Different Types Of Network

A computer **network** is formed when a group of computers are connected or linked together. Networks are usually set up to allow users to communicate electronically, share data, share peripherals and provide security and up to date information.

Computers that are not networked together are called **stand-alone** computers.

There are many different types of networks.

Local Area Network (LAN)

A **Local Area Network** is a network of computers that are all situated close together for example in a room or building. Since the distance between computers is relatively small wire cables are frequently used to connect the computers together. LANs are usually set up to allow users to share data, communicate and share expensive peripherals. A **fileserver** is used within a LAN to store data centrally. The fileserver is a powerful computer with a large amount of internal memory (RAM), fast processor and large amount of backing storage. Each authorised user of the network can use the fileserver to save data.

The **network manager** or **administrator** (the person responsible for the running of the network) has to set up a username and password for each user of the network. This allows each user to **log on**. Each user of the network is given a folder which only they can use to store their files.

Wide Area Network (WAN)

This is a network of computers connected across a distance. Telephone lines, satellites or other communication technology is required for WANs to work. Most major companies need a WAN in order to communicate with other branches either nationally or internationally.

Intranet

This is a network that allows a private connection access to Internet services. This usually happens within a particular company or organisation. Authorised users only are allowed to access these services and this makes the network relatively secure. It allows secure email communication and the distribution of information similar to the World Wide Web. It can also allow companies to advertise on the Internet.

Internet

This is the most common example of a WAN. It uses telecommunications to transfer data between computers and distribute information. The World Wide Web (WWW) is a collection of information held on the Internet. The WWW is made up of millions of documents called web pages and these pages are available to any user of the Internet. The Internet can also be used to communicate via email (webmail), chat rooms, mailing lists etc. Many e-commerce companies have set up websites so customers can bank, shop, pay for travel tickets etc. on-line.

Advantages of using networks

- ***Sharing of peripherals (printers etc.)***
- ***Sharing of storage***
- ***Sharing of files***
- ***Communication between computers***

Produced by S Lambert, R Simpson and HSDU for The Cityy of Edinburgh Council, 2004

Different Types Of Network

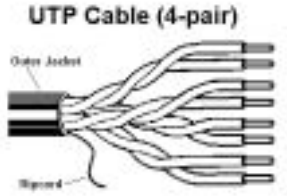
Disadvantages of using networks

- ***Too many users can slow the network down***
- ***Server crashes and data isn't available***
- ***No central storage***
- ***Cabling and transmission problems***

The type of network used depends upon several factors, usually:

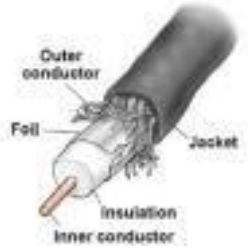
Transmission media

This allows the transmission of the electronic signals from one computer to another. There are many different types of transmission media:



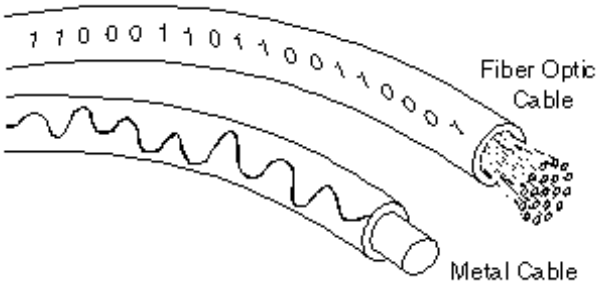
Shielded Twisted Pair (STP) – this is a type of copper telephone wiring in which each of the two copper wires that are twisted together are coated with an insulating coating that functions as a ground for the wires. The extra covering in shielded twisted pair wiring protects the transmission line from electromagnetic interference leaking into or out of the cable. STP cabling often is used in Ethernet networks, especially fast data rate Ethernets;

Unshielded Twisted Pair (UTP) - this is a type of cable that consists of two unshielded wires twisted around each other. UTP cabling does not offer as high bandwidth or as good protection from interference, but it is cheap and easier to work with;



Coaxial – this is a type of wire that consists of a center wire surrounded by insulation and then a grounded shield of braided wire. The shield minimizes electrical and radio frequency interference;

Fibre Optic – this is technology that uses glass (or plastic) threads (fibres) to transmit data. A fibre optic cable consists of a bundle of glass threads, each of which is capable of transmitting messages modulated onto light waves;



Leased Line – this is when a dedicated phone line allows network connection. Usually leased lines are used by businesses to connect geographically distant offices. A leased line is always active and as the connection doesn't carry anybody else's communications, the quality of service is usually very good;

Wireless Connection – this is when no physical cabling is used. Instead signals are usually sent by infra-red communication, laser, radio waves, microwave transmission or satellite links.

