Networks have become very widely used for a number of reasons:

**Technical Factors**

- Advances in hardware technology – faster processors, bigger memory/backing store etc.
- New transmission methods and faster data transfer rates
- Improved networking software – improved network operating systems, browsers etc.
- The development of international standards in data transmission
- The widespread use of TCP/IP and other internet related technology

**Economic Factors**

- The falling cost of telecommunication technologies and services
- Shared access to expensive hardware, software and data
- Geographical expansion of organisations
- Increased competition between companies
- The demand for up to date information

**Benefits of Computer Networks**

- Sharing resources
- Improved communication (both internal and external)
- Access to corporate/global information
- File transfer capability

**Network Uses**

- LAN - Single network enclosed within room or building
- WAN - Single network spread over a large geographical area
- Intranet – Two or more LAN’s linked together
- Internetworks (Internet) – Wide area network of networks
Characteristics of a LAN

- High quality cabling
- Fast transfer rates
- Few errors
- Owned by the company
- Users share hardware and software
- Internal communication via e-mail

Characteristics of a WAN

Lower quality cabling
Slower transfer rates
Error prone
Line rented from a telecommunications company
Access to specialised databases
File transfer/sharing
Internal/external communication via e-mail

What is a Network?

A network is a set of nodes connected by channels, communicating via a protocol.

- A node is a hardware device connected to a network
- A channel is the physical means of transferring data between nodes.
- A protocol is a set of rules that govern the way data is transmitted between nodes.

A node could be a station, a server or other device e.g. router
A station is a computer with a network interface, e.g. an NIC card, and a physical connection to the network.

Network Interface Card (NIC)

The main functions of a network interface are

- Data conversion e.g. parallel to serial
- Buffering – to compensate for different speeds of processor and network
- Signal conversion – to compensate for different voltage levels
- A physical connection – a socket/plug to connect to the network
<table>
<thead>
<tr>
<th>Topology</th>
<th>Structure</th>
<th>Type</th>
<th>Characteristics</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus</td>
<td>LAN</td>
<td>LAN</td>
<td>Nodes connected directly to backbone. There is a terminator at each end to prevent signal bounce. A sending station broadcasts to all stations. Each station has unique address and reception circuitry to detect its own messages. CSMA/CD protocol is used to detect collisions.</td>
<td>Single node failure does not affect rest of network. No complex extra hardware required. Easy to add extra stations. Reliable (CSMA stops collisions)</td>
<td>If the network is heavily used, it can grind to a halt because of the number of collisions. Damage to backbone cabling could bring network down.</td>
</tr>
<tr>
<td>Ring</td>
<td>LAN</td>
<td>LAN</td>
<td>Each station is connected to the ring via a repeater. Ring can be unidirectional or bi-directional. Packets are passed from station to station until reaching their destination. Stations know what packets are for them, because packets contain sender/receiver addresses as well as error correction information and the data itself. A monitor station removes corrupted/undetected packets.</td>
<td>Needs no central host, each node contributes to data transmission. Easy to expand the network. High data transfer rates. Performance remains stable under heavy use.</td>
<td>Cost of extra hardware. Complexity of electronics. Failure of node/repeater can lead to system failure. A break in the ring cabling causes complete network failure.</td>
</tr>
<tr>
<td>Star</td>
<td>WAN</td>
<td>WAN</td>
<td>Each station is directly connected to a central device known as the HUB, which handles switching and routing for the entire network.</td>
<td>Node failure does not disable the network, although the hub is crucial to it’s functioning.</td>
<td>Cabling costs can be high, since every station must be physically connected to the central computer. Since all traffic passes through the hub, the network can slow down when it is particularly busy (bottlenecks). If the hub goes down, the network is disabled.</td>
</tr>
<tr>
<td>Mesh</td>
<td>WAN</td>
<td>WAN</td>
<td>There is a web of connections between stations, so that an individual node may be connected to 2 or more other stations.</td>
<td>Mesh networks are very reliable since packets can take different routes to their destination. There are no bottleneck problems. Node failure does not disable network performance.</td>
<td>Network structure can be very complex. The amount of cabling required makes them expensive to set up.</td>
</tr>
</tbody>
</table>
Media Access Control (MAC) Address

