISPs are the major content providers.

The New Internet
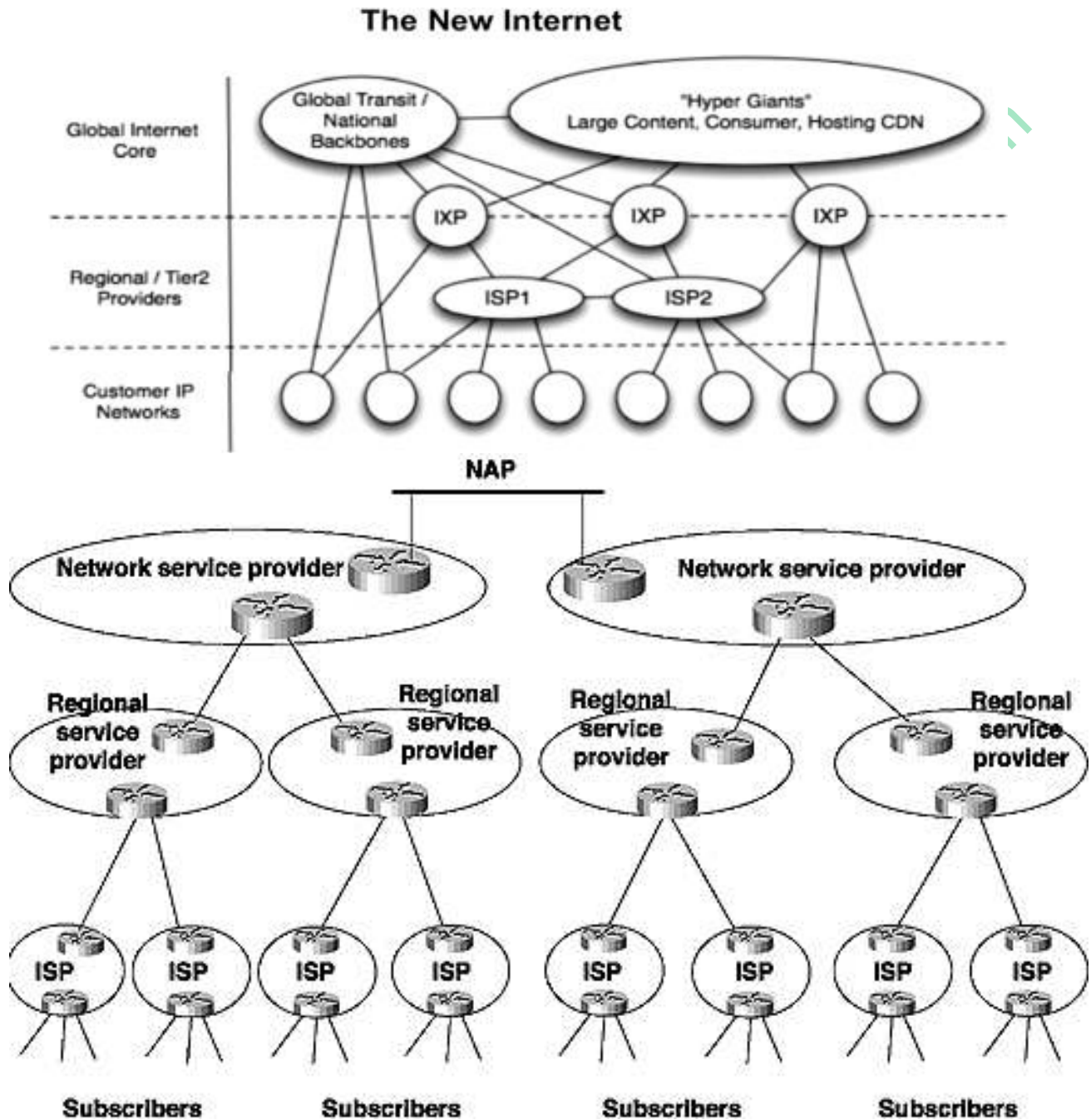
Although the Internet has grown away from the single-backbone architecture of the ARPANET described earlier, it retains a certain hierarchical structure.

At the lowest level, Internet subscribers connect to an Internet service provider (ISP). In many cases, that ISP is one of many small providers in the local geographic area (called local ISPs).

These local ISPs in turn are the customers of larger ISPs that cover an entire geographic region such as a state or a group of adjacent states. These larger ISPs are called regional service providers.

The regional service providers, in turn, connect to large ISPs with high-speed backbones spanning a national or global area. These largest providers are the network service providers, these various providers are referred to as Tier III, Tier II, and Tier I providers, respectively.

(NAPs) Network Access Points:
At the highest level, the **(NSPs) network service providers** interconnect via network access points (NAPs). A Network Access Point (**NAP**) was a public network exchange facility where **Internet service providers** (**ISPs**) connected with one another in peering arrangements, across which different providers can exchange routes and data traffic.

Networking Hardware

Network Interface Card (NIC)

Any computer that is to be connected to a network needs to have a network interface card (NIC). Most modern computers have these devices built into the motherboard, but in some computers you have to add an extra expansion card (small circuit board)
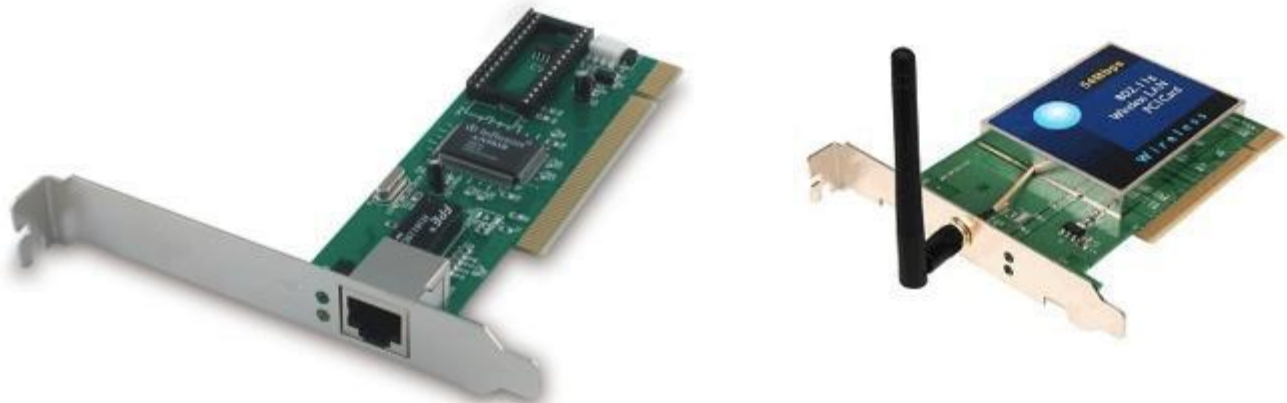
Some computers, such as laptops, have two NICs: one for **wired** connections, and one for **wireless** connections (which uses radio signals instead of wires)
In a laptop, the wireless radio antenna is usually built in to the side of the screen, so you don't need to have a long bit of plastic sticking out the side of your computer!

