Module-1

Introduction to Networks:

Network and uses of Networks:

A network is a collection of interconnected devices, such as computers, servers, routers, switches, and other communication devices, that are linked together to share resources, exchange data, and communicate with each other. In a network, these devices are connected using physical cables or wireless connections, forming a communication infrastructure that enables the transfer of information and resources between the connected devices.

Networks have become an integral part of modern life and are used in various domains to facilitate communication, data exchange, and resource sharing. Here are some of the key uses of networks:

1. Communication: Networks enable seamless communication between individuals and organizations. Email, instant messaging, video conferencing, and voice calls are all possible because of networks, allowing people to stay connected regardless of their physical location.

2. Internet Access: Networks provide access to the internet, enabling users to browse the web, access online services, and search for information from anywhere in the world.

3. File Sharing and Resource Sharing: Networks allow users to share files and resources such as printers, scanners, and storage devices, making it easier to collaborate and exchange information.

4. Business Applications: Networks are essential for businesses to manage their operations efficiently. They support enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, and other business applications that help with inventory management, sales tracking, and customer support.

5. Cloud Computing: Networks are the backbone of cloud computing, allowing users to access computing resources, applications, and data over the internet on a pay-as-you-go basis.

6. Internet of Things (IoT): Networks connect a wide range of devices and sensors in the Internet of Things, enabling data collection, analysis, and remote monitoring for various applications like smart homes, smart cities, and industrial automation.

7. Online Gaming: Networks facilitate online gaming, allowing players from different locations to connect and play together in real-time.

8. Social Networking: Social networks rely on networks to connect people globally, enabling them to share information, interact, and stay connected with friends, family, and colleagues.

9. Remote Access and Telecommuting: Networks enable remote access to corporate resources, allowing employees to work from home or remote locations and access company data securely.

10. E-commerce and Online Transactions: Networks are essential for e-commerce, enabling online stores, payment gateways, and customers to conduct secure and seamless online transactions.

11. Education and E-Learning: Networks support e-learning platforms and online education, providing students and educators with access to educational resources and remote learning opportunities.

12. Telecommunications: Telephone networks and mobile networks provide voice and data communication over vast geographical areas, connecting people across the globe.

13. Healthcare and Telemedicine: Networks facilitate telemedicine and remote patient monitoring, enabling healthcare professionals to offer medical services and consultations from a distance.

14. Transportation and Traffic Management: Networks are used in transportation systems for traffic management, vehicle tracking, and smart transportation solutions to improve efficiency and safety.

15. Research and Development: Networks are crucial for collaborative research, allowing researchers from different institutions to share data, conduct experiments, and collaborate on projects.

In summary, networks play a pivotal role in modern society, transforming the way we communicate, work, and interact. They have revolutionized numerous industries, enhanced global connectivity, and opened up new possibilities for innovation and collaboration.

Types and topologies of Networks:

Types of Networks:

1. Local Area Network (LAN):
A LAN is a network that covers a small geographic area, typically within a single building or campus. LANs are commonly used in homes, offices, schools, and small businesses. They provide high-speed data transfer and resource sharing among connected devices. Ethernet and Wi-Fi are commonly used technologies for LANs.

2. Wide Area Network (WAN):
A WAN is a network that spans a larger geographic area, connecting devices across cities, countries, or even continents. WANs utilize various communication links, such as leased lines, satellite links, and internet connections, to connect geographically dispersed locations. The internet itself is an example of a global WAN.

3. Metropolitan Area Network (MAN):
A MAN is a network that covers a larger area than a LAN but smaller than a WAN, typically spanning across a city or metropolitan area. MANs are used to connect multiple local networks within a city to provide efficient data exchange and resource sharing.

4. Personal Area Network (PAN):
A PAN is a small-scale network that connects personal devices, such as smartphones, tablets, laptops, and wearable devices, within the proximity of an individual user. Bluetooth and Zigbee are common technologies used for PANs.

Topologies of Networks:

1. Bus Topology:
In a bus topology, all devices are connected to a central communication channel, known as the bus. Each device on the network can receive data transmitted over the bus. However, communication collisions can occur when multiple devices attempt to transmit data simultaneously, leading to potential performance issues.

2. Star Topology:
In a star topology, all devices are connected to a central hub or switch. The hub acts as a central point of control for communication and facilitates data exchange between connected devices. Star topologies offer better performance and easier troubleshooting, as a failure of one device does not affect the entire network.

3. Ring Topology:
In a ring topology, each device is connected to exactly two other devices, forming a closed loop. Data circulates in one direction around the ring until it reaches its intended destination. Ring topologies provide more organized data transmission but can suffer from a single point of failure if one device on the ring fails.

