ALL SAINTS SECONDARY SCHOOL

BUSINESS STUDIES AND ICT DEPARTMENT

Computing Studies
Higher

Networking

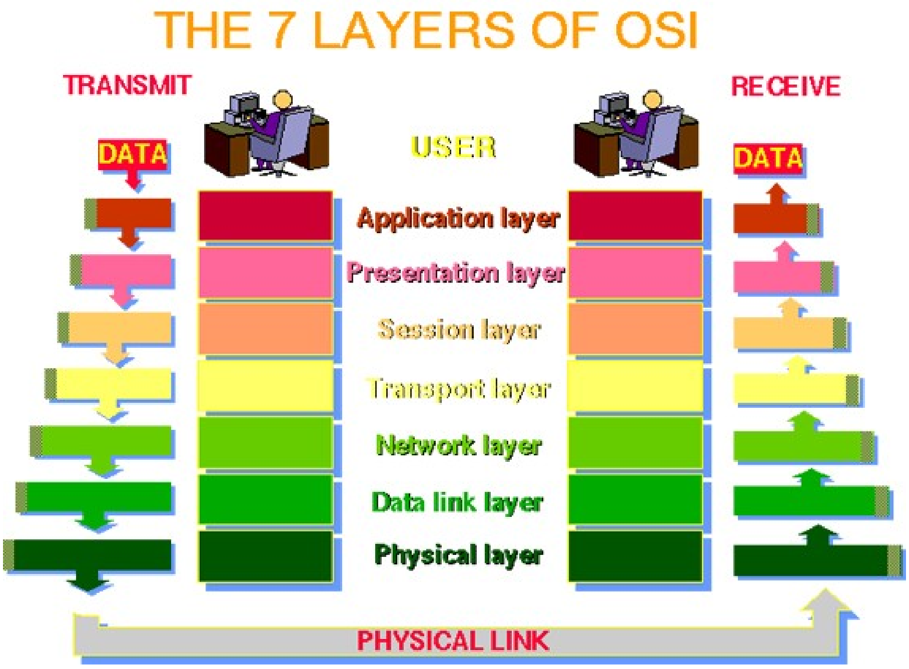
SECTION 1

Protocols and Standards

Arrangements:

Network protocols

1. Name and description of the seven layers of the OSI model
2. Brief explanation of the purpose of common protocols (TELNET, HTTP, FTP, SMTP)
3. Description of an IP address (structure — 4 octets, classes — ABCD, limitations)
4. Description of Name services (name resolution); DNS (domain names, host name resolution)



A **protocol** is an agreement for the transmission of data. Without protocols internetworks could not function. If one network is using ASCII and another EBCDIC, one transmits at 10Mbps, the other at 100Mbps, one uses data packets 256 characters long, the other uses 512 characters and so on, then it would be impossible to communicate.

> *A protocol is an agreed set of rules between two computers on how data will be transmitted*.

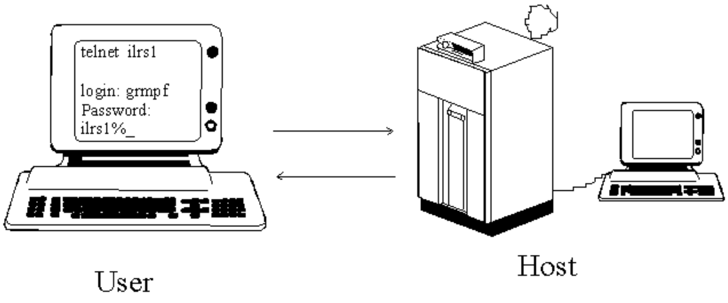
The data format, the packet size, the transmission speed, even the voltages for 1s and 0s are all protocols.

When two computers 'meet' on a network they HANDSHAKE.

A handshake is when they agree the protocols. Once this is set up they can communicate.

Common protocols:

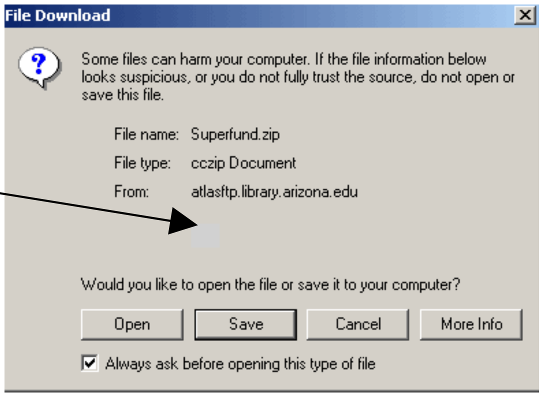
TELNET: This is a very old protocol for connecting two remote computers. *TELNET lets you log on to another computer and then use it as if it were your own*. TENET has a command driven interface and apart from login and password has no security. TELNET is little used nowadays but is useful for network technicians for monitoring hubs, switches, print servers etc.



```
telnet ilrs1

login: grmpf
Password:
ilrs1%_
```

FTP: *File Transfer Protocol is for moving a file across a network*. Whenever you download you are using FTP. You usually see ftp in the address instead of HTTP.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: Superfund.zip

File type: cczip Document

From: atlasftp.library.arizona.edu

Would you like to open the file or save it to your computer?

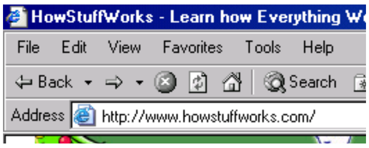
☑ Always ask before opening this type of file

HTTP : *HyperText Transfer Protocol is for transferring web pages across a network.* Each page has a URL (Uniform Resource Locator) to uniquely locate it. The pages are written in HTML (HyperText Markup Language)

URLs have 3 (or 4 parts):

HTTP : // mearnscastle.sch.uk./computing/higher/networks.htm

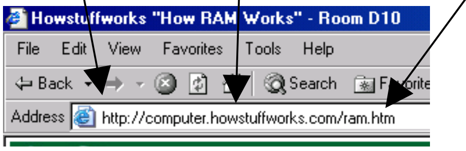
protocol // domain name / (path and) filename
(server)



HowStuffWorks - Learn how Everything W

http://www.howstuffworks.com/

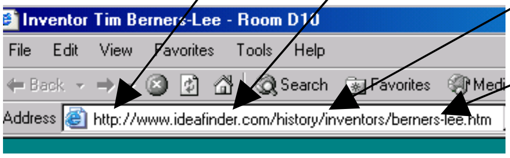
protocol // domain name / (path and) filename



Howstuffworks "How RAM Works" - Room D10

http://computer.howstuffworks.com/ram.htm

This one has protocol, domain name and full pathname to the page.

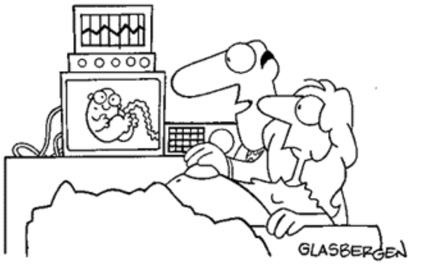


Inventor Tim Berners-Lee - Room D10

http://www.ideafinder.com/history/inventors/berners-lee.htm

Email protocols:

SMTP: *Simple Mail Transfer Protocol is for sending email across a network.* Originally everyone was always on-line and an email was sent directly from one computer to another. The idea of 'logging on' to your email came later and needed another protocol:



"Your baby is developing very nicely. Would you like to send him an e-mail?"

POP: *Post Office Protocol is for receiving email*. Your email is stored by an email server. You log on and it is forwarded to you. Called a '*store and forward'* system. We now use version 3 (POP3)

Email addresses have 2 parts separated by the @ sign: *username@domainname*

(MIME: Multipurpose Internet Mail Extensions is for coding attachments as ASCII. All email is sent by SMTP in ASCII, so a new protocol was needed for attachments. MIME takes say a JPEG picture, sends the information that it is jpeg, sends the graphics' bits in groups of 8 as if they are ASCII and at the other end MIME re-assembles the picture.)

Internetwork Protocols

TCP/IP : Transmission Control Protocol / Internet Protocol. These are very important and will come up again later.

Basically TCP breaks transmissions down into packets, so a 1 Meg file might get split into 512 packets each 2Kb long. IP routes these packets to their correct destination (the IP address).

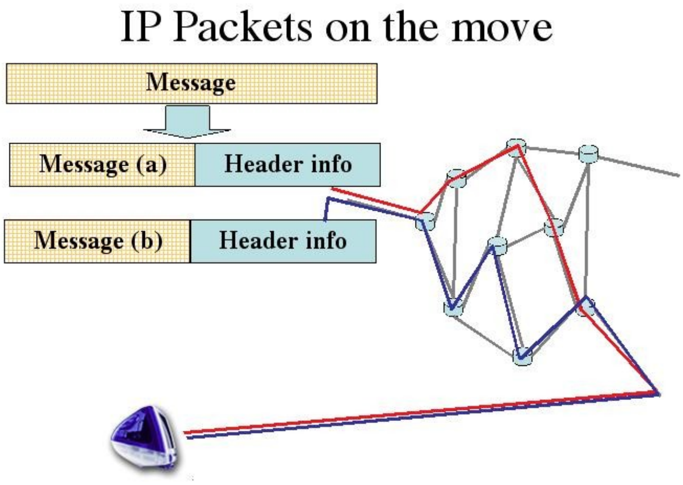
When TCP splits the data into packets it adds a header. This header contains some information about the packet and in particular a sequence number. When each packet is received an acknowledgement is sent back. If an acknowledgement is not received for a packet then TCP re-transmits it.

IP adds the sender and destination addresses to the header allowing the packet to be correctly routed.

Transmission Control Protocol breaks data down into packets and ensures they are delivered.

Internet Protocol routes the packets through the network.

A message is split into packets (a, b, c, etc), the header is added to each packet and they are routed to their destination:



The packets can follow any route, if one way is busy they branch off another way. Routers are very 'intelligent' at doing this.

The header has a sequence number so the packets can be arranged into order at the other end. The sender address is in the header so an acknowledgement can be sent. If an acknowledgement is not received, the packet is retransmitted.

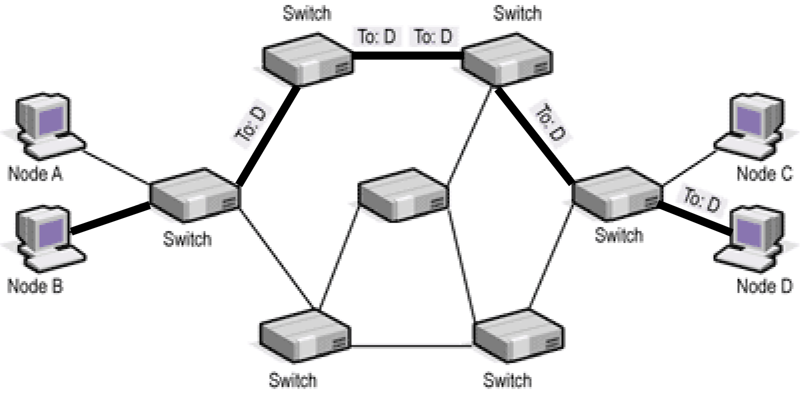
Packets get lost on the web all the time.