Hub:

A hub is a device that **connects** a number of computers together to make a **LAN**. The typical use of a hub is at the **centre of a star network** (or as part of a hybrid network) - the hub has cables plugged into it from each computer
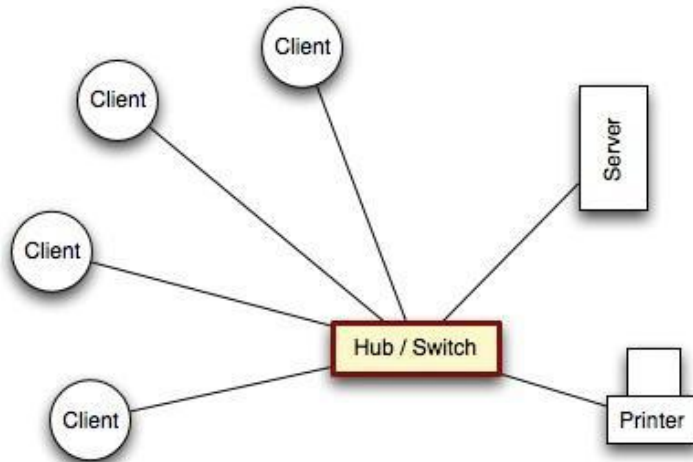
.
A hub is a '**dumb**' device: if it receives a message, it sends it to **every computer** on the network. This means that hub-based networks are **not very secure** - everyone can listen in to communications.
Hubs are pretty much obsolete now (you can't buy them any more), having been superseded by cheap switches.

Switch

A switch, like a hub, is a device that **connects** a number of computers together to make a **LAN**. The typical use of a switch is at the **centre of a star network** (or as part of a hybrid network) - the switch has cables plugged into it from each computer. A switch is a more '**intelligent**' device than a hub: if it receives a message, it checks who it is **addressed** to, and only sends it to that **specific computer**. Because of this, networks that use switches are **more secure** than those that use hubs, but also a little more **expensive**.
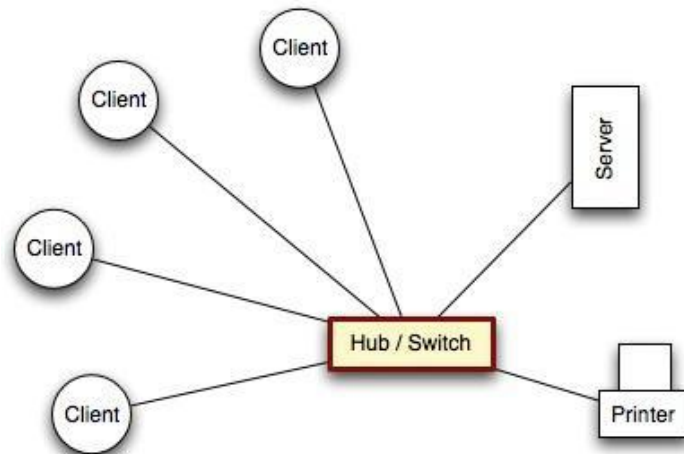
Router
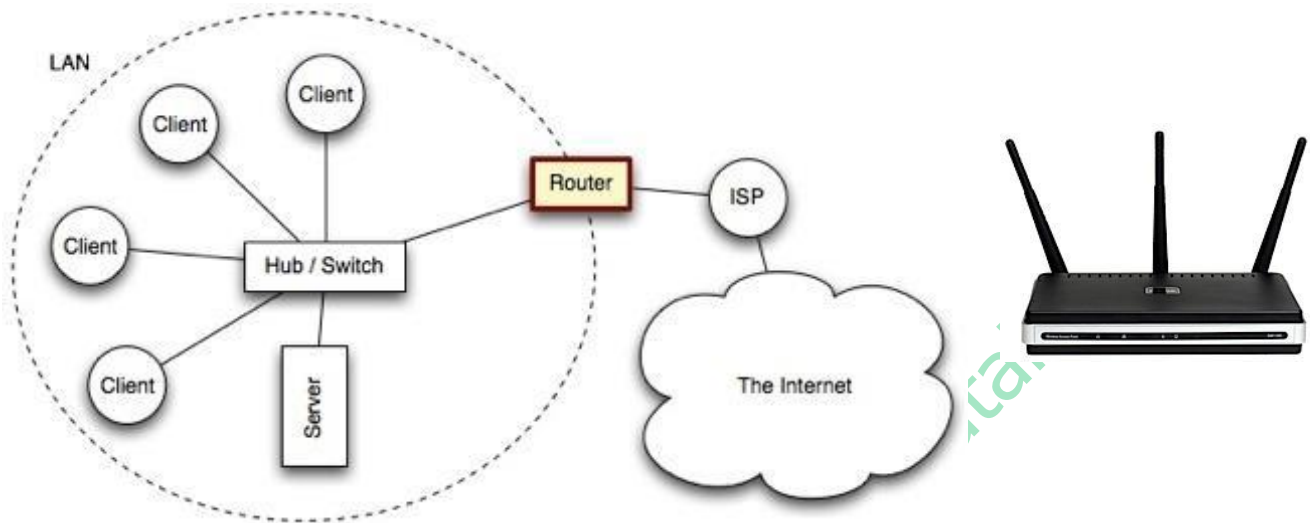
A router is a network device that **connects** together **two or more networks**.

A common use of a router is to **join** a home or business network (**LAN**) to the **Internet** (WAN). The router will typically have the Internet cable plugged into it, as well as a cable, or cables to computers on the LAN. **// acts as the single access point for**

Alternatively, the LAN connection might be wireless (WiFi), making the device a **wireless router**. (A wireless router is actually a router and wireless switch combined)

Receives packets and forwards towards the destination using the IP address of the destination. Assigns private IP addresses

Operates between similar networks // networks using the same protocol

Routers are the devices that join together the various different networks that together make up the **Internet**. These routers are much more **complex** than the one you might have in your home

CSMA/ CD:

Carrier-sense multiple access with collision detection (**CSMA/CD**)
CSMA CA operates by sensing the state of the medium in order to prevent or recover from a collision. A **collision** happens when two transmitters transmit at the same time.