4. Mesh Topology:
In a mesh topology, every device is connected to every other device, creating multiple redundant paths for data transmission. Mesh networks provide high redundancy and fault tolerance, as data can be rerouted if a direct path is unavailable. However, the high number of connections can be costly and complex to manage.

5. Tree (Hierarchical) Topology:
A tree topology is a combination of star and bus topologies. Devices are arranged in a hierarchical structure with multiple levels of interconnected hubs and switches. The root node connects to various branches, creating a tree-like structure. Tree topologies are suitable for large networks with multiple subnetworks.

6. Hybrid Topology:
A hybrid topology is a combination of two or more different topologies. For example, a hybrid topology could have a central star backbone with additional bus or ring networks connected to it. Hybrid topologies offer flexibility and can cater to specific network requirements.

The choice of network type and topology depends on the size, requirements, and budget of the network, as well as the level of redundancy and fault tolerance needed to meet the organization's needs.

TCP/IP Model:

The TCP/IP model, also known as the Internet Protocol Suite, is a conceptual framework and a set of protocols used for communication in computer networks. It is the foundation of the internet and has become the standard for network communication in modern networking. The TCP/IP model consists of four layers, each responsible for specific tasks related to data transmission and communication. These layers are:

1. Application Layer:
The Application Layer is the top layer of the TCP/IP model and is closest to the end-users and applications. It provides network services directly to user applications and allows different applications to communicate over the network. This layer includes protocols such as HTTP (HyperText Transfer Protocol) for web browsing, SMTP (Simple Mail Transfer Protocol) for email, FTP (File Transfer Protocol) for file transfer, and DNS (Domain Name System) for domain name resolution.

2. Transport Layer:
The Transport Layer is responsible for end-to-end communication between devices. It ensures reliable and orderly data delivery by breaking data into smaller packets and reassembling them at the destination. The two main transport layer protocols are:

- Transmission Control Protocol (TCP): TCP provides reliable, connection-oriented communication. It guarantees that data packets are delivered in order and without loss, performing error checking and retransmission if necessary.

- User Datagram Protocol (UDP): UDP is a connectionless, faster, and less reliable protocol compared to TCP. It is suitable for applications where real-time data delivery is more critical than error recovery, such as streaming media or online gaming.

3. Internet Layer:
The Internet Layer, also known as the Network Layer, handles routing and forwarding of data packets across multiple networks. It is responsible for addressing, fragmentation, and packet forwarding. The primary protocol of the Internet Layer is the Internet Protocol (IP). IP addresses are used to identify devices on a network, and routers use IP addresses to forward packets to their intended destinations.

4. Link Layer (Network Access Layer):
The Link Layer is the lowest layer of the TCP/IP model and is responsible for the physical transmission of data over the network medium. It defines how data is formatted for transmission and how it is sent and received through the network hardware. The Link Layer includes various protocols depending on the network type, such as Ethernet, Wi-Fi (IEEE 802.11), and PPP (Point-to-Point Protocol).

The TCP/IP model is a flexible and scalable framework that enables communication between diverse network devices and systems. It has been widely adopted and is the foundation of the internet and modern networking technologies, allowing seamless data exchange and communication across the global network.

OSI Model:

The OSI (Open Systems Interconnection) model is a conceptual framework and a seven-layered reference model used to understand and standardize communication protocols in computer networks. Developed by the International Organization for Standardization (ISO) in 1984, the OSI model serves as a guideline for the design and implementation of network protocols and communication standards. Each layer of the OSI model performs specific functions and interacts with adjacent layers to facilitate data transmission and communication between devices. The seven layers of the OSI model, from the top layer to the bottom layer, are as follows:

1. Application Layer (Layer 7):
The Application Layer is the top layer of the OSI model and is responsible for providing network services directly to user applications. It enables communication between user applications and the network. Protocols in this layer include HTTP, SMTP, FTP, DNS, and others.

2. Presentation Layer (Layer 6):
The Presentation Layer is responsible for data formatting, encryption, and compression to ensure that data from the Application Layer of one system is understood by the Application Layer of another system. It deals with data representation and translation between different data formats.

3. Session Layer (Layer 5):
The Session Layer establishes, maintains, and terminates connections between applications running on different devices. It manages sessions or dialogues between applications and provides synchronization and checkpointing mechanisms for data exchange.

