6 Computer Communications and Networking

6.1 Networks

Advantages of Networking Stand-Alone Computers

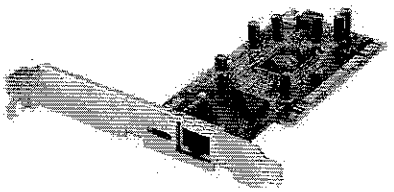
A stand-alone computer is one that is not connected to either a local or wide area network. Nowadays most organisations connect their computers to a computer network as there are obvious advantages in using this approach. The advantages and disadvantages are outlined below.

Computer Network Advantages	Computer Network Disadvantages
File sharing allows people on one workstation to share a file that has been created by someone else. This saves time in transferring files using memory sticks or other storage devices.	**System security** is a major issue in networking as hackers can use a range of tools to steal files. It is more difficult to hack into stand-alone computers as physical access is needed.
File access is improved as users can log on and work from any computer on the local area network.	
Resource sharing is possible with computer networks. Resources that can be shared include: file storage, peripherals (printers, scanners) and Internet connections.	File server reliability is important as, if it fails, then the whole computer network is unavailable to the users.
System backups are easier to control since they can be carried out centrally from the main file server.	**Computer viruses** are a big problem in computer networks as they can quickly spread between the interconnected computers.

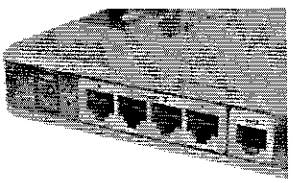
Network Components

Communication devices are the basic hardware needed when creating a network and the main components are described below:

- **Network Interface Card (NIC)** – The network card shown has an Ethernet cable input, and is simply fitted into a spare slot at the back of the computer to connect to the motherboard. On most current computers, the network interface card is integrally designed and fitted into the motherboard, as networking is now considered to be the norm rather than an extra feature.

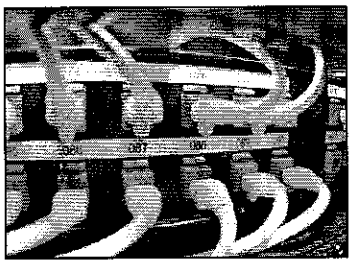


- **Cables** – Network components can be connected together using cables such as Ethernet cable or fibre optic cable. In addition, many modern computer systems will connect devices wirelessly as it gives the network a high degree of flexibility.
- **Bridge** – If the two networks are of the same type, they can be connected together using a bridge. The bridge simply copies data that is being transmitted from one network onto the other.
- **Hub** – A hub is a device for connecting many Ethernet cable-type devices, such as computers; it has several ports through which these devices are connected, and the data received is sent out again to all ports bar the input port.
- **Gateway** – If the networks are of different types then the job of passing data between them is more complicated. Data that is sent from one network to the other will need to be converted from the format that is used on the sending network into the format that is used on the receiving network. This job is done by a gateway.
- **Router** – In complex networks such as the Internet, there are many different routes that data could be sent down to travel from one computer or subnet to another. Devices called routers are used to determine an efficient route for this type of data transfer. Routers are also used in the home network environment so that the Internet can be shared by more than one computer from a single input.



 © ZigZag Education, 2013

- **Switches** – These are sometimes known as 'intelligent hubs', in that the switch does the same as a hub by connecting devices to link them as a single unit.
  However, it does not automatically send traffic to every other port, but determines the destination address of the data packet and uses switching to send it on to that destination address only. Switched data transfer is more efficient than hub transfer as the data is transferred to the destination line output, rather than every line.



- **Wireless Access Points** – This technique is used to support modern Wi-Fi computing and connectivity is based on transmitters sending and receiving data at radio frequencies from a wireless access point. So computers and other network devices have transmitter/receiver hardware to communicate with the wireless access point (WAP).

Role of Computers in Client-Server and Peer-to-Peer Networks

Client-Server Model

The client-server model has become one of the central ideas of network computing. In a typical network, the client is considered to be the many workstations on the network and the server or file server is the more powerful system that interacts with the clients; this technical configuration is widely used in educational establishments.

The basic operation is where the client makes a service request from the server, which then fulfils the request; for example, a web browser at the client computer may access information at any web server in the world.

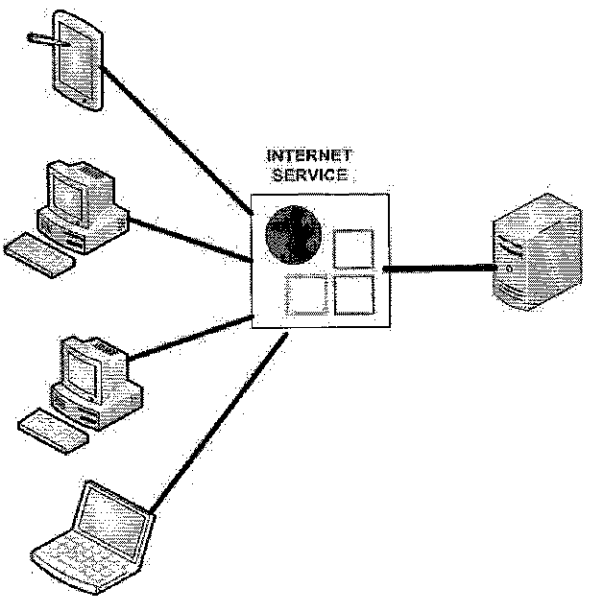
A **client-server** model is where the workstations in any network design use the server to provide a service

Client is a computer or workstation on a typical network.

