Syllabus Content

3.2 Communication and Internet technologies

3.2.1 Protocols

- protocol is essential for communication between computers
- protocol implementation can be viewed as a stack, where each layer has its own functionality
- function of each layer of the TCP/IP protocol suite
- TCP/IP protocol suite when a message is sent from one host to another on Internet
- BitTorrent protocol for Peer to Peer sharing, (HTTP, FTP, POP3, SMTP) and their purposes

3.2.2 Circuit switching, packet switching and routers

- circuit switching and where it is applicable and packet switching
- function of router in packet switching & how packet switching is used to pass messages across a network.

3.2.3 Local Area Networks (LAN)

- bus topology network, star topology network, and the implications of how packets are transmitted between two hosts
- wireless network
- hardware used to support a LAN: switch, router, servers, Network Interface Cards (NICs), wireless access points
- Ethernet and how collision detection and avoidance (such as CSMA/CD) works

Computer Networks:

Why Use Networks?

Using a computer connected to a network allows us to…

- Easily **share files** and data
- **Share resources** such as printers and Internet connections
- **Communicate** with other network users (e-mail, instant messaging, video-conferencing, etc.)
- **Store data centrally** (using a file server) for ease of access and back-up
- Keep all of our **settings centrally** so we can use any workstation

In particular, if we use a computer connected to The Internet, we can…

- Make use of **on-line services** such as **shopping** (e-commerce) or **banking**
- Get access to a huge range of **information** for research
- Access different forms of **entertainment** (games, video, etc.)
- Join **on-line communities** (e.g. MySpace, Facebook, etc.)

Computers in a Network

Computers connected together to create a network fall into two categories: **servers** and **clients** (workstations).

Clients

- Client computers, or **workstations**, are the **normal computers** that people sit at to get their **work** done.
- When you use your Web browser, you are in fact using a Web **client**. When you type in the URL of a web page, you are actually providing the address of a Web **server**. e.g. **www.bbc.co.uk** is the address of the BBC's web server. Your Web browser/client asks this server for the web page you want, and the server '**serves**' the page back to the browser/client for you to see.

Servers

- Servers are special, powerful computers that provide '**services**' to the **client** computers on the network. These services might include:
- Providing a **central**, common **file storage** area
- **Sharing hardware** such as **printers**
- Controlling who can or can't have **access the network**
- **Sharing Internet** connections

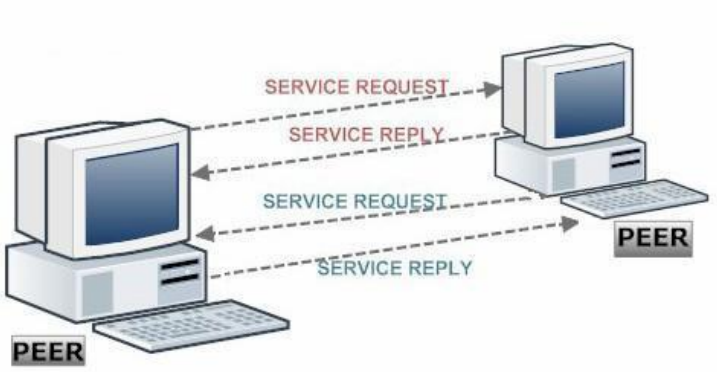
Servers are built to be **very reliable**. This means that they are more **expensive** that normal computers. In a small network one server might provide all of these services. In a larger network there might be many servers sharing the work.

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.'

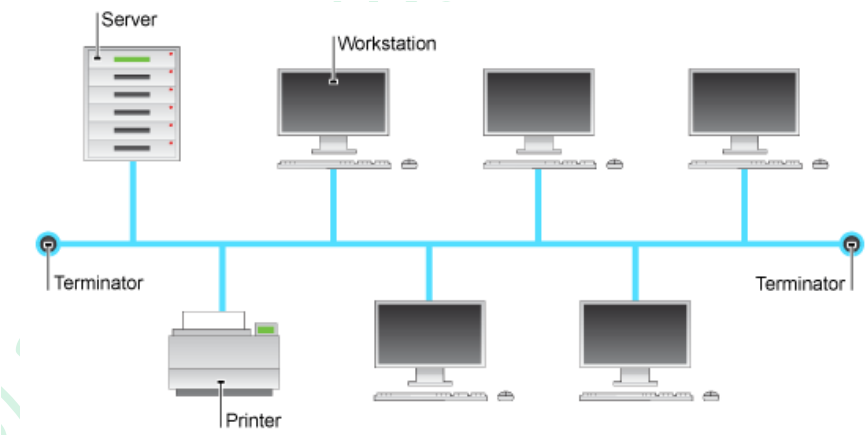
Devices on the network are referred to as 'nodes.' The most common nodes are computers and peripheral devices. Network topology is illustrated by showing these nodes and their connections using cables. There are a number of different types of network topologies, including point-to-point, bus, star, ring,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

Point-to-Point



Point-to-point topology is the simplest of all the network topologies. The network consists of a direct link between two computers. This is faster and more reliable than other types of connections since there is a direct connection. The disadvantage is that it can only be used for small areas where computers are in close proximity.

