Computer Networks

A network is a set of computers that are connected to one another.

Standalone computers are isolated from other devices.

Advantages of a network
- ✓ Share resources, such as software applications, files and hardware (eg printers).
- ✓ Allows communication (eg email) and can transfer files easily.
- ✓ Easier network management (eg can backup data onto a central fileserver; updates can be sent to all computers; users on a network can login to any computer)

Disadvantages of a network
- ✓ Greater security risk as computers can be hacked if they are connected to the internet.
- ✓ Worms can spread from one computer to another
- ✓ A problem with any shared resource, (eg file server goes down) can impact the whole network.

Types of Computer Networks

Personal Area Network (PAN) set up around an individual person. Many people have multiple devices such as tablets, phones and computers that can be interconnected using a PAN. A Bluetooth PAN uses radio waves to communicate wirelessly between devices over a range of a few metres.

Local Area Network (LAN) covers a relatively small geographical area typically extends over the range of a single organisation such as a university campus, school site. LANs are usually managed by a single organisation.

Wide Area Network (WAN) made up of many local area networks and covers a much wider geographical area. The internet the ultimate WAN. It is a network of networks with billions of interconnected devices. No single person or organisation has control over a WAN.

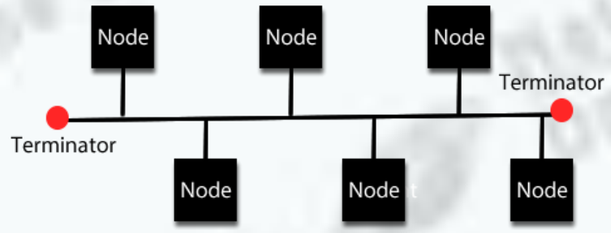
Network Topology

A network topology describes how a set of computers are arranged within a network.

Bus network topology All devices including clients, servers, printers and so on are connected to a cable called a bus. All communication is via the shared bus. At either ends of the bus is a terminator.

Advantages
- ✓ Easy and cheap to install and does not require much cable
- ✓ Easy to add more computers

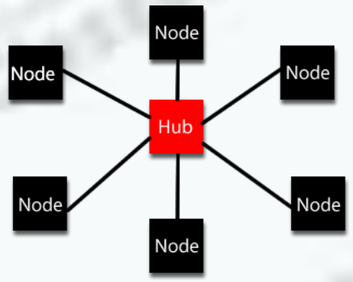
Disadvantages
- ✓ If the main cable fails then then the whole network fails.
- ✓ Less secure as data are broadcast to all devices on the network.
- ✓ Can be slow as there are collisions between data along the shared bus.
- ✓ Will get slower as more computers are added.



Star network topology all devices including clients, servers, printers and so on are connected to a central hub or switch. All communication is via the hub

Advantages
- ✓ Greater security as data are only sent to the intended recipient.
- ✓ If any of the connections fail only a single node will be affected.
- ✓ Fewer collisions between data packets

Disadvantages
- ✓ If the central hub fails then every computer on the network is affected.
- ✓ Expensive as extra cable and hardware (hubs) are needed.



Wired and Wireless

Computers can be connected using wired or wireless methods

Wired transmission methods use cables to communicate

Wireless transmission use radio waves communicate (eg Wi-Fi).

Advantages of wireless
- ✓ Can use computer anywhere and not constrained by cables

Disadvantages of wireless
- ✓ Packets can be intercepted more easily than wired connections
- ✓ Security is a much more difficult challenge, as the network can be accessed from outside the confines of a building.
- ✓ Slower than wired methods
- ✓ Signal can be interfered with by other electronic devices.

Advantages of wired
- ✓ Allows more control, security and reliability. Can restrict who has access to the network.
- ✓ Wired methods have greater speeds than wireless methods.

Disadvantages of wired
- ✓ Cables can be difficult to maintain in big organisations

Wired networks use a variety of cables, including copper and fibre optic.

Copper cables use electrical signals to transmit data. Three main types:

- ✓ **Coaxial cable** – the signal loses strength over long distances
- ✓ **Unshielded twisted pair** – A pair of copper cables are twisted together and allows data to be transmitted over longer distances
- ✓ **Shielded twisted pair** – Shielding around the twisted cables means the signal is less susceptible to interference.

Fibre optic cables are glass or plastic and use use pulses of light to transmit data

Advantages of copper cables
- ✓ Cheaper than fibre optic
- ✓ Reliable because a telephone is powered from the copper cable and does not rely on a separate electrical power supply

Advantages of copper cables
- ✓ Slow
- ✓ Low capacity
- ✓ Can only be used over short distances
- ✓ Interference can occur

Advantages of fibre optic
- ✓ Higher bandwidth than copper so can transmit more data
- ✓ Less attenuation (degrading) of the signal so fibre optic is more suitable over long distances

- ✓ Less “cross talk” interference between fibres compared with copper so the quality of the signal is better

Disadvantages of fibre optic
- ✓ Expensive
- ✓ Difficult to install

Network Security and Protocols

Why do we need network security?
- ✓ To prevent unauthorised access to our electronic devices
- ✓ To protect our data eg to prevent sensitive data being stolen
- ✓ Prevent cyberattacks

Methods of Network Security

Authentication allows us to confirm the identity an individual. There are lots of ways of confirming the identity of an individual that come under one of three factors:
- ✓ Knowledge factor: Something the user knows, eg a password
- ✓ Possession factor: Something the user owns eg a mobile phone
- ✓ Biometric factor: eg Fingerprint, iris scan

Encryption The message is garbled so if it gets intercepted during transmission it will be almost impossible for anyone without the key to read the original message.