- Every Ethernet NIC has its own unique MAC address
- This is built into the card at manufacture
- It used to identify each machine on a LAN
- The Ethernet protocol is used to direct **frames** around the network
- Each frame contains
  - The source MAC address
  - The destination MAC address
  - The data itself
  - Error detection and transmission information

Server Machines

A server is a powerful computer dedicated to a specific function

<table>
<thead>
<tr>
<th>Type of Server</th>
<th>Main Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>File</td>
<td>Creates a centralised storage area for all user files. Each user is allocated personal space that can be accessed via a centrally controlled logon and password system. All users have protected access to their work from any station</td>
</tr>
<tr>
<td>Printer</td>
<td>Allows a station to use a printer not directly attached to it. Can be used to queue and prioritise the order of print jobs</td>
</tr>
<tr>
<td>Web</td>
<td>Receives, stores, transmits Web pages. Can be used to provide extra security including restricting access to undesirable web sites. Can also be used to cache web pages</td>
</tr>
</tbody>
</table>
Mainframe with terminals and Networks compared

<table>
<thead>
<tr>
<th>Mainframe with terminals</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Dumb) Terminals are keyboards and screens with no processors or memory and often no backing store</td>
<td>Network stations are fully functioning computers</td>
</tr>
<tr>
<td>Terminals completely rely on the mainframe machine for processing power</td>
<td>Stations can function on their own, but rely on sever machines for their specialist functions</td>
</tr>
<tr>
<td>The mainframe shares its time out between each terminal, so that users think they have sole access to its processor</td>
<td>A network station may use the processing power of other stations to share out workload</td>
</tr>
</tbody>
</table>

Functions of a Network Operating System

- Deals with communication between stations - Adds send/receive addresses to data packets.
- Deals with protocols e.g. CSMA/CD (Ethernet LAN) and TCP/IP, FTP to communicate with other LANS or the Internet.
- Maintains data integrity - i.e. error detection/correction. File level and record level protection.
- Security – Controlling access to the network (logins/passwords) and remote access (firewalls). Setting access rights (read/write/execute) as well as encryption.

Communications software

To access the Internet you will need communication software provided by your ISP.

Its functions are to

- Set up the baud rate for transmission
- Set up the phone number for transmission
- Set up the IP address
- Set up the user ID
- Manage password authentication
## ISO/OSI Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
<th>Protocols</th>
<th>Data Structure</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Layer</strong></td>
<td>Concerned with applications (provides a set of interfaces to allow access to networked services) e.g. mail/file transfer, browsers and database access</td>
<td>HTTP, FTP, SMTP, POP3</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Presentation Layer</strong></td>
<td>Standardises data formats so that communicating users/applications can understand each other. Also responsible for character code conversion, compression, encryption, file locking and security</td>
<td>MIDI, HTML, ASCII, GIF</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Session Layer</strong></td>
<td>Synchronises the data flow between users during a ‘session’. Also manages log on procedures and password recognition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Transport Layer</strong></td>
<td>Breaks the file into segments and guarantees an error free connection between 2 hosts. Sets up communication between users, controlling transmission between sender and receiver</td>
<td>TCP</td>
<td>SEGMENTS</td>
<td></td>
</tr>
<tr>
<td><strong>Network Layer</strong></td>
<td>Converts segments into packets. Source and destination addresses are added. Routers operate at this level as they are responsible for routing packets around the network</td>
<td>IP</td>
<td>PACKETS</td>
<td>ROUTERS</td>
</tr>
<tr>
<td><strong>Data Link Layer</strong></td>
<td>Organises the transmitted bits into frames (and vice versa), and sets up error detection and correction</td>
<td>CSMA/CD</td>
<td>FRAMES</td>
<td>SWITCHES</td>
</tr>
<tr>
<td><strong>Physical Layer</strong></td>
<td>Organises the physical transmission of the 1’s and 0’s that make up the data being transmitted for transmission across the different media (twisted pair, coaxial etc)</td>
<td></td>
<td>BITS</td>
<td>HUBS</td>
</tr>
</tbody>
</table>
Some Common Communications Protocols

**Telnet** - Early protocol that allows users to log onto a network computer from a remote machine, treating the machine as if it were a terminal directly connected to the network computer. Can also be used to monitor network devices such as hubs and switches.