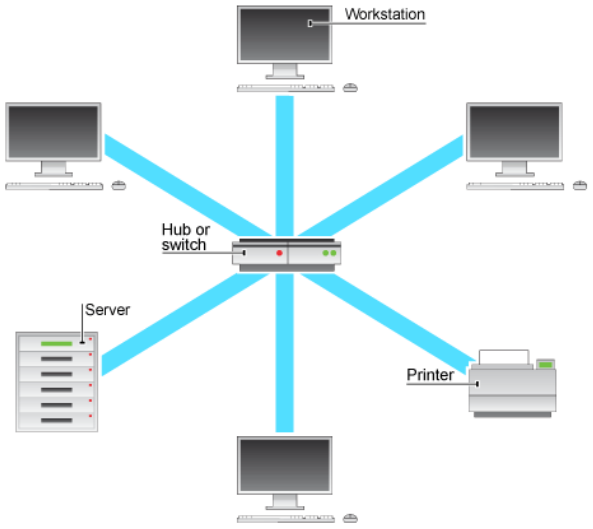
Bus Topology



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:



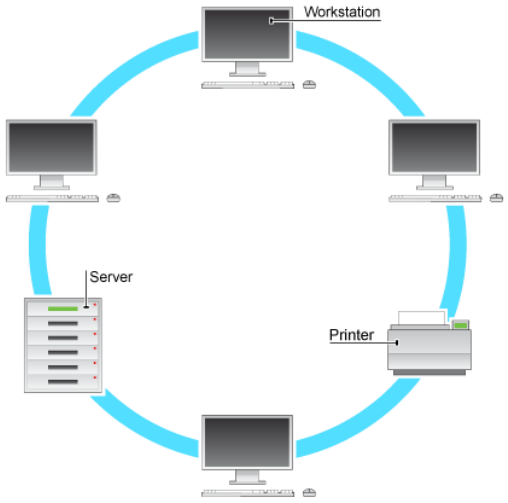
In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only

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.

Ring Topology:

In ring topology, the computers in the network are connected in a circular fashion, and the data travels in one direction. Each computer is directly connected to the next computer, forming a single pathway for signals through the network. This type of network is easy to install and manage.



If there's a problem in the network, it is easy to pinpoint which connection is defective. It is also good for handling high-volume traffic over long distances since every computer can act as a booster of the signal. On the downside, adding computers to this type of network is more cumbersome, and if one single computer fails, the entire network goes down.

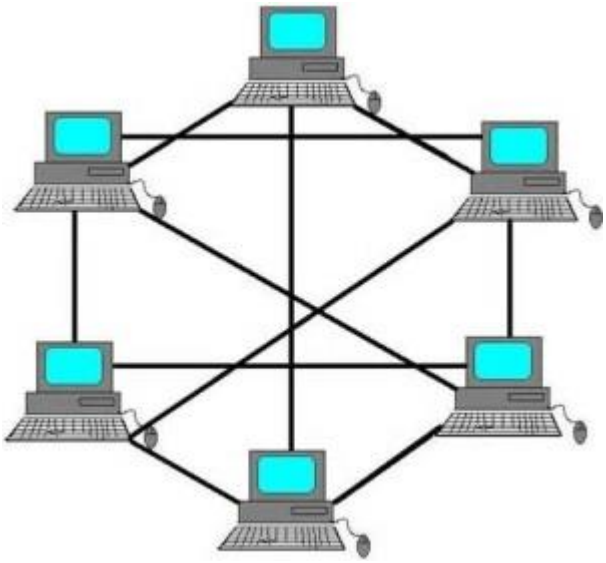
Advantage

This type of network can transfer data quickly, even if there are a large number of devices connected because the data only flows in one direction, so there won't be any data collisions.

Disadvantage

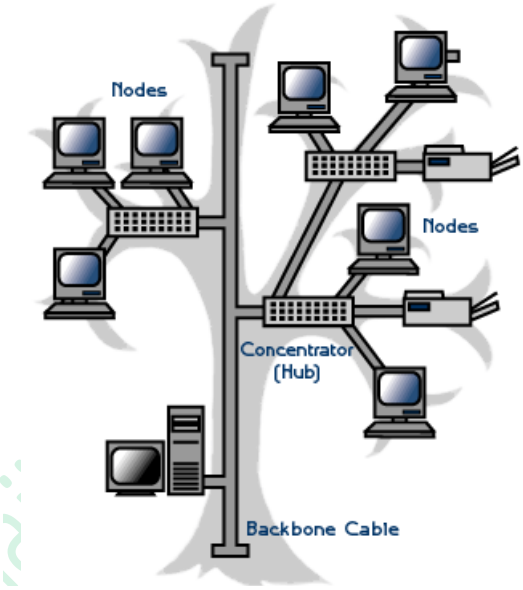
If the main cable fails or any device is faulty then the whole network will fail.

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.

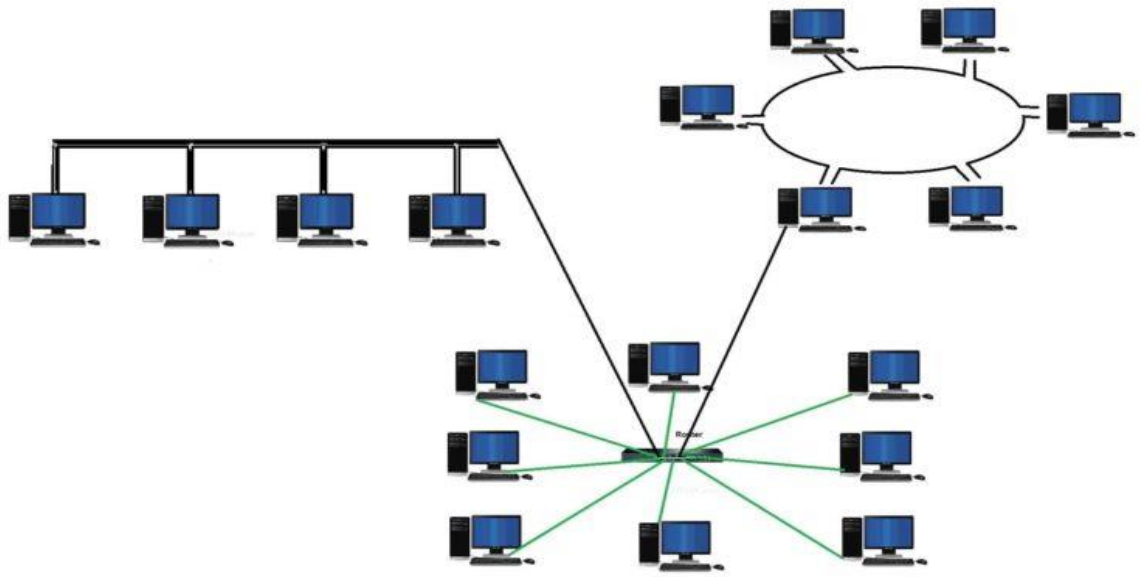


Tree Topology:

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.



