Topic 9 Fundamentals of Communication and Networking

Symbol
The term symbol refers to a pattern of bits represented by a signal. For example, a four bit symbol could be 0011.

Baud Rate
The baud rate is the median number of signal changes per second. 1 symbol change per second is 1 Baud, written as 1Bd.

Bit Rate
The bit rate is the number of bits which can be transmitted each second measured in bps (bits per second). The bitrate is the baud rate multiplied by the number of bits per signal.

Bandwidth
Bandwidth is the range of frequencies which can be transmitted and is measured in Hertz (Hz). Higher bandwidth gives a higher bit rate.

Latency
Latency is the difference between an action being initiated and its effect being noticed and is measured in milliseconds (ms). It can be best thought of as a delay, and usually increases with the distance data needs to travel.

Protocol
A protocol is a set of rules regarding communication between devices. This allows devices made by different manufacturers to easily communicate with one another.

Parallel and Serial Data Transmission
Serial Data Transmission
Serial data transmission sends data one bit at a time using a communication channel such as a copper cable or wireless signal. This method is often used for relative medium to long distance transmissions such as from a mouse to the computer.

Serial transmission does not suffer from crosstalk or skew, making it more reliable over longer distances. It is also cheaper than parallel data transmission since it uses a single line.

Parallel Data Transmission
This method uses many parallel communication lines to send many bits at the same time and is usually used between components within the computer. The more lines available, the more data that can be sent at the same time.

Each line within a parallel communication system will have very slightly different electrical properties, meaning that signals will take a very slightly different amount of time to travel across them. As a result, not all data sent at the same time will arrive at

the same time, this problem is known as skew and increases as with the distance between components. In extreme cases this can lead to data overlapping or corruption.

Where parallel communication lines are close to each other crosstalk can occur, where data from one line leaks into or interferes with another, causing data corruption.

Parallel communication methods are more expensive because they use multiple lines, and because of this they are usually used over relatively short distances between internal computer components.

Synchronous and Asynchronous Data Transmission

Synchronous Data Transmission

Synchronous transmission uses a clock signal shared between the sender and receiver to control when data is sent. It is used within processor busses in the fetch-execute cycle. The clock signals are received in the same order in which they were sent, making them well suited to use in real time systems.

Asynchronous Data Transmission

This method removes the need for a clock, and instead uses start and stop bits to indicate transmission duration. The start bit can be either 0 or 1 and the stop bit must be the opposite of the start bit. The sender and receiver have to use the same baud rate but only need to synchronise their clocks for the duration of the transmission.

1	0	1	0	0	1	0	0	1	0	0
Stop Bit	Transmitted Data									Start Bit

Network Topology (Physical)

The physical network topology refers to how the devices within the network are physically laid out and connected.

Star Network Topology

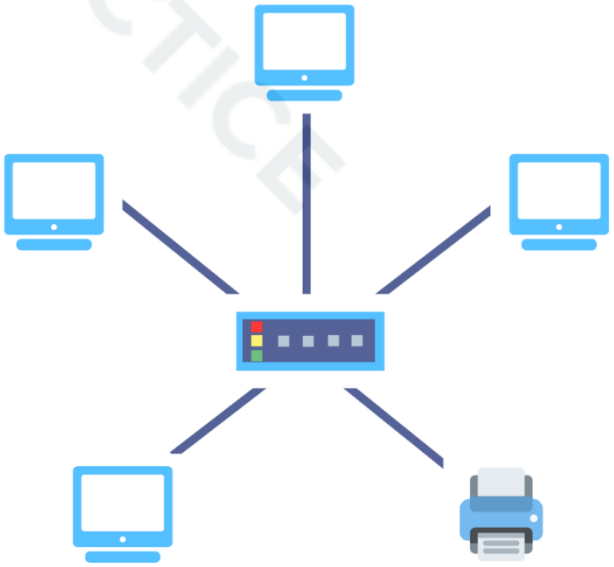
In this topology, each client has its own direct connection to a central hub. The hub receives packets for all clients and delivers them to the correct place. A server is connected in the same way as any other client.

Advantages:

- Packets are sent directly to their recipients and are not seen by other clients.
- It is easy to add or remove clients.
- Each cable has one device, meaning there are no collisions.
- The failure of one cable does not affect the rest of the network.

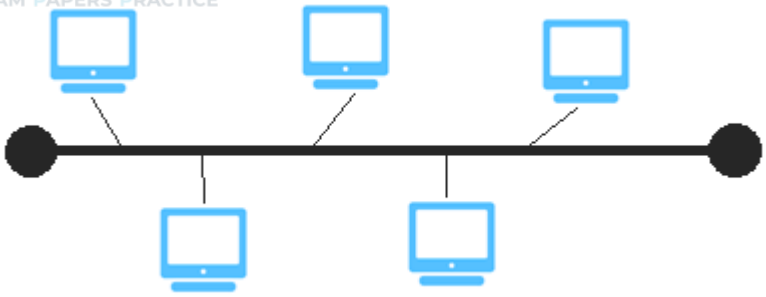
Disadvantages:

- Expensive to install due to the amount of cable required.
- If the central hub fails, the entire network fails.



