Networks and the effects of using them

- A computer network is developed by linking computer systems together so that they can communicate with each other, share computing power and storage facility. It is inclusive of all the individual computer systems, connections and hardware which enables communication

Advantages of networking

i. Computers can communicate with each other easily
ii. Computers can share data and files
iii. Computing power and/or storage facility can be shared
iv. Hardware such as printers are required
v. There is control over which programs a user has access to

Disadvantages

i. A virus can spread more easily
ii. Greater need for security
iii. If the server fails, all work stations will be affected
iv. Installation costs are high
v. Damage to cables can isolate computers from the network

Network devices

Modems

- Stands for modulator demodulator
- Converts a computers' digital signal to analogue signal for transmission over an existing telephone line
- It also converts analogue signals to digital signals to enable the computer to process the data
- Modems essentially used to allow computers to conneet to networks over long distances using telephone lines

Hubs

- Hubs are hardware devices that can have several devices or computers connected to them
- They are often used to conneet a number of devices to form a LAN
- Its main task is to distribute a received data packet to every computer on the network
- It is not a very secure or efficient method of data distribution

Switches

- They conneet a number of devices or computers together to form a LAN
- The switch checks the data and sends the data to the appropriate computers only
- This makes a more secure way of distributing data
- Each device or computer has a MAC address which uniquely identifies it
- Data packets sent to switches will have a MAC address identifying each device that should receive the data

Bridge

- Bridges are devices that connect one LAN to another LAN that uses the same protocol (communication rules)
- They are often used to connect different parts of a LAN so that they function as a single LAN
- They are used with interconnected LANs to avoid unnecessary traffic

Router

- Routers enable data packets to be routed between different networks (e.g. between a LAN and a WAN)
- A router will typically have an internet cable plugged into it and several cables connecting to computers and other devices in the LAN
- Broadband router sit behind a firewall. The firewall protects the computers on a network
- The routers' main function is to transmit internet and transmission protocols between two networks and also allow private networks to be connected together
- Routers send data packets sent to it from any computer on any of the networks connected to it
- Since every computer on the same network has the same part of an IP address, the router is able to send the data packet to the appropriate switch and it will then be delivered using the MAC address
- If the MAC address doesn't match any device on the network, it passes on to another switch on the same network until the appropriate device is found

Data packets

Packets of data usually contain the following information:

i. Some form of header to identify the data packets
ii. The sender's IP address
iii. The receiver's IP address
iv. How many data packets make up the whole message
v. The identity number of each packet

- This information allows the router to route a packet across a network to its correct destination and allows the data to be reassembled in its correct order according to identity number at the receiving station
- When a router receives a packet of data, it checks the destination IP address against a stored routing table
- The routing table stores the MAC address of the device, the assigned IP address and the lease time the IP address is assigned for
- The bits forming the destination IP address in the data packet are used to point to the correct route
- The packet is sent to a number of routers until it reaches its final destination

Gateway

- A network point or node that acts as an entrance to another network

Network interface card (NIC)

- Needed to allow a device to connect to a network

- It is usually part of the device hardware and frequently contains the MAC address generated at the manufacturing stage

Network cables

- Network cables are used because they have faster data transfer rates and can be more secure than wireless networks as compared to Wi-Fi
- Made from copper or fibre optic cables
- The fibre optic cables offer higher data transfer rates and better security

IP (Internet Protocol) and MAC (Media Access Control) addresses

- Each device on the internet is given a unique address called an Internet Protocol Address, it is written in the form of a 32 bit number
- A MAC address is a unique number that identifies a device connected to the internet
- An IP address gives the location of a device on the internet whereas a MAC address identifies the device connected to the internet

Wi-Fi

- Refers to nay system where it is possible to connect to a network through wireless communication
- A wireless transmitter (WAP) receives information from a network via its connection
- This transmitter converts the received information into radio waves and then transmits them
- A device receives the radio waves and via an installed wireless adaptor which allows it to download the information from the data source
- This works in reverse when the device wishes to transmit data over a network
- Wi-Fi is best suited to operating on full scale networks since it offers faster data transfer rates, better range and better security than Bluetooth
- In essence, Wi-Fi relies on some form of access point which uses radio frequency technology to enable the devices to send and receive signals

