1) **What is an open system and closed system?**

Open system: A system that is connected to the network and is ready for communication.
Closed system: A system that Is not connected to the network and can't be communicated with.

2) **What is a network?**

A network refers to two or more connected computers that can share resources such as data, a printer, an internet connection, applications or a combination of these resources.

Computer network:

A "computer network," on the other hand, specifically refers to a network of computers and other devices that are connected to each other for the purpose of sharing resources and exchanging data. This type of network can be as simple as a small local network (LAN) connecting a few computers in a single room or as complex as a large wide area network (WAN) that spans multiple countries and connects thousands of devices. Common examples of computer networks include the Internet, intranets, and home networks.

3) **What are the advantages and disadvantages of a network?**

Advantages of a network:

- **Resource sharing:** A network allows users to share hardware resources such as printers and scanners, as well as software resources such as applications and databases. This reduces costs and improves efficiency.
- **Communication:** A network enables users to communicate and collaborate with each other in real-time, regardless of their physical location. This makes it easier to work together on projects and share information.
- **Centralized management:** A network allows for centralized management of resources and security. This simplifies administration and reduces the risk of data loss or security breaches.
- **Scalability:** A network can be easily expanded as needed to accommodate new users and devices. This makes it a flexible and scalable solution for growing businesses.

Disadvantages of a network:

- **Complexity:** Networks can be complex to set up and manage, requiring specialized knowledge and expertise. This can be a barrier for small businesses or organizations without dedicated IT staff.
- **Security risks:** Networks can be vulnerable to security risks such as hacking, viruses, and malware. This requires careful management of security measures such as firewalls and antivirus software.
- **Dependence on infrastructure:** A network depends on infrastructure such as servers, routers, and switches. If this infrastructure fails, the network may be inaccessible, causing downtime and loss of productivity.
- **Cost:** Networks can be expensive to set up and maintain, requiring hardware, software, and ongoing maintenance and support. This can be a significant investment for small businesses or organizations with limited budgets.

Overall, the advantages of a network such as a resource sharing, communication, centralized management, and scalability can provide significant benefits for businesses and organizations. However, the disadvantages such as complexity, security risks, dependence on infrastructure, and cost should be carefully considered and managed to ensure the network is a reliable and secure solution.

4) Connecting devices can be of two types what are they?

Networking and internetworking

Networking refers to the process of connecting multiple devices together to share resources and communicate with each other. Networks can be small or large and can be used in a variety of settings, including homes, offices, and data centers.

Networking devices:

Switches: These devices are used to connect multiple devices together within a network. They allow devices to communicate with each other by forwarding network packets between them.

Hubs: These devices are similar to switches, but are less intelligent and simply broadcast incoming network packets to all devices on the network.

Network interface cards (NICs): These devices are used to connect individual devices to a network. They provide a physical connection between the device and the network, and allow the device to communicate with other devices on the network.

Internetworking, on the other hand, refers to the process of connecting multiple networks together to form a larger, interconnected network. This allows devices on different networks to communicate with each other as if they were on the same network. The Internet is a prime example of a large, interconnected network created through internetworking.

Internetworking devices:

Routers: These devices are used to connect multiple networks together to form a larger, internetworked network. They use routing protocols to determine the best path for network packets to travel between networks.

Gateways: These devices are used to connect networks that use different protocols or technologies. They translate between different network protocols and ensure that network packets can be transmitted between the different networks.

Firewalls: These devices are used to secure networks by controlling access to network resources and blocking unauthorized network traffic.

Internetworking is typically accomplished through the use of networking protocols and devices such as routers, switches, and gateways. These devices allow data to be transmitted between different networks and ensure that it reaches its intended destination.

Overall, networking and internetworking are closely related concepts that are essential for enabling communication and resource sharing between devices and networks. They are foundational technologies that have enabled many of the modern advances in computing and communication.

5) Draw the connection device category diagram.

