

Syllabus Content

14. Communication and Internet technologies

14.1 Protocols

- protocol is essential for communication between computers
- protocol implementation can be viewed as a stack, where each layer has its own functionality
- Show understanding of the TCP / IP protocol suite
- Show understanding of protocols (HTTP, FTP, POP3, IMAP, SMTP, BitTorrent) and their purposes

Notes and guidance

- Four Layers (Application, Transport, Internet, Link)
- Purpose and function of each layer application when a message is sent from one host to another on the internet

14.2 Circuit switching, packet switching and routers

- Show understanding of circuit switching
- Show understanding of packet switching

Notes and guidance

- Benefits, drawbacks and where it is applicable
- Show understanding of the function of a router in packet switching. Explain how packet switching is used to pass messages across a network, including the internet

Protocols:








Protocols are set of rules for data transmission which are agreed by sender and receiver

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.

A protocol stack


For a protocol suite the protocols can be viewed as layers within a protocol stack. There are a number of aspects relating to this concept.

-  Each layer can only accept input from the next higher layer or the next lower layer.
-  There is a defined interface between adjacent layers which constitutes the only interaction allowed between layers.
-  A layer is serviced by the actions of lower layers.
-  With the possible exception of the lowest layer the functioning of a layer is created by installed soft ware.
-  A layer may comprise sub-layers.
-  Any user interaction will take place using protocols associated with the highest level layer in the stack.
-  Any direct access to hardware is confined to the lowest layer in the stack.

There are seven layers in Network Layer OSI model (Open System interconnection)

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network.

It was the first standard model for network communications, adopted by all major computer and telecommunication companies



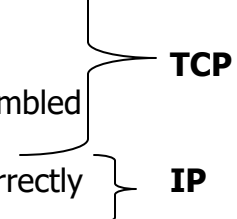
7	Application Layer	Human-computer interaction layer, where applications can access the network services
6	Presentation Layer	Ensures that data is in a usable format and is where data encryption occurs
5	Session Layer	Maintains connections and is responsible for controlling ports and sessions
4	Transport Layer	Transmits data using transmission protocols including TCP and UDP
3	Network Layer	Decides which physical path the data will take
2	Data Link Layer	Defines the format of data on the network
1	Physical Layer	Transmits raw bit stream over the physical medium

Our syllabus requires us to only focus on **four layers** so we will only discuss the following layers. 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.

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:

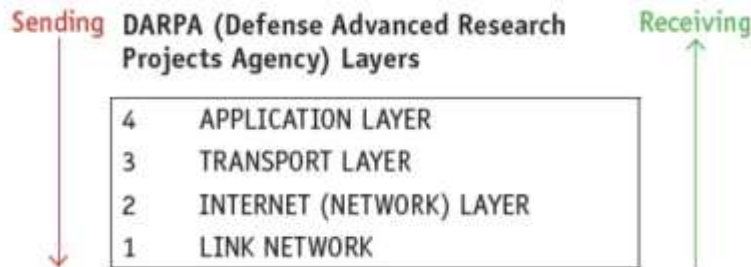
- **source** - which computer the message came from
 - **destination** - where the message should go
 - **packet sequence** - the order the message data should be re-assembled
 - **data (pay load)** - the data of the message
 - **error check** - the check to see that the message has been sent correctly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

