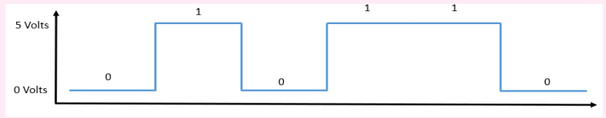
Communication

Communication Methods

Data communication is the transmission of data form one device to another (ge between computers), or between components along a bus within a computer such as between RAM and the processor.

Serial transmission

- one bit at a time are transmitted between computer components. Only a single wire is used.
- Serial transmission down a wire is sent as a change in electrical voltage which is encoded as 0 and 1s.
- The voltages are put on a wire and sent to another computer that can read these voltages and convert back into binary digital data.



Parallel transmission

- Parallel data transmission means that several bits of data are sent at the same time along multiple wires between computer components.
- Often 8 bits, 16 bits, 32 bits, 64 bits are sent at the same time
- Parallel transmission is used to communicate with a networked computer.

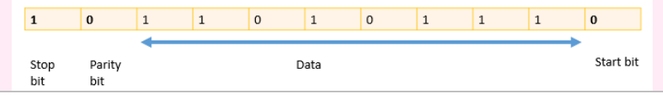
	Advantage	Disadvantages
Serial Transmission	It can be used over longer distances	It is a slow method of data transfer
Parallel Transmission	It is quicker than serial data transfer	Over longer distances bits can get skewed. This results in the bits going out of synchronisation and arriving at different times and therefore out of order. Interference between wires, so the data can become corrupted

Synchronous transmission

- Synchronous transmission requires a clock to allow synchronisation between the sender and receiver
- The sender needs to transmit the data at the same rate that the receiver reads the data.
- The signals are sent at regular intervals in a continuous stream. Timing signals are also sent allowing the sending and receiving clocks to be synchronised

Asynchronous transmission

- The data are sent in chunks normally as one byte or ACSII character.
- The transmission contains a start and stop bit that specify the beginning and end of the sequence and a parity bit for error checking.
- The start bit are used in asynchronous data transmission to prepare the receiver to start receiving data.
- The stop bit resets its state allowing it to read the next sequence.
- The values of the start bit and stop bit must be different. ie if the start bit is 0 then the stop bit is 1 and vice versa.
- Asynchronous transmission is slower than synchronous transmission.



Communication Basics

A **Protocol** is a set of common rules that determine how different devices communicate

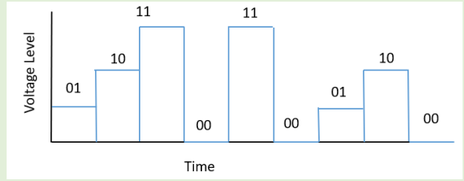
Latency is the delay in data transfer from one component to another. At the most fundamental level the speed of data transfer is limited by the speed of light. Latency is also caused by transmission in the medium itself, and other necessary processing.

Baud rate is the number of changes of signal per second (frequency) and in measure in Hertz

Bit rate is the number of bits transmitted per second.

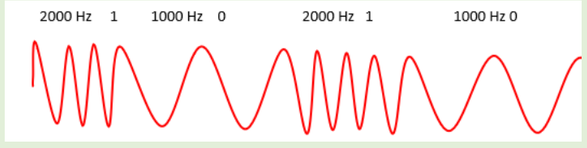
Bit rate = baud rate x bits per signal change

The baud rate will be the same as the bit rate only when one bit is sent for each change of signal. In this situation there are 2 voltage levels representing zero and one. It is possible to send more that 1 bit per signal change. For instance if there are 4 voltage levels, the voltages can be encoded as 00, 01, 10, 11.



Bandwidth

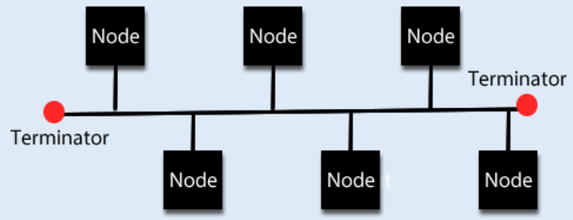
- refers to the range of frequencies at which the data can be transmitted
- relates to the volume of data that can be transmitted along the medium in a given period of time.
- It is expressed in Hertz as the difference between the lowest and highest frequency.
- The greater the bandwidth the greater the capacity of data transfer.
- Data are transmitted using frequency modulation (FM). Different frequencies are used to encode different values.
- Previously when using dial up over the phone cable two frequencies were used (2000 Hz and 1000 Hz) to transmit 0 and 1s.
- Now a greater range of frequencies can be used so a greater number of bits per frequency can be transmitted.
- Noise limits the amount of data that can be sent.
- There is a directly proportional relationship between bandwidth and bit rate. That is the greater the bandwidth the greater the bit rate.



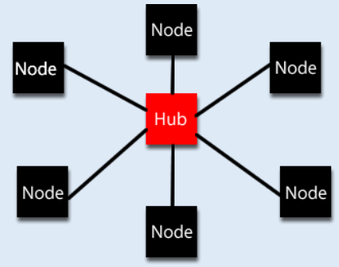
Network Topologies

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

Bus 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.



