* 1. To share the printer. To share the internet connection. To share files. To communicate with each other e.g. by email.
	2. Bus line shown. Terminators shown at each end of the bus. Three computers attached to bus. Printer attached to bus. Internet connection connected to a router. Network adapters required on each computer. Router needed to share the internet connection. Cables needed to connect the different devices.
	Diagram something similar to
	
	3. 
	4. Points to be made include:
	**How DNS servers are used**: DNS severs have a database of IP addresses. Constantly updated by other DNS servers. When you request an address (URL), the DNS server looks up the URL and returns the IP address, or searches for the address from other DNS servers.
	**Advantages**: People do not need to remember IP addresses. Easily upgradeable (eg IPv4 to IPv6) without all web addresses needing to be the same. As long as you are connected to a DNS server you can have access to all the addresses.

		1. **H**yper**T**ext **M**ark-up **L**anguage. Text file containing the text to be displayed. Uses tags which indicate how to display the text and location of pictures/other elements to include and hyperlinks to other locations/URLs.
		2. Web browser used to interpret the file and display the data correctly. HTML is an open/accepted standard so data will be display correctly on all browsers which conform to the standard.
	5. 

		1. It reduces the size of the file which needs to be transmitted. Shortens download time and reduces internet traffic.
		2. In **lossy compression**, when the data is uncompressed it is not exactly the same as the original but the difference is so small that it cannot normally be noticed e.g. music files (mp3) and images (jpg).
		In **lossless compression**, when the data is uncompressed it is restored completely to the original file e.g. compressed text files or programs.
1. Points may include:
**Physical security measures** – computers/servers in locked rooms, lockdown cables for laptops.
**Firewalls** – allow only authorised access to the network.
**User groups/access levels** – different users are given different rights to data according to their responsibility/need to protect privacy.
**Passwords enforced** – should be strong and changed regularly. Ensures privacy and protects files being accessed by malicious hackers.
**Encryption** of data on the network.
**WiFi access security**.
Get employees to sign an **Acceptable Use Policy** as part of their contract to ensure they do not put data at risk of corruption and to abide by data protection legislation.

	1. Local Area Network / A network which covers a small area like a building
	2. Can share files. Can share resources (e.g. printer/scanner/internet connection). Computers can be managed/controlled centrally. Users/computers can communicate with each other.
	3. A hub/server at the centre of the network. All computers attached to the hub/server. Resources (e.g. printer) can also be connected to the hub/server.
	
	4. The star topology requires all workstations to be connected to a central point so a hub/switch is needed. The computers need to be physically or wirelessly connected to the hub so cables and network interface cards or a wireless access point and WiFi adapters will be needed.
	5. 
		1. Different users only have permissions to files/areas/services of the network which they actually need eg the public should only be able to search eg only employees should issue books eg only managers can look at pay records. To prevent malicious or accidental corruption of parts of the network.
		2. Stops all access to/from the WAN unless it has been authorised Eg requests from other libraries. Prevents hackers from compromising the system.