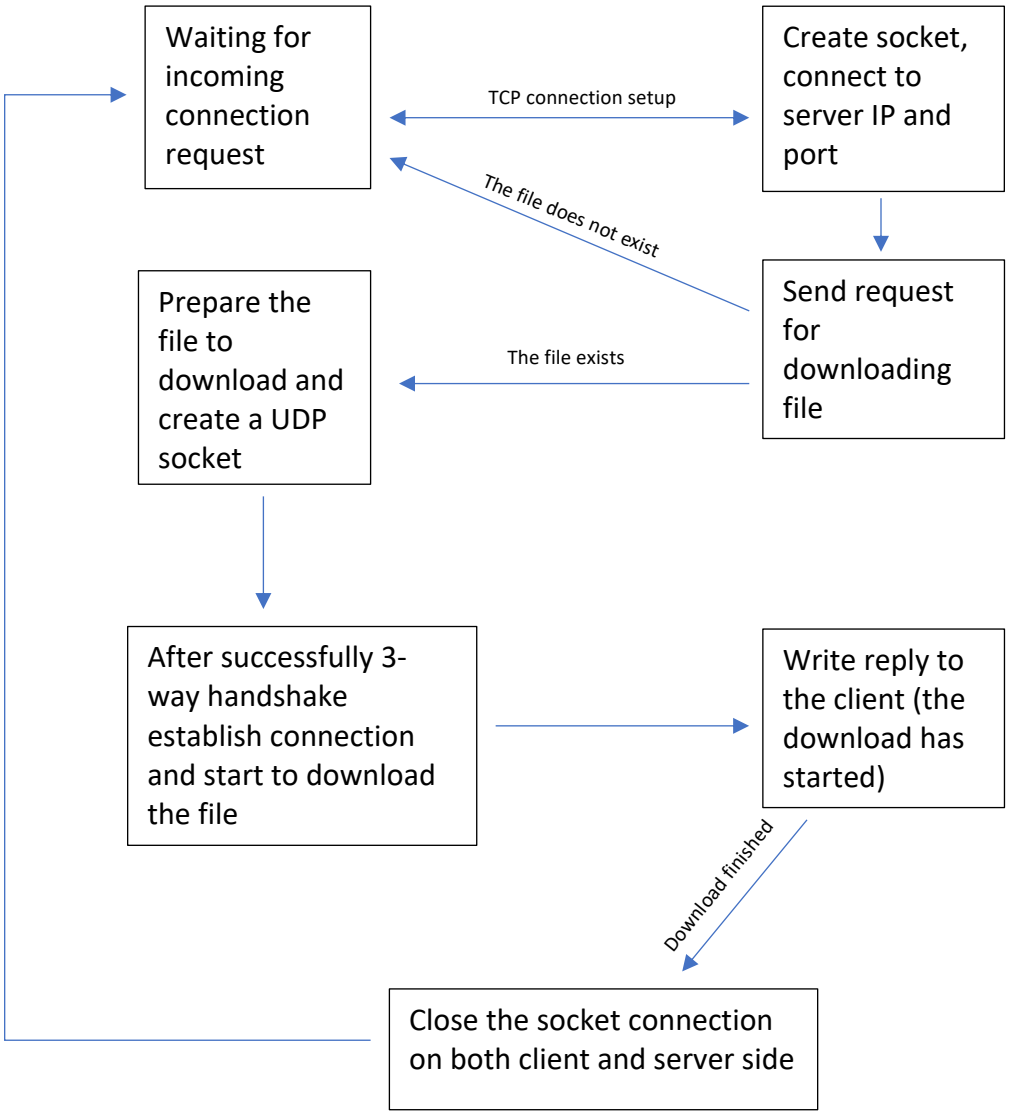
Part 2:
Situation Diagram



How the system overcomes packet loss

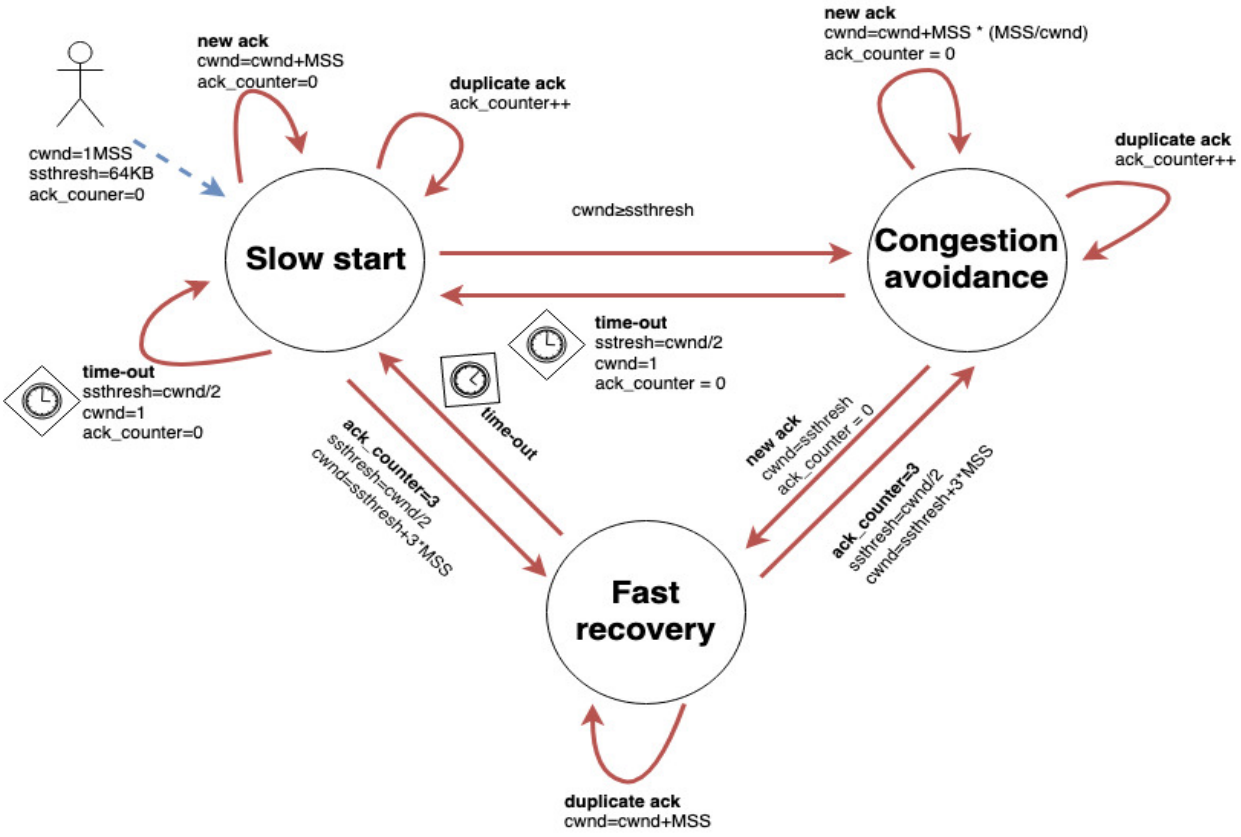
The system overcome packet loss by the 3-way handshake method. Which means, when we are trying to download a file, the system would first receive first handshake and send the second one to the client address. Then assign the second handshake back to the server and will wait for the third handshake to arrive. By that, we will loop until all steps are completed properly and then will show a "File sent successfully" message.
After each step, if some is failed error message would appear on the screen: "Error establish request".
So, the 3 way handshake is giving us the proper dealing with packet loss.