The data gets scrambled, and the receivers would not be able to discern one from the other thereby causing the information to get lost. The lost information needs to be resent so that the receiver will get it.
CSMA CD operates by detecting the occurrence of a collision. Once a collision is detected CSMA CD immediately terminates the transmission and again it starts listening, whether any data transmitting or not.

CSMA CA does not deal with the recovery after a collision. It checks whether the medium is in use or not. If it is busy, then the transmitter waits until it is idle state, before it starts transmitting data. This effectively minimizes the possibility of collisions and makes more efficient use of the medium.

CSMA CA reduces the possibility of a collision, **it is used in wireless network** while **CSMA CD** only minimizes the recovery time after collision which will occur frequently in wired network so this CSMA CD helps here better

Carrier-sense multiple access with collision detection (**CSMA/CD**) process

- Calculate a random wait time
- Wait for the random time
- Check for idle bus // Check status of bus
- Attempt to re-transmit / re-send
    - o If unable to transmit
    - o repeat above process

Proxy Server:

- A proxy server is a computer setup to **share a resource**, usually an **Internet connection**.
- Other computers can request a web page via the proxy server.
- The proxy server will then get the page using its Internet connection, and pass it back to the computer who asked for it.
- Proxy servers are often used instead of router since **additional software** can be easily installed on the computer such as anti-virus, web filtering etc.
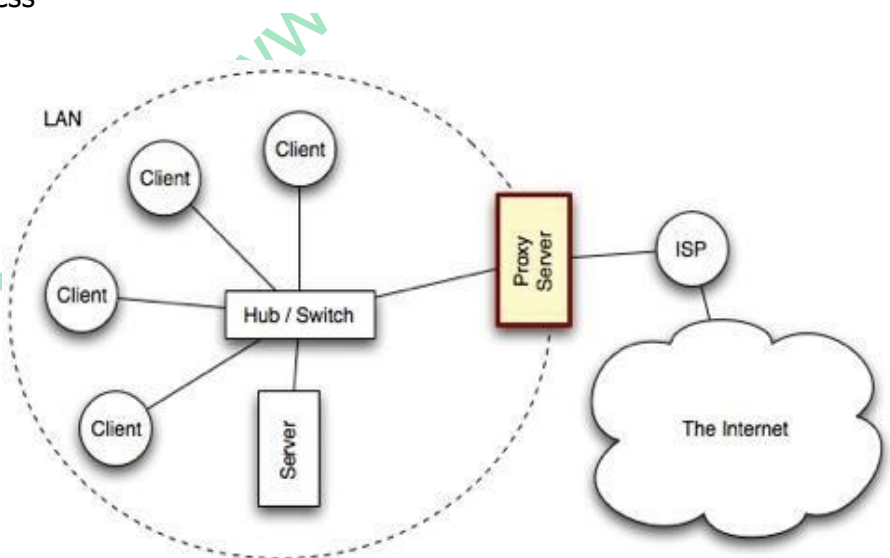
Bridge:

A bridge is a network device that typically **links** together **two different parts of a LAN**.
A router is usually used to link a LAN to a WAN (such as the Internet), whereas a bridge links independent parts of a LAN so that they act as a single LAN.
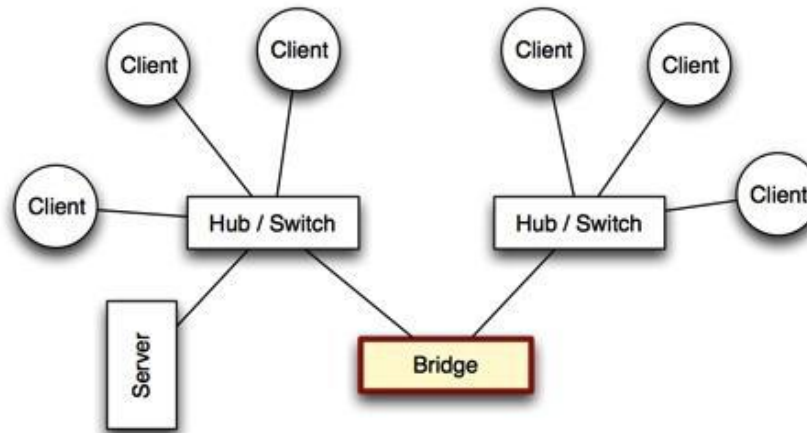
Firewall

A firewall is a **device**, or a piece of **software** that is placed between your computer and the rest of the network (where the hackers are!)
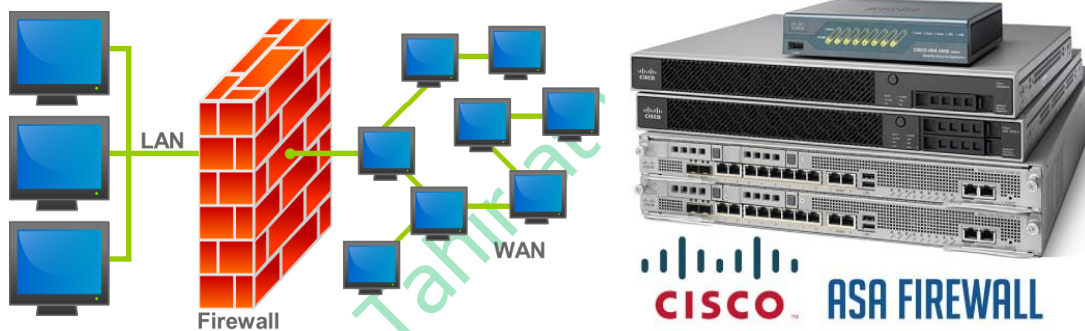
If you wish to **protect** your whole LAN from **hackers** out on the Internet, you would place a firewall **between the LAN and the Internet connection**.