**(FTP) File Transfer Protocol** - Early protocol that allows the transfer of files from one network machine to another. Still the preferred protocol for downloading files such as software installation, driver updates etc. An FTP server program must be running on the host machine.

**(HTTP) Hypertext Transfer Protocol** - Provides many of the functions of the World Wide Web (WWW). It deals with any problems that could arise from data being transferred between different machines using different operating systems etc. For the WWW to function, a web server has to be running on the host machine with a web browser on the client machine.

**HTTP** – Defines the URL’s to access web pages

```
http:// www.hp.com/ index/fp.htm
```

**PROTOCOL** | **ISP ADDRESS** | **PATH TO FILE**
-- | -- | --
http:// | www.hp.com/ | index/fp.htm

(DOMAIN)

Embedded hyperlinks in web pages make it easy for the user to access related pages transparently.

**(SMTP) Simple Mail Transfer Protocol** – Originally set up for systems that were permanently connected. It specifies how mail is delivered from one computer to another. Originally did not require any authentication but, because of the problem of ‘Spam’, most servers now require authentication before accepting mail from another machine.

**POP3** – Was originally designed to let users collect mail from a remote mailbox. Useful for users who are not permanently connected to their mail servers. Requires a username and password, but like **Telnet** and **FTP**, these are transmitted in plain unencrypted **ASCII** code.
Two very important Protocols

**TCP/IP** - Allows computers in different networks to communicate. It consists of 2 protocols…

**TCP - Transmission Control Protocol**
Splits the file into packets, adding a header with a number. This number makes sure that packets are re-assembled in the correct order at their destination.

**IP – Internet Protocol**
Adds its own header to the TCP packet. Its purpose is to make sure that packets are routed to the correct destination.

**CSMA/CD** - Associated with broadcast networks e.g. Ethernet

**CS - Carrier Sense** - Stations listen for a gap before transmitting

**MA - Multiple Access** - Stations have access to the network at all times

**CD - Collision Detection** – If 2 stations transmit at the same time, they sense the collision and retransmit after differing time intervals.

---

**Peer To Peer and Client Server Networks compared**

<table>
<thead>
<tr>
<th>Peer To Peer</th>
<th>Client Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Stations have equal status</td>
<td>Status is either as client or more powerful server</td>
</tr>
<tr>
<td>Shared access to resources, with no central control</td>
<td>Access is controlled by server</td>
</tr>
<tr>
<td>Security is difficult to implement</td>
<td>Password access controlled by server</td>
</tr>
<tr>
<td>Limited protection of files/folders</td>
<td>A hierarchy of privileges can be set to allow different levels of access</td>
</tr>
<tr>
<td>Individuals responsible for their own backing up</td>
<td>Secure backups can be taken at regular intervals at the discretion of the administrator</td>
</tr>
</tbody>
</table>
Internetwork Hardware

- **Hub** – The simplest network involves connecting 2 machines together via their network interface cards (NIC), but this presents a problem when adding more machines to the network. The NIC is being used to connect to one machine so how can it connect to others. A hub solves this problem. It acts as a link between several machines. All traffic goes through the hub and is transmitted to all other machines (broadcasted). It is up to receiving machines to decide if messages are for them. Clearly such networks can quickly become very busy.

- **Switch** – A switch (switched hub) improves on the traffic problems associated with a hub. A switch has a reference table of the computers connected to it, and reads the destination addresses of data frames, so that messages can be sent only to the correct computer. For this reason switches are described as ‘smart’ devices. Switches help to make networks less busy.

- **Routers** – Routers are used between LAN’s or across the Internet. They examine IP addresses to determine whether traffic is for its local LAN, another LAN or the Internet, and directs data accordingly, eliminating wasted data transmission. The router also keeps broadcast data within the LAN.