Bluetooth

- Bluetooth sends and receives waves in a band of 79 different frequencies (channels)
- Devices using Bluetooth automatically detect and connect to each other but they don't interfere with other devices since each communicating pair uses a different channel
- When a device wants to communicate, it picks one of the 79 channels at random
- If the channel is being used, it randomly picks another channel
- This is called spread spectrum frequency hopping
- To further minimise the risks of interference with other devices, the communication pairs constantly change frequency
- Bluetooth is useful when:
    i. When transferring data between two or more devices that are very close together
    ii. When the speed of data transmission is not critical
    iii. For low band width applications
- Bluetooth creates a secure WPAN (wireless personal area network) based on key encryption

How to set up and configure a small network

- Setting up an IP account if internet access is required
- Setting up the system (buying the appropriate hardware correctly configured) to allow for wireless connectivity
- Configure all hardware and software so that they work together
- If internet is requires, ensuring that a high speed broadband exists
- Putting all the common software onto a server and also making sure that a network licence has been acquired so that all network users can make use of the software
- Setting up privileges so that each user can only access their own area or common shared area
- Setting up a network manager level of privilege so that they can monitor network usage

Internet

- The internet is a worldwide collection of networks that allows users to:
    i. Send and receive emails
    ii. Chat online
    iii. Transfer files from computer to computer
    iv. Browse the world wide web

- The world wide web is only a part of the internet by which users can access by way of a web browser
- It consists of a massive collection of webpages and has been based on the http (hypertext transfer protocol)

Intranet

- Intranet is a computer based network based on internet technology but is designed to meet the internal needs for sharing information within a single organisation or company
- Intranets reside behind a firewall and are only accessible to: internal members of an organisation, people given various levels of access who are external to the company
- Intranets are safer than internet since there is a less chance of external hacking or viruses
- It is possible to prevent external links to certain websites
- Companies can ensure that the information available is specific to their needs
- It is easier to send out sensitive information knowing that it will remain within the organisation
- Intranets offer a better bandwidth than the internet thus there are fewer connection limits than with the internet
- It is possible to create extranets that allow intranets to be extended outside the organisation

What are the differences between internet and intranet?

- The term intranet stems from internal restricted access network
- The term internet stems from international network
- A intranet is used to give local information relevant to the company or organisation whereas internet covers topics of global interest
- It is possible to block certain websites using the intranet while this is also possible with internet, it is more difficult

- An intranet requires password and a user ID entry and can only be accessed from agreed points/computer; the internet can be accessed from anywhere provided the user has an ISP account
- An intranet is behind a firewall, which gives some protection against hackers, viruses, and so on; this is more difficult with internet access since its open on an international scale
- The internet can be public access, whereas intranets tend to be private access

Local Area Networks (LANs)

- These systems are usually restricted to one building and do not extend over a large geographical area
- A typical LAN will consist of a number of computers and devices that are connected to hubs or switches
- One of the hubs or switches will usually be connected to a router and a modem to allow the LAN to connect to the internet, doing so it becomes part of a WAN

Advantages

i. The sharing of resources
ii. Ease of communication between users
iii. A network administrator to control and monitor all aspects of the network

Disadvantages

i. Easier spread of viruses throughout the whole network
ii. Printer ques developing, which can be frustrating
iii. Slower access to external networks, such as internet
iv. Increased security risk when compared to individual computers
v. If the main server breaks down, in most case the network will no longer function

Wide Area Networks (WANs)

- WANs are used when computers or networks are located at a long distance from each other geographically
- Several LANs joined together form a WAN
- The most common examples of WAN include the internet and the network of ATMs used by banks
- Because of the long distances between devices, WANs usually make use of some public communications networks
- But they can use dedicated or leased communication lines which can be less expensive and also more secure
- A typical WAN system consists of end systems and intermediate systems

Wireless LANs (WLANs)

- They are similar to LANs but there are no wires or cables
- They provide wireless network communication over fairly short distances using radio infrared signals
- Access points or wireless nodes are connected into the wired network at fixed locations
- The Aps receives and transmits data between the WLAN and the wired network
- Users access the WLAN through wireless LAN adapters that are built into the devices or plug in model