Exercise 1

1. What is a protocol?
2. Give an example of something that would be agreed by a protocol.
3. What is *telnet* used for?
4. Which protocol is used for a) transferring files and b) transferring web pages across the Internet?
5. Name the 3 protocols used in email and explain what each is for.
6. What does TCP/IP stand for?
7. What is the job of a) TCP and b) IP?

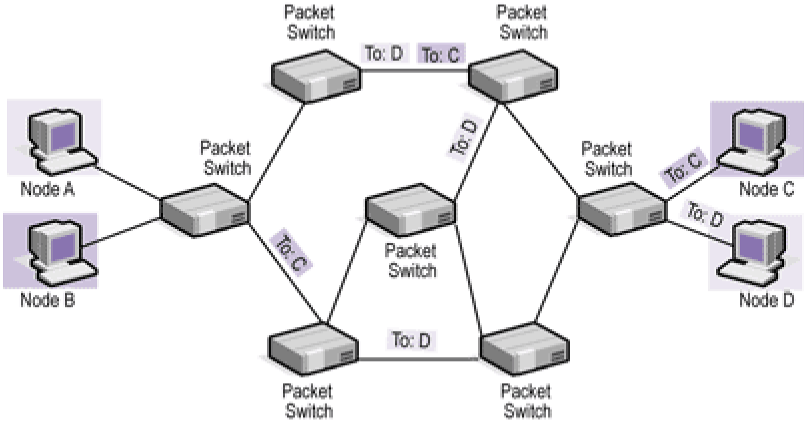
This splitting up of data into packets was very important in developing internetworks which use phone lines for data transmission. To understand this you must realise the difference between **CIRCUIT SWITCHING** which is what happens when you make a phone call and **PACKET SWITCHING** which is what happens when you use a Wide Area Network.

In circuit switching, when you phone someone there is an **actual physical connection** between you and the other end of the line. If you can imagine your phone wire as a pipe, then it would be possible to pour water down your microphone and it would come out the speaker at the other end.



Here B is sending data to D using circuit switching. B and D are physically connected and nobody else can use those lines while they are connected. 90% of the time the line will not be getting used as data transfers very quickly, so circuit switching is wasteful, in fact we couldn't have WANs this way.

In packet switching you are NEVER CONNECTED. The data is sent in small packets by all sorts of different routes and arrives in any old order where it is re-assembled into the original data.



Here node B is sending to D and A is sending to C. Packets can travel by all sorts of routes to their destination. No connection is ever made between the nodes. This is how the Internet works.

IP addresses

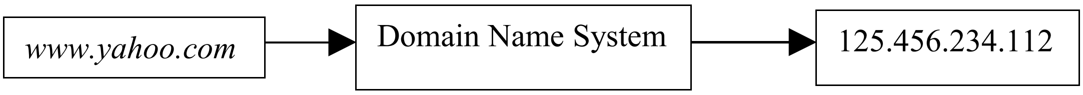
The IP address is a unique identifier for computers on an internetwork. It is 32 bits long (*this gives > 4 billion addresses*). These 32 bits are split into 4 'octets'. As each octet is 8 bits, then the range in decimal is 0 –255 and this is how we write them rather than 32 bit binary.

So IP addresses look like this:

126.34.118.4 or 255.255.32.127 or 64.0.112.37

312.15.93.87 cannot be an IP address because 255 is the maximum.

When you type in *www.yahoo.com* that name goes to a DOMAIN NAME SYSTEM (DNS) running on your ISP's server, which translates it into the 32 bit IP address. This is then used to route your request to the Yahoo server.



These Domain Name Systems are like a databases of web addresses with the corresponding IP address, however it is a bit more complex than just searching for the record.

Translating the web address into the IP address is called **resolving**, it can be quite complex but basically involves breaking the address down into different levels.

Level 1 is the **.com** or **.org** or **.net** etc at the end of the address. Each of these is subdivided into level 2 and so on.

Remember there are 4 billion addresses, there has to be a way of narrowing down what you are looking for. In addition your browser will have cached recently used DNS lookups so that it can instantly resolve them.

Now that we have the IP address, how is the request routed to this address?

Classes of IP address:

The 4 parts of the IP address have specific meaning regarding the location of the computer. It splits into 2 sections. One section is the NETWORK identifier and the second section the HOST (or node) identifier. This splitting can be done in three ways:

The network could be identified by:

The first octet :	N.h.h.h	CLASS A
The first two :	N.N.h.h	CLASS B
Or the first three :	N.N.N.h	CLASS C

So when routing, the network section is used to find the network and then just the host part is used to find the computer on that network.

Since each computer on the Internet needs a different IP address, there has to be some way of sharing out the IP addresses to accommodate big companies with millions of computers, mid size companies with thousands as well as small networks.

Since there are a *small* number of *big* companies and a *large* number of *small* companies, you can allocate class A to the large organisations, class B to middle and class C to small.

Class A addresses use the numbers 0-126 in the first octet.

So there are 127 class A networks each holding 16.8 million nodes. The addresses are:

From 000.000.000.000 to 126.255.255.255

Class B addresses use 128 – 191 in the first octet, remember the first 2 octets identify the network, so their range is:

From 128.000.000.000 to 191.255.255.255 giving 16384 networks hosting 65536 nodes

Class C uses 192 to 223 in the first octet where the first three octets identify the network, this gives:

2, 097, 152 networks each with 256 hosts

So the first octet tells you right away whether it is Class A, B or C.

64.215.87.126 is Class A because 0 – 127 in the first octet is Class A.
So 64 identifies the Network
The 215.87.126 identifies the node.

223.128.255.64 is Class C (192 – 223 in the first octet).
So 223.128.255 identifies the network
The 64 identifies the node.

There are also **class D** addresses which have the first octet in the range 224 – 239 these are used specifically for multi-casting where data is sent to a group of nodes simultaneously.

Exercise 2:

Identify the Network and the node addresses from these IP addresses:

1. 23.126.201.35 2. 135.74.201.12 3. 199.56.23.12

4. Describe the structure of a class B IP address.

5. Our school has 365 computers, 86 printers, 24 hubs and switches, which class of IP address would you suggest we use?

6. What is an IP address for? What is the connection between www.myhomepage.com and 127.45.83.122?

There is a big problem with IP addresses : there aren't nearly enough. At 4 billion we have run out. Because now every 3G mobile phone needs a permanent IP address and more and more 'always on' connections need IP addresses. There are even plans for things like fridges to have IP addresses and re-order from the web!

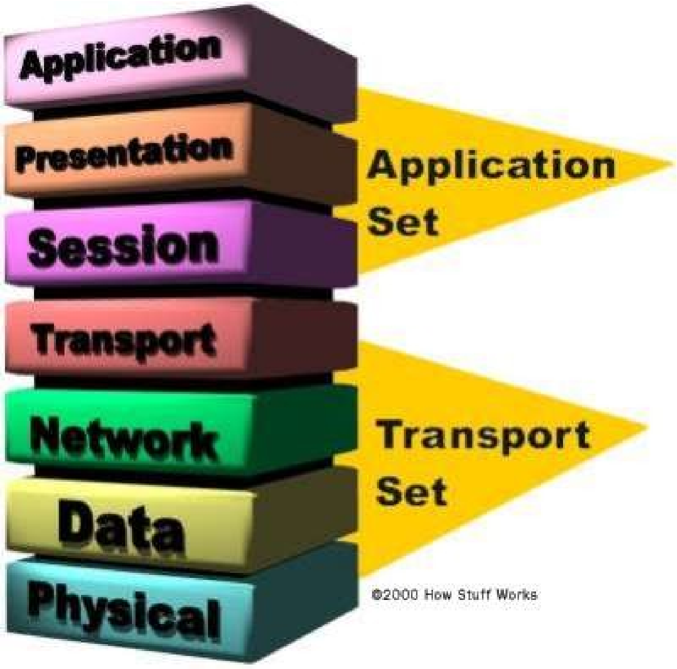
So a new IPv6 is coming with a 128 bit address. That gives a BIG number of addresses. 2^{128} is roughly 35 followed by 37 noughts (billion, billion, billion, billion)

The ISO / OSI model

The International Standards Organisation brings scientists / government representatives / company representatives together to agree common standards. For networks they produced the OSI model.

The Open System Interconnection model is an **abstract** device for setting standards in networking.

It divides data transfer across a network into 7 layers. The higher layers are implemented by software, the lower layers by hardware. The main feature is the interface between each layer that specifies how one layer communicates with another.



Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

The idea is that all manufacturers and software developers will follow the same standards so that anyone setting up a network can buy software from different companies, can buy hubs from one company and routers from another and they will all work together.

Also, of course, by following protocols and standards all the different platforms can use the Internet and communicate with each other.

<u>THE SEVEN LAYERS:</u>

7: The Application Layer

This is where programs like Outlook and Browsers operate. *This layer lets programs access network services***.**

Protocols: HTTP, FTP, SMTP etc. are defined here.

6: The Presentation Layer

Here data is converted into a standardised format. Also compression and encryption would be handled here.

Standards like ASCII, HTML operate here also the MIME protocol.

5: The Session Layer

Logging on and passwords are handled here. A 'session' is created allowing the two end users to communicate.

4: The Transport Layer

This ensures an error free connection. Data is broken into packets, at the other end packets are re-assembled into the original, acknowledgements are sent.

Protocols : TCP and UDP

(All the above run on the node you are using, the remaining 3 operate in the network).

3: The Network Layer

Here source and destination addresses are added to the packets. This is where routing takes place.

Protocol: IP Hardware : Routers

2: The Data Link Layer

Here data is packaged into frames along with error checks and receives acknowledgements that data has been received error free.

Hardware: Network interface Cards, Switches.

1: The Physical Layer

This is where the actual bits are transferred. Here the standards for cables, wireless, voltage levels etc. are set.
Hardware: Cat 5 cable, wireless etc.

An acronym for remembering the layers in reverse (7 to 1) is:

Any **P**erson **S**tudying **T**his **N**eeds **D**esperate **P**sychotherapy

There are some metaphors to try explain the model. Here is one about James Bond:
http://www.lewistech.com/rlewis/Resources/JamesBondOSI2.aspx

The OSI model is very complex and page 10 is the very minimum idea of what each layer does and which hardware or protocols operate there.