IP Addresses, Domain Name Service and Name Resolution

IP addresses can be **static**, as in a private network where every host is allocated a fixed address or **dynamic**, where hosts are allocated an IP address only when they access the network as in accessing the Internet via dial-up

- IP addressing is the method of distinguishes computers or more accurately network interfaces on a network
- No two computers on the same network can have the same IP address
- IP addresses are difficult to remember e.g.(216.239.41.100)
- Domain names are easier to remember and the Domain Name Service system translates the domain name into an IP address so that the correct computer can be found
- Name Resolution is the system of mapping a domain name to its IP address
- This is done by using the DNS (Domain Name Service)
- When a web page is requested, a DNS Resolver (built into OS) contacts the DNS to determine the server’s IP address
- If this is not found then it turns to the DNS server higher up in the hierarchy until the address is returned to the requesting machine
IP Address Structure and Classifications

- An IP address is a 32-bit number broken into four 8-bit octets
- IP addresses consist of a network identifier and a host identifier
- If more octets are used for the network identifier, more networks can be allocated, but this means fewer host machines
- If more octets are used for the host identifier, more hosts can be allocated, but this means fewer network identifiers are available
- The way that the IP address is split indicates its particular class

<table>
<thead>
<tr>
<th>Class</th>
<th>Structure</th>
<th>Organisation</th>
<th>No of hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>nnn.hhh.hhh.hhh</td>
<td>Very large companies</td>
<td>16million</td>
</tr>
<tr>
<td>B</td>
<td>nnn.nnn.hhh.hhh</td>
<td>Large companies</td>
<td>65,000</td>
</tr>
<tr>
<td>C</td>
<td>nnn.nnn.nnn.hhh</td>
<td>Small/medium companies</td>
<td>256</td>
</tr>
</tbody>
</table>

\[ n = \text{network identifier}; \ h = \text{host identifier} \]

- Class D used for multicast - this is a way of defining a group of nodes and sending packets only to those nodes, and not every node on the network

Limitations of the current classification system

- The current system is inefficient especially at classes A and B, with many allocated addresses remaining unused
- When the system was set up it was not envisaged just how many networks there would be with so many devices being connected to the Internet.
- The concern is that the world will run out of IP addresses

SOLUTIONS:

Either

- Extend the number of IP addresses by using a 6 octet system instead of 4 octets as at present
- Using 128 bits instead of 32
- This makes it possible to have $3.4 \times 10^{38}$ addresses

Or

- Do away with the IP class system
- Use Classless Inter Domain Routing (CIDR) using IP addressing space more efficiently by making it possible to allocate part of a block to a network instead of the whole block
Wireless Networking

- Wireless networking is the newest and fastest growing network technology
- No physical connection to the network, using wiring, is required
- Wireless networks can be WPANS, WLANS or WWANS
- Devices require a Wireless NIC
- Wireless networks are still generally slower than conventional networks

WPAN (WIRELESS PERSONAL AREA NETWORK)

- A method of connecting personal devices to networks e.g. mobile phones, MP3 players, laptops or PDA’s
- Bluetooth technology is commonly used
- Bluetooth will function within a 10m radius
- When 2 devices come within range of each other, they can communicate
- Bluetooth can function using both circuit and packet switching

WLAN (WIRELESS LOCAL AREA NETWORK)

- A wireless LAN replaces cables and conventional NIC’s with wireless technology and wireless NIC’s
- Each station will communicate with a wireless base station (wireless hub)
- The base station must be connected to the server (often by cable)
- There may be several base stations across a network since the range for one may be less than 100m
- Users can ‘roam’ between base stations transparently
- WLANS are useful where:
  - Portability of stations is important
  - If the network is in a temporary building
  - If it would be expensive or difficult to install conventional cabling

WWAN (WIRELESS WIDE AREA NETWORK)

At the moment this can be done by:
- Using a mobile phone to connect your laptop to the telephone network, but this is expensive and slow and not suitable for transferring large amounts of data
- Connection via a satellite modem, which is available anywhere in the world where the satellite can be accessed, but this is also expensive

Wireless broadband is a likely future solution in both rural and metropolitan areas, as long as mobile connectivity is not required
Security issues associated with Wireless Networks