Star network topology For a star 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	Disadvantages
Bus topology	Easy and cheap to install and does not require much cable. Easy to add more computers	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 topology	Greater security as data are only sent to the intended recipient. If any of the connections fail only a single node will be affected. The rest of the network will work as normal. Fewer collisions between data packets	If the central hub fails then every computer on the network is affected. Expensive as extra cable and hardware (hubs) are needed.

Logical bus network topology

- It is possible that a network that has been physically set up with cables based on one topology can behave as if is has been set up as another topology.
- For instance, a network that has physically been set up at a star topology can behave as a logical bus network.
- In this situation the hub is set up so that communication received from one computer is relayed to all the other devices on the network.

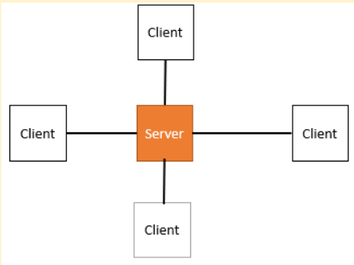
Network types

In a **client server network,** clients are connected to a server which is a central computer that provides services to the clients. These services can include:

- Providing web pages (web server)
- Providing files (file server)
- Access to email (email server)
- Database access (database server)
- Printing (print server)

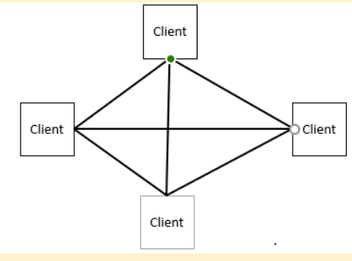
Client-Server Architecture

- The client requests a service or resource from the server
- The server is continuously waiting for a request
- The server responds to the request and waits the next request from the client



In a **peer-to-peer network** all computers are connected to one another. This allows the resources on the each of the computers to be shared with the other computers. There is no server and all computers have equal. This is a cheap network to set up because an expensive server is not needed.

A peer-to-peer network can be used for file sharing. Each computer on the network will have different files. These files can then be shared with other peers. It is also possible that each computer can host different parts of a large file such as a film. This reduces the demand on a single computer.



Wireless Networks

What is the purpose of WiFi

- WiFi uses radio waves at a designated frequency to transmit data and allows devices to be wirelessly networked.
- International Wi-Fi standards are widely used so wireless devices should be able to be attached to any wireless network.

Components for wireless networking

Wireless Access Point

- A wireless access point (WAP) allows other wireless devices to connect to a network.
- Has a range of the order of tens of metres
- For most home wireless networks the WAP is integrated with the router.

Wireless Network Adapter

For a device (eg PC) to connect to a wireless network it needs to have a wireless network adapter. The adapter can send and receive transmissions to the WAP so long as it is in range and operating on the same frequency.

CSMA/CA

Wireless networks will often have multiple nodes each transmitting data packets. The purpose of the Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA) protocol is to reduce collisions between data packets.

CSMA/CA Protocol

1. The node listens to the network (channel) to determine whether data are being transmitted by another node.
2. If the network is busy then the node waits a random period of time. The node keeps listening and waiting until the network becomes clear.
3. Once the network is clear the data can be transmitted.
4. The receiver send an acknowledgement back to the sender.
5. If no acknowledgement is received the data need to be retransmitted.

CSMA/CA with RTS/CTS

If more than one node are send data at exactly the same time then a collision occurs. In this event the data will not be received so there will be no acknowledgement and the sending node will need to transmit. To get around this problem we use CSMA/CA with RTS (Request to Send) / CTS (Clear to Send). Nodes on a wireless network are hidden from one another and communicate through the WAP.

CSMA/CA with RTS/CTS Protocol

1. The node listens to the network (channel) to determine whether data are being transmitted by another node.
2. If the network is busy then the node waits a random period of time. The node keeps listening and waiting until the network becomes clear.
3. The node sends an RTS signal to the WAP, which returns a CTS signal once the network has been confirmed to be clear.
4. The node then transmits the data.
5. The receiver sends an acknowledgement back to the sender.
6. If no acknowledgement is received the data need to be retransmitted.

Securing Wireless Networks

MAC Address whitelist

A MAC address whitelist is a list that only allows devices with a specified MAC address to access the network. The MAC address of a device attempting to connect to the network is checked against the list. If the MAC address of the device is on the list then the device will be allowed to connect to the network otherwise it will not be able to access the network.

Turn off the SSID broadcast

The SSID (Service Set Identifier) is the name given to a wireless network so that it can be identified. WiFi networks often broadcast their SSID. By turning off the SSID broadcast you are hiding the network, but you can still access if already know what the SSID of the network that you are trying to access is.

Encryption

WEP (Wired Equivalent Privacy), WAP (WiFi Protected Access), WAP2 and WAP3 are the principal security protocols used to encrypt the data between the network adaptor and the access point. Therefore if any of the packets are intercepted the packets will at least be encrypted.

Passcode

Passcodes can be added to WiFi networks to prevent unauthorised access to the networks.