A firewall **blocks unauthorized connections** being made to your computer or LAN. Normal data is allowed through the firewall (e.g. e-mails or web pages) but all other data is
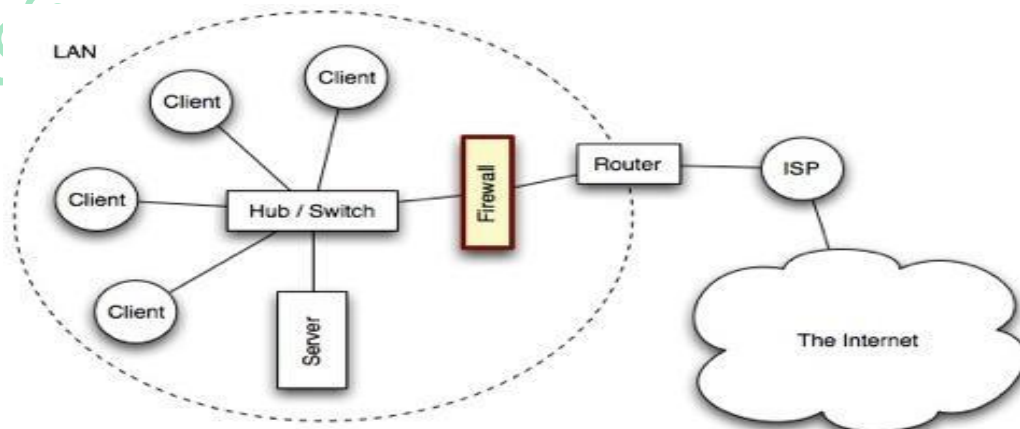
blocked.

In addition to physical devices, firewalls can also be software. In fact most computer operating systems have a software firewall built in (e.g. Windows, Linux and Mac OS)
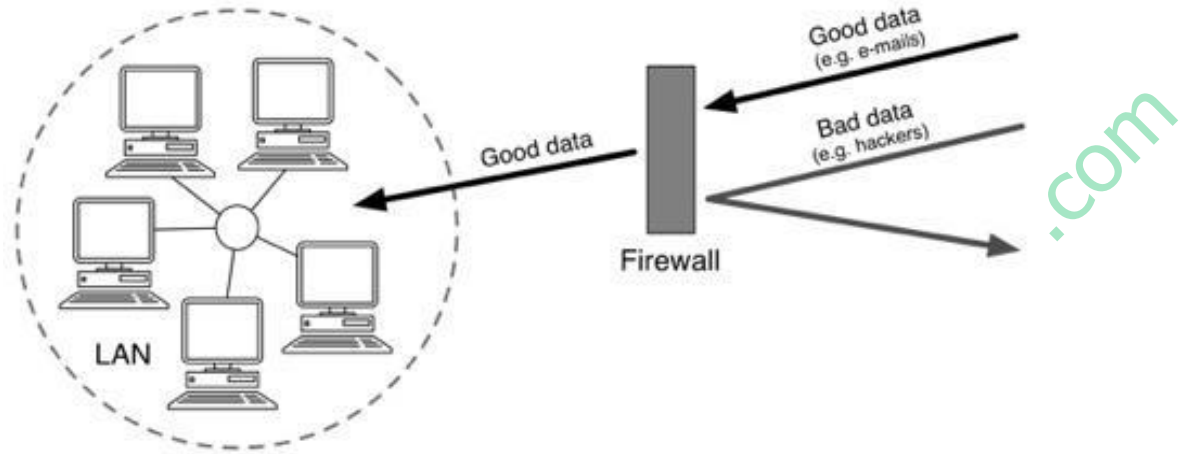
Hardware firewall advantages:

A single hardware firewall can protect your entire network

They run on their own dedicated CPU and memory not taking away computer resources

Hardware firewalls cannot be disabled by malware as easily as software firewalls can

A single hardware firewall can protect multiple computers not needing a license for each computer

Hardware firewalls still protect the computer when the operating system crashes

Hardware firewall disadvantages:

A single router firewall is considerably more expensive than a license for a single software firewall

Hardware firewalls are more difficult to configure than software firewalls

Hardware firewalls need physical space where to install it and cable layout

A hardware firewall protecting the whole network will affect multiple computers if it fails

Gateway:

A gateway is a network node connecting two networks that use different protocols.

The term Gateway is used in networking to describe the "Gate" to the Internet. The Gateway controls traffic that travels from the inside network to the Internet and provides security from traffic that wants to enter the inside network from the Internet.

Connect two (or more) networks

Can connect a network to a WAN // acts as the single access point for

- Receives packets and send packets towards the destination
- using the IP address of the destination
- Assigns private IP addresses
- **Connects two dissimilar networks // networks that use different protocols**
- Gateways can take several forms -- including routers or computers -- and can perform a variety of tasks.
- These range from simply passing traffic on to the next <u>hop</u> on its path to offering complex traffic <u>filtering</u>, <u>proxies</u> or protocol translations at various <u>network layers</u>.
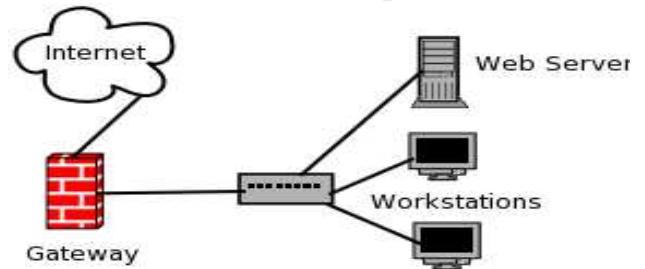
In most <u>IP</u>-based networks, the only traffic that doesn't go through at least one gateway is traffic flowing among <u>nodes</u> on the same local area network (<u>LAN</u>) segment -- for example, computers connected to the same <u>switch</u>.

Difference between Router & Gateway:

A **gateway** acts as a conversion from one protocol to another or in the case of Voice over IP (VoIP) from the VoIP (Voice over internet protocol) network to the POTS (Plain Old Telephone Service) network.

A **router** works by looking at the IP address in the data packet and decides if it is for internal use or if the packet should move outside the network (to the WAN).

