Definitions for Computer

MAC address:

MAC address stands for Media Access Control Address. It refers to a number **that uniquely identifies a device on a network**. It refers to the Network Interface Card which is part of the device. It is made up of 48 bits which are shown as 6 groups of Hex values. For example, 'NN: NN: NN:DD:DD:DD'. In this address the first half 'NN: NN: NN' is identity number of the manufacturer and the second half 'DD:DD:DD' is the serial number of the device.

IP address:

Each device connected to the Internet is given an address known as the Internet protocol (IP) address. It has two mainly used formats. IPv4 and IPv6. IPv4 is a 32-bit number written in denary or hexadecimal. The newer version of IPv4 is IPv6 which is written in 128 bits and broken into 16 chunks represented by Hexadecimal values.

HTML colour codes:

Hyper text Mark up language (HTML) is a mark up language that is used to represent colour or writing on any type of web page design or document. Colours used in a web page are assigned different hexadecimal values based on red, green, and blue colours.

Colour depth:

It is the number of bits used to represent the number of a pixel. It is also the number of distinct colours that can be represented in an image. It is often measured in bits per pixel and determines the richness of colours in an image.

ASCII Code:

American Standard Code for Information Interchange (ASCII) is a character encoding standard that assigns numerical values to letters, digits, and symbols. The standard ASCII code consists of 7-bit codes (0 to 127 in denary and 00 to 7F in hexadecimal) that represent the letters, numbers and characters found on standard keyboard, together with 32 control codes (that use codes 0 to 31 in denary or 00 to 19 in hexadecimal).

Extended ASCII:

It uses 8-bit codes (0 to 255 in denary or 00 to FF to in hexadecimal). This gives another 128 codes which include non-English alphabets and some graphical characters. Its disadvantage is that it only includes characters from Western languages and not from Non-Western languages which limits its usage worldwide.

Unicode:

Unicode is also an information interchange code which represents **all** languages in the world. Thus, it is used globally. The first 128 characters are identical to ASCII code. Unicode can support several thousand characters in total. ASCII uses one byte to represent one character but Unicode uses up to 4 byte which allows the large range of characters in this code.

Sampling Resolution:

Sampling resolution is the number of bits used to represent sound amplitude in a digital sound recording. It affects accuracy as it tells us how many bits were stored from each point of the sound. The more the bits the higher the accuracy and file size. When the sound is converted to digital form, approximate values are stored.

Bit depth:

Bit depth is the number of bits used to represent the smallest unit in a sound file.

Sampling Rate:

It is the number of sound samples take per second in a digital sound recording. It is measured in hertz (Hz) and is the term used to describe the accuracy of the representation of the original sound.

Bitmap Image:

It is an image composed of pixels where each pixel is individually defined by its colour and position. Bitmap images are also referred to as raster images and can be edited pixel by pixel.

Image Resolution:

It refers to the pixels that make up an image for example it has 4096 pixels in the x axis and 3072 pixels in the y axis of the image then Image resolution will be written as 4096 x 3072 pixels

Pixel density:

It is the number of pixels per square inch in an image.

Calculation of file size:

File size of image is calculated by:

Image resolution (in pixels) x Colour depth (in bits).

And size of mono sound file can be calculated by:

Sample rate (in Hz) x Sample resolution (in bits) x Length of sample (in bits).

Data Packets:

Data that is being sent is broken down into small parts called data packets. Data packets are sent independently from start to end and they are reassembled to form the original message or data when it reaches the receiver.

Nodes:

They are stages in a network that can receive and transmit data packets e.g., router are nodes in the communication network.

Parity Check:

It is a method used to check if data has been transferred correctly. It uses an even parity (Even number of 1 bits) or an odd parity (Odd number of 1 bits). Whether the parity shall be even or odd is decided by the sender and receiver's device before the data is sent.

Parity bit:

A bit (either 1 or 0) added to a byte of data in the most significant bit position to ensure that the byte follows the correct even parity or odd parity protocol.

Parity byte:

It is an extra byte of data sent at the end of a parity block that is composed of parity bits generated from a vertical parity check of the data block.

Checksum:

It is verification method in which we can check if a file has been altered or corrupted. Bothe the receiver and sender agree upon an algorithm to check the checksum value. If the value is the same then there has been no error and vice versa.

SIMPLEX DATA TRANSMISSION:

It is in one direction only (i.e. from sender to receiver). Example: data being sent from a computer to a printer.

HALF-DUPLEX DATA TRANSMISSION:

It is in both directions but not at the same time (i.e. data can be sent from 'A' to 'B' or from 'B' to 'A' along the same line, but not at the same time). Example: a phone conversation between two people where only one person speaks at a time a Walkie Talkie.