Produced by S Lambert, R Simpson and HSDU for The Cityy of Edinburgh Council, 2004

Different Types Of Network

Bandwidth

This is the amount of data that can be transmitted in a fixed amount of time or the range of frequencies that a channel can handle. Bandwidth can be given as a transmission rate. This is usually in megabits per second (Mbps) which is 1 million bits per second. Bandwidth may also be given as a frequency and this is usually measured in kilohertz (kHz).

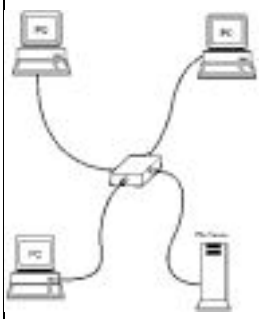
Geographical spread

This is the distance that the network has to cover.

Functions

These are the tasks that the network has to perform.

The table below defines typical factors for the different types of networks.

Network Type	Transmission Media	Bandwidth	Geographical Spread	Functions
LAN 	Coaxial cable	Typically 10Mbps	Up to 500 metres	• share data • share peripherals • communication • centrally store data
	Shielded Twisted Pair (STP)	16 Mbps up to 500 Mbps	100 metres	
	Unshielded Twisted Pair (UTP)	10 Mbps up to 100 Mbps	100 metres	
	Fibre optic	Typically 100Mbps	Kilometres	
	Wireless	Up to 54Mbps		
WAN	Fibre optic	Typically 100Mbps	Kilometres	• share data • communication • centrally store data
	Wireless	Up to 54 Mbps	Kilometres	
	Leased line	Between 10Mbps and 100 Mbps	Kilometres	

Produced by S Lambert, R Simpson and HSDU for The Cityy of Edinburgh Council, 2004

Different Types Of Network

Intranet 	Fibre optic Wireless Leased line	Typically 100Mbps Up to 54 Mbps Between 10Mbps and 100 Mbps	Kilometres Kilometres Kilometres	• share data • share peripherals • shop, bank, travel etc. • communication • centrally store data • advertise
Internet	Fibre optic Wireless Leased line	Typically 100Mbps Up to 54 Mbps Between 10Mbps and 100 Mbps	Kilometres Kilometres Kilometres	• share data • shop, bank, travel etc. • communication • centrally store data • advertise

Produced by S Lambert, R Simpson and HSDU for The Cityy of Edinburgh Council, 2004

Mainframes and Servers

Mainframe with terminals

Mainframes are very large computers which can be accessed by other computers called **terminals**. Mainframes are capable of supporting hundreds, or even thousands of users simultaneously. Terminals consist of usually a keyboard and monitor only and rely on the mainframe to carry out all the processing and backing storage required. Mainframes are generally used by huge organisations that have massive amounts of data to be stored and processed. These companies generally require central database management, for example, banks, insurance companies, government offices etc. Mainframes are usually kept in separate rooms due to security and their physical size. A mainframe computer's functions is not so much defined by their CPU speed as by their massive internal memory, high capacity external storage and reliability. These machines can and do run successfully for years without interruption, with repairs taking place whilst they continue to run.

Terminals usually consist of just a keyboard and a monitor. The mainframe is responsible for doing all the "work" that the terminal needs processed.