TCP

IP

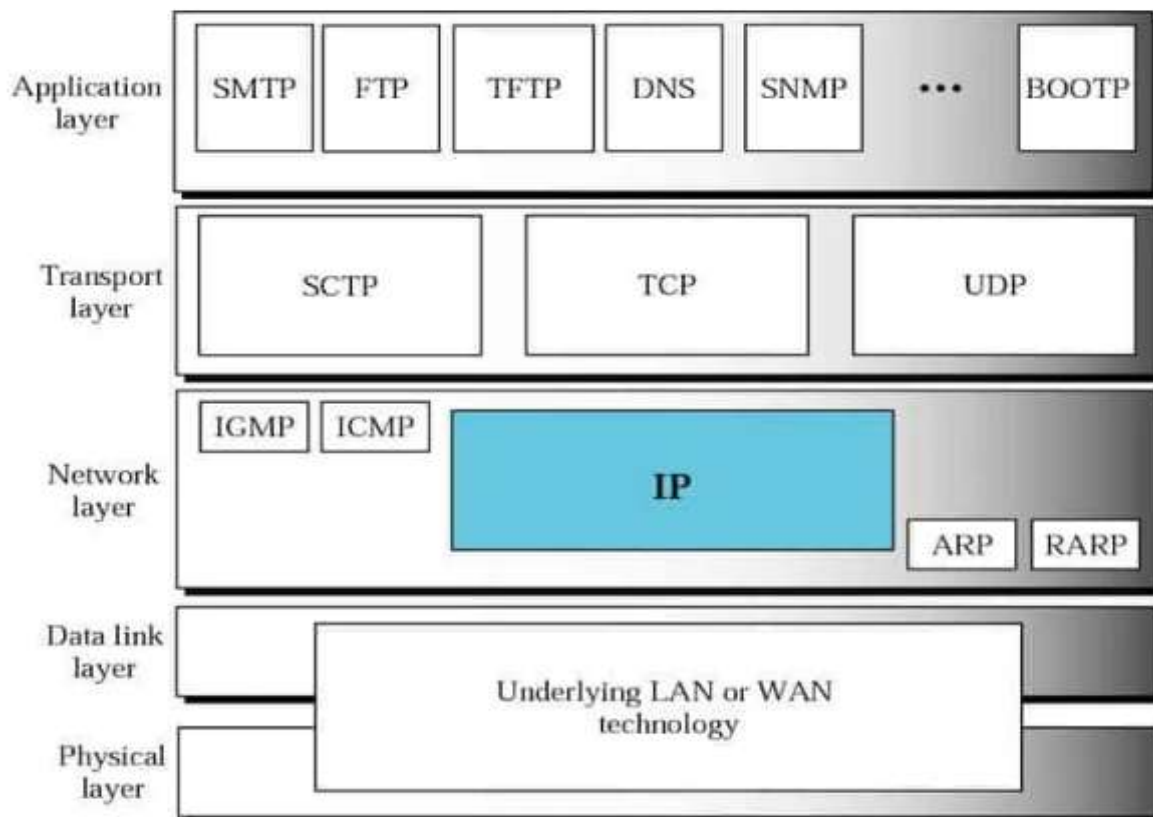
TCP/IP protocols

This is the four-layer structure for TCP/IP protocols:



Using layers breaks the process down into manageable self-contained modules (this process is known as **decomposition**), making it easier to develop and easier to make software and hardware compatible.

When sending data across the internet (network), the layers are used in the order layer 4 to layer 1; when receiving data across the internet (network), the layers are used in the order layer 1 to layer 4. Each of the layers is implemented using software.







Internet Protocols






Within [TCP/IP](#) there are several key [protocols](#). These include the following.

TCP (Transmission Control Protocol)

If an application is running on an end-system where a 'message' is to be sent to a different end-system the application will be controlled by an application layer protocol as described above.

-  The protocol will transmit the user data to the transport layer.
-  The TCP protocol operating in the transport layer now has to take responsibility for ensuring the safe delivery of the 'message' to the receiver.
-  The TCP protocol creates sufficient packets to hold all of the data.
-  Each packet consists of a header plus the user data.

IP (Internet Protocol)

-  The function of the network layer, and in particular of the IP, is to ensure correct routing over the Internet.
-  IP protocol takes the packet received from the transport layer and adds a further header. The header contains the IP addresses of both the sender and the receiver.
-  The IP packet, which is usually called a 'datagram', is sent to the data-link layer and therefore to a different protocol suite.
-  The data-link layer assembles datagrams into 'frames'. Once the IP packet has been sent to the datalink layer, IP has no further duty.
-  IP will have no knowledge of whether or not it reached its destination. If IP receives a packet which contains an acknowledgement of a previously sent packet, it will simply pass the packet on to TCP with no awareness of the content.

IP address

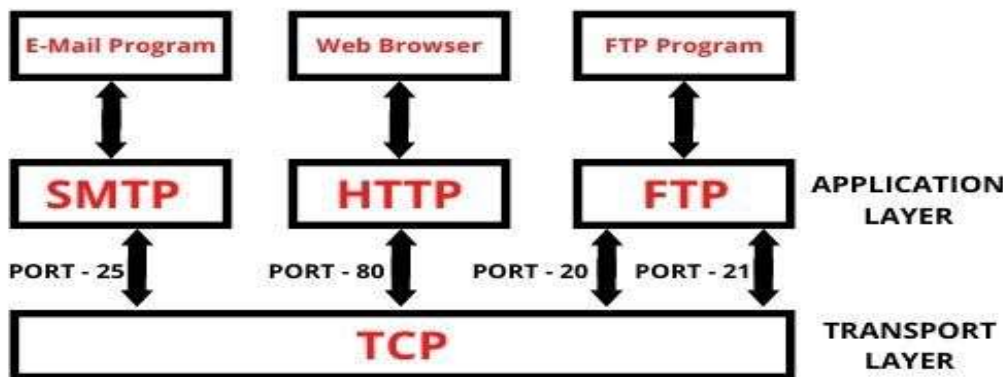
Every device on the internet has a **unique IP address**. The [IP address](#) is included in a data packet. IP addresses are either 32-[bit](#) or 128-bit numbers. The address is broken down into four 8-bit numbers (each is called an [octet](#)). Each octet can represent a number between 0 and 255 and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



