# Research

1. Conduct research on the following topics and write a brief summary of each:

* Types of Computer Networks:
* Local Area Network (LAN): A LAN is a network that connects devices within a limited geographical area, such as an office building or a school. It allows for easy sharing of resources such as printers, files, and internet access.
* Wide Area Network (WAN): A WAN is a network that spans a large geographical area, such as a city, country, or even the world. It connects devices over long distances and is often used by organizations with multiple branches or offices in different locations.
* Metropolitan Area Network (MAN): A MAN is a network that covers a larger area than a LAN but smaller than a WAN. It connects devices within a city or metropolitan area, such as a university campus or a hospital.
* Personal Area Network (PAN): A PAN is a network that connects personal devices such as laptops, smartphones, and tablets, usually over a short distance, such as within a room or a building.
* Networking Protocols:
* Transmission Control Protocol/Internet Protocol (TCP/IP): TCP/IP is the most widely used protocol on the internet. It is responsible for breaking down data into packets and transmitting them across a network.
* Hypertext Transfer Protocol (HTTP): HTTP is a protocol used for transferring web pages over the internet. It allows clients (such as web browsers) to request web pages from servers and receive the responses.
* File Transfer Protocol (FTP): FTP is a protocol used for transferring files over the internet. It allows users to upload and download files between a client and a server.
* Simple Mail Transfer Protocol (SMTP): SMTP is a protocol used for sending email over the internet. It defines how email messages should be transmitted from one server to another.
* Domain Name System (DNS): DNS is a protocol used for translating human-readable domain names (such as www.google.com) into IP addresses, which are used by computers to communicate with each other.
* Network Hardware Components:
* Router: A router is a networking device that forwards data packets between computer networks. It connects multiple networks together, such as a LAN and a WAN, and allows devices on those networks to communicate with each other.
* Switch: A switch is a networking device that connects devices on a single network. It allows devices to communicate with each other by forwarding data packets to their intended destinations.
* Modem: A modem is a device that converts digital signals from a computer into analog signals that can be transmitted over a phone line or cable line. It allows devices to connect to the internet using a wired or wireless connection.
* Network Interface Card (NIC): A NIC is a hardware component that connects a computer to a network. It allows the computer to send and receive data over the network and is essential for connecting to the internet or other networks.

The TCP/IP protocol and a router:

TCP/IP is a protocol suite that includes two main protocols: Transmission Control Protocol (TCP) and Internet Protocol (IP). TCP breaks data into smaller packets and adds sequence numbers to ensure reliability, while IP is responsible for routing the packets to their destination.

A router, on the other hand, is a network device that connects multiple networks together and forwards data packets between them. It uses IP addresses to determine the best path for packets to take, based on information in its routing table.

When a device on one network sends data to a device on another network, the data is broken into packets by TCP and sent to the router. The router uses its routing table to determine the best path for the packets to take to reach their destination, and forwards them along the way. The router also performs network address translation (NAT), which allows multiple devices on a LAN to share a single public IP address, enabling them to access the internet.

In summary, TCP/IP and routers work together to facilitate network communication by breaking data into packets, routing the packets to their destination, and allowing multiple devices to share a single public IP address. This enables devices on different networks to communicate with each other and access the internet.

# Part 2: Analysis

1. Consider a hypothetical scenario in which a small business needs to set up a computer network. What type of network would be best suited for their needs? Justify your answer.

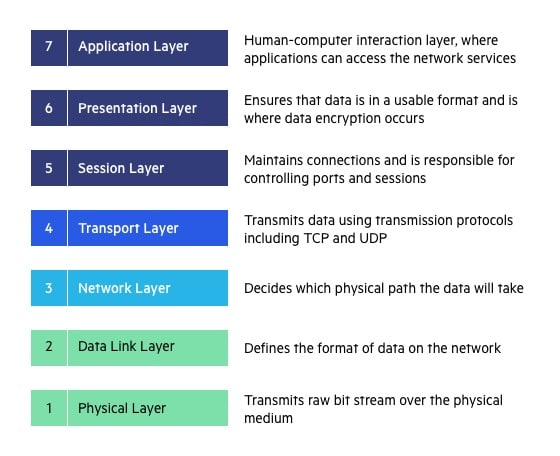
If the business is relatively small with a single location, a Local Area Network (LAN) would be the most appropriate type of network. A LAN is a network that covers a small geographic area, typically within a single building or campus. It allows devices to communicate with each other and share resources such as printers and files. Setting up a LAN is relatively simple and cost-effective, making it a good choice for small businesses.

1. Explain how the OSI model is used to facilitate communication between devices on a network. Provide an example of how information is transmitted through each layer.