Advantages

- cheap to buy

Disadvantages

- have no processing power or backing storage of their own
- if mainframe crashes or goes down the terminal is deemed useless

Network Of Computers

Most computer networks have stations that can work efficiently on their own without the aid of a mainframe. These networks usually consist of desktop computers being linked together. **Servers** are used to carry out various tasks across the network. There are many different types of server:

File server

This provides a central disk storage area for any users across the network. The file server stores users files separately. Users can then access their files from any workstation on the network;

Web server

This computer deals with web pages across a network. Every web server has an IP address and possibly a domain name. For example, if you enter the URL http://www.yahoo.com/index.html in your browser, this sends a request to the server whose domain name is yahoo.com. The server then fetches the page named index.html and sends it to your browser;

Print server

This computer allows the management of printing across the network. It uses a spooler to store users' files and can provide a queuing facility with prioritising if necessary;

CD-ROM server

This server allows all workstations across the network to obtain data from CD-ROM disks;

Mail server

Mail servers move and store mail over networks and across the Internet. When you send an email it is sent to the server that then processes it and sends it to the recipient;

Application server

This server runs one or more applications that can be shared by workstations.

Produced by S Lambert, R Simpson and HSDU for The City of Edinburgh Council, 2004

Peer-To-Peer and Client Server Networks

Peer-to-peer

This network is generally easy to set up, operate and maintain. This is a type of network which each workstation has equivalent capabilities and responsibilities. Each computer on the network has equal status. Any station can make its resources available to the rest of the stations on the network. The decision to share resources and what they are is taken by the user currently working on that station. There is no central control over resources. Usernames and passwords and access rights of shared files can be set up, but it is not a secure network.

Client server

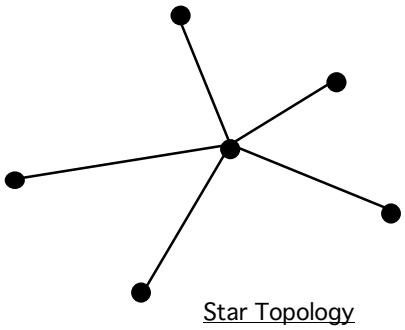
This network is does not have stations with equal status. Basically a workstation is either a **client** or a **server**. A server is a computer that carries out various jobs across the network. A client is a computer that is connected to the network. A user works on this computer in order to carry out tasks on the network and access the servers. A user is allocated privileges that permit access to some of the resources on the servers and deny access to others. A user logs onto the server using a username and password. The server then authenticates (checks) that the user is authorised to use the network and sets appropriate access privileges. A **network administrator** or **manager** is usually responsible for setting up users and allocating their access rights.

Network Type	Advantages	Disadvantages
Peer-to-peer	• No need to pay for servers • No or little network congestion due to smaller number of users • Network can still function if any clients fail to work on the network	• No central storage of files • Security across the network is poor since it is not centrally controlled • Backups of network data is difficult since there is no central storage • Each client on the network has equal rights
Client server	• Backups of data stored on servers can be carried out regularly • All shared files are stored on servers which means data is up to date and correct • Security is controlled more easily due to the central storage of data and setting up of users' access rights	• Servers can fail and hence stop data, applications etc. being shared across the network • Servers are expensive to buy • Due to the number of users network congestion is likely

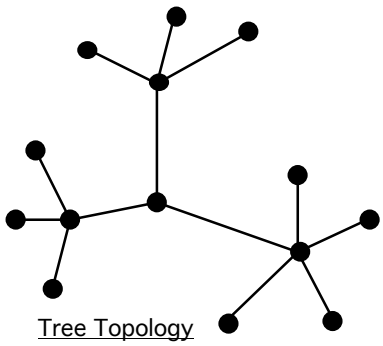
Produced by S Lambert, R Simpson and HSDU for the City of Edinburgh Council, 2004

Network Topologies

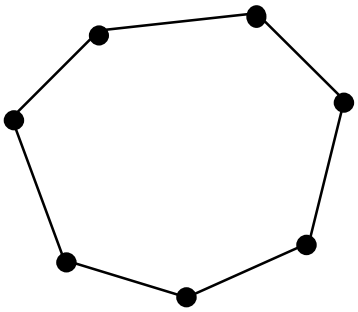
Networks can be arranged in different ways. The design of a network is called its topology. There are 5 main types of networking design. These are bus, star, ring, tree and mesh. How their topologies are arranged are shown below:



