Grade 10 review

> Application software refers to all the programs that are designed to solve problems in the real world, helping the computer user. Most of the programs that you use in your computer, like word processing programs, browsers for surfing the Internet, games and media player programs are all application software.

> System software, on the other hand, manages the computer system itself. It provides the tools and an environment in which application software can be created and run. System software often interacts directly with the hardware and provides more functionality than the hardware itself does.

Remember the fetch-execute cycle? We said that an executing program is loaded in main memory and its instructions are processed one after another by the CPU. All computers support multiprogramming, which is the technique of keeping multiple programs in the main memory at the same time. These programs compete for access to the CPU in order for them to be executed. So, it is the operating system's job to perform

memory management to keep track of what programs are in memory and where in memory they are located.

The operating system must also perform process management.

A process is defined as a program you can execute. Since many active processes in the CPU want to execute their instructions at the same time, the operating system has to keep track of the progress of each and carefully manage them so that as they take in using the CPU, they continue from where they left off.

Memory management

The operating system must:

> track where and how a program is located in memory > convert logical program addresses into actual memory addresses.

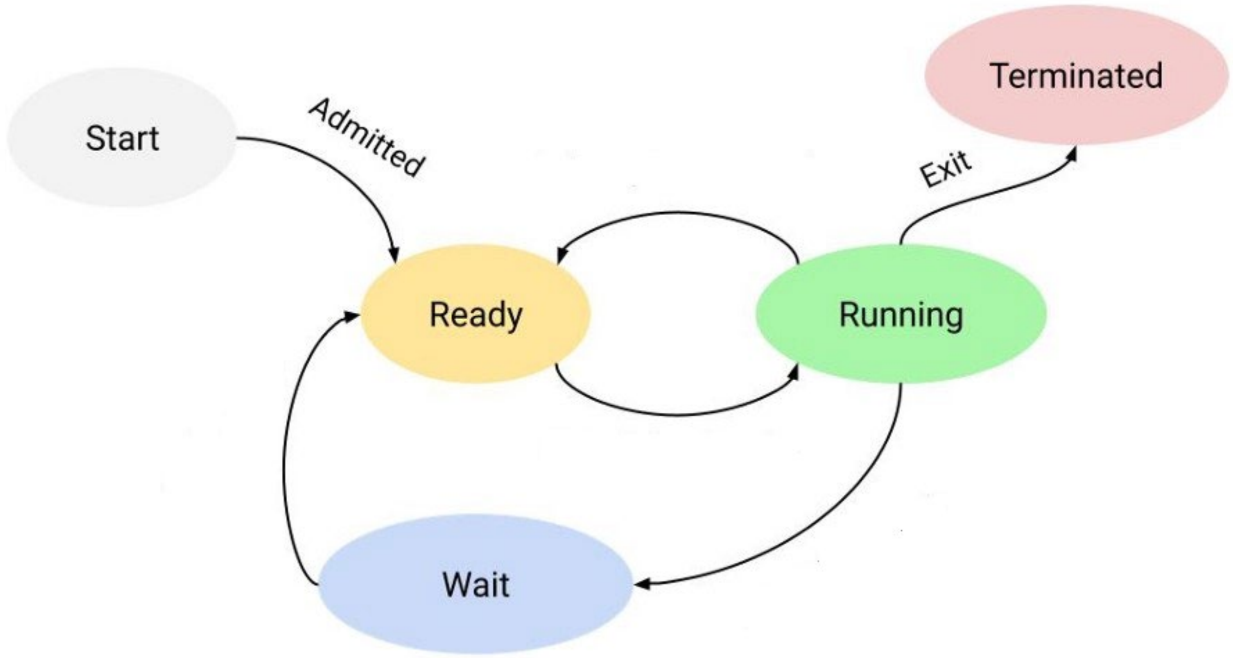
The main memory is seen by the operating system as a continuous storage space that is divided into groups of bits, containing instructions or data. Each of these parts needs to be uniquely identified so it is given an address. Addresses are just integers starting from 0, which is the first memory address.

The problem is that, each program does not know beforehand which addresses in memory are going to be assigned to it. So, a program refers to its other instructions and data by using relative addresses called logical addresses. It is the operating system's job to map a program's logical addresses to the corresponding physical addresses, which are the actual addresses of the main memory, after the program has been placed in memory. This process is called address binding.

Process management

The operating system must also manage the use of the CPU by the individual processes. Only one process can execute part of its instructions at any given time in the CPU so every process goes through a life cycle of various process states as it gains and loses control of the CPU. More specifically, a process enters the system, is ready to be executed, is executing, is waiting for a resource, or is finished.

Let's see what happens to a process as it goes through each stage.