4. Transport Layer (Layer 4):
The Transport Layer is responsible for end-to-end communication and data transfer between devices. It ensures reliable and orderly data delivery by breaking data into smaller segments and reassembling them at the destination. The main protocols in this layer are TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

5. Network Layer (Layer 3):
The Network Layer is responsible for routing and forwarding data packets between different networks. It handles logical addressing, such as IP addresses, and determines the best path for data transmission. The main protocol in this layer is IP (Internet Protocol).

6. Data Link Layer (Layer 2):
The Data Link Layer is responsible for framing data into frames, addressing, and error detection in the physical transmission of data over the network medium. It ensures reliable point-to-point communication between directly connected devices. Ethernet and Wi-Fi (IEEE 802.11) are common examples of Data Link Layer protocols.

7. Physical Layer (Layer 1):
The Physical Layer is the lowest layer of the OSI model and deals with the actual physical transmission of data bits over the network medium. It defines the characteristics of the hardware, such as cables, connectors, and network interfaces, used for data transmission.

The OSI model provides a common language and framework for network designers, administrators, and developers to understand and troubleshoot network communication. While the OSI model is a conceptual reference, most practical network implementations are based on the TCP/IP model, which is more widely used in real-world networking.

The OSI vs TCP/IP reference model:

The OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) model are both conceptual frameworks that describe the functions and protocols used in computer networks. While they serve similar purposes of understanding and standardizing network communication, they have some key differences:

1. Number of Layers:
- OSI Model: The OSI model consists of seven layers, each with a specific set of functions and responsibilities. The layers are Application, Presentation, Session, Transport, Network, Data Link, and Physical.
- TCP/IP Model: The TCP/IP model, also known as the Internet Protocol Suite, is a four-layer model. The layers are Application, Transport, Internet, and Link.

2. Standardization:
- OSI Model: The OSI model is a theoretical model that was developed by the International Organization for Standardization (ISO) in 1984. While it provides a comprehensive framework, it is not as widely implemented in real-world networking.
- TCP/IP Model: The TCP/IP model is the de facto standard for internet communication and is the basis for the actual implementation of the internet and most modern computer networks. It was developed by the U.S. Department of Defense and was designed to work with the internet's architecture.

3. Layer Nomenclature:
- OSI Model: The OSI model uses descriptive names for its layers, such as Application, Transport, and Data Link, which indicate the functions performed by each layer.

- TCP/IP Model: The TCP/IP model uses different names for its layers, such as Application, Transport, Internet, and Link. The layers in the TCP/IP model do not precisely align with the functions of the OSI model.

4. Encapsulation:
- OSI Model: The OSI model follows a strict encapsulation hierarchy, where data is encapsulated at each layer with a header specific to that layer's function. As data moves down the layers, each layer adds its header to the data.
- TCP/IP Model: The TCP/IP model also follows encapsulation, but it is more flexible and less rigidly structured compared to the OSI model. It allows for some layers to combine functions and does not have a one-to-one mapping with the OSI model's encapsulation process.

5. Adoption and Use:
- OSI Model: The OSI model is used primarily for educational and theoretical purposes. It is not commonly used as a practical networking reference in the industry.
- TCP/IP Model: The TCP/IP model is the foundation for the actual implementation of the internet and most modern computer networks. It is widely used and serves as the basis for the design and configuration of real-world networks.

In summary, while both the OSI and TCP/IP models serve as reference frameworks for understanding network communication, the TCP/IP model has become the de facto standard in practical networking and is the basis for the functioning of the internet and modern network infrastructures. The OSI model, on the other hand, provides a more comprehensive and detailed theoretical model, but its practical adoption is limited.

Architecture of Internet:

The architecture of the internet refers to the structure and design principles that underlie the functioning and organization of the global network of interconnected computers. The internet's architecture is based on a decentralized and distributed model, allowing information and data to flow across a vast network of interconnected devices. Here are the key components of the internet's architecture:

1. Packet Switching:
The internet uses packet switching as its fundamental method for transmitting data. Data is divided into smaller units called packets before being sent over the network. Each packet contains a portion of the data, along with the source and destination addresses. These packets are then independently routed through various network nodes to their destination, where they are reassembled to reconstruct the original data. Packet switching allows for efficient and reliable data transmission, as it can adapt to varying network conditions and ensure data delivery even if some packets are lost or delayed.

2. IP Addressing:
The internet relies on IP (Internet Protocol) addressing to uniquely identify devices connected to the network. Each device, whether it is a computer, smartphone, server, or any other networked device, is assigned a unique IP address. IP addresses are used to route data packets to their intended destinations across the internet.

3. Domain Name System (DNS):
To make it easier for users to access resources on the internet, the Domain Name System (DNS) is used. DNS translates human-readable domain names (like www.example.com) into their corresponding IP addresses. This allows users to access websites and resources using domain names instead of having to remember numerical IP addresses.