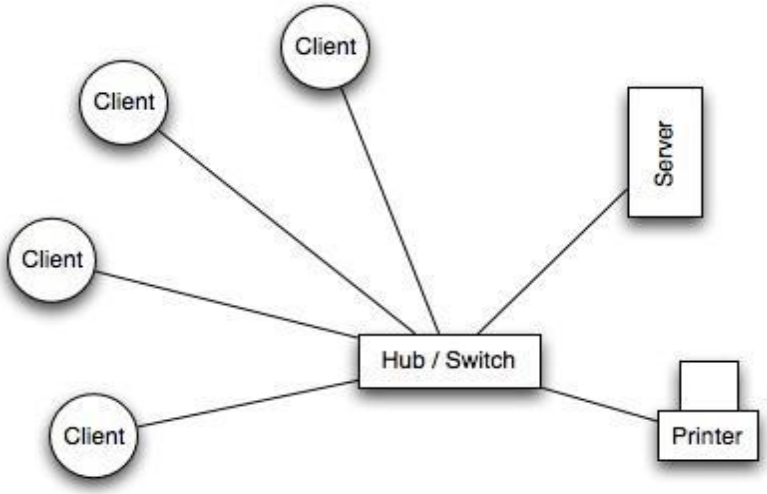
A hybrid topology is always produced when two different basic network topologies are connected.

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

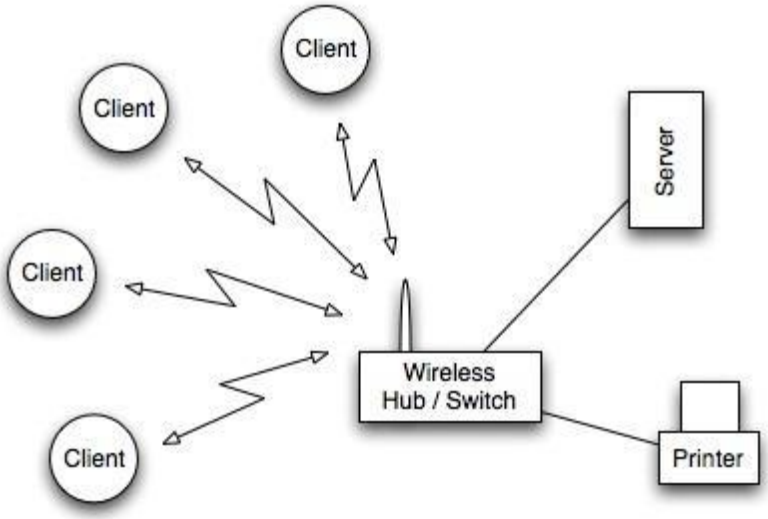
Types of Network

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.



Wireless Local Area Network (WLAN)



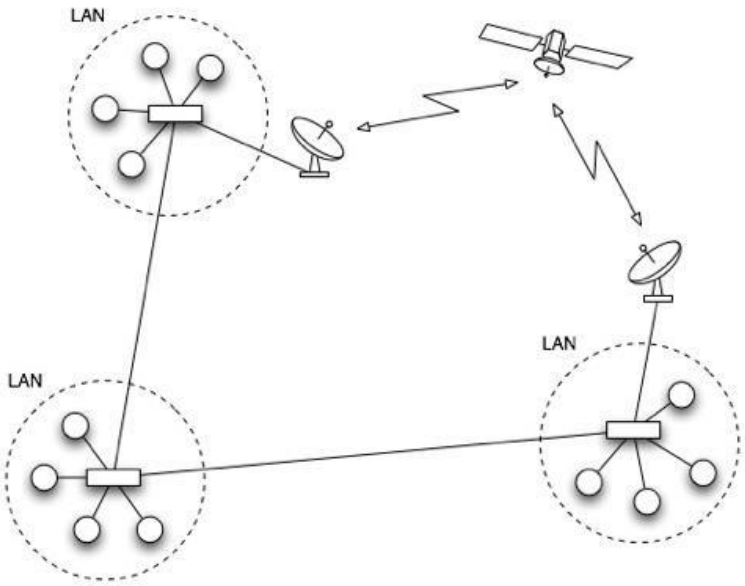
A wireless LAN (WLAN) is a LAN that uses **radio signals** (**WiFi**) to connect computers instead of cables. At the centre of the WLAN is a **wireless switch or router** - a small box with one or two antennas sticking out the back - used for **sending and receiving data** to the computers. (Most laptops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



Internet

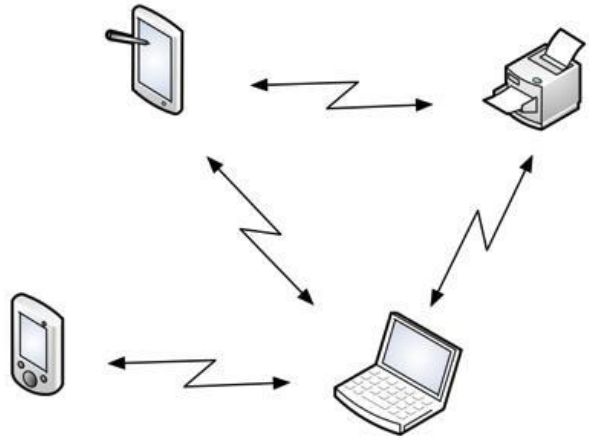
The **Internet** is an example of a **global WAN** .In fact it is the world's largest WAN. Computers on the International Space Station are linked to the Internet, so then you could say that the Internet is now the first off-planet WAN!

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



Common terminologies in network

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.