Try these references to read more about the layers:

http://www.webopedia.com/TERM/O/OSI.html

follow the links to the *breakdown of the 7 layers* and also the one to *Understanding Layers.*

http://www2.rad.com/networks/1994/osi/layers.htm

Click on each layer for more information.

http://computer.howstuffworks.com/osi.htm

EXERCISE 3:

1. Name the 7 layers of the OSI model.

2. What is the purpose of
    a. The Transport layer
    b. The Physical layer
    c. The Network layer

3. In which layer would these operate?
    a. HTML
    b. TCP
    c. IP

4. In which layer does
    a. A router operate
    b. A hub operate

5. Which common protocols operate in the Applications layer?

6. Which layer ensures data is received correctly?

7. Why are standards like the OSI model important?

SECTION 2

Network Applications

Arrangements:

-

1. Description of a web page using HTML tags (start, header, body, title, style, font size, alignment, section headers)

2. Explanation of the advantages and disadvantages of browsers and microbrowsers for use with wireless data (WAP)

3. Description of a web page using WML tags (wireless markup language)

4. Description of the methods used by search engines to build its indexes (spiders, meta-search engines)

5. Description of the advantages of e-commerce

6. Implication of fraud in e-sales payment and how it is overcome

7. Description of the social implications of networks; information rich and information poor, the family, the community and employment

8. Description of the ethical implications of networks; personal privacy and censorship

9. Description of the implications of the Regulation of Investigatory Powers Act 2000

HyperText Markup Language

HTML is a very basic page description language designed for TEXT. Modern web pages need Java, Flash, Quicktime etc. plugins in order to give the Multimedia experience of the Web today.

Commands in HTML are based on **tags**. There is a start tag with a command in angled brackets e.g <BODY> and an end task in angled brackets with a forward slash e.g. </BODY>

The start tag for any HTML page is : <HTML>

The header section that does not actually appear on the webpage is <HEAD> Inside the header section you can have various definitions of *styles* as well as a *title* definition:

The title appears on the blue bar at the top and also in the system tray.
<TITLE> A name for the page </TITLE>

A style is where you define a font / size / colour, then when you use the name for that style it will make the text whatever font etc. you specified.
<STYLE>

The main page section has the tag <BODY>

In the body section you can define individual fonts / colours / size etc:

<FONT FACE = "Times">
<FONT size = 18>

Header tags can be used to emphasise headings

e.g. <H1> A big heading </H1>

<ALIGN = "Center"> or <ALIGN ="left"> etc. will align text on the page.

HTML Example

```
=====================================
<HTML>
<HEAD>
<TITLE>
My First Web Page
</TITLE>
</HEAD>
<BODY>
Welcome to My Home Page!
<P>
This is my first web page. I'm learning the most important HTML tags.
</BODY>
</HTML>
======================================
```

A browser is a program that interprets HTML to display web pages.

Browsers are designed for full sized monitors on PCs, nowadays we can access webpages from PDAs or mobile phones. To display these we need **microbrowsers**. Also a modified language called **WML** (Wireless Markup Language).

WML is designed to deal with the constraints of small screen devices, possibly no keyboard which probably also have a slow web connection (*narrowband*). The constraints include:

1) Small display and low resolution
2) Limited user input facilities (no keyboard);
3) Narrowband network connection;
4) Limited memory and processing ability.

The last two severely restrict the ability to deal with multimedia content.

A new protocol was created to use with hand held devices to replaces HTTP. It is called WAP (Wireless Application Protocol).

HTTP retrieves pages written in HTML, WAP retrieves pages written in WML.

WML is ideal for simple small pages, short menus to choose from rather than typing in, easily read, simple screens for speed of access.

The WML page is sent in a compact binary which is compiled by the microbrowser for display.

WML pages are called cards and the cards are organised in decks. Easy navigation is provided between cards in the decks.

A WML file would look like this:

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "//WAPFORUM//DTD 1.1//EN"
"http://www.waponline.com/wml_1.1.xml">
<wml>
<card>
<p>
<do type="ACCEPT" label="preview">
<go href="#preview"/>
...
<br/>
and after that select OPTIONS and PREVIEW your message.
</p>
</card>
<card id="preview">
<p>
<do type="PREV" label="Back"><prev/></do>
You entered:
$(id) <br/> $(message)
<a href="/cgi-bin/sendwap.cgi?id=$(id)&message=$(message)&loc=test">
SEND IT HERE!</a>
</p>
</card>
</wml>
```

As you can see, WML has many of the familiar tags of HTML, the main differences are the start tags in WML as you see above, navigation is between cards in a deck. Also there is a lot less formatting commands in WML. For instance the <H1> tag in HTML has many options but only a few in WML. Finally WML is sent in a compressed binary.

See tutorial on WML
http://www.softsteel.co.uk/tutorials/wmltut/index.html

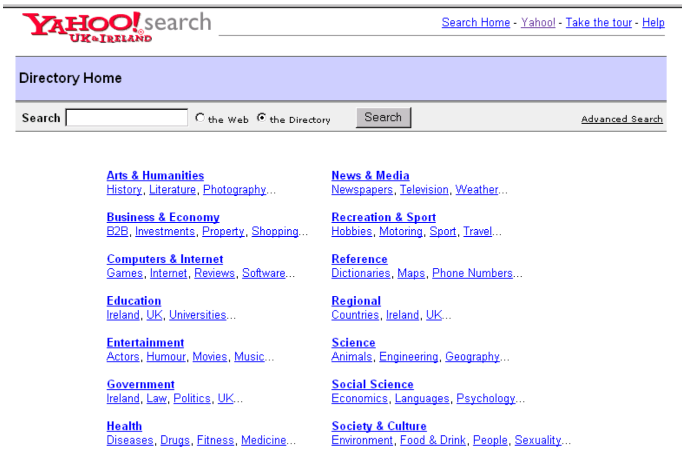
EXERCISE 4:

1. What are the tags that must appear first and last on an HTML page?
2. Describe two other tags that can be used on a page?
3. How would you make a piece of text centred on a page?
4. What language is used in microbrowsers?
5. Why do pages in this language transmit more quickly than HTML?
6. Why can we not just use HTML for microbrowsers?
7. What is the big difference between WML and HTML in the way pages are organised?
8. Give another difference between WML and HTML.

Search Engines

Everyone knows search engines and we all use Google, Yahoo, MSN etc. all the time.

There are actually two types of search. The first is a **DIRECTORY**. This provides a list of topics, you choose the topic then another list comes up and you choose from that until you narrow down what you want. Directories are created manually. These used to be very popular, but going through endless menus annoys most people and they have fallen out of favour, also of course it is a great deal of work maintaining a directory. Yahoo! was mainly a directory, but has now switched to mainly a search engine.


YAHOO! search
UK & IRELAND
Search Home - Yahoo! - Take the tour - Help
Directory Home
Search
○ the Web ● the Directory
Search
Advanced Search

Arts & Humanities
History, Literature, Photography...

Business & Economy
B2B, Investments, Property, Shopping...

Computers & Internet
Games, Internet, Reviews, Software...

Education
Ireland, UK, Universities...

Entertainment
Actors, Humour, Movies, Music...

Government
Ireland, Law, Politics, UK...

Health
Diseases, Drugs, Fitness, Medicine...

News & Media
Newspapers, Television, Weather...

Recreation & Sport
Hobbies, Motoring, Sport, Travel...

Reference
Dictionaries, Maps, Phone Numbers...

Regional
Countries, Ireland, UK...

Science
Animals, Engineering, Geography...

Social Science
Economics, Languages, Psychology...

Society & Culture
Environment, Food & Drink, People, Sexuality...

Search engines use programs called 'bots' or 'spiders' or 'web crawlers' (Googlebot is Google's web crawler, Yahoo's is called Yahoo!Slurp). These programs scan web servers for new pages and send the information back to the main database. This is how Search engines work. When you search, you are going through their database to find relevant pages.

Usually there are millions of hits for any search[1], so how is it decided which site appears at the top? Well there are always 'sponsored' links. Companies that pay to get their site displayed, but what of the rest? It

[1] There is a search engine game called Googlewhack, the object being to find a two word search that you enter into Google that returns just 1 hit.

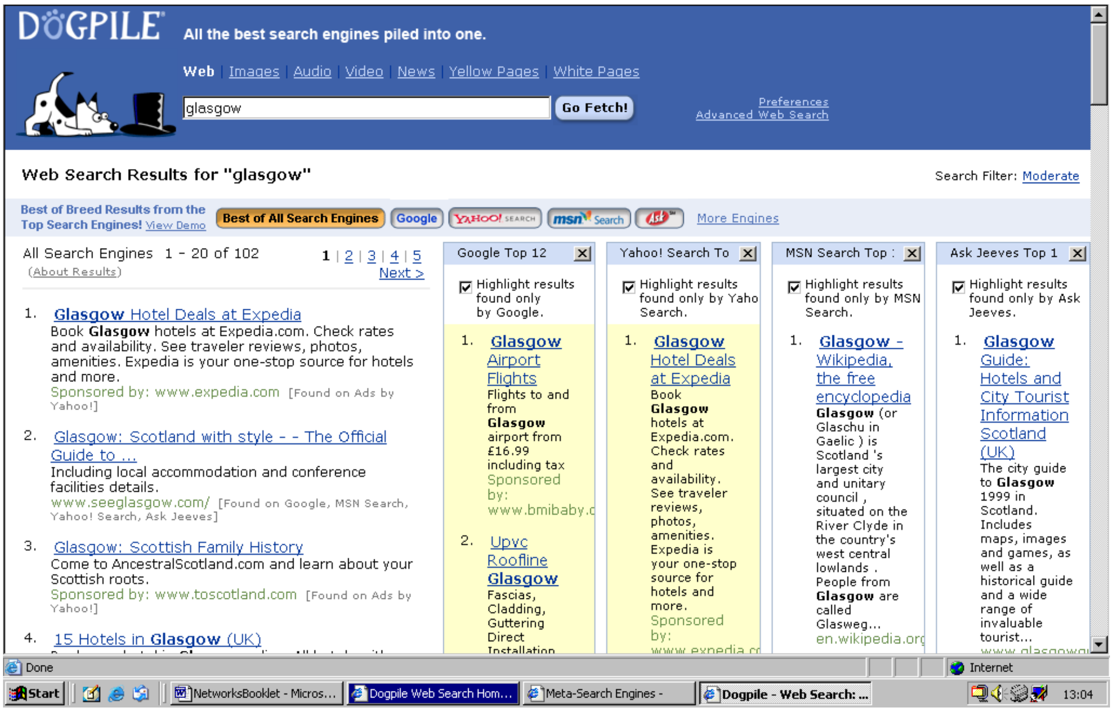
was Google that thought up a very effective method, count all the links from other pages that connect to that pages. The more links there are, then the more important that page is.

Unfortunately there are now many sites that create a multitude of dummy sites that link to them. Google employs many methods to try and stop this, but it still goes on. Yahoo rates sites on 'relevancy', it analyses the page's text, title and description and rates its relevance.

A **meta search engine** is a search engine that sends your search to a number of search engines

metacrawler®
SEARCH THE SEARCH ENGINES!®
Including Google, Yahoo!, MSN Search and Ask Jeeves. Learn More
Web | Images | Audio | Video | News | Yellow Pages | White Pages
SEARCH
□ Exact Phrase | Advanced | Preferences

The Dogpile Metasearch site is useful in that you can see the top searches from the various search engines. Here is a search for *Glasgow*:


DOGPILE
All the best search engines piled into one.
Web | Images | Audio | Video | News | Yellow Pages | White Pages
glasgow
Go Fetch!
Preferences
Advanced Web Search
Search Filter: Moderate
Best of Breed Results from the Top Search Engines! View Demo
Best of All Search Engines
Google
YAHOO! SEARCH
msn Search
Ask
More Engines
Done
Internet
Start
NetworksBooklet - Micros...
Dogpile Web Search Hom...
Meta-Search Engines -
Dogpile - Web Search: ...
13:04

Web Search Results for "glasgow"

All Search Engines 1 - 20 of 102 (About Results) 1 | 2 | 3 | 4 | 5 Next >

1. **Glasgow** Hotel Deals at Expedia
   Book **Glasgow** hotels at Expedia.com. Check rates and availability. See traveler reviews, photos, amenities. Expedia is your one-stop source for hotels and more.
   Sponsored by: www.expedia.com [Found on Ads by Yahoo!]
2. Glasgow: Scotland with style - - The Official Guide to ...
   Including local accommodation and conference facilities details.
   www.seeglasgow.com/ [Found on Google, MSN Search, Yahoo! Search, Ask Jeeves]
3. Glasgow: Scottish Family History
   Come to AncestralScotland.com and learn about your Scottish roots.
   Sponsored by: www.toscotland.com [Found on Ads by Yahoo!]
4. 15 Hotels in **Glasgow** (UK)

Google Top 12

☑ Highlight results found only by Google.

1. **Glasgow** Airport Flights
   Flights to and from **Glasgow** airport from £16.99 including tax
   Sponsored by: www.bmibaby.c
2. Upvc Roofline **Glasgow**
   Fascias, Cladding, Guttering Direct Installation

Yahoo! Search To

☑ Highlight results found only by Yaho Search.

1. **Glasgow** Hotel Deals at Expedia
   Book **Glasgow** hotels at Expedia.com. Check rates and availability. See traveler reviews, photos, amenities. Expedia is your one-stop source for hotels and more.
   Sponsored by: www.expedia.co

MSN Search Top :

☑ Highlight results found only by MSN Search.

1. **Glasgow** - Wikipedia, the free encyclopedia
   Glasgow (or Glaschu in Gaelic) is Scotland 's largest city and unitary council , situated on the River Clyde in the country's west central lowlands . People from **Glasgow** are called Glasweg...
   en.wikipedia.org

Ask Jeeves Top 1

☑ Highlight results found only by Ask Jeeves.

1. **Glasgow** Guide: Hotels and City Tourist Information Scotland (UK)
   The city guide to **Glasgow** 1999 in Scotland. Includes maps, images and games, as well as a historical guide and a wide range of invaluable tourist...
   www.glasgowg

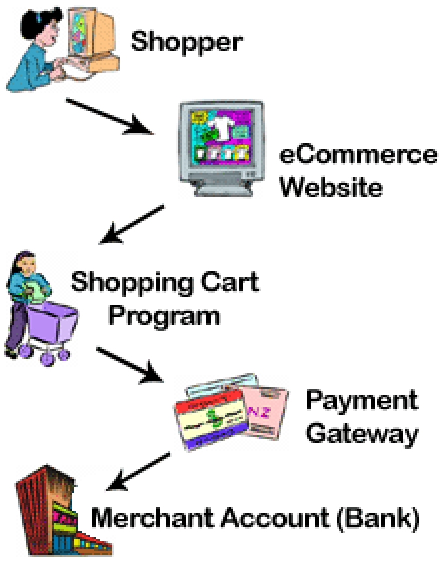
Notice how *Upvc Roofline* is number 2 in Google. This is obviously a site that has set up hundreds of dummy links to itself.

E-commerce

Shopping on the Web has become a huge business in just a few short years. There are many obvious advantages:

- Being able to compare prices very quickly without having to trudge from Dixons to PC World to Comet etc.
- Not having to travel, particularly useful for people in more remote areas.
- Saving time by getting Tesco / Asda etc. deliver weekly groceries.
- Being able to buy from abroad

www.offthemark.com
AFTER BUYING MOST OF HIS STUFF OVER THE WEB, ED GOT A BIT TOO COMFORTABLE SHOPPING IN HIS UNDERWEAR
ATLANTIC FEATURE SYND. © 1999 MARK PARISI



There are so many forms of e-commerce, some that only exist because of the web like E-bay or insurance sites giving instant quotes, U-switch telling you where to get your Gas / Electricity cheapest, i-tunes, DVDs by post.

Using e-commerce to purchase software or music on the web where the consumer downloads the product cuts out the manufacturer and the retail shop!

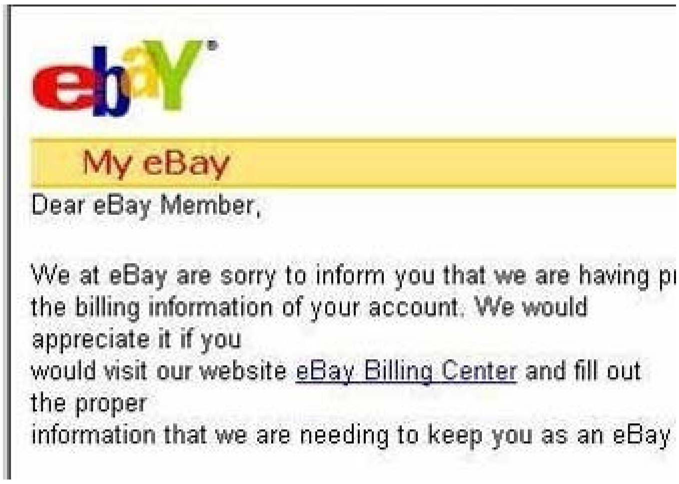
Downloading videos and TV programmes will become more common as bandwidth increases. In the future you should be able to receive all media over the web, some time-limited allowing you to rent it.

Some disadvantages of e-commerce are that retail jobs disappear, it is difficult to sort out problems when purchasing from another country and even in this country it is not as easy as taking faulty goods back to a store. Post & Packing can be expensive and finally fraud can be a problem.

CRIME

Where a lot of money is changing hands, criminals soon follow. Fraud is a danger for on-line transactions. There have been many stories of fraud on E-bay, people worry about releasing credit card details, phishing is a very sophisticated scam that has hit a lot of people.

In phishing the fraudsters set up a dummy website exactly the same as a bank's. Using spam they send out millions of emails purporting to be from that bank and so are bound to hit some of the actual customers. The emails give a link to the dummy site and entice the recipient to enter their login and password. Immediately the fraudsters use that to empty the account on the real site.



Dear eBay Member,

We at eBay are sorry to inform you that we are having p
the billing information of your account. We would
appreciate it if you
would visit our website eBay Billing Center and fill out
the proper
information that we are needing to keep you as an eBay

Similar to phishing is setting up dummy wi-fi hotspots, getting people to enter their credit card details to use the wi-fi connection and then using their credit card.

Another sophisticated scam is to set up a proxy server then install spyware on people's machines which forces every web request to go through the crooks' Proxy Server. These pages are copied to the Proxy's hard disk. At leisure the crooks can go through the web pages to see if they can obtain passwords, credit card details etc.

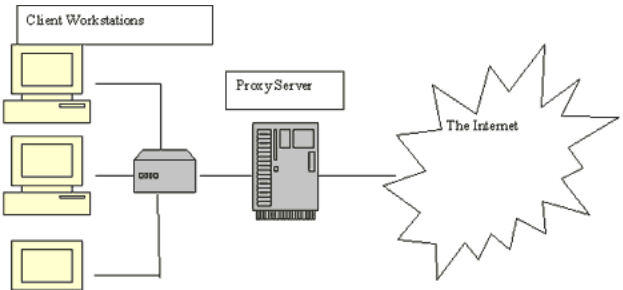


Figure 1. Network Architecture using a Proxy server

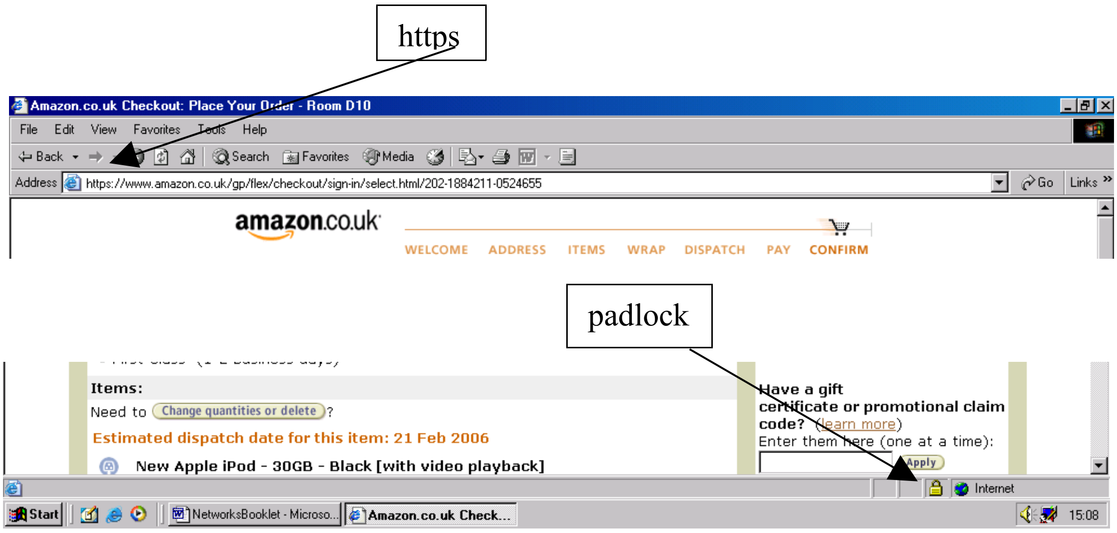
To **counteract crime** there are a number of strategies employed:

You get asked for the security number on your credit card, so that you must have the actual card, not just the number to use online[2].

Credit card firms use programs to look out for 'unusual' purchases, particularly on the web, they then phone the card holder for verification.

Companies can use secure payments PayPal like

Consumers should always check for the **https** protocol on the web page and for a **padlock** at the bottom which shows that encryption is used. Encryption means that anyone intercepting the traffic will not be able to get your details.


https
Amazon.co.uk Checkout: Place Your Order - Room D10
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
amazon.co.uk
WELCOME ADDRESS ITEMS WRAP DISPATCH PAY CONFIRM
padlock
Change quantities or delete
Apply
Internet
Start
NetworksBooklet - Microso...
Amazon.co.uk Check...
15:08

https://www.amazon.co.uk/gp/flex/checkout/sign-in/select.html/202-1884211-0524655

Items:

Need to Change quantities or delete?

Estimated dispatch date for this item: 21 Feb 2006

New Apple iPod - 30GB - Black [with video playback]

Have a gift certificate or promotional claim code? (learn more)
Enter them here (one at a time):

https is a separate protocol for transmitting web pages called SSL (Secure Socket Layer). It means all data is encrypted.

[2] When fraudsters mange to get someone's credit card number, they then phone them pretending to be from the bank and ask for the 3 figure security number 'to confirm your details'! People, very innocently tell them.

EXERCISE 5:

1. What is the difference between a search engine and a directory?
2. How do search engines create and maintain their databases of websites?
3. What is a meta search engine?
4. Many people are cautious about using e-commerce. Explain why this might be so.
5. What are the benefits to companies in using e-commerce?
6. Give an example of how fraudsters try to exploit e-commerce.
7. Give two examples of how on-line companies can try to protect themselves and their customers from fraud

SOCIAL IMPLICATIONS

Although the web is ubiquitous, we must remember that

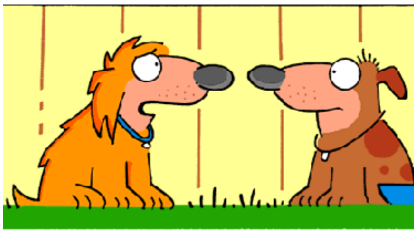
a) some people can't afford a computer,
b) some can't afford broadband,
c) many people don't have credit / debit cards and
d) even those that have a, b and c might not have the confidence / ability to use a computer effectively.

This creates a danger of dividing society into two classes **information rich** / **information poor**.

The information rich can use the web to access cheaper shopping, use ebay, book hotels/holidays at cheaper prices, use budget airlines and the multitude of services available on-line. Also there is a big push for E-government (including Local Authorities) and only the information rich will be able to access services this way. There is even the possibility that we might vote on-line in the future. Lack of IT skills also makes people less employable.

As the Web becomes more and more important, Governments need strategies to ensure that some sections of the community do not get left out causing more problems in our society.

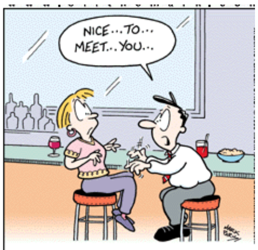
Another implication is social isolation. Years ago people knew everyone in their area. Mothers did not work, there were no supermarkets. Many people didn't have fridges. Shopping had to be done every other day, you went from shop to shop (grocers, bakers, butchers etc.).



I MET SOMEONE WONDERFUL IN A CHAT ROOM... AND THEN I FOUND OUT SHE'S A CAT!"

In each shop you queued and chatted to the other shoppers. Everyone knew everybody else.

Nowadays we go by car to the supermarket once a week. We stay in at night watching rubbish on TV, surfing/chatting on the web, playing games. Even the weekly shop is become rarer, trips up town shopping become less due to e-commerce. People can go whole weeks without meeting other people other than at work. Teleworking can mean you don't even have work colleagues! Most people couldn't name more that one or two neighbours in their street. Teenage boys can spend all their free hours playing computer games. People are frightened by crime on our streets. All this causes **Social Isolation**.



HOW TO TELL WHEN SOMEONE'S SOCIAL LIFE USUALLY DOESN'T EXTEND BEYOND THE INTERNET.

Often the only communication you have nowadays is by text and messaging, you never meet people. (Over 1 million people have used Internet Dating services, surely proof that there are limited opportunities nowadays to meet people).

Your ID:

Password:

Dear Magia Date,
I would like to thank you for your services. I have found the love of my life from your website. It's a great place to meet people without the worries or blind dates and so forth. Thanks again! More Success Stories

Country: United States

I am a: Man looking for a Woman

Age range: 18 - 24

Some information regarding special membership offers goes here.

Michael	Sandrine	Alexander	Nadin
Age 31	Age 18	Age 27	Age 23
London	New York	Sydney	Paris
UK	USA	Australia	France

If you want to be a featured member on the front page of Magia Date click here. View more photos here.

Copyright © Your Company Site layout by MAGIA Register ▪ FAQ ▪ Contact us ▪ Advertising ▪ Affiliates ▪ Privacy policy

TELEWORKING

This means working from home rather than going to an office. Modern communications, email, scanners, the web and video conferencing all make this possible for many people nowadays.

Advantages :

Employee:

- No travel time or cost
- Work times that suit you / breaks when you want
- Very useful for child care

Employer

- Don't need to provide expensive office buildings
- Can employee people in cheaper parts of the country / the world
- Happier employees

Also advantage for society, less commuters, less crowded transport, less cars on road, less pollution

Disadvantages

Employee

- Social isolation, no colleagues to meet, chat etc.
- Difficult to motivate yourself, too many distractions.

Employer

- Less control
- Don't get to know employees (who is right for promotion etc.)
- Dependant on reliability of communications / the web
- Security problems

ETHICAL IMPLICATIONS

People are always concerned with **personal privacy**. We certainly don't want others snooping on our business. With e-commerce, credit cards, mobile phones, email and so on we all leave a trail of everything we do. Every search made on Google is recorded. This can be traced back to you through the ISP and IP address. A determined government could snoop on us all. At work all emails and communications can be looked by employers and many people have been sacked because of the contents of their emails or web searches.

Cookies are left by websites that you visit on your computer, but even worse **spyware** can be planted which lets remote computers monitor your actions on-line.

Encryption can be used for payments on-line, but it is illegal to use this for email (so that the Security Services can read everyone's mail). PGP (Pretty Good Privacy) is an encryption method that is freely available, but the programmer who released it was prosecuted in America. Basically it works on knowing the KEY. If you don't have the key, you have no way of working out how the data was encoded.

Censorship has been a big problem on the web as it has no borders and what is illegal here is acceptable elsewhere. Pornography is big business online and although some of what is available on-line would be illegal here, it is impossible to prosecute. Where more serious scenes like child pornography exist then our authorities try hard to monitor and trace its use here, but are generally powerless against the provider in a foreign country. The biggest problem is of course keeping young people away from such stuff.

There are other censorship problems like libellous material, extreme right racist websites and so on which can't be removed. For instance there is a sight for pupils to comment on teachers based in America and although it contains a great deal of libellous comments, nothing can be done about it from this country.

Netiquette is the way you should behave on-line, particularly with email and newsgroups. You shouldn't spam or flame. Don't use capitals (SHOUTING). Keep messages short and to the point etc.

Some joker is going to get well and truly flamed

Other ethical considerations around the Web concern its misuse. There is the obvious like pornography and fraud, also downloading music and software without paying for it. Or setting up 'health' websites and selling quack cures. Even the sale of Viagra – mostly harmless pills – probably responsible for 50% of spam emails.

Regulations

You already know about the Data Protection Act, Copyright Design & Patents Act and Computer Misuse Act.

Other legal implications of modern networks include: Countries have to be careful with their taxation laws. Buying from abroad, where is the VAT paid? With Teleworking, employees might be in another country. Where is tax paid, N.I., which country's employment laws apply?

There is also one other act that you need to know about:

The Regulation of Investigatory Powers Act.

This gives Governments and Employers wide ranging powers to monitor employees' emails, phone calls and other forms of communication.

The Security Services can monitor anyone's Internet usage through their ISP, and can read all their emails. Employers can do likewise within the workplace.

Many people think that this is draconian and infringes on Human Rights. The Government argues that is essential for tracing paedophiles, criminals and for national security. Employers must be able to guard against viruses, industrial espionage and other misuses in the workplace. Also the Home Secretary must approve any monitoring by security services.

If any encrypted messages are used then the person must hand over the key or be imprisoned. This is also seen as reversing the burden of proof. People are innocent until proven guilty.

EXERCISE 6:

1. What exactly is meant by the term *information rich*?
2. Why would Governments be concerned about the information poor?
3. How are on-line activities making people more socially isolated?
4. Give 2 advantages to each of a) Employers and b) Employees of teleworking.
5. State 2 rules of Netiquette.
6. Why are Governments against encryption of messages?
7. What does the Regulation of Investigatory Powers Act cover?
8. Why are some people concerned about this Act?

SECTION 3

Network Security