How the system overcomes latency problem's

Our system overcomes latency by congestion control.
Slow start: It's starts from 'slow start' and sending an ack. If we getting the same ack, it means that the status is 'duplicate ack', so we increase the ack-counter and sending again an ack with the same 'cwnd' and 'sstresh'.
If we receive new ack number, it means that the packet received and we increase the 'cwnd' by the MSS (maximum segment size the sender will accept) and assign ack-counter to 0.
If after some try's we got a time out (which means too many packet did not got received) we divide cwnd by 2 and assign this to the sstresh.
If after some packet send's, and it's not got received after 3 losses, from slow start we go to the 'Fast recovery'.
If we come across situation in which the 'cwnd' ≥ 'sstresh' then we are going to 'Congestion avoidance'.
Fast recovery: If we got an duplicate ack (which means the packet did not received again) we increase the 'cwnd' by MSS unit and start again the 'Fast recovery'.
If we got a time out we divide cwnd by 2 and assigns it to sstresh, assign cwnd to 1 and go back to 'Slow start'.
If we received new ack we going to the 'Congestion avoidance'.
Congestion avoidance: In case of duplicate ack, we increase the ack-counter and start again the 'Congestion avoidance'.
If we are received new ack, we using this formula: $cwnd = cwnd + MSS \cdot (MSS \div cwnd)$
,assign the ack-counter to 0 and start 'Congestion avoidance' again with the new parameters which was assign.
If we got a time out, we divide cwnd by 2, assign it to ssthresh, assign cwnd to 1, assign 0 to ack-counter and go back to 'Slow start'.
If after some try's of sending the packet we did not received it for 3 times ($ack_{counter} = 3$)
We are doing the follow: $ssthresh = \frac{cwnd}{2}, cwnd = ssthresh + 3 \cdot MSS$
And go to the 'Fast recovery'.
By this methods as described below, we trying to overcome latency problems.

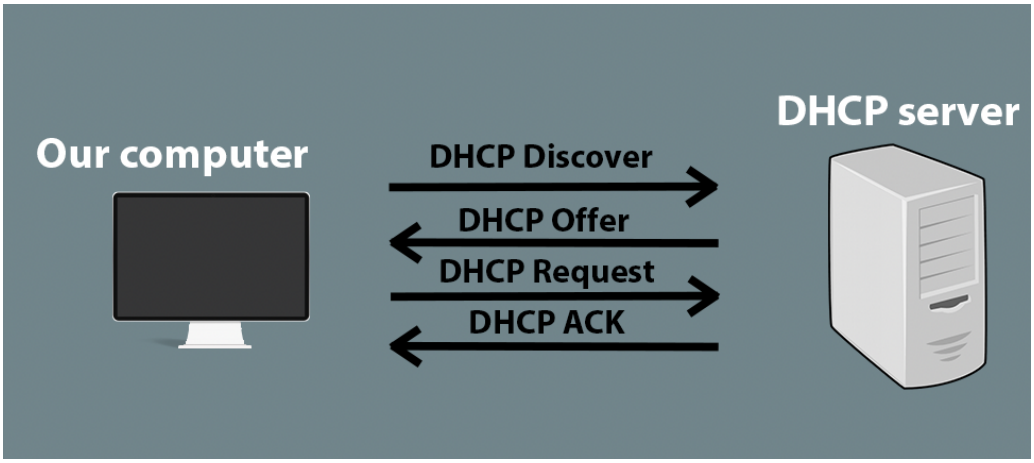
- When the ack number is equal to Next Sequence number, duplicate ack happens.
- When ack number is more then the Next Sequence number, new ack happens.
- When the thread detects a time out, the time out event is triggered to switch the congestion status.

Diagram of the Congestion Control:



Part 3

1. In order to connect our computer to the internet at first, our computer needs some information such as his own IP address (for sending packets), what is his network mask (for understanding which computers are in his subnet mask and which aren't).
In this part, the computer knows only what is the MAC address of the network adapter (because this address is physically burned on the network adapter).
The computer can get the IP address and the rest of the information in several methods - the most common is using DHCP protocol.
Using this protocol our network adapter sends DHCP Discover messages.
The messages sent using broadcast means that all the entities on the network will receive them. DHCP server sees the message and sends back DHCP offer (this message includes all the network information offered to our network adapter: his IP address, the relevant DNS server, and more). Because in our network, there is only 1 DHCP server therefore no other offers will appear. The computer will send a DHCP request that informs the DHCP server that he would like to take the offer. Eventually, the DHCP server will send a DHCP ACK message, which after that our computer is able to use the IP address that he gave.