Network Protocols:

These are basically set of rules which computers make use of when they communicate with each other over a network. A network communication protocol is a standard method for transmitting data from one computer to another across a network.
The internet group of protocols may be represented in a 5 layer model as shown:

LAYER		PROTOCOL	FUNCTION
1)	Physical	Modems	This is the layer at which the basic communication takes place bit by bit from device to device.
2)	Data Link	Ethernet/ WiFi	This layer acts as a correspondent between the network and physical layer. It receives requests of services from the network layer and in turn requests services from the physical layer.
3)	Network/ Internet	Internet Protocol	This layer is responsible for the transmission of data. It makes sure that the data packets reach the destination. It also performs routing i.e. deciding on the path to be taken by the packets to the destination.
4)	Transport	TCP, UDP	This layer divides the data into smaller packets and writes the source and destination addresses on each packet as well as the sequence number of the packet.
5)	Application	FTP, TELNET, HTTP, SSH	This layer consists of protocols which provide services to the network layer via the transport layer.

Ethernet:

Ethernet, pronounced "E-thernet", is the standard way to connect computers on a network over a wired connection.
Ethernet is a name given to basic set of protocols that are used to operate a Local Area Network.

- Ethernet LAN is made up of devices that send or receive data, such as PCs, Printers and various types of servers.
- Network devices that receive and forward data packets such computers, **routers,** and **switches**.
- The medium connecting devices, such as twisted pair cable, fibre optic cables or coaxial cables.
- With a single router and a few Ethernet cables, you can create a **LAN,** which allows all connected devices to communicate with each other.
- A standard Ethernet cable is slightly thicker than a phone cable and has an **RJ45** connector on each end.
- Ethernet **ports** look similar to telephone jacks, but are slightly wider.
- You can plug or unplug devices on an Ethernet network while they are powered on without harming them.

While Ethernet is still the standard for wired networking, it has been replaced in many areas by **wireless** networks. **Wi-Fi** allows you to connect

NOTE: Still, wired connections are less prone to interference and are more secure than wireless ones, which is why many businesses and organizations still use Ethernet.

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**) is a media access control method used most notably in early Ethernet technology for local area networking. It uses a carrier-sensing scheme in which a transmitting station detects collisions by sensing transmissions from other stations while transmitting a frame. When this collision condition is detected, the station stops transmitting that frame, transmits a jam signal, and then waits for a random time interval before trying to resend the frame. CSMA/CD is a modification of pure carrier-sense multiple access (CSMA). CSMA/CD is used to improve CSMA performance by terminating transmission as soon as a collision is detected, thus shortening the time required before a retry can be attempted.

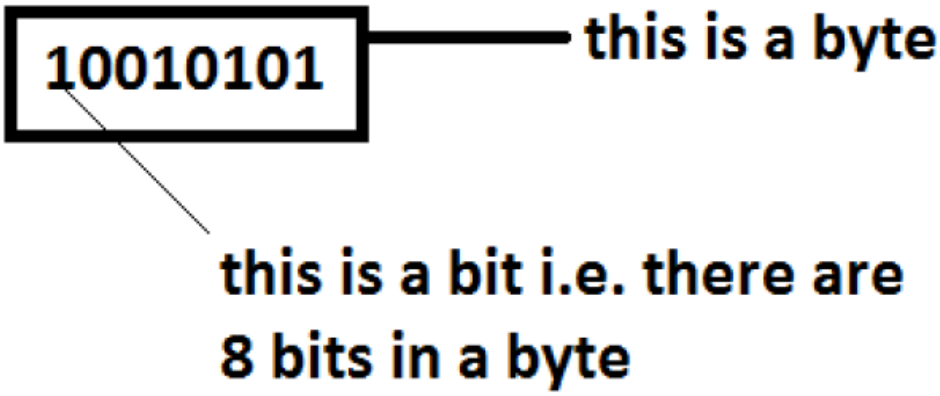
TCP/IP (transmission control protocol/internet protocol)

TCP/IP (also known as the internet protocol suite) is the set of protocols used over the internet. It organises how data packets are communicated and makes sure packets have the following information:

- **source** - which computer the message came from
- **destination** - where the message should go
- **packet sequence** - the order the message data should be re-assembled
- **data** - the data of the message
- **error check** - the check to see that the message has been sent correctly

HANDSHAKING:

- This is the process which takes between two devices after a physical link is established.
- The devices agree on rate of data transfer, the protocol to be used, the process of interruption (i.e. devices send a signal for attention in case of non-arrival of a data packet) as well the alphabetic code to be used.
- Parity Check is a check performed on transmitted data where one of the bits in a byte is checked to ensure that data transmitted is accurate:



- The left most bit in a byte is called the parity bit while the rest of the seven are data bits.
- The parity bit is set as 1 or 0 to keep the number of ones as even.
- Errors in transmission may disturb the bits in the data therefore the parity may be disturbed as well. A disturbed parity would thus indicate an error.
- However, parity check fails to detect an error of transposition i.e. when only position of a bit is changed. Moreover it may fail in case more than one bit is changed.

Internet Protocols

Within TCP/IP there are several key protocols. These include the following.

IP address

Every device on the internet has a **unique IP address**. The IP address is included in a data packet. IP addresses are either 32-bit or 128-bit numbers. The address is broken down into four 8-bit numbers (each is called an octet). Each octet can represent a number between 0 and 255 and is separated by a full stop, eg 192.168.0.12.

To find your IP address you can use the ipconfig command line tool.
Home and small business routers often incorporate a basic dynamic host configuration protocol (DHCP) server which assigns IP addresses to devices on a network.

FTP (File Transfer Protocol)

FTP is used to transfer large files. It is often used for organising files on a web server for a website. You can have private access to an area on an FTP server where you

can upload your files. You can then give another user access to download the documents that you have shared.