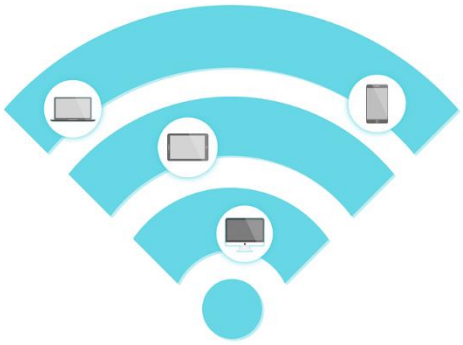
Bus Topology

A central bus connects clients along a single cable, known as a backbone. A terminator is placed at each end of the backbone. There is on central hub and servers can be connected anywhere on the backbone.



Advantages:

- There is no central hub, making the setup cheaper to install and less likely to fail.
- Less cabling is required making it cheaper to install.



Disadvantages:

- Packets sent on the shared backbone can be seen by all clients.
- The backbone is used by all clients, introducing a risk of collisions.
- If the backbone fails, the whole network cannot be used

Logical Network Topology

The logical topology refers to the flow of data packets through the network. A logical bus network delivers packets to all clients on the network. A logical star network delivers packets to only the intended recipient.

Mixed Topologies

Physical and logical topologies can be mixed, for example, it is possible to setup a network in a physical star topology but to behave as a logical bus topology. This could be achieved by using a physical star layout when cabling but operating a bus protocol.

Hosts & Clients

A host is a device on a network which provides services to other systems. This is often a server and could provide file or print services. A client is a device which accesses services from another host on the network. Systems on a network can be both clients and hosts at the same time.

Client-Server Networking

Client-server networks use a central server to provide services to clients on the network. The server is connected to the network in the same way as the client but is usually a more powerful computer.

Clients request services from the server, which responds with the required services. The server could provide file storage, user accounts, print queue or email services. Sometimes a single server provides all services, whilst other times multiple servers are used.

This type of network is commonly used by schools and businesses to allow central management of clients. This improves security but requires additional expertise to set up and manage the network.

Peer to Peer Networking

This setup does not require a central server and instead services are provided by one or more of the clients themselves, with every client having equal status. One client might provide file services, whilst another manages storage for example.

The main disadvantage here is that a client must always be switched on and working in order to provide services, and if a client fails or is switched off the network is not fully operational. On the other hand, it is more cost effective as it does not require a powerful central server to run the network. It is also easier to setup and manage than client-server networks.

This arrangement is used by large file and multimedia sharing networks to provide high performance services without the need for a powerful server.

Wireless Networks

A wireless network allows communication without requiring a physical cable. They require a wireless access point and a wireless network adapter in the client. The wireless access point acts as a bridge between the wired network and the wireless.

<u>WiFi</u>

WiFi is the most commonly used method of providing wireless networks and refers to a wireless network based on international standards.

Traffic travelling over a wireless network should be encrypted using WPA or WPA2 to improve security. WPA stands for WiFi Protected Access and requires clients to enter a key before connecting to the network.

Wireless network security can also be improved by disabling SSID broadcast. The SSID (Service Set IDentifier) is the name used to identify the wireless network. Disabling SSID broadcast prevents wireless clients from seeing the network is there, allowing only clients who know of its existence and the SSID to connect.

MAC Address Filtering uses the MAC (Media Access Control) address built into every network card to control access to the network. A MAC whitelist allows only approved devices to connect to the network and prevents all other devices from connecting. On the other hand, a blacklist allows all devices to connect apart from a set of blocked addresses.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

This protocol is commonly used in wireless networks to avoid data collisions if multiple devices transmit at the same time.

When a device wants to transmit data, it listens to the communication channel to see if it is idle. If it is, the data is transmitted. If the channel is already in use, the device waits a random length of time and tries again. An exponential back off algorithm is used to increase the time period the device waits with each retry.

CSMA/CA suffers from a problem known as hidden nodes. This is where a device cannot see parts of the network where communication might be taking place. To get around this, another protocol called request to send/clear to send (RTS/CTS) is used. This adds an additional step into CSMA which requires the client to send a request to send to the server once it has detected the transmission media is clear.

If the server is idle, it responds with a clear to send message and the client sends its data. If the client does not receive a clear to send message it assumes the server is busy and waits before trying again.