Application-layer protocols associated with TCP/IP

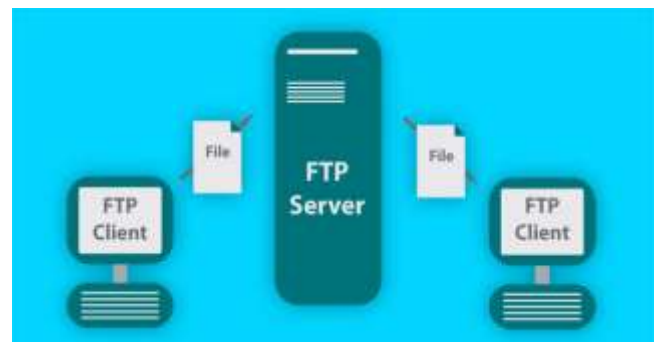
The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the [Hypertext Transfer Protocol](#) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

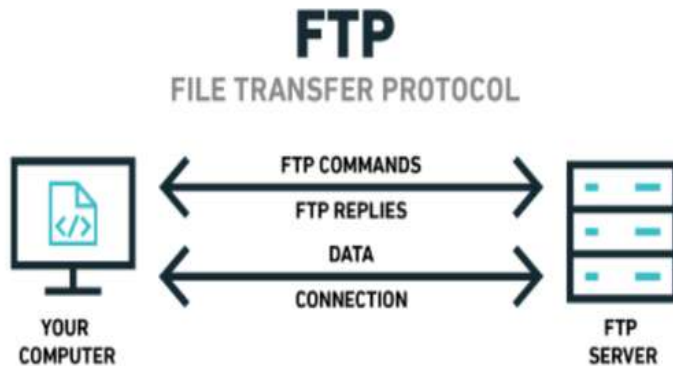


FTP (File Transfer Protocol)

[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

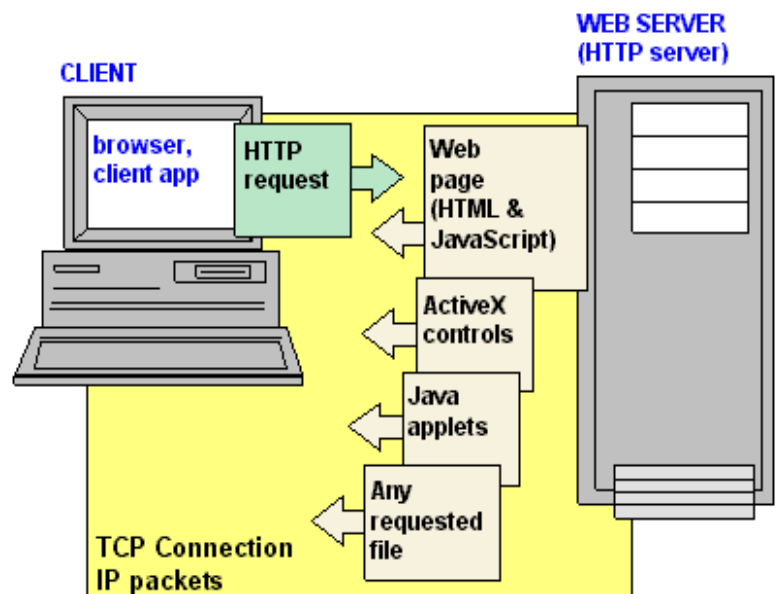
FTP Client: A computer that requests a file from FTP server is called FTP client.

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 Locator (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.

The following summarizes what happens when a user requests a web page from a website.

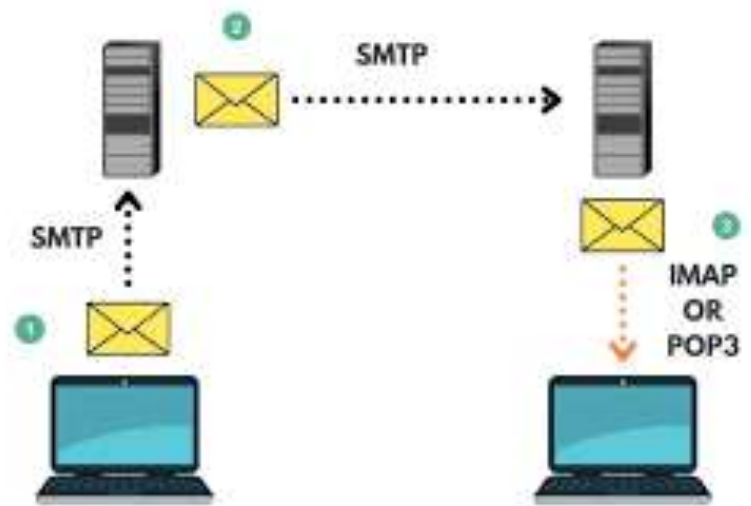
1. The user types URL into their browser. HTTP(s) transmits the request from the application layer to the transport layer (TCP).
2. The TCP creates data packets and sends them to the destination port(s).
3. The DNS server stores a database of URLs and matching IP addresses.
4. The DNS server uses the domain name typed into the browser to look up the IP address of the appropriate website.
5. The server TCP sends back an acknowledgement.
6. Once communication has been established, the web server sends the web page back in HTML format to the browser. The browser interprets the page and displays it or sends the data in the correct format to the media player.