FULL-DUPLEX DATA TRANSMISSION:

It is in both directions simultaneously (i.e. data can be sent from 'A' to 'B' and from 'B' to 'A' along the same line, both at the same time). Example: broadband connection on a phone line.

SERIAL DATA TRANSMISSION:

It is when data is sent, one bit at a time, over a single wire or channel (bits are sent one after the other in a single stream). (Note: bits can be transmitted as simplex, half-duplex or full-duplex.). This method of data transmission works well over long distances. However, data is transmitted at a slower rate than parallel data transmission. Since only one wire or channel is used, there is no problem of data arriving at its destination out of synchronization. An example of its use is sending data from a computer to a modem for transmission over a telephone line.

PARALLEL DATA TRANSMISSION:

It is when several bits of data (usually 1 byte) are sent down several wires or channels at the same time; one wire or channel is used to transmit each bit. (Note: bits can be transmitted as simplex, half-duplex or full-duplex.) .This method of data transmission works very well over short distances (over longer distances, the bits can become 'skewed' – this means they will no longer be synchronised). It is, however, a faster

method of data transmission than serial. An example of its use is when sending data to a printer from a computer using a ribbon connector.

Echo Checks:

With ECHO CHECK, when data is sent to another device, this data is sent back again to the sender. The sender compares the two sets of data to check if any errors occurred during the transmission process. As you will have no doubt worked out, this isn't very reliable. If the two sets of data are different, it isn't known whether the error occurred when sending the data in the first place, or if the error occurred when sending the data back for checking! However, if no errors occurred then it is another way to check that the data was transmitted correctly.

ARQs (Automated Repeated Request):

This method can best be summarised as follows:

ARQ uses positive and negative acknowledgements (messages sent to the receiver indicating that data has/has not been received correctly) and timeout (this is the time interval allowed to elapse before an acknowledgement is received)

The receiving device receives an error detection code as part of the data transmission (this is typically a Cyclic Redundancy Check); this is used to detect whether the received data contains any transmission errors.

If no error is detected, a positive acknowledgement is sent back to the sending device.

If an error is detected, receiving device sends a negative acknowledgement to the sending device and requests re-transmission of the data.

A time-out is used by the sending device by waiting a pre-determined amount of time …. » ... and if no acknowledgement of any type has been received by the sending device within this time limit, it automatically re-sends the data until a positive acknowledgement is received …. or until a

pre-determined number of re-transmissions has taken place » ARQ is often used by mobile phone networks to guarantee data integrity.

Check Digit:

Number added to a code (such as a bar code or account number) to derive a further number as a means of verifying the accuracy or validity of the code as it is printed or transmitted. A code consisting of three digits, for example, such as 135 may include 9 (sum of 1, 3, and 5) as the last digit and be communicated as 1359.

Check digits can identify 3 types of error:

(1) If 2 digits have been inverted e.g., “23459” instead of “23549”

(2) An incorrect digit entered e.g., 23559 instead of 23549

(3) A digit missed out altogether e.g., 2359 instead of 23549

Example 1: Generation of the check digit from the other 12 digits in a number by ISBN-13.

The following algorithm generates the check digit from the 12 other digits:

1- add all the odd numbered (positioned) digits together
2- add all the even numbered (positioned) digits together and multiply the result by 3.
3- add the results from step1 and step2 together and divide by 10

4- take the remainder, if it is zero then use this value 5- otherwise subtract the remainder from 10 to find the check digit.

Data Compression Notes

Q: What is Data Compression?

Ans: Data compression is a method in which the number of bits of a file are reduced for following reasons:

- To save storage in devices such as hard disks or other storage devices.
- To reduce the time taken to stream a music or video file.
- To reduce time taken to download or upload a file from the internet.
- Reduced data size results in a faster transfer rate because or less bits.
- In some cases, like cloud storage where more file size means more cost, it helps reduce cost.

Q: What are the two types of data compression?

Ans: They are:

1. Lossy compression
2. Lossless compression

Lossy compression:

In lossy compression, data is compressed by deleting unnecessary information from photos, videos, and sound. It is also known as irreversible compression as once it is applied the lost data is not recoverable. In short, it is the compression of data in a way that the quality remains noticeably same.

Examples are MPEG-3 (MP3), MPEG-4 (MP4), and JPEG.

For example, in images, it may reduce the resolution and/or bit/ colour depth. It removes the differences between such colours that cannot be differentiated by the human eye and also the bright part of the images can be detected well but the detail in the dark parts of photos can be

removed. And by separating pixel colour from brightness, the image can be split into 8x8 pixel blocks which allows to discard some parts of the image without causing significant change in quality

And in sound files, it may reduce sampling rate and/or resolution. Two main concepts are used. Firstly, the sounds that are out of humans hearing range are removed and secondly, is that if two sounds are played, only the louder one will be heard by us so the softer one will be removed. It can reduce the sound file size about 90%.

