- **Differentiate between various networking approaches, namely, internet and intranet.**

When you apply web technology within an organisation, you get an intranet, and thus - from a strictly technical standpoint - intranets are almost identical to the public Web on the Internet (Stenmark, 2005). However, the Internet and intranet are two distinct networking approaches used in various contexts. This is how they differ:

Internet: The Internet is a global network of interconnected computers and servers that use the standard Internet Protocol (IP) to communicate. Its vast network allows people and organisations to access and share information, display, and conduct transactions. The Internet is a public network that is accessible to everyone with an internet connection, and it is often referred to as the "World Wide Web". The Internet is governed by various organisations and is subject to different regulations and laws (Leiner, 2009).

Intranet: An intranet is a private network designed for use within an organisation or a specific group of people. It is a closed network that can only be accessed by authorised users who are connected to the network. Intranets are used to share information, collaborate on projects, and communicate within an organisation. Intranets often include features like email, chat, document sharing, and other tools specific to the organisation's needs. Intranets are generally more secure than the Internet, as firewalls and other security measures protect them (Clark, 2003).

In summary, the Internet is a global network that allows people and organisations to access and share information. At the same time, an intranet is a private network designed for use within an organisation or a specific group of people. The main difference between the two is that the Internet is accessible to everyone. At the same time, an intranet is a closed network that authorised users can only access.

- **Identify various network topologies and appreciate the technologies and protocols that make these networks work.**

Every network has a topology that governs how various devices are arranged and communicate. Physical and logical topologies are distinguished. The former refers to the network's physical layout or how devices are physically connected via cables or direct wireless communication links (Espina, 2014). According to Clark, M.P. (2003), a network topology refers to a network's physical or logical layout. There are several network topologies, each with its advantages and disadvantages. For instance, here are some of the most common network topologies:

Bus Topology: All devices are connected to a single communication line in a bus topology. The devices share the same line, and data is transmitted from one end to the other. The bus topology is simple and inexpensive but can be prone to network congestion and data collisions.

Ring Topology: In a ring topology, devices are connected in a circular pattern, and data is sent in a single direction around the ring. The ring topology is efficient and reliable, but it can be expensive to install and maintain.

Star Topology: A star topology connects devices to a central hub or switch, and all communication is routed through the hub or switch. The star topology is easy to install and maintain. Still, it can be expensive if many devices need to be connected.

Mesh Topology: In a mesh topology, all devices are connected. This topology provides redundancy and is highly reliable, but it can be expensive and difficult to maintain.

These networks operate using a variety of technologies and protocols, including:

Ethernet: Ethernet is a standard protocol for connecting devices in a local area network (LAN). Ethernet is reliable, scalable, cost-effective, and the most commonly used LAN technology.

Wi-Fi: Wi-Fi is a wireless networking technology that allows devices to connect to a network without needing physical cables. Wi-Fi uses radio waves to transmit data and is commonly used for connecting mobile devices and laptops to the internet.

TCP/IP: The Transmission Control Protocol/Internet Protocol (TCP/IP) is a standard protocol for online communication. It is a reliable and secure protocol ensuring data is transmitted correctly and securely.

VPN: A Virtual Private Network (VPN) is a secure way to connect to a network over the internet. A VPN allows remote workers to access a company's intranet securely and provides a secure connection for sensitive data.

In summary, there are several network topologies, each with its advantages and disadvantages. Various technologies and protocols such as Ethernet, Wi-Fi, TCP/IP, and VPN make these networks work.

- **Critically review a topology selection for a network and review the cybersecurity threats.**

Topology selection is essential in designing a network that meets business requirements and provides optimal performance, scalability, and security. There are various topologies, such as star, bus, ring, mesh, hybrid, etc. Each topology has strengths and weaknesses, and the selection should be based on the organisation's

needs, budget, and security requirements. In this review, I will consider the star topology and discuss the cybersecurity threats that can affect it.

The star topology is a network configuration where every device is linked to a central hub or switch. It is a widely used topology in local area networks (LANs) due to its simplicity, ease of installation, and scalability. The central hub or switch acts as a mediator between devices, managing the flow of data and preventing collisions. This topology is ideal for small to medium-sized businesses with a limited number of devices and a limited budget.

One of the main advantages of the star topology is its ease of management. Each device is connected to the central hub, making it easy to identify and isolate any issues that may arise. The hub or switch can also control the data flow, ensuring each device receives the necessary information without interfering with other devices. Star topology makes it an ideal topology for businesses requiring high reliability and uptime.

However, the star topology has weaknesses, particularly regarding cybersecurity threats. One of the primary concerns is the central hub or switch. Suppose hackers gain access to the hub or switch. In that case, they can access the entire network and all connected devices, losing sensitive data and causing system downtime and reputational damage. Therefore, securing the central hub or switching with strong passwords, firewalls, and other security measures is crucial.

Another cybersecurity threat to the star topology is the use of rogue devices. These unauthorised devices connect to the network, often without the network administrator's knowledge, and can be used to launch attacks on the network or steal sensitive information. To prevent this, network administrators should implement network access control (NAC) policies to restrict unauthorised access.

Finally, the star topology is vulnerable to network congestion. Suppose too many devices are connected to the central hub or switch. In that case, it can result in slower network speeds and decreased performance, making the network more vulnerable to cyber-attacks, particularly those that rely on overwhelming traffic. To prevent this, network administrators should implement Quality of Service (QoS) policies to prioritise critical traffic and ensure the network operates efficiently.

In conclusion, the star topology is a helpful network topology that offers simplicity, ease of installation, and scalability. However, it is essential to consider the cybersecurity threats that can affect this topology and implement appropriate security measures to protect against them, which includes securing the central hub or switch, implementing network access control policies, and ensuring network efficiency through QoS policies.

Reference: (Rawal, 2022).

References:

Stenmark, D. (2005). How Intranets Differ From The Web: Organizational Culture's Effect on Technology.

Leiner, B.M., Cerf, V.G., Clark, D.D., Kahn, R.E., Kleinrock, L., Lynch, D.C., Postel, J., Roberts, L.G. & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM computer communication review*, *39*(5), pp.22-31.

Clark, M.P. (2003). *Data networks, IP and the Internet: protocols, design and operation*. John Wiley & Sons.

Espina, J., Falck, T., Panousopoulou, A., Schmitt, L., Mülhens, O. & Yang, G.Z. (2014). Network topologies, communication protocols, and standards. *Body sensor networks*, pp.189-236.

Rawal, B.S., Manogaran, G. & Peter, A. (2022). Cybersecurity and Identity Access Management. Springer.