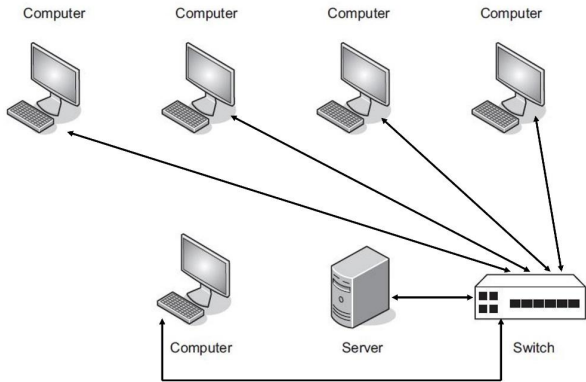


5(a)	1 mark per bullet point, max 2 marks - Covers a small geographical area - Normally privately owned / dedicated infrastructure - Can use wired or wireless communication
5(b)	1 mark per bullet point, max 2 marks - All computers directly connected to switch and no other connections - Switch connected directly to server 
5(c)	1 mark per bullet point, max 3 marks - The sending device sends the packets to the switch - The switch checks the destination address on each packet ... and sends them only to the intended receiver
5(d)	1 mark per bullet point, max 3 marks - The use of <u>CSMA/CD</u> // Carrier Sense Multiple Access with Collision Detection - The workstations listen to the communication channel ... and send data only when there is no data being transmitted / the line is idle - If a collision is detected, transmission is aborted ...and a jamming signal is sent - The workstation calculates a random wait time before trying to re-transmit - The random time is increased if there are multiple collisions

5(e)

1 mark for correct threat

1 mark corresponding description

1 mark for correct method of prevention

Threat	Description	Prevention
Malware / Virus	Malicious code that can alter/delete files	Anti-virus // Anti-malware // Firewall
Spyware	Records keystrokes which are sent to third party	Anti-spyware // Firewall // Anti-malware
Hacking	Gaining <u>unauthorised</u> access to a computer network / device	Authentication // Firewall
Phishing	<u>Emails</u> supposedly from reputable companies are sent to trick people into revealing personal information	Use a spam filter // Do not open emails from unknown sources
Pharming	Users are directed to a bogus <u>website</u> that looks legitimate to obtain personal information	Use a VPN // Anti-malware// Do not open links or download attachments