Unit 9: COMPUTING

Internal Structure: Overview

Motherboard

The motherboard is the main board which holds/connects all of the major components. They contain slots/sockets for CPUs, RAM chips, data disks, video/sound cards and peripherals. The BIOS is a firmware used for basic set-up of the system that is stored on a memory chip on the motherboard.

Internal Structure: Components

CPU

The CPU (Central Processing Unit, Processor) is the name for the circuitry in a computer that deals almost all of the calculations and logical instructions given to it by programs. However, normally we call modern microprocessors CPUs, which actually consist of more components than a basic processing units. Modern processors often have multiple CPUs and almost always have multiple tiers of their own incredibly fast onboard volatile memory caches, going from very small capacity and the fasted read/write speed, to progressively slower but larger in capacity.

RAM (Random Access Memory)

RAM is computer memory that is very fast to access, secondary in speed to that of the processors onboard memory caches. It is volatile, meaning that it must be powered to store data, so all data is lost once the system is shut down.

The speed of reading & writing data is often a major bottleneck in computing systems, so a slower form of memory is only used when ultimately necessary. RAM is considerably faster than a hard drive to access, and is much larger in capacity than the storage available onboard the processor. Current program's data and open files are stored in the RAM.

GPU

The GPU (Graphics Processing Unit/Video Card), is a specialized chip that is used to process visual output to the display device and also manage most 3D calculations. They are much better suited for dealing with large blocks of data at a time than the CPU, often utilising their own on-board RAM (VRAM). The

hardware is often specialized to support certain functions such as accelerated video decoding, texture mapping and rendering.

Certain CPUs also have their own integrated graphics, which is often less powerful than a dedicated graphics card, but is completely suitable for basic tasks such as watching videos and browsing the web, but, in most cases, isn't suited for more graphics-intensive tasks such as playing 3D games. Integrated graphics cards often use a portion of the system's RAM, which is considerably slower to access than a GPU's VRAM. Integrated Graphics Processors can have up to 30 GB/s of memory bandwidth from the system's RAM, compared to the 264 GB/s of bandwidth that a modern GPU might have with it's onboard memory.

PSU (Power Supply Unit)

This is a fairly obvious one. The power supply's main job is to convert an AC current from the mains supply into the low-voltage DC current that the computer system uses. They often have features such as over/under-voltage, temperature and surge protections built-in. You can buy PSUs that can output a range of wattages, that are suited to different systems. The majority of the power is used by processors in the CPU and GPU, and you can often calculate the rough wattage required for your system by the sum of the required power level of these two components plus an extra 100-200W for the motherboard and extra peripherals.

HDD/SSD (Hard Disk Drive/ Solid State Drive)

HDD's are encased magnetic storage disks, with a read/write head on an actuator arm to access the data. They can come in a variety of form factors, today's most common being the 3.5" and the 2.5".

SSD's often come in the same standardised sizes. They use flash memory, which can be much faster to access, with speeds up to around 500 MBit/s.

They both most commonly use the SATA interface as a controller.

Network Interfaces

Ethernet (IEEE 802.3)

This a wired solution to networking, which requires computers to be connected by cables via switches, which is a device which directs incoming data to the device for which it was intended. This can arguably create a much more reliable network than wireless solutions, as factors such as physical obstructions and electromagnetic interference are much less of an issue. The most common cables used for this currently are fibre optic and twisted-pair ethernet cables. They

are called twisted-pair cables as they are quite literally made from twisted pairs of wires, which is a technique used to reduce electromagnetic interference. The most recent standard of this cable is the Cat. 8 cable, which supports speeds of up to 40 Gbit/s, over distances of less than 30 metres.

Wi-Fi (IEEE 802.11)

Wi-Fi is a solution for a network between devices that is wireless. It is supported by most modern consumer computers such as mobile phones, gaming/entertainment systems, tablets and printers, partly because of it's ease of use. Once a wireless modem (often called a Wi-Fi hotspot) is set up, a Wi-Fi enabled device can connected very easily. Though you can get password-protected Wi-Fi, it is still a much more vulnerable to attacks than a wired network, as the transmissions between devices are literally sent through the air, a medium much more accessible to the average hacker. The most common frequency for Wi-Fi transmissions are 2.4GHz and 5.8GHz, with the most recent consumer standard being the 5.8GHz wireless 802.11ac, boasting speeds of up to 3.5Gbit/s, though devices still only support up to wireless 802.11n, a previous consumer standard, with support for both the 2.4 and 5.8GHz bands.

Wi-Fi is not always a reliable solution though. It is quite susceptible to interference from any devices that might run at similar frequencies. For example devices such as microwaves or bluetooth devices both emit 2.4GHz electromagnetic (em) waves, which some wireless standards also use. Another issue is that higher speed Wi-Fi standards use higher frequencies, which are more easily obstructed. Mediums such as brick walls will absorb higher frequency waves than lower frequency ones, meaning that by using a higher frequency standard you will have to use many more hotspots to connect the same area than you would if you were using a standard that uses 2.4GHz.

Network Types

There are many different network types, not exclusive to these examples:

PAN (Personal Area Network)

A PAN describes a network of personal devices such as mobile phones, tablets and wireless peripherals such as bluetooth headphones and speaker. These networks are being used more and more with the advent of development of wearable tech such as smartwatches and augmented reality (AR) devices.

LANs (Local Area Network) and WANs (Wide Area Network)

Both of these are networks between a number of computers most commonly via Wi-Fi and Ethernet connections, The difference fairly self explanatory, WANs are networks that cover a larger geographical area. The term LAN might be used when describing a network contained in one building such as an school or home network, whereas WAN might be used to describe an office network spanning multiple sites or even larger networks, such as the Internet. A WLAN is a Wireless Local Area Network, which an example of is any network over Wi-Fi.

EPN (Enterprise Private Network)

This is also commonly called an intranet. This is a secure network (it could also be a WAN or LAN) that is only accessible to members of an organisation. These are often used for sharing private work-related and/or commercially sensitive data. Depending on the sensitivity of this data, these networks my be protected behind expensive firewalls. For example, in an industry such as the VFX industry these networks are incredibly important as some film/TV studios that they work often put lots of money into the security and confidentiality of their own data due to fears of losing profits, therefore they would prefer to work with a vfx studio that shares a similar respect for this.

VPN (Virtual Private Network)

A VPN is the result of encrypting transmissions between devices on an otherwise public network. An EPN that spans multiple locations over a public network is a VPN. Another use for these is for people wanting to anonymize their online activity from potential snoopers (The technical term for people who would spy on someone elses data traffic). For example some people might use these to hide from their government to take part in illegal activity, such as unregulated trading or piracy. For these reasons, some politician hold the controversial view of being in support of banning VPNs and encryption. China is an example of a country who has ordered it's state-owned telecommunications firms to ban all VPN traffic as of February 2018.