File server is the powerful computer that interacts with the clients.

A client-server system diagram on the right shows a range of client devices connected via the Internet.
In the school context, a student logs on to a workstation and opens a word-processor application. The student then selects a file or document for editing (requested from the server) and the document is sent to them from the server to make the required changes. Whenever the document is saved, the changes will be made to the file server location for the document.

Online banking is a typical example of a client-server interaction, where the home user logs on via a web browser to the bank database to make a range of transactions.



The main advantages of the client-server structure are:

- The system facilitates a centralised backup.
- Security policies for access control and associated usernames are managed centrally.
- Centralised data is more consistent as there is only one copy in use.
- Lost data can be restored centrally for all users.

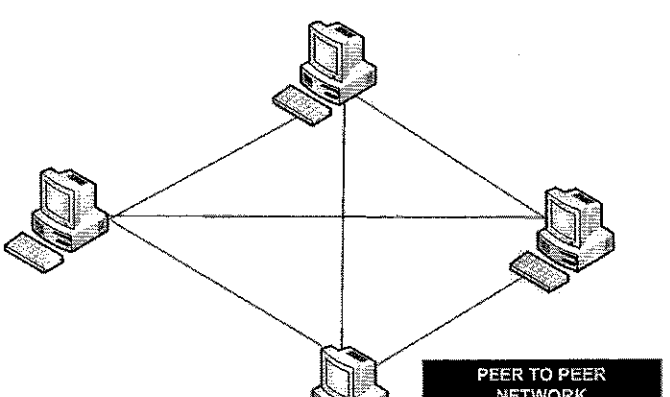
The main disadvantages of the client-server structure are:

- Server failure can cause the whole network to be inoperative.
- Network management is a skilled and necessary task for system maintenance.
- It is expensive and time-consuming to implement, due to the cost of a network operating system, which is usually priced by the number of clients and the labour involved in the initial set up.

 © ZigZag Education, 2013

Peer-to-Peer Host

Peer-to-peer networks are different from client-server networks as they do not have special workstations which are used as servers. Instead any workstation on the network can load information from the hard disk or use a local printer for any other workstation.

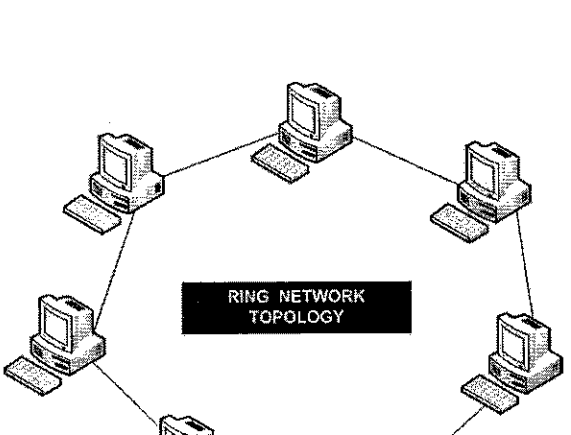


In the diagram, it should be noted that all workstations are linked to each other. However, it is obvious that this structure could not work efficiently for a large number of workstations due to the quantity of cabling and connections. The complexity of cabling is often reduced nowadays by the use of Wi-Fi.

Peer-to-peer networks are commonly used as local area networks (LANs) for general administration by either small businesses or in the home. In a typical home network, the Internet is shared using a broadband router.

Network Topologies

A network topology is a way of describing the interconnections and cabling of a group of computers. The three main topologies used are outlined below.



Ring Topology

The ring topology is shown in the diagram. Each workstation is connected to the workstations on either side of it; the last workstation is linked to the first to complete the ring.
It is often used for a small network as there is no central server in the ring system; it is normal that one workstation may control access to the network.
Each workstation can communicate with any other in the ring by addressing it directly.

Ring Topology Advantages	Ring Topology Disadvantages
It is ideal for a small network as expense is reduced since there is no dependency on a file server.	If a network cable breaks anywhere, then the whole system fails.
As data flows in one direction only, there is little risk of data collisions.	Ring topology is likely to have very long cable runs, which can be a problem as signal degrades over long distances.
It is easy to add more devices to this system as workstations are daisy-chained together.	

 © ZigZag Education, 2013

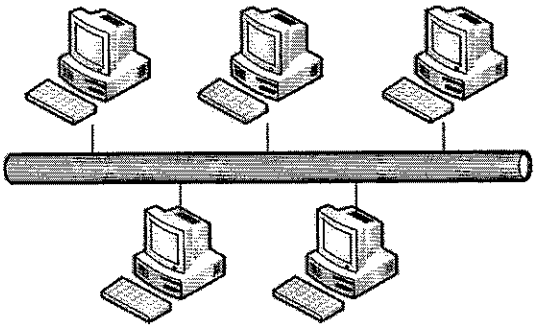
Bus Topology

When the bus (or line) topology is used, each workstation is connected to a single cable (or backbone) which links all the workstations.

The file server is connected to the main bus for data distribution to all the workstations.

Data can be transmitted in either direction along the main cable and workstations can communicate with their peers.

A range of peripherals can also be connected to the main bus for shared usage.