SMTP and POP3




Email uses these protocols to communicate with mail [servers](#). **SMTP Simple Mail Transfer Protocol** is used to send the email; It is sometimes referred to as a **push protocol** (in other words, a client opens a connection to a server and keeps the connection active all the time; the client then uploads a new email to the server).

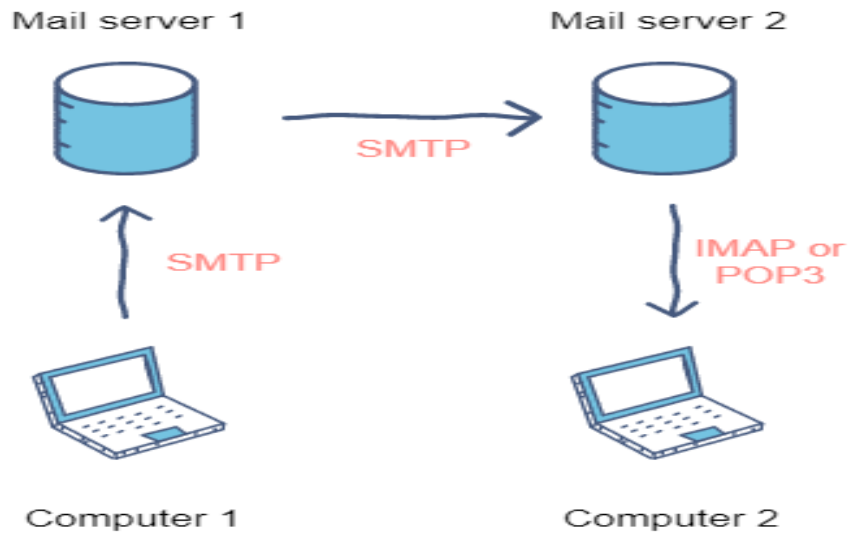
1. Since SMTP is text-based only, it doesn't handle **binary files** (a binary file is a file containing media/images as well as text and is regarded as being computer-readable only). If an email contains attachments made up of, for example, images, video, music then it is necessary to use the **multi-purpose internet mail extension (MIME)** protocol instead.

2. A **MIME header** is used at the beginning of the transmission; clients use this header to select which media player is needed when the attachment is opened.



POP (Post Office Protocol Version 3) & IMAP (Internet message access protocol)

-  These protocols are used to receive email.
-  These are known as **pull protocols** (the client periodically connects to a server; checks for and downloads new emails from the server – the connection is then closed; this process is repeated to ensure the client is updated).
-  IMAP is a more recent protocol than POP3/4, but both have really been superseded by the increasing use of HTTP protocols. However, SMTP is still used when transferring emails between email servers.



VOIP

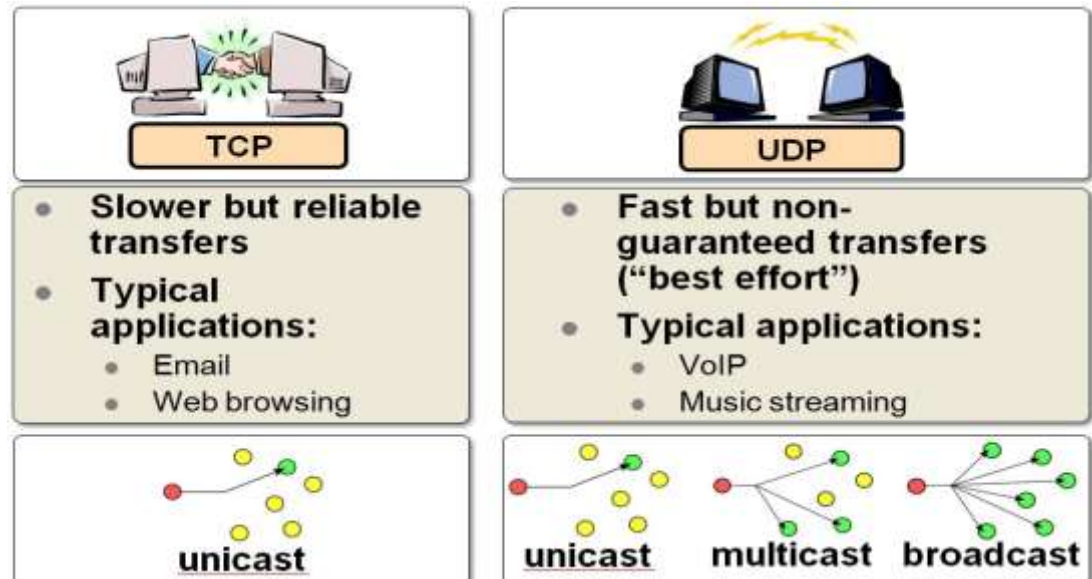
VOIP is a set of protocols that enables people to have voice conversations over the internet.

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 **Live streaming**.

Peer-to-peer (P2P) file-sharing:

The network traffic generated by peer-to-peer (P2P) file sharing is one of the main features of Internet use. P2P is an architecture that has no structure and no controlling mechanism. Peers act as both clients and servers and each peer is just one end-system. When a peer acts as a server it is called a 'seed'.

The BitTorrent protocol is the most used protocol because it allows fast sharing of files. There are three basic problems to solve if end-systems are using BitTorrent.

1. How does a peer find others that have the wanted content? Every content provider should provide a content description, called a torrent, which is a file that contains the name of the tracker (a server that leads peers to the content)
2. How do peers replicate content to provide high-speed downloads for everyone? Peers download and upload chunks at the same time, but peers have to exchange lists of chunks and aim to download rare chunks for preference. Each time a rare chunk is downloaded it automatically becomes less rare!
3. How do peers encourage other peers to provide content rather just using the protocol to download for themselves? This requires dealing with the free-riders or 'leechers' who only download.

11

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.

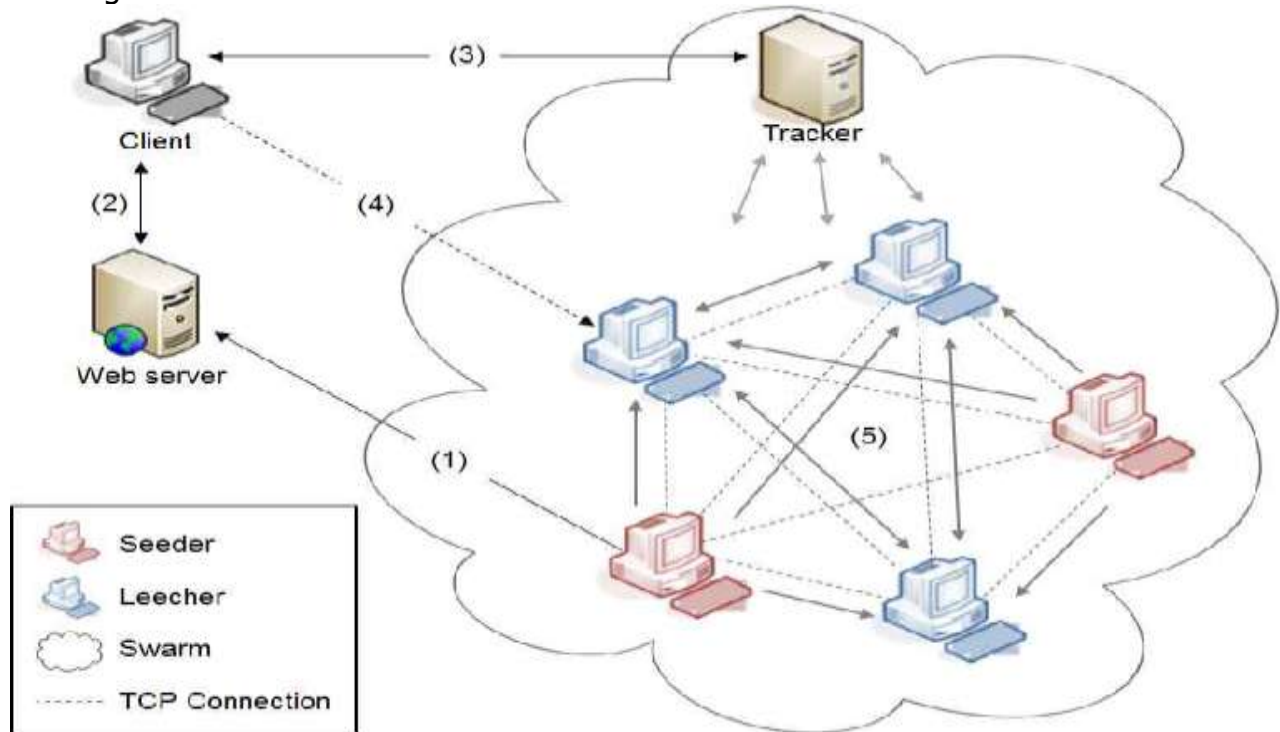
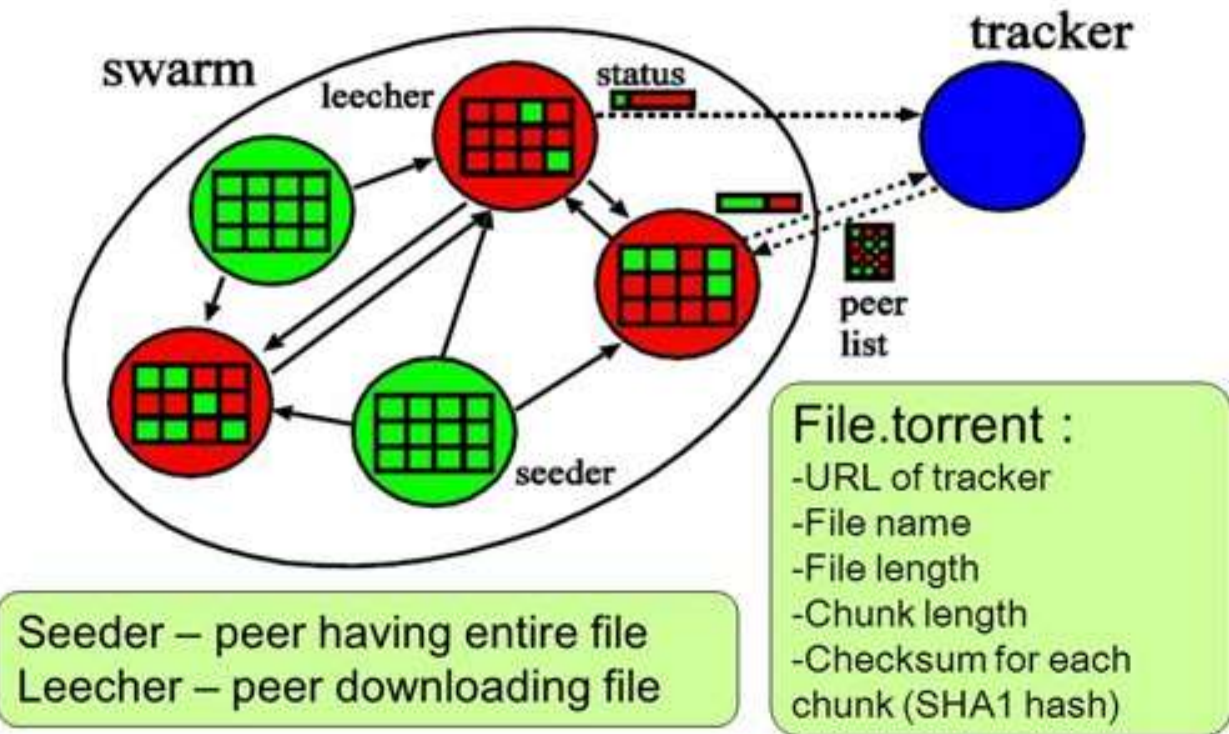