Firewall prevents packets containing malware getting on to the computer

MAC address filtering A MAC (Media Access Control) address is a unique identifier for any device that is connected to a network. Each network interface card has a unique MAC address that is a 12 digit hexadecimal code (e.g. 12-F3-EE-56-44-A1).

- ✓ *White list filtering* only allows devices on a list to connect to the network.

- ✓ *Black list filtering* devices in a black list blocked from accessing the network.

Network Protocols

A **network protocol** is a set of rules that allow computers to communicate and exchange information over a network. There are many types of protocols depending on the application.

HTTP (Hypertext transfer protocol) is the protocol used for the World Wide Web. An exchange begins with a request for a web page from a client web browser to a web server. The server then sends the web page to the client.

HTTPS (Secure Hypertext transfer protocol) is a secure way of transferring data between a web browser and a server because the data are encrypted during transfer. Used for e-commerce and online banking.

FTP (File Transfer Protocol) is usually used to download or upload large files from a server to a client.
Ethernet is not a single protocol but a collection of related protocols. LANs most commonly use ethernet. The following is a simplified procedure:
1) Check whether there is any traffic on the ethernet
2) If so wait for traffic to clear
3) Send the packet
4) If collision detected, go to step 1 to resend.

Wi-Fi is a collection of protocol that use radio waves to transmit data between devices. Wi-Fi is a trademark and WLAN (Wireless LAN) is the generic term. Data are transmitted when the medium is clear, and an acknowledgement is received if the transmission was successful. If no acknowledgement is received, then the data are resent as it is assumed that a collision occurred, and the packets did not reach their destination.

Email protocols

SMTP (simple mail transfer protocol) Sends the mail from the user onto the mail server.

IMAP (Internet Message Access Protocol) Retrieves the mail from the mail server to the client (user) and allows access from anywhere on any device because the email remains on the server.

TCP (Transport Control Protocol) When files are sent over the internet they are broken up into small chunks called packets. When they arrive at the destination computer they are reassembled back into the original format. TCP handles and controls all this. TCP waits for acknowledgements to verify whether the packets have reached their destination. TCP will also retransmit packets of they have not arrived at the destination or become corrupted.

IP (Internet Protocol) The internet protocol is a set of rules that govern the transmission of data across the internet.

UDP (User Datagram Protocol) is used as an alternative to TCP. It is used in video conferencing and online gaming when speed is necessary as huge volumes of data are transferred in real time. It improves speed by not checking for lost packets so they do not get re-sent.

TCP/IP

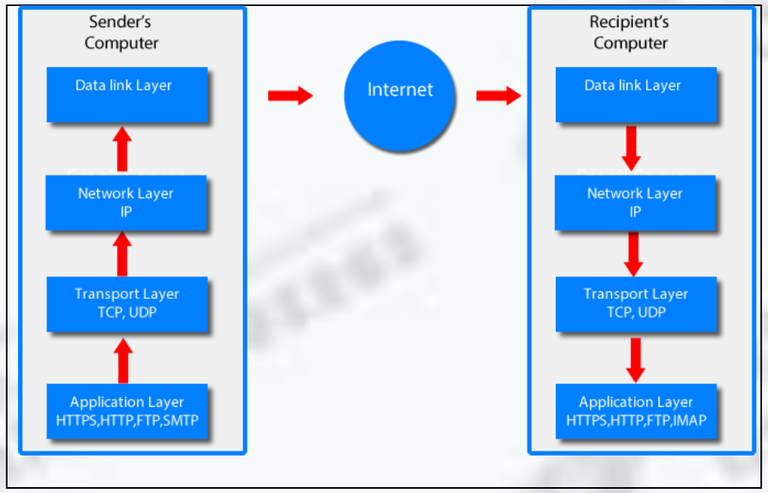
The TCP and IP protocol work closely together and are referred to as TCP/IP. The TCP/IP model consists of four layers that pass data between each layer.

Application layer contains protocols related to the application such as HTTP, HTTPS for web browsers, FTP for file transfer and SMTP and IMAP for email. The application layer interacts with the user via appropriate application software (eg web browser / ftp client).

The **transport layer** establishes the end to end connection. When files are sent over the internet, they are broken up into small chunks called packets. When they arrive at the destination computer they are reassembled back into the original format. It is the role of the transport layer to split the data into packets and pass the data onto the network layer. On the recipient’s computer the transport layer reassembles the packets into the original form. The packets are numbered by this layer to allow them to the reassembled. The transport layer chooses the port number for sender and receiver. TCP and UDP are the main protocols used in this layer.

The **network layer** adds the source and destination IP address and route the packets over the network. At the destination the network layer strips out the IP addresses. The IP operates on this layer.

The **data link layer** has a network card and deals with the physical connection and adds the physical addresses (MAC address) of the hardware to the packets that it receives from the network layer. For each step the sender and receiver MAC address is removed then a new sender and receiver MAC address is added. The receiver MAC address becomes the sender MAC address.


Sender's Computer
Data link Layer
Network Layer IP
Transport Layer TCP, UDP
Application Layer HTTPS,HTTP,FTP,SMTP
Internet
Recipient's Computer
Data link Layer
Network Layer IP
Transport Layer TCP, UDP
Application Layer HTTPS,HTTP,FTP,IMAP