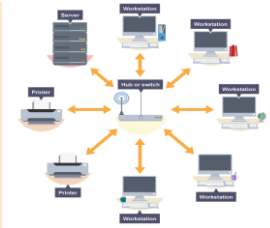
J276 1.5 Network topologies, protocols and layers

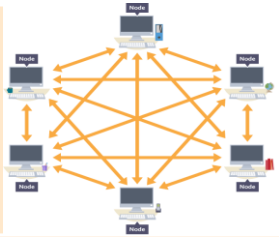
Network Topologies

Star Network



- ✓ Data is only directed to the intended computer directly
- ✓ Network traffic is kept to a minimum
- ✓ If one link fails, all the other devices will continue to operate.
- × If the central point fails then so will the entire network
- × Requires a lot of cable as each computer is connected individually to the central component

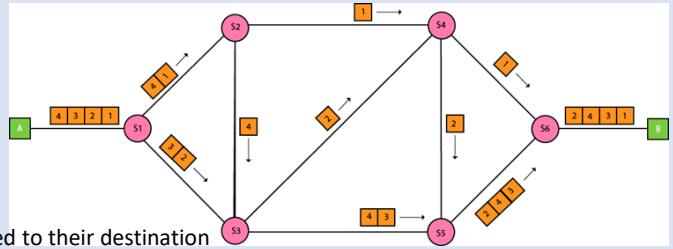
Mesh Network



- ✓ Data can be transmitted from different devices simultaneously
- ✓ If one component fails, there is always an alternative route for data.
- ✓ It can handle high volumes of data traffic
- ✓ Adding more devices will not slow the data transmission
- × Overall cost is high. More cable is required unless a wireless network is used
- × Difficult to managed and requires expert supervision

Packet Switching

1. The sender's large file is broken up into smaller packets



2. Packets are directed to their destination by routers. Routers inspect the packets and decided the most efficient path to the next router.

3. Packets take different routes across the network. They may not arrive in the correct order.

4. The receiving computer assembles them in the correct order using information in the headers.

WiFi Frequencies and channels

Networks can be classified as wired or wireless. A wired network uses cables (copper or fibre optic) to form the connections between the networked devices. Ethernet is a protocol that describes how data is transmitted in wired networks.

A wireless network uses wireless Wi-Fi signals to connect nodes. Wi-Fi signals use radio frequencies in the 2.4 gigahertz (GHz) and 5 GHz wavebands. Each node has a radio transceiver, which allows it to connect to a wireless access point (WAP). WAPs can be physically connected by wire to a network switch, or wirelessly to other WAPs.

Wi-Fi wavebands can be separated into channels, or sub-frequencies. WAPs use several channels to allow many devices to connect wirelessly without their transmissions interfering with one another.

Packets

Data must be transferred between computers as securely and efficiently as possible.
When data is transferred between computers, (e.g. via email or uploading to cloud storage), it is split into **packets** to avoid the high bandwidth needed for large files.
Each packet consists of:

- Header containing the source and destination addresses and the position of the pack in the complete message
- Body containing some of the data
- Footer to inform the receiving device that this is the end of the packet.

Network Protocols

Protocols are the rules that computers must follow when they are communicating and sending and receiving data over a network.

Protocol	Explanation
TCP/IP	Transmission Control Protocol/Internet Protocol – dictates how data is sent between networks over the internet.
HTTP	Hyper text transfer protocol – used by web browsers to access websites and communicate with web servers.
HTTPS	Hyper text transfer protocol secure – more secure version of HTTP as it encrypts all information sent and received.
FTP	File transfer protocol – used to access, edit, and move files between devices on a network
POP	Post Office Protocol – used to be retrieve emails from a server, holds the email until downloaded.
IMAP	Internet Message Access – used to retrieve emails for a server, holds the email until it is deleted.
SMTP	Simple Mail Transfer Protocol – used to send emails and transfer emails between servers,

Encryption

Encryption is the process of disguising a message so that it cannot be understood by anyone but its intended recipient. Encryption requires the use of a key. The key is secret as to how the message has been disguised.

Today, most communications sent via the internet are encrypted in some way:

- purchases made online are encrypted to try to prevent theft of credit card details
- tools enable a user to encrypt a document, such as a spreadsheet, before sending it to a colleague via the internet
- satellite TV transmissions are encrypted to prevent users who are not subscribed from watching TV shows

Network Layers

Network layers are the organisation of software components into functional components.

- **Application layer** - encodes/decodes the message in a form that is understood by the sender and the recipient.
- **Transport layer** - breaks down the message into small chunks (packets).
- **Network layer** - adds the sender's **IP address** and that of the recipient. The **network** then knows where to send the message, and where it came from.
- **Data link layer** - enables the transfer of packets between **nodes** on a network, and between one network and another.

Benefits of organising protocols into layers:

- ✓ The overall model is simplified by dividing it into functional parts
- ✓ Different layers can be combined in different ways as required
- ✓ One layer can be developed or changed without affecting the other layers
- ✓ Allocating specific tasks makes it easier to identify and correct networking errors and problems
- ✓ It provides a universal standard for hardware and software manufacturers to follow so that their devices will be able to communicate with each other

IP address: a unique identifier given to a device when it accesses an IP network. They can be static or dynamic. Either 32 or 128 bit binary numbers.

MAC address: a unique identifier assigned to a device that cannot be changed. They are assigned to all network-enabled devices. They are 48 or 64 bit binary numbers, converted to hexadecimal. Used by Ethernet protocol.