BUS NETWORK TOPOLOGY

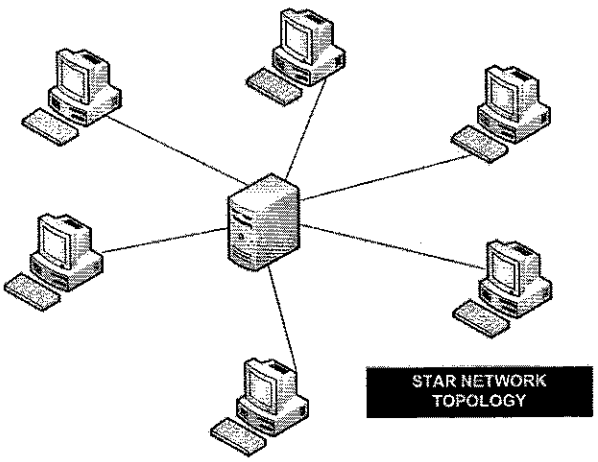
Bus Topology Advantages	Bus Topology Disadvantages
If one workstation fails, it does not affect the rest of the network.	If the main network cable breaks anywhere, none of the workstations can access the network.
It is cheaper to install as it uses the least cable as the cost of network cabling (particularly fibre optic) and the cost of network cable installation can be significant.	If there is heavy network traffic, the system performance will fall off dramatically.

Star Topology

The star network topology is based on connecting each workstation to a single point, such as a hub, which is linked to a file server.

This solution uses the most cable as each workstation has an individual link to the hub.

Different workstations may need to move different volumes of data and this topology allows for different cable capacities to be implemented, suiting the needs of a particular workstation.



STAR NETWORK TOPOLOGY

Star Topology Advantages	Star Topology Disadvantages
If one of the network cables breaks, only the computer connected to that cable is affected.	All communications takes place via the central hub and, if it fails, the whole network will break down.
It has a fast response time and no problems with data collision as each workstation has its own cable. Security can be installed at the central hub.	It uses the most cable which can be expensive to purchase and install. Also, long cable runs can cause the data signal to degrade.

 © ZigZag Education, 2013

Local and Wide Area Networks

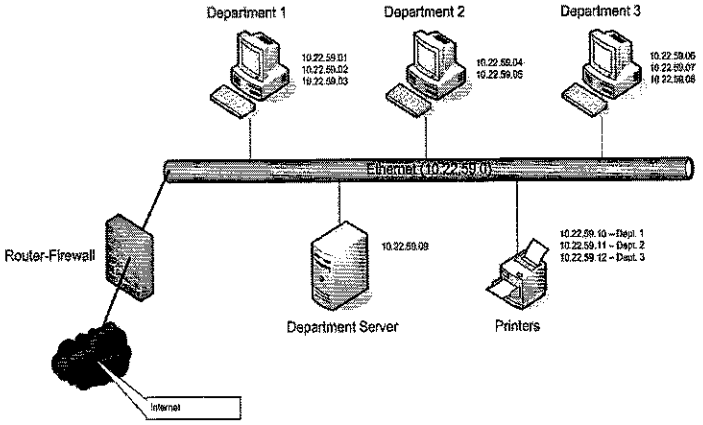
Local Area Networks

A LAN (local area network) operates over a relatively small area; in most cases, LANs are either a single building or group of buildings such as a school or a small manufacturing business.

As shown in the diagram, a typical LAN connects a series of workstations, personal computers and peripherals.

The advantage of this system is that most users can share peripherals such as printers and data or files.

Ethernet LAN Diagram



In the example shown, an Ethernet cable system is used; this is commonly used for PC networks. Apple Macintosh computers also support this standard networking technology, allowing them to be connected to PCs using routers or a direct connection.

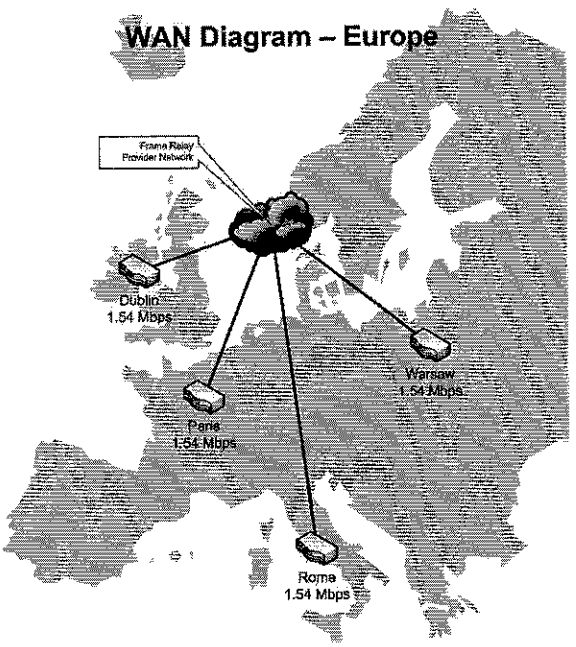
The diagram shows a shared connection to the Internet via a router and firewall for distribution and security purposes.

Wide Area Networks

LANs are capable of transmitting data at faster rates than data can be transmitted over telephone lines, but for larger areas or very large sites it is possible to join more than one LAN together to form a wide area network (WAN) using normal telecommunication links. Telecommunication link options include telephone lines, satellite channels or microwave links.

