Q1

(a)

(i)

Issues and considerations to be taken in include,

1. Who will the people be connecting to the network as it could be Employees, or customers.
2. Will the enterprise connect to many local branches or just one and whether they will be remote.
3. The users who connect may have different authorization levels.

(ii)

Issues and considerations to be taken in include,

1. The scope of the wan could be on a local, regional, or global scale.
2. What method will be used from one to one, one to many, or many to many

(ii)

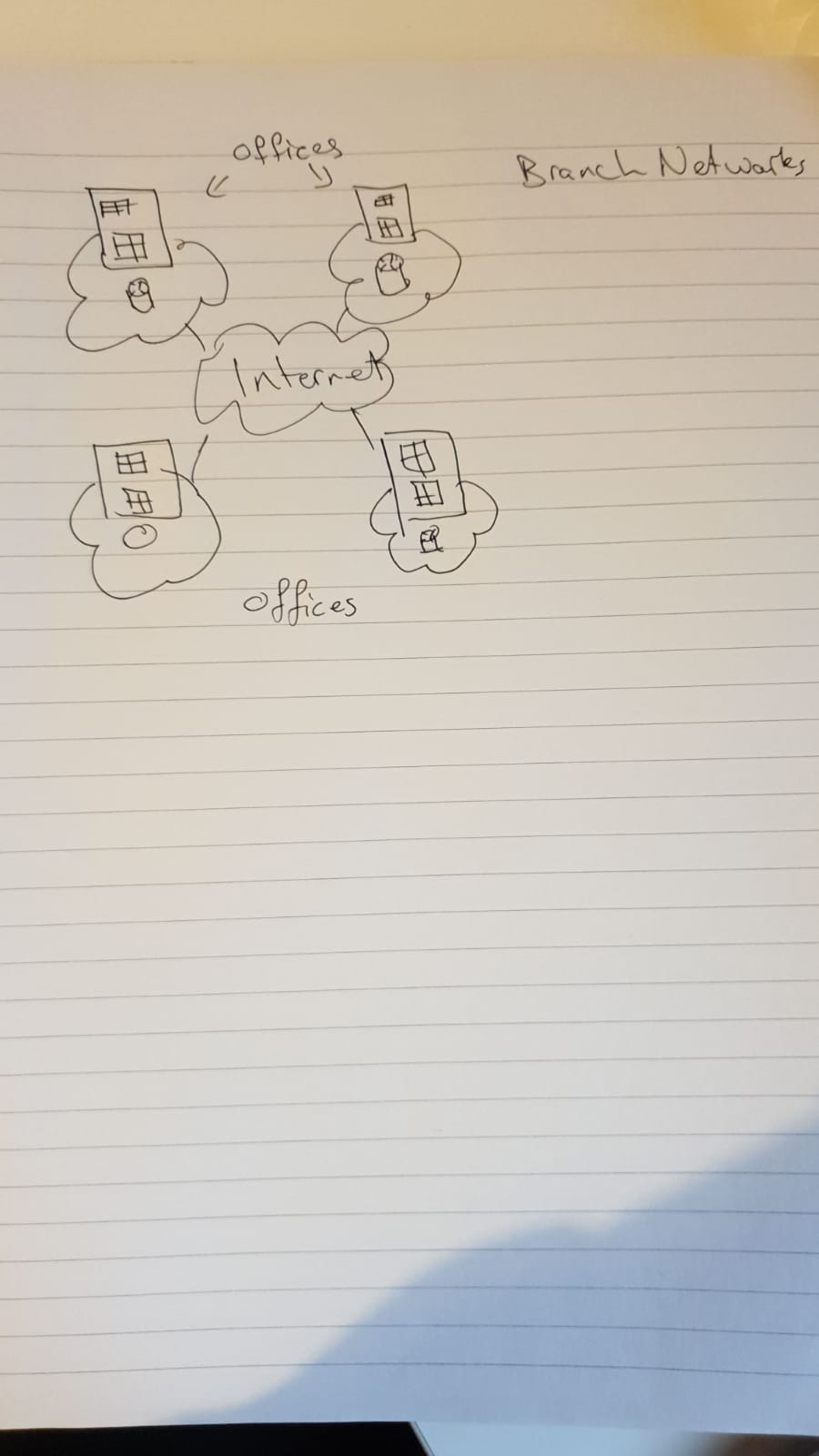
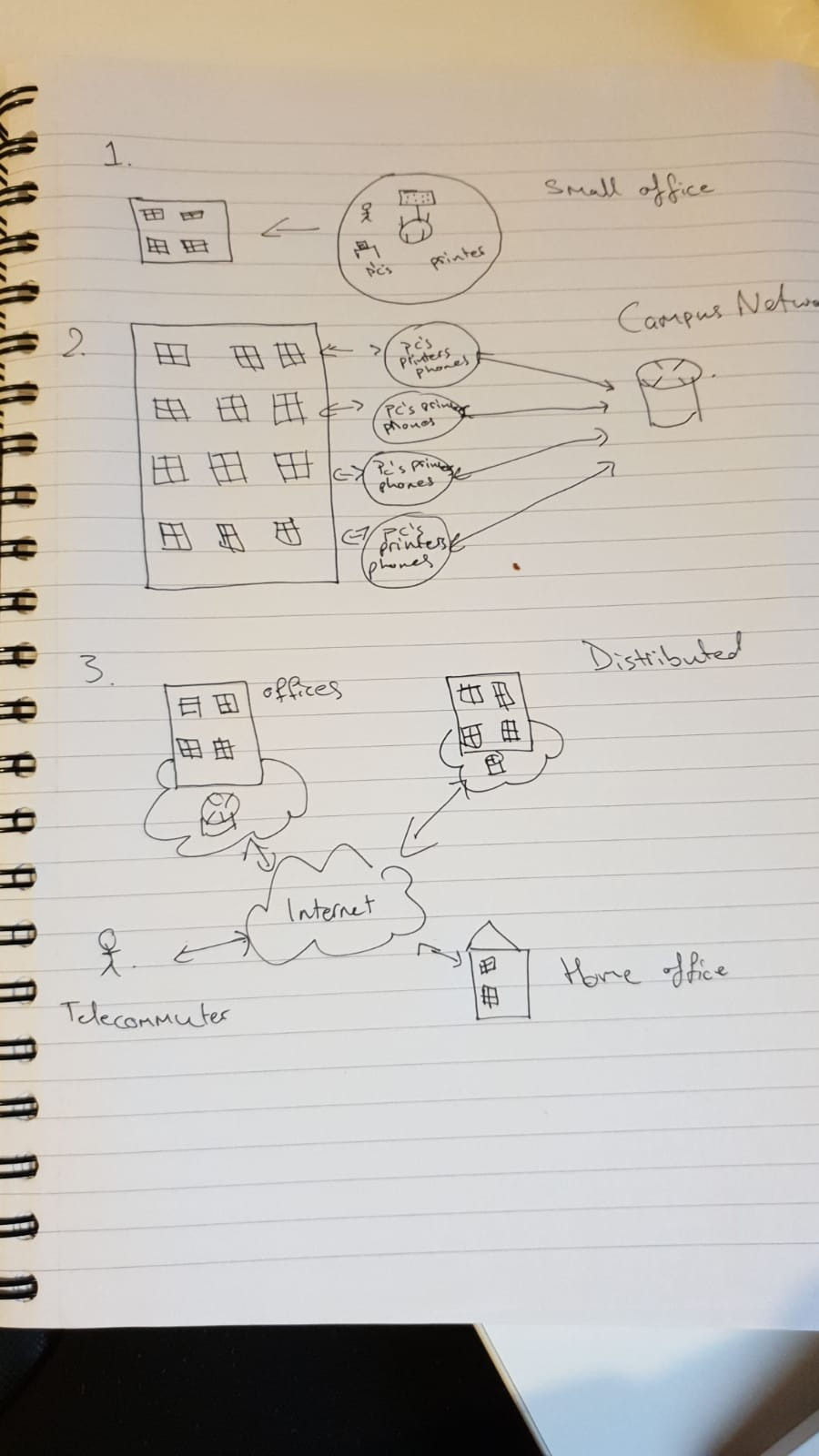
Issues and considerations to be taken in include,

1. The type of traffic as this business has many. This will affect the quality and performance of connections.
2. The volume of Data that must be factored into the connection to ensure reliability.
3. Security measures that need to be taken into account to secure the network.