PSTN (Public Switched Telephone Network)

- The PSTN consists of many different types of communication lines
- Data is transmitted in both directions at the same time // (full) duplex data transmission.
- The communication passes through different switching centres

Dedicated Lines:

Benefit:

- (Probably) faster connection / communication / transmission of data
- (Usually) more consistent transmission speed
- Improved security

Drawback:

- Expensive to set-up / maintain
- Disruption to the dedicated line would leave no alternative

Repeaters

In telecommunications, a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.
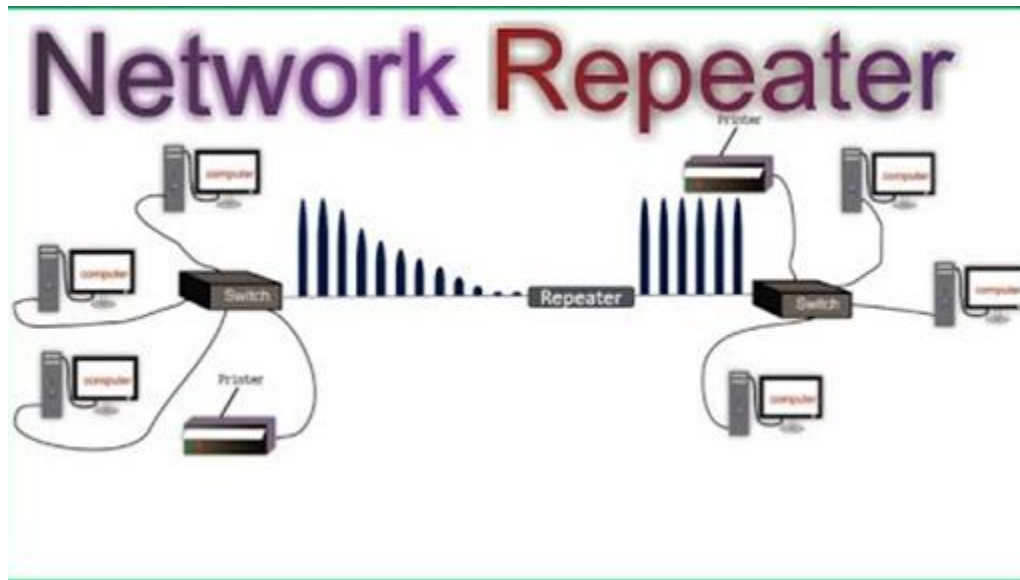
Transmission media
Network Cables

To connect together different devices to make up a network, you need cables. **Cables** are still used in most networks, rather than using only wireless, because they can carry much more **data per second**, and are more **secure** (less open to hacking).

The most common type of network cable in use today looks like the one shown above, with plastic plugs on the ends that snap into sockets on the network devices. Inside the cable are several copper wires (some used for sending data in one direction, and some for the other direction).

Cable:

The options for a cable are twisted pair, coaxial or fibre-optic. (The first two use copper for the transmission medium.)
In discussing suitability for a given application there are a number of factors to consider. One is the cost of the cable and connecting devices. Another is the bandwidth achievable, which governs the possible data transmission rate. There are then two factors that can cause poor performance: the likelihood of interference affecting transmitted signals and the extent of attenuation (deterioration of the signal) when high frequencies are transmitted. These two

factors affect the need for repeaters or amplifiers in transmission lines. Table 2.01 shows some comparisons of the different cable types.

	Twisted pair	Coaxial	Fibre-optic
Cost	Lowest	Higher	Highest
Bandwidth or data rate	Lowest	Higher	Much higher
Attenuation at high frequency	Affected	Most affected	Least affected
Interference	Worst affected	Less affected	Least affected
Need for repeaters	More often	More often	Less often

Table 2.01 Comparisons between cable types

Fiber optics

Fibre optic cabling is made from glass that becomes very flexible when it is thin. Light is passed through the cable using a <u>transmitter</u>. Light travels quickly through the light-reflecting internal wall of the cable.
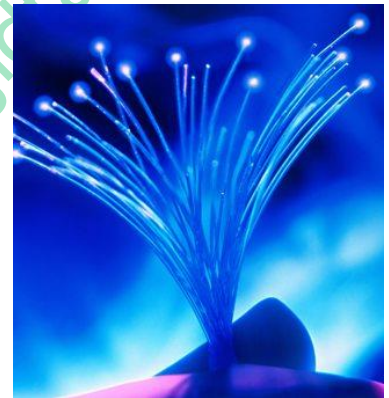
The transmitter in the <u>router</u> sends light pulses representing <u>binary</u> code. When the data is received, it is decoded back to its binary form and the computer displays the message.
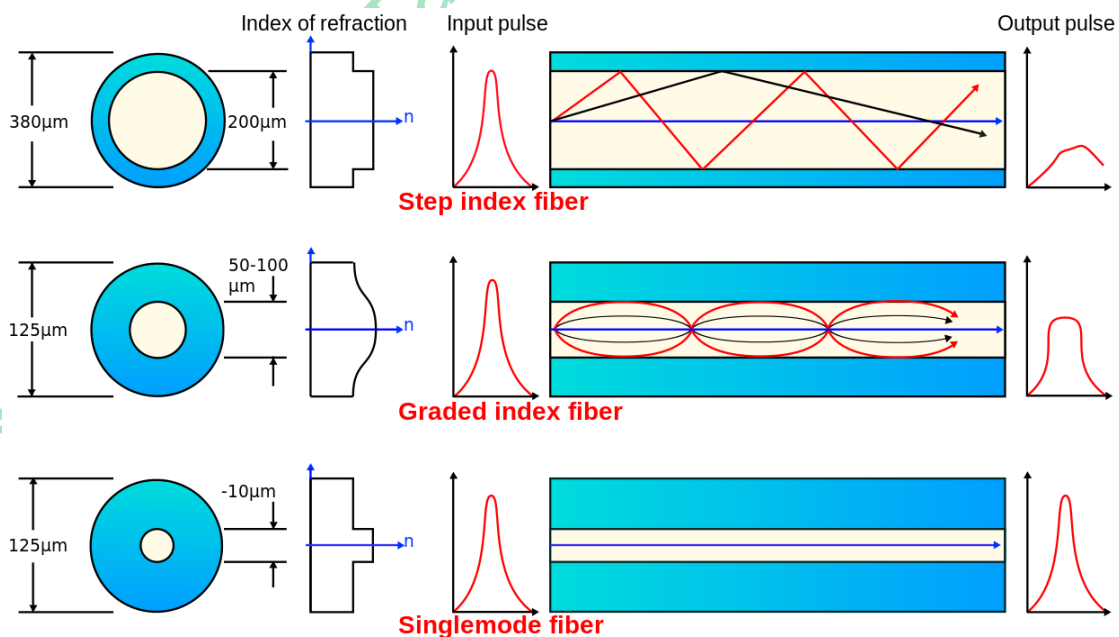
Fiber optics is a technology that uses glass (or plastic) threads (fibers) to transmit data. A fiber optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves.

