PC Passport

Internet and Online Communications
Student Workbook

Published date: August 2008

Publication code: CB4120

Published by the Scottish Qualifications Authority
The Optima Building, 58 Robertson Street, Glasgow G2 8DQ
Ironmills Road, Dalkeith, Midlothian EH22 1LE

www.sqa.org.uk

Introduction

This student workbook is one of a range of eight titles designed to cover topics for the refreshed PC Passport. Each title in the range covers the required subject material and exercises for candidates studying PC Passport.

This workbook covers all three levels of PC Passport — Beginner, Intermediate and Advanced.

There are a number of exercises associated with each subject and it is recommended that centres download and use the sample exercise files provided.

Each workbook will help prepare candidates for the assessments for the refreshed PC Passport. It is recommended that centres use the most up-to-date Assessment Support Packs appropriate for their type of centre, eg either school, FE or work-based.

Contents

Internet Overview

The internet is a worldwide collection of millions of computers all linked together. Although most people think the internet and the *World Wide Web* (or simply the *web* or the *net*) are the same thing, in fact the web is only part of the internet. The internet is made up of a number of different parts, all of which communicate using different languages called *protocols*. Web pages, for example, use the *HTTP* protocol to transfer web pages from the server they're stored on to your browser, while e-mail uses *SMTP* to transfer mail messages from one user to another.

The *World Wide Web* is made up of millions of *web pages* (specially formatted documents written in a language called *HTML* (*HyperText Markup Language*). You can often jump from one page to another related page using *hyperlinks* (or simply *links*) that have been included for this purpose. For example, on the BBC News site, the front page contains many headlines as hyperlinks that you can click to jump to the full story and other links for returning to the front page or viewing other stories.

E-mail messages are transferred from one computer user to another using the SMTP protocol. These might be messages that are typed, or they might include files stored on the sender's computer (these are called *attachments*).

Chat is the term given to *real-time* (occurring immediately) communication between two or more computer users. When one user enters their message on their computer, it appears on the other user's computer. In this way, users can communicate as if they were chatting in the same room or on the phone.

Also known as *forums*, *bulletin boards* or just *groups*, newsgroups are online discussion groups. Unlike chat, though, newsgroups are not real-time. One user *posts* a message to the newsgroup and others reply to it in their own time. There are many thousands of newsgroups on the internet, covering every area of interest you can think of.

Connecting to the Internet

Normally, your home computer will connect to the internet using a modem and a telephone line, and your computer at work will use a network and a faster connection. This might not always be the case — you might use a faster connection at home if you use the internet a great deal or you download large files such as music or video. This will depend on the speed of the connection and factors like the *contention ratio* — a ratio of 50:1 means you could, at worst, be sharing your bandwidth with up to 49 other users at one time. If the ratio of users using the ISP service is high, speeds will slow, if the ratio of users is low, then access speed will be higher.

To connect to the internet, you will need three items:

- A connection device such as a computer (with web browser software).
- A communication link such as a *modem*, *cable modem*, *router* (wireless or cabled) or an *ISDN line*.
- An *internet service provider* (*ISP*) user account. The amount of space an ISP might allow is dependent on the type of files you might store. For example you may want to store lots of large digital photos and require the ISP to offer a separate storage space just for storing images.

Connection Devices

Although you'll usually use a computer to connect to the internet, there are other devices that can be used. For example, some modern mobile telephones are also able to connect. In this case, you don't need a modem or ISP account as these are built into the phone and are part of the service you receive when you purchase these phones.

Your computer will use a program called a *web browser*. Using this browser you can enter and find your way around the web, displaying the web pages you are interested in. You can also *bookmark* pages you may want to return to later; use search facilities called *search engines* to find what you're after, and you can save information from the web on your own computer.

Two popular browsers are Internet Explorer (from Microsoft) and Firefox — although there are others available such as Opera.

Communication Links

The most common devices in homes for connecting to the internet are the modem or a broadband router which could be connected to your computer with a network cable or connected with wireless technology. You can even connect through your satellite provider now. In business, there will usually be a number of users connecting to the internet via their computer network, therefore, businesses will usually invest in one of the faster, more powerful internet communication devices, known collectively as *broadband*.

Modem

There are two different types of modem devices. Modem stands for **Mo**dulation and **Dem**odulation device, as the modem has to convert the signals it receives into a language the computer can understand.

A *dial-up modem* is a link that plugs into a standard telephone line. You dial a supplied phone number to connect to your ISP's server (using the given username and password for your user account), which then gives you access to the internet.

Cable Modem

A *cable modem* is a communication link that uses cable TV lines because they have greater *bandwidth* (the amount of data that can be transmitted in a fixed time) than telephone lines and so the *data transfer rates* that can be reached are much higher than those of telephone line-based modems.

ISDN (Integrated Services Digital Network) Line

ISDN is an international standard link that sends voice, video and data over digital or normal telephone lines.

ADSL (Asymmetric Digital Subscriber) Line

ADSL is a link that allows more data to be sent using existing copper telephone lines. This type of connection needs a special ADSL modem. *Asymmetric* refers to the rate at which data is sent and received, the received (downstream) data is more than the sent (upstream) data. *Digital* refers to the digital technology used to transfer data and *Subscriber* is the rental of a line from a provider like an ISP.

Phone Line ISDN Speed — 128 kbps

It is important to note that the faster the data transfer rate, the more throughput (data) can be processed. For example a standard modem transfers data at 56 kbps (kilobits per second) and a cable modem transfers data at 2 Mbps (megabits per second) — this means the web page (especially if it has lots of graphics) loads much faster. If you were downloading files, you might make use of other methods like file compression to improve data transfer rates.

Satellite Technology

The use of *satellite broadband* has enabled users (especially in remote locations) to make use of satellite technology to connect to TV, radio and now the internet. Typically you use an ordinary telephone line and a modem to send data, but use a satellite dish to receive data.

Mobile Devices

Mobile devices like mobile phones, *personal digital assistants* (*PDA*s) and laptop computers are another way that remote users can access the internet and other services. These devices make use of a wireless local area network which may use radio waves to send signals to the wireless devices or connect through a cellular phone network. Connection speeds vary and the connection quality also depends on the strength of the signal.

Wireless Connections

Wireless connections via mobile computing, is becoming increasingly popular and the technology is improving each year. Some networks are now run without any cables and make use of wireless connection devices in the PC and on the central server to transfer and connect to each other and the internet. Wireless technology can make use of a number of satellite technologies to connect, however they are still prone to disruption, for example due to positioning of satellites, sun spots or bad weather.

Most wireless connections still need line-of-sight to be able to connect, and in wireless networks a transceiver is installed for the signal to 'beam into' so it can be passed on to the next PC or the internet. Wireless hand-held devices such as mobile phones and PDAs make use of the *wireless application protocol* (*WAP*) to decide how to communicate and transfer data from the mobile devices over the internet.

You often hear mobile phone providers talking about WAP-enabled phones; this means they are using the wireless protocol to transfer data. When using wireless computers or mobile devices you can make use of wireless connections in a variety of public places like internet cafes, airports and even on trains. These types of connection points are often referred to as *hotspots*.

Note: Although it's not commonplace yet, it's also possible to use existing power lines to communicate. This requires a special modem, usually called a *home gateway* that connects to your home power supply and a special type of internet service provider.

Here's a rough guide to the current speeds available from each of these devices, although these are liable to change as technology advances.

Remember modem speeds are measured in *kbps* (*kilobits* per second) and *Mbps* (*megabits* per second). A *bit* is the smallest unit of data that computers recognise; a kilobit is 1,000 bits, and a megabit is 1,000,000 bits.

Device	Data Transfer Rate
Modem	56 kbps
Cable modem	512 kbps – 2 Mbps
ISDN	64 kbps
ADSL	1.5–9 Mbps (receiving data);16–640 kbps (sending data)
Satellite	16 kbps –2 Mbps (receiving data); 64 kbps – 1 Mbps (sending data)
Mobile phone	varies

File compression

A number of file compression utilities have been developed to enable file transfer to be as fast as possible. These allow the bandwidth to be used more efficiently and will speed up the transfer of data or software programs. There are a number of commercially available products. The two most popular are:

- *WinZip:* a file compression utility which is freely downloadable for use for a limited period to try. It compresses files and programs to make transfer faster. Most files have a .zip extension, eg sqa.zip.
- *Stuffit:* is a file decompression utility which unpacks or decompresses files sent via the web, or by e-mail. This will restore the file to its original size. These files normally have a file extension of .sit, eg sqa.sit.

Internet Service Providers (ISPs)

An ISP is a company that provides access to the internet. When you sign up with an ISP, they'll provide you with an account with its own username and password, and a telephone number that your communication device can use to connect to the internet, depending on which device you use (if you use a cable modem, for example, it's directly connected to the ISP's network and so you don't have to dial-up, your connection is always 'live').

They'll usually also give you a CD-ROM that will help you set up your internet connection, and a support telephone number you can use if you get stuck. Some ISPs also provide you with a small amount of web space that you can use for your own web pages if you want. The ISP will also keep a track of all of its authorised users for identification and billing purposes.

Many websites and internet service providers will record attempts you make to put in the correct user ID and password, and if you fail to put the password in correctly will lock your account until you have contacted them another way to verify your account credentials to them.

Most ISPs charge a monthly fee for their service, although some are free, and you'll usually have to pay a one-off installation fee for cable modems, ISDN lines and ADSL connections, and depending on where you live, some of these services may not be available. For example, cable modems are available only in areas that have been wired for cable TV.

If your connection uses a telephone line, you'll also have to pay for the calls you make when you connect to the internet. However, the telephone number supplied by your ISP will usually be a local or Freephone number to keep the call charges as low as possible, especially at off-peak times, although the charges will increase with the amount of time you spend online, just as they would if you made a long telephone call.

Examples of well-known ISPs are AOL, BT OpenWorld, Tiscali and Orange.

Typing Web Addresses

One way of displaying a website is to type its address (or URL) into the **Address** box in the browser window. To recap on web address structures:

- Each web page has an address that is unique on the web. Addresses will nearly always begin with **http://www.** followed by more letters, dots and slashes, though not always. You don't always need to remember the whole structure. For example, in most browsers you can start with **www.**

- When typing web addresses, it's important that you type it exactly as it should be — a single dot or letter in the wrong place will mean that the page you're looking for won't be found.

Using Hyperlinks

Hyperlinks allow you to move to another page or part of a page. These links might take the form of text or graphics that you can click once to move to the related part of the web. Hyperlinks are underlined to emphasise that they're links and may be displayed in a blue colour. It is quite a common mistake for users to double-click these links however a single click is the correct way to activate a hyperlink. When you move your mouse pointer to a hyperlink, it changes to a small hand shape, indicating the link. If the link to the web page is not available the pointer will change to a pointing hand with a no-entry sign. Web pages or links you have visited previously will normally be displayed in a different colour when you return to the originating page or search engine results pane. You will learn more about web addresses later on.

Internet Browser Software

Screen Elements

Every time you connect to the internet, your home page is displayed in the *application window*. The *home page* is the page that's been set to be your default page, ie the page that always opens first when you open your internet browser. This can be changed using **Internet Options** on the **Tools** menu.

PC Passport web page at http://www.sqa.org.uk/pcpassport

Note: Each website also has a home page. This is the main page of the site and will usually have hyperlinks to let you access the rest of the site.

Some of the screen elements can be switched on and off, so your screen may look slightly different from the illustration. For example if you wanted to display more search results in the browser window you might use the **View** menu to adjust the text size to gain more space in the window to ensure every search result was displayed in the window. You may even decide you do not need to display all the menus and run the screen in 'full screen' mode. From the View menu you can choose '**Full Screen**' mode which temporarily hides the menus and toolbars, so you can so you can gain more space in the window and display more results.

Browser navigation

As you explore the internet, your browser 'remembers' which pages you've visited and records these in different ways. For instance, you can re-visit pages that you've viewed this session using the **Back** button on the browser toolbar, and if you do, you can return to the pages you visited subsequently using the **Forward** button. Internet Explorer also records your visits using the **History** facility, which will be discussed later in this section.

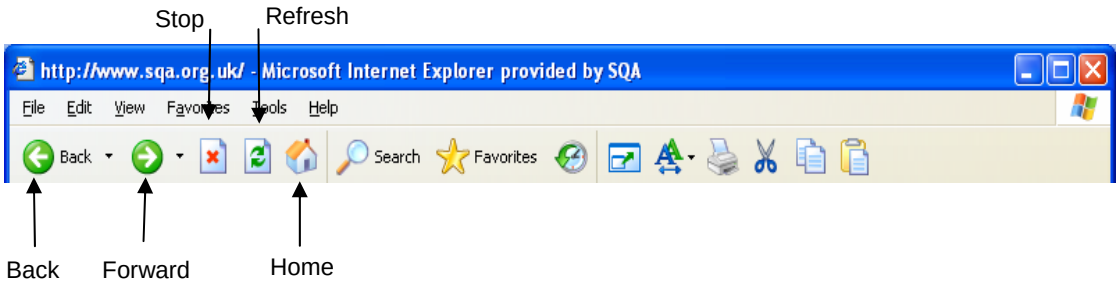
Using the Stop, Refresh and Home Buttons

These are buttons that appear on the toolbar beside the **Back** and **Forward** buttons.

The **Stop** button: If the page you've asked to see is taking too long to open, you can click **Stop** to cancel the request.

The **Refresh** button: This reloads the current page. You may want to do this if you get an error when trying to open the page, or to make sure you have the latest version of the page. The **[F5]** function key also refreshes the page.

The **Home** button: This button always displays the page that's been set as the home page on the computer you're using. This can be set to any page you like, or it can be set to a blank page.



There are also options in the **View** menu to allow you to change the text size to help people who might have difficulty reading text (or have poor eye sight) on a web page. Also by pressing **F11** or clicking on the full screen mode you can temporarily display the web page in full screen mode — useful if there is a lot of text and you want to see it all at once.

Exercise 1: Performing a simple search

1 Open up your web browser software and open up **www.google.co.uk**.

2 In the search box put in WinZip and find the link to the WinZip product page and read about what WinZip can do.

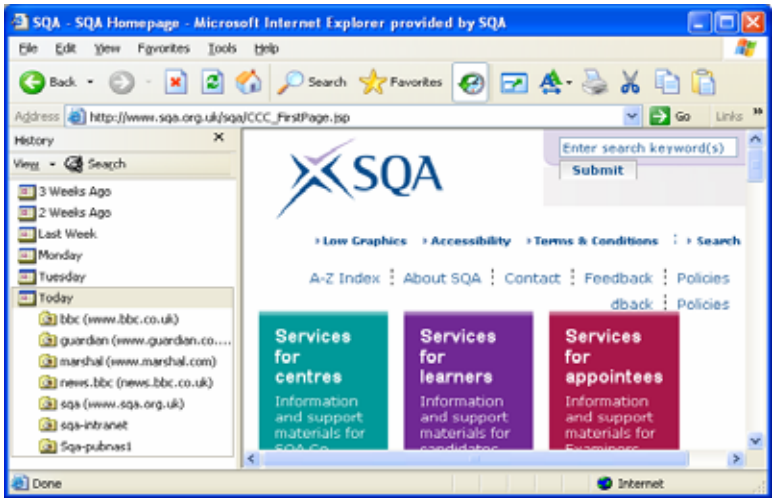
3 Now go back to **www.google.co.uk** and search for Stuffit and find the link to the product web page, read about what Stuffit can do. When finished close your web browser.

Using the History Facility

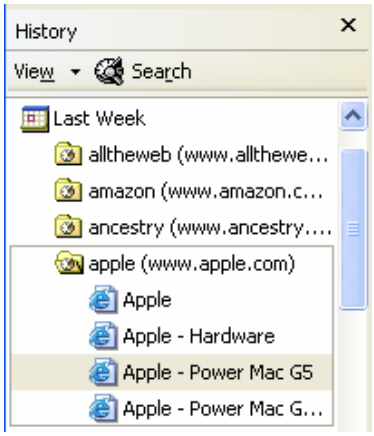
The History facility provided with Internet Explorer records the web pages you visited on the current day and a specified number of previous days. This can make it easier to find pages you've visited before.

To view the History recorded on your computer, click the **History** button on the Internet Explorer toolbar. This button looks like this:  .

This will display the History bar at the left of the window.



You can access pages from the History bar by clicking the entries in the bar. For instance, using the example below, to re-visit pages visited last week on the **www.apple.com** site, you would click **Last Week** then **apple** (**www.apple.com**) and then the page you want to view again.

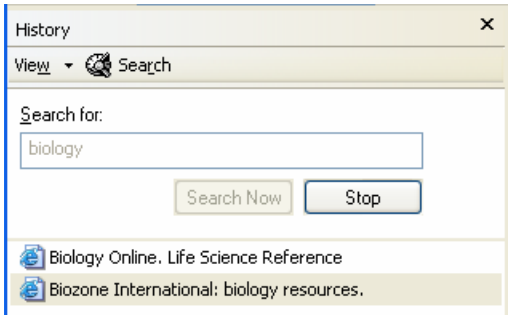


Sorting the History Log

Although the History log is initially sorted into the date the sites were visited, you can change this using the **View** button at the top of the list.

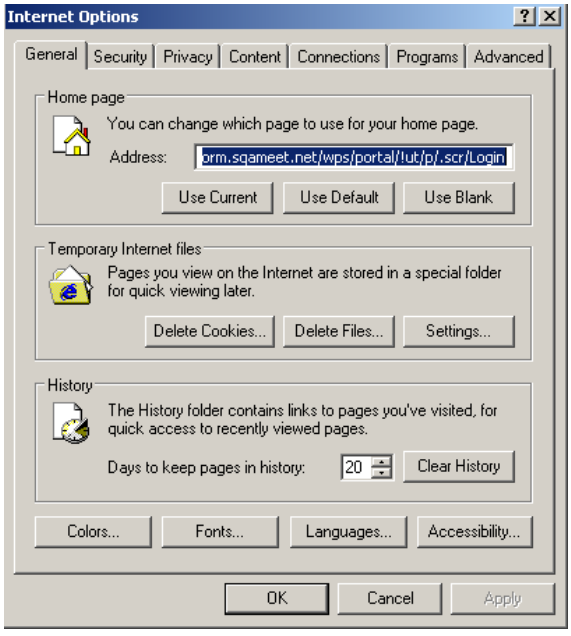
Searching the History Log

It's also possible to search your History log to find a site that you've visited during the History period. This search looked for the word 'biology' on any of the pages that were viewed recently:



Clearing the History Log

To empty the History folder, you need to go into **Tools**, **Options** and under the **General** tab, click **Clear History**. This will temporarily free up disk space on your computer.



Using the Favourites List

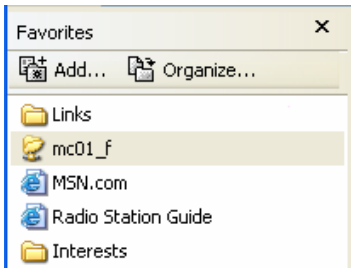
When you find a website you like and you want to keep a link to it you can add it to your *Favourites* list so that you can find it again quickly. When you want to visit the page again, you simply click it on the list. Sometimes the items on the list are called *bookmarks*. These bookmarks contain the URLs of websites or web pages you have visited. Within the Favourites menu you can decide to call the web link something more meaningful for you, but the browser will save the URL to know how to get back to the website. The name you give the bookmark and the associated bookmark, allow you to navigate back to the website or web page you bookmarked.

Viewing Pages from the Favourites List

To see the pages that you've added to the Favourites list, click the **Favourites** button on the Internet Explorer toolbar.

Adding Pages to the Favourites List

When you want to add the page that you're currently viewing to the Favourites list, display the **Favourites** list then click the **Add** button at the top of the list.



When you click this button, a small dialogue box will be displayed allowing you to change the way the page will appear on the list.

Making Pages Available Offline

To save on call costs, you can choose to make your Favourites available offline. This means you can view the pages even when you're not connected to the internet. When you choose this option, you then specify whether you want just the page you're adding to your Favourites, or the pages that it links to as well. You also choose how and when you want to refresh the offline content (this is called *synchronisation*).

To make the page that you're adding available offline, select the option in the **Add Favourite** dialogue box. When you do this, the **Customise** button becomes available. Click this button to start a series of dialogue boxes (called a *wizard*) that will help you set the options.

Organising the Favourites List

You can rearrange your Favourites list using the **Organise** button at the top of the list. Using this facility you can remove pages you no longer want to keep on the list, and rename those whose given names aren't suitable.

Exercise 2a: Browser controls

1 Open your internet web browser. We are using Microsoft Internet Explorer. For example, you might click the **Start** button and then **Internet Explorer**, or you may have to use a different method.

2 Examine the screen to familiarise yourself with the elements described on previous pages.

3 Click in the **Address** box to highlight the address that's already there.

When the address that's in the Address box is highlighted, it will look like this.

4 Now type **www.bbc.co.uk** and press **[Enter]**. The address you type here replaces the original address because you'd highlighted it first.

When you press [Enter] after typing an address, HTTP:// is added at the start if you didn't type it.

The BBC home page (the main page of the BBC site) is now displayed. On this screen, there are hyperlinks to take you to whatever part of the BBC website you're interested in. These include News, Sport, TV and Radio. When you point to these headings, the pointer changes to a small hand to show that you can click these parts of the screen to jump to the related area of the site.

5 Move the mouse pointer around the BBC home page and watch as it changes to a small hand when you point to the hyperlinks.

6 Click one of the hyperlinks to jump to an area of your choice and then explore that part of the website for a short while. Watch the **Address** box to see that the address changes as you move from page to page.

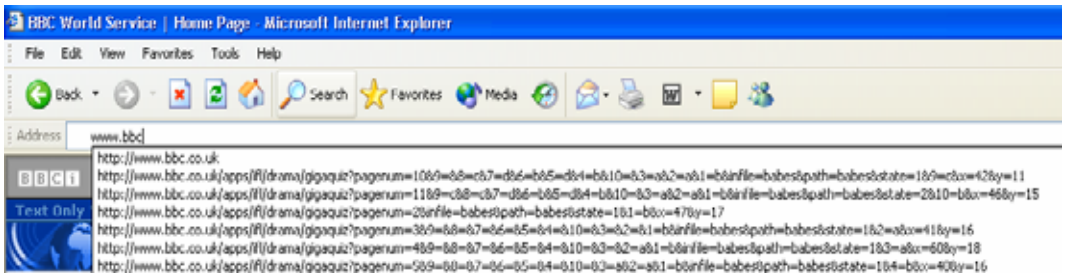
This is the address of the TV page that you can visit from the BBC home page.

For example, the BBC site has a series of pages relating to the schools' education system and exams. The illustration below shows the address for the BBC's Scottish Higher exam page.

7 When you have finished exploring, select the **File**, **Close** menu option. This means click the **File** menu and then the **Close** option. The browser window closes.

Exercise 2b: Re-visiting and saving web pages

1 Open your internet web browser again and go to the BBC website home page. Its address is **www.bbc.co.uk**. When you start typing the address in the **Address** box, the drop-down list opens to display addresses that you've previously visited that match what you've typed. You can finish typing the address yourself or, since you visited this page earlier, **click** it in the drop-down list.



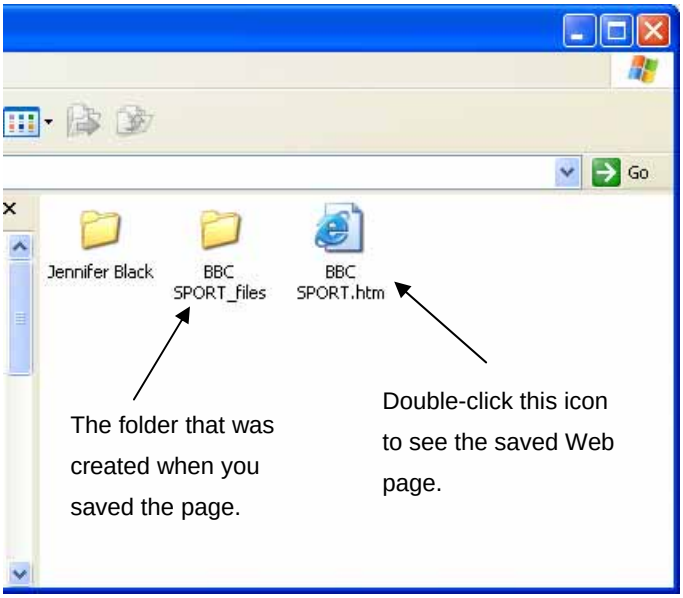
2 Click the **Sport** hyperlink to take you to the sport section of the website. Look at the **Address** box to see that the address of this page is **news.bbc.co.uk/sport**. If you wanted to visit this page in the future, you could simply type this address rather than opening the home page and clicking the link.

3 Follow the instructions below to save this page on your computer so that you can view it later without going online.

- Select the **File**, **Save As** menu option. If necessary, follow this procedure to save this page in your **PC Passport Student folder**.
- The web page title **BBC Sport** has been entered as the file name, so click the **Save** button to accept this name and save the page.

4 Open the Windows Explorer program and display the contents of your **PC Passport Student folder**.

5 Double-click the **BBC Sport** file. Notice that this file uses the Internet Explorer icon to show it's an HTML file. You can also see the **BBC Sport_files** folder that was created when you saved the page.



6 Click any of the links on the page and look at the **Address** box again. Although the Sports front page was taken from your computer, the links jump back to the website again.

In fact, if you rest your mouse pointer on any of the links, the **status bar** at the bottom of the window shows the name and file path of the page that will be displayed by that link:

7 Move your mouse pointer onto one or two of the links on the page that you're looking at then look at the status bar at the bottom of the window. The names won't always be in plain English as some websites will use codes and shortcuts in some of their page names.

The status bar at the bottom of the window shows what the link will display.

8 Close the browser window and the Windows Explorer program. Make sure you include your name and the date at the bottom of the file. Be sure to show the file to your tutor, or print a copy to keep in your portfolio of work.