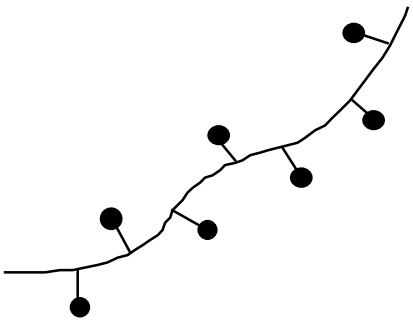
Star Topology



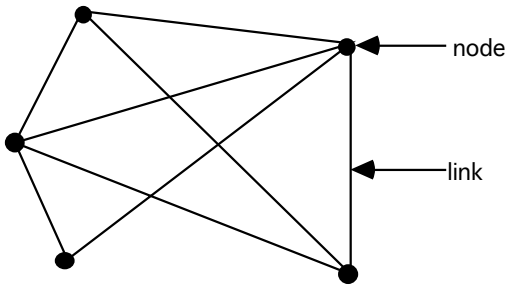
Tree Topology



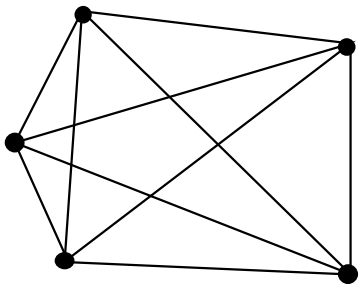
Ring Topology



Bus Topology



Mesh Topology



Fully Connected

Node (computers within the network)

links or channels to connect nodes together

Produced by S Lambert, R Simpson and HSDU for The City of Edinburgh Council, 2004

Network Topologies

Characteristics of Different Network Topologies
The table below highlights some of the characteristics of different network topologies.

Type Of Network	Advantage	Disadvantage	Affect On Performance
Mesh (WAN)	Fault in one cable doesn't affect whole network. Data is rerouted.	Lots of cabling required. Expensive.	Excellent peformance.
Tree (WAN)	Multiple transmissions can occur at the same time. Local central nodes support cluster of outer nodes. This reduces the number of links to the central node.	Lots of cabling required. Expensive.	Excellent performance.
Bus (LAN)	Fault in one node does not affect the rest of the network. Very easy to expand. Cheap.	All nodes use the same line (backbone) and hence contention occurs.	Instant access but high rate of data crashing.
Ring (LAN)	Control system in charge of transmission. Nodes guaranteed access to transmission.	Additional expense for control software and control system. Nodes may have to wait their turn to transmit data.	Network rarely fails to data crashes.
Star (LAN)	Short path between two nodes.	Fault in central node means whole network is unusable.	Central node gives more robust network, but slows down communications between nodes as data always has to pass through central node.

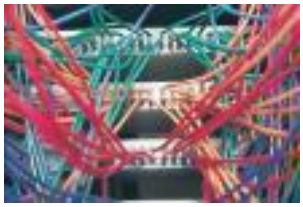
Produced by S Lambert, R Simpson and HSDU for The City of Edinburgh Council, 2004

Network Hardware

Certain hardware devices are necessary to enable a network to function properly.

Network Interface Card (NIC)
This is an expansion board that can be inserted into a computer so the computer can be connected to a network. Most NICs are designed for a particular type of network although some can serve multiple networks. A common NIC is an Ethernet card that allows a computer to be connected to an Ethernet network.

Hub
This is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. The function of a hub is simply to extend the distance between nodes on the network.



Switch (switched hub)
This device filters and forwards packets (parts of data) between LAN segments. A switch splits the network up into a number of different parts, usually to help avoid collisions within the network. These are called **collision domains**. A collision in one domain will have no effect on network traffic in another collision domain.

Router
This device forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at **gateways**, the places where two or more networks connect. A router creates or maintains a table of all the available routes around the network and uses this table to determine the best route for any given packet of data.

Bridge
This device connects two local area networks, or two segments of the same LAN that use the **same protocol** (an agreed format for transmitting data between two devices), such as Ethernet . Sometimes LANs are divided up into smaller networks to reduce the traffic of data and avoid collisions. These separate networks can be connected using bridges. This enables the traffic of data to be localised to a smaller network and reduces the number of collisions.

Repeater
When data is send across a large distance within a network, the signal can deteriorate as the distance increases. This may cause data to be incomplete or corrupt when it arrives at the receiving node. Therefore the data is sent to an intermediate node (a repeater) which boosts the signal. Every packet that arrives at a repeater is retransmitted across the network.