6) Write a short note on Repeaters, bridges, switch, hub, Routers and gateways.

Repeaters: Repeaters are used to regenerate network signals in order to extend the range of a network. They receive a weak or degraded signal from one network segment, amplify it, and re-transmit it to another segment. Repeaters are useful for extending the range of wired networks, but they cannot be used to connect different types of networks or to isolate network segments.

Bridges: Bridges are used to connect two or more network segments together to form a larger network. They operate at the data link layer of the OSI model and use MAC addresses to forward network packets between different segments. Bridges are useful for segmenting larger networks into smaller, more manageable segments, and for improving network performance by reducing network congestion.

Switches: Switches are similar to bridges, but are more advanced and provide more advanced features. They use MAC addresses to forward network packets between different network segments, but can also support advanced features such as virtual LANs (VLANs), Quality of Service (QoS) management, and port mirroring. Switches are commonly used in local area networks (LANs) to provide high-speed, reliable connectivity between devices.

Hubs: Hubs are similar to switches, but are less advanced and simply broadcast incoming network packets to all devices on the network. Hubs are typically used in small, simple networks where cost is a primary concern. However, they can be less efficient and can create network congestion in larger networks.

Routers: Routers are used to connect multiple networks together to form a larger, internetworked network. They use routing protocols to determine the best path for network packets to travel between networks, and can provide advanced features such as network address translation (NAT), virtual private networks (VPNs), and firewalling. Routers are essential for enabling communication between devices on different networks, and are a key component of the Internet.

Gateways: Gateways are used to connect networks that use different protocols or technologies. They translate between different network protocols and ensure that network packets can be transmitted between the different networks. Gateways are useful for enabling communication between devices on different types of networks, such as connecting a LAN to the Internet. They can also provide advanced features such as security, authentication, and content filtering.

7) What is a model and protocol.

Model: The specification set by standards organization as a guideline for designing networks.

Protocol: A set of rules that controls the interaction of different devices in a network/internetwork.

8) What are the factors to consider while choosing a network topology.

There are several factors to consider when choosing a network topology, including:

- **Scalability**: The ability of the network to expand and support additional devices and users in the future.
- **Cost**: The cost of implementing and maintaining the network topology, including hardware, software, and personnel costs.
- **Reliability:** The ability of the network to function consistently and reliably, with minimal downtime and failures.
- **Performance**: The speed and efficiency of the network, including data transfer rates, latency, and throughput.
- **Security:** The ability of the network to protect against unauthorized access, data breaches, and other security threats.

- **Flexibility:** The ability of the network to adapt to changing business requirements, such as the need to support new applications or devices.
- **Management**: The ease of managing and monitoring the network, including the ability to identify and troubleshoot problems.
- **Compatibility:** The ability of the network topology to support existing hardware and software, as well as future technologies and standards.

By considering these factors, organizations can choose a network topology that meets their specific needs and requirements, while also providing a reliable, efficient, and secure network infrastructure.

9) What are the categories of a network and the devices used. Write a short note of each.

The network allows computers to connect and communicate with different computers via any medium.

LAN, MAN, and WAN are three major types of computer network designs. One of the major differences is the geographical area they cover.

- **Personal Area Networks(PAN)**

  This is the most basic type of network. This network is restrained to a single person.

- **Local Area Network**

  A Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

  LAN-devices

  - Wired LAN (Ethernet- hub, switch)
  - Wireless LAN (Wi-Fi)

- **Metropolitan Area Network**

  A MAN is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area(city).(2 more LANs connected together.

  MAN-devices.

  - Switches/hub
  - Routers/bridges

- **Wide Area Network**

  A wide area network (WAN) is a telecommunication network that extends over a large geographical area for the primary purpose of computer networking.

  WAN- Devices

  - End devices and intermediary devices

10) What are the types of topologies write the advantages and disadvantages.

STAR Topology

This topology consists of a central node to which all other nodes are connected by a single path.

Advantages

- Ease of Service
- One device per connection.
- Centralized control/Problem diagnosis.
- Simple access protocol

Disadvantages

- Central node dependency
- Long cable length
- Difficult to expand.

BUS Topology

This topology consists of a single length of the transmission medium (coaxial cable) on to which the various nodes are attached.

Advantages

- Short cable length and simple wiring layout.
- Resilient architecture.
- Easy to extend.

Disadvantages

- Fault diagnosis is difficult.
- Fault isolation is difficult.
- Repeater Configuration.
- Nodes must be intelligent.

RING Topology

In this Topology, each node is connected to two and only two neighboring nodes, and is transmitted onwards to another. Data travels in one direction; from node to node around the ring.

Advantages

- Short cable length
- No wiring closet space required.
- Suitable for optical wires.

Disadvantages

- Node failure causes network failure.
- Difficult to diagnose faults.
  Network reconfiguration is difficult.

Mesh topology

A mesh topology is a type of network topology in which each device in the network is connected to every other device through dedicated point-to-point links. In a full mesh topology, each device has a direct connection to every other device, while in a partial mesh topology, some devices have direct connections to only a subset of other devices.

Advantages of mesh topology:

- **Reliability**: A mesh topology provides high levels of reliability, as there are multiple paths for data to travel between devices. If one link or node fails, data can be rerouted along an alternative path.
- **Scalability**: Mesh topologies are highly scalable, as additional devices can be added to the network without impacting the overall performance or reliability.
- **Security:** Mesh topologies are inherently secure, as each device has its own dedicated link to other devices. This makes it difficult for unauthorized users to gain access to the network.

Disadvantages of mesh topology:

- **Complexity:** Mesh topologies can be complex to design, implement, and manage, as each device requires multiple connections and there are many potential paths for data to travel.
- **Cost:** Mesh topologies can be expensive to implement, as each device requires multiple connections and dedicated hardware.
- **Performance:** While mesh topologies provide high levels of reliability, the multiple paths for data to travel can result in longer transmission times and increased latency, which can impact overall network performance.

11) What is the internet and provide few examples for internet applications.

The internet is a global network of interconnected computers and servers that communicate with each other using standardized protocols and technologies. It enables users to access a wide range of information and services, communicate with others, and conduct business transactions from virtually anywhere in the world.

Some examples of internet applications include:

- **World Wide Web (WWW):** The most popular and widely used internet application, the World Wide Web enables users to access a vast array of information, resources, and services through web browsers such as Chrome, Firefox, and Safari.
- **Email**: Email is a popular form of electronic communication that enables users to send and receive messages and attachments over the internet.
- **Social Media**: Social media platforms such as Facebook, Twitter, Instagram, and LinkedIn enable users to connect and interact with others, share information and media, and engage in online communities.
- **E-commerce**: E-commerce websites such as Amazon, eBay, and Alibaba enable users to purchase and sell goods and services online.
- **Cloud Computing**: Cloud computing services such as Google Drive, Dropbox, and Microsoft OneDrive enable users to store, share, and access files and applications over the internet.
- **Video Conferencing**: Video conferencing tools such as Zoom, Skype, and Microsoft Teams enable users to conduct virtual meetings and collaborate with others in real-time.
- **Online Gaming:** Online gaming platforms such as Steam, PlayStation Network, and Xbox Live enable users to play games with others over the internet.

These are just a few examples of the many internet applications that are available today, each of which offers unique benefits and opportunities for users around the world.

12) Write about Internet vs WWW vs WAN.

The internet, WAN, and WWW (World Wide Web) are all related concepts, but they refer to slightly different things.

The internet is a global network of interconnected computers and servers that communicate with each other using standardized protocols and technologies. It enables users to access a wide range of information and services, communicate with others, and conduct business transactions from virtually anywhere in the world.

WAN (Wide Area Network) refers to a network that covers a large geographic area, such as a city, country, or even multiple countries. WANs are often used by organizations that have multiple locations and need to share resources and data between them.

The **World Wide Web (WWW)** is a system of interconnected documents and resources that are accessed over the internet. It was created in 1989 by Tim Berners-Lee and has since become the primary means by which people access and share information on the internet. The WWW is accessed through web browsers, such as Chrome, Firefox, and Safari, and enables users to access a vast array of information, resources, and services.

In summary, the internet is the global network of interconnected computers and servers, WAN refers to a large-scale network that covers a wide geographic area, and WWW is the system of interconnected documents and resources that are accessed over the internet. The WWW is just one of many applications that run on the internet, which also includes email, social media, cloud computing, and more.

13) What is a server?

A server is a computer or a program that provides services to other devices or programs, referred to as clients, over a network. Servers are designed to handle and manage data and information, and they can serve different purposes, such as hosting websites, storing and managing files, managing network traffic, or running applications.

In a client-server architecture, clients make requests to servers, which then respond by providing the requested services or data. Servers can be physical machines or virtual machines running on a larger physical server, and they are typically designed to operate continuously and reliably, with high availability and redundancy.

Some common types of servers include web servers, file servers, email servers, database servers, and game servers. Web servers, for example, host websites and web applications, while file servers provide centralized storage and file sharing capabilities for users within a network. Email servers manage email communications, and database servers store and manage data for various applications.

Overall, servers are essential components of modern computer networks and play a critical role in enabling various network-based services and applications.

14) Explain what is meant by the Internet and why it's getting slow in Covid 19 pandemic situation. Explain your answer in your own words

The Internet is a global network of interconnected computers and servers that communicate with each other using standardized protocols. It allows people to exchange information, communicate, and access a wide range of digital resources such as websites, applications, and services.

During the Covid-19 pandemic situation, the Internet has been experiencing slowdowns and disruptions due to the increased demand for online services and the shift to remote work and education. Here are some reasons why the Internet has been getting slow during the pandemic:

Increased demand for online services: With more people working, learning, and socializing from home, there has been a significant increase in the demand for online services such as video conferencing, streaming video, and online gaming. This has put a strain on Internet infrastructure and caused congestion on networks.

Limited network capacity: The infrastructure and capacity of Internet networks are not unlimited, and they have limitations on how much data they can handle at any given time. With the sudden surge in demand for online services, the capacity of some networks has been exceeded, causing slowdowns and disruptions.

Geographical limitations: The Internet infrastructure and network capacity vary depending on location and geography. Some areas may have limited or outdated infrastructure, which can contribute to slower Internet speeds and lower capacity.

Changes in user behavior: The pandemic has led to changes in user behavior, such as increased use of social media, online shopping, and video streaming. These activities require more bandwidth and can contribute to network congestion and slowdowns.

Overall, the Internet has been experiencing slowdowns and disruptions during the Covid-19 pandemic due to the increased demand for online services, limited network capacity, geographical limitations, and changes in user behavior. Service providers and network operators are working to address these issues and improve Internet performance, but it may take time to fully resolve the problems.

15) By considering the computer network in NSBM Green university as for example answer the following questions. I.

I. What are the benefits of computer network for different users involved with the university?

Students: Computer networks provide students with access to a wide range of resources, including course materials, online libraries, and research databases. They can also communicate with their peers and professors via email, messaging apps, or online forums. Furthermore, they can submit their assignments online, take online exams, and receive feedback from their professors.

Faculty and staff: Computer networks enable faculty and staff to share information, collaborate on research projects, and communicate with each other more efficiently. They can also use online tools to manage their courses, grade assignments, and keep track of student progress.

Administration: Computer networks help the university administration to streamline their operations and improve their services. They can use online tools to manage student enrollment, track financial transactions, and generate reports. They can also communicate with faculty, staff, and students more easily, and provide them with timely updates and announcements.

Researchers: Computer networks provide researchers with access to large datasets, research papers, and scientific journals. They can also collaborate with other researchers from around the world and share their findings more easily. Furthermore, they can use advanced computing resources to run simulations, analyze data, and conduct experiments.

IT professionals: Computer networks provide IT professionals with the tools and infrastructure they need to manage the university's technology resources. They can monitor network performance, troubleshoot issues, and implement security measures to protect the university's data and systems. They can also provide technical support to users and train them on how to use new technologies.

II. Considering the size of the organization which type of a network is more suitable?

Yes, a university can also have a local area network (LAN) in addition to or instead of a wide area network (WAN), depending on the size and requirements of the organization. A LAN is a network that covers a relatively small area, such as a building, a campus, or a department. It allows users within the same location to connect to the same network and access the same resources, applications, and services.

A LAN can be suitable for a small university with a single campus and a limited number of users. It would allow students, faculty, and staff to connect to the network and access resources such as printers, shared files, and databases. It can also provide a secure and reliable environment for communication and collaboration between users.

However, as the university grows in size and complexity, a LAN may no longer be sufficient to meet its needs. In this case, a WAN would be necessary to connect multiple locations and enable users to access resources and services from different locations. Therefore, the choice between a LAN and a WAN depends on the specific requirements and goals of the university, as well as its budget and resources.

III. What are the factors need to be considered in choosing a network topology?

The pattern of the interconnection of nodes in a network is called a TOPOLGY. Different types of topologies affect different the choice of media and the access method used. Factors to consider while choosing a network topology.

- **Cost**
  Minimizing of the installation cost can be done by reducing the distance involved and by identifying the most suitable Network toplogy.

- **Flexibility**
  Because the arrangement of furniture and internal walls etc… in offices often change. The topology should allow easy reconfiguration. This includes moving existing nodes and adding new nodes.

- **Reliability**
  There are two types of network failures, A failure of a node and the failure of the entire network. The topology chosen for the network can help by allowing the location to be detected and to provide some means of isolating.

IV. Discuss the advantages and disadvantages of network topology STAR

STAR Topology

This topology consists of a central node to which all other nodes are connected by a single path.

Advantages

- Ease of Service
- One device per connection.
- Centralized control/Problem diagnosis.
- Simple access protocol

Disadvantages

- Central node dependency
- Long cable length
- Difficult to expand.

V. What are the possible network risks associated with the university network?

There are several possible network risks associated with a university network, including:

Unauthorized access: This occurs when someone gains access to the network or its resources without permission. Hackers, malicious insiders, or even students or staff with malicious intent can exploit vulnerabilities in the network's security measures to gain access to sensitive data, steal personal information, or disrupt operations.

Malware and viruses: These are malicious software programs that can infect the network and cause damage or steal data. They can be spread through emails, downloads, or by exploiting vulnerabilities in software or hardware.

Denial of service attacks: This occurs when the network is flooded with traffic or requests, making it unavailable to users. These attacks can be launched by hackers or other malicious actors to disrupt operations, cause damage, or steal data.

Phishing and social engineering attacks: These are tactics used by cybercriminals to trick users into divulging sensitive information, such as usernames, passwords, or financial data. They can be carried out through emails, phone calls, or social media.

Insider threats: These are risks associated with users who have legitimate access to the network but misuse their privileges. This can include intentional or accidental actions that compromise the security of the network or its data.

Physical security breaches: These occur when someone gains physical access to the network infrastructure, such as servers, routers, or switches. This can result in theft or damage to the equipment, or unauthorized access to the network.

Lack of security updates and patches: This can leave the network vulnerable to known security vulnerabilities that have not been addressed through updates or patches.

To mitigate these risks, universities should implement a comprehensive security strategy that includes firewalls, intrusion detection and prevention systems, antivirus software, access controls, and employee training programs. Regular security assessments and audits should also be conducted to identify vulnerabilities and ensure compliance with security policies and regulations.