Exercise 2c: Using history facilities

During this exercise, if any page you visit appears to be taking a long time to load, click the **Stop** button on the browser's toolbar and then click the **Refresh** button to try to reload it. You may have to type the page address again or click the link again. Print or save any pages that you're particularly interested in.

1 Open your internet web browser.

2 Visit the **Our Dynamic Earth** website by typing its address into the **Address** box and pressing **[Enter]**. The address is **http://www.dynamicearth.co.uk**.

3 Follow the instructions below to investigate this site using the links supplied on the site.

- Click the **Visitor information** link at the top of the Dynamic Earth page.
- Clikc the back button, then click the **Education** link at the top of the Dynamic Earth page.
- Read through this page and then click the **Downloads** link at the left of the page. You may have to use the scroll bar to see this link.
- Now click the **Back** button on the browser's toolbar to return to the Education page.
- Click **Back** again to return to the Dynamic Earth page.
  The **Forward** button is now available, giving you the option to return to the pages you already viewed.
- Click the arrow next to the **Forward** button to see this list of pages.
  There are two pages on the list and, because of the way the pages have been created, they're both listed as **Dynamic Earth** rather than **Visitor Information** and **Education**, although these are the pages that this list refers to.

- Click the **Home** link at the top of the page you are on.
- Investigate some of the other parts of the Dynamic Earth site.

4 Visit and explore the CIA's World Factbook site — you'll find lots of information about just about every country in the world!
Its address is **www.odci.gov/cia/publications/factbook**.

5 Visit and explore the Warner Brothers website (**www.warnerbros.com**) or the Fox Kids site (**www.foxkids.com**).

6 Return to your home page by clicking the **Home** button on your browser's toolbar.

7 Go to the **www.encyclopedia.com** site and find out what biology is then find out what is meant by marine biology.

8 Visit **www.scottishfa.co.uk** and find out which teams Scotland played in the qualifying rounds of the last football World Cup and what the scores were.

9 Use the **Back** and **Forward** buttons on the toolbar to return to some of the pages you've visited during this session. Close down you web browser.

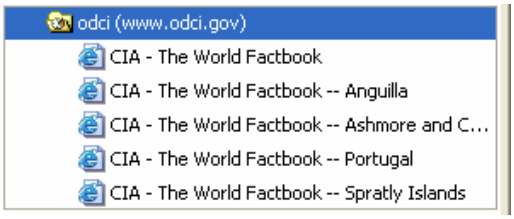
10 Open your web browser, then click the **History** button. This button looks like this:  .
When the **History** bar is displayed, the amount of information and the actual information shown will depend entirely on how your computer has been set up and how it's been used recently. You'll find therefore, that although some of the pages that appear on your list are the same pages as those in the illustrations in this exercise, you shouldn't expect yours to look exactly the same.

The History bar shows the pages you've visited today, although you could go back through any of the days or weeks shown on your list. You might have to click **Today** to see these pages.

11 Follow the instructions below to re-visit some of the pages you saw earlier.

- Click the **odci** (**www.odci.gov**) entry in the History bar to see a list of the pages you visited on that site (this was the site where you saw the CIA World Factbook).

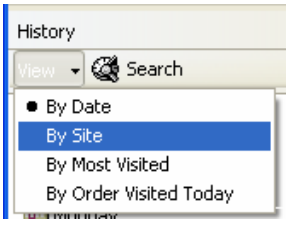
  This part of your History list will look something like this, but remember, since you visited pages of your choice on this site, it won't be exactly the same.



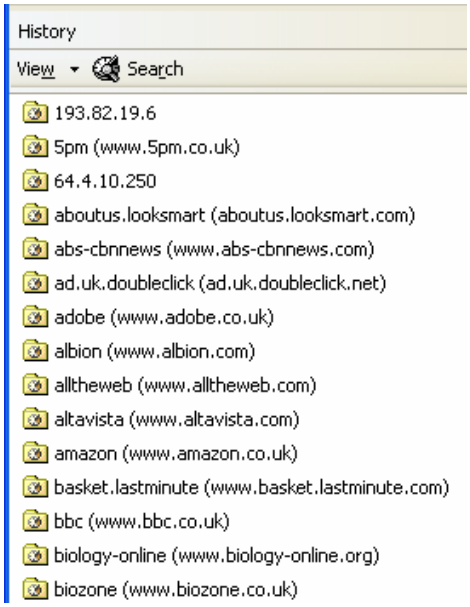
- Click the **CIA – The World Factbook** to view it again.
- Use the History list to view some of the pages you visited on the Fox Kids or Warner Brothers sites.
- Now re-visit the BBC Sport page you saw earlier.
- View any of the pages you're interested in seeing again.

12 Follow these steps to change the way the History list is shown.

- Click the **View** button at the top of the History list then click **By Site**:



The sites are no longer sorted by day, so all the sites that have been visited within the History list's time range are listed in alphabetical order of site name.



- Experiment with the other options on the View list then return to By Date.

13 Click the **History** button again to hide the History bar. Make sure you include your name and the date at the bottom of the file. Be sure to show the file to your tutor, or print a copy to keep in your portfolio of work.

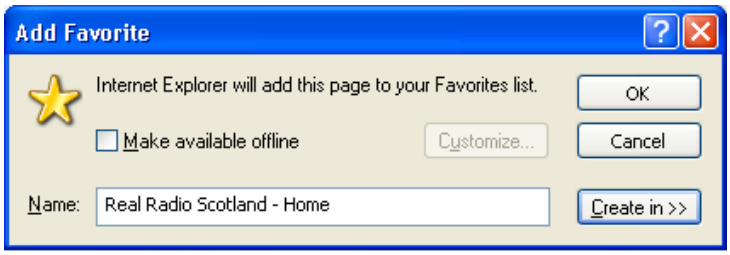
Exercise 2d: Creating bookmarks (favourites)

During this exercise, if any page you visit appears to be taking a long time to load, click the **Stop** button on the browser's toolbar and then click the **Refresh** button to try to reload it.

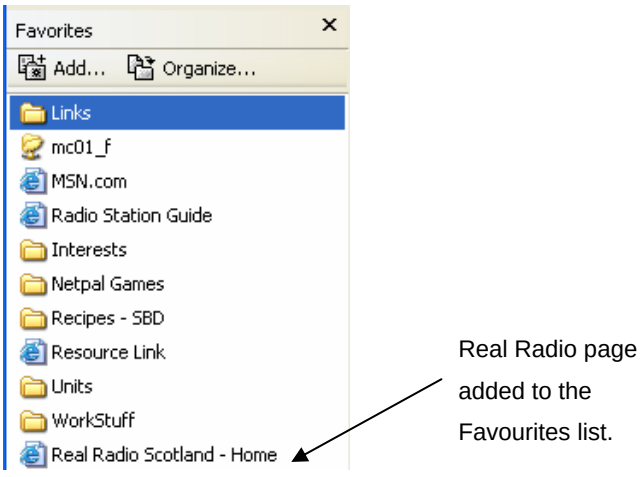
1 Ensure that your web browser is running then click the **Favourites** button.

2 Visit the Real Radio Scotland website. Its address is **www.realradiofm.com/Scotland**.

3 In the Favourites list, click the **Add** button.



4 Click **OK** to add this to your Favourites list with the name **Real Radio Scotland – Home.**



5 Add the BBC 1 page to your Favourites list. Its address is **www.bbc.co.uk/bbcone**

6 Follow these instructions to add another site and make it available offline.

- Add the Dynamic Earth site to your Favourites list. Its address is **www.dynamicearth.co.uk**
- Change the long name that's suggested to simply **Our Dynamic Earth**.
- Choose to make this page available offline. Click **OK** to add the page to the Favourites list. This may take a few moments to make it available offline.

  When you next go offline, use the Favourites list to access the Dynamic Earth site without connecting again to the internet.

7 Go to the BBC website and find the Bitesize page for Higher Grade revision and add this page to your Favourites.

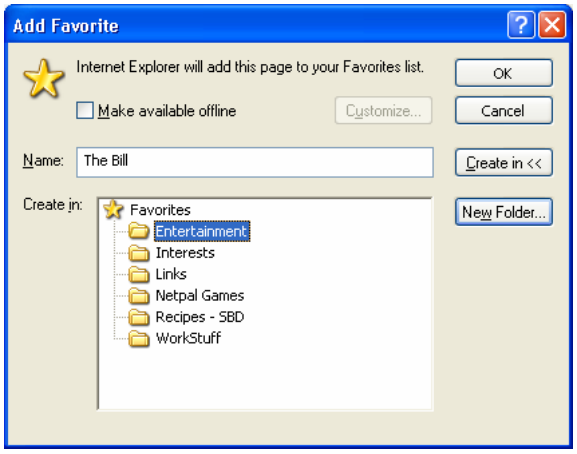
8 View the *The Bill* TV programme page then follow these steps to create a new folder in your Favourites list for it.

Hint: View the **www.itv.com** site and use the links there to find the 'mini-site' for this programme. There's a drop-down list on the ITV main page that will take you directly to the page you need.

- Click the **Add** button then click **Create in**.
- Next click the **New Folder** button and type the folder name **Entertainment**.

- Click **OK** to add this folder to the list shown in the dialogue box.

  Remember that the list of folders shown on your system will depend on how it's been used in the past.



- Make sure the **Entertainment** folder is highlighted then click **OK**.
- In the Favourites list, click the **Entertainment** folder to see that it contains **The Bill** link.

9 Follow the instructions below to organise some of the pages you've added to the Favourites list.

- The name given to the BBC Bitesize page is a little long, so now you'll rename it. First click the **Organise** link at the top of the Favourites list.
- Select the link to BBC Bitesize page (just now it reads **BBC – Education Scotland – Higher Bitesize**) then click the **Rename** button.
- Edit the page name so that it reads **BBC Bitesize – Higher** then press **[Enter]** to complete the edit.
- Rename the Real Radio entry as simply **Real Radio**.
- To move the Real Radio link to the **Entertainment** folder, first click the **Real Radio** link in the list then click the **Move to Folder** button.
- Use the **Create Folder** button to create a folder called **Revision** then move the **Bitesize** page to that folder.
- Close the **Organise Favourites** box.

10 In the Favourites list, click the **Entertainment** folder to see the contents then visit the Real Radio site.

11 Now visit the Bitesize page using the Favourites list.

12 View **The Bill** site using the Favourites list.

13 Create a folder called **Days Out** and move the **Our Dynamic Earth** link to this folder.

14 Add the site for the National Galleries of Scotland to the **Days Out** folder in your Favourites list. Make this site available offline without customising the synchronisation settings, and call it **National Galleries of Scotland** rather than the name it suggests.
The address for this site is **www.natgalscot.ac.uk**.

15 Close the Favourites list. Close your web browser. Make sure you include your name and the date at the bottom of the file. Be sure to show the file to your tutor, or print a copy to keep in your portfolio of work.

Saving a Web Page

- Select the **File**, **Save As** menu option, ie click the **File** menu and then the **Save As** option. The **Save Web Page** dialogue box will be displayed:
- Choose where the page is to be saved, eg on the desktop, or somewhere on **My Computer** by selecting an option from the **Save in** drop-down list. You can display this list by clicking anywhere on the box or the small arrow at the end of it.
- This is known as a *drop-down arrow* as clicking it displays a *drop-down list.*

Note: The **Places bar** at the left of the dialogue box can be used to quickly display the contents of the listed folders. Simply click the appropriate button.

Note: When you save a web page, the *file extension* **.htm** or .**html** (which, as you've seen, represents the language that web pages are written in) will be added to the name you supply so that it can be recognised as a web page. Depending on how your system has been set up and used in the past, you may see this extension in the dialogue box. If you don't see it, you don't have to add it — the system will do that for you.

You'll also find that when you save a web page, a new folder is created in the location where you save the web page. This folder will be given the file name you specified for the web page plus _**files**. So, for example, if you save a web page using the name **Personal Web Page** in the **Webs** folder, a new folder called **Personal Web Page Files** will also be created in the **Webs** folder.

Printing a Web Page

To print a web page, you would click the **Print** button on the toolbar. This will print one copy of the page to your default printer, ie the printer that has been identified as the one you will use unless you specify another at the time of printing.

It is important to check the **Print Preview** to see if your web page will print correctly — sometimes printed web pages can appear 'clipped' (word may be missing from the right-hand side). You may have to adjust the printer page settings to get all the web page printed.

To specify another printer, you would use the **File**, **Print** menu option that will display a dialogue box where you can specify non-default printing options.

Understanding the Structure of a Web Address

Each web page has an address that is unique on the web. Addresses will nearly always begin with **http://www.** followed by more letters, dots and slashes. You don't always need to remember the whole structure. For example, in most browsers you can start with **www.** The computer will automatically insert the protocol being used which is http://

Note: A web address is often referred to as the **URL**. This stands for **Uniform Resource Locator**.

A web address can give you information about the type and location of the site: for example, **.co** indicates a commercial organisation, while **.uk** indicates a UK-based site. So most website addresses for UK businesses end with **.co.uk**, while UK government sites end with **.gov.uk** and US government sites end with **.gov**. Other codes are shown below. These are a general guide, but not all sites using these codes adhere to their standard uses.

Site Types

gov	Government body	org	Non-profit making organisation
co	Commercial organisation (non-US)	com	Commercial organisation
ac	Academic (UK)	edu	Educational institution
mil	Military	net	Internet technical services

Countries

uk	United Kingdom	ca	Canada
au	Australia	de	Germany
fr	France	it	Italy
pl	Poland	sp	Spain

Note: If no country code is shown, the site is usually, but not always, a US-based site.

You can display a web page in any one of these ways:

- By entering an internet address or, if you've previously visited the page, by choosing it from a list.
- By browsing through pages, clicking links to move from one page to another.
- By using a search engine to retrieve pages on the topic of your choice.

Entering an Internet Address

You can either type the address into the **Address** box in the browser window or, if you're looking for a page you've looked at before, choose its address from the **Address** drop-down list. As you start to type an address, the list will show addresses you've visited before that match what you've typed. Remember that you can type the address starting with **www.** rather than starting with **HTTP://** The address bar in your web browser communicates the path followed by your computer to get to the web page or directory your browser is currently looking at — notice how it changes as you surf through a website.

Browsing

Web pages are designed with *hyperlinks* (or just *links*) to other pages on the site so that you can easily move around the site to find the information you need. You will also find that websites often contain links to other related sites, so this browsing can be a useful way of finding your way around the web. When you are 'surfing' the internet you may lose your connection and this can be frustrating if you had not been keeping a history log or bookmarking web links. Very often your web browser software keeps a *Temporary Internet Folder* which contains all the website files you have been accessing, you may find this useful if you want to re-visit or re-load pages you may have lost when your connection was lost.

It is important that you should periodically clear out this folder as it can cause your internet web browser to slow down after prolonged use (several weeks) because the Temporary Internet folder has become too big.

What is a Search Engine?

With a search engine you can enter *key words* relating to the topic you're interested in and the search engine will find information about sites containing those key words. With most search engines, you fill out a form with the key words you want to use then perform the search by clicking a button. The search engine then searches its database that holds information about all the websites it knows about. Any sites that the search engine finds will be listed for you, usually in order of relevance to your search.

It's important to learn to use search engines properly to get the best out of them and the internet. Each engine has rules about how to construct a search, but most also provide help on how to do this. This will be discussed in more detail next.

Using Search Engines

Many newcomers to the internet worry about how they are going to find the addresses of websites that might be of interest to them. There is no equivalent of a phone book for the internet — but with a little practice you will find it remarkably easy to find what you are looking for.

As mentioned before, you can use search engines to find information that you're looking for. This might be text, numbers or even graphics. If you have a broadband connection a typical search engine will search through 3 billion pages on the WWW in just seconds. However this can be slower during peak periods of activity like early evening when people get home from work and demand for access increases.

A search engine is a directory of millions of web pages that allows you to track down topics by typing in key words. With most search engines, you fill out a form with the key words you want to use then perform the search by clicking a button. Any sites that the search engine finds will be listed for you, usually in order of relevance to your search.

These are some of the most popular search engines and their web addresses:

Yahoo!	http://www.yahoo.co.uk
(kids version	http://www.yahooligans.com)
AltaVista	http://www.altavista.com
Excite	http://www.excite.com
Lycos	http://www.lycos.co.uk
Google	http://www.google.co.uk
The Internet Sleuth	http://www.isleuth.com
Infoseek	http://infoseek.go.com
Ask Jeeves	http://www.ask.co.uk
(kids version	http://www.ajkids.com)

This site gives you access to search engines from a single page: **http://www.allsearchengines.com**.

There are various ways of doing this which are related to the *search terms* — the words and phrases for your search — and how they are structured.

A search engine's help system will describe how that engine works and will often give you hints for better searching.

Most search engines ignore common words like, 'the', 'and', etc as they tend to slow down searches and do not necessarily improve the results. It's unlikely that all the results in the *hit list* will be relevant and you will have to go through them picking the best ones. As results are usually listed in order of relevance to your search, the first 20 or so results should cover what you're after. Sometimes the results will display hyperlinks as *cached*. This means that the hyperlink has been found previously by the search engine and a 'snapshot' has been taken and been cached in the search engine's server memory.

If they do not, you may want to revise your search by, for instance, using additional search terms or different words.

Using Key Words in a Search

Most search engines provide search instructions and advice that will make your searches more effective. These can usually be found under *Help* or *Search tips*. Following these suggestions should improve the effectiveness of your searches. Some engines will also show you more advanced search methods or criteria, such as how to narrow down your search if you receive too many hits by, for example, removing commonly used words from your search and replacing them with more specific terms, or enclosing specific words that must appear next to each other in quotation marks.

This may include specifying whether to search for the exact phrase, the file format eg HTML, words in the title of the resource and even perhaps the date, will all ensure the relevance and timeliness of the search.

There are two key decisions to be made when searching. The first is deciding the actual words (or search terms) that you'll use for your search. The second is to do with how you organise the words. These decisions can make the difference between finding lots of relevant information and not finding any.

When analysing the search criteria results (the web pages returned) hits can often be rejected based on the grounds of brevity, accuracy, clarity, depth, relevance or timeliness. For example, suppose you search for how to use BOOLEAN operators the results you get back might relate to BOOLEAN, Operators — this could include word processing operators, typists, machine operators etc.

If you had a rough idea of the URL you were looking for you could use an advanced page specific search. For example, you know that the Royal College of Nursing has a website starting www.rcn.org but you might not know all the web address — you could search using one of the search engines and it would return page specific results that are closest to your URL.

Using Common Operators in a Search

Using operators such as the + sign can help you make your search more specific. Standard ways of making your search more specific include those shown below. They are supported by most, but not all, the search engines. The + and - signs should be placed directly in front of each word, with a space between the end of that word and the next. These operators are referred to as Boolean operators and include AND, NOT, OR, XOR and NEAR). These Boolean operators are often used to link word or phrases in your keyword search.

For example, you search for Edinburgh AND Tattoo OR Festival NOT Book would return all occurrences of Edinburgh and include words related to Tattoo or Festival, but exclude words related to book. However because Tattoo has several meanings you might have to be more specific.

Operator	Example
+	**+Icon +Internet +Books** will find pages containing all the words, together in any order, or separately. A '+' in front of a word makes it mandatory that it is present. Some search engines use the operator **AND** instead of a '+'.
-	**+Icon –Internet +Books** will find pages that contain **Icon** and **Books**, together in any order, or separately, but will exclude pages that include the word **Internet**. Some search engines use the operator **NOT** instead of a '-'.
"…"	"**Icon Internet Books**" will find pages that contain the whole phrase, with the words in that order.
* ?	You can also make use of a range of search 'wildcards' search for characters. This will allow you to bring back pages which match the wildcard character. The use of the wildcard was to enable easy searching for words with more than one ending with a star "*", as in a search for "run*" to designate "run", "runners", "running", etc. Modern search engines are able to search with more sophistication now.
Occurrences, Exact phrases, Dates, Time etc	If you are searching for a specific title, phrase or occurrence of word in a title, page or article, you can use advanced search criteria to specify where you would like the search engine to look for the search criteria and in what part of the web page it should look at. This will help narrow down searches to clearly defined parameters.

Further Tips on Searching

Read the instructions at each search site. The way you perform a search can vary quite a bit from engine to engine.

- Include synonyms or alternate spellings in your search statements.
- Check your spelling.
- Use the correct mix of upper and lowercase letters if the search engine is case sensitive (uppercase = capital letters; lowercase = small letters). This will refine the search.
- If your results are not satisfactory, repeat the search using alternative terms.
- If you have too few results:
  - drop off the least important words to broaden your search
  - use more general wording
  - experiment with different search engines. No two search engines work from the same index.

- Try search engines that allow you to search multiple search engines simultaneously. Copernic is an example of this type of engine. You can download Copernic free of charge from its website. The address is **www.copernic.com**.

If you want to search for images on the internet, you can use special facilities provided by some of the search engines. For instance, using Google or AltaVista you enter key words but click the **Images** tab above the search box before searching. Yahoo also has a facility for finding images using the page: **http://dir.yahoo.com/arts/visual_arts/**

Search String Examples

String	Result
"chart music" –Britney	will find pages relating to **chart music**, but not if they include **Britney**
Justin Timberlake	will find pages containing either the word **Justin** or the word **Timberlake** or both
"Justin Timberlake" OR "The Darkness"	will find pages containing either the phrase **Justin Timberlake** *or* the phrase **The Darkness**
"Justin Timberlake" AND "The Darkness"	will find pages containing both the phrase **Justin Timberlake** *and* the phrase **The Darkness**
country house hotels	will find pages containing the words **country**, **house** *and* **hotels** (in some search engines, this is the same as putting a '+' in front of each word)
country house hotels –"St Andrews"	will find pages containing the words **country**, **house** *and* **hotels** *unless* they also include the phrase **St Andrews**
"St Andrews" +golf	will find pages containing the phrase **St Andrews** *and* the word **golf**
"St Andrews" NEAR golf	will find pages containing the phrase **St Andrews** *and* the word **golf** in close *proximity*
"St Andrews" OR Gleneagles +golf	will find pages containing either the phrase **St Andrews** or the word **Gleneagles** *and* the word **golf**
"St Andrews" OR Gleneagles –golf	will find pages containing the phrase **St Andrews** *or* the word **Gleneagles** *but not* if they contain the word **golf**

Meta-Search Engines

In a meta-search engine, you submit keywords in its search box, and it transmits your search simultaneously to several individual search engines and their databases of web pages. Within a few seconds, you get back results from all the search engines queried. Meta-search engines provide a quick way of finding out which engines are retrieving the best results for you and are useful when searching for obscure topics.

Ask Jeeves — prepares answers to common questions asked in natural language. Natural language is using plain English to express a query to a search engine. Meta search engines are better for general queries than for finding specific information. They are very easy to use but results are not ranked according to relevancy so the results should be checked carefully.

Dogpile — searches the web, Usenet, download sites, stock quotes, news and weather. Dogpile searches three databases at a time and then provides options allowing you to select further databases to search. You can limit the amount of time you are prepared to wait for results. Results are grouped by site and organised from the most specific to the most general.

Hotbot — provides a good collection of features in a single, easy-to-use interface. Sites are frequently re-indexed so Hotbot can provide more updated sites than many search engines. Its flexible search interface can limit searches by date, domain, or media and it has some unique search features, including sorting results by date or media type.

Ixquick — very fast and comprehensive, searching 14 engines. Results are ranked by relevancy, and if a page is listed by more than one search engine it shows how it was ranked in each case. Ixquick allows natural language searches, advanced Boolean searches, and knows which engines can cope with different types of searches.

Meta IQ — searches 10 of the top search engines at one time, or you can select individual engines (automatically selects five to start). Results are returned in one long easy-to-read list.

Structured Directories and Gateways

Information is gathered by user input (they rely on a user typing in information about a resource) and usually the user specifies the category to which the resource belongs and relevant keywords. These resources tend to be more accurate, because of the human intervention, but are less comprehensive because of the lack of automation. Structured directories usually deliver a higher quality of content and fewer results out of context than search engines.

EINet Galaxy — entitled 'the professional's guide to a world of information', Einet Galaxy, like Yahoo!, offers the user elaborate search facilities across a broad range of topics, covering everything from geoscience to philosophy. The presentation is not quite as clear as Yahoo!, but there is a great deal of useful information listed here.

GeniusFind — categorises thousands of topic-specific search engines and databases.

WWW Virtual Library — the oldest catalogue of the web, providing one of the highest-quality guides to subject-specific information gateways. The WWW Virtual Library is a large text-based collection of databases of online resources on several hundred topics, from general subjects to very specialised sites. Selecting a category gives access to relevant web links, and with recommended or new sites indicated.

Subject gateways have been created to offer organised and categorised access to particular subjects or topics. Whilst they may produce a more relevant search result, this may not be as extensive as that from a search engine and it may not be as up-to-date. Library gateways point to research and reference information that has been reviewed and evaluated by subject specialists. Use library gateways when you are looking for high-quality information sites.

ADAM — Gateway to resources in art, design and architecture.

Biz/ed — Business Education on the internet.

BUBL — A general resource for the Higher Education community.

Exercise 3a: Simple Search

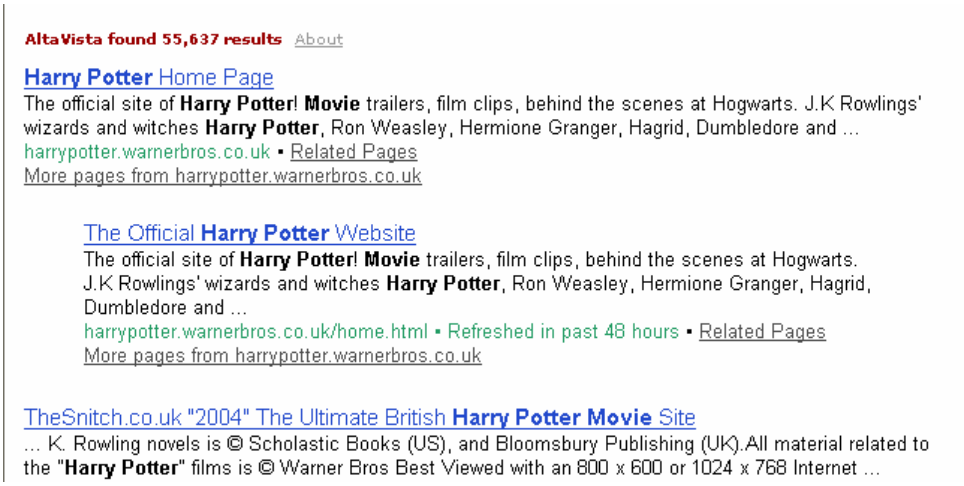
1 Ensure that your internet web browser software is open then type **www.altavista.co.uk** in the **Address** box and then click **Go**.