- FTP or File Transfer Protocol is an extensively used for downloading. It uses TCP/IP for transmission of data.
- FTP allows the transfer of files over the internet between two computers.
- It follows a client-server relationship i.e. users(client) have to log in using a username and password before being able to download files from or upload files to the server.
- FTP is weak in terms of security and does not have any encryption. Therefore SSH or SSL protocols are used with it to provide additional security.

FTP Server: central computer stores files that are to be downloaded

FTP Command: user can send action/instruction (or by example, e.g. change directory) that are carried out on server

FTP Client: A computer that requests a file from FTP server is called FTP client.

Anonymous: allows user to access files user does not need to identify themselves to server

HTTP (Hyper Text Transfer Protocol)

HTTP transfers web pages from web servers to the client. All web page addresses start with http. An **https** address is a secure web address which has been encrypted. An https address is used for sites holding bank details and secure information.

- HTTP is a protocol used to transfer data across internet. It is a set of rules which must be followed while transferring data such as files, image, sound, videos etc on the World Wide Web.
- It is also based on a client-server relationship i.e. when a user opens the web browser and types in or clicks on a Uniform Resource Locater (URL), the request is sent and URL is converted into an IP address which is used to locate the server.
- The server contains text, images etc in HTML format or PDF or in original formats.
- HTTP daemon is the program which acts upon the requests from clients and sends the requested file to them.
- **HTTPS** is **Hyper Text Transfer Protocol Secure** when data is encrypted and send with security.

SMTP and POP3

Email uses these protocols to communicate with mail servers.
SMTP **Simple Mail Transfer Protocol** is used to send the email;
POP **(Post Office Protocol Version 3)** is used to receive email. Most email clients allow for transfers of up to 10 MB.

VOIP

VOIP is a set of protocols that enables people to have voice conversations over the internet.

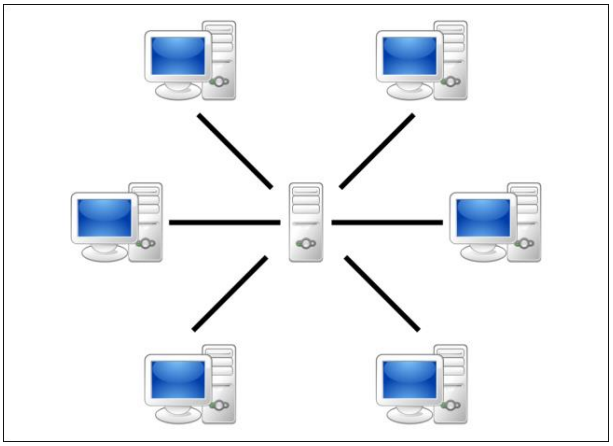
VOIP or **Voice over Internet Protocol** is not a protocol but the use of internet to send voice data in form of digital data packets using internet protocols.

UDP (User Datagram Protocol):

- UDP or User Datagram Protocol, unlike TCP is a connectionless service i.e. it does not require handshaking to take place and does not have a congestion control mechanism. It is a very basic protocol.
- Data packets are sent to the destination with its address attached to the packet. However sequence numbers are not attached to packets.
- It is useful for real time applications such as video on demand systems.

BitTorrent Protocol:

BitTorrent may be popularly known as a method of piracy, but it isn't just for pirates. It's a useful, decentralized peer-to-peer protocol with significant advantages over other protocols in many situations.



How BitTorrent Works

When you download a web page, your computer connects to the web server and downloads the data directly from that server. Each computer that downloads the data

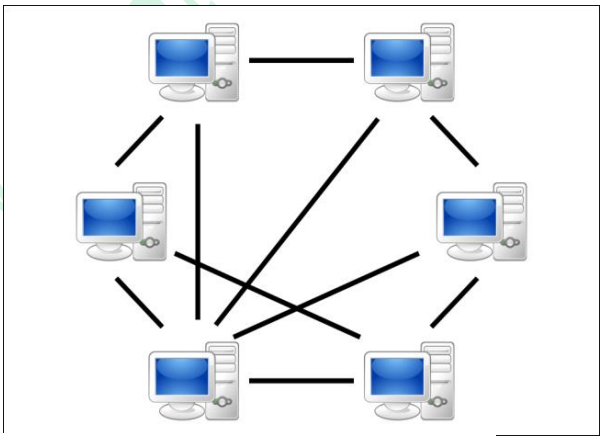
downloads it from the web page's central server. This is how much of the traffic on the web works.

BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent **swarm:** (a group of computers downloading and uploading the same torrent) transfer data between each other without the need for a central server.

Traditionally, a computer joins a BitTorrent swarm by loading a .torrent file into a BitTorrent client. The BitTorrent client contacts a "tracker" specified in the .torrent file.

Tracker: The tracker is a special server that keeps track of the connected computers. The tracker shares their IP addresses with other BitTorrent clients in the swarm, allowing them to connect to each other.

Once connected, a BitTorrent client downloads bits of the files in the torrent in small pieces, downloading all the data it can get. Once the BitTorrent client has some data, it can then begin to upload that data to other BitTorrent clients in the swarm. In this way, everyone downloading a torrent is also uploading the same torrent. This speeds up everyone's download speed. If 10,000 people are downloading the same file, it doesn't put a lot of stress on a central server. Instead, each downloader contributes upload bandwidth to other downloaders, ensuring the torrent stays fast.