- It is more difficult to check which stations are connected, than with a cable network
- The network may function beyond the walls of the building
- It is relatively easy to illegally intercept data on a wireless network

SOLUTIONS

A wireless network can be secured by:

- Using the MAC address of the devices NIC to authenticate users
- Wireless technologies come equipped with encryption and other security features to restrict what machines can connect to the network
- This means that anyone intercepting the wireless signals will be unable to extract any useful information

Browsers and Microbrowsers compared

<table>
<thead>
<tr>
<th>Browsers</th>
<th>Microbrowsers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsers are designed to work with desktop computers and incorporate e-mail, news, HTML editing facilities, favourites, history, and include plug-ins for multimedia content. They use higher bandwidth, so files can be larger and communication costs are usually cheaper.</td>
<td>A microbrowser is one designed for use with a wireless hand held device e.g. mobile phone. They are written to be as small as possible to make best use of the low memory available on such devices and the low bandwidth constraints of the networks to reduce expensive communications costs.</td>
</tr>
</tbody>
</table>

HTML - Hypertext Markup Language

The HTTP protocol interprets the HTML scripts in a transmitted file to format it properly and create the web page on the screen.

- A markup language annotates text with additional information about how it should be displayed
- HTML uses tags to do this
- Tags are used to identify elements
- Elements should have a start and end tags around them
**HTML - Example**

The **HTTP** protocol interprets the **HTML** scripts in a transmitted file to format it.

Example:

```html
<html>
<head>
<title>My first web page</title>
</head>
<body>
  <h1>Headline - Welcome to my first web page!</h1>
  <p>This section is normal text</p>
  <p><b>This section is in bold</b></p>
  <p><u>This section is underlined</u></p>
  <img src='http://ww.google.co.uk/intl/en_uk/images/logo.gif' alt='google logo'>
</body>
</html>
```

You should be able to recognise and demonstrate tags for:

- start
- header
- body
- title
- style
- font
- size
- alignment
- section headers

**WML (Wireless Markup Language)**

- WML applications consist of one or more “decks” of “cards”
- Each card has user content as well as content for the microbrowser to control how the user moves from one care to another
- This means that several cards can be sent together, so that the server does not have to be accessed each time the user requests a new card
- Written very like HTML – elements, start/end tags
- Each card element has its id attributes specified so that the user can move between each card
**HTML and WML compared**

<table>
<thead>
<tr>
<th>HTML</th>
<th>WML</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed for creating documents</td>
<td>Designed for creating applications</td>
</tr>
<tr>
<td>Read by browsers</td>
<td>Read by microbrowsers</td>
</tr>
<tr>
<td>Interpreted by the HTTP protocol</td>
<td>Interpreted by the WAP protocol</td>
</tr>
<tr>
<td>Used by fully functioning computers: - powerful processors, large screens, high bandwidth, cheap connections</td>
<td>Used by WAP enabled devices: - small screens, low processing power, low bandwidth, expensive connections</td>
</tr>
<tr>
<td>Creates multimedia documents</td>
<td>Creates text based output</td>
</tr>
</tbody>
</table>

**Search Engines – Crawler-based and Directories**

The Internet is so large that we need software to help us find what we are looking for.

There are 2 main types of search engine: -

**crawler-based search engines** have databases that are built by robot programs called **spiders**
- Spiders ‘crawl’ the web finding pages for inclusion by following links in pages that they already have in their databases
- They also rely on contributors submitting web pages to be indexed
- The index is built using page titles, page content and HTML **meta tags**.
- A meta tag is a tag that is placed in the header element of a web page and is invisible to the browser, but can be used by search engines to index pages
- The most common meta tags are **keywords** and **descriptions**
- The search engine only looks for matches in the keywords and description submitted by the owner of the web page
- If a web page is not linked to any other page in the database, the spider search engine will never find it
- The URL of the web page would have to be submitted to the search engine company to be included