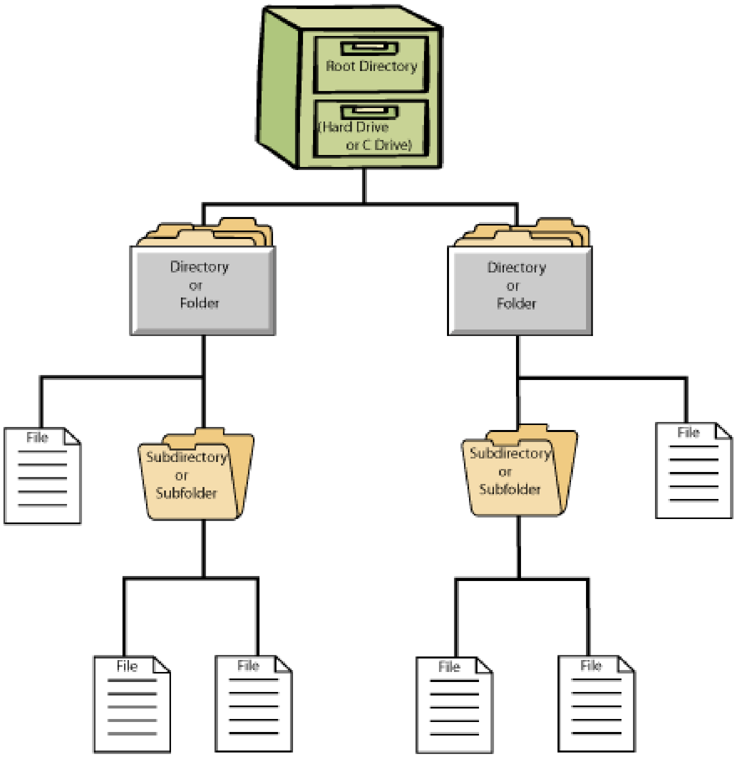
File systems

The organization of secondary storage, like hard disks, is also one of the most important jobs of an operating system. Remember, secondary storage is non-volatile, so this is where all our programs and data reside when the computer is turned off.

Information on a hard disk is organized and stored in files. A file is a named collection of related data and it is the main organizational unit of a hard disk. A file can contain a program, or data of one type or another. For example, your browser program and a digital image are both files on your hard disk.

A **file system** is the logical view that an operating system provides so that users can manage information as a collection of files. A file system is often organized by grouping files into directories. A directory is a named collection of files**.** Think of a folder in which you can store data files, program files or other folders.

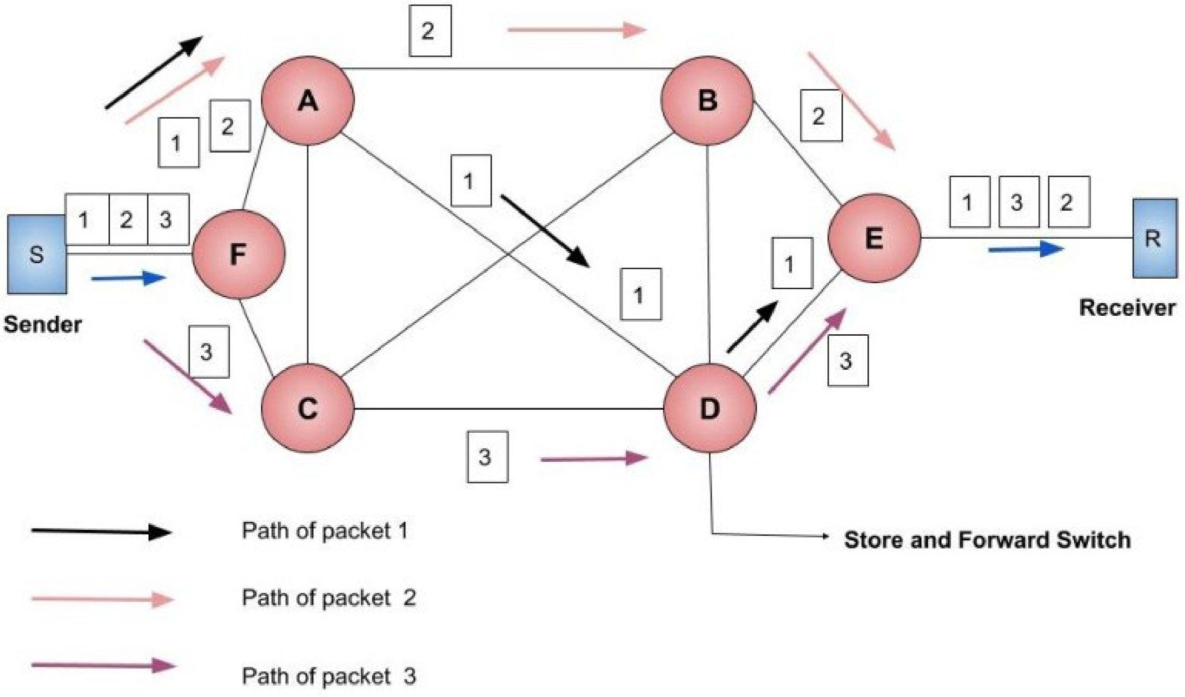
So, a directory of files can be contained within another directory. The directory containing another is usually called the parent directory, and the one inside is called a subdirectory. You can create as many such nested directories as you need to organize your data. Of course, one directory can contain multiple subdirectories and each of these subdirectories can contain their own subdirectories creating a hierarchy structure. From this concept, you can easily understand that a file system can be viewed as a directory tree, showing directories and files within other directories. The directory at the highest level is called the root directory.