Figure 1. BitTorrent architecture

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 (complete file)**, 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

Users downloading from a BitTorrent swarm are commonly referred to as “**leechers**” or “**peers**”.

Seeders:

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**”.

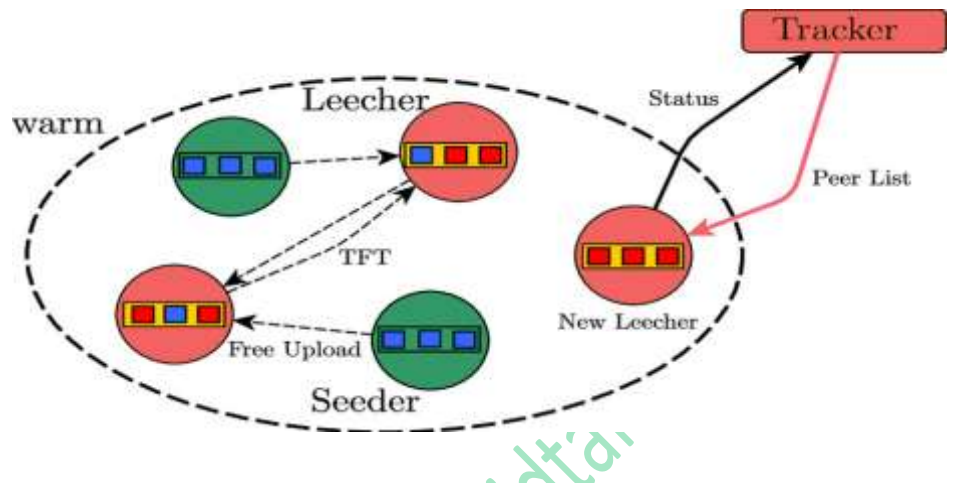
For a torrent to be downloadable, one seeder – who has a complete copy of all the files in the torrent – must initially join the swarm so other users can download the data. If a torrent has no seeders, it won’t be possible to download – no connected user has the complete file.