Note: When you do this exercise you may find that the visual appearance of the site has changed from that shown in the activity's illustrations, as websites are constantly updated and improved. You may also find that the sites returned by your search are different from those shown here.

2 Enter **harry potter movie** into the search box, then press **[Enter]** or click **Find**.

A list of sites that match your search enquiry is displayed. These may be called documents, hits or matches. As the sites on the web are constantly changing, the list you get may vary from that illustrated on the following page.

3 These sites contain all three words **harry**, **potter** and **movie** although not necessarily all together or in that order. Click one of the hits to view the website.


AltaVista found 55,637 results About

Harry Potter Home Page
The official site of Harry Potter! Movie trailers, film clips, behind the scenes at Hogwarts. J.K Rowlings' wizards and witches Harry Potter, Ron Weasley, Hermione Granger, Hagrid, Dumbledore and ...
harrypotter.warnerbros.co.uk • Related Pages
More pages from harrypotter.warnerbros.co.uk

The Official Harry Potter Website
The official site of Harry Potter! Movie trailers, film clips, behind the scenes at Hogwarts. J.K Rowlings' wizards and witches Harry Potter, Ron Weasley, Hermione Granger, Hagrid, Dumbledore and ...
harrypotter.warnerbros.co.uk/home.html • Refreshed in past 48 hours • Related Pages
More pages from harrypotter.warnerbros.co.uk

TheSnitch.co.uk "2004" The Ultimate British Harry Potter Movie Site
... K. Rowling novels is © Scholastic Books (US), and Bloomsbury Publishing (UK).All material related to the "Harry Potter" films is © Warner Bros Best Viewed with an 800 x 600 or 1024 x 768 Internet ...

4 Use the **Back** button on the toolbar to return to the page of search results.

5 Display the next page of search results — there will be link to other pages at the bottom of the current list:


Results Pages: 1 2 3 4 5 6 7 8 9 10 Next >> back to top

6 Go to one of the sites listed on this page and then return to the search results page using the **Back** button.

7 Search for **the beatles** and investigate one or two of the sites that are listed.

8 Return to AltaVista's main page.

Exercise 3b: Complex search

1 Try searching for each of the phrases below and compare the search results.

2 "**sunshine holidays**" — only sites that contain this complete phrase are listed.

3 **sunshine NEAR holidays** — sites that contain both words within 10 words of each other.

4 **holidays –sunshine** — Sites that contain holidays but not if they contain the word sunshine.

5 Use the **www.google.co.uk** search engine to find information on your favourite pastimes.

6 Follow the instructions below to search Google for various images.

7 Display the Google home page at **www.google.co.uk**

8 Click **Images** above the box and type **aberdeen** in the search box.

9 Press **[Enter]** to perform the search. A number of images are returned.

10 Search for information about the Hard Rock Café and find the closest branch to you.

Exercise 3c: Meta and Directory Searches

1 Display the **Dogpile** metasearch engine then search for information about the pastime you researched at step 5 in Exercise 3b. Compare the results with those you got earlier.
The website address is **www.dogpile.com**.

2 Try the same search using the Mamma metasearch engine, comparing the hits returned with those returned by Dogpile. Mamma's address is **www.mamma.com**.

3 Visit this directory search engine at **http://timeanddate.com**. It contains information for several other search engines. Find out the following:

- Under Current time, look in The World Clock — Time Zones.
- Under Calendar, look up the calendar for the UK for 2010.
- Under Other Planning tools, look up International Dialling codes.

4 Using the WWW Virtual Library at http://vlib.org. Look up the following section:

- Communications and Media — Telecommunications.
- Open the Resources and Issues sub-library, then Other sources.
- Under Other Sources, use the structured directory to go to Internet Tools and Search engines. Save the result in your favourites list.

5 When you've finished, close your web browser. Make sure you include your name and the date at the bottom of the file. Be sure to show the file to your tutor, or print a copy to keep in your portfolio of work.

Copyright

You should remember to check whether material that you find on the internet is subject to copyright laws and act accordingly when using any material or images you find there. There are Acts that you must be aware of when accessing content on the internet.

The Computer Misuse Act

The Computer Misuse Act is used to protect people from hackers, who steal your information, use viruses to corrupt your computer or commit criminal acts, through identity theft. This Act of Parliament covers three broad categories and offences:

1 The unauthorised access to computer materials — this includes using someone else's password to gain access to their computer files and carries a six month jail sentence or fine.

2 The unauthorised access to computer materials, with intent — this is where there is intent to commit criminal acts with the data, or use the data in a criminal way. This carries up to five years in jail and a large fine. It covers areas like identity theft of your personal details and using them for other purposes.

3 The unauthorised modification to computer materials — this includes many viruses which change your desktop, delete files or impair the operation of a computer. This is the most serious offence and carries a five year jail sentence and a very large fine. The impact on a business in this area can be catastrophic with loss of business, time for systems to be repaired and loss of confidence by the public. For example, what would happen if all your results were lost because the school system had been hacked.

To see the full Act go to:

http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Copyright, Designs and Patents Act

Important! Just because images, clip art and multimedia files are available on the web doesn't mean that you have the right to download or copy them — they may be copyrighted. Check the site thoroughly for a copyright statement. If in doubt, do not download or use the file. You should also consider acknowledging the source of the data. Notice how you had to sign a service agreement on the Microsoft Clip Art site to download clip art.

Whenever you decide to create any type of document with graphics included it is important before you use any graphics, images, video clips or files that you check you are not infringing the copyright of that object. Copyright laws exist to protect the people who created the object and their permission must be sought before you can use any piece of text, reference material, image, clip art or video clip in your presentation.

The Copyright, Designs and Patents Act 1988 gives the creators of literary, dramatic, musical and artistic works the right to control the ways in which their material may be used. The rights cover: broadcast and public performance, copying, adapting, issuing, renting and lending copies to the public. In many cases, the creator will also have the right to be identified as the author and to object to distortions of their work.

Copyright arises when an individual or organisation creates a work, and applies to a work if it is regarded as original and exhibits a degree of labour, skill or judgement.

Interpretation is related to the independent creation rather than the idea behind the creation. For example, your idea for a book would not itself be protected, but the actual content of a book you write would be.

In other words, someone else is still entitled to write their own book around the same idea, provided they do not directly copy or adapt yours to do so. Names, titles, short phrases and colours are not generally considered unique or substantial enough to be covered, but a creation such as a logo that combines these elements may be.

Types of work covered

1 Literary

Song lyrics, manuscripts, manuals, computer programs, commercial documents, leaflets, newsletters and articles, etc.

2 Dramatic

Plays, dance, etc.

3 Musical

Recordings and score.

4 Artistic

Photography, painting, architecture, technical drawings/diagrams, maps, logos, etc.

5 Typographical arrangement of published editions

Magazines, periodicals, etc.

6 Sound recordings

May be recordings of works, eg musical and literary.

7 Films

Broadcasts and cable programmes.

Copyright Notices

It is strongly recommended that you include one on your work, it will:

- announce that copyright exists in the work
- make it clear who is the owner
- deter infringement.

By having a copyright notice you are helping to prevent infringement occurring. For more information on the current Copyright and Patents Act refer to the appendix at the end of this pack or go to:
http://www.copyrightservice.co.uk/copyright/uk_law_summary

Online Communications

Instant Messaging

Instant messaging (or *IM*) allows you to use your computer to have a private 'chat' with one or more users of your choice. This means that you can 'chat' to your friends or colleagues as if they were in the same room or on the telephone.

There are a number of programs that you can use to chat with, such as Microsoft Windows Messenger, or Yahoo! Messenger. As well as sending text messages, some of these programs also allow you to use video and voice messaging if you have the right equipment (a webcam and a microphone). Microsoft Windows Messenger is provided as part of the Windows program, and the other programs can be downloaded from the internet free of charge. Just click the link on the provider's page and follow the instructions.

Signing Up for Instant Messaging

How you do this depends on the provider whose program you use. If you use a Microsoft messaging program, for example, you need a Microsoft Passport account to sign into the program. If you use Yahoo's messaging program, you need a Yahoo! account to use the software. The people you want to chat with will usually have to have the same software as you.

Using Instant Messaging

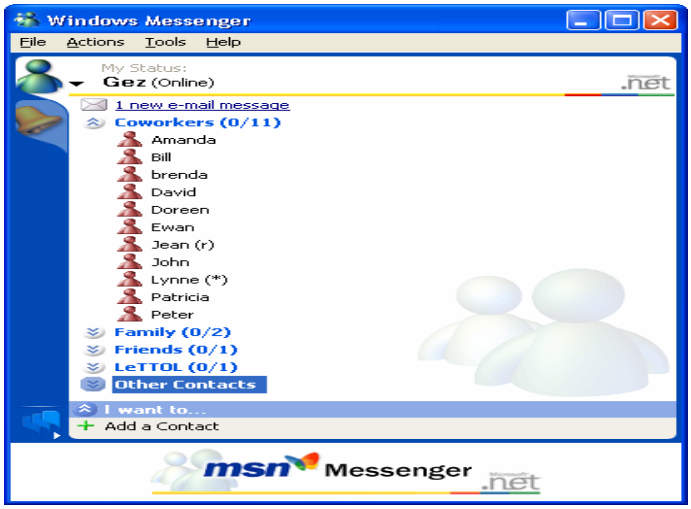
First start the messaging program then sign in using the name and password you created when you signed up. Once you have signed in, you'll see a list of the people you can chat with (called *contacts* or sometimes *buddies*).

To begin a chat with one of your contacts, double-click their name and then type your message in the window that appears.

When you press **[Enter]** your message is sent to them and is displayed in a similar window on their computer. In this way, you can exchange messages with one another, inviting others to join your conversation if you want.

Note: Each program has a menu option that lets you add people to your contact list as long as they allow it. Use the Help system in your messaging program to find out more about this.

This is a sample of the Microsoft Windows Messenger program.



Chat Rooms

The chat facility offered by many ISPs allows real-time communication between two or more users in *chat rooms*, usually dedicated to a particular topic. You will have to have an account with the provider or a separate 'chat' account that gives you a *nickname* for use in the chat rooms.

Safety in Chat Rooms

Since anyone can create an account giving details which may or may not be true, it's important that you are aware of the rules and guidelines that will help you use chat rooms safely. Each provider will usually have a list of these guidelines online so that you can access them whenever you need to.

Remember: Use chat rooms and instant messaging safely and wisely and be cautious of giving out personal details.

Signing Up for a Chat Account

This process is similar to signing up for an e-mail account, but usually much shorter. You provide the nickname you'd like to use and an e-mail address where the provider can send your password. Once you've received your password, you use that and your nickname to log in.

Using Chat Rooms

Once you've logged into chat, you'll usually be presented with a list of the rooms that are available, perhaps with some additional information highlighting particular categories of chat room, such as those for specific interests like gardening, music etc. You simply click the room you want to join and then you'll be shown a window where the conversation that's currently taking place in that room will be displayed. To join in, just type your message and press the **[Enter]** key.

Chat Shorthand and Emoticons

You'll find that experienced chatters use shorthand of their own to cut down on the amount of typing they have to do.

Note: Some chat providers now use graphics as emoticons (☺ ☹) rather than character combinations.

You can use many different types of emoticons, see some of these at:

http://www.smiley.smileycentral.com

Internet Netiquette

Netiquette is short for *internet etiquette* and refers to a system of rules relating to the use of the internet in general and with specific rules relating to use of e-mail, chat rooms and newsgroups.

Some newsgroups and chat rooms are moderated, ie a real person oversees the discussion in a chat room or judges a message's suitability for the target newsgroup before allowing it to appear there. This is used in situations where, for example, children are the target audience of the room or group. Below is a brief overview of the rules.

Overview

- **Don't type in block capitals:** This is taken as shouting.
- **Remember that other people online are human too:** Don't say anything online that you wouldn't say to someone's face; remember your manners, be polite; don't use bad language.
- **Respect the law:** Breaking the law is bad netiquette.
- **Know where you are online:** Make sure you're in the correct chat room or newsgroup for the topic you want to discuss. Posting a message on the wrong topic often ends up with other users sending e-mail (often nasty) to the 'offender'. This is called *flaming* — which itself is bad netiquette and can cause users to be banned from a chat room or group.
  Most sites have their own additional netiquette, which will often be found in their *FAQ (Frequently Asked Questions)* section.
- **Be brief and simple:** Keep your discussions to the point and don't waffle. Use simple fonts and little or no formatting — other users may not have the same systems as you, so the effect could be lost anyway. Make sure that what you contribute is clear and precise and that you know what you're talking about.
- **Help others:** If you're an expert in a particular area, help other users who ask questions online.
- **Have patience with new users** (*newbies*) — you were new once too.

Newsgroups

Newsgroups, also known as *forums* and sometimes as simply *groups* or *e-groups*, are online discussion groups. The discussion group can either be private (access is strictly controlled by the group's moderator or owner) or public (access is freely available to any person wishing to access the group's topic or thread). *Mailing lists* operate in exactly the same way as forums. People are invited to join a mailing list, which can be private (closed — only available to specific people like friends and family) or open (freely available to everyone on the internet). You might have a personal mailing list used by friends and family to organise events, or be part of a commercial mailing list for notification of new products or services.

The moderator has an important role.

- They control who has access, and ensure members are aware of the forum guidelines.
- They check that the posts sent by members are appropriate. For example suppose someone who had very little IT experience posted a question about setting up their home printer and another member sent a reply post giving very technical specifications about printers to the group. This post would be too technical and is not really relevant to the subject matter — 'How to setup a printer' so the moderator would probably reject this technical post as inappropriate.
- They ensure posts from members are not repetitive or contain offensive language.
- They ensure posts are not too familiar — or the language is inappropriate for the topic.

Newsgroups differ from chat rooms in that they are not real-time. One user posts a message then others reply to it in their own time.

Each of the many thousands of newsgroups relates to a particular topic or theme. For example, there are newsgroups for music lovers in general, each individual genre of music, and for specific performers.

You can access newsgroups either through a provider's site, much in the same way as chat, or using a *newsreader* program like Microsoft Outlook or Microsoft Outlook Express.

Here you'll see how to access the groups via the provider's site. Remember that the way that the screens look will vary depending on your provider, but the features work in a similar way.

Signing Up for a Newsgroup Account

This process is similar to signing up for a chat account. You provide the nickname you'd like to use and an e-mail address where the provider can send your password. Once you've received your password, you use that and your nickname to log in.

Viewing Newsgroups

Once you've logged into newsgroups, you'll usually be presented with a list of the groups that are available, perhaps with some additional information highlighting particular categories of group, such as those for painting or for music lovers.

Joining a Newsgroup

Once you find a newsgroup you'd like to take part in, you usually have to join or subscribe to it if you want to contribute to the discussion, although you can often read the messages without joining. You can join a group by means of a button or link on the newsgroup's 'home' page. Once joined to your group, there will be various group page navigation options which will vary but may allow you to access a database of other members, poll members on topics, store files or folders, use chat and calendar facilities or simply post messages.

Reading Messages

To read a message posted in a newsgroup, click its title. When the message opens, you'll see that it looks much like an e-mail message. The screen will have buttons or links that allow you to work with the message. For example, to reply to a message or forward it to an e-mail address, as well as navigation links to move around the messages posted in the same group.

Replying to and Forwarding Messages

Replying to and forwarding others' messages is similar to working with e-mail. To answer a message that you've read, you click the **Reply** link from that message and type your answer. To forward a message (if this is available on the newsgroup you're using), click the **Forward** link then address the message and send as usual.

Posting New Messages

Newsgroup messages are arranged in *threads*, another word for *topics*. To add a new thread to a newsgroup, you click a link that reads **New**, or **Post New Topic** or something similar. In the example illustrated above, you would click **Post** to start a new thread. Then simply type your message and post it to the group.

Wikis

A *wiki* is a special website that allows visitors to add, remove, edit and change content. You do not need to register to do this. A wiki will link many pages together and often has a wiki engine (software) to allow this process to happen. The wiki has become a very powerful tool for finding out information about a topic and the best known example is Wikipedia which is an online encyclopaedia containing millions of pages about different things. Look up the section on wikis at: http://en.wikipedia.org/wiki/Wiki.

Blogs

A *blog* ('web log') is a form of online journal that allows text, images and video clips (and links to websites) to be displayed as a webpage but also allows comments to be posted by readers of the blog.

Some blogs ask you to register with the site first before allowing you to post anything. There can be moderation of posts as with forums but that is determined by the owner/administrator.

Blogs will often contain information about a particular topic like food, politics or local news. A blog will contain text, images and links to other blogs, forums or other web pages related to the blog topic. There are over 57 million blogs in the world today.

More information about the different types of blogs can be found at: http://en.wikipedia.org/wiki/Blog

Podcasts

A *podcast* is a media file available from the internet to download for play back on a range of portable media players like MP3 players, iPods, etc. It uses *web syndication feeds* (content supplied by companies for people to listen to eg BBC news podcasts).

A podcast can be a mixture of audio or video or both, which can be downloaded from a website for listening to on your portable device. Podcasts are not done in real-time. They are recorded and can be downloaded from the web feed internet site and listened to whenever you wish.

If you subscribe to a web feed site like iTunes, you can get the site to automatically send you podcasts. More information about podcasts can be found at: http://en.wikipedia.org/wiki/Podcast.

Mobile phones

Mobile phones are used by lots of people today to talk, send text messages, take and send pictures, listen to music, or surf the internet. In fact you can do so much with a mobile phone it can be a complete communication tool.

There are many different types of mobile phone and it is important to understand some of the basic terminology you will see in mobile phone adverts. The terminology tells you what features the mobile phone has and what it can be used for. When you see *3G* or *4G* it simply means '3rd generation' or '4th generation' of mobile communications and often relates to the service the phone provides like speed for transferring text, video, data, internet access etc. Many mobile phones have colour screens, the ability to send and receive text, pictures or even video. Most new phones can also play music and have additional features like internet access.

Bluetooth is a specification for wireless communication for data and voice between mobile phones. It specifies how mobile phones talk to each other. Any Bluetooth-enabled device can talk to another Bluetooth-enabled device up to a range of about 30 feet. To use a mobile phone you need to subscribe to a service provider. There are many to choose from including Vodafone, O2, Orange, Virgin etc.

Each provider will give you the option to have a *contract* phone where you pay a monthly fee, or a *pay-as-you-go* phone, when you pay for the phone and then buy top-up cards with credit on them to use in your phone.

Every mobile phone contains a *Subscriber Identity Module* (*SIM*) card. This card is inserted inside the phone and identifies the user account on the subscribed network. It authenticates the user and provides some data storage.

The *Short Message Service* (*SMS*) allows text messages up to 1260 characters long to be sent and received via your subscriber service. If the phone you are sending the text message to is out of range or turned off, the service provider will store the text message until it can be delivered.

PDA

PDAs (*personal digital assistants*) are hand-held computer devices that can perform a number of different things, like receiving e-mails, sending messages, writing text (in a word processor). Newer PDAs are also telephone devices, receiving both audio and video. A PDA connects either through a local telephone network, or a local intranet or an internet connection.

The *Wireless Application Protocol* (*WAP*) is a set of communication standards for accessing online services through your mobile phone or PDA. There are many different types of mobile phone and PDA, each one has its own set of features.

E-commerce and E-retailing

E-commerce is one of the fastest growing areas of the internet. It is the conducting of business, communication and transactions over the internet, over networks or via computers of any kind including wireless, cabled, hand-held devices and now even mobile phones. E-commerce includes:

- **E-retailing** — online shops selling a variety of goods like http://www.play.com for example which sells DVDs, CDs, games, electronic goods etc. When setting up an e-retail website an important consideration is how to 'load' balance the use of your web server(s), to ensure customers can access and buy products from you. You may have dedicated servers that handle credit card transactions, another for handling product selection and another perhaps for delivery — say for example something like Sainsbury's or ASDA online shopping. It is important that you maximise the availability and reliability of all your servers. This can be achieved by ensuring correct load balancing procedures are in place to ensure a consistent service for customers. (Load balancing is distributing processing and communications activity evenly across a computer network, so that no single server is overwhelmed.)

- **E-business** — banks who allow customers to view their accounts online, insurance companies, like http://directline.com who sell all kinds of insurance for the home, car, pets etc.
- **E-government** — **local government and national government** departments such as the Scottish Government, providing up-to-date information about recent legislation, surveys and developments. Try looking up the Scottish Government at http://www.scotland.gov.uk/Home or the Houses of Parliament at http://www.parliament.uk/.
- **E-marketing — companies advertising products** by sending e-mail messages to millions of people. You can often see this as unsolicited e-mail spam messages in your inbox of your e-mail program, or as pop-ups when you view some web pages.

All of these areas of e-commerce require that the service they provide is efficient, reliable and available 24 hours a day, 7 days a week — the internet does not shut down after normal work in over — people shop anytime and anywhere on the internet. Ensuring your systems are reliable ensures customers will come back and shop again. For example, many companies find that as more people access their web servers the website responds more slowly because of slow internet speeds. This has cost implications as it may require them to upgrade the processor or memory of the server to cope with increased demand.

E-commerce and e-business are still emerging technologies and people are often reluctant or deterred from using these facilities for a number of reasons:

- Constant virus threats and fear of these being spread to your computer when accessing websites
- Fear of supplying credit card details in case of credit card fraud
- Fear that the website owners will release your personal details to others
- Fear that the goods will not be delivered or will be faulty and that you will have no re-dress against the supplier because you bought it online.

Online forms

Almost all types of e-commerce will ask you to fill out some type of online form. Whether is for purchasing something from an online store to registering to receive information, the online form has become a way of internet life. It is important when filling out an online form that you understand why you are filling out the form. Here are points to remember:

1 Is the form required to make a purchase, if so what kind of security does it have for making payments? Does it use a secure method to transfer credit card details?

2 Does the form ask for more personal details than it needs to complete the transaction? For example, does it ask about your interests and hobbies? These could be used to market information to you.

3 Does the form allow you to opt-out of receiving information from them about their products or supplying your details to other third party companies? Sometimes it is a very small tick box at the bottom of the form.

4 Does the form state clearly its purpose, are there terms and conditions listed, or that you have to accept before completing the online transaction?

5 Has the form come through your e-mail, or is it on the website you are looking at. If the form has come as an e-mail attachment, it might not be a real form, but some form of hacking, to get personal information about you.

Remember, information you supply online can be used for malicious purposes, so always protect yourself, by ensuring only the minimal amount of information required is supplied. Never volunteer extra information.

Internet Telephony

Internet telephony is hardware and software that enables people to use the internet as the transmission medium for telephone calls. For users who have internet access through an ISP, internet telephony software provides free telephone calls anywhere in the world. It is not quite as good as direct telephone connections because you are reliant on your internet connection.

There are many internet telephony applications available. Internet telephony products are sometimes called *IP telephony, Voice over the Internet (VOI) or Voice over IP (VOIP)* products and protocols. VoIP phones can integrate with other services available over the internet, including video conversation, message or data file exchange in parallel with the conversation, audio conferencing, managing address books and passing information about whether others (eg friends or colleagues) are available online to interested parties.

Skype is a peer-to-peer internet telephony network. Skype allows users to call other users from their computers and communicate via microphone, as well as call and be called from regular phones.

Picture sharing

Sharing pictures and photos online has become very popular and there are numerous sites which allow you to upload, manage and share your photo images with other members.

Most will require you to create an account with them and fill out an online registration form. Look at this one from Snapfish.
http://www.snapfish.co.uk/registration

Almost all online providers will give you some disk space to store your images, which you can upload from your computer, your mobile phone or your digital camera.

There are normally editing facilities within the online website, or you can use your own, like Adobe Photoshop to manipulate, change, improve and enhance your photos and images.

Other sites include: www.Smugmug.com, http://www.webshots.com/ and http://www.kodakgallery.com

Exercise 4: Using Online Communication Tools

1 Go to the internet and find out about the online communication tools you have read about so far, eg instant messaging, newsgroups or forums, internet telephony, blogs, wikis or picture sharing. Bookmark the websites you visit to gather the information. Show your tutor which sites you visited.

2 Fill out at least one online form (your tutor will advise you on the best one). Keep a copy of the form offline or print a copy to show your tutor.

3 Write a short report (no more than 500 words) on one of the methods. The report should describe its features and the suitability of its use.

4 Make sure you include your name and the date at the bottom of the report. Be sure to show the file to your tutor, or print a copy to keep in your portfolio of work.

Regulation of Investigatory Powers Act

With technology moving forward at a faster pace, governments are only just beginning to catch up with legislation to monitor and ensure that people's rights are clearly upheld. One of a range of Acts concerning people's rights is the UK Regulation of Investigatory Powers Act of 2000. This Act was brought about because of the growth in electronic communication across the world and the way it is increasing used for criminal purposes. We have all heard about theft of identity — where your personal data is used by someone else for fraudulent purposes such as credit card misuse.

This Act replaced an earlier Act from 1985 which gave certain powers to law enforcement bodies (police and security agencies etc) to intercept or view communication if they suspected a felony or act of terrorism was taking place especially if the data was encrypted. In summary it covered:

- the interception of communications like e-mail and phone calls
- intrusive surveillance (on residential premises/in private vehicles)
- covert surveillance in the course of specific operations

- the use of covert human intelligence sources (agents, informants, undercover officers)
- the acquisition of communications data (eg billing data)
- access to encrypted data or other network traffic.

For each of these powers, the Bill will ensure that the law clearly covers:

- the purposes for which they may be used
- which authorities can use the powers
- who should authorise each use of the power
- the use that can be made of the material gained
- independent judicial oversight
- a means of redress for the individual.