**DIRECTORIES**

- **Human-powered** indexing facilities
- **Built up by editors** working for directory company
- **Users submit short description** of their site to directory
- **Editors write a short description** for sites they review
- When query entered, search engine **only looks for matches in the descriptions submitted**
Meta search engines eg ask.com; dogpile.com; metacrawler.cm; pass queries to several search engines and directories and

- Summarise results
- Remove duplicate engines
- Result should be aggregate of best search engines on the web

Circuit Switching and Packet Switching

CIRCUIT SWITCHING

- This involves setting up a dedicated communication circuit, which remains in place until the communication has been completed.
- All data follows the same physical path.
- No other data can use this path until the communication is complete and the circuit is broken

PACKET SWITCHING

- No fixed communication circuit is set up
- Messages are broken into small units called packets and they are routed around the network to their correct destination based on the destination address held within each packet
- Packets may take different routes before arriving at their destination and being reassembled into the correct order
- Since there is no fixed circuit, there is no restriction to the routes that other data may take
- The Internet uses this system of packet switching

Asynchronous and Synchronous Data Transmission

<table>
<thead>
<tr>
<th>Synchronous</th>
<th>Asynchronous</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal clocks of the sending and receiving machines are synchronised. (Start frame used to synchronise receiving station with transmitting station)</td>
<td>Sending and receiving machines are not synchronised</td>
</tr>
<tr>
<td>Data transmitted in blocks (up to 8Kb in length)</td>
<td>Data transmitted byte by byte</td>
</tr>
<tr>
<td>Start/stop frames needed only at beginning and end of each block of data</td>
<td>Start and stop bits required for every single byte</td>
</tr>
<tr>
<td>Low percentage of control information transmitted with the actual data</td>
<td>Higher percentage of control information transmitted with the actual data</td>
</tr>
<tr>
<td>Error checking data usually included in</td>
<td>Does not normally include error checking</td>
</tr>
<tr>
<td>the data block</td>
<td>data</td>
</tr>
<tr>
<td>----------------</td>
<td>------</td>
</tr>
<tr>
<td>Capable of high speed data transfer</td>
<td>Normally involves only low speed data transfer</td>
</tr>
</tbody>
</table>

**Error checking – Parity Checking and Cyclic Redundancy Check**

**PARITY CHECKING**

- Used to detect errors in the transmission of **single** characters
- An extra bit called a parity bit is added to each character
- The parity bit is sent **along with the actual data**
- There are 2 types of parity check - Odd Parity or Even Parity
- If odd parity is used then the parity bit will be set so that the number of 1’s transmitted in any byte will always be an odd number
- The receiving machine counts the number of bits received and if it is an odd number then it is assumed that the data is correct
- If the calculation results in an even number, an error is assumed and the data will require to be re-transmitted
- Obviously 2 errors in a transmitted byte could result in a corrupted byte being accepted

**CYCLIC REDUNDANCY CHECK**

- More sophisticated and less error prone than parity checking
- Carried out on **blocks** of data
- May involve a calculation including division
- The result of the calculation is transmitted **along with the original data**
- Receiving machine carries out same calculation
- If the result is the same, data is assumed to be error free
- Slows down transmission due to the calculations needed at transmission and receiving end
- However, data is more accurate, as mistakes are discovered, and corrections can be made

**Internet Connections**

**DIAL UP**

- Requires a modem
- Speed – up to 56 Kbps
- Slow ISP dial up (15-20 secs)
Not as fast or reliable as ISDN
- Uses – Internet access

### Internet Connections (continued)

**ISDN (INTEGRATED SERVICES DIGITAL NETWORK)**
- Requires an ISDN terminal adapter
- Speed – 2 x 64 Kbps for data or voice (digital)
- Cost is equivalent to 2 phone calls
- Channels can be used independently
- So a single ISDN line can give 128 Kbps Internet access
- Fast access to ISP
- Must be within 5.5 kilometres of telephone exchange
- ISDN channels can be combined to increase quality, but this also increases costs
- Uses – Fast Internet access, often used by schools, one to one video conferencing