Now we've got IP address and our router this similar process in order to get its own IP address (The router communicated with the DHCP server of our network provider).
The message got to the DHCP server because we were on the same broadcast domain, which means the message should arrive without reaching any other router.
Also, our computer is connected to a switch (as more computers are connected).

2. Cyclic Redundancy Check (CRC) is a technique used to detect errors in digital data. Similar to checksum, the CRC produces a fixed-length data set based on the build of a file or larger data set.
CRC is a hash function that detects accidental changes to raw computer data commonly used in digital telecommunications networks and storage devices such as hard disk drivers.
It's based on binary division and is also called "polynomial code checksum".

3. HTTP 1.0 vs HTTP 1.1: The main difference between them is that to signify successful requests and to identify transmission problems, HTTP 1.0 status codes were utilized. HTTP 1.1 supports chunk transfers, which enabled material to be streamed in chunks and extra headers to be delivered after the message body. There is some bandwidth waste in HTTP 1.0 but there is less bandwidth waste in HTTP 1.1.
HTTP 1.1. vs HTTP 2.0: HTTP 1.1 loads resources one after the other, so if one resource cannot be loaded, it blocks all the other resources behind it. In contrast, HTTP 2.0 is able to use a single TCP connection to send multiple streams of data at once so that no one resource blocks any other resource. HTTP 2.0 solves this problem by allowing a server to push content to a client before the client asks for it. The server also sends a message letting the client know what pushed content to expect.
Small files load more quickly than large ones. To speed up web performance, both HTTP 1.1 and HTTP 2.0 compress HTTP messages to make them smaller, however HTTP 2.0 uses a more advanced compression method called HPACK that eliminates redundant information in HTTP header packets.
HTTP 2.0 vs QUIC: The aim of HTTP 3 (QUIC) is to provide fast, reliable, and secure web connections across all forms of devices by resolving transport-related issues of HTTP 2.0. To do this, it uses a different transport layer network protocol called QUICK (originally developed by Google). The fundamental difference between them is that HTTP 3 runs over QUIC, and QUIC runs over connectionless UDP instead of the connection-oriented TCP (that is used by all previous versions of HTTP).

QUIC overcomes the limitations of TCP, which means faster handshaking but no handshaking dialogues. A dropped packet only holds up one steam, not all streams. Existing connections are not required to set up communication channels. Better error handling, error correction are used to minimize retransmitting lost data.
QUIC is built at the user level (above the kernel) so doesn't require changes at the protocol level when upgraded.

Comparison of protocol stack changes delivered with each new version after HTTP 1.0:

HTTP 1.1	HTTP 2.0	HTTP 3(QUIC)
● Some methods and response codes are added. ● "Keep-Alive" becomes officially supported. "Host" header becomes supported for a virtual domain. ● System and semantics are separated.	● Support of parallel request transmission bt "stream". ● Addition of flow-control and prioritization function in units of "stream". ● Addition of server-push function (send related file without request).	● Lower protocol changes from TCP+TLS to UDP+QUIC ● Streams and flow-control function are moved to QUIC. ● Parallel request transmission is supported by QIC steam(eliminating TCP HoL blocking).