This Bill has implications for all e-mail sent from a company for example, or even e-mails you might send from your own home computer. Under the Act employers can monitor e-mail and internet use by employees, to ensure that no viruses are being sent and that only appropriate websites are accessed, ensuring sensitive data is kept secure. ISPs must also maintain a reasonable intercept capability to allow security agencies to intercept electronic communications if national security is threatened.

If your company has an IT use policy it should take into account any Acts like the two mentioned here.

For more details about Acts or Parliament look at the following web link: http://www.parliament.the-stationery-office.co.uk/pa/cm199900/cmbills/064/2000064.htm

Using E-mail

You can keep in touch with friends, family and business contacts using e-mail, sending and receiving messages almost instantaneously, where in the past you might have sent a letter, a memo, or made a phone call.

E-mail messages can contain any mixture of text and graphics that you want to send. The typical size of a short e-mail is between 1–10 kb.

It is also good practice (when using a slow connection like a dial-up modem) that you construct longer e-mails offline in a text editor, so you do not waste valuable connection time writing the e-mail. You can also attach files to the message that are stored on your system so that the recipient can view or work with the same information as you. You might, for example, send family photographs to a friend, or you might have to send a monthly budget spreadsheet to your boss, or your homework to your teacher. E-mail is a cost effective way of communicating, because you are only paying the cost of your ISP account but you could be e-mailing anyone around the world. For the cost of a 'local call' (the cost for you to connect to your ISP) you could be e-mailing someone in Australia or the USA.

You may already have an e-mail account — you will usually have an account set up when you open your own ISP account and often employers and schools provide their employees and students with e-mail addresses for their own use. If this is the case, you may use a non-internet based e-mail program. Almost all e-mail systems require you to have a *user name* (log-in ID) and a *password* to access your account. Otherwise, you can sign up for an internet e-mail account. Whilst your ISP might keep a database of all of its subscribers and their e-mail account details there is no central directory of global e-mail addresses. This is because people do not want to be listed centrally in case of spam or virus e-mails from unknown sources.

Non-internet E-mail Programs

If you use an e-mail account that is not internet-based, you will likely use a program such as Microsoft Outlook, Novell GroupWise or Lotus Notes to read and write e-mails. To use one of these programs, you run it in the same way as you run any other program, by choosing it from the Start menu or by double-clicking its icon on the desktop.

Once you run the program, you use it the same way as you use internet e-mail which is described on the following pages (although you don't have to log in since your program will already be set to look at your account).

If you already have software that can be used on your PC, you may have to set-up a number of things. These include:

- Your account details and identity you will use. This normally takes the form of an e-mail address supplied by your ISP.
- The protocol, you will use, to connect to your e-mail provider (ISP). This is normally the *Post Office Protocol* called *POP3*, which defines how your e-mail will be delivered.
- Any security settings for protecting your e-mail account.

The type of e-mail extensions you will allow like *Multipurpose Internet Mail Extensions* (*MIME*). The MIME standard is recognised by most browsers and e-mail programs and enables the automatic recognition of many files types. MIME is the standard for sending and receiving non-ASCII files (like graphics, sound files, spreadsheets etc) as attachments to e-mail messages. If your e-mail software account stops working, you can often still use the details in a web browser (in an internet café for example) or perhaps add your e-mail details to a friend's e-mail account set-up.

If you don't have an account already, for example if you use a computer in a public learning centre or cyber café, you can sign up for a free account on the internet.

Signing Up for an Internet E-mail Account

First you have to find a site that has this facility. Some sites that provide this service include:

Orange www.orange.co.uk

Yahoo! **www.yahoo.com**

Hotmail **www.hotmail.com**

Next you click the link that will allow you to sign up for a new account. On the Orange site, for example, this is a link that reads **Sign up for free e-mail!** which appears under the log-in boxes for existing users.

One of the advantages of this type of e-mail account is the fact that you can check your e-mail from any computer with internet access, anywhere in the world. Many businesses also set up their e-mail accounts so that they can be accessed over the internet so that workers can use the system from home or when they're away on business.

After you've clicked the link to create an account you'll be asked to supply some personal details. Some of these you'll have to supply and some will be optional, depending on the e-mail provider.

Note: Bearing in mind the need to be careful when revealing personal details on the internet, you might want to consider carefully the optional information you supply here.

As each provider's signing-up process differs slightly, only general instructions can be given here. However, each provider will give on-screen instructions as you complete the process.

Once you have signed up, you'll be shown a screen confirming your new e-mail address and will usually be shown a link that will display your *inbox* — the folder where your incoming messages are stored.

E-mail Addresses

All e-mail addresses follow the same format:

yourname@something.something
or:

yourname@something.something.something

As with web addresses, you have to type the e-mail address exactly as it should be or your message will not reach its intended recipient.

Logging into Your E-mail Account

When you create your account, you specify a password that you use to access your e-mail. This prevents anyone who doesn't know your password from reading your messages or sending them on your behalf without your knowledge.

There are various laws (Computer Misuse Act 1990 and the Regulation of Investigatory Powers Act 2000) that restrict the viewing of e-mails (especially in the workplace, by your employers) to protect and ensure your human rights are not being violated.

The logging-in process (sometimes referred to as *signing in*) is usually the same regardless of your internet e-mail provider. You type your username and password then click a button to log in. Your username will usually be your full e-mail address, or it may be just the part before the @ sign.

Once you've logged in, you'll usually be shown your inbox (or a link to it) so that you can see any messages that are there. Messages that haven't been read yet are shown with an envelope icon; a paperclip on a message indicates that a file is attached to the message.

Links to other e-mail folders that make up your *mailbox* are usually shown on this screen too.

Other providers may arrange the window slightly differently, but they all have more or less the same parts

Reading E-mail Messages

In your inbox, you can see who the sender of each message is and, if the sender has added a subject, what the message is about as well as the date and time the message was received.

To read a message, simply click it. You can click any part of the message that is underlined to show that it's a link.

Replying to E-mail Messages

If you need to answer a message that you receive, simply click the **Reply** button shown when the message is open and type your message. The message will be automatically addressed to the person who sent the original to you. When you're ready, click the **Send** button.

Note: If you are one of a number of recipients of a message, you can send your reply to the sender and the other recipients by clicking **Reply All** instead of **Reply**. You can see who the original message was sent to by looking at the message header information.

Forwarding E-mail Messages

If you receive a message that may be of interest to other people, you can send a copy of the message to them. To do this, click the **Forward** button shown when the message is open. Next, address the message by typing the e-mail addresses you want to send the message to into the **To** box and add any additional message you want to include. Finally, click **Send**.

Deleting E-mail Messages

You will usually have a limited amount of space for storing your e-mail, although the exact amount will depend on the provider you use. This means that you should remove messages you no longer need. You do this by selecting the message and clicking **Delete** or, if the message is open, clicking the **Delete** button shown in the message window.

Usually, messages that you delete will be placed in a **Deleted Mail** folder so that you can retrieve them if necessary, although this folder may have a different name. The messages will be permanently deleted when you select to empty the **Deleted Mail** folder; until then, these messages count towards your space limits.

Writing E-mail Messages

When you want to send a message, click the **Write Mail** tab in the e-mail window. Sometimes this is shown as a simple link and it may be named *Compose Mail* or *New*, or something similar. When you click **Write Mail**, a new blank e-mail form will be displayed. You simply complete this form and then send the message. Here's an overview of each of the message parts:

To, Cc, and Bcc: These fields should be filled with the names of the recipients of the message. The main recipients' addresses should be typed in the **To** box, with those the message should be copied to in the **Cc** box.

Any addresses you enter into the **Bcc** box will be hidden from other message recipients.

Note: The Address Book that's available on most internet e-mail systems can usually be used for adding addresses to these fields, although the method of adding the addresses of your contacts to the Address Book can differ from system to system. Use the Help link on your e-mail page to find out the details of your Address Book.

Subject: As you saw earlier, the subject appears in the message list when a user logs into their e-mail, so it can be important that you choose the subject carefully. If the recipient isn't interested in the subject of the message, they may not even open it.

Attach: This link is used to attach files that you have on your system to the message. For example, family photographs or documents which need to be reviewed. When you attach a graphic as an attachment, it is also usually shown within the message.

You are able to customise how your e-mail text will look by using the formatting options in your e-mail program These include text, size, style,colour, bullets and numbering, indenting, spelling and grammar checking.

Mailing Lists and Address books

You may have different types of mailing lists that you would use, for example:

- A personal mailing list which includes address book entries of family and friends. This is useful if you want to share personal information, or organise things like parties or special events for a family member. This mailing list would be a *closed* type of mailing list as it is restricted to those people you have included and no others. This is also true if you were creating an online group or using instant messaging.
- A business or commercial mailing list might include address book entries of people you do business with and you want to inform them of new products or prices.
- Lists can either be a *closed* (restricted to your known clients) or *open* (an open list means that anyone may join) and also applies if it was an online group you had created. People who join may be those who have accessed your website and have asked to be informed of new products by supplying their e-mail address details.
- Specific groups that you can create to send out a monthly e-mail or newsletter. This type of mailing list would be a closed list, which you might have made up from both your personal or business mailing lists, or from individual people in your address book.

Attaching Files

No matter which provider you use, there will be a link or a button that allows you to attach files from your system to your messages. When you click this link or button, you'll be given the chance to locate the file you want to attach.

You may need to use compression if your attachments are too large to travel over your e-mail link and if you receive a compressed file you may need tools like WinZip to decompress the attachment before you can read it.

Note: When you send other users a file as an attachment, they must have a program that's capable of opening the file. For example, if you send someone a Microsoft Word document, they must have either Microsoft Word on their computer or a program that can open Word files.

Note: When you send, reply to or forward a message, a copy is normally saved in the **Sent Mail** folder (this may be named slightly differently, eg **Sent Items**) provided for this purpose. Most providers allow you to choose whether or not to keep copies of sent messages. To save storage space, this option could be switched off when it's not needed. Copies of messages kept in this folder count towards your storage limits.

Notice that the folder for putting unwanted messages could go into a number of differently named folders for example:

- Trash can — is the US English version of a waste bin or recycle folder for files you no longer want.
- The junk e-mail folder can be for junk mail, or spam mail (if you decided that is where you want this type of mail to go).
- In a standard e-mail program like Outlook Express you might put your junk e-mail, re-direct your spam mail or even trash e-mails into the deleted folder.

It is also important to make sure you create folders for saving your e-mails to. This might include one for personal use and one for business, or one for order confirmations about shopping you have done online. Your e-mail program will allow you to create folders for storing your e-mails to make them easier for you to find them.

Signatures

If you are sending an e-mail you may want to add a signature. This can be either a personal signature, like your first name and e-mail address or a more formal one which gives your full name, job title, work and mobile phone numbers and your work e-mail address.

Signatures can often be set up using the Tools menu in your e-mail program. You can have several different types of signature and you can have every e-mail automatically assign your signature to the bottom of your e-mail before it goes out of your e-mail program.

Your e-mail program will have many features to allow you to send e-mails. You might be able to set priorities on your e-mails, so important ones go first, or you may wish to ensure they can only be read by certain people, so you can encrypt the contents of the e-mail. You may want to add in a web link to a specific website.

Dealing with unwanted or malicious e-mail

Viruses

A *virus* is a piece of computer code that attaches itself to a program or file so it can spread from computer to computer, infecting as it travels. Viruses can damage your software, your hardware, and your files. Often found in programs which require you to 'boot' your computer (re-start your computer), these programs can be located on a portable disk drive, downloaded from the internet or even sent as an e-mail attachment. Viruses cannot spread unless you open or run an infected program. Always make sure you get your programs from trusted sources.

A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or information. Just as human viruses range in severity from Ebola to the 24-hour flu, computer viruses range from the mildly annoying to the downright destructive. The good news is that a true virus does not spread without human action to move it along, such as sharing a file or sending an e-mail.

A *worm virus* is designed to copy itself from one computer to another, but it does so by taking control of features on the computer that can transport files or information. Once you have a worm in your system it can travel alone. The great danger of worms is their ability to replicate in great volume.

For example, a worm could send out copies of itself to everyone listed in your e-mail address book. When new worms are unleashed, they spread very quickly, clogging networks and possibly making you wait twice as long for you (and everyone else) to view web pages on the internet.

A worm can consume memory or network bandwidth, thus causing a computer to stop responding. Because worms don't need to travel via a 'host' program or file, they can also tunnel into your system and allow somebody else to take control of your computer remotely. Recent examples of worms included the Sasser worm and the Blaster worm.

Just as the mythological Trojan horse appeared to be a gift, but turned out to contain Greek soldiers who overtook the city of Troy, today's *Trojan horses* are computer programs that appear to be useful software, but instead they compromise your security and cause a lot of damage. A recent Trojan horse came in the form of an e-mail that included attachments claiming to be Microsoft security updates, but turned out to be viruses that attempted to disable anti-virus and firewall software.

Trojan horses spread when people are lured into opening a program because they think it comes from a legitimate source. Trojan horses can also be included in software that you download for free. Never download software from a source that you don't trust.

The Spread of Viruses

Viruses and many worms cannot spread unless you open or run an infected program. Many of the most dangerous viruses were primarily spread through e-mail attachments (the files that are sent along with an e-mail message). The virus is launched when you open the file attachment (usually by double-clicking the attachment icon).

Tip: Never open anything that is attached to an e-mail unless you were expecting the attachment *and* you know the exact contents of that file.

If you receive an e-mail with an attachment from someone you don't know you should delete it immediately. Unfortunately, you're no longer safe opening attachments from people you do know. Viruses and worms have the ability to steal the information out of e-mail programs and send themselves to everyone listed in your address book. So, if you get an e-mail from someone with a message you don't understand or a file you weren't expecting, always contact the person and confirm the contents of the attachment before you open it.

Other viruses can spread through programs you download from the internet or from virus-ridden computer disks that you borrow from friends or even buy in a store. When you 'boot' from these computer disks, they overwrite your operating system or insert malicious code.

These are less common ways to contract a virus. Most people get viruses from opening and running unknown e-mail attachments.

Infected PC

When you open and run an infected program, you might not know you've contracted a virus. Your computer may slow down, stop responding, or crash and restart every few minutes. Sometimes a virus will attack the files you need to start up a computer. In this case, you might press the power button and find yourself staring at a blank screen.

All of these symptoms are common signs that your computer has a virus although they could also be caused by hardware or software problems that have nothing to do with having a virus.

Beware of messages warning you that you sent e-mail that contained a virus. This may mean that the virus has listed your e-mail address as the sender of a tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses. You might hear this referred to as *spoofing*.

Unless you have up-to-date anti-virus software installed on your computer, there is no sure way to know if you have a virus or not. There are a range of companies supplying anti-virus software for businesses and home users alike.

Junk (Spam) Mail

These are all types of *e-mail abuse*; that is, abuse of the e-mail system. They differ from abuse on the e-mail system (eg stalking, sexual harassment) in that they endanger the usability of electronic mail as a communications medium.

- *UBE* stands for 'unsolicited bulk e-mail' and is an e-mail message that is unsolicited (ie it wasn't explicitly requested by the recipient) *and* bulk or broadcast (ie substantively identical messages were sent to a non-trivial number of recipients).

Most of the junk e-mail messages that arrive in your e-mail box every day are UBE. UBE isn't necessarily advertising, and e-mailed advertising is not necessarily UBE (advertising isn't UBE if you request it, but most UBE is advertising). It comes in many forms:

- Political — politicians love to make direct contact with the electorate. Many of them will see UBE as an ideal medium for this.
- Charitable — the world's worthiest causes need our help. Many charities don't understand the issues surrounding bulk e-mail and might think it would be okay to send UBE requesting donations.
- Religious — people have found the internet to be an ideal medium to send others information on a religious viewpoint and use UBE to reach a large number of potential converts.
- *UCE* — stands for 'unsolicited commercial e-mail' and is often used as an alternative to UBE. Which term you prefer is largely a matter of style. UCE is easier to prove than UBE — it's easier for one individual to see if an e-mail is commercial in nature than to see if it is sent in bulk — but UCE doesn't necessarily endanger the e-mail system if it isn't UBE.

As a spam-victim, you will probably be in no place to judge whether a suspected spam you received really was sent in bulk, as you'll only get one copy of the spam yourself. For the most part, this doesn't matter, as you can make a good guess based upon what it looks like and whether you solicited anything like it. Unsolicited advertising is rarely sent individually.

Many *spammers* (senders of spam) try to equate junk e-mail with junk postal mail. However, there are several important differences:

- Junk postal mail is free to the recipient, whilst junk e-mail must be paid for by the recipient. (Many people pay per-minute for internet access, and spam means more mail to retrieve, which means more time online. Also, many ISPs have had to install extra capacity and employ extra staff in order to cope with spam, the money for which is raised by increased subscription charges for the subscribers.)
- Junk postal mail won't stop your legitimate mail from being delivered. However, many people still have limited sizes (quotas) of e-mail boxes; the more spam that they receive the less space there is for legitimate e-mail. And if their e-mail box is full of spam, any legitimate e-mail sent to them will be lost.
- Junk e-mail can also cause loss of legitimate e-mail by overloading mail servers.
- Junk postal mail scales, because there is a significant cost for sending each individual junk mail, ie the cost of printing, the cost of the paper, the cost of postage, the cost of the envelope-stuffer to put everything together. This forces the junk mailer to send only to a relatively small number of people — it simply isn't economical to send mailshots to everyone in the country. In contrast, junk e-mail is nearly free for the sender, which means that it doesn't scale. There's nothing to discourage every business in the world from sending spam to every person in the world.

Spam may also form a *denial of service attack* (*DOS*) if it is sent in sufficient quantity. It can cause legitimate e-mail to be lost as mailboxes fill with spam, can cause the network to slow down, and can even crash mail servers. This may be a crime where you live. (Note that 'denial of service attack' has the same acronym as 'disk operating system' and the two should not be confused as they mean different things.) Spam which forges header information to appear as if it's from another entity can be illegal in your country, and it is in this area that most successful court actions have thus far taken place. Yahoo! for example, won a well-publicised court case against spammers who had forged 'yahoo.com' in their spams.

Dealing with Spam (Junk) E-mail

There are various ways of dealing with spam or junk mail that comes into your e-mail program:

- You could e-mail the company that sent you the mail and ask to be removed from their list. However this may cause more problems if it was forged header information in the spam mail. You may just be confirming to the spammer that you have a valid and active e-mail address.
- You could set-up rules within your e-mail program that automatically remove spam mail straight into the junk or deleted folder. You run the risk of also sending valid mail into the junk folder if your rules are too strict.
- You could ask your ISP to set-up server side rules that are applied to your inbox even before the e-mail is delivered, but again you may risk losing valid e-mails if the rules are too strict.

It is most likely that you will use combinations of these methods to ensure spam and junk e-mails are kept to a minimum. Sometimes looking at the e-mail header information can give you clues about the sender.

E-mail Headers

An e-mail message is divided into two parts, the *headers* and the *body*. The headers contain all the technical information, such as who the sender and recipient are, and what systems it has passed through. The body contains the actual message text. The headers and body are separated by a blank line. In some mail programs, the headers are shown separately.

Most programs have an option that will display all the headers of the message. Another technique is to read your e-mail with a standard text editor as opposed to an e-mail program. Check the docs that come with your e-mail reader or read the online help. You could also contact your ISP for assistance or talk to your help desk if this takes place at work. You'll know that you're viewing the headers when you see several lines that start with the word 'Received'. These lines are very important in tracking the source of a spam.

To find them in various e-mail programs look in:

Elm, Pine, and Mutt
Press ‘h’ from the message selection menu to view the full headers of the currently selected message.

Eudora
Open the message. Under the title bar are four options. The second from the left is a box which says ‘Blah, Blah, Blah.’ Click on that to display the full headers.

Hotmail
Go into **Options**, **Preferences**, and choose **Message headers**. You’ll want to choose the **Full** option to display Received: headers. **Advanced** will display that as well as MIME headers.

Lotus Notes 4.6.x

Open the offending mail. Click on **Actions**, then **Delivery information**. Cut and paste the text from the bottom box, marked **Delivery information**.

Netscape Mail
Choose **Options** from the options menu bar. Listed as an option is **Show Headers.** Choose **full headers**.

Outlook Express
Open the message. Choose **File** from the options menu bar. Listed as an option is **Properties**. Another window will open, showing two tabs. You want to choose the one titled **Details**. Then cut and paste the headers into the message you want to forward.

Outlook 2000
Double-click on the message to open it, click on **View**, **Options**, and you will see the message headers in a box at the bottom of the window. You can copy and paste them from that window.

Pegasus
Choose **READER** from the options menu bar. Listed as an option is: **Show all Headers**. This does not work for HTML messages, however. A workaround is to select the message properties, and de-select **Contains HTML data**.

Phishing

Phishing is where people who e-mail pretend to be from a company or bank and they ask you to confirm your username and password or even to supply credit card details. This type of e-mail should be **DELETED** immediately. The information you supply can be used to charge money to your credit card or even take out a loan in your name. It is fraud and there are laws protecting you against this. Common companies targeted are eBay and PayPal.

E-mail Spoofing

E-mail *spoofing* is when a user receives an e-mail that appears to have come from a known source (a friend or a business associate), but it was actually sent from another source. Spoofing is often used to try and trick the user into giving out sensitive information. For example you get an e-mail message from your bank asking to provide your bank account details because they had a problem with their computers.

These e-mails will seem real and people often respond but they are giving away valuable information, do not be fooled.

Computer software called *spyware* can often be installed without your knowledge to intercept or take partial control over your interaction with the computer, without your consent.

Spyware secretly monitors the user's behaviour and can collect various types of personal information, but can also interfere with the user's control of their computer in other ways, such as installing additional software, redirecting web browser activity, or diverting advertising revenue to a third party. Running anti-spyware software is also recommended.

Employers Acceptable Use Policy

Most employers and public sector organisations have adopted an acceptable use policy with regard to using IT and sending e-mail. It is common practice to expect employees to read and sign an AUP when they start working for an employer. With e-mail an AUP might include things like:

- Policies on filtering and monitoring of e-mail content.
- Policies for e-mail attachments, and relevant information on guarding against viruses.
- Policies regarding use of web-mail services.
- Policies regarding bullying by e-mail.
- Actions for reporting misuse, including receipt of mail from unknown senders and spam.
- Sanctions for misuse of e-mail.

The generally accepted view in the UK is that it's OK to monitor employee e-mail that is sent or received for business purposes, but you should always tell employees (and recipients of messages) that you do it.

As for personal e-mail, some companies simply ban all personal e-mail. Others allow it, but point out that the company monitors it. Others provide a separate PC, not linked to the LAN, that staff can use to send and receive unmonitored personal e-mail.

Exercise 5: Viruses

1 Go to the following website and read about viruses, print at least two pages from the website and bookmark the website for future reference in your Favourites list: www.sophos.com/virusinfo/explained/

Archiving your e-mail

The high and rising volumes of electronic communications including e-mail, web mail, web transactions, instant messages and every other type of internal and external communication require a consistent approach to archiving. Archives need to be constructed intelligently.

Most good e-mail systems have an archiving feature built into the e-mail software. It is usually found in the **Tools** menu under **Options**, or something similar. It is a way of compacting (compressing) your e-mails into an archive folder, which you can retrieve if you need to.

Most companies will employ some kind of archiving mechanism for files as well. Space is limited and each person may only have a certain amount of e-mail space allocated to them. When it fills up — and it often does — you will be prompted to archive old mail messages, or delete some. As most people dislike deleting e-mails, archiving provides a way of keeping a compressed copy to access if the need arises.

It should be noted that some e-mail programs can get corrupted and may need to automatically archive the e-mail database to restore it back to its original state — often back-up copies are periodically stored on the local hard disk under a user's profile and can contain things like address books.

Exercise 6: Using E-mail

1 You are going to create some e-mails to send to a group of people. This could be your classmates, friends or work colleagues. Open your e-mail program. Your tutor will advise you which one to use.

2 Create an address book of people you know, that you send e-mails to. Set up at least two groups eg a personal group and a business group. Put people from your address book into these two groups.

3 Create a personal signature in your e-mail program that will be added to any e-mails you send out.

4 Create some folders to hold e-mails you receive, eg personal and business, or friends and family, shopping or hobbies. Make sure you nest folders correctly, eg Personal, might contain a Friends folder and a Family folder.

5 Create several e-mails making effective use of formatting like font, colour, indents, bullets and numbering and alignment. Include at least one web link in an e-mail.

6 Send e-mails to a group of people using both cc and bcc. Make sure you put in a suitable subject heading and send at least one with a high priority. Ensure you spell check your e-mail before sending it.

7 Create a simple document to send as an attachment and send it to someone in your e-mail group. Make sure you are able to compress the document and encrypt the e-mail if required. Find out how this is done in your e-mail program.

8 Be sure to show what you have done to your tutor, or print copies to keep in your portfolio of work.

Internet and Online Communications

Student Workbook — Advanced

Web Design

Design works differently in print than it does on the web because the online audience has different needs and expectations. While printed design has to persuade and be visually impressing, web design has to often pass unnoticed and let people reach the content quickly. This requires a special design technique and it is difficult for people who are just starting out to design for the web to adapt to these new issues. It takes a lot of practice to succeed in designing a website for users that appeals and is accessible to everyone. The first step would be to plan the hierarchical structure of the website — how users will navigate to various pages and/or sections of the website. Creating a diagram showing how this would work is often the first step.

The Background — Colour or Image?

At the beginning of web design everyone used different free graphics on their websites — whether they were animated gifs, backgrounds or clip art. However, over the years it has become recognised that the best background for a web page is white. If you use a photograph, a texture or pattern or even worse an animated gif as a background, it slows down the display of pages and can make it impossible for users to read the content.

If a background is coloured then because there are so many colours in images, it’s very likely that often the colour of the text will be identical with certain colours of the background thus making it impossible to read the text.

If an image must be used as a background it should be barely visible and not disrupt the process of reading. Often, the best choice for a background has proved to be a single colour that contrasts well with the text colour.