Each layer of the OSI model performs specific functions that are necessary for the transmission of data. When a device sends data to another device on a network, the data is passed down through each layer of the OSI model. Each layer adds its own header and data to the data that was received from the layer above it, creating a packet that is sent to the layer below it. The packet is then transmitted over the network to the receiving device, which then processes the packet in reverse order, with each layer removing its own header and data until the original data is reconstructed.

An example of how information is transmitted through each layer of the OSI model is as follows:

* Physical layer - Converts the data into electrical or optical signals that can be transmitted over the physical medium, such as a cable or wireless signal.
* Data link layer - Adds a header to the data that includes the source and destination MAC addresses, and checks for errors in the transmission.
* Network layer - Adds a header to the data that includes the source and destination IP addresses, and determines the best path for the data to take through the network.
* Transport layer - Adds a header to the data that includes the source and destination port numbers, and ensures that the data is transmitted reliably.
* Session layer - Establishes, manages, and terminates sessions between devices, and manages data synchronization and recovery.
* Presentation layer - Formats, encodes, and encrypts the data for transmission, and decodes and decrypts the data upon receipt.
* Application layer - Provides access to network services and applications, such as email, web browsing, and file sharing, and includes protocols for specific applications.



# Part 3: Application

1. Imagine you are a network administrator for a company and you have just received a report of a network outage. What steps would you take to troubleshoot the issue and restore network connectivity?
2. Check physical connections: Ensure that all cables are securely connected to the appropriate ports on the devices and that there are no loose or damaged cables.
3. Check power: Ensure that all devices are powered on and that the power supply is functioning correctly.
4. Restart devices: Try restarting the devices that are experiencing connectivity issues, such as the router, switch, or computer.
5. Check IP addresses: Ensure that each device has a valid IP address and that the subnet masks and default gateways are configured correctly.
6. Ping devices: Use the ping command to test the connectivity between devices on the network. This can help determine if the issue is with a specific device or the network as a whole.
7. Check firewall settings: Ensure that firewall settings are not blocking network traffic and that the appropriate ports are open.
8. Check DNS settings: Ensure that DNS settings are configured correctly and that devices can resolve domain names to IP addresses.
9. Check network logs: Check the network logs on devices to determine if there are any errors or issues that may be causing connectivity problems.
10. Update firmware: Check for firmware updates for network devices and update them if necessary.

Develop a plan for securing a wireless network against unauthorized access. Your plan should include specific security measures and protocols.

* Change default SSID and Password: The first step is to change the default SSID and password of the wireless network. This helps to prevent unauthorized access by making it more difficult for attackers to guess or obtain the credentials.
* Enable encryption: Enable Wi-Fi Protected Access (WPA2) or Wi-Fi Protected Access III (WPA3) encryption on the wireless network. This encryption helps to protect the wireless network by encrypting all data transmitted over the network.
* Disable SSID Broadcast: Disable the broadcasting of the SSID, which makes it harder for attackers to identify the wireless network and reduces the chances of unauthorized access.
* MAC Address Filtering: Configure the wireless router to only allow devices with specific MAC addresses to connect to the network. This adds an extra layer of security by ensuring that only authorized devices can connect.
* Firewall: Configure the firewall on the router to block unauthorized access attempts and to allow only authorized traffic.
* Regular Password Changes: Set a schedule to regularly change the password of the wireless network, and ensure that all devices connected to the network also have strong and updated passwords.
* Regular Firmware Updates: Regularly update the firmware of the wireless router to ensure that known security vulnerabilities are patched and the latest security features are in place.
* Segmentation of Networks: Segmentation of networks through the use of VLANs, Subnets or other technologies helps to reduce the surface area of attack by isolating sensitive systems and data from other network traffic.

Reference:

1. Cure, A. (2015). C#/.NET/Core Training in Denver, CO – May 2019. *www.cypressdatadefense.com*. https://www.cypressdatadefense.com/blog/unauthorized-data-access/
2. *Types of Computer Network - javatpoint*. (n.d.). www.javatpoint.com. https://www.javatpoint.com/types-of-computer-network
3. *Types of Network Protocols and Their Uses*. (n.d.). https://www.w3schools.in/types-of-network-protocols-and-their-uses
4. Barney, N., & Lutkevich, B. (2022). network security. *Networking*. https://www.techtarget.com/searchnetworking/definition/network-security#:~:text=Why%20is%20network%20security%20important,stolen%20assets%20and%20reputational%20harm.
5. GeeksforGeeks. (2021). How Communication happens using OSI model. GeeksforGeeks. <https://www.geeksforgeeks.org/how-communication-happens-using-osi-model/>
6. Raza, M. (n.d.). OSI Model: The 7 Layers of Network Architecture. BMC Blogs. <https://www.bmc.com/blogs/osi-model-7-layers/>