Advantages

- the individual cables are thinner, so larger quantities of cable can be joined together compared to copper
- there is less interference than copper
- there is less chance for degeneration

PE jacket
Water blocking tape
Loose tube
FRP
Flooding compound
Optical fiber
Filling compound

Disadvantages

- replacing copper with fibre optic cabling is expensive
- They are more fragile than wire and are difficult to splice.

Optical fibre submarine systems

Uses:

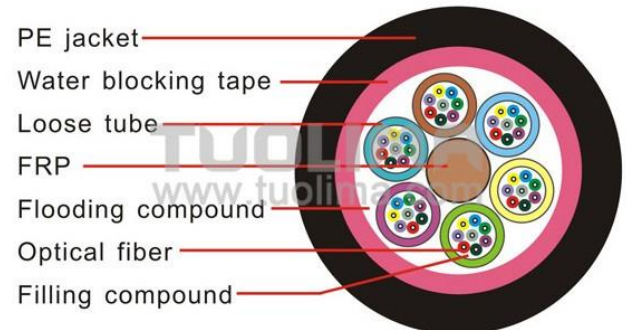**Optical** fibers are **used** most often as a means to transmit light between the two ends of the **fiber** and find wide usage in **fiber-optic** communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than wire **cables**

In **submarine** communications **cable**s laid on the sea bed between land-based stations to carry telecommunication signals across stretches of ocean. ... Modern **cables use optical fiber** technology to carry digital data, which includes telephone, Internet and private data traffic.
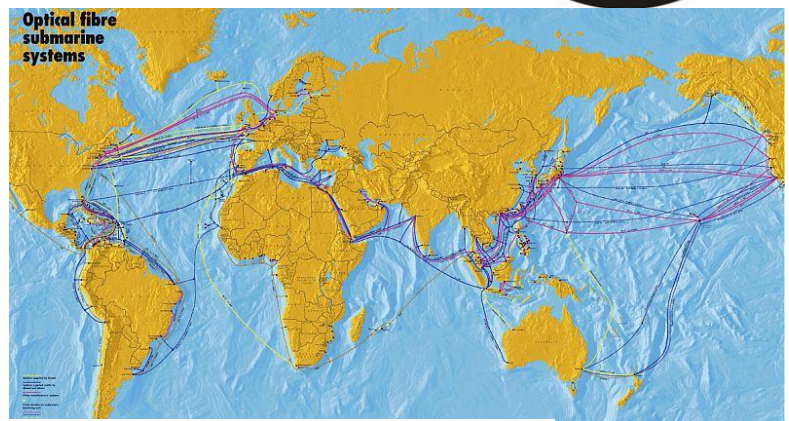
Record speeds [Wikipedia]

- **2006** – Nippon Telegraph and Telephone Corporation transferred 14 terabits per second over a single 160 km long optical fiber
- **2009** – Bell Labs in Villarceaux, France transferred 100 Gbit/s over 7000 km fiber
- **2010** – Bell Labs in Villarceaux, France transferred 100 petabits per second.
- **2010** – Nippon Telegraph and Telephone Corporation transferred 69.1 Tbit/s over a single 240 km fiber multiplexing 432 channels, equating to 171 Gbit/s per channel
- **2012** – Nippon Telegraph and Telephone Corporation transferred 1 Petabit per second over 50 kilometers over a single fiber

Copper cable

Copper cable uses electrical signals to pass data between networks. There are three types of copper cable: coaxial, unshielded twisted pair and shielded twisted pair.

- **Coaxial** degenerates over long distances.

Coaxial Cables

Invented back in the 1880s, "coax" was best known as the kind of cable that connected television sets to home antennas. Coaxial cable is also a standard for 10 Mbps Ethernet cables.

A conducting wire surrounded by a plastic non-conducting layer, which is in turn covered by a cylinder of conducting material and finally surrounded by PVC jacket.
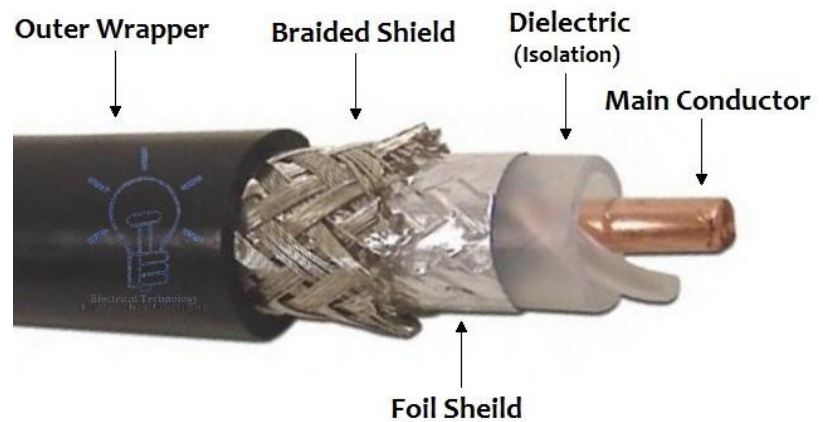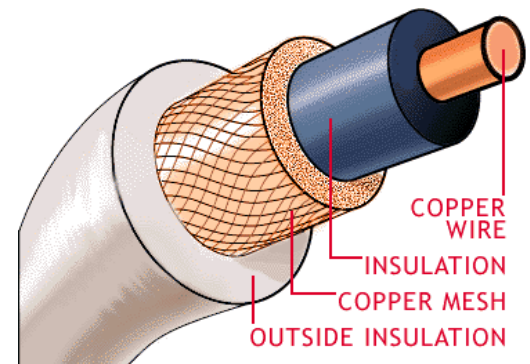
Twisted Pair Cables

Twisted pair eventually emerged during the 1990s as the leading cabling standard for Ethernet, starting with 10 Mbps (10BASE-T, also known as Category 3 or Cat3), later followed by improved versions for 100 Mbps (100BASE-TX, Cat5 and Cat5e) and successively higher speeds up to 10 Gbps (10GBASE-T).

Ethernet twisted pair cables contain up to 8 wires wound together in pairs to minimize electromagnetic interference.

