4.7 Communication methods

Many methods of communication using networks exist. These include **fax**, email, **video conferencing** and VOIP.

Fax

The term **fax** is short for the word 'facsimile'. With this system, documents are scanned electronically and converted into a **bit map** image (a bit is a *b*inary dig*it* and is a 1 or a 0). This is then transmitted as a series of electrical signals through the telephone network. The receiving fax machine converts this electronic image and prints it out on paper.

It is also possible to generate fax signals from a computer to allow files and documents to be sent to a fax machine – this saves printing out the document first and then passing it through a fax machine. Fax/modem software in the computer converts the image into a form recognised by a fax machine. However, this is not as efficient as the email system where the electronic copy is sent and is then stored electronically thus permitting the document to be edited, for example.

Email

This is an electronic method for sending text and attachments from one computer to another over a network (see Section 4.4 for further details).

The advantages of using email include:

- the speed of sending and receiving replies using the email system
- the low cost, since stamps, paper and envelopes are not needed
- not needing to leave home to send the mail.

Disadvantages include:

- the possibility of virus threats and hacking
- the need for the email address to be completely correct
- the inability to send bulky objects via emails.

Video conferencing

This is a method of communication between people at two separate locations (e.g. in different countries). This is done in **real time** and makes use of a LAN, if internal, or through a WAN, e.g. the internet, if national or international. The system works in real time and uses additional hardware such as webcams, large monitors/television screens, microphones and speakers.

The system also uses special software such as:

- CODEC, which converts and compresses analogue data into digital data to send down digital lines
- echo cancellation software, which allows talking in real time and synchronises communications.

Delegates at one end speak into a microphone and look at a webcam. The other delegates can see them and hear them using large monitors and speakers.

There are potential problems with these systems such as time lag (the time it takes for the signal to reach its destination, which can be difficult when trying to have a conversation since there seems to be a delay). Also, sound quality and picture quality can be poor unless expensive hardware and software is used.

However, these systems are becoming increasingly popular as the cost of travelling increases and the risk of terrorist attacks becomes higher. One large company, which reduced travelling from Europe to USA and used video conferencing wherever possible to discuss product development, claims to have saved several million US dollars over a 12-month period. The savings were due to reduced travelling (mostly air fares) and to reduced overnight accommodation. Since little or no travelling is involved meetings can be held at short notice, but time differences between countries can become an issue.

VOIP

Voice over internet protocol (VOIP) is a method used to talk to people using the internet. VOIP converts sound (picked up by the computer microphone or special VOIP telephone plugged into the USB port of the computer) into discrete digital packets which can be sent to their destination via the internet. One of the big advantages is that it is either free (if the talking is done computer to computer, i.e. both computers have VOIP telephones or use their built-in/plugged-in microphones and speakers) or at a local rate to anywhere in the world (when VOIP is used to communicate with a mobile or land line telephone rather than another computer).

To work in real time this system requires a broadband ISP. The main problems are usually sound quality (echo and 'weird sounds' are both common faults). Security is also a main concern with VOIP, as it is with other internet technologies. The most prominent security issues over VOIP are:

- identity and service theft
- **viruses** and **malware** (malicious software)
- **spamming** (sending **junk mail**)
- **phishing** attacks (the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft).