|  |
| --- |
| **Assignment Brief** |
| You are employed as a Network Engineer by organization, a high-tech networking solution development company, which have branches across the world  The company has been contracted to implement a networking project from a local educational institute. The specification of the project is given below:  People: 20 students, 2 teachers, 2 marketing and administration staff, 2 higher managers including  the head of academics and the program manager, 1 computer network administrator. (The learner should provide names to the systems, which should be unique from others)  Resources: 10 student lab computers, 1 staff computers,1 admin computer 1 printers. (the number of servers, routers, switches, hubs, NICs, Cables, Repeaters etc. should be specified by the learner)  Building: One floor, all computers and printers are on the same floor.  As a first task, the CEO of the company has asked you to investigate and explain networking  principles, protocols and devices and submit a report.  **Part 1**  You will need to produce a report that includes the following:   1. An introduction to provide an overview of your report. 2. Benefits and limitations of different types of networks and networking standards. 3. The impact of network topology, speed of communication and bandwidth requirements. 4. Effectiveness of networking systems. 5. Discussion on networking devices and server types. 6. Explore a range of server types and justify the selection of a server, considering a given scenario regarding cost and performance optimization. 7. For the given specification, identify the topology protocol for the efficient utilization of a networking system.   The CEO is happy with your first report and now he has asked you to analyze the specification  from the institution, as given earlier.  You need to design and implement the networking project within a given timeframe:  **Part 2**  Design efficient networked systems   1. Prepare a written step-by-step plan of how you are going to design a Local Area Network including a blueprint of your LAN. 2. Justify your choice of devices for your network design. 3. Produce a test plan to evaluate this design for the requirements of bandwidth and cost constraints as per user specifications. 4. Justify the security requirements and quality of services needed for selection of accessories. 5. Suggest a maintenance schedule to support the networked system.   **Part 3**  Implement test and diagnose networked systems   1. Implement a networked system based on your prepared design. 2. Conduct verification with e.g. Ping, extended ping, trace route, telnet, SSH, etc.(screenshots to be attached) 3. Record the test results and analyze these against expected results. 4. Investigate what functionalities would allow the system to support device growth and the addition of communication devices. 5. Discuss the significance of upgrades and security requirements in your recommendations. |

**LO1: Examine networking principles and their protocols**



**1.1: INTRODUCTION**

This assignment provides an overview of all the aspects related to networking and a comprehensive explanation of all the factors that are involved in the process of networking. the assignment also contains a sample network and its examination and implementation supported by feedback questions.

**1.2:**

**P1: Discuss the benefits and constraints of different network types and standards.**

A network is a collection of a connection of computers, servers, peripheral or other network devices to allow the sharing of data (Different types of networks, standards and protocols available, 2021).   
In the linked world of today, networking is essential for promoting resource sharing, communication, and cooperation between people, groups, and machines. Networking promotes the smooth movement of information, access to common resources, and effective use of technology by creating links between multiple groups. The notion of networking will be thoroughly examined in this part, along with its main benefits.  
  
**Networking for Communication:**

Facilitating effective communication is one of the main goals of networking. Networks offer a framework for data and information transmission between devices, enabling people and organizations to interact remotely and share ideas. Globally accessible, quicker, and more dependable communication has been made possible by the development of the internet and modern networking technology.

**Networking for Information Access:**

Access to the massive volumes of data and resources on the internet and intranets is made easier through networking. Through networks, people may access digital libraries, search engines, online databases, and other knowledge repositories, facilitating effective information retrieval and study. Additionally, networks offer connectivity to cloud services, enabling on-demand access to software, data storage, and computing capabilities.  
  
Following are the different types of networks along with their benefits and constraints:

**Local Area Networks (LAN):**

LAN is a high-speed system of communication which is configured to connect together the computers and networking devices that work together in a small geographical location. (Sherry, 2021)

**Benefits:**

* Lower investment costs
* Devices connected through LAN can easily share and transfer data among each other.
* Devices can connect to other peripheral devices such as printers.
* Security protocols can easily be installed to prevent hackers.
* High-speed communication within a limited geographic region.
* Deployment is affordable, especially for small businesses.
* Efficient resource sharing, including the use of printers and storage devices.
* Security measures that are simple to deploy can prevent unauthorized access.
* Enhanced user communication and productivity inside the LAN environment.
* Data confidentiality and integrity are ensured by simple installation and monitoring of security mechanisms.

**Constraints:**

* Limited coverage area, generally confined to a single building or campus, limiting connectivity outside LAN bounds.
* If there are more connected devices than the LAN can handle, there might be network congestion and performance problems.
* Greater susceptibility to localized failures since any connected user might be impacted by a problem with the LAN server.
* It is difficult to expand the LAN infrastructure to handle large expansion because to the limited scalability.
* Dependence on a single LAN administrator, which might cause delays in maintenance and troubleshooting.

**Wide Area Network (WAN):**

WAN is a collection of a number of LANs and other networks spread over a large geographical area and connected through a router. It covers larger distances compared to other types. (Mitchell, 2021)

**Benefits:**

* Broad coverage area that connects geographically scattered places and allows for long-distance communication.
* Effective resource sharing and centralized data management between several sites.
* Allows for remote access to data and apps, facilitating a mobile and remote workforce.
* Enables multinational organizations’ networking and collaboration on a global scale.
* High availability and dependability are ensured through redundancy choices and load balancing strategies.
* Supports the use of cutting-edge networking tools for secure remote access, such as virtual private networks (VPNs).
* Permits the integration of many network service providers, offering flexibility and cost optimization.

**Constraints:**

* Specialized equipment, connectivity choices, and network service subscriptions are required, which results in higher initial investment costs.
* Less secure than LANs, requiring additional security measures like firewalls, VPNs, and encryption.
* WAN performance is vulnerable to service interruptions and outages due to reliance on external network service providers.
* There is a chance that performance will suffer because of the increased delay brought on by long-distance data transfer.
* Complex requirements for network configuration and design necessitate the use of expert network engineers to assure appropriate execution.
* When establishing connections across networks in many nations and jurisdictions, legal and regulatory compliance are important factors.

**Metropolitan Area Network (MAN)**

MAN is a network that connects its users that are located within a geographical area which is larger than LAN but smaller than that covered by WAN. It is a larger controllable network in comparison to other network types. (Wright,2021)

**Benefits:**

* Covers a greater geographical area than LANs, such as a city or metropolitan region, allowing communication between numerous locations.
* Improved cooperation and information sharing through faster data transfer and communication between LANs.
* Provides flexibility and scalability to support future expansion and growth within the metropolitan area.
* Greater bandwidth capacity when compared to LANs, allowing for the transfer of enormous data quantities.
* Encourages the integration of various communication technologies, including wireless and fiber optics, for improved connection possibilities.
* Enables the creation of public services like projects for citywide internet access and Wi-Fi hotspots.

**Constraints:**

* Compared to LANs, requires more connecting cables and networking infrastructure, raising installation and maintenance expenses.
* As the MAN grows, management becomes more complex, necessitating strong network administration abilities and centralized control systems.
* Data transfer speeds may slow down due to potential network congestion and performance degradation during periods of high usage.
* Reliance on dependable network access, as network outages might interfere with communication and teamwork.
* Due to interference and signal deterioration brought on by the wider service area, adequate network planning and optimization are required.
* Network performance is impacted by the lack of accessible, inexpensive high-speed connectivity choices in some urban regions.

**Global Area Network (GAN)**

GAN is a network that connects computers across an unlimited geographical area. This is also known as the Internet which is a global network type. (Rouse, 2011)

**Benefits**:

* Global low-cost network connectivity enabled by the Internet, allowing for global communication and information sharing.
* Research and education are supported by easy access to the large amount of information and resources on the Internet.
* Seamless interconnection of people, companies, and organizations across borders and continents.
* Expands business options beyond local markets by enabling international marketing and e-commerce
* Collaboration and information exchange across teams and groups that are separated by distance.
* Supports hosted services and cloud computing, offering scalable and affordable solutions.
* Enables people and organizations to produce and distribute digital content on a global scale.

**Constraints**:

* Network maintenance can be difficult (Different types of networks, standards and protocols available, 2021).
* Compared to private networks, GANs have less security, leaving them vulnerable to hacking, data leaks, and unauthorized access.
* Because the Internet and its infrastructure are spread, network maintenance and troubleshooting can be challenging.
* Variability in network speed and performance because the Internet's functionality depends on elements like bandwidth accessibility and network congestion.
* Relying on external service providers and Internet governance organizations, with limited control over the Internet infrastructure.
* Reliance on dependable internet connectivity since interruptions or outages can affect online communication and resource availability.
* Sharing sensitive and personal information over international networks raises privacy issues and potential security hazards.
* Regulatory and legal difficulties in many countries necessitate adherence to various rules and regulations.

**Network standards**

These are a set of rules and regulations of communication of networking devices which ensure the interoperations of networks (Different types of networks, standards and protocols available, 2021). These are present to make sure that different devices can work together over a network without incompatibility. Following are the common network standards:

1. **International Telecommunication Union (ITU):**

It is a UN agency which regulates international telecommunication comprising of TV and radio frequencies, networking infrastructure, satellite specifications and tariffs that are implied on global communications. It consists of three main areas: ITU-R (Radiocommunication sector), ITU-T (Telecommunication sector) and ITU-D (Development sector).

1. **IEEE (Institute of Electrical and Electronics Engineers):**

This is an international society of engineering professionals that promote the development education in the computer science and electrical engineering fields. They also maintain a board of standard which establishes its own protocols and standards for computer networks and electronic industry. Some of the well-known IEEE standards are:

* IEEE 802.1 (LAN/MAN) used in local environments
* IEEE 802.3 (Ethernet) used to dictate the bandwidth of Ethernet and how the network will function.

1. **International Organization for Standardization (ISO):**

This ais an alliance of national standard bodies which has been formed globally. Its goal is to promote the standardization of networks across the world and develop cooperation of goods and services.

1. **Internet Engineering Task Force (IETF):**

This is an organization that provides the standards for how the systems will communicate over the Internet, especially how the protocols and operate. Its purpose is to promote Internet standards while working closely with other standards organizations and undertake its development (Different types of networks, standards and protocols available, 2021).

**1.3:**

**P2: Explain the impact of network topology, communication and bandwidth requirements.**

A network topology it's defined as the layout in which the components of the network such as the nodes, peripherals and links are connected and undergo communication with each other. The volume of the data which can be transferred across a network during a given time is known as the bandwidth of the network. A high bandwidth network can transfer much larger data much quickly in comparison to a low bandwidth network. Following are the various network topologies:

1. **Bus topology:**

This topology is set up through a single line of communication or a main cable which connects all the nodes directly to it. the main cable of this topology acts as the backbone for the networks that are connected to it. In this topology, one computer acts as the server and provides data to all the other computers.

**Advantages:**

* Bus topology is cheap and easy to implement.
* Less cable is required to implement bus topology.

Disadvantages:

* The entire bus topology will become unusable if the main cable fails
* Cannot be used for larger networks
* It is difficult to troubleshoot under bus topology.

1. **Star topology**

Under star topology, each device is connected to a central computer. the central server of the star topology acts as a hub. the hubs are separately associated with a focal connection point which is similar to a switch.

**Advantages**:

* Even if anyone connection fails other connections remain intact
* Startup cost of this topology is low

Disadvantages:

* If the central hub of the star topology fails, all the other networks will become unusable.

1. **Ring topology**

In a ring topology, all the nodes of the network are connected in a circular manner with each other. Each node of the ring topology connects to two other nodes and form a continuous single pathway for the network signals. This topology is used for both LAN and WAN setups.

**Advantages**

* Each node and gets the opportunity to transmit data which makes it very organized.
* Identification of faulty networks under ring topology is comparatively easier

Disadvantages:

* Failure of a single node will cause the entire network to fail.
* Any changes made in network nodes will affect the entire network.

1. **Tree topology**

This is one of the most common topologies that consist of a group of workstations that are connected to a linear cable. in this topology one star network is connected to another star network through a cable. In this network a cable failure happening in one star network we'll isolate that particular workstation While all the other workstations will continue to function normally without any mishaps. However, if the central computer goes down, all the workstations connected to it this suffer.

**Advantages**:

* Expansion of network is easy
* Fault identification in the network is easy

Disadvantages:

* + The maintenance of network is very difficult

1. **Mesh topology**

Mesh topology allows each node of the network to connect to every other node present in the network. Every node in this topology sends its own signals and also acquires the data from all the other nodes. If one component fails in mesh topology, there is always an alternative present and the data transfer will not be affected. This topology can also be expanded or modified without any effect on the other nodes.

**Advantages**:

* + Mesh topology can handle high volume or data traffic.

Disadvantages:

* + The overall cost of this network is very high compared to other networks (Advantages and disadvantages of networks - Network types and topologies BBC Bitesize, 2021).

**M1: Compare common networking principles and how protocols enable the effectiveness of networked systems:**

**Comparison of Common Network Standards:**

IEEE and the International Telecommunication Union (ITU):

* The ITU is primarily concerned with international telecommunications laws and standards, such as those governing TV and radio frequencies, networking setups, and satellite requirements.
* While developing protocols and standards for computer networks and the electronic sector, IEEE is primarily focused on the subjects of computer science and electrical engineering.
* ITU and IEEE both play significant roles in assuring networking interoperability and standardization, although their areas of emphasis are different.

The Internet Engineering Task Force (IETF) and the International Organization for Standardization (ISO):

* The goal of ISO, a global coalition of standardizing organizations, is to advance collaboration in the production of goods and services as well as industry standardization.
* The creation of standards for Internet communication and protocols is the sole objective of IETF.
* The core focus of the IETF is the creation of Internet standards and protocols, whereas ISO serves a wider variety of sectors.

In conclusion, each network standard has a distinct purpose and range:

* ITU mainly focuses on international telecommunications laws and infrastructure.
* IEEE specializes in protocols and standards for the electronics sector and computer networks.
* ISO pursues standardization in a variety of sectors, including networking.
* The IETF is responsible for creating standards and protocols for Internet communication.

**1.4:**

**Protocols Making Networked Systems Effective:**

By simplifying communication and guaranteeing data integrity, protocols play a crucial part in enabling the effectiveness of networked systems. The following are some ways that protocols improve the performance of networked systems:

* **Standardization**: By establishing a set of guidelines and requirements for communication, protocols ensure that various systems and devices are compatible with one another. This enables smooth data interchange and network collaboration.
* **Error Detection and repair**: To guarantee the integrity and dependability of transmitted data, protocols include techniques for error detection and repair. These methods, which aid in locating and fixing transmission mistakes, include checksums, error control codes, and acknowledgement systems.
* **Addressing and Routing**: Within a network, protocols offer ways to address and route data packets. To discover the most effective channel for data transmission, they create routing protocols, assign unique addresses to devices, and identify the devices. This makes it possible to distribute data effectively over intricate network architectures.
* **Security**: To protect data from unauthorized access and to guarantee the confidentiality and integrity of network communications, protocols contain security mechanisms like encryption, authentication, and access control. Secure connections and the protection of sensitive data are made possible by security protocols like Secure Socket Layer (SSL) and Internet Protocol Security (IPsec).
* **Quality of Service (QoS):** QoS techniques are included into protocols to control network traffic and prioritize traffic, ensuring that vital applications and services have access to enough bandwidth and resources. Time-sensitive applications like speech and video streaming benefit from QoS protocols' effective network resource utilization and improved user experience.
* **Scalability and Flexibility**: Protocols are made to be flexible and expandable in order to support the development of networked systems. In addition to supporting different network topologies, they offer mechanisms for adding and deleting devices as w  
    
  ell as adjusting to shifting network configurations. Networks can develop and adapt to organizations’ shifting needs thanks to the scalability and flexibility of the network.

**1.5:**

**LO2: Explain networking devices and operations**

**P3: Discuss the operating principles of networking devices and server types.**

Following are the most common networking devices:

1. **Hub**

This is a simple network device that connects multiple devices and computers together. Hub is a common connection point a device present in a network. Devices and other multiple computers can be connected to a hub through a network cable so that they can communicate with each other. A hub again broadcast data by receiving it in a form of an electrical signal from one computer and sending it to other computers in the form of electrical signals (Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouwer) - GeeksforGeeks, 2021).

1. **Router**

This is a network device that connects different networks to each other. A router forwards data to a different router of a different network. Router is used to determine the best way to transfer data from one destination to another. It configures a table of all available paths and their conditions and then transfers the specific data based on those parts and conditions.

1. **Switch**

A switch is a network device which connects several computers together on a network. A switch is different from a hub on the basis of its function. Switch can be used to send data from any computer to any other computer in the network but a hub can only send data from one computer to every single computer in the network.

1. **Firewall**

Firewalls or a network security system which control and monitor outgoing and incoming traffic under a network. These are user applied set of rules to control the transmission of data. A firewall can be placed to decide if a particular packet of data can pass or not.

1. **Repeater**

I don't think there is an electronic device which release the signal received with a higher bandwidth and also a prolonged network barrier then that present in the original signal. Its main goal is to extend the transmission of the network to a longer distance.

1. **Bridges**

This is a type of device of computer network which prepares disconnection of one Ethernet to that of another Ethernet that may carry the same protocol. Bridges operate at the data link layer of the OSI model by combining two varying types of networks and then communicating between them.

1. **Access point**

These are the network devices that connect the Wi-Fi devices to a wired network system. With the help of access points, the wireless devices can also be connected to a network system which is wired. Access points can also be connected with several Wi-Fi devices.

1. **Modem**

This is a device which allows a computer to transfer the data over a cable or telephone line. The term modem is a combination of modulation and demodulation as it modulates and demodulates the analog carrier signals of data into digital information. This digital information is then transferred between personal computers over the network (Networking || Definition, Types, Advantages, Disadvantages & Applications, 2021).

**Network servers:**

These are the computer programs that provide different services to other computer programs. Servers are as follows:

1. **Web server:**

It is a program that needs an HTTP protocol to provide services to its end users through the Internet. This server is responsible for storing and hosting website files.

1. **File server**

This is a server that facilitates the user’s approach to files and acts as a central file storage so that all the other computers on the same network can access the files. It also allows the user to transfer information without the requirement of physically transferring the files into an external storage.

1. **Database server**

This server comprises of the hardware and the software which is used to start the database. It is similar to a data store where the website is stored.

1. **Virtualization**

This is the process of creating a virtual source such as a desktop, file storage, operating system or a server. This is a feature which does not require the installation of hardware components and allows the users to quickly deploy their resources.

1. **Print server**

A print server is a software application which allows the computers on the network to print their tasks. This server is used in both large and small networks (Networking || Definition, Types, Advantages, Disadvantages & Applications, 2021.

**P4: Discuss the inter-dependence of workstation hardware with relevant networking software.**

The system of computer comprises of two main elements which are hardware and software. If the computer system has to function smoothly, an essential role must be played by both the hardware and the software. In case the necessary software and hardware of a computer system are not available, the computer system will not work properly. Hardware is a collection of all the physical elements of the computer which one can touch. On the other hand, the software is a program which contains a set of instructions for the computer in order to perform certain operations. There are a number of ways in which both the hardware and software are interdependent upon each other. These two systems of the computer black interdependently and are useless without each other. Both these components, the hardware and the software of the computer, must interact with each other accordingly to make the computer system work.

**Required workstation hardware:**

* Processor
* Motherboard
* 4 GB RAM
* Router
* Hard disk
* Printer
* 150mb bandwidth
* Access pointer
* Firewall
* Network interface card

**Required workstation software:**

There are a number of network programs that have their own software based upon their function and specialty. There are different types of software which can be used by the user are client software or server software.

A client software is a software which acts as a link between the client and server computers. For a client software, the user needs a server. The user connects the services through a network server. The user also requires switches and routers to support the network.

A server software is designed to connect the server hardware to the memory processor and the other communication ports in a computer. It also requires an operating system for the proper functioning of its functions.

**Interdependency:**

Both the hardware and the software at a workstation are completely interdependent upon each other. Without the hardware support, a software cannot be used at a workstation. On the other hand, to perform a work at the workstation and appropriate software package must be installed in the hardware. This software thus acts as a connection between the hardware and consequently the user. Therefore, both of them are it required to run any system at a workstation (Networking || Definition,Types, Advantages, Disadvantages & Applications, 2021).

**1.6:**

**M2: Explore a range of server types and justify the selection of a server, considering a given scenario regarding cost and performance optimization.**   
  
**Virtual Server**

* On a single physical server, a virtual server—also called a virtual machine (VM)—runs various virtualized operating systems.
* By combining hardware resources, it gives cost savings and enables effective server resource use.

**Message Server**

* Email messages are transmitted, received, and stored by a mail server.
* It manages email communication using email protocols including SMTP (Simple Mail Transfer Protocol) and IMAP (Internet Message Access Protocol).

**DNS Server**

* Domain names are converted into IP addresses by a DNS (Domain Name System) server.
* Instead of utilizing numerical IP addresses, it enables users to access websites or services using human-readable domain names.

**Application Server**

* A platform for managing and operating web-based applications is provided by an application server.
* It manages user authentication, data storage, and the execution of application logic, allowing access to applications across a network.

**Backup Server**

* Data from network devices and servers is backed up and restored by a backup server.
* It aids disaster recovery, guarantees data redundancy, and automates data backup procedures.

**Database Server**

* In a database management system (DBMS), a database server stores, controls, and retrieves structured data.
* It enables efficient and safe access to data by various users or applications.

**Print Server**

* A print server controls access to network printers and manages printing processes.
* It manages print job scheduling, manages print job queues, and guarantees effective printer utilization.

**DHCP Server**

* Dynamically assigning IP addresses to networked devices is done by DHCP (Dynamic Host Configuration Protocol) servers.
* By automatically allocating IP addresses, subnet masks, and other network characteristics, it makes network configuration simpler.

Considering the cost and performance optimization in the current environment, it is critical to select servers that balance efficiency and affordability. Here are a few suggestions:

* **Virtual Server**: By integrating hardware resources and improving server utilization, virtualization technology implementation can result in cost savings.
* **Database Server**: Based on the organization's needs for data management, pick a database server that offers a balance between performance, scalability, and licensing costs.
* **Web server**: Take into account a web server that is affordable and effective at hosting and delivering websites or online applications. Popular options include NGINX or Apache HTTP Server.
* **Mail Server**: Consider your alternatives for a mail server that offers dependable email connectivity, security features, and affordability. Microsoft Exchange Server and Postfix are common choices.
* **DNS Server**: Choose a DNS server that delivers dependable and efficient domain name resolution. One of the most popular DNS server program is called Bind (Berkeley Internet Name Domain).

**1.7:**

**LO1 & L2: D1: Considering a given scenario, identify the topology protocol selected for the efficient utilization of a networking system**

Following the guidelines provided for the network of the educational institution, the hybrid architecture utilizing the Ethernet protocol has been chosen for effective utilization.

**Hybrid Topology**

Various topologies, including mesh, star, bus, ring, and tree, are combined in the hybrid topology to create a strong and adaptable network structure. The hybrid topology in this situation combines the bus and tree topologies. The following variables all had a role in the choice to choose the hybrid topology:

* Redundancy and Fault Tolerance: The hybrid architecture guarantees a robust network where even if one device or link fails, others won't be impacted. Redundancy like this improves network dependability and cuts down on downtime.
* Effective management of enormous amounts of data flow without collapsing or creating congestion is possible with hybrid topologies. It offers improved data routing and effective network resource use.
* Scalability: The hybrid architecture makes it simple to connect more devices to the network by adding routers or hubs. The network can support future expansion and rising network needs thanks to its scalability.
* Utilization of Integrated Topologies: The network may utilize the advantages and strengths of Integrated Topologies by choosing the Hybrid Topology. Each topology has a strategic deployment option that may be used to fulfil unique network requirements and enhance performance.

**Ethernet Protocol**

The most popular protocol in wired local area networks (LANs) has been chosen for the hybrid architecture, and it is Ethernet. Data transmission via a LAN is controlled by the IEEE 802.3 standard, which is known as Ethernet. Ethernet has advanced and developed throughout time to handle data transfer rates more than a gigabit per second.

Advantages of implementing Ethernet in a hybrid topology:

* High Speed: When compared to wireless connections, Ethernet delivers quicker data transmission rates. Ethernet can transmit data at fast speeds through physical lines inside a local area network (LAN), allowing for speedy access to shared resources and effective communication.
* Reliability: Compared to wireless connections, wired Ethernet connections are often more dependable and steady. They provide persistent network connectivity since they are less prone to interference and other influences.
* Ethernet is extensively supported by computers, networking hardware, and other devices. It offers smooth compatibility and interoperability across a range of hardware and software systems.
* Security: To safeguard data transferred across the network, Ethernet enables the adoption of strong security mechanisms like access restrictions and encryption. By lowering the possibility of unauthorized access, wired connections also have intrinsic security benefits.
* Broad Industry Adoption: Ethernet is a well-known networking technology that has seen extensive adoption. Assuring compatibility and interoperability with other network components, it is widely utilized in corporate networks, academic institutions, and a variety of sectors.

The educational institute's network may gain from a dependable, scalable, and efficient network architecture that allows high-speed data transfer and secure communication by using hybrid topology with the Ethernet protocol.

**LO3 Design efficient networked systems  
P5 Design a networked system to meet a given specification.**

LAN refers to the local area network. Designing LAN requires a variety of factors to be considered as it is a complicated procedure. Appropriately designed LAN will be able to provide a high quality and consistent service to each device that is attached to its network.

**2.1:**

**Step-by-step plan to design LAN network:**

**Step 1: Determine the Network Requirements**

* I will examine the particular local services and assets that must be reachable across the network, such as servers, printers, and shared storage.
* I'll make a list of the devices that need network access and give each one a special IP address.

**Step 2: Wired Infrastructure:**

* The use of a wired LAN infrastructure would be given priority whenever possible to provide improved performance and security.
* Using common Ethernet cables, fiber optic wall plates, patch cables, and optical connectors for high-performance connections, I will arrange and install Ethernet cables.

**Step 3: Networking Hardware:**

* I will choose networking equipment, including switches, wireless routers, and cable routers, carefully based on the needs of the organization.
* To improve versatility, I'll select a cable router with built-in wireless functionality.

**Step 4: Configure DHCP and the router:**

* I will set up the cable router's LAN ports and configure it to function as a DHCP server as part of the implementation.
* I'll assign connected devices IP addresses based on their current needs while maintaining an adequate DHCP address range.
* Additionally, I'll give servers and other equipment that needs them static IP addresses.

**Step 5: Connect Devices:**

* I will connect PCs, servers, and other devices as the network engineer utilizing common Ethernet connections.
* I will guarantee correct wiring and communication by utilizing the right Ethernet cables to connect the switch to the cable router's LAN ports through an uplink or direct port.

**Step 6: Network performance testing:**

* To make sure the LAN network performs properly and satisfies performance standards, I will carry out extensive testing.
* In order to ensure adequate connectivity, I will check each workstation's ability to access the internet and local network resources.
* As part of the implementation phase, shared printer capability will be tested, and read and write access to shared data servers will be verified.

**Design of the network**

A diagram of a network

Description automatically generated with low confidence

The above design shows that all lab computers are connected, and other computers are connected. Distributing them as per requirement. Printer is configured in Printing Area and all computers can access it.

This network has been designed on Cisco Packet Tracer.  
**2.2:**

**Justification for Network Design:**

**Routers: CISCO 1841 router (5 units)**

* The CISCO 1841 router was selected because to its dependability, effectiveness, and cutting-edge capabilities. As the network grows, it is a modular router that can accept more modules.
* In order to safeguard network traffic and data, the router has strong security features such firewall protection, support for virtual private networks (VPNs), and intrusion prevention system (IPS) capabilities.
* The CISCO 1841 router's integrated services make it possible to efficiently combine voice, video, and data services in the network, facilitating unified communication and collaboration.
* Future network expansion and technological improvements can be accommodated by the router's scalability and flexibility.

**Switches: 2950-24 switch (7 units)**

* The 2950-24 switch is chosen for LAN installations because to its dependability, performance, and controllable features.
* Each switch has 24 Fast Ethernet ports, enabling the connecting of several hardware items including servers, PCs, and printers.
* In order to improve network efficiency and traffic management, the switch provides sophisticated switching capabilities such VLAN support, quality of service (QoS), and port mirroring.
* The 2950-24 switch's small form size makes it ideal for network environments in businesses where space may be at a premium.
* Redundancy and better network resilience are ensured by the availability of numerous switches, allowing for smooth communication and little disturbance in the event of a switch failure.

**PCs:**

* Based on the needs of the educational institution, the number of PCs is chosen. There are enough PCs available to meet the demands of the students, instructors, administrators, and other staff members.
* Budget, required performance levels, and software compatibility are only a few examples of the variables that may influence the choice of certain PC models and specs. In order to handle a variety of educational apps and duties, it is essential to use robust and capable PCs.

**Printer:**

* Users may simply print their papers from any connected device thanks to centralized printing services made possible by the presence of a printer in the network design.
* Depending on the organization's printing requirements, such as color printing, etc., the exact printer type may change.
* The printer is selected to guarantee compliance with the network architecture and offer users dependable and effective printing services.