Arrangements:

1. Description of security measures: user access rights to data — file and folder permissions, user access rights to hardware

2. Description of computer and network security requirements (confidentiality, data integrity and availability)

3. Description of threats to network security in terms of passive (monitoring of transmission) and active (modification of the data stream or the creation of a false stream) attacks

4. Description of the denial of service attack:
    a. effect: disruption or denial of services to legitimate users
    b. costs of attack: system downtime, lost revenue and labour involved in identifying and reacting to an attack
    c. intent: malicious, personal or political
    d. types of attacks: bandwidth consumption, resource starvation, programming flaws and routing and DNS attacks

5. Comparison of Internet content filtering methods:
    a. Firewalls,
    b. Internet filtering software and
    c. Walled gardens

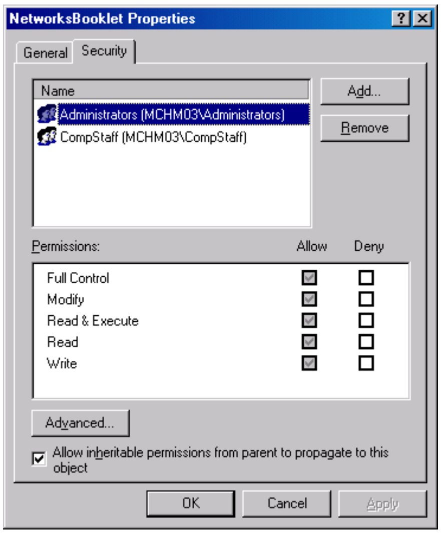
6. Description of how a firewall can protect a LAN with an Internet connection from outside attacks.

7. Description of disaster avoidance;
    a. use of anti-virus software,
    b. use of fault tolerance components,
    c. use of uninterrupted power supply,
    d. regular maintenance

8. Description of backup strategy: backup server, mirror disks, tape, backup schedule

Security is a big problem with networks. The front line is ID and password. IDs are generally available, passwords are all too easily hacked or phished. Too many people still write their password down and put it in the top drawer of their desk. Either that or they use their partner's name, child's name, favourite football player or movie star. Knowing a little about someone can easily lead to their password.

The next line in security is what data the login gets access to. Different users can be given different **access rights** on the Network determining which files they can open, whether they can just read a file or alter and save and so on. This can also be applied to whole folders and even to hardware (i.e. which printer you can access, if any).



NetworksBooklet Properties

General | Security

Name
- Administrators (MCHM03\Administrators)
- CompStaff (MCHM03\CompStaff)

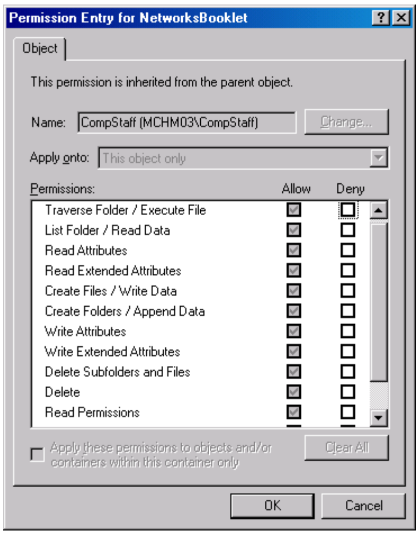
Add... Remove

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□

Advanced...

☑ Allow inheritable permissions from parent to propagate to this object

OK Cancel Apply



Permission Entry for NetworksBooklet

Object

This permission is inherited from the parent object.

Name: CompStaff (MCHM03\CompStaff) Change...

Apply onto: This object only

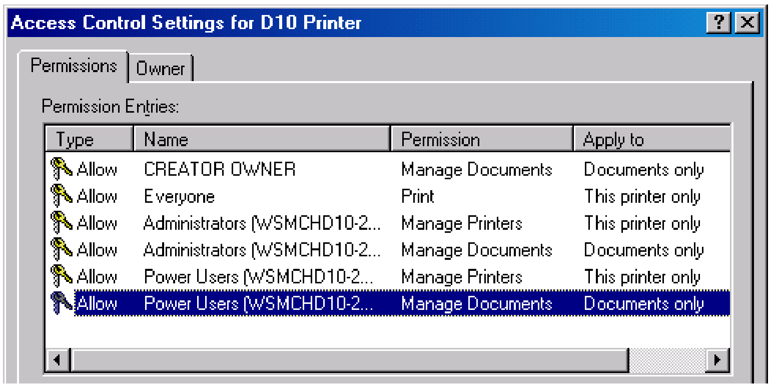
Permissions:	Allow	Deny
Traverse Folder / Execute File	☑	□
List Folder / Read Data	☑	□
Read Attributes	☑	□
Read Extended Attributes	☑	□
Create Files / Write Data	☑	□
Create Folders / Append Data	☑	□
Write Attributes	☑	□
Write Extended Attributes	☑	□
Delete Subfolders and Files	☑	□
Delete	☑	□
Read Permissions	☑	□

□ Apply these permissions to objects and/or containers within this container only

Clear All

OK Cancel

It is the Network Operating System that handles all the logins and passwords and the access rights and it is the Network administrator that determines who can do what.



Access Control Settings for D10 Printer

Permissions | Owner

Permission Entries:

Type	Name	Permission	Apply to
Allow	CREATOR OWNER	Manage Documents	Documents only
Allow	Everyone	Print	This printer only
Allow	Administrators (WSMCHD10-2...	Manage Printers	This printer only
Allow	Administrators (WSMCHD10-2...	Manage Documents	Documents only
Allow	Power Users (WSMCHD10-2...	Manage Printers	This printer only
Allow	Power Users (WSMCHD10-2...	Manage Documents	Documents only

Hardware can have access rights as well.

The main problem for networks is to make data available to everyone who needs access, while keeping confidential data that others shouldn't see (e.g. Advisor's comments on pupils).

Another problem is maintaining **data integrity**. For instance someone with full access rights opens a database file to make some changes to it. At the same time someone else wants to do the same with other changes. It would be impossible for the Networking Operating System to combine simultaneous changes (some might conflict anyway). So what happens is the first person gets access and the Network O/S denies *write* access to everyone else. The second person would be locked out from making changes.

Data integrity just means ensuring that the data is correct.

Threats to a network can comprise:

- ***passive*** (monitoring of transmission) and
- ***active*** (modification of the data stream or the creation of a false stream)

attacks.

A passive attack could involve someone intercepting the data flow and being able to read the data, thereby discovering confidential information or passwords. This can be done by 'packet sniffing' hackers and is very difficult to detect.

"Somebody has hacked into our computer, sir."

An active attack will actually modify data, destroy it, alter it, redirect it, even add false data.

A simple way to protect data is the use of **encryption**. However you slow down the network because of all the coding and decoding that has to be done.

Another security method is simply locking away the server but also having locks on workstations. Also using a switch instead of a hub is better because then the data only follows one path instead of going to everyone.

Denial of Service Attack

A **denial of service attack** is simply bombarding a server with requests or data until it crashes.
There have been many instances of DoS attacks. Once Yahoo! was put off line by a DoS attack. They are also used by blackmailers and nobody knows who might be paying to keep them at bay.

DoS attacks are a serious problem, they can knock out sites for a considerable time, very costly for an e-commerce site plus the cost of protecting the system. The attackers can sometimes just be acting maliciously, sometimes because of personal reasons to get back at a company or for criminal intent as in blackmail. There could even be political reasons e.g. Governments attacking 'terrorist' websites.

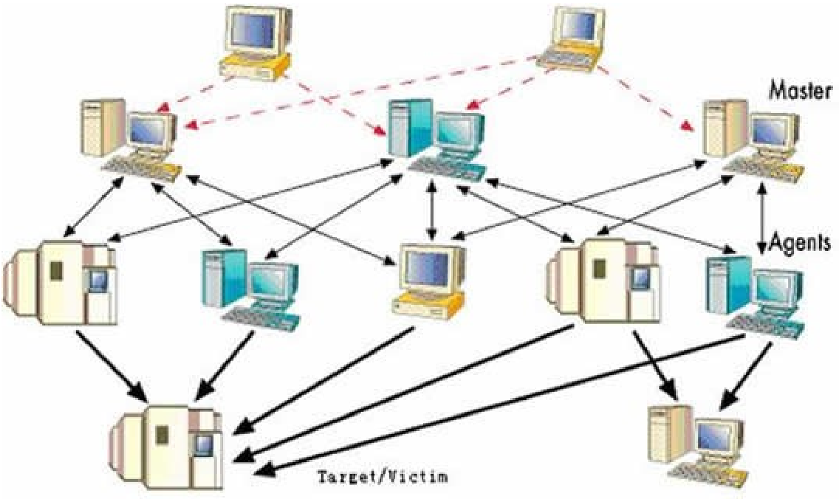
The attacks usually take the form of flooding the target with an overwhelming number of packets, a common way of achieving this is planting a program in thousands of computers then activating these programs to flood the target with requests. This consumes all the bandwidth and resources and forces it to shut down.

Bombarding a server with emails is another form of DoS attack which could also bring down a server by consuming all its resources.

The 'Ping of Death' is a form of DoS attack from about 10 years ago where a corrupted packet is sent causing a system crash. Updated Operating systems can now deal with that.

Wikopedia has a good article on Denial of Service attacks:

http://en.wikipedia.org/wiki/Denial_of_service



Here is an article from the BBC website about a DoS attack:

Alex Tew gained unwanted attention from net attacks

The site of a UK student who had the idea of selling pixels as advertising space has been hit by a web attack.

Alex Tew, 21, hit the headlines at the start of the year when he revealed his Million Dollar Homepage had made him a million dollars in four months.

But the publicity brought the unwanted attention of extortionists who knocked the site over with a massive denial-of-service attack.

> **“I haven't replied to any of them as I don't want to give them the satisfaction and I certainly don't intend to pay them any money”**
>
> Alex Tew

Police alerted

Mr Tew's encounter with the net criminals began when he received an e-mail threatening to bombard the site with data unless he paid a ransom of $5,000 (£2,800).

He did not respond and the deadline passed without incident. But the following day the site went down. More e-mails followed, upping the ransom to £28,000.

"I haven't replied to any of them as I don't want to give them the satisfaction and I certainly don't intend to pay them any money," Mr Tew told the BBC News website. Both the FBI and the Hi-Tech Crime Unit of the Wiltshire Constabulary have been notified about the problem.

"Their instinct is that this attack originates in Russia although it is not possible to track the e-mail back to its source," said Mr Tew.

"There is not much more that they can do," he added.

Instead, Mr Tew's web hosting firm Sitelutions worked to solve the problem, initially coming up with a hardware solution. It did not work because of the size of the attack.

Currently traffic to Mr Tew's website is being filtered via a US-based firm DDoSprotection.com - experts in dealing with such attacks - and that solution appears to be working.

Preventing denial-of-service attacks can be a costly business but, ever the entrepreneur, Mr Tew is hopeful he can do a deal with his new partner - offering them free ad space in return for them keeping his site up and running.

Zombie PCs

It has become common practice for extortionists to target net firms and threaten to cripple their websites with deluges of data unless they pay a ransom. So-called Distributed Denial-of-Service (DDoS) attacks overwhelm servers with requests until they are forced offline.

Computers are innocently recruited from all over the world to take part in the attack, each sending only a small part of the entire data flood. The recruiting of machines to take part in attacks is typically done by infecting them with a virus or worm. The net address of compromised machines - dubbed zombies or bots - is sent back to the criminal, who will use it to launch a DDoS.

EXERCISE 7:

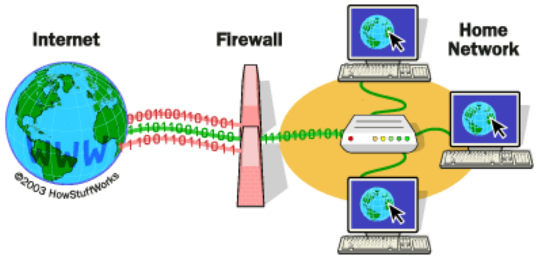
1. How can hackers obtain someone's secret password.
2. Network manager's used to insist that everyone changed their password once a month as a security measure. Why do you think this practice has fallen out of favour?
3. After the login and password, what is the next level of security on a network?
4. What is meant by maintaining data integrity?
5. How does the Network O/S ensure that data files can only be altered by one user at a time?
6. a) What is meant by a passive attack on a network?

   b) How can the Network be protected from passive attacks?
7. What is a Denial of Service attack?
8. Give an example of a DoS attack.