When choosing the colour of the background one must take into consideration the fact that people will not always see the colour as it was intended. This is due to monitor screens being different in quality and settings (such as colour calibration).

Visually impaired users such as the colour blind might find your background colour difficult to use. If the design requires other than a white background, make sure you test the design with visually impaired users.

When testing a design, it's best to see how it looks in black and white. If the design works in these circumstances then it can be successfully used by almost all users. For testing, try turning a snapshot of the site to grayscale and then try to figure out the location and functions of significant elements such as navigation, text and layout.

The Fonts — Sanserif

In print, the fonts that traditionally have worked best are serif fonts — Times New Roman is one example. Serif fonts are extremely detailed fonts that don't work well on-screen due to low resolutions imposed by technology. Sanserif fonts are preferred by organisations concerned with readability for print as well as on-screen. You will need to experiment with different types of font to get the best readability.

Using the same font size throughout your text is not only monotonous — it can discourage users from reading the entire page. Using different sizes for headings, subheadings and paragraphs makes a document much more usable.

It is important for people who are visually impaired to be able to increase font size for easier reading. Nearly all browsers have an option to increase text size, but the feature only works if the web page is designed to allow it.

The Text Content

Structuring content appropriately can significantly shorten the time by users to read it. Long blocks of text can discourage users from reading it closely. No matter how good the screen or the conditions for reading (colours, light) are, it is still much more difficult to read screen text than printed text.

The content of a web page should have first and foremost a *primary heading* which briefly describes the content of the page and *secondary headings* for each important section. The actual content should be broken into short paragraphs using short phrases that can be read quickly and using few 'stop' words like 'and', 'to', 'when' etc. Dashes and bullets can be used in order to increase readability and highlighting such as bold and italics can make key ideas and points stand out. One-and-a-half or double paragraph line height can be used.

Colours — Links and Text

In the early days of the web people expected hyperlinks to be displayed in underlined blue text and visited hyperlinks in violet or dark red. Everything else, like text, was black. However, due to increased design possibilities, web designers started using non-standard colours for links and text. It is now quite common to have hyperlinks without an underline, or even the same colour as the rest of the text. Some have dismissed completely the use of a visited link colour. However, to ensure accessibility:

- Links should always stand out and be easily distinguished from regular text.
- A different colour (than regular text) should be used for visited links.
- Text colour should contrast well with the background. Bear in mind the needs of disabled users and difficulties people with older computers encounter.
- If possible use *web safe colours*.

The pathways which people can take through a site are referred to as website navigation. A site's navigation must be well constructed, easy to use and intuitive. Poor navigation can frustrate users and they will quickly go elsewhere in search of information. **Navigation is the single most important element in creating accessible and usable websites.**

Checklist and Key Points to Consider When Designing Navigation

- People can enter a site through any other page, not just the homepage. Using other pages as entry points is achieved through search engines, links from other websites or bookmarks.
- Think about what people expect from good website navigation: primary navigation (most important links, categories etc), secondary navigation (secondary links, subcategories etc), position of navigation, link titles, number of links per page etc.
- A frame page could be used to present navigation, content, etc
- Labelling across the site should be consistent.
- A logo should be placed on a contrasting background so it can be seen.
- Keep in mind the 'less clicks the better' concept when designing website navigation. You must aid your visitors in finding the information they seek as quickly as possible. The website must respond instantly to their instincts.
- Think and act like the average user does.
- Consider using a generic e-mail (not your main e-mail account) to handle any malicious, junk or spam mail you may get in response to your website. This will ensure when you publish your website, it will not get clogged with unwanted junk mail.

Designers are often misled into thinking that their website's navigation is fine when in fact it might not be. You can reach this impression simply because you are familiar with a site. Always try to experience your website from the user's perspective.

People tend to ignore everything that looks remotely like advertising. If you intend to put graphics in the header of the page make sure the navigation bar is situated below the graphics and not above it. People might ignore the graphics and the navigation bar along with it. They might end up thinking that there's nothing more to that website. This is a classic example of the importance of *secondary navigation*.

Links which do not belong in the primary navigation are used to make up the secondary navigation. Such links might include: Contact Us, About Us, Privacy Policy, Terms of Use, Site Map, Links and so on. Secondary navigation can be placed just below primary navigation while making sure it does not stand out as much as the primary navigation. Web designers can make the link text smaller, use a separator or leave a reasonable amount of space for the eye to be able to make a distinction between the two. When using top navigation, secondary navigation can be placed on the left-hand side of the page.

Internal linking

One important aspect of navigation is *internal linking* between the pages. You can place links to other pages within the site in the actual body text of the page. This can help users find related information quickly. Internal linking can also help search engine spiders to find their way to every single page. For example, if you're talking about text-based browsers link the word browsers to a related page like a glossary for instance.

Placing a small set of links just below the text to related pages or resources is also a very successful way to interlink pages of similar interest.

Website navigation checklist

- Titles of navigation links should be short, descriptive and intuitive. Users should easily understand what every link leads to. The title labels should clearly indicate and inform the user what will happen if a link is clicked.
- The primary navigation should not have more than 6–7 links. Keep only the most important links in the primary navigation and leave the rest for the secondary navigation.
- Make the primary navigation stand out by using simple graphics or different links style.

- If using graphics or JavaScript links, a text alternative should be available. Some people might have the graphics turned off or JavaScript disabled when browsing the internet. In such cases an alternative option should be available.
- On every page there should be a reasonable number of links. Pages with 20–30 links are harder to use than pages with 10 links.
- Users should at any time be able to tell their whereabouts in a website.
- Colour links don't necessarily have to be standard but a user should be able to tell if a link has been clicked before or not.
- The hierarchy of the website pages should be kept to an absolute minimum. If the user has to navigate more than four levels to find what they are looking for, they will get frustrated and are liable not to return to the website.
- Useability options like the provision of Help and FAQ areas to help answer common questions or provide help on navigating the web pages and about the content listed on the pages can be very important for first time visitors to your website. Useability should be about having a clear consistent website, where clarity is more important than the visual impact — the website's purpose should very clear.

Publishing Web Pages

The language used to write web pages is called *Hyper Text Mark-up Language (HTML)*. The codes used to identify the start of a section, or a paragraph, are referred to as *HTML tags*. When you create the start of your web page you will probably want to tell the browser some things about the web pages. This information is often stored in *meta tags* at the start of your web page. The meta tags will identify the creator of the page and provide a description of the web page including things like its refresh rate. Because the meta tags contain information about the web page, they are often used in the keyword search for most search engines.

HTML tags are used to identify the start and end of a heading (<h1></h1>), the start and end of a paragraph ( ) and things like font types. Notice how each HTML starts with a <> and ends with a </>. Together the HTML meta tags and mark-up language create web pages that can be viewed and referenced by search engines so other people can view them.

You could also use other types of language like JavaScript, JAVA, Dynamic HTML (DHTML) and WMl to create your web pages.

You might also make use of *frames* to emphasis areas of your web page. Framing sections of your web page can enable the designer to present a consistent user interface across a website, so every framed page has the same look and feel, even though the content may be different on each page. Adding a navigation frame along the top or down the left side of the web page also provides a clear guide on how to navigate the page you are on and any others you may wish to view in that particular website.

When you have finished creating your web pages you need to upload your pages to your website, which may be a dedicated web server used for hosting web pages. This is often referred to as *web publishing*.

The New Technology — Flash Summary

In recent years the web appears to have become trendier and more multimedia oriented than in its early days. While in some domains the new technologies work and prove successful in most cases they don’t add to the user experience, on the contrary, they just make browsing the internet more difficult and time consuming.

Flash is probably the newest and trendiest technology currently used in web design. Flash is often used to display animations, images, interactive pop-up menus and even video. While Flash can be successfully used in websites with profiles in music, multimedia, online games, interactive activities etc, on most sites Flash is used for the sake of using it and this can raise serious issues for users.

When most people are presented with a Flash website they are compelled by the visuals, motion and sound. They appreciate it's 'good looks' and we cannot deny that Flash design looks good.

When people on an average internet connection look for information through search engines, links from other sites or their own bookmarks, Flash annoys them. It makes them wait an extra 1 or 2 minutes before they get to the information they seek and they're likely to move to another site where that doesn't happen.

Flash is often used because it's visually compelling. Special care must be taken when designing with Flash to consider accessibility issues.

Feedback Facilities and Data Protection

Take care when using feedback facilities, such as guest books. Whilst these can be great fun, allowing visitors to leave a permanent record of their visit to your website and providing some useful feedback, think carefully about the level of detail you collect and reveal via your site.

Many guest books will ask visitors to provide details of their name, e-mail address, where they are visiting from and their comments — many people will provide these details without caution, hence revealing a great amount of personal information about them and possibly providing a direct route for contact.

If using such tools, ensure that stringent moderation is in place before any postings are published on your site to strip out any problematic information. Think also about the data protection implications of collecting information via your website.

Registering Domain names

If you want to create a website you may need to register the domain name — this allows you to have exclusive rights to use the name on the internet. However, there are some major pitfalls if you pick a name already in use, or someone else attempts to use your domain name. Your name identifies your website and is crucial to the number of hits (people accessing) that you receive at your site.

If the name is well known you should get more hits, if it is confused with something else it can cause you serious problems, especially if the other site is used for material of an inappropriate nature.

Cyber squatting and typo squatting are recognised problems in the area of domain name registration.

- *Cyber squatting* is when companies or individuals register the domain names of legitimate companies or organisations, often in the hope of making quick financial gains by selling the domain name back to the company.
- *Typo squatting*, also referred to as 'typo piracy', is when mis-spellings of domain names are registered in order to poach potential visitors away, often to inappropriate websites.

Although both of these issues are more likely to affect commercial companies, anyone who wants to set up a website should be aware of them, and check their domain names periodically.

Of course one of the most important functions (once you have created your web pages and website) is to provide *web maintenance*. This involves updating the text content, adding and deleting links, renewing graphics and ensuring all aspects of the website are functioning and up to date.

Using Graphics and Images

The internet can provide a wonderful source of images, many of them copyright free, but finding appropriate images can be a challenge. Make sure you do not infringe the Copyright Designs and Patents Act mentioned earlier.

Many major search engines offer pre-set image searching from the homepage, often with safe searching options to filter results. However, such searches and filters generally work on the basis of filename and description, and so can lead to misleading, unexpected or inappropriate results, sometimes of an adult nature.

An alternative to search engines is to use specialist web-based image collections — sites that deal specifically with key subjects such as the arts, animals, history or scientific concepts. These have the benefit of being closed collections, monitored and moderated by specialists within their field. Many now have an educational focus and provide copyright permissions specifically for educational use. The following sites are child-friendly and have copyright permissions for educational use.

ArtMagick
ArtMagick is a non-profit virtual art gallery displaying paintings from art movements of the 19th and early 20th centuries. It contains over 3,000 paintings by more than 100 artists: www.artmagick.com

Kids Domain
Kids Domain is a family resource aimed at children (aged 3–12), their families and carers, and teachers. It provides a range of downloadable resources including clipart and icons organised by category such as holidays, sport, animals and seasons: www.kidsdomain.com

National Geographic
The website of the National Geographic Society provides access to an online photo gallery, organised by topic: www.nationalgeographic.com

AHDS (Arts and Humanities Data Service) Visual Arts website
Although primarily aimed at further and higher education, the AHDS Visual Arts website offers a searchable archive of visual arts images which may be of interest to older pupils. Covering subjects such as art and design, photography and fashion, materials can be used for personal, educational and research purposes only in accordance with the terms of the Copyright, Designs and Patents Act (1988). You will need to register to use this resource: www.vads.ahds.ac.uk

Living Library
Provided by RM (Research Machines), the Living Library provides access to collections of clipart, sound and video, categorised by primary or secondary education. This is a subscription service: www.livinglibrary.co.uk

NASA Earth Observatory
The main purpose of this site is to provide free access to new satellite imagery and scientific information about Earth. Images are generally free to use, unless copyright statements indicate otherwise: http://earthobservatory.nasa.gov

Image sites which should be used with caution

The following sites provide a good source of images for use in the classroom but should be used with caution — these sites may provide access to full web search facilities, or may contain links to advertising or age-inappropriate content.

Awesome Clipart for Kids
This website provides a school clipart collection, and links to two other favourite school clipart sites with a clear warning to 'watch your kids while surfing'. Some of the sub-categories have links to sites, which may provide full web searches: www.awesomeclipartforkids.com

Clip Art Warehouse
The Clip Art Warehouse contains thousands of clip art images, which are mostly free to use. However the site does contain commercial advertising and links to commercial search engines: www.clipart.co.uk/index.shtml

Security

It is important to keep your computer secure, not only to protect data on the computer itself, but data that may be stored on the network as well. A good security system confirms the identity of the people who are attempting to access the resources on your computer, protects specific resources from inappropriate access by users, and provides a simple, efficient way to set up and maintain security on your computer. Whether the computer is a stand-alone system (not connected to any others) or part of a network (several computers connected together), security must be implemented to ensure stored data is secure but available to the right people when they need it. It should only allow access to those people who have been allowed access and block people who do not have access.

Users and Passwords

Most computers start by nominating one person (during installation of the operating system) to control and look after other people who might want to use the computer. This person is usually referred to as the *Administrator*.

Tools like *Users and Passwords* in Control Panel allow the administrator to add users to your computer and to add users to a group. In Windows 2000/XP, permissions and user rights are usually granted to *Groups*. By adding a user to a group, the user is given all the permissions and user rights assigned to that group.

For instance, a member of the Users group can perform most of the tasks necessary to do his or her job, such as logging on to the computer, creating files and folders, running programs, and saving changes to files. *Users and Passwords* lets you create or change the password for local user accounts, which is useful when creating a new user account or if a user forgets a password.

A *local user* account is an account created on a specific computer. If the computer is part of a network, the administrator can add *network user* accounts to groups, and those users can use their network passwords to log on. The administrator cannot change the password of a network user.

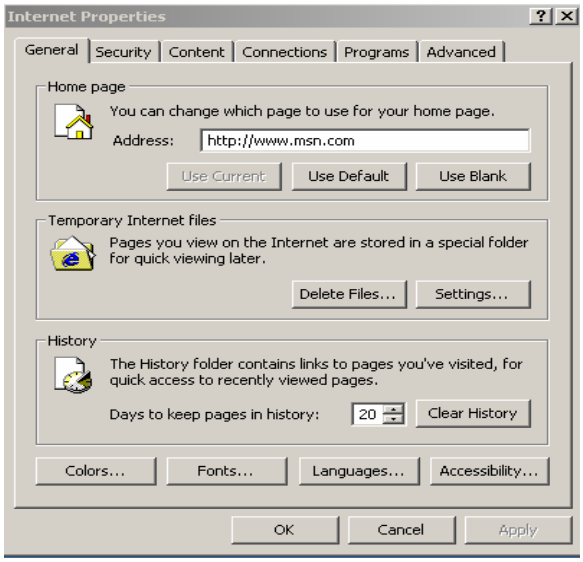
Internet Web Browser Security

An administrator can use group policy to administer web browser security on client computers. This allows a central administrator to set security for every user, or for individual users, dependent on their requirements. By adding people to groups an administrator can manage users better, and does not need to note every security setting for each user, only those they applied to a group. The areas you can administer include the browser settings, connection settings, important internet addresses (such as Favourites, links, home, and search pages), channels, security, and program associations as you will see later.

When accessing your internet web browser for the first time you may be prompted to set up your connection to the internet. At this point you need to know:

- How you are going to connect — via modem or local area network.
- Details of the e-mail account you wish to set.
- Details of your proxy or firewall.

If you do not know the above information, your internet web browser will still be set-up for you, but it may not allow you to connect until you have specified some of the above options.



The example used here is Microsoft's Internet Explorer. There are normally a number of tabs (depends on the version you are running) on the Internet Explorer Options (found either under **Tools, Internet Options** or by right clicking the Internet Explorer icon and choosing Internet Properties on your desktop.

- The **General tab** asks for specific information like home web page, location, how long you want to keep temporary files, and information about the history of your web activity.
- The **Security tab** allows security to be set at various levels, from *Trusted* sites to *Customised* settings.
- The **Privacy tab** lets you decide how to set privacy on your web browser and also how you will allow *cookies* (these are special programs used by websites to hold information about how you log onto them. Cookies reside on your computer, and the website uses its reference to decide whether to let you log on or not). This tab may not be available in older versions of Internet Explorer, it appeared in version 6.0.
- The **Content tab** specifies which content you will allow on your web browser.
- The **Connections tab** lets you set-up connections with your ISP, newsgroups and lets you decide how that connection will be established using protocols (rules) on transmitting the data.

- The **Programs tab** lets you decide which application software you would use for e-mail etc.
- The **Advanced tab** is generally, used by experienced administrators, to determine how content, graphics and certain types of programs (called scripts) will run on your web browser.

Common Attacks Against Security

We spend a significant amount of time investing in security for our homes and businesses. Failure to do so usually results in being robbed, damage or loss of business. Modern day IT managers realise it is equally important to protect their communications networks against intruders and saboteurs from both inside and outside.

There are many reasons and threats why this is the case. These include:

- Packet sniffing: to gain access to clear text network data and passwords. The packer sniffer will decode the information found in the packet header to find out sensitive information about the computers sending packets of information over a network.
- Impersonation: to gain unauthorised access to data or to create unauthorised e-mails by impersonating an authorised entity.
- Denial-of-service: to render network resources non-functional by flooding the network with useless messages, causing everything to slow down.
- Replay of messages: to gain access to information and change it in transit.
- Password cracking: to gain access to information and services that would normally be denied (Often referred to as a dictionary attack, a large database is searched to decipher the password. Many people use short passwords like names, films etc, which can be found easily by a hacker.
- Guessing of keys**:** to gain access to encrypted data and passwords referred to as a brute-force attack.
- Viruses: to destroy data.
- Port scanning**:** to discover potential available attack points in a network by looking for unprotected ports.

Hackers can easily exploit vulnerabilities using the methods listed. Though these types of attack are not exclusively specific to TCP/IP networks, they must be considered potential threats to anyone who is going to base their network on TCP/IP, which is the most prevalent protocol in use.

Exercise 7: Create a Website

1 You investigated various types of viruses and security issues with the internet in Exercise 5. These included viruses e-mail, worms, threats to confidential information, phishing, and denial of service attacks.

2 Create a simple website explaining one on these security risks and prevention strategies consisting of at least 5 pages using appropriate software. Your tutor will advise you what to use. Try to think about the design, use of text, colour and images when creating your personal web site.

3 Your website design should include internal and external hyperlinks, images including alternative text for accessibility, and colours.

4 It should also make use of tables, bulleted lists and suitable use of formatting including fonts, backgrounds and colours. Make use of any web tools to help create your web site.

5 Once you have created it, you should ask another person to evaluate its design — you might be biased. Save your finished web pages. Make sure you include your name and the date on the website.

6 Be sure to show what you have done to your tutor, or print copies to keep in your portfolio of work.

Networking

There are numerous ways to connect computers or create a network using networking software such as Windows 2000. The most common models or types are *peer-to-peer networks* and *server-based networks*. Each approach is different and has distinct capabilities. The type of network you choose is determined by several factors, including the number of computers that you want to connect, the level of security you require, and the needs of the users who use network resources.

There are two basic types of network. Each one relies on security being implemented either on each individual computer as in peer-to-peer networks or by a central administrator as in the client/server network model. All networking requires the use of specialised equipment, and security to make sure the correct people have access to the correct resources, whether that is a printer, data on the local hard disk or held on a central server, communication through e-mail, the internet or other resources like mobile computing and phones.

Peer-to-Peer Networking

A peer-to-peer network, often called a *workgroup*, is commonly used for home and small business networks. In this model, computers directly communicate with each other and do not require a centralised server to manage network resources. In general, a peer-to-peer network is most appropriate for networks where there are less than ten computers located in the same general area. It is less expensive and easier to maintain, but it is also less secure and has fewer features than a server-based model.

The computers in a workgroup are considered peers because they are all equal and share resources among each other without requiring a server. Each user determines which data on their computer will be shared to the network.

Sharing common resources allows users to print from a single printer, access information in shared folders, and work on a single file without transferring it to a floppy disk.

In order to establish a peer-to-peer network, you must ensure that all of the necessary hardware, settings, protocols, and services are configured properly. This includes:

- Installing a *network adapter* (sometimes referred to as a *Network Interface Card* or NIC) in each computer that you want to include in the network.
- Connecting the computers. You will need to decide which design layout, or *topology*, will work best for your network. The topology you choose will determine what type of cabling and connectors you will need.
- Installing a network service. This is the software that allows you to connect to other computers on the network.
- Installing the correct *network protocol* (set of rules). Each computer must be using a compatible network protocol, such as NetBEUI, IPX/SPX, or TCP/IP to be able to talk to each other.
- Each protocol (set of rules) has a different way of communicating over the network. Both network adapters must be using the same protocol to speak to each other.

In modern networking the peer-to-peer networking model has been extended to include sharing and caching facilities via a central server. This central server *caches* files sent from client computers, sometimes referred to as client hosts, and holds them for other client hosts to access. This reduces the burden on each client host holding copies of all the files another host might require.

On the internet, peer-to-peer networking has come to mean organised file sharing by individuals on a global scale, where people access files, help facilities and programs.

Client Server Network

Larger businesses or those with more complex networking needs rely on a *server-based network*. In a client/server model, computer tasks are split between a stand-alone personal computer, which acts as the client, and a server, which can be a personal computer, a minicomputer, or a mainframe. The server computer stores files for users in a central location and provides access to other network resources, such as printers, CD-ROM drives, and software. The server also provides data management, information sharing, network administration, and security features.

The server-based network has become the standard model for networking, primarily because it provides reliable management of network resources and a common security database. This model can support thousands of users, but is managed by a central group of administrators who oversee the network operation and ensure that security is maintained. Client users rarely perform work on the server computer.

Setting up a client/server network requires more resources than a peer-to-peer network. You will need to ensure that all of the necessary hardware, protocols, settings, and services are configured properly, and you will have additional resource requirements, including:

- One or more computers to be used solely as network servers. A large network may have more than one server, depending on the number of users, volume of traffic, number of peripherals, and so on. For example, you might find a print server, a communications server, and a database server all on the same network.
- Trained administrator staff to oversee network operations.

Security in this model can be set at different levels, for different groups of users. Some users may only have access to a particular printer, or the central administrator may have configured the security settings for Internet Explorer access through a proxy server or firewall.

Local Area Networks (LANs)

The *local area network* (LAN) is the most common type of data network. A LAN serves a local area (typically the area of a floor of a building, but in some cases spanning a distance of several kilometres). Typical installations are in office buildings, colleges or schools.

Various types of equipment is used to allow LANs to be connected together to form larger LANs. A LAN may also be connected to another LAN or to WANs (wide area networks) and MANs (metropolitan area networks) using more specialised equipment. In summary, a LAN is a communications network which is:

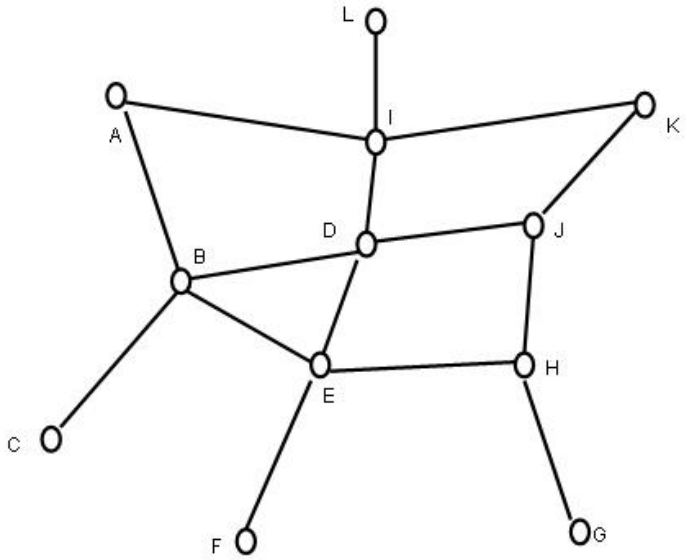
- local (ie one building or group of buildings)
- controlled by one administrative authority
- assumes other users of the LAN are trusted
- usually high speed and is always shared.

LANs allow users to share resources on computers within an organisation, and may be used to provide a (shared) access to remote organisations through a router. A *router* consists of a computer with at least two network interface cards supporting the *internet protocol* (IP) — a special set of rules for communicating in/between networks. Routers may be used to connect two or more IP networks (like MANs and WANs), or an IP network to an internet connection.

Wide Area Networks (WANs)

The term *wide area network* (WAN) usually refers to a network which covers a large geographical area, and uses communications circuits to connect the intermediate nodes. A major factor impacting WAN design and performance is a requirement that they lease communications circuits from telephone companies or other communications carriers.

Numerous WANs have been constructed, including public packet networks, large corporate networks, military networks, banking networks, stock brokerage networks, and airline reservation networks. Some WANs are very extensive, spanning the globe, but most do not provide true global coverage. Organisations supporting WANs using the internet protocol are known as *network service providers* (*NSP*s). These form the core of the internet.