Produced by S Lambert, R Simpson and HSDU for The City of Edinmburgh Council, 2004

Widespread Use Of Networks

The advantages of users having their computer systems networked, in particular, to the Internet, have encouraged a computer sales boom. Users can now invest and shop on-line, keep in touch with friends and relatives cheaply and frequently, enjoy multiplayer games, surf the vast resources of the Internet and so on. The main reasons for having networked computers are:

- § simultaneous high speed Internet access using a single ISP account
- § peripheral sharing
- § sharing files and applications
- § entertainment

Due to user demand for on the spot information, most computer systems are now manufactured with network capabilities. It does not matter what the computer system may be, whether it be desktops, laptops, palmtops etc. The development of networks can be explained by many different factors including economic and social, however the most crucial is the technical factors that are involved.

Some of the results of these technical developments are:

- advances in computer technology
- new data transmission media and techniques
- improved quality of networking software
- establishment of communications standards
- adoption of Internet technology.

There have been many advances in computer hardware and software over the years that have allowed networking to be increasingly widespread within computer systems.

Advances In Hardware

Hardware prices have dropped, available network speeds have accelerated, and signal attenuation and noise problems have been addressed using low cost, high performance signal processing. The majority of computer systems have a typical system specification that can cope with most network functions. Computer systems can now process, store and deal with large amounts data very quickly. Even a low specification computer can now work as a server across a network. This is mainly due to advances in:

- q **processors (typically 2GHz and beyond)**
- q **RAM (typically 1Gb and beyond)**
- q **backing storage (hard disk capacity typically 40Gb)**
- q **data transfer rates**

  When networking first started only text data was processed across the network and the bandwidth didn't need to be very high. Today networks have to deal with all media types such as text, video, graphics, sound and animation. The bandwidth of a network has to be high in order to deal with this memory intense data. The table below shows three different networks and the typical bandwidth of each.

	Dial up	**Ethernet**	**Wireless**
Speed	100 Kbps - 10 Mbps	10 Mbps - 100 Mbps	700 Kbps - 11 Mbps

Produced by S Lambert, R Simpson and HSDU for The City of Edinburgh Council, 2004

Widespread Use Of Networks

Advances In Software

Software prices have generally risen dramatically over the last 10 years. However the majority of computer systems are now equipped with system software that supports networking and have a variety of browsers installed. These items of software have improved dramatically over the years and support networking as standard. There have also been improvements in communications software and network operating systems. Typical networking software is:

- **browsers (Internet Explorer and Netscape Communicator)**
  These allow users to surf the Internet i.e. to locate and display Web pages.

- **operating systems with networking functions (Windows XP, Mac OS X, UNIX)**
  These stand alone operating systems can allow networking functions to be carried out.

- **network operating systems (Windows Server, Mac OS X Server, Novell Netware)**
  Typical tasks involve encryption of data, authenticating users, setting privileges and access rights etc.

- **communications software**
  This software controls networking cards, encodes and manages the flow of data.

Although hardware and software capabilities have improved other aspects of networking need to be catered for.

The need for higher bandwidth

When networks were first introduced much of the information that had to be dealt with was textual or binary. Therefore the bandwidth required for file transfer was quite low. Nowadays most networks need to deal with larger non text files and so the file sizes become larger. Users really want to work with multimedia data so networks have to cope with not only text but still images, audio and video clips as well.

The addition of more users on any network, for example on the Internet, causes the traffic within the network to increase substantially. Another example is if users are sending e-mail, these small packets add up quickly and require more bandwidth or the mail will be delayed. Also if the users are clients accessing servers, as on the World Wide Web, that also adds more traffic, especially if much of the traffic is graphics, video and audio.

Wireless communications

Wireless networks use electromagnetic airwaves, either infrared or radio to communicate information from one point to another without relying on any physical connection.

Some wireless networks can be implemented using PCMCIA cards in notebook computers, PCI cards in desktop computers, or integrated within hand held computers. Adapters provide an interface between the client network operating system and the airwaves (via an antenna).

In 1999, Apple sparked the wireless revolution with the introduction of AirPort, the first affordable and easy to use solution for accessing the Internet without restrictive cables. Apple's AirPort Express continues to advance wireless technology, delivering the first device to pack wireless networking, audio, printing and bridging capabilities into a single affordable, portable unit. Bluetooth is also a widely used technology to connect devices without wires. It provides short range connections between mobile devices and to the Internet via bridging devices to different networks (wired and wireless) that provide Internet capability.