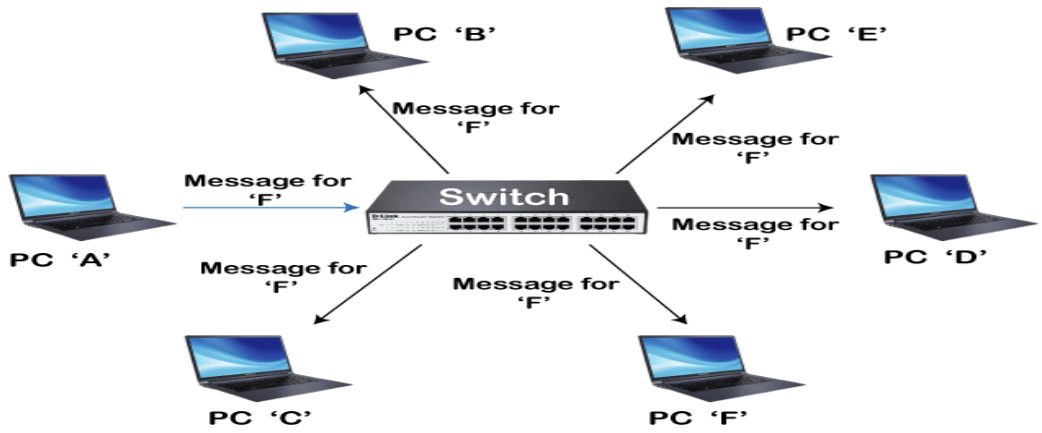
4. In general port number is a way to identify a specific process to which an internet or other network message is to be forwarded when it arrives at a sever. All network-connected devices come equipped with ports that have an assigned number. The most common reason for needing to use ports is for remote access.
A single system can host multiple services. When accessing those services within the network using a combination of <IP address>.<port number>.
The port number decides the service you are interested in among all the services hosted by a device with some IP address.
For example, imagine that you have two cameras on your network, connecting through the same router and you want to be able to connect remotely to both your cameras which are both on port 80.
You decide that you want to access your cameras from the Internet and to set up port forwarding. But you can't forward a single port onto more than one local IP address at the same time. As such you can't access both cameras simultaneously when they're both using port 80.

The solution is to use two separate ports. In our example, you could use port 8000 for the HTTP port on one camera and 8001 for the other camera.
In order to access your camera from the Internet you would need to type HTTP://"IPADDRESS":8000 and HTTP://"IPADDRESS":8001 where the IP address is the external IP address of the router.

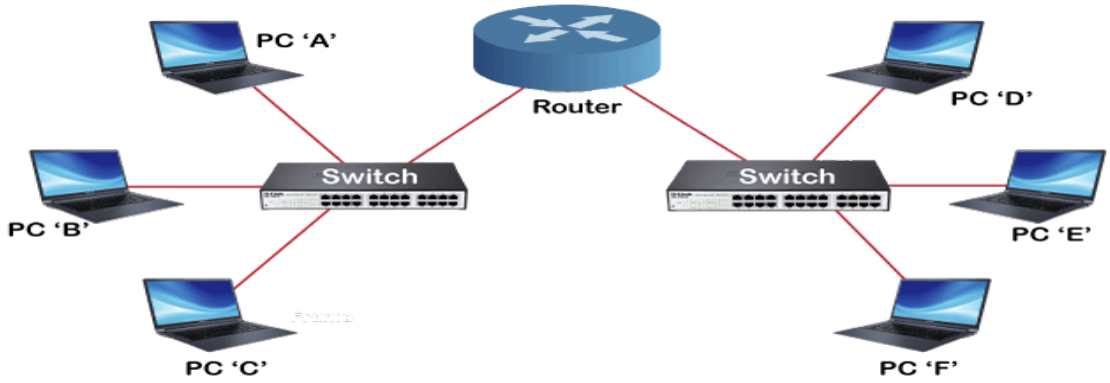
5. In general, the goal of subnetting is to create a fast, efficient, and resilient computer network. As networks become larger and more complex, the traffic traveling through them needs more efficient routes. If all network traffic was traveling across the system at the same time using the same route, bottlenecks and congestion would occur resulting in sluggish and inefficient backlogs.
Creating a subnet allows you to limit the number of routers that network traffic has to pass through.
So, what is subnetting used for: organizing a network in an efficient way is crucial for large firms and those companies seeking to expand technologically. IP addresses can be kept geographically localized meaning that a subnet can be used to specific staffing structures to maintain efficiency and order.

6. Each computer has both an IP address and MAC address assigned to it.
MAC addresses handle the physical connection from computer-1 to computer-2 while IP addresses handle the logical routable connection from both computer-1 to computer-2 and network to network.
For example Computers A, B and C know each other. Computers 1, 2, and 3 know each other. But computer C and computer 3 are special in that they also know each other. So if computer A wants to send a message to computer 2, he will send a message to computer C and ask it to send this message to computer 2. But because computer C doesn't know computer 2 directly it can ask computer 3 to send the message to computer 2. Through this sample message passing, all the computers A, B, C, 1, 2, and 3 can talk to each other even though only computer C from the first group knows computer 3 from the second group.
IP addresses are logical and routable addresses. Computer A could potentially learn the IP address of computer 2. However, MAC addresses are physical and are NOT routable. So, computer A could not really learn the MAC address of computer 2.
And that's why each computer has both MAC address and IP addresses.