(b)

Wan topologies that can be used:

1. Small office: usually business with only one LAN at one location, that connects to internet through a broadband technology
2. Campus network: Small- to medium size business that has multiple LAN’s with one location, with Business grade equipment to connect to the internet
3. Branch Networks: Multiple locations with multiple LANs. Use wan contracts to connect to the internet
4. Distributed Network: Many locations with many ways to access the network. Very complex WAN strategies to securely connect different regions and sites.



(c)

Design issues when implementing a teleworker infrastructure:

1. The connection needs to be constantly secured, which relies on the service provider.
2. Home office solutions require a laptop/desktop with VPN client software to eb installed, which the teleworker may not know to use themselves.
3. The office end has to be well equipped with VPN- capable routers, and multifunction security application to authenticate and secure the connections as well .

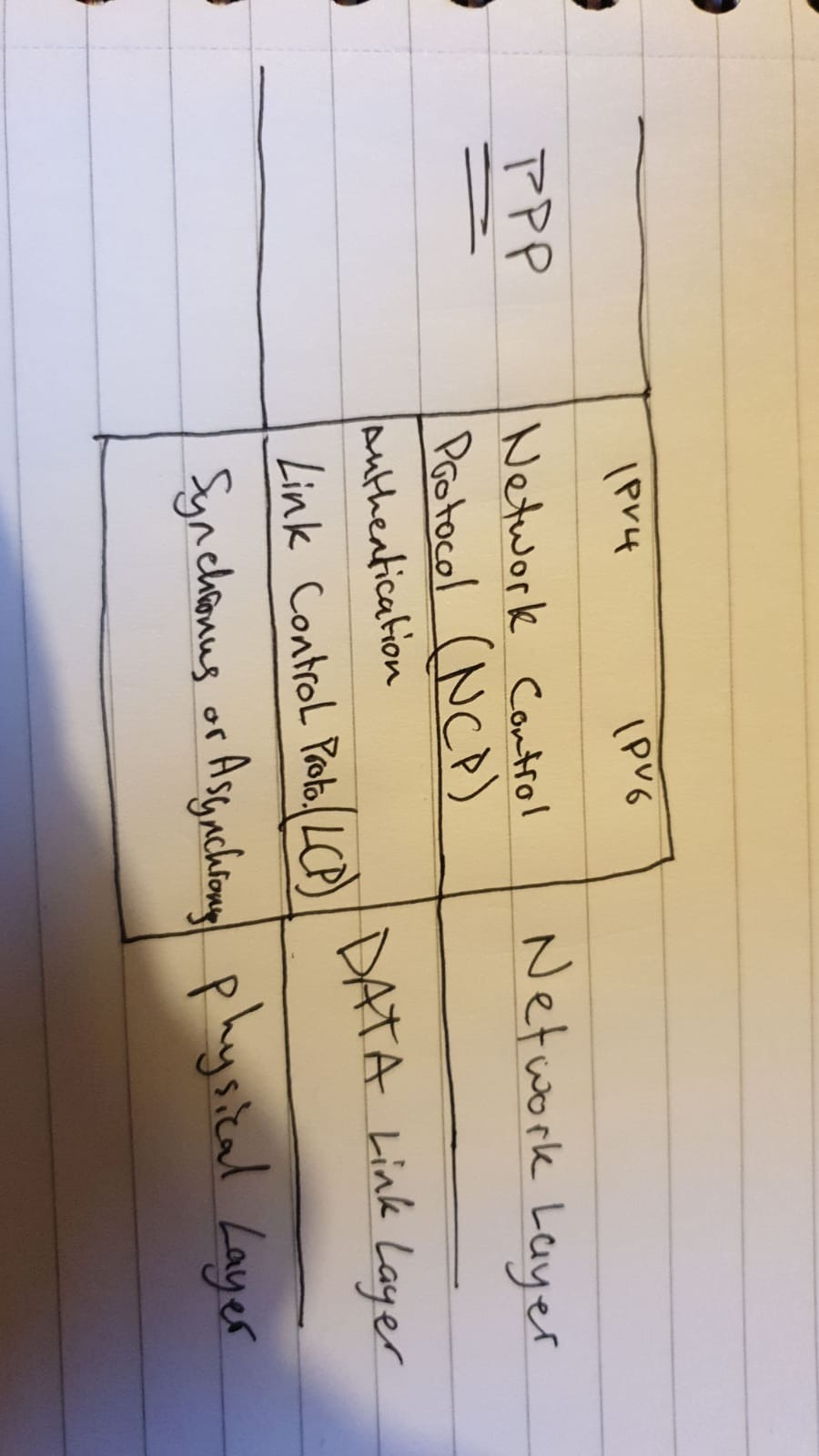
Q2

(a)

PPP is a WAN protocol that works at layer 2 by encapsulating frames for transmission over a variety of physical links such as serial cables, cell phones, fiber optic cable among others. it offers many more features as compared to HDLC and it is an open standard. Point-To-Point also includes authentication methods using PAP or CHAP. LCP and NCP in the second layer and third layer respectively in the osi model, is where they function.

(b)

The PPP and OSI Model share the same physical model however PPP spreads the LCP and NCP in the Data Link, and Network Layer. The requirement that PPP has is that there is a full duplex circuit, that can operate in an asynchronous or synchronous bit-serial mode.



(C)

(i)

The four phases that PPP go through is:

1. **Link establishment and configuration negotiation.** Originating PPP node sends LCP frames to configure and establish the data link.
2. **Link quality determination.** Link is tested to determine whether the link quality is sufficient to bring up network layer protocols.
3. **Network layer protocol configuration negotiation.** Originating PPP node sends NCP frames to choose and configure the network layer protocols.