Wide area networks (WANs) span broad geographical distances – entire regions, states, continents or the entire globe. The most universal and powerful WAN is the Internet.

Computers connect to a WAN through public networks such as the telephone system or private cable systems, or through leased lines or satellites, using data transmission techniques as described above.



The diagram shows a wide area network for a multinational company with four offices in Europe. There is no real limit to the amount of offices they could have on their WAN.

 © ZigZag Education, 2013

Network Addressing

IP Address

Every device on a network needs a unique identifier to ensure that data is sent to the specific computer that requests it. The unique identifier for a computer in a network is known as the IP address and consists of the network ID and the host ID.

The IP address is needed to allow one computer on a network to communicate with the server or any other device. It is also widely used on the Internet which operates in a similar way to a smaller network.

The addressing technique used operates in the same way as a normal postal address, where letters and parcels find the correct address based on the unique house number and postcode.

An **IP address** is a number that uniquely identifies every host on an IP network.

A **network ID** identifies the network on which a device or computer can be found.

A **host ID** identifies a specific device on the network.

IP addresses consist of four numbers of up to three digits, separated by dots.
For example, the search engine Google has several unique IP addresses including: 74.125.224.72

Practical Task: IP Address
Read the notes and watch the video on IP addresses at the following link.
http://computer.howstuffworks.com/internet/basics/question549.htm

MAC Address

The **MAC** (media access control) address is the physical address of a device such as a **NIC** (network interface card).

It is a unique identifier assigned by the manufacturer and is stored on the network interface card in a ROM (read-only memory) device.

MAC addresses uniquely identify a network adaptor on a LAN (local area network); on a LAN, all devices that are connected can access the network traffic.

Security can be improved on a wireless network as follows: the router for a wireless network can be set up to allow access only to a list of computers – these computers are identified by their unique MAC addresses.

MAC stands for media access control and it is a physical address assigned to a device by the manufacturer.

Packets and Protocols

In networks, data is both transmitted and received. For example, if you download a web page, an email or a file, the data is broken down into a series of packets; these networks are known as packet-switched networks. **Packets** can be defined as 'data that is sent over a network in manageable amounts; the actual size and structure of a packet is determined by the protocol (or rules) being used'.

TCP/IP protocol is used as a standard to allow communication on most networks today; this protocol provides a unique identifier for a device or computer, known as its **IP address**.

Packets: Data is sent over a network in manageable amounts, known as packets.

A **router** is a device that forwards data packets within networks.

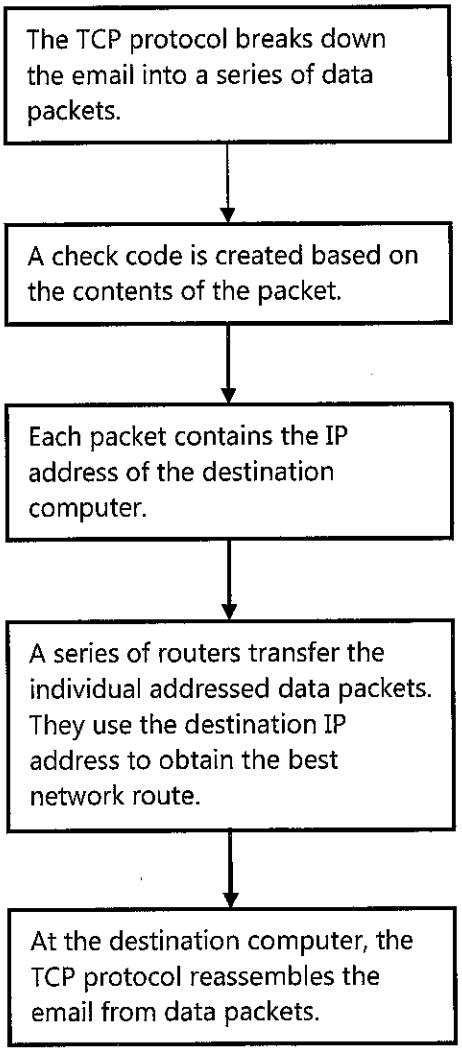
TCP/IP is the Transmission Control Protocol / Internet Protocol that is used to carry data packets on the Internet.

Protocol means a set of rules or standards.

IP stands for Internet Protocol; it is a set of rules that enable communications between networks.

© ZigZag Education, 2013

This TCP/IP protocol is used to transfer an email using the simplified flow chart diagram below:



Data packets are normally less than 128 KB and contain details of the destination computer.

The check code is sent in the data packet and is used to confirm the accuracy of the data sent at the destination computer.

The **IP address** for the destination computer contains the **host ID** and the **network ID**. This ensures that the packet is only received by the computer requesting the data.

The data packets for the email can travel via different routes, with the best route determined by the routers based on the destination address.

The reassembled message is checked for accuracy. If any data packet shows an error, it is rejected and requested again from the sending computer.