4. Routers:
Routers are essential components of the internet's architecture. They are responsible for forwarding data packets between different networks. Routers use routing tables to determine the best path for data packets to reach their destinations, ensuring efficient data transmission across the network.

5. Internet Service Providers (ISPs):
Internet Service Providers play a crucial role in the internet's architecture. ISPs provide access to the internet for end-users and organizations. They connect their customers to the internet through various means, such as DSL, cable, fiber, or wireless connections.

6. Protocols:
The internet uses a wide range of protocols, including TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) for transport, IP (Internet Protocol) for network layer, HTTP (Hypertext Transfer Protocol) for web browsing, SMTP (Simple Mail Transfer Protocol) for email, and many more. These protocols define how data is formatted, transmitted, received, and processed across the internet.

7. Autonomous Systems (AS):
The internet is composed of numerous interconnected networks, each operated by different organizations or entities. These networks are known as Autonomous Systems (AS). Each AS is independently managed and has its own unique IP address space.

8. Peering and Internet Exchange Points (IXPs):
Peering refers to the direct interconnection of networks to exchange traffic without the need to go through third-party networks. Internet Exchange Points (IXPs) are physical locations where multiple networks come together to establish direct peering connections. IXPs facilitate efficient and cost-effective data exchange between networks.

The decentralized and distributed architecture of the internet allows for scalability, fault tolerance, and efficient data transmission. It enables seamless communication, access to information, and the delivery of services to users worldwide, making the internet one of the most transformative inventions in modern history.

Guided and wireless transmission media:

Guided Transmission Media:

Guided transmission media, also known as wired transmission media, are physical pathways that use cables or wires to transmit data signals from one point to another. These cables provide a guided path for the data signals, ensuring secure and reliable data transmission. Some common types of guided transmission media include:

1. Twisted Pair Cable:
Twisted pair cables consist of pairs of copper wires twisted together to reduce electromagnetic interference (EMI) and crosstalk. They are widely used for Ethernet networking and telephone connections. Twisted pair cables are available in two types: Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP).

2. Coaxial Cable:
Coaxial cables have a central copper conductor surrounded by insulation, a braided shield, and an outer jacket. They are commonly used for cable television (CATV) and broadband internet

connections.

3. Fiber Optic Cable:
Fiber optic cables use thin strands of glass or plastic to transmit data as pulses of light. They offer high data transmission rates, immunity to electromagnetic interference, and long-distance capabilities. Fiber optic cables are widely used in high-speed internet connections, telecommunications, and data center networks.

4. Ethernet Cables:
Ethernet cables are a type of guided transmission media used for local area networks (LANs). They can be either twisted pair cables (UTP or STP) or fiber optic cables, depending on the network's requirements and data transmission speed.

Wireless Transmission Media:

Wireless transmission media use electromagnetic waves to transmit data signals without the need for physical cables or wires. Wireless communication provides mobility and flexibility, allowing devices to connect and communicate without being tethered to a specific location. Some common types of wireless transmission media include:

1. Radio Waves:
Radio waves are used for wireless communication in various applications, such as radio broadcasting, Wi-Fi networks, Bluetooth, and cellular networks. Devices like radios, mobile phones, laptops, and IoT devices use radio waves to communicate wirelessly.

2. Microwaves:
Microwave signals are used for point-to-point communication over long distances, such as in satellite communication and microwave links used by telecommunications providers to connect remote areas.

3. Infrared:
Infrared signals are used for short-range communication between devices, such as in infrared remote controls for televisions and other consumer electronics.

4. Visible Light:
Visible light communication (VLC) uses light-emitting diodes (LEDs) to transmit data signals. VLC can be used for indoor positioning, data transmission in environments where radio frequency (RF) communication is restricted, and for certain applications in smart lighting systems.

5. Satellite Communication:
Satellite communication involves the use of artificial satellites in space to relay signals over long distances. Satellite communication is commonly used for television broadcasting, global positioning systems (GPS), and long-distance data transmission.

Wireless transmission media offer the advantage of mobility and convenience, allowing users to access data and communication services from anywhere within the coverage area. However, they are susceptible to interference and signal degradation due to factors like distance, obstructions, and environmental conditions. Guided transmission media, on the other hand, provide a more reliable and secure connection but may have limitations in terms of flexibility and mobility. The choice between guided and wireless transmission media depends on the specific requirements and constraints of the network or communication system.

Switching.