Two primary types of twisted pair cable industry standards are defined –Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).
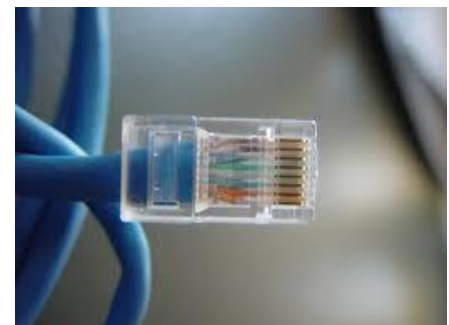
Modern Ethernet cables use UTP wiring due to its lower cost, while STP cabling can be found in some other types of networks.

- **Unshielded twisted pair** is made by twisting the copper cables around each other and this reduces degeneration.

- **Shielded twisted pair** uses copper shielding around the twisted wires to make them less susceptible to interference.

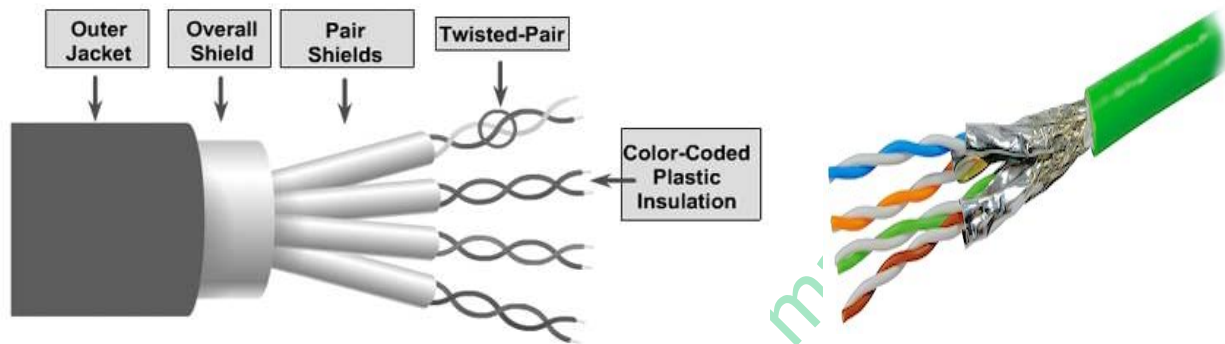The extra covering in **shielded twisted pair** wiring protects the transmission line from electromagnetic interference leaking into or out of the **cable**. STP cabling often is used in Ethernet networks, especially fast data rate Ethernets. Contrast with UTP.

Advantages

- a cabled telephone can be powered directly from the copper cable, so the phone will still work if there is a loss of power
- copper can be cheaper to set up than fibre optic cabling

Disadvantages

- degenerates over long distances

Wireless Communication:

Radio waves are an electromagnetic radiation with differing wavelengths. These waves are similar to an ocean wave. Radio waves are used for many processes. For example they are used to broadcast TV, in communication between satellites and it enables computers to share information without wires.

Radio waves have a large wavelength so they experience less interference and can travel over large distances.
However, since they do not have a high frequency, they cannot transmit as much data. However, they can carry more signals than wires; they are often used for linking buildings on a college campus or corporate site and increasingly for longer distances as telephone companies update their networks.

Microwave transmission: refers to the technology of transmitting information by the use of electromagnetic waves whose wavelengths are measured in centimeters; these are called microwaves. This part of the radio spectrum ranges across frequencies of roughly 1.0 gigahertz (GHz) to 30 GHz. These correspond to wavelengths from 30 centimeters down to 1 cm.

- Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna.
- This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do.
- Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it.
- The attenuation of microwave is less than twisted pair or coaxial cable.

A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can. It is also affected by anything blocking the line of sight, such as rainfall.
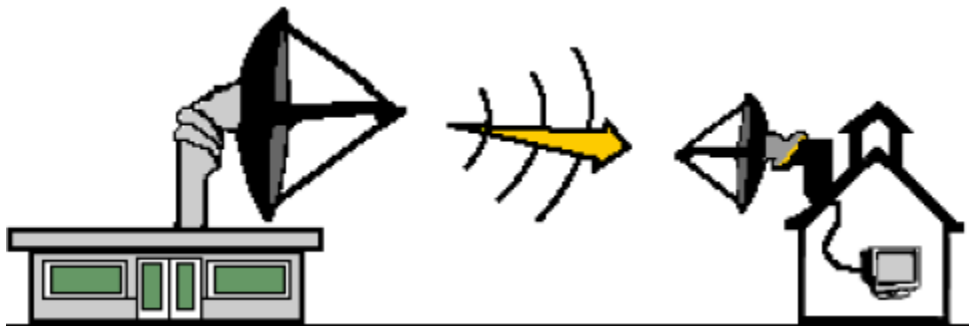
Satellite

is any object that revolves around a planet in a circular or elliptical path. The moon is Earth's natural satellite at 240,000 miles distant. Other satellites that fulfill this definition are man-made and have been launched into orbit to carry out specific functions. These satellites are typically between 100 and 24,000 miles away.

Geostationary Satellite

Microwave Towers

Satellites have many purposes including data communications, scientific applications and weather analysis. Satellite transmission requires an unobstructed line of sight. The line of site will be between the orbiting satellite and a station on Earth. Satellite signals must travel in straight lines but do not have the limitations of ground based wireless transmission, such as the curvature of the Earth.

Microwave signals from a satellite can be transmitted to any place on Earth which means that high quality communications can be made available to remote areas of the world without requiring the massive investment in ground-based equipment.

What is a Bit Stream?

A **bit stream** is a contiguous sequence of **bit**s, representing a **stream** of data, transmitted continously over a communications path, serially (one at a time).

Millions of bits, travel over thousands of computer networks every day. The system works much like the modern post office, which has to constantly send and receive letters from all over the world. Like those letters, computer bits arrive in a continuous, ordered stream known as the bit stream.

The bits identify where they are coming from (often a computer) and where they are traveling to (often another computer).

All the information sent to and from a computer turns into a series of 1's and 0's that represent data. When the computer sends a message, the bits travel in a specific order through a wire to their destination. Typically, the bit stream starts with information about where it's going and how to process the information once it arrives.

An email, for example, contains information on the sender, the recipient, and the message itself. When the user sends it, it's broken down into bits of data which travel over the bit stream to the recipient's computer.

Video on demand (VOD) is a system that may allow users to select and

watch/listen to video or audio content when they choose to, rather than having to watch at a specific broadcast time (Live streaming). Some TV VOD systems such as Netflix or Hulu allow users to watch their favorite shows whenever they please.

Live streaming or real time, as the name suggests, is streaming a video that is

happening at that exact moment. Examples may be a football match, a concert, or a lecture happening at your university.