Wireless technologies allow more flexible use of applications and devices. With the number of mobile users continuing to increase, this flexibility is even important than ever.

Produced by S Lambert, R Simpson and HSDU for The City of Edinburgh Council, 2004

Misuse Of Networks

Due to the nature of using large quantities of data across a network, it is important that this data is not abused. There are various ways that networks can be misused for illegal purposes.

Breaching copyright
This is when some users deliberately:

- steal other people's intellectual property ;
- use other people's computer based resources without their permission;
- copy or use software that has not been paid for.

The purposes of copyright are:

- to allow authors/creators of materials to control use of their work by other people;
- to allow creators to gain economically from their work, thereby encouraging creativity and developments which will benefit society as a whole;
- to give creators moral rights to be known as the author of their piece of work.

Copyright is an important but confusing issue, particularly in relation to electronic and web-based material. The Internet for example is allowing more and more people to become authors and create and publish original pieces of work. It is also allowing easier and quicker exchange of information. However, this in turn has increased the opportunity for copyright breaching, either intentionally or otherwise.

Hacking
This is what happens when someone who breaks into someone else's computer system, bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security. The end result is whatever is on the computer can viewed and sensitive data stolen without anyone knowing. Sometimes, tiny programs are 'planted' on the computer so that they can watch out for specific types of data, seize the data and then transmit the data to another computer.

Planting Viruses
Some network users deliberately install viruses on computer systems in the hope that they will cause havoc across a network. Viruses are developed with an intention to cause damage to computer files, or cause inconvenience or annoyance. The virus usually occupies the first few instructions of a program and starts when the user executes the program. When executed the virus runs in the first sequence and usually copies itself on the hard drive somewhere in the operating system code. The virus can then continue to run doing whatever damage it was written for. Some viruses lie dormant waiting for a trigger, some do a set of instructions each time the computer is running and these build up in time to e.g. filling up the available space on the hard drive, some will format the hard drive wiping all data. A 'logic bomb' is a virus waiting to start executing given a certain trigger, or a failure to cancel.

A computer system can catch a virus by launching an infected application or starting up your computer from a disk that has infected system files. Once a virus is in memory, it usually infects any application that is run, including network applications (if the user have write access to network folders or disks). For example, a virus may be designed to conceal itself until a predetermined date, then flash a message on all network computers. However, a properly configured network is less susceptible to viruses than a stand alone computer.

Produced by S Lambert for the City of Edinburgh Council, 2004

Misuse Of Networks

There are various laws that have been passed to help prevent illegal use of networks.

Computer Misuse Act
Three specific computer misuses covered by the Computer Misuse Act of 1990 are: unauthorised access to computer programs or data, unauthorised access with a further criminal intent, unauthorised modification of computer material i.e. programs or data.
Some of the crimes are:

- deliberately planting viruses into a computer system to cause damage to program files and data;
- using computer time to carry out unauthorised work;

- copying computer programs;
- hacking into someone's system with a view to seeing or altering the information.;
- using a computer to commit various electronic frauds.

Copyright Designs and Patents Act
The Copyright, Designs and Patents Act of 1988, makes it illegal to:

- copy software;
- run pirated software;
- transmit copyrighted software over a telecommunications line.

Licences are bought from a software company in order to legally run software. There are limitations for multiple users and special licences have to be bought for running the software on a network.

Data Protection Act
The aim of the Data Protection Act 1998 is to protect the rights of the individual about whom data is obtained, stored, processed or supplied rather than those of the people or organisations who control and use personal data. The Act applies to both computerised and paper records. Data users have to notify the Office of the Information Commissioner of the information held and its uses.

Across a network with many users, data users must ensure that they provide proper security. This could be done using:

Secure rooms
Making sure that servers containing sensitive data are under locked away in a secure area. A room that has no windows, secure doors, a burglar alarm and limited access to keys should be suitable.

Usernames and passwords
If an unauthorised person does break into the building and any secure area it would be useful if the network will only accept authorised users. i.e. users who are known to the system and given limited access. This can be done by giving authorised users identification names and passwords.

Produced by S Lambert for the City of Edinburgh Council, 2004