Other protocols widely used in computing include:

- POP3 (Post Office Protocol for email delivery)
- FTP (File Transfer Protocol for copying files to a network host)
- DNS (Domain Name System for converting domain names into IP addresses)

Practical Task: Routers / MAC Address

Watch the video on MAC addresses at the following link.
www.youtube.com/watch?v=mLYsPgeHFu4

Read the notes on how routers work:
http://computer.howstuffworks.com/router8.htm

 © ZigZag Education, 2013

Security Measures in Networks

There are many aspects associated with network security as described in the table below:

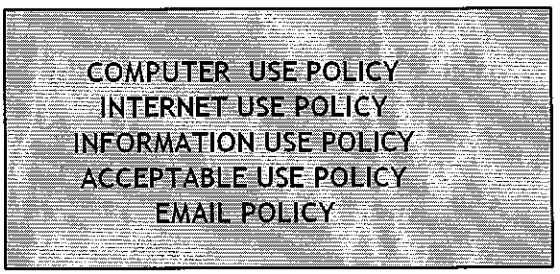
Feature	Explanation
Physical Security	Physical security is essential for servers and also important for normal workstations. It can involve locked doors with keys, keypads or biometric devices. Backup tapes and disks also need to be secured in a locked fireproof safe to avoid damage from natural disasters as well as theft.
User Access Permissions	The network administrator will give users access to the essential parts of the system that they need to do their work. User groups will be created so that workers can access and share each other's work where necessary.
User Access Passwords	Each user account will be password-protected. Passwords need to be created that are strong or not easy to guess. The network administrator will try to make sure that passwords conform to a set of rules and are changed on a regular basis.
Firewall and Intrusion Detection Systems (IDS)	Hacking is the practice of breaking into computer systems and it is essential that preventative measures are taken. Network firewalls protect computer devices from illegal access to the system. They can be hardware devices (part of the router) or software programs (part of the network operating system) or a combination of both. Intrusion detection systems (IDS) are designed to monitor the network or computer system for malicious activities. Once an incident is detected, a report is produced which is sent to the network administrator for further action to prevent any risk to the system.
Encryption	Encryption is widely used to make sure that data transmitted on a network is protected from hackers. It is the process of coding files before transmission and encryption ensures that the information is only readable by the person or persons who have the encryption key to decode it.
Virus Protection	A computer virus is a program designed to cause damage to a computer system or network; it can corrupt or damage files and spread throughout the network. The use of anti-virus software or a virus scanner can help to minimise the risk from viruses; this software searches the computer system for viruses and deletes them when detected. Spyware can be loaded onto a computer network as a software virus; it is important to detect and delete spyware as it can gather data from the network and illegally pass it on to other interested parties.

Network Policies

Organisations make use of detailed policies to ensure that computers are used and managed efficiently. These policies can help to avoid security and reliability problems.

Many organisation use a third party to help create their policies as it can save time and they can benefit from the advice of professionals.

One such company providing this service is:
www.computerpolicy.com.



 © ZigZag Education, 2013

Organisations might have different policies in place depending on the business they are in; details of the main policies used in a typical network are described below:

- **Acceptable Use Policy (AUP)** – This policy is a set of rules created by the network management to restrict the way in which the networks can be used and also to advise employees of their professional responsibilities. Normally employees sign up to show their agreement to this policy before they are given a user ID and access to the network, and they are also advised of any sanction in place for non-compliance.

  The main content of this policy includes rules such as:

  - Not using the network to send spam emails or for any other commercial activity
  - Not attempting to hack into the system
  - Personal use of email and the Internet
  - To use respectful language online
  - To manage and maintain password security

  Employee network accounts are normally audited to ensure that they are complying with the rules, and sanctions would be applied if they fail to conform to the required standards.

- **Disaster Recovery Policy** – It is necessary to have a policy to take account of a possible disaster, no matter how unlikely this is; typical disasters could be fire, flood or even earthquakes.

  The organisation will create a disaster recovery plan which will be based on them determining what risks they fear and the actions that they can take to minimise these risks.

  Finally, the plan will outline how the organisation will respond to the disaster, such as:

  - An off-site copy of the backup data is stored in case there is a disaster at the site and the system or data is destroyed.
  - In case the organisation's computer system is damaged or destroyed, they may maintain a hot site which is a duplicate of the original site with mirrored data to permit a speedy recovery from a local disaster.

- **Backup Policy** – It is necessary to have a policy to outline the backup strategy to make sure that data is not lost. The policy would outline who would carry out the backup, how often they would take backups, what media they would use, where they would be stored and to keep a detailed log of each backup. It is essential to document how the backup can be recovered where necessary, and for the recovery procedure to be tested.

  Typically, a backup for an organisation would be based on:

  - Data to be backed up onto an external device, such as a hard drive or magnetic tape.
  - A local copy of the backup should be kept on site so that the network can be recovered quickly if there is a problem.
  - A further backup copy is to be kept off site in case there is a disaster on site.
  - Each backup is to be logged and tested to ensure that it was successful.

Further policies would also be created by an organisation, including:

- **Failover** – This is where a computer system automatically switches over to a standby system when a problem is detected; failover allows the system to run continuously. The detected problem can then be fixed while the system is still operating; typically failover is used where two servers are mirrored and, if a problem is detected, the spare server is automatically switched in.
- **Archiving** – This is where data that is rarely used is backed up and stored in case it is ever needed. The data will be removed from the system after it has been successfully archived. Organisations will put in a place a policy to determine when data should be archived; for example, an online trader may archive data that is more than seven years old.

 © ZigZag Education, 2013

6.2 The Internet

The **Internet** can be thought of as a massive network of networks, where it connects millions of computers together globally, forming a network in which any computer can communicate with any other computer providing that they are both connected to the Internet. Information that travels over the Internet does so using the TCP/IP protocol (Transmission Control Protocol / Internet Protocol) to transport data packets over the Internet.