Overall, the CISCO 1841 routers, 2950-24 switches, PCs, and printers are carefully chosen as part of the network architecture to deliver a reliable, secure, and scalable LAN network. These components provide cutting-edge features, dependability, and performance to satisfy the needs of the educational institution, promote effective resource sharing and communication, and enable the organization's expansion and future technological improvements while staying under budget.

**P6: Test and evaluate the design to meet the requirements and analyze user feedback**.

**2.3:  
Test Plan:**



**2.4: Justify the security requirements and quality of services needed for selection of accessories:**

The selection of accessories must justify the security needs and the quality of services required in order to secure the integrity, confidentiality, availability, and performance of the network. I will offer a thorough and in-depth rationale for accessory selection in terms of security needs and service quality as a network specialist.

**Security prerequisites**

* **Access Controls**: To prevent unauthorized access to the network and critical resources, accessories should offer strong access control techniques like authentication, authorization, and accounting (AAA).
* **Data Encryption**: To provide safe data transfer over the network and guard against unauthorized interception and modification, the accessories should include built-in encryption capabilities.
* **Intrusion detection and prevention features**: IDPs such as intrusion prevention systems (IPS) and intrusion detection systems (IDS), should be included in the chosen accessories.
* **Industry-standard security protocols**: Protocols such as IPsec (Internet Protocol Security) and SSL/TLS (Secure Sockets Layer/Transport Layer Security), should be supported by the accessories in order to provide secure communication channels.
* **Vulnerability Management**: The accessories must be able to update their firmware or software on a regular basis to fix any security flaws that are found over time.
* **Logging and Auditing**: Accessories with strong logging and auditing capabilities make it possible to track and monitor network activity, which helps with the investigation of security events and compliance needs.

**Quality of Services (QoS)**

* **Bandwidth management**: To guarantee effective use of available bandwidth and enhance network performance, accessories should enable QoS capabilities like traffic shaping and prioritization.
* **Low Latency**: To ensure a seamless user experience in real-time applications like video conferencing, voice over IP (VoIP), and online gaming, accessories must have low latency characteristics.
* **Packet Loss Prevention**: To reduce packet loss and preserve data integrity during transmission, accessories should make use of methods such error detection and correction, buffering, and traffic prioritization.
* **Network Scalability**: The chosen accessories ought to be expandable in order to meet the network's increasing demands. This will guarantee that performance doesn't suffer as the network grows.
* **Quality monitoring**: A high-quality user experience is ensured, which is made possible by accessories that have built-in monitoring and diagnostic capabilities.
* **Reliability and Redundancy**: To reduce service interruptions and offer high availability, accessories should have redundant components and failover methods.

**2.5:**

**D2: Suggest a maintenance schedule to support the networked system.**



**LO4 Implement and diagnose networked systems:**

**P7 Implement a networked system based on a prepared design.**

This process has to be completed through a number of steps:

1. Create a workstation through VMWare Workstation

Chart

Description automatically generated with low confidence

1. Configure the network adapter through the control panel

Graphical user interface, text, application

Description automatically generated

1. Install the active directory

Graphical user interface, application

Description automatically generated

1. Create a domain:A picture containing graphical user interface

   Description automatically generated
2. Install the DNS server

Graphical user interface, application

Description automatically generated

1. Install the DHCP server

Graphical user interface, application

Description automatically generated

1. Add file server

Graphical user interface, application

Description automatically generated

This will the successfully allocate the network drive.

Graphical user interface, text, application

Description automatically generated

**M4: Discuss the significance of upgrades and security requirements in your recommendations:**

A networked system may benefit from improvements, but there are a number of things to keep in mind when doing so, including better scalability, performance, security, and resource efficiency. Here are a few potential networked system improvements:

* **Upgrade Network Infrastructure**: Examine the existing network architecture and think about updating switches, routers, and cables to provide more bandwidth, quicker data transmission, and enhanced dependability.
* **Implement virtualization**: By operating several virtual computers on a single physical server, virtualization technology enables greater hardware resource utilization. As a result, there may be financial savings, simpler management, and more flexibility in the rollout of new services or applications.
* **Enhance Network Security**: Review the security precautions already in place and think about adding further layers of protection, such intrusion detection and prevention systems, data encryption, and cutting-edge firewalls. To find and fix any possible vulnerabilities, routine security audits and vulnerability assessments should be carried out.
* **Enhance network monitoring and management**: By using thorough network monitoring solutions that allow you to proactively discover and fix network problems. This includes the continuous observation of security incidents, device performance, and network traffic. Tasks involving administration and configuration may be made simpler by implementing centralized network management solutions.
* **Implement Quality of Service (QoS):** QoS algorithms prioritize network traffic based on established criteria, ensuring that vital applications or services have sufficient bandwidth and lower-priority traffic has no negative performance effects. In settings where real-time applications like voice-over-IP (VoIP) or video conferencing are used, QoS can be very helpful.
* **Expand Wireless Network Coverage**: Evaluate the current wireless network architecture and think about adding access points or utilizing mesh networking to increase coverage. Better connection and mobility throughout the network will be made possible for wireless devices as a result.
* **Integrate Cloud Services**: Look at ways to use cloud services for backup, disaster recovery, and storage. Scalability, flexibility, and cost-effectiveness can be provided through cloud-based services, negating the need for on-premises equipment.
* **Enable VPN and remote access**: Implement VPNs and remote access security measures to enable authorized users to safely connect to the network from faraway places. This enhances teamwork and makes it possible to operate remotely.
* Enable Network Segmentation: By dividing the network into distinct virtual LANs (VLANs) or subnets, you may increase security, boost network performance, and make management simpler. In order to lessen the effects of security breaches or network problems, critical systems might be isolated from the rest of the network.