Reward for Seeders:

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).

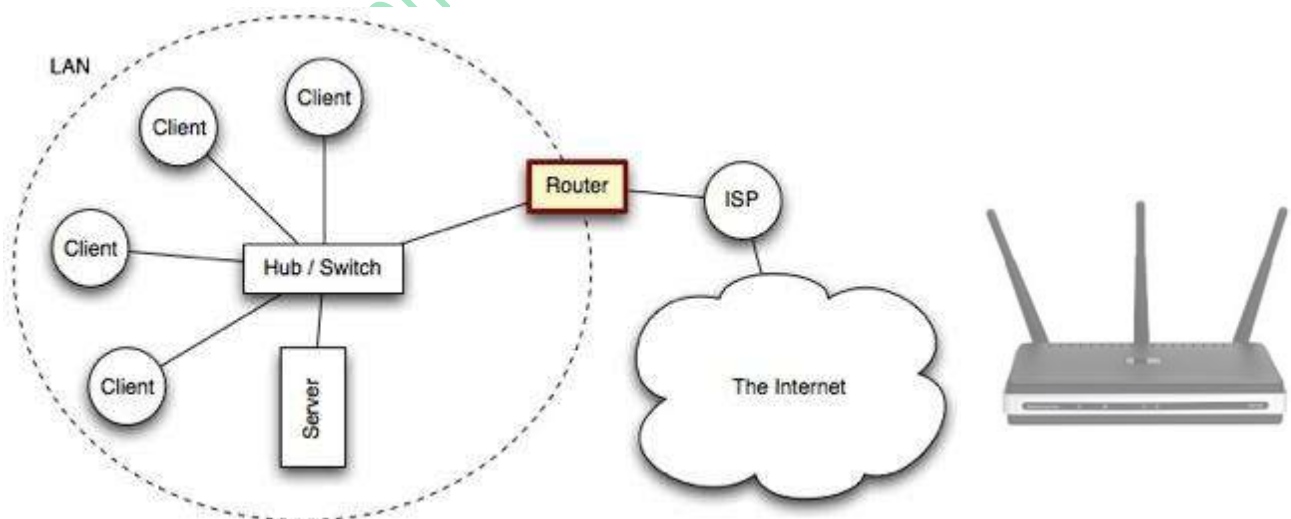
A **seed** is then broken into pieces and the pieces are sent to other peers who want to download them.



Lurker – a peer that **downloads many files** but **does not make available** any **new content** for the community as a whole.








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).




Routers that join together the various different networks that together make up the **Internet** are much more **complex** than the one you might have in your home. Following steps explain how **routers** work on internet

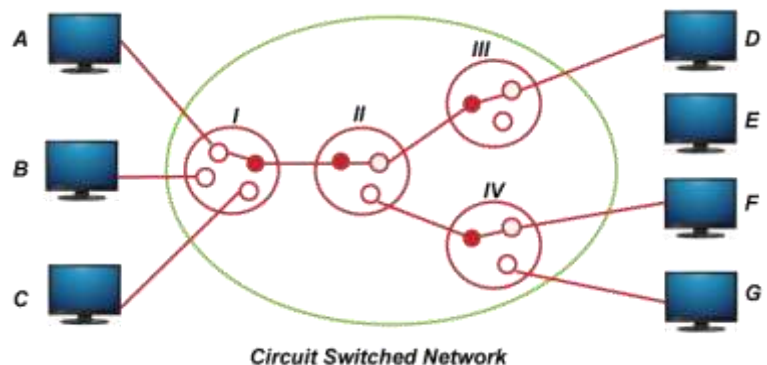
-  The frame sent by the data-link layer will arrive at a router during transmission (more likely at several routers). At this stage, the datagram content of the frame is given back to IP.
-  It is now the function of the router software to choose the next target host in the transmission.
-  The software has access to a routing table appropriate to that router. The size and complexity of the Internet prohibits a router from having a global routing table. Once the appropriate address has been inserted into the datagram, IP passes it back to the datalink layer of the router.
-  The routing table for every router has details of any current problems with any of the options for the next transmission step. This ensures that packets are delivered to their destination in the shortest possible time available.
-  The major distinction between a switch and a router as a node in a network is that when a frame arrives at a switch, it is transmitted on without any routing decision. A switch operates in the data-link layer but has no access to the network layer.