Do not confuse the Internet with the **World Wide Web** (often termed the **Web**) as this is simply the vast amount of web pages that are hosted by the Internet. The Internet can also be used for communication via email and for file sharing between computers using FTP (File Transfer Protocol).

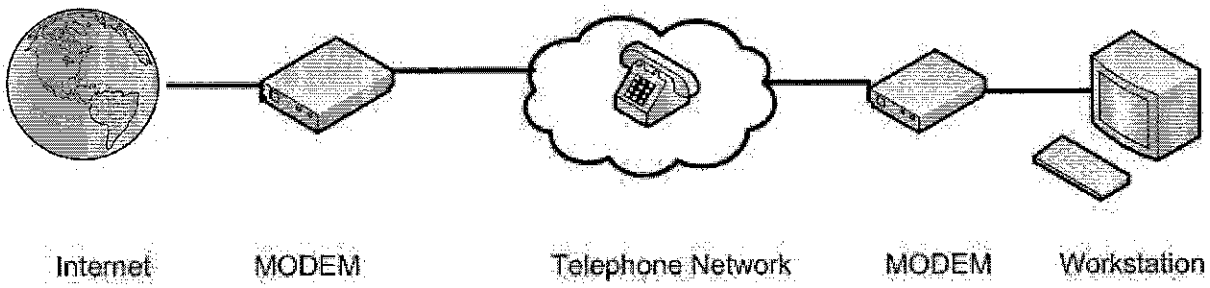
Internet Connection Hardware

Modems and routers are the types of hardware that are needed to connect to the Internet; further detail are included below.

Modem

The term 'modem' has been taken from 'modulator' and 'demodulator'. The task it performs is to communicate digital data using the telephone system infrastructure.
The conventional telephone network deals with analog signals and computer systems use digital data so the modem is used to carry out the necessary conversions, as follows:

- **Modulation** – The sending modem converts digital data into analog which is compatible with the telephone system.
- **Demodulation** – The receiving modem converts analog data from the telephone into digital data for use in computer systems.



The block diagram above shows how modems interface between the telephone network and computer systems.

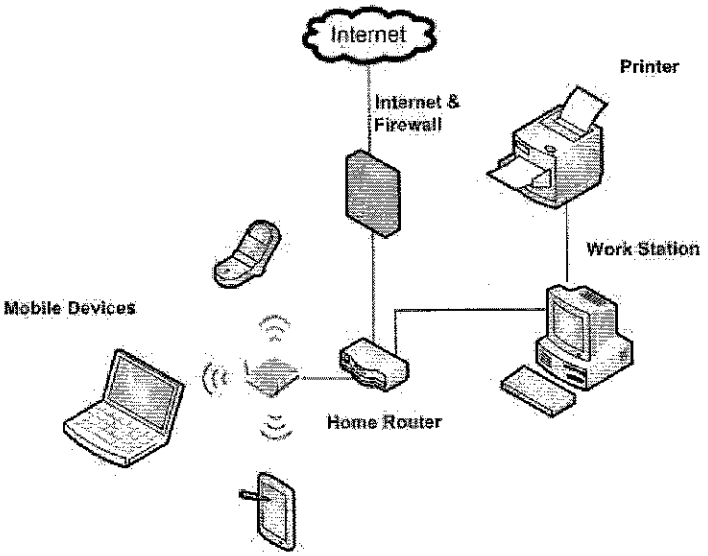
Modem performance is slow and limited to about 56 Kbps (kilobits per second) which is barely adequate for modern Internet connection. Some improvement in performance was gained by the use of ADSL connectivity using the telephone system. ADSL is based on the fact that most users download more than they upload, so the bandwidth of the telephone is set up asymmetrically to allow this, which can give an increased performance of up to 8 Mbps (megabits per second).

 © ZigZag Education, 2013

Router

Devices called routers are used to determine an efficient route for data transfer between computer systems and to transmit web pages to users throughout the world.

Routers are also used in the home network environment so that the Internet can be shared by more than one computer from a single input. Increasingly, they are used to share the Internet between several devices using a mixture of Wi-Fi and Ethernet cable connectivity, as shown in the diagram below.



The use of Wi-Fi in the home has increased recently with the use of smartphones and tablet PCs, so it necessary for home routers to be able to provide Wi-Fi as well as Ethernet cable services.

The broadband Internet can be connected to a local router using a range of services such as satellite TV services, cable TV services or telephone company fibre optic and digital lines.

Broadband speeds have increased sharply in recent years and the price for services has decreased; at the time of writing (September 2013), services advertised include BT Infinity Superfast broadband with speeds of up to 76 Mbps download and 19 Mbps upload.

DNS Services and IP Addressing

The most commonly used method for accessing a website is to enter its web address or domain name which is more commonly known as a uniform resource locator or URL.

As discussed earlier, IP addresses consist of four numbers of up to three digits, separated by dots. Domain names are far more memorable than IP addresses, for example it is easier to learn or type in **www.google.co.uk** than the IP address **74.125.224.72**.

A website **domain name** is an easy-to-remember numerical IP address.

A **domain name server** translates domain names into their unique IP addresses.