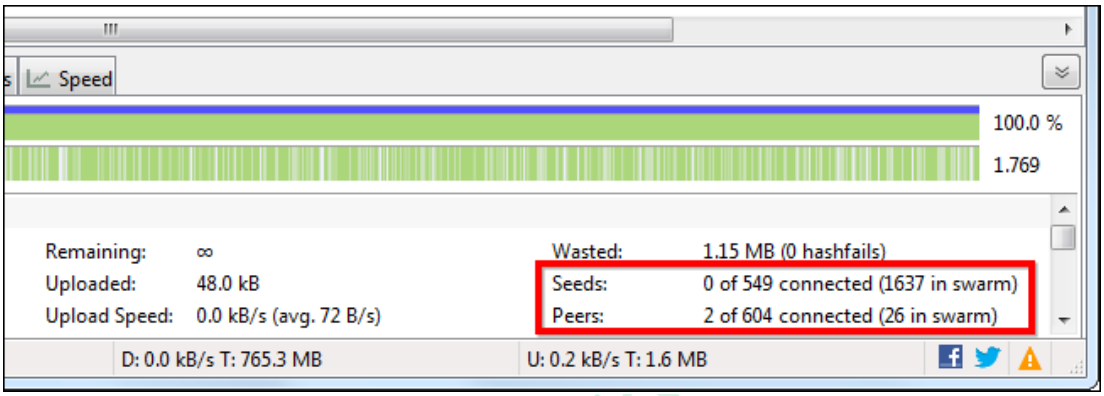
Importantly, BitTorrent clients never actually download files from the tracker itself. The tracker participates in the torrent only by keeping track of the BitTorrent clients connected to the swarm, not actually by downloading or uploading data.

Leechers and Seeders

Users downloading from a BitTorrent swarm are commonly referred to as "**leechers**" or **"peers"**. Users that remain connected to a BitTorrent swarm even after they've downloaded the complete file, contributing more of their upload bandwidth so other people can continue to download the file, are referred to as "seeders". For a torrent to be downloadable, one seeder – who has a complete copy of all the files in the torrent – must initially join the swarm so other users can download the data. If a torrent has no seeders, it won't be possible to download – no connected user has the complete file.

BitTorrent clients reward other clients who upload, preferring to send data to clients who contribute more upload bandwidth rather than sending data to clients who upload at a very slow speed. This speeds up download times for the swarm as a whole and rewards users who contribute more upload bandwidth.

Each "**seeder**" is a user (or "**peer**" whose computer holds the complete file to share. A **seed** is then broken into pieces and the pieces are sent to other peers who want to download them.



TELNET:

- TELNET or Telecommunication Protocol is a network emulator i.e. it enables a computer to gain access to another computer and run software and execute commands on that computer.
- The user's computer has TELNET CLIENT SOFTWARE whereas the remote computer has TELNET SERVER SOFTWARE to make the connection possible.
- A disadvantage of TELNET is that all the data is transferred as plain text and not in encrypted form.
- However, it is considered helpful in detecting problems in a network. Network administrators use it to make changes to network settings and carry out diagnostic tests.

SSH:

- SSH or Secure Shell Protocol has the same function as the TELNET.
- However it offers higher levels of security during the transmission of data in the sense that the data is encrypted.
- It also uses Public Key Authentication which is a feature of encryption that allows one computer to ensure that a genuine computer is trying to communicate with it.

- Public key is a key given by a computer to other computers to encrypt and send data to it.

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!

Network Cables

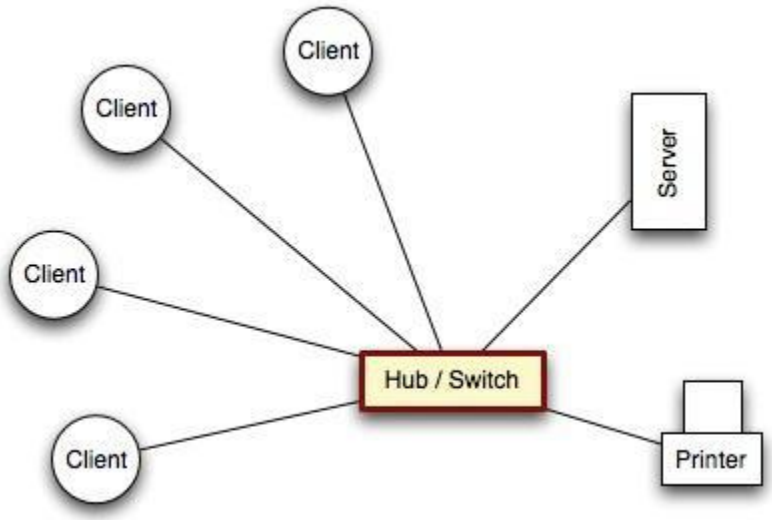
To connect together different devices to make up a network, you need cables. **Cables** are still used in most networks, rather than using only wireless, because they can carry much

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).

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.

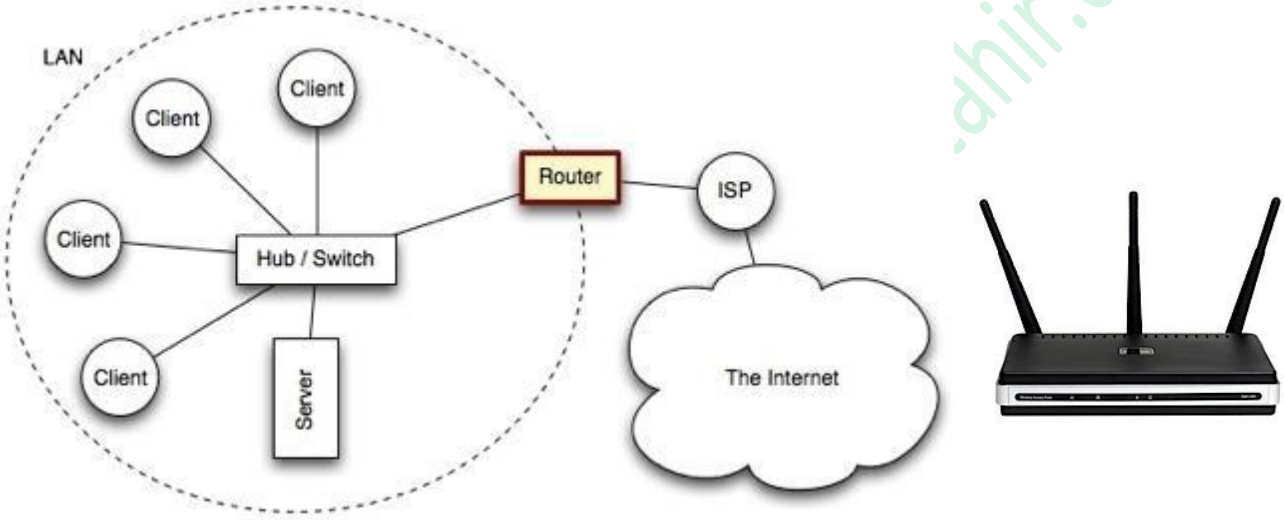
Hubs are pretty much obsolete now (you can't buy them any more), having been superseded by cheap switches.