Typical 'mesh' connectivity of a wide area network

Metropolitan Area Networks (MANs)

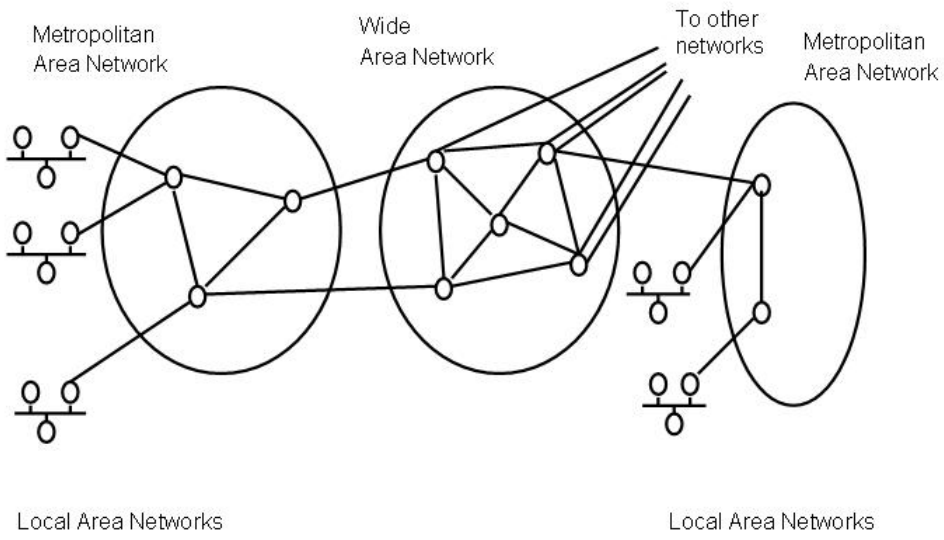
A *metropolitan area network* (MAN) serves a role similar to an ISP, but for corporate users with large LANs. There are three important features which discriminate MANs from LANs or WANs:

1 The network size falls intermediate between LANs and WANs. A MAN typically covers an area of between 5–50 km in diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings or as large as the North of Scotland.

2 A MAN (like a WAN) is not generally owned by a single organisation. The MAN, its communications links and equipment, are generally owned by either a consortium of users or by a single network provider who sells the service to the users.

3 A MAN often acts as a high speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

A typical use of MAN to provide shared access to a wide area network is shown in the figure below.

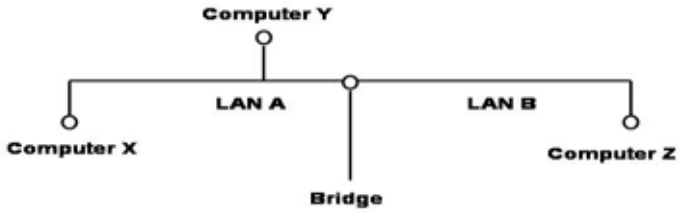


Repeaters (Hubs)

Repeaters regenerate (boost) the signal and allow the message from one PC to travel further to another PC. The major problem is if the signal travels too far, it starts to degrade and lose its pattern, which means the receiving PC might not get a clear message. Repeaters are used in LANs, MANs and WANs.

Bridges

A *bridge* is a device which is used to join two LAN segments (A and B), constructing a larger LAN. A bridge is able to filter traffic passing between the two LANs by looking at the IP address of the sending PC and determining whether its on the same segment (part of the network) as the receiving PC. If they are on different segments the bridge passes the message onto the next segment. To do this, the bridge needs to learn which computers are connected to which LANs. More formally, it needs to learn whether to forward to each address.

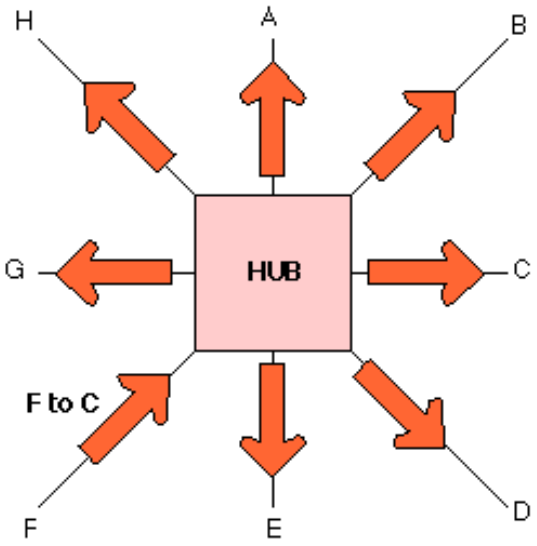


A bridge connecting two LAN segments (A and B)

In the figure above, consider three computers X, Y and Z. Assume each sends message packets (frames) to the other computers. The source addresses X and Y are observed to be on network A, while the address of computer Z will be observed to be on network B.

Multiple Port Bridges (Switches)

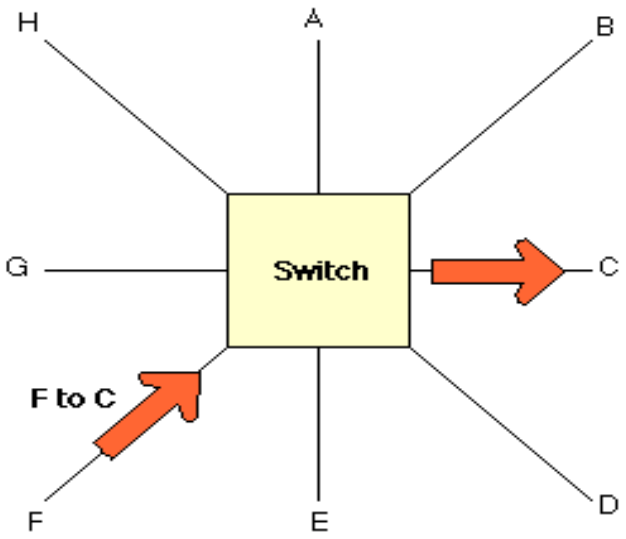
A bridge with more than two interfaces (ports) is also known as a *switch*. There are important differences between switches and repeaters (hubs). In particular, the way in which they forward frames.



A hub sending a packet from F to C

A hub (or repeater) forwards a received frame (message) out of all the interfaces (ports), resulting in the frame reaching all connected equipment, even though the frame may be only destined for a system connected to one particular interface (C, in the previous diagram).

A switch, forwards the frame to only the required interface. The switch learns the association between the PC system addresses (each PC has a unique IP address) and the interface ports in the same way as a bridge (see previous). By sending the packet only where it needs to go, the switch reduces the number of packets on the LAN segments (and hence the load on these segments), increasing the overall performance of the connected LANs.



A switch sending a packet from F to C

Routers

Routers are used to connect two or more IP networks, or an IP network to an internet connection. A *router* consists of a computer with at least two network interface cards (network card, often referred to as a LAN card) supporting the internet protocol. The router receives packets from each input interface and forwards the received packets to an appropriate output network interface. The router uses the information held in the IP header to decide whether to forward each received packet, and which network interface to use to send the packet.

The router contains routing and filter tables to know where/how to send message packets (often referred to as *frames*). A router forwards packets from one IP network to another IP network.

Architecture of a router

Routers are often used to connect together networks which use different types of links. A router may therefore use IP to provide segmentation of packets into a suitable size for transmission on a network.

Network Cards and Ports

To connect your computer to the network you need to have a special card installed in your computer called a network interface card (NIC). These cards come with a special RJ45 connection, which can be used with a network cable to connect to the network.

You can have various types of network cards now. These include ones that do not need cables called Wireless Network Cards which often work with wireless routers and devices like laptop computers. Some network cards work through the Universal Serial Bus (USB) port. These USB ports can connect multiple devices with special cables. You can connect memory sticks, network cards and other things like a digital camera and printers. A USB port needs to be available on the network card. Most modern network cards have an RJ45 and USB port on the card to enable you to make a choice on how you connect the cable from your computer to a network.

Network Cabling

UTP Ethernet (10BT/802.3i)

One of the most common forms of cabling is *unshielded twisted pair* (UTP) cable. This type of cable is very cheap to purchase and is flexible and easy to install. It is also used by other networking systems to provide telephone lines to offices. The official name for this cable is *10 BasebandT* (10BT), indicating that it is specified for baseband communications (ie not modulated) at 10 Mbps using twisted pair cabling. Some types of twisted pair cables can be used for communications up to 1 Gbps.

The 10BT cabling system uses a RJ-45 connector and 100 ohm unshielded twisted pair cabling. This connects the computer directly to a wiring hub which acts as a repeater. The maximum distance of a 10BT link is 100 m. It is normally used to connect work groups of users like a peer-to-peer network.

The photographs below shows the 10BT cable (with an RJ-45 connector plug) and the socket for the cable on a network interface card in a computer.

1

2

Connection of transceiver on equipment to a 10BT ethernet network

The other end of a cable is connected to a 10BT hub. The hub is a repeater with a number of 10BT ports. Some hubs also have a *transceiver AUI port* or *10B2 port* to also allow connection to other media.

There are other types of cable, like co-axial, fibre optic etc. These are used for more specialised areas in a network and when security or loss of signal are major concerns. Costs are more expensive, and sometimes specialised installation is required.

Source: http://www.erg.abdn.ac.uk/users/gorry/course/lan-pages/10bt.html

Network Protocols

Telnet Protocol

Telnet is an older, complicated application protocol that provides network terminal emulation capabilities. Telnet supports a wide variety of terminals and remains the primary protocol for remotely logging into a host. Other protocols use the remote login portion of the Telnet standard to provide authentication services to the remote host. Telnet clients and servers can provide and support a secure login capability.

File Transfer Protocol (FTP)

FTP is a protocol used to transfer files over the internet. It maintains two connections. The first connection uses a remote login protocol to log the client computer onto the FTP download. The second connection is used for the data transfer process. The first connection is open throughout the FTP session, the second connection is opened and closed for each file transfer. The FTP protocol is still used by major sites to enable client computers to access and download files and programs. Even if you access an FTP site like the one listed below, remember copyright laws still apply. Be sure you have permission to use and download files from these sites.

http://www.ftpplanet.com/

Hyper Text Transfer Protocol

Most web enabled browsers will use HTTP. HTTP is a generic, stateless, object-oriented protocol. It is generic because it transfers data according to the URL and handles different Multipurpose Internet Mail Extension (MIME) types. Because it treats every request as an isolated event, HTTP is stateless.

Although an HTTP server is small and efficient, the client bears the burden of the work. The client processes the HTML-encoded document and manages all the tasks involved in retrieval and presentation of the retrieved objects.

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol is a very sophisticated protocol. The mail handling system (MHS) consists of the mail transfer agent (MTA), the mail store (MS or mailbox), and the user agent (UA).

The mail transport agent (such as Sendmail, Exim or Exchange server) receives mail from the user agent and forwards it to another mail transport agent. Because the mail transport agent for SMTP receives all mail through port number 25, it makes no distinction between mail arriving from another mail transport agent or from a user agent.

The mailbox stores all mail destined for the mail transport agent. The user agent reads mail from the mailbox and sends mail to the mail transport agent.

The most popular protocol for reading remote mail is the *post office protocol version 3* (*POP3*). POP3 transfers all of the mail to the user agent and enables the mailbox to be kept or cleared. Because keeping the mail in the mailbox means that it is downloaded every time, most users choose the clear mailbox option. Users who need a more sophisticated approach to mail management might use *Internet Mail Access Protocol* (*IMAP*). With IMAP, the mail server becomes the mail database manager. This method enables a user to read mail from various workstations and still see one mail database that is maintained on the mail server.

Multipurpose Internet Mail Extension

The MIME standard defines the general content header type with a subtype to define a particular message format. Once again, the client (the user agent for a message handling system) must take care of building and displaying MIME attachments to mail messages. The MIME standard is used to extend the content of other protocols like HTTP and e-mail protocols.

What is an IP Address?

Every computer that accesses the Internet is assigned a unique IP address. IP addresses are given out by an organisation known as the *Internet Network Information Center* (InterNIC). By controlling the IP addresses, this ensures that each one is a unique number. You will either configure each computer separately so that each one on the network has its own IP address, or your ISP might assign IP addresses to the various computers on the network each time a computer connects to the internet.

A *dynamic IP address* is assigned each time a computer logs onto the network. This assigned address is valid for the duration of your online session and is fine for the majority of home network users.

The IP address that is fixed and assigned permanently is known as a *static IP address*. You must have a static IP address assigned by your ISP if you plan to host websites or offer access to a hardware device over the internet. It usually costs considerably more to get a static IP address.

TCP/IP Background

The *TCP/IP protocol suite* is a common set of rules to define how data should look, what information it should contain, and how the data is communicated to other computers on a network. TCP/IP is more than just one protocol, it is a set of related protocols.

There are two things to remember about TCP/IP:

- The TCP/IP standard is a system of rules defining how communication works on TCP/IP networks. The standards are set to ensure that regardless of the version or vendor any TCP/IP implementation will be compatible with other TCP/IP suites.
- A TCP/IP implementation is a software component that performs the functions that enable computers to participate in a TCP/IP network. This can be demonstrated by Microsoft's implementation of the TCP/IP suite.

In the 1970s the internet was being developed by the United States Department of Defence as a collection of computers which needed to be connected together to share information. The Defence Department Advanced Research Projects Agency (ARPA) came up with a set of rules (protocols) for communication with different types of computers — called Arpanet.

When, a few years later, the National Science Foundation wanted to connect various research institutions around the United States and beyond — they adopted the Arpanet protocol system and began to build what we now call the internet. The original decentralised Arpanet is now commonly known as the TCP/IP protocol suite. There are another two important things to remember about TCP/IP in a decentralised environment.

When two computers communicate, they are responsible for acknowledging and verifying the transmission. Often referred to as *end nodes*, there is no centralised control over data transmissions. Nodes can be connected through multiple paths and the router chooses the communication path based on the current conditions of the network.

When local area networks (LANs) started to become popular, there was no access to the internet — LANs had their own protocols, some did not support routing of data between networks at all. Software vendors who supplied the LAN operating systems saw the need to supply a protocol that could talk to different types of networks (Windows, UNIX, MacOS etc). The network interface card (NIC) has a unique *media access control* (*MAC*) address burnt into a chip, which identifies it on the network. Hardware conscious protocols can detect this address on the card and use it to find computers to 'talk' to on the network. As we have said computers will listen for messages on the network and if they 'hear' their Mac address they will respond.

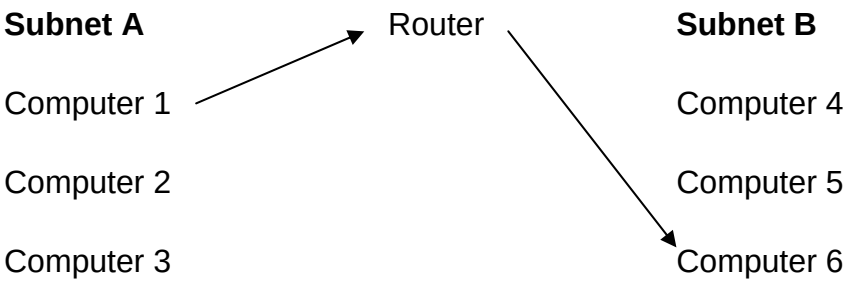
Segments

On larger networks this would be much more difficult with perhaps hundreds of computers listening or all trying to send messages at once — this would cause lots of collisions and nothing would be transmitted. To make it easier, network administrators use routers to *segment* networks into smaller more manageable sections so data can be sent more efficiently. These segments are often referred to as *subnets*.

Each computer in a segment or subnet can detect other computers on the same segment and send messages to them easily. If a message needs to go to a computer which is not on that segment, but on a different part of the network, the router knows how to get to the other segment and can pass the message on to the receiving computer.

For example:

We have two subnets and computer 1 on subnet A wants to send a message to computer 6 on subnet B:



Computer 1 only knows the address of computer 2 and computer 3 plus the address of the router. The router knows the addresses of computers, 1, 2, 3, 4, 5, 6, so can route the message for computer 1 easily.

Because the MAC address is different for each NIC and in large networks it would be difficult to remember them all, a logical address scheme is used in TCP/IP to help identify segments on the network. A computer's *logical address* is often referred as its IP address. The logical address consists of:

- A network ID number identifying the network; remember we could be talking about lots of different networks like the internet
- A subnet (segment) ID number identifying a subnet on a particular network
- A host ID identifying the specific computer on the network — a logical version of the MAC address.

Routers are special devices that can understand both logical addressing and MAC addressing and so can direct data requests from computers across many subnets and networks. Not all data goes through the router — remember local data transmission for computers on the same subnet are sent from computer to computer using either the MAC address of the logical IP address. Only data transmissions destined for another part of the network or another network are passed to the router to direct to the destination computer.

TCP/IP Protocol Layers

The TCP/IP protocol suite consists of four different layers. Each layer is responsible for specific tasks relating to sending and receiving data transmissions for computers on a network or between networks.

The *network access layer* is the interface with the physical network. It formats the data for transmission medium and address data for the subnet based on the MAC address. It also provides some error control.

The *internet layer* provides the logical addressing so data can pass between subnets. It provides routing to reduce traffic and ensure delivery across networks. It relates the MAC address to the logical IP address.

The *transport layer* provides control over the flow of data, error checking and acknowledgement services. It is the interface for network applications.

The application layer provides applications for troubleshooting, file transfer, remote control and internet activities.

These four layers loosely relate to the OSI model we talked about earlier:

TCP/IP Layers	**OSI Layers**
Application	Application
	Presentation
	Session
Transport	Transport
Internet	Network
Network Access	Data Link
	Physical

You can see that the four TCP/IP layers perform similar tasks to the OSI model, but use fewer layers to do the same tasks. Each layer in the sending computer has a corresponding layer in the receiving computer and each layer must agree how it will work — just like the OSI model.

TCP/IP Protocol Layers

Let's look at TCP/IP layers in greater detail.

At the application layer we have a range of network applications (network operating system or similar) that communicate with the transport layer ports. At the transport layer there are two ports:

- TCP which is a connection-oriented protocol, which provides sophisticated flow controls and error checking — a bit like you making a telephone call, you dial a number and remain connected during your call. TCP ensures the call will not be interrupted by anyone else.
- UDP is a connectionless protocol, faster than TCP but not as reliable — it's like you putting a letter in the post, you trust it will get there but have no guarantee it will be delivered.

Data is transmitted by either method — the network application usually decides which to use (TCP or UDP). Once the data segment is passed to the internet layer, the IP protocol provides the logical IP addressing information and wraps the data in a *datagram*. The IP datagram enters the Network Access layer where it interfaces with the physical network — which could be ethernet, token ring, FDDI etc.

It uses protocols such as *address resolution protocol* (ARP) which translates IP addresses to physical addresses or *reverse address resolution protocol* (RARP), which translates physical addresses to IP addresses. Remember the physical address is the MAC address number burnt into the Network Interface Card. This unique 6 byte number is used to identify a node (computer) on the network. The data is then converted into a stream of bits to be transmitted over the network cable.

TCP/IP Delivery

As we said earlier, physical addressing on a single subnet (segment) can be done just using the MAC address burnt into the NIC. This only works if there are a few computers on a single subnet, but it gets too complex if there are lots of computers spread over great distances.

TCP/ IP makes the physical address invisible and instead organises the network around a logical, hierarchical addressing scheme. The ARP (address resolution protocol) table keeps a database of all the physical addresses and the corresponding logical IP addresses and is the link between the burnt-in MAC address and the logical IP address. Remember we said that a logical IP address consists of three distinct bits.

Let's look at sending a letter from London to a postcode in Edinburgh: EH10 3SB.

- The network ID number is like the first bit of your postcode eg EH for Edinburgh — it tells the postal service where the network is generally.
- The subnet ID number is like the second bit of your postcode eg 10 — it tells the postal service which part of Edinburgh we should look in (what subnet to connect to).
- The host ID number is like the last bit of your postcode eg 3SB — it tells the postman which street and house number you live in.
- All three match your MAC address — EH10 3SB it is unique for your house and no-one else has the same postcode. We have just broken it down logically so the Royal Mail can deliver your mail.

Let's look at how the network ID number is broken down to make it easier to find its destination:

An IP address consists of a 32-bit binary address which is subdivided into four 8-bit segments called *octets*. Because we do not work well using binary or binary octets we often use something called *dotted decimal notation* which gives each octet a decimal number separated by periods in the range 0–255.

A dotted decimal IP address looks like this: 128.96.0.255.

TCP/IP Addressing

When IP addressing was first designed, it was decided to break the network ID into classes of addresses to make finding a network easier.

There are three main class addresses:

Class A addresses are often referred to as "/8's" because they have an 8-bit network prefix. One bit is reserved as the high order bit (set to 0).

0	7 bit network number	24 bit host number

There are 128 (2^7) addresses in a Class A address range but only a maximum of 126 addresses are used. Two addresses are reserved; one for the loopback address 127.0.0.0 and the other for the default route address 0.0.0.0.

There are 24 bits left for host IDs so that is 2^{24} which equals 16,777,216 hosts. However, two host addresses are always deducted — 'all zeros' and 'all ones'. They are not normally assigned to hosts because they have a special meaning in most networks, for identification and broadcasting. In reality they can be used, but generally they are not used for hosts.

The problem with a Class A address is that the number of networks we can have (126) is good but the number of hosts on each network is 16, 777,214 which is too much for most transmission media to cope with, so it's a waste of host IDs (remember we have deducted two because of the 'all zeros' and 'all ones' above).

Class B addresses often referred to as "/16's" because there is a 16-bit network prefix. Two bits are reserved as the high order bits (set to 1–0).

1–0	14 bit number	16 bit host number

There are 16,384 (2^{14}) addresses in a Class B address range. There are 16 bits left for host IDs so that is 2^{16} which equals 65,536 hosts.

However remember we said two host addresses are always deducted because they have a special meaning in most networks, for identification and broadcasting.

The problem with a Class B address is that the number of networks we can have is good (16,384) but the number of hosts on each network is still too much for most transmission media to cope with (65,534 — remember we have deducted 2 because of the all zeros and all ones above, so it's a waste of host IDs.

Class C addresses often referred to as "/24's" there is a 24 bit network prefix. Three bits are reserved as the high order bits (set to 1-1-0).

1–1–0	21 bit number	8 bit host number

There are 2,097,152 (2^{21}) addresses in a Class B address range. There are 8 bits left for host IDs so that is 2^8 which equals 256 hosts. However remember two host addresses are always deducted, for identification and broadcasting.

The problem with a Class C address is that the number of networks we can have (2,097152) is too high but the number of hosts on each network is just about right for most transmission media to cope with (254 — remember we have deducted two because of the 'all zeros' and 'all ones' above).

There are also Class D and E addresses used mainly for research, which we will not discuss here.

Remember in 1981 when class addressing was first thought out a 32 bit address range was considered huge and no-one expected there to be a massive increase in computer and internet usage. 32 bit addressing is limiting because lots of the class ranges are being fully used. A new scheme is being developed and used to segment networks. This is referred to as IPv6 which increases the size from 32 bits to 128 bits to support more levels of the addressing hierarchy and a much large number of addressing nodes (hosts).

Subnetting

We have explained how we use the classes to tell us which network ID to use and which host ID we can use, but how do we find out the subnet we can use to identify subnets on the network?

If we sent all data transmissions to the same Class A network ID eg 99.0.0.0, how do we know where on the network it should go? Do we look up the host ID portion of the IP address? We can, but which bit of the network is the host located on? If we searched the network, we might spend more time searching for the host than delivering the data transmission. In a Class A addressing scheme you can have up to 16 million hosts on a network — that's a lot of searching.

TCP/IP allows us to use a second tier of logical organisation beneath the network ID through a subnet (this is a logical division of the network address space which generally corresponds to a network subnet (segment). Remember this is the area in the town that we want to send our postal mail to, eg the '10' in 'EH10'.

How did we get the subnet ID if we have used all the 32 bits up in our TCP/IP address? Remember 8 bits for the network ID and 24 bits for the host ID. We borrow bits from the host ID to create the subnet ID – we use a parameter called a *subnet mask* to tell us how much of the address should be used to create the subnet ID and how much is left for the host ID.

A subnet mask is like a TCP/IP address — it is 32 bits long and arranged in a pattern that reveals the subnet ID. Because the address is understood in binary by the computer (1s or 0s) any 1s (which convert to 255 in dotted decimal notation) are used to identify the network ID and any 0s are used to identify the subnet mask eg 255.255.255.0. When you add the subnet mask to the IP address of the computer, it tells you which segment (subnet) it is on.

Most network administrators will spend a significant amount of time working out how many computers they have, how many subnets will they need to make data travel around the network efficiently, and how many IP addresses they will need to give them enough to use for current network operations and have some subnets and host IDs spare to allow the network to grow.

Sockets and Socket APIs

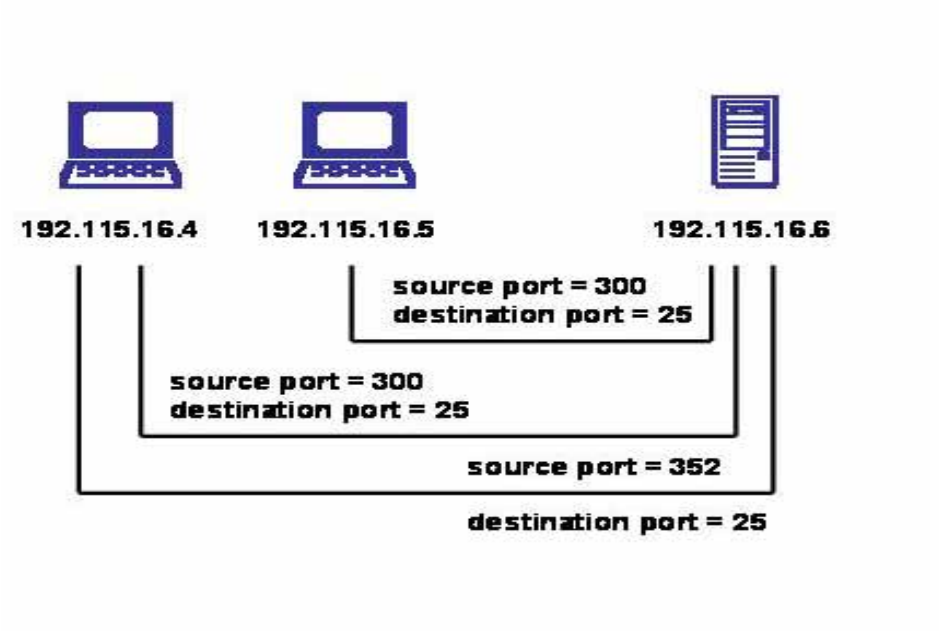
The *port number* is an application identifier that links the application layer to the transport layer. However, because multiple users can run the same application, the identification of a unique connection requires additional information. The transport layer creates a unique connection via a *socket*, which is the port number plus the IP address. The combination of the sending socket plus the receiving socket provides a unique identification for every connection.