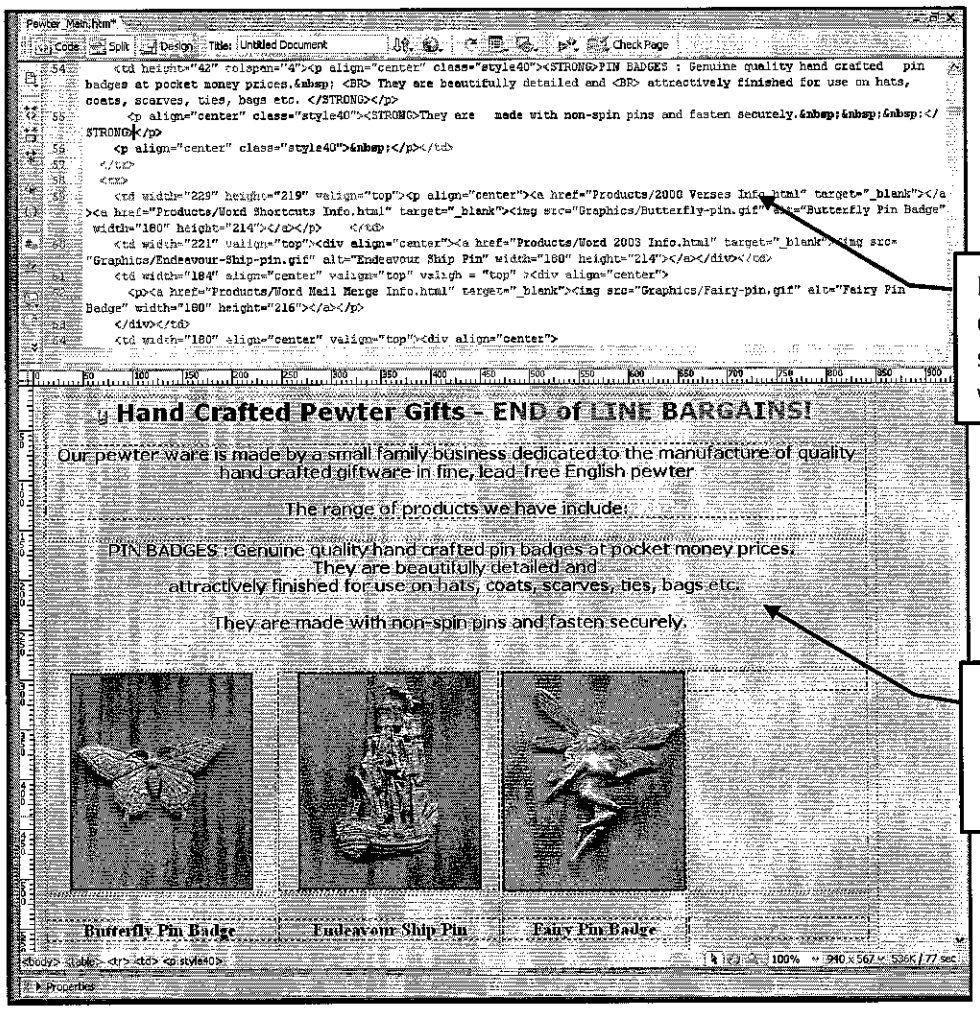
When we type a domain name into a web browser, it has to be converted into an IP address so that it can connect to the website. This conversion takes place by using the Domain Name System (DNS) which keeps details of the unique domain names used and translates them into IP addresses when needed.

Another function of the Domain Name System is to register new domain names and ensure that they are unique; it is involved in collecting any fees for domain name registration.

 © ZigZag Education, 2013

HTML and Web Page Creation

Web-development software is used to design and develop web pages; sites can be developed on a wide range of software by either using HTML code directly or by using wizard-type software that can be converted to HTML for publishing; although there are several different versions of HTML, it is the standard that is used for the creation of web pages.



Adobe Dreamweaver is a very popular website-development software package as it contains many easy-to-use features. The screenshot above shows a web page in editing mode; note that the HTML code is shown as well as the finished web page in a separate window. This is very useful as the novice can use Dreamweaver by editing in the view window and the expert can edit the HTML code directly.

In the web page example above, all the image and text content is organised into a table, as shown by the dotted lines in the design view; note these lines will not be shown in the published web page.

HTML (**H**yper**T**ext **M**arkup **L**anguage) is a text-based language that is used to create web pages.

Hyperlinks are one of the main features contained on web pages, where they are used as navigation links. When the hyperlink is clicked on, one of the following actions takes place:

- Another program is opened either in the current window or in a new window.
- The internal hyperlink takes you to another part of the current website.
- The hyperlink takes you to an external website, which can be opened in the current or in a new window.

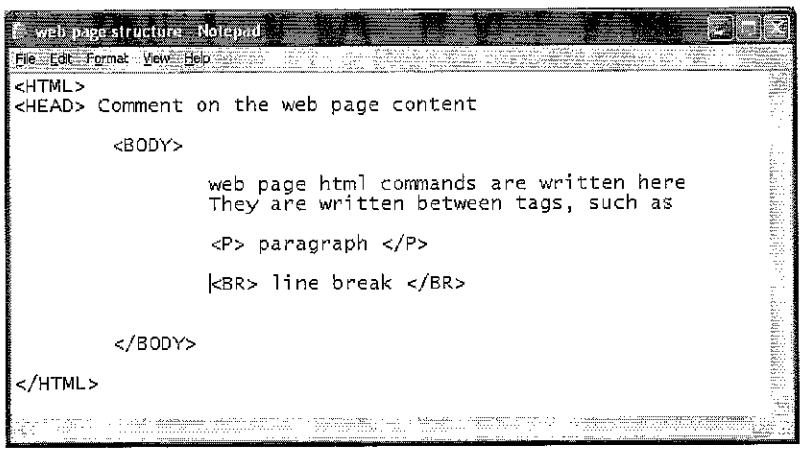
Hyperlinks are used on web pages to navigate to other web pages.