**ADSL (ASYMMETRIC DIGITAL SUBSCRIBER LINE)**
- Requires an ADSL modem
- Makes use of circuit switching
- Speed – In theory can operate at 9Mbps download and 640 Mbps upload
- Speed – In reality will be much slower since others will be sharing
- Can combine data usage and voice usage
- Operating distance – up to 5 kilometres
- ‘Always on’ connection means:
  - Use of static IP addresses
  - Need for firewall protection
- Uses – Web browsing, video on demand, some client server applications

**CABLE**
- Requires a cable modem (usually supplied free by cable company)
- Uses the optical cable network infrastructure
- Speed – 1.5 mbps (due to sharing with others) up to a maximum of 30Mbps
- Uses – Can combine cable TV with Internet access

**LEASED LINES**
- Permanent dedicated circuit between 2 points
- Speed – Over 1.5 Mbps up to a maximum of 44Mbps
- Leased from a telecommunications company
- Expensive to set up and maintain
- Gives exclusive use to the company
- Uses – To give high speed Internet link between company branches, to transmit video or audio data

**Network Security**

Security on a network is always a compromise between security and convenience. The network must be protected, but legitimate users must have access to what they need.

Both internal and external security is required.

Security is required to:

- Protect data on the network
- Protect network software and resources
- Protect network users

**Passive Attack** – This involves the monitoring of data being transmitted around a network

**Active Attack** – This involves the modification of the data stream or the creation of a false stream of data on a network

**INTERNAL SECURITY (PHYSICAL)**

- Servers and backup discs can be held in a locked room
- Workstation areas can also be physically locked and access can be by magnetic swipe card, smart key or typing a security number
- No disc drives connected to workstations
- Other solutions include biometric security systems e.g. fingerprint, face or iris pattern recognition

**INTERNAL SECURITY (SOFTWARE)**

- All network users need a user ID and password
- These are usually encrypted when being sent to the file server so that they can’t be intercepted and used by others
- Users can be placed into groups giving them different access rights depending on their status within a company
- Groups can be restricted to certain stations or times of day
- Access rights to every file and folder can be set by the OS e.g. a users own files will be read/write, but shared files may be read only and OS files will not be accessible at all
Other hardware and software, e.g. important databases, can have individual password protection

EXTERNAL SECURITY

- The network also has to be protected from outside attack
- It is best if access to the outside world is via a single machine
- Anti-virus software should be installed on network file servers and stations
- Any suspect files will be repaired or quarantined and the network manager informed
- Anti-virus software must constantly be updated since viruses can evolve and new ones appear
- Proxy servers add security since they protect the networks private IP addresses from the outside world
- Only the proxy servers IP is accessible
- A firewall blocks network traffic by examining each packet passing through
- Packets not using appropriate protocols can be blocked
- Routers can be set up to block traffic from particular IP addresses
- It is best to use both a firewall and a router
- Monitoring software can be set to detect unusual activity that might signify hacker or virus activity

Internet Filtering Software

FIREWALL

A firewall is hardware/software located on a network computer. It protects a private network from users on other networks. A firewall, working in conjunction with a router, filters all network traffic to decide whether to forward data to its intended destination e.g. a private network which allows internet access will use a firewall to prevent unauthorised access to its own data from outside, as well as limiting internet access by its own users.

FILTERING SOFTWARE

Filtering software allows the user to access anything on the web except those sites that have been identified as unsuitable. A simple method is to ban access to sites containing key words in their titles. More sophisticated systems use a regularly updated list of banned sites or a proxy server maintained by the company supplying the filtering software. Sites can be added/removed as needed

WALLED GARDEN
A walled garden only allows users to access certain parts of the web. There will be a list of permitted sites that a user can access. Sites can be added or removed from the list. This is a very effective method of filtering content, but is quite restrictive since users can only access those listed sites.

**Denial of Service Attacks**

This is an attack on a network that significantly reduces the capacity of the network to provide resources to legitimate users. There are several types of attack:

- **Exploitation of software flaws** - Bugs in software can allow hackers to exploit a network, causing it to crash in such a way that they can take control of the system.
- **Exploitation of network management flaws** – Getting access to default network manager passwords on popular server software to bring a server down.
- **Resource starvation** – Where attacks that consume the bandwidth of the network denying users access to services. Viruses and worms can be examples of this as they attempt to propagate themselves.
- **DNS attacks** – A large number of queries are sent to DNS servers. These queries contain a spoofed IP address of the target server. The DNS servers respond with a large response, which is routed to the target, causing congestion and consumption of bandwidth.