Packet Switching

In order to achieve more efficient transfer of messages between different devices over networks, each message is divided into fixed-sized, numbered packets. The packets are then sent over network to their destination, where they are received and reassembled to form the original message. This process is known as packet switching.

The individual packets of a message may take different routes in the network on their way to their destination. As a result, they may arrive in a different order than the one they were sent in. So, upon arrival, the destination device must put them into the proper order to recreate the original message.



Packet Switching

Network addresses

In order for two computers to communicate with each other, they need to be able to identify each other from amongst all the other computers in the world. This is done in two ways.

A hostname is a unique name that specifies a particular computer on the internet**.** Hostnames are generally readable words separated by dots. For example: wikipedia.org

Although it is convenient for us humans to use and remember hostnames, network devices like routers that transfer the actual messages back and forth use another kind of identification mechanism called IP address. An IP address is a series of four decimal numbers separated by dots. For example: **91.198.174.225**

Each of the four numbers that make up an IP address can be in the range 0-255. As you can understand, each hostname has a corresponding IP address. So, in order for us to be able to use convenient and easy to remember hostnames we need a way to translate (resolve, as it is called) each hostname into the corresponding IP address. This is done automatically by the domain name system (DNS) which is a network of computers that constantly store and provide the mappings from hostnames to IP addresses.

Protocols

Generally speaking, a protocol is a set of rules that defines how two things speak to each other or interact. So a network protocol is a set of rules that defines how data is formatted and processed on a network. Network protocols are layered so that each one relies on the protocols that underlie it, forming in that way a **protocol stack**.

TCP/IP

TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. The name TCP/IP refers to a suite of protocols and utility programs that support low-level network communication. The name TCP/IP implies that TCP relies on the IP foundation below it. Those lower two layers of the protocol stack form the foundation of Internet communication.

IP software is responsible for the routing of packets through the web of the various networks to their final destination. TCP software splits the messages into packets, passes them to the IP software for transmission, and then reorders and reassembles the packets at their destination. TCP software also deals with any errors that occur, such as if a packet never arrives at the destination or the contents of a packet are corrupted.

UDP stands for User Datagram Protocol. It is an alternative to TCP. The main difference is that TCP is highly reliable, at the cost of decreased performance, while UDP is less reliable, but generally faster. Note that UDP is part of the TCP/IP suite of protocols.

FTP	File transfer protocol	Transfers files
SMTP	Simple mail transfer protocol	Transfers electronic mail
HTTPS	Hypertext transfer protocol secure	Offering secure communication
DNS	Domain name system	Translate host name to IP address

Web pages are created with HTML**.**

[Hypertext markup language]

URL: Uniform Resource Locator.

Firewalls

A firewall is a software or hardware-based network security system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not. It can be found as a software program running on your computer, embedded in networking hardware devices like routers or as a standalone device. A firewall creates a security barrier that separates and protects a single computer or a local network from the Internet.

First generation

The first firewalls acted as packet filters by inspecting each individual packet that wanted to come in or out of the local network. The firewall filters packets based on the TCP/IP information they contain and decides if a packet will pass by consulting a set of rules configured by the owner of the network under protection. For example, a firewall can be configured to only allow packets of a specific protocol and block all others or allow packets coming from a specific server.

Second generation

Second-generation firewalls perform the work of their first-generation predecessors but retain packets until enough information is available to make a judgment about its state. Known as Stateful Packet Inspection, it records all connections passing through it and determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection.

Third generation

The latest firewalls, called application layer firewalls, are able to inspect traffic by filtering high level protocols like FTP, DNS and HTTP and block any unwanted protocols or detect if a protocol is being abused in any harmful way. They can "understand" the use of data packets and reject anything that seems strange.