 © ZigZag Education, 2013

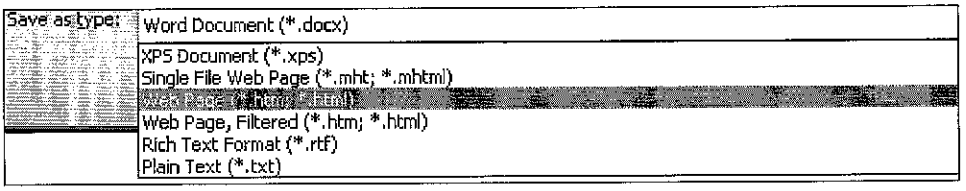
An example of the code for an HTML hyperlink to the OCR exam board's website is shown below:

```
<a href="http://www.ocr.org.uk">OCR Exam Board Web Page </a>
```

It is possible to create HTML web pages in any text editor, such as Window Notepad and the basic structure for a typical web page is shown in the screenshot below.



Students can also create HTML documents by using a word processor and saving their document and choosing file type as a web page (see below).



The web page can then be opened in a text editor such as Notepad to view the HTML source code; this is a useful method for learning the basic HTML tags and their structure.

File Compression

File compression can be defined as the process of reducing file size. In computer systems, reduced file sizes help to save secondary storage space.

It is important that files transmitted via the Internet are compressed as this decreases transmission time:

- **Images** – When an image is loaded onto a web page, the time taken to load it is related to the size of the file, so if the file size is compressed or reduced then it will load in a faster time. In the case of image files, they are usually compressed to a level where the image is still acceptable for website viewing.
- **Downloads** – When a program is downloaded from the Internet it is normally compressed into a ZIP file; this reduces the overall size of the downloaded files which can then be transmitted faster. Once the program has downloaded, it is not possible to run it without decompressing it using files such as WinZip; this then expands the compressed file back into the exact original format.

File compression is the process of reducing file size to save storage space or to save transmission time.

Zip files are used to compress files for transmission over the Internet or between computers.

There are two different types of file compression: lossless compression and lossy compression.

 © ZigZag Education, 2013

Lossless compression is used when the compressed file has the option to be expanded back into exact original format after it has been transmitted or processed. It is necessary to use lossless formatting in the following situations:

> **Lossless compression** is where a file can be compressed but the facility exists to expand the compressed file into the exact original format.

- An image might be compressed to low resolution for display on a website, but may also be needed in a higher resolution in a publication.
- A program may be compressed to be downloaded over the Internet, but it will need to be expanded to an exact copy of the original file before it runs.
- A document might be compressed into a zip file for attachment and transmission using email. Again the document will need to be expanded to an exact copy of the original to ensure that it can be understood.

Lossy compression is entirely different and it is not possible to recreate an exact copy of the original file using this method. It is used when some data can be removed from the file to make it smaller, but the final compressed file is still acceptable for the use for which it was intended.

> **Lossy compression** is where a file is compressed by removing unnecessary data to reduce file size.

Lossy formatting can be used in the following situations:

- A copy of an image might be compressed to a small file size for display on a website, but there is no need to expand back to an exact copy of the original file.
- Sound files reduce unnecessary data to compress the files, but overall output quality is acceptable for the user.

 © ZigZag Education, 2013

File Standards

Commonly used files associated with the Internet are described below:

File Standard	Extension	Detail
JPG	.jpg	JPG – Joint Photographic Experts Group. 24 bit colour depth bitmap format with lossy compression that is normally used for high-quality photographs; can be compressed to create acceptable small website images.
GIF	.gif	GIF – Graphic Interchange Format. A lossless compression bitmap format based on a colour depth of 256 colours. Mainly used on websites for logos and animated images.
PNG	.png	PNG – Portable Network Graphic. 24 bit colour depth lossless compression raster graphic file that is used widely for transferring images on the Internet.
PDF	.pdf	PDF – Portable Document Format. This de facto standard was developed by Adobe for exchanging documents where text, formatting and images are presented as an accurate copy of the original document.
MP3	.mp3	MP3 – Moving Pictures Expert Group Audio Layer 3. An MP3 audio file is a lossy compression file format to approximately 10% of normal digital audio file size. Sounds that are not normally audible to most people are reduced in amplitude to achieve this compression standard.
MPEG	.mpg or mp2	MPG – Moving Pictures Expert Group. MPEG is a lossy compression format used for audio and video information. Different versions of the standard are available with MPG files used for short video clips and MP2 files used for high-resolution movies.

Internet Research Tasks

Check out the following YouTube videos about the Internet and DNS:

How the Internet works:
www.youtube.com/watch?v=Jj6EHgSsx_U
www.youtube.com/watch?v=Zq9bYizXVkI

How DNS works and DNS Made Easy:
www.youtube.com/watch?v=2ZUxoi7YNgs
www.youtube.com/watch?v=E7mNcgqQcPw

© ZigZag Education, 2013