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**

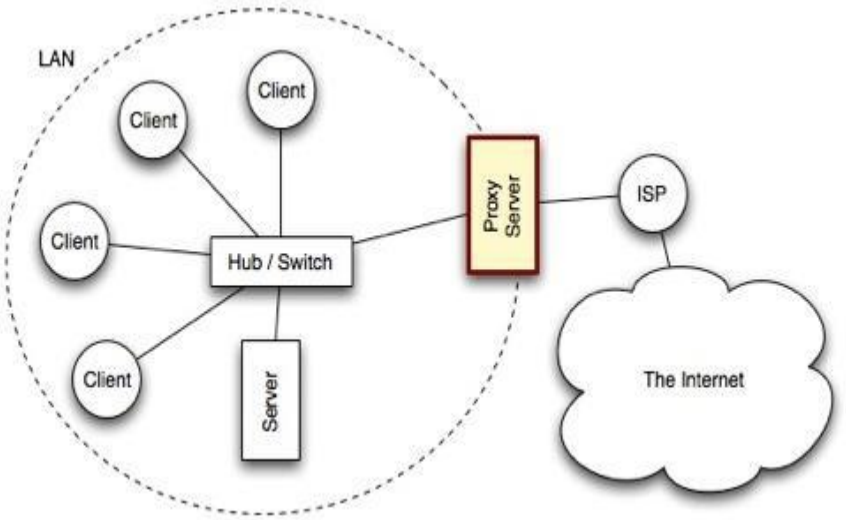
Router



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.
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)
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

Proxy Server

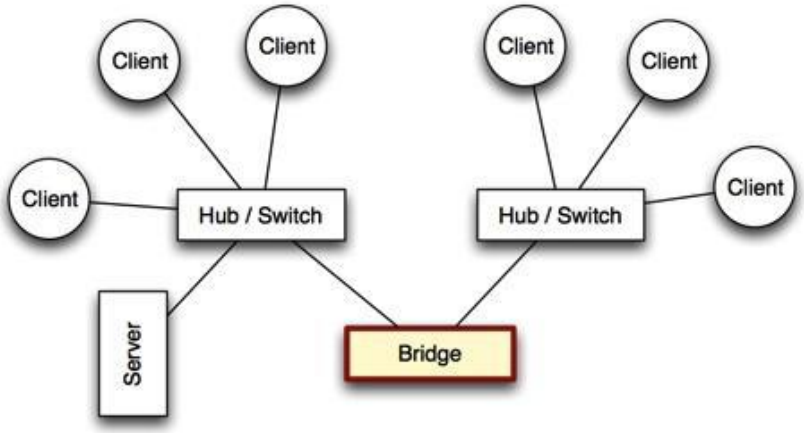
A proxy server is a computer setup to **share a resource**, usually an **Internet connection**. Other computers can request a web page via the proxy server. The proxy server



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

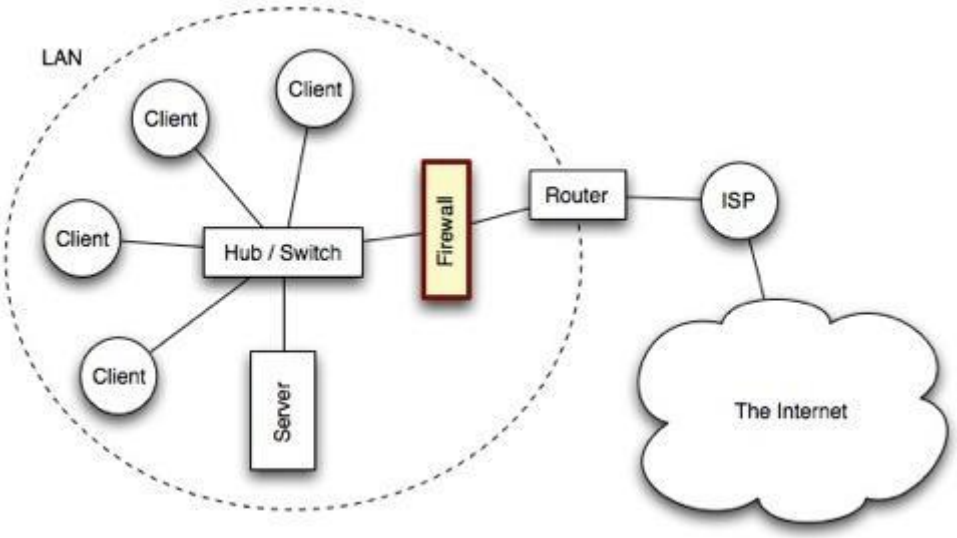
A bridge is a network device that typically **links** together **two different parts of a LAN**. A router is usually used to link a LAN to a WAN (such as the Internet), whereas a bridge links independent parts of a LAN so that they act as a single LAN.