7. Switch is a networking device, which provides the facility to share information and resources by connecting different network devices, such as computers, printers, and servers within a small business network. With the help of a switch, the connected devices can share the data and information and communicate with each other.



The router is a networking device used to connect multiple switches and their corresponding networks to build a large network. These switches and their corresponding networks may be in a single location or different locations.
So, the router is an intelligent device and is responsible for routing the data packets from source to destination over a network.



So, the key differences between the Switch & Router:

- The main function of a switch is to connect the end devices such as computers, printers, etc., whereas the main function of a router is to connect two different networks.
- A switch works at the data link layer of the OSI model, on the other hand, a router works at the network layer of the OSI model.
- The switch aims to determine the destination address of the received IP packet and forward it to the destination address. On the other hand, the router's main

purpose is to find the smallest and best routers for the packets to reach the destination, determined using the routing table.

- A switch stores MAC address in the lookup table or CAM table to ger the source and destination address.

In conclusion: we can conclude that both are important devices for setting up a network and both have their own significance in the network. To set up a home-bases network and connect devices, we need a switch, and to connect to networks we need a router.

8. IPv4 is the fourth version of the Internet Protocol that has some limitations that IPv6 is designed to deal with.
Although IPv4 allows only about 4 billion unique addresses we still can't be sure it will be enough for the devices on earth to have their own unique address and as we already know - without a unique address there is no way to ensure that a packet delivered to the correct destination.
Using IPv6 we can extend the 32-bit address of IPv4 to a 128-bit address that allows a humongous number of addresses to own.

Another method is to use NAT (Network Address Translation). This service is used in routers and its purpose is to translate a set of IP addresses to another set of IP addresses. The reason for having the NAT service is to help to preserve the limited amount of IPv6 public IP addresses that we have available around the world.
So instead of asking our internet provider for public IP for each device we want to connect to the internet (which is more expensive, unnecessary, and wasting public IP addresses) we give each device we want to connect a private IP address, and using NAT the router will translate it into a public IP address and then we can have access to world internet. The huge benefit of NAT is that it not only translates private to public, it also translates public to private.

9e. 3C is located in the AS3 area which is based OSPF protocol. Moreover, 3C is on the edge and between AS3 and AS4 there is an BGP protocol. In such case, 3c -> 4c are over BGP and from 4c to 4b and to 4a and eventually to a is on RIP. So the protocols are BGP and RIP.
9f. 3a is located in AS3 (OSPF as mention in 9a). In order to communicate with 3b, we will need OSPF and also from 3b to 3c. From 3c to 4c its BGP as mention in 9c.
From 4c to 4b and to the inside AS4 its RIP. The protocols were used are: OSPF, BGP and RIP.
9g. 1c is located in AS1 which runs RIP protocol. We can notice that 1c is on the edge and in order to communicate with 3a which is in AS3 we need BGP. Then, from 3a to all

the other 3b and 3c we need OSPF. From 3c to 4c its again BGP and from 4c to all the other fours its RIP as mention in 9b that area AS4 runs RIP. The protocols used here: GBP(1c->3a),OSPF(3a->3b,3b->3c),GBP(3c->4c),RIP(4c->4b,4b->4a,4a->c)
9h.2c is located in AS2 area which runs OSPF. In order to get to x we need to go trought AS1,AS3 and eventually AS4.
From 2c to 2a its OSPF, from 2a to 1b its BGP, from 1b to 1a its RIP (because its area AS1),from 1a to 1c its still RIP, from 1c to 3a its BGP from 3a to 3b its OSPF again (area AS3 OSPF),3b to 3c its OSPF again, from 3c to 4c its BGP, from 4c to 4b its RIP,from 4b to 4a still RIP.