9. Why would a DoS attack be very serious to an e-commerce site?

INTERNET FILTERING

1. Firewall

A firewall can be hardware or software. It is liked a locked door, only those with a key can get in. It screens all the traffic going out to and coming in from the Internet.



Broadly speaking, firewalls work by checking all the traffic passing through them, blocking data which does not conform to pre-determined security criteria and allowing everything else through.

Firewalls can be set up to block specific sites or type of sites or entire parts of the internet. For example, schools might use their firewall to block all web based email and newsgroups.

On a LAN, firewalls stop anyone from outside logging onto any node in the Network. They can ban access to certain ports (DoS attacks often come in on port 139). They can be used to only allow 'trusted' sites to gain access.

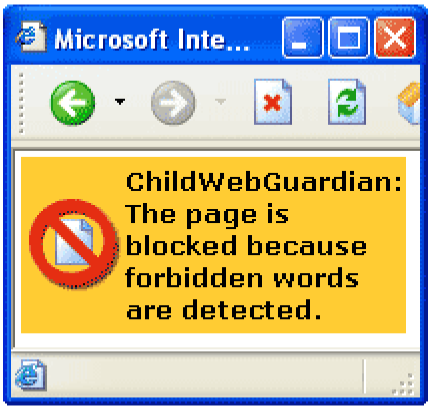
So firewalls:

Filter data from the Internet / close ports or monitor them for certain activities / keep out unauthorized users.

DON'T TOUCH ANYTHING UNTIL YOU WASH THOSE HANDS, YOUNG LADY... AND DON'T GIVE ME THAT LOOK!
DARN PARENTAL CONTROLS

2. Internet Filtering Software

This is like Parental Controls implemented by ISPs like AOL. You can get programs like *CyberNanny* or *CyberSitter* or *Norton Parental Controls* which can be set up to block unsavoury sites, lock out P2P file sharing, scan emails for certain words, monitor chat rooms and instant messaging. When the filtering system is turned on, users cannot open or link to sites that the filtering system recognises as unsuitable. Many filtering systems will also provide facilities to filter incoming and outgoing email. Basically filtering is just a list, anything on the list is blocked. Our school uses a filtering system on the Proxy Server e.g. any site with 'Shopping' in its description is blocked.



ChildWebGuardian: The page is blocked because forbidden words are detected.

3. Walled garden

A walled garden is a collection of websites that have been selected, vetted and approved for access. Users can only access these particular sites, as opposed to filtering products whereby users are allowed access to every site except those blocked by the filter. Users can usually choose whether to view sites that have not been rated.

Some ISPs undertake all the selection and vetting of sites, while others allow subscribers to supplement or amend the 'allow' list themselves. Several ISPs are also now offering subscribers the ability to create an additional 'deny' list of sites that they wish to have blocked. Some ISPs also provide password access to the Internet, allowing password holders to 'jump over' the wall.

A walled garden is like a subset of the Web where only approved sites can be accessed.

ISPs also often provide other filtering products like a pop-up blocker, spam filter, their own anti-virus product etc.

Disaster Avoidance

Networks going down can disable a business; loss of data could be catastrophic and even put a company out of business. Networks must take further steps than just filtering to protect themselves.

Filtering will not deal with viruses so in addition to a firewall and filters you also need **anti-virus software** on your network.

This must scan all incoming emails and files as they open. It must also perform full system scans whenever needed.

You have to use components **that can deal with faults** as far as possible without crashing. Power surges can disable sensitive electronic components so an **uninterrupted power supply** should be used. Fluctuations in the power supply are very common.

Large networks also use RAID storage (Redundant Array of Independent Disks) also called *mirror disks*. This just means that **all data is saved twice** on a second disk**,** if one drive goes, the system automatically switches to another.

Some companies have backup servers, or if they have a number of servers, the others can take over the job of one that goes down.

Then of course like all valuable equipment, companies need to invest in **regular maintenance** of hardware as well as utilities like disk defragmenters to keep their systems in good condition.

Most important of all is a **BACKUP STRATEGY**. There must be a regular schedule of backups A technician will be responsible for (preferably) daily backups. They will keep a number of backup tapes. Ideally a van comes round each day, takes a backup tape away to a storage depot, returning an old one for re-use). Large networks often use **incremental backups**. Software keeps track of the *data that has changed* and just backup up the changes.
Mirror disks also provide instant backup

EXERCISE 8:

1. What is a firewall?
2. How might a firewall help prevent a network from a Denial of Service attack?
3. List the main functions of a firewall.
4. Who might use Internet Filtering Software?
5. How does Internet Filtering Software work?
6. What is a Walled Garden?
7. How does a Walled Garden differ from Filtering Software?
8. List three methods by which companies might avoid their networks going down.
9. a) Why is a backup strategy important,
   b) How might one be implemented?

SECTION 4

Data Transmission

Arrangements:

1. Description of synchronous and asynchronous data transmission

2. Description of error checking in data transmission (parity and CRC)

3. Description of the process of transmitting data over a network using TCP/IP

4. Description of CSMA/CD and its implications for network performance

5. Description of network switching (circuit and packet switching) and its implications for network performance

6. Description of the application of modern wireless communication methods:
   a. WPAN — connect mobile phones, mobile computers and other portable handheld devices
   b. wireless LAN — connecting a mobile LAN
   c. wireless WAN — connection in rural and heavily built-up areas

7. Description of the speed and bandwidth of the types of Internet connections (dialup, cable modem, leased line, ISDN and ADSL)

   a. Explanation of which type of connection would be most appropriate in a given context

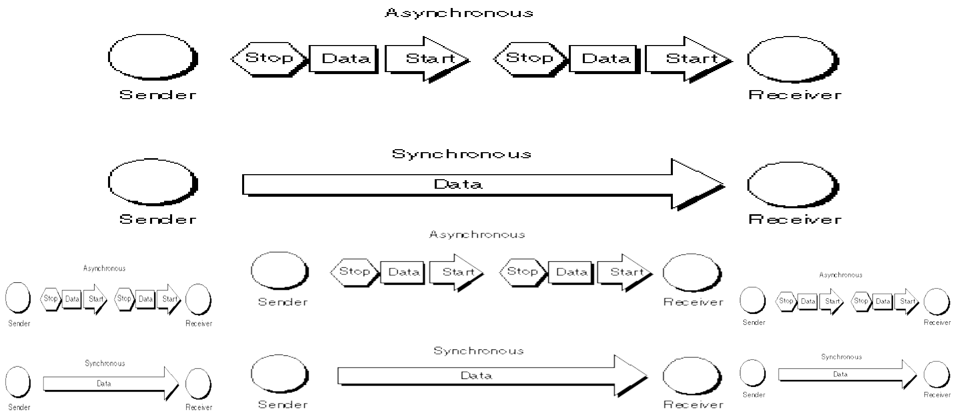
8. Description of function of network interface card

9. Explanation for the need of a MAC address when transmitting data over a network

Two methods of sending data over a LAN are called SYNCHRONOUS and ASYNCHRONOUS.

Asynchronous sends **A** letter at a time (1 byte at a time). It is for slow connections where the devices are not synchronised. Start and stop bits have to be sent with every byte.

Synchronous is where the devices are synchronised, i.e. clocks are set at the same speed. A start frame is sent to synchronise, a packet of data follows then a stop frame. This is harder to implement than asynchronous and is used with high bandwidth like 100 Mbps Ethernet LANs. A packet of data can hold a number of kilobytes and can also have error detection.



ERROR CHECKING

It is very important to check that data is received correctly on any network. A simple method for single characters is PARITY CHECK.

Remember ASCII is a 7 bit code, but computers work with bytes, so we have an extra bit. An EVEN parity check ensures the number of 1s (and 0s) is even.

Capital A in ASCII is 1000001, using even parity it is sent as 010000001

Capital B in ASCII is 1000010, using even parity it is sent as 010000010

Capital C in ASCII is 1000011, using even parity it is sent as 110000011

When the receiving computer receives a character it counts the 1s and if it is not even it knows there is an error and asks for retransmission.

You can just as easily use **odd** parity.

Note that 12.5% of all data is redundant using parity check.

For packets of data, checksums can be used for error checking where the bytes are treated as numbers, added up and a total is sent.

message	ASCII representation	
I OU1	49 4F 55 31	
0 0 . 9	30 30 2E 39	
9 BOB	39 42 4F 42	
	B2 C1 D2 AC	checksum

CRC (**Cyclic Redundancy Check**) is, in principle, just like a checksum, though like check digits, some sort of calculation is done[3] and the result is sent at the end of the packet. When the receiving computer receives the packet it does the same calculation and if it doesn't get the same answer then it asks for the packet to be retransmitted.

As packets can be a number of Kilobytes, then there is much less redundancy with CRC.

Transmission using TCP/IP

This was covered in Section 1, but is worth repeating.

TCP: Transmission Control Protocol, breaks data down into packets. It adds header information to the packet including a packet number. At the other end TCP re-assembles all the correct packets, sending an acknowledgement for each one. If an acknowledgement is not received, it retransmits the packet. So TCP ensures data is received. It also supports error detection which ensures the packets are received correctly.

IP: Internet Protocol adds the IP address (a 4 byte number) to each packet which is used to route the packets to their destination. It also adds the sender's IP address which is used to send an acknowledgement.

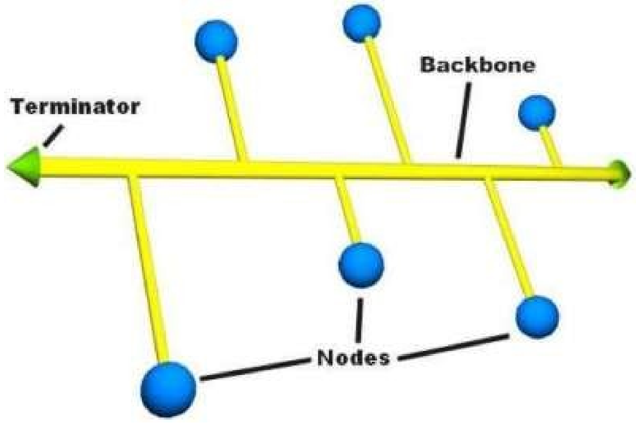
All this is done by packet switching so that you never have an actual connection between sender and receiver. In the future all land line phone calls will be by this method as well (VOIP – Voice Over Internet Protocol). IP addresses and packets are taking over all data transmission.

[3] It treats the binary digits of the entire packet as co-efficients in a polynomial … $x^7 + x^6$ etc., it divides it by a fixed polynomial which generates a remainder. The remainder is the checksum.

CSMACD

Carrier Sense, Multiple Access with Collision Detection.

On a bus network, all the nodes are connected to the main 'backbone' cable called the bus. They are all sensing the bus to see if there are any messages on it.



When a node wants to sends a message, it senses the bus is free and places its message on the bus, the message has an address header and all the nodes read the address to see if it is for them. If no node picks up the message, the terminators destroy it. **However**:

What if two nodes put a message on the bus simultaneously?

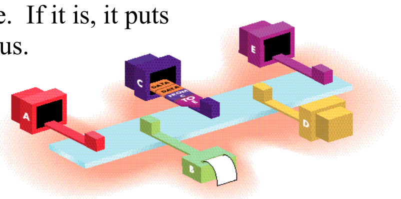
The power on the bus is doubled, so the nodes know that there has been a collision. The first node to sense it destroys the messages and the two nodes wait a random time interval before retransmitting (millionths of a second).