Prioritizing improvements is crucial, and should be done in accordance with the particular needs, financial constraints, and network environment resources.

**P8 Document and analyze test results against expected results.**

|  |
| --- |
| **Question 1** |
| Was the client able to log in to the domain from his node? |
| The client was successfully able to log in to the domain |

|  |
| --- |
| **Question 2** |
| Was the client able to access the file? |
| The client was successfully able to access the files |

|  |
| --- |
| **Question 3** |
| Was the client able to access permitted files and folders? |
| The client was successfully able to access the permitted files |

|  |
| --- |
| **Question 4** |
| Was the client able to read and write on the network drive? |
| The client was successfully able to read and write on the network DRIVE |

This shows that the network implementation has been successful and it can be used by the clients for their benefit.

**D3: Use critical reflection to evaluate own work and justify valid conclusions.**

Critical reflection was adopted throughout the networked system's design, implementation, and maintenance to assess the effort and reach reliable findings. The evaluating procedure took into account the following factors:

* **Design Assessment**: The initial network design underwent a thorough assessment to make sure it complied with the demands of the educational institution. The design included the right network topologies, hardware, and software to enable the functionality and scalability required. The efficiency of the design in addressing the needs of the institute might be evaluated through critical reflection.
* **Implementation Evaluation**: The implementation step included setting up connectivity, configuring network devices, and checking that services operated correctly. To find any problems or flaws, frequent testing and troubleshooting were carried out. Critical reflection made it possible to assess the implementation procedure while taking into account elements like effectiveness, correctness, and adherence to best practises.
* **Maintenance Assessment**: The maintenance plan was created to assist the networked system by addressing normal chores as well as prospective problems. Key components of maintenance were routine inspections, performance monitoring, security audits, and user management. The success of the maintenance programme was assessed through critical reflection, taking into account elements including punctuality, completeness, and influence on network performance and security.
* **Test Plan Evaluation**: To evaluate the functionality and performance of the networked system, a complete test plan was developed. Various tests, anticipated outcomes, feedback systems, and cost factors were all incorporated in the test plan. An evaluation of the test plan's coverage, precision, and compliance with the network requirements was made possible by critical reflection.
* **Security and Quality of Service Evaluation**: Security needs and quality of service considerations were rigorously justified and integrated into network design and execution. The efficiency of the chosen security measures and quality of service methods might be assessed through critical reflection. Considerations were made for elements including risk reduction, data security, and user happiness.
* **Potential Enhancements Evaluation**: After carefully examining the current infrastructure and anticipated future requirements, prospective improvements for the networked system were recommended. Critical analysis enabled an assessment of the suggested improvements, taking into account elements including viability, performance impact, cost-effectiveness, and alignment with organisational goals.

**BIBLIOGRAPHY**

AnswerKid.co.uk. 2021. *Different types of networks, standards and protocols available*. [online] Available at: <https://www.answerkid.co.uk/different-types-networks-standards-protocols-available/> [Accessed 23 December 2021].

Wright, G. (2021). Metropolitan Area Network (MAN). TechTarget. Retrieved from <https://www.techtarget.com/searchnetworking/definition/metropolitan-area-network-MAN>

Mitchell, B. (2021). Wide Area Network. LifeWire. Available at: <https://www.lifewire.com/wide-area-network-816383

Rouse, M. (2011). Global Area Network (GAN). Techopedia. Available at: <https://www.techopedia.com/definition/7368/global-area-network-gan>

BBC Bitesize. 2021. *Advantages and disadvantages of networks - Network types and topologies - GCSE ICT Revision - BBC Bitesize*. [online] Available at: <https://www.bbc.co.uk/bitesize/guides/z36nb9q/revision/2> [Accessed 23 December 2021].

GeeksforGeeks. 2021. *Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter) - GeeksforGeeks*. [online] Available at: <https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/> [Accessed 23 December 2021].

Mechanical Notes. 2021. *Networking || Definition,Types, Advantages, Disadvantages & Applications*. [online] Available at: <https://mechanicalnotes.com/networking-definition-types-advantages-disadvantages-applications/> [Accessed 23 December 2021].