**EFFECTS OF DENIAL OF SERVICEAttacks**

Denial of service attacks can be devastating to a company. The outcome could be:

- Loss of business
- Loss of user confidence
- Costs of repair
- Disruption to the organisation

**DISASTER AVOIDANCE**

Remember that as well as potential malicious disasters; things like fire, flood and power failure, can also be disastrous to a system.

**SOFTWARE SOLUTIONS**

- The best possible software solution is to have an automatic backup system in place.
- Backups should be made daily.
- Usually at night when the system is quiet.
- Keeping backups over several days.
- Storing the tapes on a separate site.

**HARDWARE SOLUTIONS**

- Regular maintenance and the use of high quality components
- **Fault tolerant components** – components that have duplication built in – if one part fails the other part can take over
- **Hardware redundancy** – having backup devices ready to take over e.g. backup servers
- **Uninterruptible Power Supplies (UPS)** – A separate power supply that can take over temporarily if the main power supply fails, avoiding system crashes
- **Disk Mirroring** – Writing to 2 hard discs simultaneously so that if one fails, the other is available

**E-Commerce**

E-Commerce is the buying and selling of goods and services over the Internet

**CUSTOMERS**

**Advantages**

- 24-hour access
- Can be accessed from anywhere worldwide
- Uses EFT so no cash needed
- Can compare products and prices before buying
- Goods delivered to your door

**Disadvantages**

- May have difficulty recovering funds if goods are not what was ordered, faulty or if they don’t arrive at all
- Must rely on the vendor to protect your credit card details
- Extra costs for delivery and packing
- Local shops may go out of business
- You may have to pay import tax

**MERCHANT**

**Advantages**

- Deal directly with customer – no middlemen
- Vast customer base
- No costly high street retail outlets to pay for
- **EFT** means no cash security issues
- On-line profile does not depend on the size of your organisation
- Stock control, funds transfer, order tracking, packing and delivery can be automated

**Disadvantages**

- Need robust security to protect against credit card fraud
- Need to employ a web designer
- Must ensure that web site is secure and that servers are protected from hackers

**HTTPS (HTTP over a Secure Socket Layer)**

Most e-commerce sites use HTTPS that encrypts credit card data being transmitted over the Internet, so that it cannot be stolen if intercepted

**PHISHING**

Phishing describes a method of attracting customers to bogus bank or credit card sites, enticing them to enter credit card details, passwords and PIN numbers so that criminals can steal them

Many credit card companies now use **AI** (Artificial Intelligence) systems to spot unusual card activity quickly, since customers may only spot problems when they receive their monthly statements

**Tele-working**

**EMPLOYEE**

**Advantages**

- Can save on travel time and transport costs
- Flexible hours means that you can on child minding costs
- Can deliver work to employers and customers electronically

**Disadvantages**

- Feelings of isolation
- May feel pressured to work too hard
- Need office space at home
- May need to insure employer’s equipment

**EMPLOYER**

**Advantages**
- Can save money on office space
- Tele-workers often work harder than they would in an office
- Can save money by employing people in countries where wages are low

**Disadvantages**

- Staff may have to be trained
- Will have to pay for computer equipment and communications costs
- Security issues associated with home workers accessing company networks
- You may have less control over the quality of work produced

**Social Implications of Networks**

- Tele-working
- Video conferencing
- Information rich or information poor
- Social isolation

**Legal Implications of Networks**

- **Data Protection Act** – Designed to protect the individual whose details are held by institutions and companies
- **Computer Misuse Act** – Brought in to protect against hacking and viruses
- **Copyright Designs and Patents Act** – Combats the illegal copying of materials on-line
- **Regulation of Investigatory Powers Act** – Law allowing government and employers to monitor the computer use of individuals

**Ethical Implications of Networks**

- Censorship
- Monitoring by Government
- Pornography
- Use of ‘cookies’ to monitor Internet activity