So CARRIER SENSE, MULTIPLE ACCESS with COLLISION DETECTION means:

Two nodes transmit simultaneously, a collision is detected. The node that senses this first sends out a signal to clear the bus. The two nodes wait a random time interval before retransmitting.

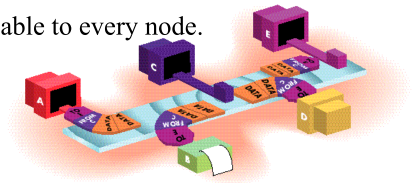
Carrier Sense: the nodes sense the bus to see if it is free. If it is, it puts its message on the bus.

1



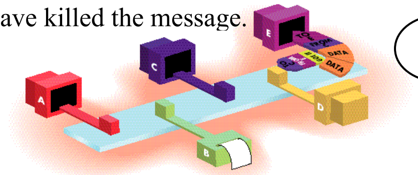
The message is available to every node.

2

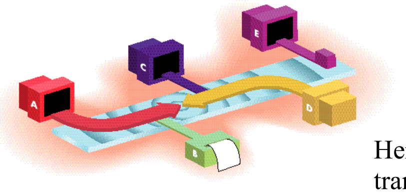


The message gets picked up by the node it is addressed to, this node sends a receipt back to the sender. If the node had been switched off, terminators would have killed the message.

3

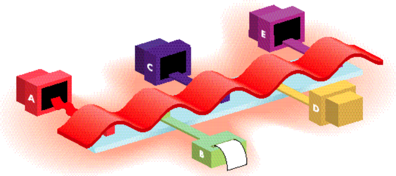


4



Here two nodes try to transmit simultaneously.

5

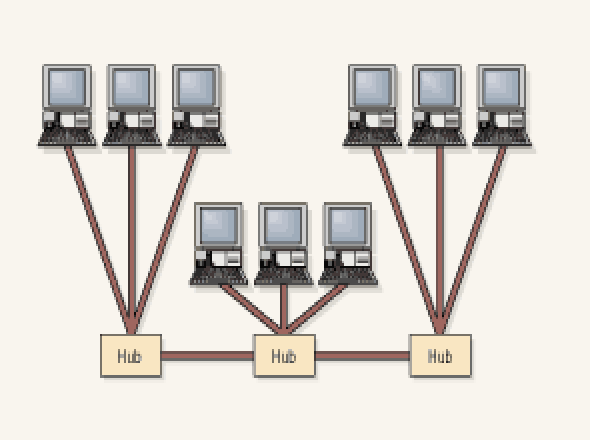


The collision is detected and a jamming signal put on the bus. Each node waits a random time interval before sensing the bus again.

More than one node trying to access the carrier at the same time is called contention.

Contention obviously slows down a network and the more nodes you add the more contention you will get.

To get round this, you can divide a network into 'collision domains' by using separate hubs/switches for groups of nodes.



Circuit Switching vs Packet Switching

This has been dealt with previously. The advantages and disadvantages could be summarised as:

CIRCUIT		PACKET	
FOR	**AGAINST**	**FOR**	**AGAINST**
Ideal for a steady, continuous stream eg video	Takes time to establish a connection	Ideal for bursts of data	Packets have to be reconstructed when received.
	Does not use full capacity of line	Maximises line utilisation, packets can be routed along less congested paths	Some packets go missing and have to be resent
	Nobody else can use the lines	Lines can be shared by other packets	

EXERCISE 9:

1. What is meant by synchronous data transfer?
2. What advantage is there in using asynchronous transfer?
3. Which error check has been used on these ASCII codes, and which byte has an error?
   a. 10010011 01110100 11110000 01011000 10011010
   b. 10010110 00011100 10101110 00011100 11001000
4. A cyclic redundancy check after performing a calculation on the bytes might add them up then the check is the remainder when the total is divided by eleven. Give two reasons the CRC method is superior to the Parity Bit method.
5. If parity bit is being used as an error check, what percentage of data is redundant -- i.e. not the actual ASCII code?
6. If a 1Kbyte packet is being sent with 1 CRC remainder byte, what percentage of the data is redundant?
7. Fully describe the job of the TCP protocol.
8. Describe the involvement of the IP protocol in transmitting the TCP packets.
9. Describe the difference between circuit switching and packet switching.
10. What is the advantage of using packet switching.
11. What do the initials stand for in CSMA/CD?
12. Outline the steps involved in dealing with contention by CSMA/CD.
13. What are the implications of CSMA/CD on Network performance?

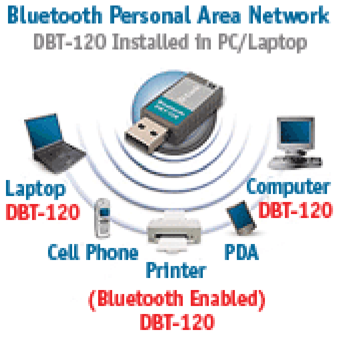
WIRELESS NETWORKS

Wireless connections are becoming very popular. Home networking and sharing of broadband with a wireless router, wireless hotspots for picking up Web connections, Blackberrys and PDAs providing mobile email, Bluetooth connections for mobile phones and even game machines.

Its advantages are fairly obvious, no more spaghetti of wires, easy to install with no cables. You can move around without worrying about where you are connected.

WPAN is a Wireless Personal Area Network. A wireless network for connecting devices centred around an individual. It is very localised (up to about 10 metres) and can connect mobiles, PDAs, laptops etc.

Each device must have a receiver /transmitter using the same standard. A wireless network card is needed on PCs and Laptops.



BLUETOOTH: Named after a Viking leader called Harold Bluetooth, is the most common standard for WPAN.
It operates up to 10 metres, speed about 700Kbps.

Infra-red is another possible wireless link.
IrDA is the standard. It only has a range of 1m, but a speed of 5760Kbps.

The standard for PCs and routers is 802.11 of which there are a number of versions as it gets upgraded frequently.

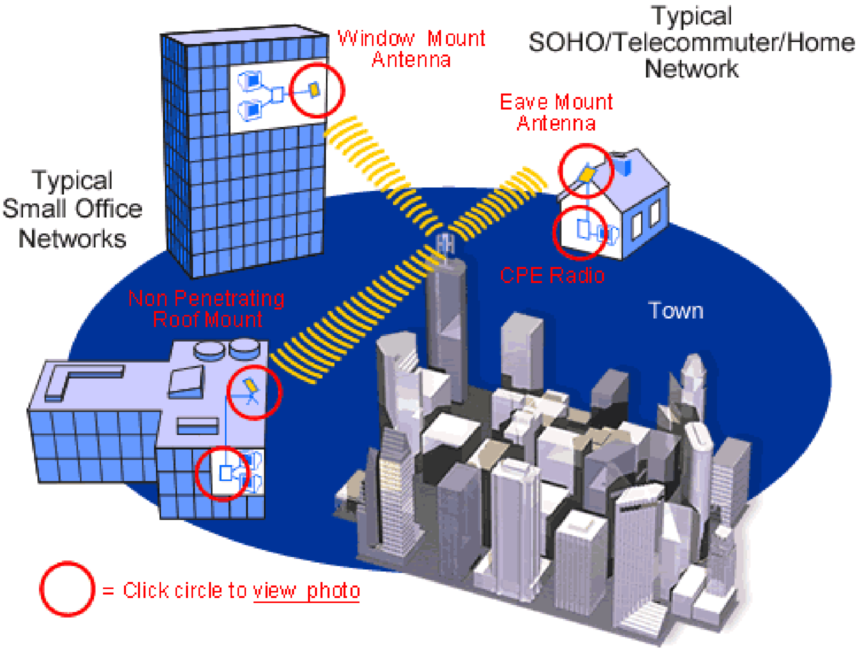
The important thing is that all the devices are using the same standard.

A Wireless LAN is often used in homes to share broadband, it is also good for setting up in temporary places like a weekend meeting. Another obvious use is in a place where cabling would be unsuitable, certain factories and such like.

The problems with Wireless LANs are

a) **Interference** disrupting the signal and
b) **Security** as it could be easy to listen in or steal use of the Internet connection.

A Wireless WAN is also possible. You can get satellite based broadband in rural areas (as broadband is only available to people who live near a telephone exchange).


Window Mount Antenna
Typical SOHO/Telecommuter/Home Network
Eave Mount Antenna
Typical Small Office Networks
CPE Radio
Town
Non Penetrating Roof Mount
= Click circle to view photo

See http://www.netchain.com/Services/Broadband.Diagram.asp

You can also get cellular based broadband in city areas (like mobile phones).

INTERNET CONNECTIONS

There are a number of ways of connecting to the Internet. For five of these, you need to know the bandwidth and what they are most suitable for.

1. **Dial Up**. Suitable for occasional home users. Speed can be frustrating on multimedia sites. Current speed 56Kbps.

2. **Cable modem**. Suitable for home users or people working from home, uses cable TV lines. Always on, so no dialling needed. You share the bandwidth with everyone else in your area, so speed is variable. Security is not tight. Download speeds of 30Mbps are *theoretically* possible, up to 10Mbps uploading, but you share this with others and 1 or 2 Mbps is all that can be relied on.

3. **Leased Line**. A permanent, dedicated connection that you rent from BT. Very expensive but very secure. Used by large companies that need an always on, high speed connection (not actually an Internet connection, could just be connecting a branch to Head Office). Speed ranges from 1.5Mbps to 200Mbps

4. **ISDN**: Integrated Subscriber Digital Network, a digital connection that uses phone lines (no need for a modem). It is dial up and is circuit switched, using synchronous transmission. Basic speed of 128Kbps (using 2 lines of 64Kbps, you pay two call charges), but there are ways of increasing this to 1.5Mbps. Generally used by small businesses. Ideal for video conferencing with the circuit switched connection, best with 4 lines of 64Kbps.

5. **ADSL**: Asymmetric Digital Subscriber Line, provides broadband to homes and small businesses. Lets you share the line with phone calls. You need to be within 3 miles of an exchange. Speeds of up to 8Mbps. (Downloads, Uploads are usually much slower, so *not symmetric*).

If you have broadband at home, google 'broadband speed test' and choose a link to find out the actual speed of your connection for up/download.

NETWORK INTERFACE CARDS

Essential for connecting nodes to a network. There are different types of NICs depending on which type of cable you use and what type of network.

Like all interfaces, NICs have to carry out data conversion: parallel to serial and changing the voltages of 1s and 0s. Also buffering for instance to store serial bits before sending them in parallel. They also put data into frames and add headers with addresses and end bits with error checks.

MAC address: Media Access Control is a 48 bit address unique to every NIC ---- there are 2^{48} different possible addresses. The first 3 bytes identify the card manufacturer, the last three the card. It is used to identify each node on a network. In practice nowadays IP addresses are assigned to each node, but a piece of software translates the IP address into the MAC address so that the NIC recognises data intended for that node.

MAC addresses operate at the Data Link Layer of the OSI model.

Networks have grown for all sorts of hardware and economic reasons:

ECONOMIC:

Multi-national companies need to communicate across the world, National within a country.
Companies use computers for all their data and their offices need to communicate.
Ecommerce is becoming more and more important
We want to buy on-line, download music, play on-line games etc.

HARDWARE:

Computers more powerful – faster processors, more RAM, bigger Hard Disk and so File Servers can operate large networks.
Improvements in cabling, routers, switches can handle more traffic.
Bandwidth has increased greatly and can cope with multimedia data transmission.
Adoption of standards / protocols means we can all communicate.
(Software) Better, more reliable Operating Systems.

We are becoming more and more dependant on Networks, the Web of course then email, using computers in school and at work. This trend will continue until they are a fundamental part of our lives. Then what happens when they go wrong?!

EXERCISE 10:

1. What does WPAN stand for?

2. What kinds of devices would be included in a typical WPAN?

3. What are WLANs usually used for in homes?

4. Describe two disadvantages with WLANs.

5. a) Where might a wireless WAN be used for broadband internet connection? b) How could it be implemented?

6.
    a. Where might a leased line be used to connect computers in a network?
    b. What are the two main advantages of a leased line?
    c. What is the main disadvantage?

7. Which type of connection is best for video conferencing and why is this so?

8. Why is our DSL broadband called Asymmetric?

9. Joe has an ADSL broadband connection rated at 2Mbps download. How long would it take to download an Mp3 file of 3.8 Mbytes?

10. Joe finds it takes longer than it should. Give two reasons why this might be.

11. What speed do you get from dial up and why is this not sufficient nowadays?

12. State two functions of a Network Interface Card.

13. What is a MAC address?

14. Glasgow City Council has its own district wide network linking all the schools and Council Offices. Give three technological advances that have made this possible.