However, if both the sending host and receiving host use the port number defined in the services file, then multiple connections between two hosts for the same application (for example, two FTP connections) results in identical socket pairs. To solve this problem, the source port number is some unique number not related to the services file. This number depends on the particular implementation. This scheme guarantees the uniqueness of any socket pair.

Port numbers are specified by a 16-bit number. Port numbers in the range 0-1023 are called *well known ports*. These port numbers are assigned to the server side of an application and, on most systems, can only be used by processes with a high level of privilege (such as root or administrator). Port numbers in the range 1024–49,151 are called *registered ports*, and these are numbers that have been publicly defined as a convenience for the internet community to avoid vendor conflicts.

Server or client applications can use the port numbers in this range. The remaining port numbers, in the range 49,152–65,535, are called *dynamic* and/or *private ports* and can be used freely by any client or server.

The following diagram gives a basic illustration of how sockets work.



The transport layer keeps track of these socket pairs by storing them in a port table. Although this device solves the technical problems, the use of socket APIs hides the details of the interface from the programmer.

TCP/IP v6

Since the introduction of TCP/IP to the Arpanet in 1973, the internet has grown — connecting more than 90 million users worldwide. Current estimates project the internet as connecting hundreds of thousands of sites and tens of millions of computers. This phenomenal growth is placing an ever-growing strain on the internet's infrastructure and underlying technology.

Due to this growth of the internet and the problems with the TCP/IP protocols, inadequacies in the network's current technology have become more evident. The current Internet Protocol version 4 (IPv4) was last revised in 1981 and since then the Engineering Task Force (IETF) has been developing solutions to resolve the inadequacies. These sets of solutions, which have been given the name IPv6, are becoming the backbone for the next generation of communication applications.

Virtually all the devices with which we interact, at home, at work, and at play, will be connected to the internet. In order to meet this vision the TCP/IP protocol is evolving and expanding its capabilities. The first significant step in that evolution was the development of the next generation of the Internet Protocol — version 6, or IPv6. The emergence of IPv6 will allow IP addressing to become far more flexiible, however the overhead for many companies will be to re-assign and re-calculate all their IP addressing to accept the new standard.

Address Expansion

One of the main needs for IPv6 is the rapid exhaustion of the available IPv4 network addresses. To assign a network address to every car, machine tool, television, traffic light, EKG monitor, and telephone, we will need hundreds of millions of new network addresses. IPv6 is designed to address this problem globally, providing for billions of billions of addresses with its 128 bit architecture.

Automatic Configuration of Network Devices

It is not an easy task to manually configure and manage the huge number of host computers connected to many networks, public or private. IPv6's auto-configuration capability will dramatically reduce the administrative burden by recognising when a new device has been connected to the network and automatically configuring it to communicate. For mobile and wireless computer users the power of IPv6 will mean much smoother operation and enhanced capabilities.

Security

For everyone connected to the internet, invasion of privacy is a concern. IPv6 will have a whole host of new security features built in, including system-to-system authentication and encryption-based data privacy. These capabilities will be critical to the use of the internet for secure computing.

For a really good technical white paper on TCP/IP addressing and subnetting go to:

http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf

Other Networking Terms

Data Transfer

Data transfer across computer networks, or even the internet, involve finding ways to minimise the amount of time spent sending data and keeping the transfer medium free of traffic for the least amount of time. Decisions are often made about how the data will be sent, for example:

- *Packet switching* is a method of dividing data into small blocks for transmission over a network, between two computers or over the internet. Packets are sent by the use of a routing algorithm which calculates the best *route* (path across the network or internet) to the destination host (computer).
- *Circuit switching* establishes a dedicated connection (circuit) to its destination before transmitting any data. The circuit cannot be used by any other nodes (computers) until the circuit/connection is released. Whilst the circuit remains open, data is sent in one continuous stream (one single chunk of data) and all data follows the same path across the network. This method takes up much more resources on the data transfer medium.

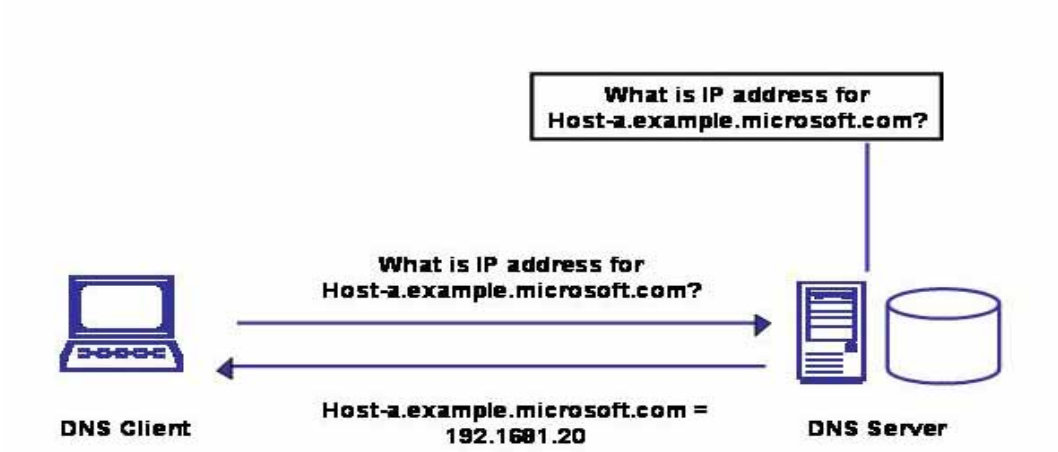
Domain Name System (DNS)

DNS is an abbreviation for *Domain Name System*, a system for naming computers and network services that is organised into a hierarchy of *domains*. DNS naming is used in TCP/IP networks, such as the internet, to locate computers and services through user-friendly names. When a user enters a DNS name in an application, DNS services can resolve the name to other information associated with the name, such as an IP address.

For example, most users prefer a name such as ‘example.microsoft.com’ to locate information such as a mail or web server on a network. A user-friendly name can be easier to learn and remember. However, computers communicate over a network by using numeric addresses.

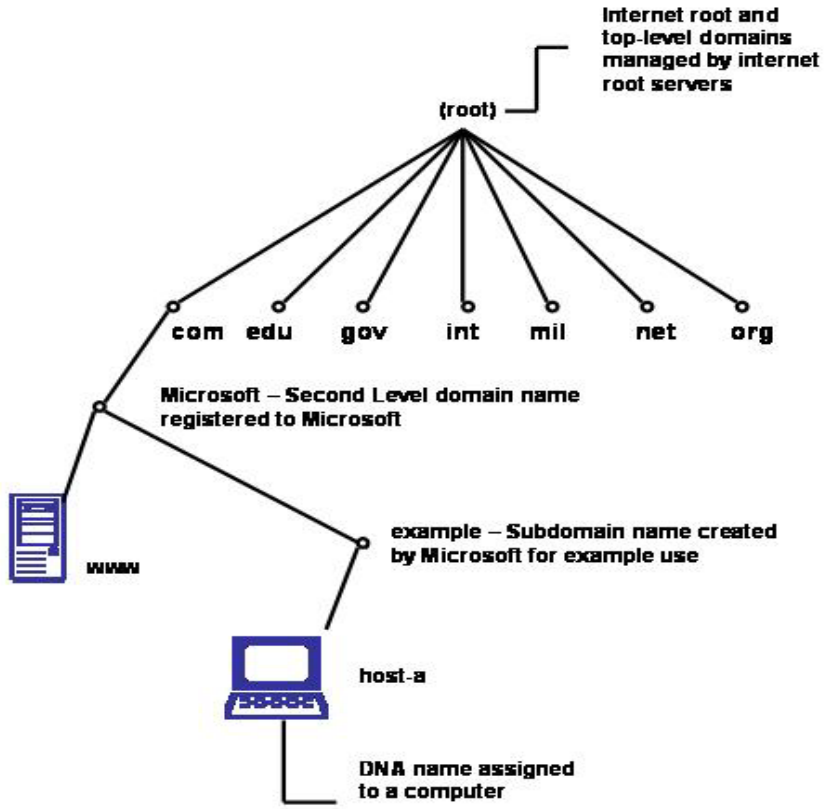
To make use of network resources easier, name services such as DNS provide a way to map the user-friendly name for a computer or service to its numeric address. If you have ever used a web browser, you have used DNS.

The following graphic shows a basic use of DNS, which is finding the IP address of a computer based on its name.



Understanding the DNS domain namespace

The DNS domain namespace, as shown in the following figure, is based on the concept of a tree of named domains. Each level of the tree can represent either a branch or a leaf of the tree. A branch is a level where more than one name is used to identify a collection of named resources. A leaf represents a single name used once at that level to indicate a specific resource.



When you dial (look up a web address) you are supplying the domain name which the computer translates into an IP address, which is a unique 4 octet number (eg 192.168.2.3) that identifies computer systems (including those on the internet). The web address request is forwarded onto a server that might know where to find the page. It starts with what it knows (how to get around its network), then how to get to the internet, and finally how to access the web address of the requested page, as in the previous example.

Because domain names are alphabetic, they're easier for humans to remember. The internet, however, is really based on IP addresses. Every time you use a domain name, DNS translates the name into the corresponding IP address either on the local area network (LAN) or on a larger system like a MAN, WAN or the internet. It is similar to a phonebook for the internet.

The domain naming service is also used by internet mail to support message routing. It maps domain addresses to IP addresses so internet messages can be delivered to a particular server. IP addresses can also be used instead of using the domain name to trace which computers visited the website.

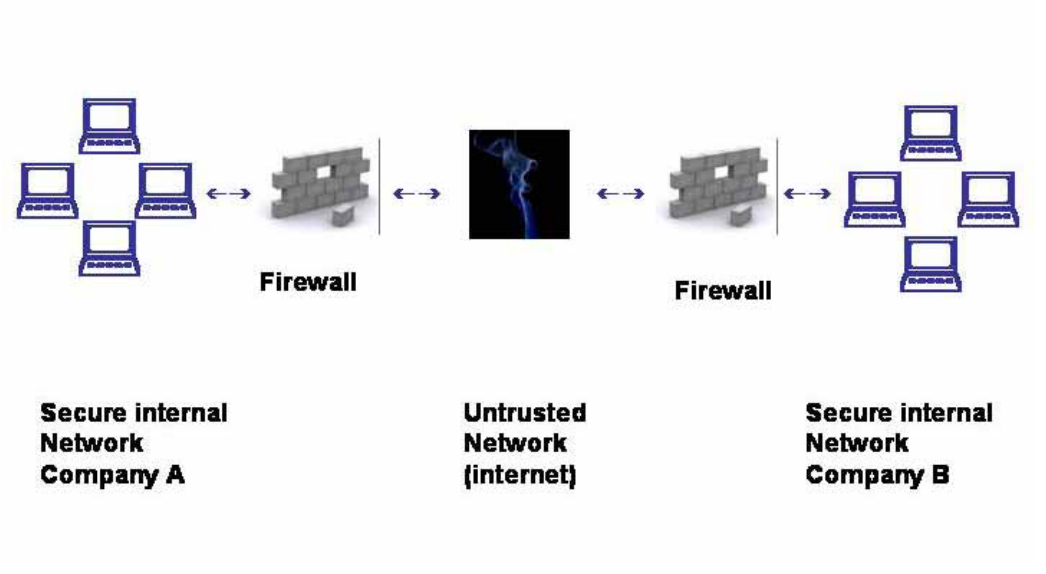
When a host on the internet needs to obtain a host's IP address based upon the host's name, a DNS request is made by the initial host to a local name server. The local name server may be able to respond to the request with information that is either configured or cached at the name server. If necessary information is not available, the local name server forwards the request to one of the root servers. The root server, then, will determine an appropriate name server for the target host and the DNS request will be forwarded to the domain's name server.

Name server data files contain the following types of records including:

- *A-record*: an address record maps a hostname to an IP address.
- *PTR-record*: a pointer record maps an IP address to a hostname.
- *NS-record*: a name server record lists the authoritative name server(s) for a given domain.
- *MX-record*: a mail exchange record lists the mail servers for a given domain.
- *CNAME-record*: canonical name records provide a mechanism of assigning aliases to host names, so that a single host with an IP address can be known by multiple names.

Firewalls

Firewalls have significant functions within security. Therefore, it is important to understand these functions and apply them to the network properly. A *firewall* is a system that enforces a security policy between a secure internal network and an untrusted network such as the internet. Firewalls tend to be seen as a protection between the internet and a private network. However, a firewall should be considered as a means to divide the world into two or more networks: one or more secure networks and one or more non-secure networks.



Photos © istockphoto.com – Pedro Tavares and Olga Zaichenko

The firewall can be a PC, a router, a Linux/Unix workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Your firewall is usually installed at the point where the secure internal network and untrusted external network meet.

In order to simplify the firewall concept, consider the network to be a building where access must be controlled. The building has a lobby as the only entry point. In this lobby, receptionists welcome visitors, security guards watch visitors, video cameras record visitor actions, and badge readers authenticate visitors who enter the building.

Although these procedures can work well to control access to the building, what if an unauthorised person succeeds in entering, there is no way to protect the building against this intruder's actions? However, if the intruder's movements are monitored, it can be possible to detect any suspicious activity.

A firewall is designed to protect the information resources by controlling the access between the internal secure network and the untrusted external network (the internet). However, it is important to note that even if the firewall is designed to permit the trusted data through, deny the vulnerable services, and prevent the internal network from outside attacks, a newly created attack can penetrate the firewall at any time.

In order to provide continual protection all logs and alarms generated by the firewall must be examined. Otherwise, it is not possible to protect the internal network from outside attacks.

Components of a firewall system

As mentioned previously, a firewall can be a PC, a Unix/Linux workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components:

- packet-filtering router
- application-level gateway (proxy).

Each of these components has different functions and shortcomings.

Packet-filtering router

Most of the time, packet-filtering is accomplished by using a router that can forward packets according to filtering rules. When a packet arrives at the packet-filtering router, the router extracts certain information from the packet header and makes decisions according to the filter rules as to whether the packet will pass through or be discarded.

Application-level gateway (proxy)

An application-level gateway is often referred to as a *proxy*. An application-level gateway provides higher-level control on the traffic between two networks in that the contents of a particular service can be monitored and filtered according to the network security policy. Therefore, for any desired application, the corresponding proxy code must be installed on the gateway in order to manage that specific service passing through the gateway.

A proxy acts as a server to the client and as a client to the destination server. A virtual connection is established between the client and the destination server. Though the proxy seems to be transparent from the point of view of the client and the server, the proxy is capable of monitoring and filtering any specific type of data, such as commands, before sending it to the destination. For example, an FTP server is permitted to be accessed from outside. In order to protect the server from any possible attacks, the FTP proxy in the firewall can be configured to deny specific FTP commands.

Proxy servers are a form of firewall that allows frequently accessed websites to be stored centrally for faster retrieval when requested from individual users (PCs) on the network. Proxy servers can be configured to use caches of saved web addresses, which reduces the time to retrieve the web page being requested. Proxy servers can help restrict users to use certain paths to access the internet and they can block access to areas not approved by the network administrator.

Exercise 8: Networking

1 Name two basic types of network:

_____

_____

2 What is a:

- LAN
- MAN
- WAN

_____

_____

_____

3 What is the most common type of cabling in networks?

_____

_____

_____

4 Name the top level 7 domains used in DNS?

_____

_____

5 How do you know you are using Secure Sockets Layer when you look at the web address?

_____

_____

_____

6 Name two of the TCP/IP layers?

_____

_____

7 What provides the protection between the internet and a private network?

_____

_____

8 What is a system for naming computers and network services that is organised into a hierarchy of domains?

_____

_____

Network Address Translation (NAT)

Network address translation is commonly known as NAT. The process is also called network masquerading, native address translation or IP masquerading.

Overview

NAT first became popular as a way to deal with the IPv4 address shortage and to avoid all the difficulty of reserving IP addresses. It has become a standard feature in routers for home and small-office internet connections, where the price of extra IP addresses would often outweigh the benefits.

In your typical configuration, a local network uses one of the designated 'private' IP address subnets, and a router on that network has a private address (such as 192.168.0.1) in that address space. This router is also connected to the internet with a single public address or multiple public addresses assigned by an ISP. As traffic passes from the local network to the internet, the source address in each packet is translated 'on the fly' from the private addresses to the public address.

The router tracks basic data about each active connection (particularly the destination address and port). When a reply returns to the router, it uses the connection tracking data it stored during the outbound phase to determine where on the internal network to forward the reply; the TCP or UDP client port numbers are used to *demultiplex* the packets in the case of NAT, or IP address and port number when multiple public addresses are available, on packet return.

To any other system on the internet, the router itself appears to be the source/destination for this traffic.

Why do we use NAT?

Well, it is one attempt at preserving the address space available for use on the internet. The majority of ISPs no longer use the A, B, and C classes of address. The reason why NAT is so important is that address space under IPv4 (in the current version) is limited.

Eventually the IPv4 address space will eventually run out. The stop-gap measure NAT has succeeded in preserving the current IPv4 address space for longer.

To use NAT, the router which connects your LAN to the internet will have two addresses. On the LAN side, it will have an address from the particular address range you chose to use and, on the internet side; it will have an address assigned to you by your current ISP.

NAT offers a small measure of protection and security to the machines hidden behind the NAT translation system. To the outside world it looks like a single machine, even if you have 10 computers connected up.

Using NAT can slow down the process of transmission, and limits the total number of sessions to the router to slightly less than 65, 000 at any one time. This is a very large number of computers and only likely to affect large networks who use NAT.

Dynamic vs Static NAT

Most network address translation is dynamic, each dynamic address uses the public source address assigned by your router. There is one drawback with this. If the router is the only device with a public address, then there is no way for you to provide information services on any computer internally in your network — for example FTP services. No one on the internet has any way of specifying that they want to connect to the specific computer containing the server.

However, static NAT allows this to happen. First, your ISP must allocate you a block of public addresses. Most ISPs will allocate you a block of 4, 8 or 16 addresses. The computer (for example the FTP computer) on your LAN gets assigned an address. Next, you configure the router with a static NAT mapping rule. You tell it the internal number in use on your LAN for the relevant computer, and you tell it the public address from your ISP-assigned address block that relates to it.

Now that this is properly setup, if someone FTPs to the public IP address listed in the static NAT mapping you made, your router will re-write the packets and transmit them inside to the correct machine on your LAN.

Secure Sockets Layer

Secure sockets layer is a protocol and works by using a private key to encrypt data that is transferred over the SSL connection. SSL encrypts sensitive data which is being transmitted over the internet. Most internet web browsers support SSL and many websites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with **https**: instead of **http**.

SSL provides an alternative to the standard TCP/IP socket API that has security implemented within it. Therefore, in theory, it is possible to run any TCP/IP application in a secure way without changing the application. In practice, SSL is only widely implemented for HTTP connections. SSL is composed of two layers:

- At the lower layer, a protocol for transferring data using a variety of predefined cipher and authentication combinations, called the *SSL record protocol.*
- On the upper layer, a protocol for initial authentication and transfer of encryption keys, called the *SSL handshake protocol*.

An SSL session is initiated as follows:

1 On the client (browser), the user requests a document with a special URL that starts with https: instead of http:, either by typing it into the URL input field, or by clicking a link.

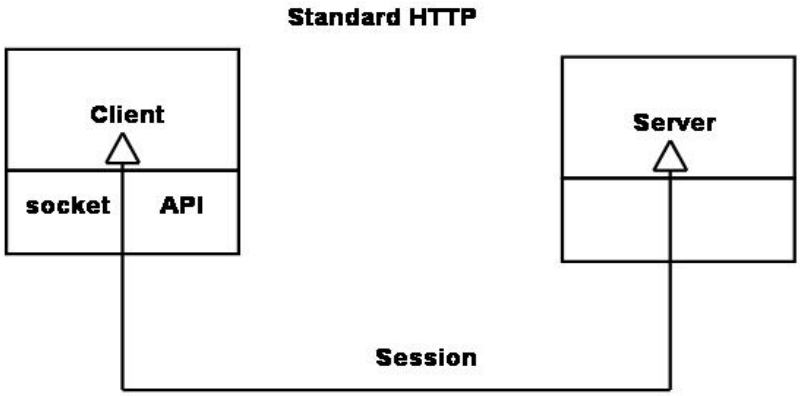
2 The client code recognizes the SSL request and establishes a connection through TCP port 443 to the SSL code on the server.

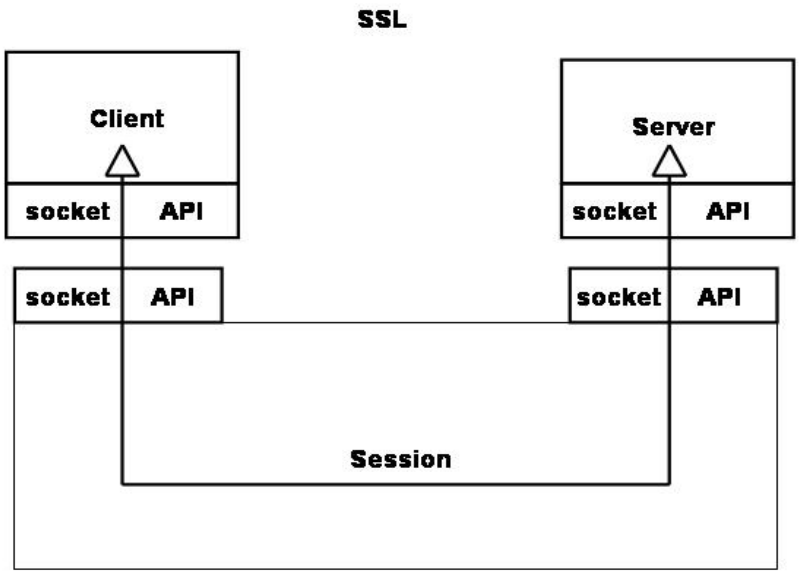
3 The client then initiates the SSL handshake phase, using the SSL record protocol as a carrier. At this point, there is no encryption or integrity checking built in to the connection.

- **SSL server authentication** allows a user to confirm a server's identity. SSL-enabled client software can use standard techniques of public-key cryptography to check that a server's certificate and public ID are valid and have been issued by a *certificate authority* (CA) listed in the client's list of trusted CAs (you can find this information in **Internet Explorer Tools**, **Internet Options** in the **Contents Tab**). This confirmation might be important if the user, for example, is sending a credit card number over the network and wants to check the receiving server's identity. This can often be seen on the screen in the bottom left corner of the web browser window as a golden padlock icon indicating that SSL is being used.
- **SSL client authentication** allows a server to confirm a user's identity. Using the same techniques as those used for server authentication, SSL-enabled server software can check that a client's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the server's list of trusted CAs. This confirmation might be important if the server, for example, is a bank sending confidential financial information to a customer and wants to check the recipient's identity.
- **An encrypted SSL connection** requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, thus providing a high degree of confidentiality. Confidentiality is important for both parties to any private transaction.

In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering — that is, for automatically determining whether the data has been altered in transit. Hackers constantly try to tamper with data and use special programs called *packet sniffers*. These programs monitor information on the network or over the internet and open the packets of data sent revealing sensitive data like bank account details or credit card numbers — this has led to an increase in data theft.

The diagrams below show the difference between a normal HTTP connection and a SSL connection.





The SSL protocol addresses the following security issues:

- *Privacy*: after the symmetric key is established in the initial handshake, the messages are encrypted using this key.
- *Integrity*: messages contain a message authentication code (MAC) ensuring the message integrity.
- *Authentication*: during the handshake, the client authenticates the server using an asymmetric or public key. It can also be based on certificates.

SSL requires that each message is encrypted and decrypted and therefore has a high performance and resource cost.

(SSH) Secure Shell (1 and 2)

SSH can secure connections between systems. It allows application traffic, such as that generated by Telnet, FTP, POP3, or even X Window System, to be both encrypted and compressed. Compression is useful over slow modem links. Implementations allow the user a choice of encryption methods. The client software often offers both SSH1 and SSH2 support.

The user is authenticated by password or public/private key.

- SSH1 offers Blowfish, DES, 3DES, and RC4 encryption ciphers.
- SSH2 offers 3DES, RC4, and Twofish encryption ciphers.

SSH establishes a single TCP/IP connection from the client to the server. The traffic sent down this connection is encrypted and optionally compressed using LempleZiv compression. Public/private keys can be used to verify both the user and the identity of the remote system.

Certificates

Many internet sites are set up to prevent unauthorised people from seeing the information that is sent to or from those sites. These are called ‘secure’ sites. Browser software supports a range of security measures for example Internet Explorer supports the security protocols used by secure sites.

When you visit a secure website, it automatically sends you its certificate, and Internet Explorer displays a lock icon on the status bar. A certificate is a statement guaranteeing the identity of a person or the security of a website.

You can use a personal certificate to protect your identity over the internet. A *certificate* is a statement guaranteeing the identity of a person or the security of a website. You can control the use of your own identity by having the private key that only you know on your own system. When used with mail programs, security certificates with private keys are also known as *digital IDs*.

Internet Explorer uses two different types of certificate:

- A ‘personal certificate’ is a kind of guarantee that you are who you say you are. This information is used when you send personal information over the internet to a website that requires a certificate verifying your identity.
- A ‘website certificate’ states that a specific website is secure and genuine. It ensures that no other website can assume the identity of the original secure site.

The digital signature component of a security certificate is your electronic identity card. The digital signature tells the recipient that the information actually came from you and has not been forged or tampered with.

Before you can start sending encrypted or digitally signed information, you must obtain a certificate and set up Internet Explorer to use it. When you visit a secure website (one that starts with ‘https’), the site automatically sends you their certificate.

Cookies

Some websites store information in a small text file, called a *cookie*, on your hard disk. Cookies contain information about you and your preferences. For example, if you inquire about a flight schedule at an airline’s website, the site might create a cookie that contains your itinerary. Or it might only contain a record of which pages within the site you visited, to help the site customise the view for you the next time you visit.

Only the information that you provide, or the choices you make while visiting a website, can be stored in a cookie. For example, the site cannot determine your e-mail name unless you choose to type it. Allowing a website to create a cookie does not give that or any other site access to the rest of your computer, and only the site that created the cookie can read it.