Advantages

i. All computers can access the same resources from anywhere within the access point
ii. As there is no cabling there is greater safety improvement and increased flexibility
iii. Adding new computers and devices is very easy and the costs are reduced since extra cabling isn't needed

Disadvantages

i. Security ~ anyone with a WLAN enabled laptop can access the network
ii. There may be problems with interference which can affect the signal
iii. The data transfer rate is slower than a wired LAN

Accessing the internet using a mobile phone/tablet

Advantages

i. Portability, can be used anywhere provided there is a network signal
ii. A person is more likely to have their mobile phones with them at all times
iii. It is easier to use a mobile phone while on the move

Disadvantages

i. Expensive to use if Wi-Fi hotspot is not available
ii. Signal is not as reliable or stable as a wired system
iii. The displays on mobile phones are smaller which may make it difficult to read web pages
iv. Keyboards are very small and difficult to type in messages or navigate websites
v. Not all websites are mobile friendly therefore not all websites may be accessible

Accessing the internet using a laptop

Advantages

i. Laptops are more portable as compared to desktops but heavier and less portable than mobile phones
ii. Touchpads on laptops are easier to use than touch screens on mobile phones
iii. The keyboards on laptops are easier to use than those on mobile phones but not as compact as those on a desktop computer

Disadvantages

i. Although the screen is usually larger than mobile phones and tablets it is not as large as those on a desktop computer
ii. Laptops require expensive dongles to access phone networks
iii. Processors used in laptops are not as powerful as those in desktops, so access speed is not as quick

Accessing the internet using a desktop computer

Advantages

i. Tend to have a more powerful/faster processor than other devices

ii. Usually have a more stable and reliable internet connection since they use a wired system rather than Wi-Fi
iii. All web pages are accessible due to larger screen size than other devices
iv. Use of full sized keyboard and pointing devices makes navigation of webpages easier

Disadvantages

i. They are not compact and portable
ii. Require expensive dongles to access phone network

Network issues and communication

Should the internet be policed?

Reasons in favour of control

- It would help to prevent illegal material being posted on websites
- People find it much easier to discover dangerous information, although available in books, it is easier with a search engine
- It would help to prevent children and other vulnerable groups from being subjected to undesirable websites
- It would help to stop incorrect information being published on websites

Arguments against control

- Material published on websites are already available from other sources
- It would be expensive to police all websites and users would have to pay for access
- It would be difficult to enforce rules and regulations on a global scale
- It can be argued that policing would go against the freedom of information
- Laws already exist to deal with those who deal with immoral content

Inappropriate sites and the accuracy of information

Reliability of information

- Information on the internet is more likely to be more up to date than books
- It is much easier to attain information from websites
- Information could be incorrect, biased or inaccurate

Undesirability of certain websites

- There is always a risk of finding undesirable websites
- There is a risk of connecting to in genuine websites
- Security risks

Security issues

Passwords

Protection of passwords:

1. Run anti spyware software to ensure that your passwords aren't being relayed back to whoever put spyware on your computer
2. Change passwords on a regular in case they have been possessed illegally or accidently

3. Passwords should not be very easy to break or guess

Characteristics of a strong password:

1. At least one capital letter
2. At least one numerical value
3. At least one keyboard character

Authentication techniques

- User IDs and passwords
- Digital certificates
- Biometrics
- Magnetic stripes/ID cards/passwords

Methods of avoiding viruses

Anti-virus software

- They check the software of files before they are run or loaded onto a computer
- Antivirus software compares a possible virus against a database of known viruses
- They carry out heuristic checking (checking for behaviour that detects a possible virus)
- Any possible programs that are infected are then put into quarantine that allows the virus to be deleted o allows users to make the decision of deletion
- Anti-virus software need to be kept up to date as new viruses are constantly being discovered
- Full system checks should be carried out at least once a week

Avoiding viruses when accessing the internet

- Avoid unknown or suspicious looking websites
- Look for security indicators such as 'https' or the padlock symbol
- Look out for odd behaviours on the URL
- Copy and paste links into the URL as opposed to clicking on direct links
- Don't open emails from unknown source
- Apply common sense

Viruses from hardware devices

- it is possible to pick up viruses from any device that is plugged into your computer
- even with the precaution of scanning, it is unsafe to plug in a device from unknown sources

Data protection acts

- There are general guidelines about how to stop data being obtained unlawfully:
    i. Don't leave personal information lying around on a desk when unattended
    ii. Lock filing cabinets at the end of the day when the room in unoccupied
    iii. Do not leave data on a computer monitor is if it unattended
    iv. Use passwords and user IDs
    v. Make sure that information being sent via fax or email is not sensitive

Data Protection Act

1. Data must be fairly and lawfully processed
2. Data can only be processed for the stated purpose
3. Data must be adequate, relevant and not excessive
4. Data must be accurate
5. Data must not be kept longer than necessary
6. Data must be processed in accordance with the data subject's rights
7. Data must be kept secure
8. Data must not be transferred to another country unless they also have adequate protection

Network communication

Fax- fax is short for the word facsimile

- Documents are scanned electronically and converted to bit map image (a bit is a binary digit either 1 or 0)
- This is then transmitted as a series of electrical signals through the telephone network
- The receiving fax machine converts this image and prints it out on paper
- More modern ways of faxing occurs electronically which makes use of computer technology and the internet

E-mail

- This is an electronic method of sending text and attachments from one computer to another over a network

Advantages

i. It is fast to send and receive replies using the email
ii. Low costs since stamps, paper and envelopers are not needed
iii. There is no need to move around to send the mail
iv. Can be sent to several people at one go

Disadvantages

i. High chances of downloading viruses attached to emails
ii. The email address has to be completely correct to send to the right person
iii. One cannot send bulky items over emails
iv. You cannot send or sign legal documents over email

Faxes	Emails
More likely to be intercepted as it needs to be printed	More secure than faxed
Signatures on faxes are accepted legally	No need to print the document
The quality of documents can be quite poor	The document is usually a better quality
If telephone network is busy-there can be a delay	Can be modified, copied and pasted to other documents
Can be slow if several documents are to be scanned to be transmitted	Much easier to send to multiple recipients at the same time
	People are more likely to have access to email accounts than a fax machine

Video Conferencing

- This is a method of communication between two or more people at separate locations in real time
- It makes use of internet or LAN
- Requires hardware such as: web cams, large monitors or television screens, microphones and speakers
- Special software such as CODEC and echo cancellation software
- CODEC converts and compresses analogue data into digital data
- Echo cancellation software allows talking in real-time and synchronises communication

Advantages

i. Reduces travelling costs
ii. Reduces booking costs
iii. Meetings can be called at short notice
iv. Travelling time is eliminated
v. It reduces chances of terrorist attack

Disadvantages

i. It is an expensive system to set up and maintain
ii. Sound and picture quality can be pure
iii. Different time zones between countries can be a problem
iv. Time lagging is a problem as well
v. You cannot sign documents

Audio Conferencing/Phone Conferencing

- Audio conferencing refers to meetings held between people using audio or sound equipment
- An audio conferencing can be done over a telephone network and that is referred to as phone conferencing

The following are steps carried out when having a phone conferencing:

1) The organiser of the conference is given two PINs by the phone company, one PIN is the personal PIN given to the organiser and the second PIN is given to the participants
2) The organiser contacts all participants and informs them of their PIN and the time of conference
3) Just before the beginning of the conference the organiser dials the conference phone number; once connected the personal PIN number is keyed in
4) The participants call the same conference number and then when connected, they key in their PIN numbers. Then the conference will begin

Web Conferencing

- Referred to as webinar
- Uses internet to permit conferencing to take place
- Multiple computers are used connected to the internet
- Carried out in real time
- Allows business meetings, presentations, and online training/education to take place
- Only requirement is high speed, stable internet
- Web conferencing is carried out on an app or website

- The organiser can decide who can speak with a control panel on their computer
- If a delegate wishes to say something- a flag is raised next to their name
- Delegates can posy comments

Main features

i. Slide presentations
ii. Possible for delegates to draw on a 'whiteboard' using their keyboard/mouse
iii. Transmit images or videos via webcam
iv. Documents can be shared by uploading to website before conference
v. Possible to chat verbally or use instant messaging

- Web conferencing interlinks with audio and video conferencing through the use of web cams and built in microphones