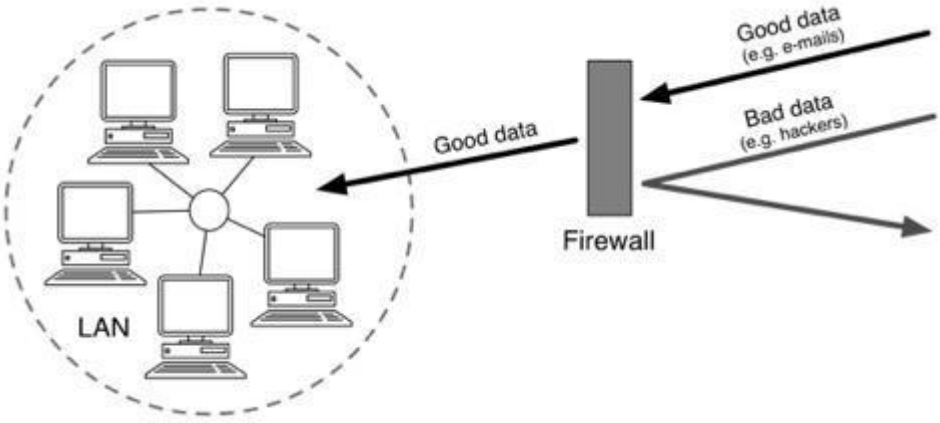
Firewall

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)

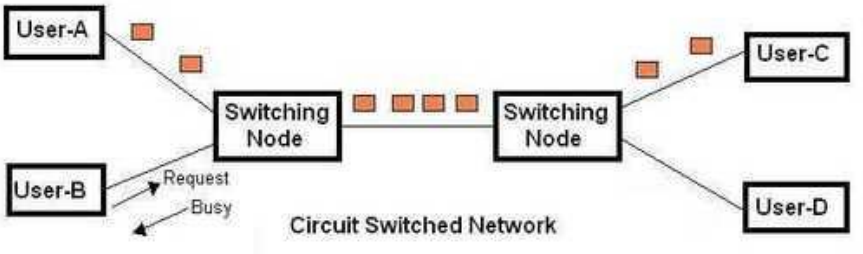


Packet switching and circuit switching:

Packet switching and circuit switching are two networking methods for transferring data between two nodes or hosts.

Circuit Switching

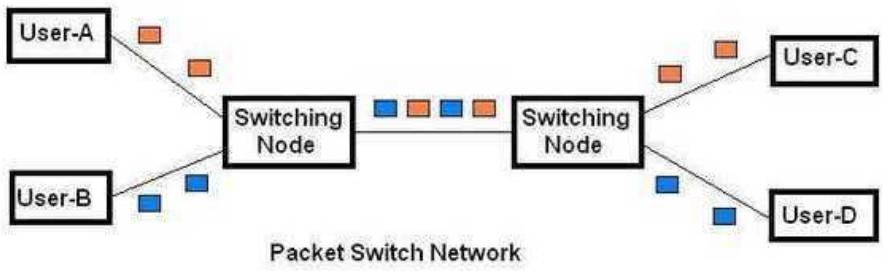
In circuit switching network dedicated channel has to be established before the call is made between users. The channel is reserved between the users till the connection is active. For half duplex communication, one channel is allocated and for full duplex communication, two channels are allocated. It is mainly used for voice communication requiring real time services without any much delay.



As shown in the figure 1, if user-A wants to use the network; it need to first ask for the request to obtain the one and then user-A can communicate with user-C. During the connection phase if user-B tries to call/communicate with user-D or any other user it will get busy signal from the network.

Packet Switching

In packet switching network unlike CS network, it is not required to establish the connection initially. The connection/channel is available to use by many users. But when capacity or number of users increases then it will lead to congestion in the network. Packet switched networks are mainly used for data and voice applications requiring non-real time scenarios.



Packet Switch Network

As shown in the figure 2, if user-A wants to send data/information to user-C and if user-B wants to send data to user-D, it is simultaneously possible. Here information is padded with header which contains addresses of source and destination. This header is sniffed by intermediate switching nodes to determine their route and destination.
In packet switching, station breaks long message into packets. Packets are sent one at a time to the network. Packets are handled in two ways, viz. datagram and virtual circuit.

In datagram, each packet is treated independently. Packets can take up any practical route. Packets may arrive out of order and may go missing.

In virtual circuit, preplanned route is established before any packets are transmitted. The handshake is established using call request and call accept messages. Here each packet contains virtual circuit identifier(VCI) instead of the destination address. In this type, routing decisions for each packet are not needed.

For a packet-switched network, data is transferred by dividing the data into individual packets and passing it through the circuits to the other host. In packet-switched networks, the route is not exclusively determined when the packets hit the wire. Using routing algorithms, each packet may actually take a different route through the network to arrive at the destination host.

Unlike a circuit-switched network where a static route is setup and pre-established prior to initializing connections to the host.

Comparison between CS vs. PS networks

As shown above in Packet switched (PS) networks quality of service (QoS) is not guaranteed while in circuit switched (CS) networks quality is guaranteed.
PS is used for time insensitive applications such as internet/email/SMS/MMS/VOIP etc.
In CS even if user is not talking the channel cannot be used by any other users, this will waste the resource capacity at those intervals.
The example of circuit switched network is PSTN and example of packet switched network is GPRS/EDGE.
Following table summarizes difference between circuit switching and packet switching of type datagram and virtual circuit.

Circuit Switching	Packet Switching(Datagram type)	Packet Switching(Virtual Circuit type)
Dedicated path	No Dedicated path	No Dedicated path
Path is established for entire conversation	Route is established for each packet	Route is established for entire conversation
Call setup delay	packet transmission delay	call setup delay as well as packet transmission delay
Overload may block call setup	Overload increases packet delay	Overload may block call setup and increases packet delay
Fixed bandwidth	Dynamic bandwidth	Dynamic bandwidth
No overhead bits after call setup	overhead bits in each packet	overhead bits in each packet

References:

www.vuze.com/about-bittorrent/what-is-bittorrent
https://www.howtogeek.com/141257/htg-explains-how-does-bittorrent-work/
http://www.bbc.co.uk/schools/gcsebitesize/ict/datacomm/networktopsrev1.shtml
http://www.rfwireless-world.com/Terminology/circuit-switching-vs-packet-switching.html