Lossy compression reduces file size more than lossless compression.

Lossless Compression:

Lossless compression is a technique in which the data from the original file can be reconstructed. It is particularly used when some important file is being compressed such as spread sheet or when downloading a large file. It is reversible compression. One method of Lossless compression is RLE or Run-Length-Coding.

Run Length Coding:

It is a form of Lossless compression which can be used on images and text.

- It is a form of reversible compression.
- It reduces the size or string of adjacent data. It is encoded into two values. The first value represents the number of identical data items and the second value represents the code of the data item (such as ASCII or Unicode).
- It is only affective when there is a long string of repeated calculated data.

For example, 'aaaabbbbccccdddd,' can be written in RLE. If code for a is 97, b is 98, c is 99, d is 100, it can be written as 04 97, 04 98, 04 99, 04 100. As one number uses 1 byte it will only require 8 bytes instead on the 16 bytes used first.

Data Transmission notes

Q: What are data packets? Why are they used and what are its benefits?

Ans: Data that is to be sent over long distances is broken up into small data packets of 64 KiB which makes it easier to control and send it over a long distance. They are also known as datagrams. Each data packet contains a header, payload and a trailer. The header consists of:

- IP address of sender.
- Ip address of receiver.
- The sequence number of the packet.
- The size of packets in bits.

The payload consists of the actual data that is stored in the packet. The trailer consists of:

- Some way of identifying the end of the packet.
- An error checking method CRCs are used to check if the data is correct.

Q: What are CRCs?

Ans: Cyclic redundancy checks are used to check data packets by:

- First the sending computer adds up the number of 1-bits in the payload and stores this a hex value in the trailer.
- Once the receiving computer receives the data it checks the number of the 1-bits through the value stored in the payload.
- If the values match, then there has been no error in the data transmission otherwise the data needs to be resent.

Q: Explain packet switching?

Ans: Packet switching is a method of data transmission in which a message is broken into a number of different data packets and are sent independently on from start to end and are reassembled (using the

information in the header) when all packets reach their destination. At each stage of transmission there are nodes that contain a router. Each router (after seeing the destination IP address) decides the best path for the packet to reach its destination. Following are its characteristics:

- Each packet will follow its own path or route.
- Routers will determine the route of each packet.
- Routing selection depends upon the number if packets waiting to be processed at each node.
- The shortest path **AVAILABLE** will be selected.
- The packets reach their destination in a different order than that of in which they were sent.

Benefits of packet switching are:

- There is no need to use a single communication line and overload it.
- It is easy to overcome faulty lines by just re-routing the packets.
- It is easy to expand the package usage.
- A high data transmission rate can be achieved.

The drawbacks of packet switching are:

- Packets can be lost and need to be resent.
- There is a delay when the packets need to be reassembled.
- This method is more prone to errors in real time live streaming.

Q: What is a USB?

Ans: Universal Serial Bus (USB) The UNIVERSAL SERIAL BUS (USB) is a form of serial data transmission method. It is the most common type of input/output port found on computers. It has quickly become the standard method for transferring data between a computer and a number of devices. Essentially, the USB cable consists of: a four-wire shielded cable two of the wires are used for power and the earth two of the wires are used in the data transmission.

When a device is plugged into a computer using one of the USB ports: the computer automatically detects that a device is present (this is due to a small change in the voltage level on the data signal wires in the cable).

The device is automatically recognized, and the appropriate DEVICE DRIVER is loaded up so that computer and device can communicate effectively.

If a new device is detected, the computer will look for the device driver which matches the device; if this is not available, the user is prompted to download the appropriate software.

Benefits	Drawbacks
devices plugged into the computer are automatically detected and device drivers are automatically loaded up	standard USB only supports a maximum cable length of 5 m; beyond that, USB hubs are needed to extend the cable length
connections can only fit one way preventing incorrect connections being made	
it has become an industry standard, which means considerable support is available	even though USB is backward compatible, very early USB standards (V1) may not always be supported by the latest computers
can support different data transmission rates (from 1.5 Mbps to 5 Gbps)	
no need for external power source since cable supplies +5 V power	even the latest version 3 (V3) and version 4 (V4) USB-C systems have a data transfer rate which is slow compared to, for example, Ethernet connections (Note: USB V2 has a maximum data transfer rate of 480 Mbps.)
USB protocol notifies the transmitter to re- transmit data if any errors are detected; this leads to error-free data transmission	
it is relatively easy to add more USB ports if necessary, by using USB hubs	
USB is backward compatible (that is, older versions are still supported)	