Microsoft's Internet Explorer is set up to allow the creation of cookies; however, you can specify that you be prompted before a site puts a cookie on your hard disk, so you can choose to allow or disallow the cookie; or you can prevent your internet web browser from accepting any cookies.

IP Security Risks

If there were no security risk concerns about connectivity on the internet, there would not be a need for firewalls and other defence mechanisms either. Thus, the solutions to the security concerns of IP-based protocols are widely available in both commercial and freely available utilities, but as you will realise, most of the times a system requires administrative effort to properly keep the hackers and crackers at bay.

As computer security becomes more of a public matter it is nearly impossible to list all of the tools and utilities available to address IP-based protocols' security concerns. There are various hardware technologies and application software to help you audit the security of your network, but first you need to understand the security weaknesses of the protocols used for connections over the internet. So we need to identify the flaws and possible workarounds and solutions.

TCP/IP Security Risks and Countermeasures

There are no security features built into IPv4 itself, and the few security features that do exist in other TCP/IP protocols are weak. A sound internetworking security involves and requires a careful planning and development of a security policy so that unauthorised access can be prevented and difficult to achieve, as well as easy to detect.

There have been many devices developed to add security to TCP/IP networks. Also internal policies normally allow users in the protected network to freely communicate with all other users on this same network, but access to remote systems and external networks (internet) are usually controlled through different levels of access security.

These access strategies can range from simple to complex. For example, a password could be required to gain access to a system, or complex encryption schemes might be required instead.

The most common adopted internet security mechanism is the firewall. But the security features that do exist within the TCP/IP protocols are based on authentication mechanisms.

IP Spoofing

A common method of attack, called *IP spoofing* involves imitating the IP address of a 'trusted' host or router in order to gain access to protected information resources. One avenue for a spoofing attack is to exploit a feature in IPv4 known as *source routing*, which allows the originator of a datagram to specify certain, or even all, intermediate routers that the datagram must pass through on its way to the destination address.

The destination router must send reply datagrams back through the same intermediate routers. By carefully constructing the source route, an attacker can imitate any combination of hosts or routers in the network, thus defeating an address-based or domain-name-based authentication scheme.

Hackers can use IP spoofing to gain root access, by creating packets with spoofed source IP addresses. This tricks applications that use authentication based on IP addresses and leads to unauthorised use and very possibly root access on the targeted system. Spoofing can be successful even through firewalls if they are not configured to filter income packets whose source addresses are in the local domain.

When spoofing an IP to crack into a protected network, hackers are able to bypass one-time passwords and authentication schemes by waiting until a legitimate user connects and logs in to a remote site. Once the user's authentication is complete, the hacker seizes the connection, which will compromise the security of the site.

Solutions to network security problems

It has to be noted that any of these solutions only solve a single (or a very limited number) of security problems. Consider a combination of several such solutions to guarantee a certain level of safety and security. These solutions include:

- Encryption: to protect data and passwords.
- Authentication by digital signatures and certificates: to verify who is sending data over the network.
- Authorisation: to prevent improper access.
- Integrity checking and message authentication codes: to protect against improper alteration of messages.
- Non-repudiation: to make sure that an action cannot be denied by the person who performed it.
- One-time passwords and two-way random number handshakes: to mutually authenticate parties of a conversation.
- Frequent key refresh, strong keys, and prevention of deriving future keys: to protect against breaking of keys (*cryptanalysis*).
- Address concealment: to protect against denial-of-service attacks.
- Disable unnecessary services: to minimise the number of attack points.

The following protocols and systems are commonly used to provide various degrees of security in a computer network.

- IP filtering
- Network address translation (NAT)
- IP security architecture (IPSec)
- Secure sockets layer (SSL)
- Secure shell (SSH)
- Application proxies
- Firewalls
- Kerberos and other authentication systems (AAA servers)
- Secure electronic transactions (SET)

The following table tries to show where these solutions fit within the TCP/IP layers.

Applications	S-MIME, Kerberos, Proxies, SET, IPSec (ISAKMP)
TCP/UDP (Transport)	SOCKS, SSL, TLS
IP (Internetwork)	IPSec (AH, ESP), packet filtering, tunnelling protocols
Network Interface (Data link)	CHAP, PAP, MS-PAP

Encryption Systems

The incredible growth of the internet has the promise of changing the way we live and work. But a major concern has been just how secure the internet is, especially when you are transmitting sensitive information across it.

There is a lot of information that we would not like other people to see, such as:

- credit-card information
- National Insurance numbers
- private correspondence and messages
- personal details
- sensitive company information
- bank account information.

General information security is provided on computers and over the internet by a variety of methods. A simple but straightforward security method is to only keep sensitive information on removable storage media, but of course you must then keep them in a secure location to avoid security breaches.

The most popular forms of computer security all rely on encryption, the process of encoding information in such a way that only the person (or computer) with the correct key can decode it. Most computer encryption systems can be placed into one of two categories:

- Symmetric-key encryption
- Public-key encryption

Symmetric Key

In *symmetric-key encryption*, each computer has a secret key that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric key encryption requires that you know which computers will be talking to each other so you can install the key on each one.

Symmetric encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message.

Public Key

Public key encryption uses a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. A very popular public key encryption utility is called *Pretty Good Privacy* (*PGP*), which allows you to encrypt almost anything. Some e-mail client systems allow you to code your e-mails using this encryption method.

The sending computer encrypts the document with a symmetric key, and then encrypts the symmetric key with the public key of the receiving computer. The receiving computer uses its private key to decode the symmetric key. It then uses the symmetric key to decode the document.

A popular implementation of public-key encryption is the Secure Sockets Layer (SSL) discussed earlier. Look for the ‘s’ after ‘http’ in the address whenever you are about to enter sensitive information, such as a credit-card number, into a form on a website. In your browser, you can tell when you are using a secure protocol, such as TLS or SSL, in a couple of different ways. You will notice that the ‘http’ in the address line is replaced with ‘https’, and you should see a small padlock in the status bar at the bottom or top of the browser window. This small padlock symbol lets you know that you are using encryption.

Authentication

Authentication is used to verify that the information comes from a trusted source. Basically, if information is ‘authentic’, you know who created it and you know that it has not been altered in any way since that person created it.

These two processes, encryption and authentication, work hand-in-hand to create a secure environment.

There are several ways to authenticate a person or information on a computer:

- Password: the use of a user name and password provides the most common form of authentication. You enter your name and password when prompted by the computer. The computer checks the pair against a secure file to confirm. If either the name or the password does not match, then you are not allowed further access.
- Pass cards: these cards can range from a simple card with a magnetic strip, similar to a credit card, to sophisticated smart cards that have an embedded computer chip.
- Digital signatures: a digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file) is authentic. The *digital signature standard* (*DSS*) is based on a type of public-key encryption method that uses the *digital signature algorithm* (*DSA*). DSS is the format for digital signatures that has been endorsed by the US government. The DSA algorithm consists of a private key, known only by the originator of the document (the signer), and a public key.
  If anything at all is changed in the document after the digital signature is attached to it, it changes the value that the digital signature compares to, rendering the signature invalid.

A more sophisticated form of authentication is biometrics. Biometrics uses biological information to verify identity. Biometric authentication methods include:

- Fingerprint scan
- Retina scan
- Face scan
- Voice identification

Source: www.encrypt-easy.com/how_encryption_works.asp

Acceptable Use and Security Policies

Many centres and organisations have security and acceptable use policies that their users must adhere to as part of the terms and conditions of their use of the facilities. These can include personal use of the internet connection, awareness of copyright laws regarding the downloading of information from the internet, virus protection, use of firewalls, password policies and backing up of important files. Breaching these policies can have serious consequences, for example, you may lose your job if you use your employer's computer system to do something illegal.

Acceptable Use Policies

If you use a computer other than at home, you should check whether there is an acceptable use policy directing and controlling what you are able to do and what you should not do while using the system. This may include, for example, whether you're allowed to use your company's computer for personal purposes such as sending personal e-mail or perhaps checking your bank balance online during the working day. It may be that you can use the facilities in this way during your breaks or maybe not at all. It will certainly include a section on using the system for illegal purposes such as downloading copyrighted materials such as music and video or starting arguments online (referred to as *flame wars*).

Security Policies and Viruses

Since viruses can even bypass some security systems, anti-virus software has been created to identify and where possible clean any virus it recognises on your computer. When you have anti-virus software on your system, it will alert you to any potential virus from transferred or downloaded files and prevent it from infecting your system.

To add another level of security, many public access systems (for example, schools or libraries) don't allow the transfer of information from other systems or the internet to help prevent viruses infecting their networks.

Although you can buy anti-virus programs, you can also find freeware versions of some of the major manufacturer's software for use on home computers on the main manufacturers' websites.

URL	Instructions and Description
http://www.grisoft.com	From the AVG Anti-Virus home page, click the AVG Free Edition link and follow the on-screen instructions. This software offers resident protection (it runs in the background monitoring your system at all times) and e mail scanning.
http://www.vcatch.com/download.html	From the home page, click the Free Download of VCatch Basic V5 and follow the on-screen instructions. This program checks files arriving via an e-mail, instant messaging or file sharing application.
http:/www.trendmicro.com	From the home page, click the red Personal tab at the top of the screen then click the Scan Now link under the TREND MICRO Housecall heading. This is an online scan, which means that you will not install a program on your computer but simply scan it for viruses. It will not warn you if your computer becomes infected later unless you run Housecall again.

Loading and running anti-virus software isn't enough. You also have to check for updates to the software so that it continues to recognise new viruses as they are developed and released.

When you purchase an anti-virus program you will be required to:

1 Register the product with the supplier, by giving them details of the product; they in turn will supply you with a valid product key.

2 After registration of your product has completed, the latest virus definitions will be downloaded. At regular intervals this will happen for the life of the product — typically one year.

3 The anti-virus software will perform a complete scan of your computer to detect and correct any viruses it may find. You can schedule the anti-virus software to perform scans regularly.

Important! Be sure to check the terms and conditions of use of any program you download or run online to be sure you don't break copyright laws. There are some programs like viruses which install themselves onto your computer, but often send information about your computer and you back to a third party person or organisation. These programs are referred to as *spyware*. You should also check to make sure these are not installed on your computer.

Password Policies

When you use computers and the internet, you'll find that you have a number of different passwords to create and then remember. For instance, if you work on a network, you may have a password to log on to the network, another one for your e-mail system and perhaps others for websites or internet service providers that you've signed up for (subscribed to).

So that your personal information is kept private and confidential, it's important that you don't give anyone else your passwords or use passwords that anyone who knows you could guess, eg your name or your birthday, or your pet's name. This also stops anyone else acting in your name without your knowledge. For the same reason, you should also consider whether it's safe to leave your computer without logging off.

It is also important to note that when accessing secure websites you may often be asked to key in extra characters that might be displayed on the screen. (Have you ever booked tickets online or joined an online group like Yahoo! groups?). Sometimes you may be asked to think of an answer to a 'secret question'. This question would be displayed if you incorrectly typed in or forgot your password; you could type in the answer to gain access to your account.

If you cannot remember the secret question's answer you would be prompted to send an e-mail request to the company to supply you with the password for the website you are trying to access.

A good password includes a combination of letters and numbers, and if it's *case-sensitive* (it matters whether you type it in capital or small letters), you should include a combination of capital and small letters along with the numbers. Some systems are set up to ensure that you include at least one letter and one number and have also set a minimum password length.

Some systems also have a built-in check to make sure you change your password every so often, every month for example, and won't let you use the same password twice. Modern networks often implement this type of check to ensure data is secure and no one is using your password illegally. Many websites and internet service providers will record attempts you make to put in the correct user ID and password and if you fail to put the password in correctly will lock your account until you have contacted them another way to verify your account credentials to them.

Technology Used in the Workplace

Video Conferencing

Video conferencing (VC) is a useful technological solution for situations where people need to meet but where travel distances, times and costs make it difficult for them to do so. VC enables collaborative working by transmitting audio, video and data between two or more locations. Several arrangements are possible as follows:

Point-to-point (one-to-one) meetings involve users at two locations. Audio and video are usually transmitted both ways.

One-to-many communication involves broadcasting audio and video from one central location to many participants but where there may only be audio communication for the return channel.

Multi-point (many-to-many) communication involves audio and video communication between three or more sites. Multi-point introduces the problem of which site to display on-screen at any one time. This can be resolved by manually switching between sites or by incorporating a voice activation mechanism which enables everyone to see the current speaker.

Video conferencing need not require a dedicated meeting room with cameras, microphones and a large screen. Two desktop PCs with webcams, microphones and speakers, network cards, video cards and suitable software would be sufficient for a one-to-one meeting.

Bandwidth and Compression

The bandwidth is the amount of information which can be transmitted every second. The higher the bandwidth, the better quality the signal that can be transmitted. For a video conference audio and video signals must be transmitted in real-time, ie a lot of information has to be sent every second, requiring a very high bandwidth.

For example a ‘true colour’ image will need 24 bits (3 bytes) per pixel. A full screen image might be 640 x 480 pixels, over seven million bits. For full motion video, the image is refreshed 25 times per second. This adds to over 184 million bits per second. It is not realistically possible to transmit this amount of information, and your PC certainly could not receive it at this rate.

For digital video some form of compression is required. The type and degree of compression used varies from system to system. For most uses, we are more tolerant of poor video than poor audio, and so some systems concentrate on providing consistently good audio.

Source: http://www.agocg.ac.uk/brief/vc.htm

Streaming video is becoming quite common today. *Streaming video* is a sequence of ‘moving images’ that are sent in compressed form over the internet and displayed by the viewer as they arrive. Streaming media is streaming video with sound.

With streaming video or streaming media, a web user does not have to wait to download a large file before seeing the video or hearing the sound. Instead, the media is sent in a continuous stream and is played as it arrives. It is widely used on the Web to deliver video on demand or a video broadcast at a set time.

Standards

Most major vendors now support the H.320 suite of ITU recommendations that define videoconferencing mechanisms over switched digital services such as ISDN.

Delivery

ISDN

Integrated Services Digital Network (ISDN) is a telephone network system, designed to allow digital transmission of voice, data and full-motion video over ordinary telephone copper wires. In the UK service providers such as BT offer ISDN services for business users. In April 2007 BT announced that it would withdraw ISDN services for consumer use later in the year (http://news.bbc.co.uk/1/hi/technology/6519681.stm) as a result of falling broadband prices.

IP

Video conferencing systems based on IP rather than ISDN offer several advantages, the main one being that many people already have a connection to an existing IP infrastructure. Codecs supporting the H.323 standard are widely available, some of which are free, making an IP based system the cheapest solution in many cases. The main disadvantage is bandwidth.

Though often not a problem on an internal local area network (LAN), IP videoconferencing across the internet can be subject to many delays, producing a poor frame rate (1 or 2 fps) and often unacceptable quality audio.

Satellite and Cable broadcast

Satellite and cable transmissions are usually used for one-to-many conferences. Although they are expensive, cost is not affected by distance and, therefore, they may be of use where very large distances or many sites are involved.

Source: http://www.agocg.ac.uk/brief/vc.htm

Optional Exercise 9: Using Video Conferencing

If your tutor can arrange it:

1 Visit your centre's video conferencing facilities.

2 Take notes on the type of system they use.

3 Ask about the available bandwidth and what is mainly used for.

4 What would you need for desktop video conferencing?

Finally

The candidate should (after consultation with their tutor) be able to do the assessment for this Unit.

This completes all the learning Outcomes for the PC Passport Internet and Online Communications subject.

Appendix

Copyright, Designs and Patents Act

This Act covers the copyright of:

(a) Original literary, dramatic, musical or artistic works.

(b) Sound recordings, films, broadcasts or cable programmes.

(c) Typographical arrangement of published editions.

The owner of the copyright in a work of any description has the exclusive right to do what they wish with their work, but if you are not the owner you are not allowed to use the copyrighted materials. The owner of the copyright has:

(a) The right to be identified as author or director.

(b) The right to object to derogatory treatment of work.

(c) The right to privacy of certain photographs and films.

The following is an extract from the Act. For a more detailed look at the Act go to: http://www.opsi.gov.uk/acts/acts1988/ukpga_19880048_en_1

Descriptions of work and related provisions

Literary, dramatic and musical works

- "literary work" means any work, other than a dramatic or musical work, which is written, spoken or sung, and accordingly includes a table or compilation, and a computer program;
- "dramatic work" includes a work of dance or mime; and
- "musical work" means a work consisting of music, exclusive of any words or action intended to be sung, spoken or performed with the music.

Artistic works

- "artistic work" means, a graphic work, photograph, sculpture or collage, irrespective of artistic quality, or a work of architecture being a building or a model for a building, or a work of artistic craftsmanship.

- “graphic work” includes any painting, drawing, diagram, map, chart or plan, and any engraving, etching, lithograph, woodcut or similar work;
- “photograph” means a recording of light or other radiation on any medium on which an image is produced or from which an image may by any means be produced, and which is not part of a film;
- “sculpture” includes a cast or model made for purposes of sculpture.

Sound recordings and films

- “sound recording” means, a recording of sounds, from which the sounds may be reproduced, or a recording of the whole or any part of a literary, dramatic or musical work, from which sounds reproducing the work or part may be produced, regardless of the medium on which the recording is made or the method by which the sounds are reproduced or produced; and “film” means a recording on any medium from which a moving image may by any means be produced.

Broadcasts

- a “broadcast” means a transmission by wireless telegraphy of visual images, sounds or other information which is capable of being lawfully received by members of the public, or is transmitted for presentation to members of the public; and references to broadcasting shall be construed accordingly.
- An encrypted transmission shall be regarded as capable of being lawfully received by members of the public only if decoding equipment has been made available to members of the public by or with the authority of the person making the transmission or the person providing the contents of the transmission.

References in this Part to the person making a broadcast, broadcasting a work, or including a work in a broadcast are to the person transmitting the programme, if he has responsibility to any extent for its contents, and to any person providing the programme who makes with the person transmitting it the arrangements necessary for its transmission; and references in this Part to a programme, in the context of broadcasting, are to any item included in a broadcast.

For the purposes of this Part the place from which a broadcast is made is, in the case of a satellite transmission, the place from which the signals carrying the broadcast are transmitted to the satellite.

References in this Part to the reception of a broadcast include reception of a broadcast relayed by means of a telecommunications system.

Cable programmes

- "cable programme" means any item included in a cable programme service; and "cable programme service" means a service which consists wholly or mainly in sending visual images, sounds or other information by means of a telecommunications system, otherwise than by wireless telegraphy, for reception at two or more places (whether for simultaneous reception or at different times in response to requests by different users), or for presentation to members of the public, and which is not, or so far as it is not, excepted by or under the following provisions of this section.

The following are excepted from the definition of "cable programme service":

(a) a service or part of a service of which it is an essential feature that while visual images, sounds or other information are being conveyed by the person providing the service there will or may be sent from each place of reception, by means of the same system or (as the case may be) the same part of it, information (other than signals sent for the operation or control of the service) for reception by the person providing the service or other persons receiving it;

(b) a service run for the purposes of a business where no person except the person carrying on the business is concerned in the control of the apparatus comprised in the system, the visual images, sounds or other information are conveyed by the system solely for purposes internal to the running of the business and not by way of rendering a service or providing amenities for others, and the system is not connected to any other telecommunications system;

(c) a service run by a single individual where all the apparatus comprised in the system is under his control, the visual images, sounds or other

information conveyed by the system are conveyed solely for domestic purposes of his, and the system is not connected to any other telecommunications system;

(d) services where all the apparatus comprised in the system is situated in, or connects, premises which are in single occupation, and the system is not connected to any other telecommunications system, other than services operated as part of the amenities provided for residents or inmates of premises run as a business;

(e) services which are, or to the extent that they are, run for persons providing broadcasting or cable programme services or providing programmes for such services.

Published editions

In this Part “published edition”, in the context of copyright in the typographical arrangement of a published edition, means a published edition of the whole or any part of one or more literary, dramatic or musical works.

Authorship of work

1 In this Part “author”, in relation to a work, means the person who creates it.

2a That person shall be taken to be in the case of a sound recording or film, the person by whom the arrangements necessary for the making of the recording or film are undertaken;

2b in the case of a broadcast, the person making the broadcast or, in the case of a broadcast which relays another broadcast by reception and immediate re-transmission, the person making that other broadcast;

2c in the case of a cable programme, the person providing the cable programme service in which the programme is included;

2d in the case of the typographical arrangement of a published edition, the publisher.

3 In the case of a literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken.

4 For the purposes of this Part a work is of “unknown authorship” if the identity of the author is unknown or, in the case of a work of joint authorship, if the identity of none of the authors is known.

Duration of copyright in literary, dramatic, musical or artistic works

1 Copyright in a literary, dramatic, musical or artistic work expires at the end of the period of 50 years from the end of the calendar year in which the author dies, subject to the following provisions of this section.

2 If the work is of unknown authorship, copyright expires at the end of the period of 50 years from the end of the calendar year in which it is first made available to the public; and subsection (1) does not apply if the identity of the author becomes known after the end of that period.

For this purpose making available to the public includes:

(a) in the case of a literary, dramatic or musical work, performance in public, or being broadcast or included in a cable programme service;

(b) in the case of an artistic work, exhibition in public, a film including the work being shown in public, or being included in a broadcast or cable programme service;

3 If the work is computer-generated neither of the above provisions applies and copyright expires at the end of the period of 50 years from the end of the calendar year in which the work was made.

Duration of copyright in sound recordings and films

1 Copyright in a sound recording or film expires at the end of the period of 50 years from the end of the calendar year in which it is made, or if it is released before the end of that period, 50 years from the end of the calendar year in which it is released.

2 A sound recording or film is “released” when it is first published, broadcast or included in a cable programme service, or in the case of a film or film sound-track, the film is first shown in public; but in determining whether a work has been released no account shall be taken of any unauthorised act.

Duration of copyright in broadcasts and cable programmes

1 Copyright in a broadcast or cable programme expires at the end of the period of 50 years from the end of the calendar year in which the broadcast was made or the programme was included in a cable programme service.

2 Copyright in a repeat broadcast or cable programme expires at the same time as the copyright in the original broadcast or cable programme; and accordingly no copyright arises in respect of a repeat broadcast or cable programme which is broadcast or included in a cable programme service after the expiry of the copyright in the original broadcast or cable programme.

3 A repeat broadcast or cable programme means one which is a repeat either of a broadcast previously made or of a cable programme previously included in a cable programme service.

Duration of copyright in typographical arrangement of published editions

Copyright in the typographical arrangement of a published edition expires at the end of the period of 25 years from the end of the calendar year in which the edition was first published.

Infringement of copyright by copying

1 The copying of the work is an act restricted by the copyright in every description of copyright work; and references in this Part to copying and copies shall be construed as follows.

2 Copying in relation to a literary, dramatic, musical or artistic work means reproducing the work in any material form. This includes storing the work in any medium by electronic means.

3 In relation to an artistic work copying includes the making of a copy in three dimensions of a two-dimensional work and the making of a copy in two dimensions of a three-dimensional work.

4 Copying in relation to a film, television broadcast or cable programme includes making a photograph of the whole or any substantial part of any image forming part of the film, broadcast or cable programme.

5 Copying in relation to the typographical arrangement of a published edition means making a facsimile copy of the arrangement.

6 Copying in relation to any description of work includes the making of copies which are transient or are incidental to some other use of the work.

Infringement by issue of copies to the public

1 The issue to the public of copies of the work is an act restricted by the copyright in every description of copyright work.

2 References in this Part to the issue to the public of copies of a work are to the act of putting into circulation copies not previously put into circulation, in the United Kingdom or elsewhere, and not to any subsequent distribution, sale, hiring or loan of those copies, or any subsequent importation of those copies into the United Kingdom; except that in relation to sound recordings, films and computer programs the restricted act of issuing copies to the public includes any rental of copies to the public.

Infringement by performance, showing or playing of work in public

1 The performance of the work in public is an act restricted by the copyright in a literary, dramatic or musical work.

2 In this Part “performance”, in relation to a work includes delivery in the case of lectures, addresses, speeches and sermons, and in general, includes any mode of visual or acoustic presentation, including presentation by means of a sound recording, film, broadcast or cable programme of the work.

3 The playing or showing of the work in public is an act restricted by the copyright in a sound recording, film, broadcast or cable programme.

4 Where copyright in a work is infringed by its being performed, played or shown in public by means of apparatus for receiving visual images or sounds conveyed by electronic means, the person by whom the visual images or sounds are sent, and in the case of a performance the performers, shall not be regarded as responsible for the infringement.

Infringement by broadcasting or inclusion in a cable programme service

The broadcasting of the work or its inclusion in a cable programme service is an act restricted by the copyright in a literary, dramatic, musical or artistic work, a sound recording or film, or a broadcast or cable programme.

Infringement by making adaptation or act done in relation to adaptation

1 The making of an adaptation of the work is an act restricted by the copyright in a literary, dramatic or musical work. For this purpose an adaptation is made when it is recorded, in writing or otherwise.

2 The doing of any of the acts specified in sections 17 to 20, or subsection (1) above, in relation to an adaptation of the work is also an act restricted by the copyright in a literary, dramatic or musical work. For this purpose it is immaterial whether the adaptation has been recorded, in writing or otherwise, at the time the act is done.

3 In this Part “adaptation” in relation to a literary or dramatic work, means a translation of the work; a version of a dramatic work in which it is converted into a non-dramatic work or, as the case may be, of a non-dramatic work in which it is converted into a dramatic work; a version of the work in which the story or action is conveyed wholly or mainly by means of pictures in a form suitable for reproduction in a book, or in a newspaper, magazine or similar periodical;

4 In relation to a musical work, means an arrangement or transcription of the work.

5 In relation to a computer program a “translation” includes a version of the program in which it is converted into or out of a computer language or code or into a different computer language or code, otherwise than incidentally in the course of running the program.

Reproduced from:

http://www.opsi.gov.uk/acts/acts1988/ukpga_19880048_en_1