Video On-demand

- High quality (HD) video and audio
- Plays on computers and smart phones
- Plays smoothly at any Internet speed
- More economical than live streaming

Live Streaming

- No time delay
- Ability to live chat
- Ability to ask and respond to questions
- May require additional hardware and software

A crucial point with media streaming is whether the technology has sufficient power to provide a satisfactory user experience. When the media is created it is the intention that the media is to be delivered to the user at precisely the same speed as used for the creation; a song that lasted four minutes when sung for the recording will sound very peculiar if, when it is received by a user, it lasts six minutes. More specifically, the process of delivering the content will be quantified by the bit rate.

For example, a relatively poor-quality video can be delivered at a bit rate of 300 kbps but a reasonably good-quality audio file only requires delivery at 128 kbps. Below **Figure** shows a simple schematic diagram of the components involved in the streaming.

**Figure** Schematic diagram of bit streaming Media server.

- The bit rate for delivery to the user from the buffer must match the defined rate for the specific media in use but the planned transmission rate to the buffer should be higher to allow for unexpected delays.
- These rates are controlled by the media player by continuous monitoring of the extent of filling of the buffer in relation to the defined high- and low-water marks.
- It is essential to have a buffer size that is sufficiently large for it never to get filled.
- The rate of transmission to the buffer is limited by the bandwidth of the network connection.

For a connection via a PSTN, a broadband link is essential. For good-quality movie presentation the broadband requirement is about 2.5 Mbps. Because this will not be available for all users it is often the practice that an individual video is made available at different levels of compression. The most highly compressed version will be the poorest quality but the bit rate may be sufficiently low for a reasonable presentation with a relatively low bandwidth Internet connection.
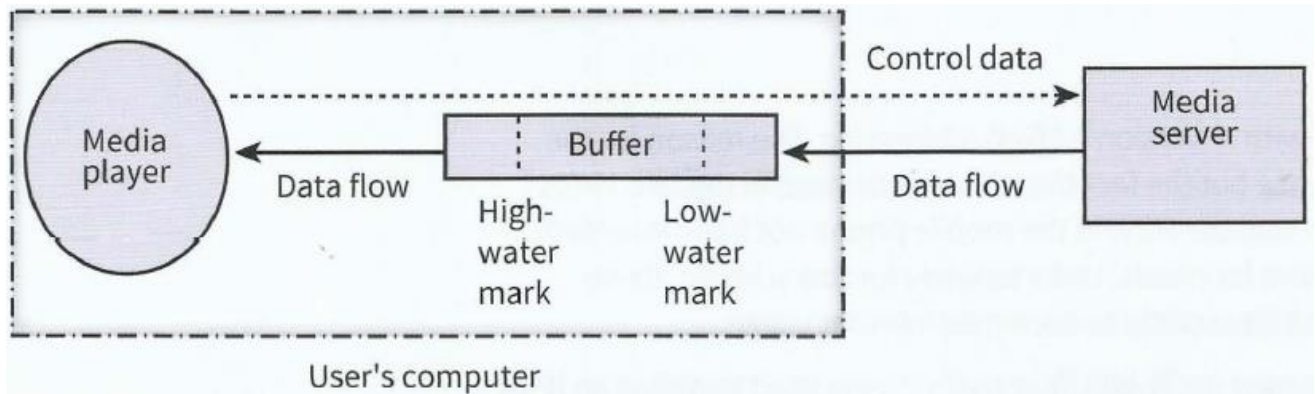
Buffering

A **buffer** is a temporary storage space where data can be held and processed. The buffer holds the data that is required to listen to or watch the media. As data for a file is downloaded it is held in the buffer temporarily. As soon as enough data is in the buffer the file will start playing.
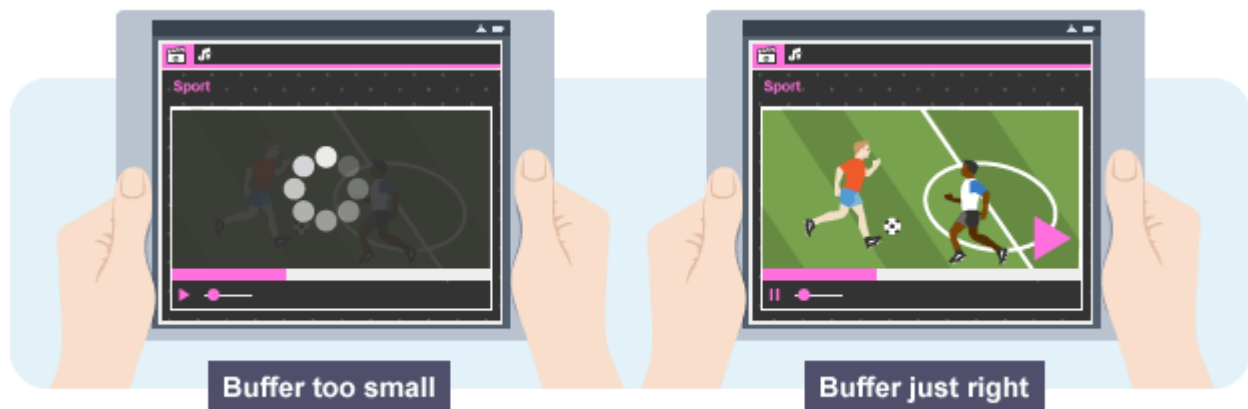
When you see the warning sign 'buffering' this means that the client is waiting for more data from the server. The buffer will be smaller if the computer is on a faster network.

Cellular networks

A mobile phone is often called a 'cell phone' because of the fundamental infrastructure provided for mobile phone users. This is illustrated in Figure 17.08.
Each cell has at its Centre a base station. The system works because each cell has a defined frequency for transmission which is different from the frequencies used in adjacent cells.
Figure 17.08 A collection of mobile phone cells
The technology available in a mobile phone has progressed dramatically through what are described as generations:

- 1G was designed for voice communication using analogue technology.
- 2G went digital.
- 3G introduced multimedia and serious Internet connection capability.
- 4G introduced smartphones with high -bandwidth broadband connectivity.

Refrences:

AS & A level Coursebook by Sylvia Langfield and Dave Duddell.

AS & A level Coursebook by Hodder Education

https://flylib.com/books/en/2.295.1.24/2/

https://www.techstack.in/wp-content/cache/all/blog/country-highest-number-internet-users/index.html