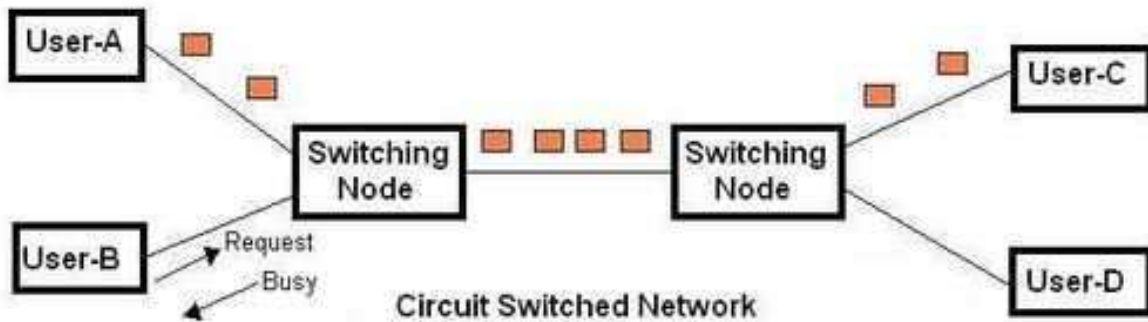
Packet switching and circuit switching:

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.





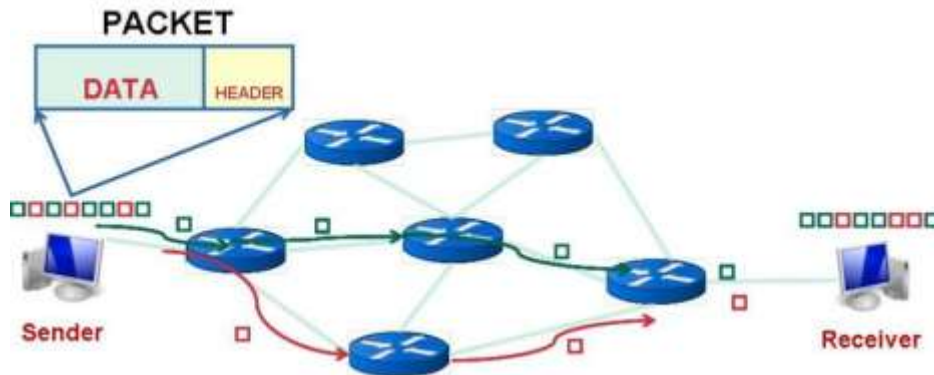
As shown in the **figure**, if **user-A wants** to use the network; it need to first ask for the request to obtain the one and then **user-A** can communicate with **user-C**.

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.

Pros	Cons
the circuit used is dedicated to the single transmission only	it is not very flexible (for example, it will send empty frames and it has to use a single, dedicated line)
the whole of the bandwidth is available	nobody else can use the circuit/channel even when it is idle
the data transfer rate is faster than with packet switching	the circuit is always there whether or not it is used
the packets of data (frames) arrive at the destination in the same order as they were sent	if there is a failure/fault on the dedicated line, there is no alternative routing available
a packet of data cannot get lost since all packets follow on in sequence along the same single route	dedicated channels require a greater bandwidth
it works better than packet switching in real-time applications	prior to actual transmission, the time required to establish a link can be long

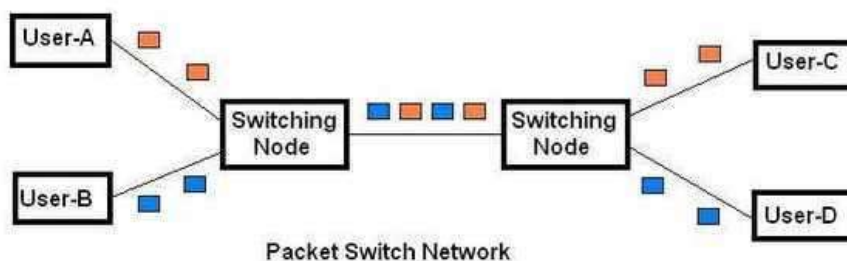
Packet Switching

- 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.



As shown in the **figure**, 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.

Pros	Cons
no need to tie up a communication line	the protocols for packet switching can be more complex than those for circuit switching
it is possible to overcome failed or faulty lines by simply re-routing packages	if a packet is lost, the sender must re-send the packet (which wastes time)
it is easy to expand the traffic usage	does not work well with real-time data streams
circuit switching charges the user on the distance and duration of a connection, but packet switching charges users only for the duration of the connectivity	the circuit/channel has to share its bandwidth with other packets
high data transmission is possible with packet switching	there is a delay at the destination while packets are reassembled
packet switching always uses digital networks which means digital data is transmitted directly to the destination	needs large amounts of RAM to handle the large amounts of data

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.



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

References:

Computer Science course book by Sylvia Langfield and Dave Duddell (Cambridge University Press)



Computer Science course book by David Watson and Hellen Williams (Hodder Education)

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>