4. **Link termination negotiation**. Link remains configured for communications until NCP or LCP frames close the link or some external event happens.

(ii)

The two protocol sublayers are LCP and NCP.

LCP

* LCP establishes the PPP link and negotiates and sets up control options on the WAN data link which is handled by NCP.
* LCP also agrees on the encapsulation such as authentication and error detection

NCP

* PPP permits multiple network layer protocols to operate on the same comms link. For every network layer used, there is a separate NCP
* NCP manages the needs required by its respective layer protocols.

(iii)

The two authentication configurations are PAP and CHAP.

PAP

* Very basic two-way process that does not use encryption, with the username and password sent in plain text

CHAP

* More secure three-way exchange of a shared secret. Chap is more secured and therefore more recommended from a security stand point.

Q3

(a)

VPNs are an end-to-end private network connection, used over the public internet. There are many benefits to VPNs such as cost saving, scalability, compatibility with broadband tech, and very importantly security. The most common two types of VPNs are Site-to-Site and remote Access

(b)

There are many benefits to VPNs such as:

* Cost-saving: compared to other solutions to connecting to a secured network VPNs are extremely cost-effective solutions,
* scalability: it is very easy to scale up or down the number of users on VPN connections,
* compatibility with broadband tech: Household and third-party broadbands can allow users to connect to the network so there is very little requirements on the users end,
* and very importantly security: VPNs are easy to manage and it is very important to be securing the connection from malicious attackers.

(c)

The most common two types of VPNs are Site-to-Site and remote Access

Site-to-Site

•Site-to-site VPNs connect entire networks to each other, for example, they can connect a branch office network to a company headquarters network.

Remote Access

•Remote-access VPNs are used to connect individual hosts that must access their company network securely over the Internet.