Switching in the context of computer networks refers to the process of forwarding data packets from a source device to a destination device within a network. It involves making decisions about how data should be routed or forwarded to ensure efficient and reliable communication between devices. Switching can occur at different layers of the OSI (Open Systems Interconnection) model, depending on the type of network and the technology used. The two main types of switching in computer networks are:

1. Circuit Switching:
Circuit switching is a method used in traditional telecommunication networks and was commonly used in early telephone systems. In circuit switching, a dedicated communication path, or circuit, is established between the source and destination devices before data transmission begins. Once the circuit is established, data is transmitted continuously along this dedicated path until the communication session is completed. During the transmission, the entire bandwidth of the circuit is reserved for the duration of the communication session, regardless of whether data is being transmitted or not. Circuit switching is characterized by low latency and guarantees a constant data rate, making it suitable for real-time applications like voice calls. However, it is less efficient for bursty or sporadic data transmission and can be less flexible in handling varying traffic loads.

2. Packet Switching:
Packet switching is the prevalent method used in modern computer networks, including the internet. In packet switching, data is divided into smaller units called packets before being transmitted over the network. Each packet contains a portion of the data, along with the source and destination addresses. Packets are individually routed and forwarded through the network to their destination using the most efficient path available at that time. Unlike circuit switching, packet switching does not require the reservation of a dedicated communication path for the entire duration of the transmission. Instead, each packet can take different paths through the network based on the current network conditions and available resources. Packet switching is more flexible and efficient for handling varying traffic loads and is well-suited for data transmission, including web browsing, email, and file transfer.

Switching Devices:

Switching in computer networks is facilitated by specialized devices called switches or routers. These devices examine the destination address of each incoming data packet and make decisions about where to forward the packet next. Switches are typically used in local area networks (LANs) and are responsible for forwarding data between devices within the same network segment. Routers, on the other hand, are used in wide area networks (WANs) and are responsible for forwarding data between different networks or network segments.

In summary, switching is a fundamental process in computer networks that enables data packets to be efficiently and reliably forwarded from source to destination. Circuit switching and packet switching are the two main approaches to data transmission, with packet switching being the dominant method used in modern computer networks and the internet. Switches and routers are the key devices used for switching data packets within networks and between different networks.

Module-2

Physical & Data Link Layer:
Ethernet:

Ethernet is a widely used technology that operates at both the Physical Layer and the Data Link Layer of the OSI (Open Systems Interconnection) model. It is a set of standards for wired LAN (Local Area Network) communication, enabling devices to connect and communicate within a network. Ethernet defines the physical and data link protocols necessary for transmitting data between devices over Ethernet cables.

1. Physical Layer (Layer 1):
At the Physical Layer, Ethernet specifies the hardware characteristics and transmission media used for communication. It defines the physical medium over which data is transmitted, including the type of cable, connectors, and signaling techniques. Some common physical layer specifications for Ethernet include:

- Ethernet Cables: The most commonly used Ethernet cables are twisted pair cables and fiber optic cables. Twisted pair cables, such as Cat5e, Cat6, and Cat6a, use copper wires twisted together to reduce interference. Fiber optic cables use thin strands of glass or plastic to transmit data as pulses of light, offering higher bandwidth and longer distances compared to copper cables.

- Ethernet Connectors: Ethernet cables typically use RJ-45 connectors for twisted pair cables and various types of connectors (ST, SC, LC) for fiber optic cables.

- Ethernet Speeds: Ethernet supports various data transmission speeds, commonly referred to as Ethernet standards. Some common Ethernet speeds include 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), 10 Gbps (10 Gigabit Ethernet), and higher.

- Ethernet Hubs and Switches: In older Ethernet networks, hubs were used to connect devices within a network. However, modern Ethernet networks use switches, which provide more efficient data transmission and help reduce network collisions.

2. Data Link Layer (Layer 2):
At the Data Link Layer, Ethernet defines the frame format and the media access control (MAC) protocols for Ethernet networks. The Data Link Layer ensures the reliable transmission of data frames between devices on the same local network. Ethernet uses the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol for shared Ethernet networks. In CSMA/CD, devices listen to the network before transmitting data to avoid collisions. If a collision is detected, the devices back off and retry later to avoid further collisions.

- Ethernet Frames: Data packets in Ethernet are encapsulated in frames at the Data Link Layer. An Ethernet frame typically includes a preamble, destination and source MAC addresses, type or length field, data payload, and a cyclic redundancy check (CRC) for error detection.

- MAC Address: Each network interface card (NIC) in an Ethernet device is assigned a unique MAC address. The MAC address is used to identify devices on the local network and is essential for delivering data frames to their intended destinations.

Ethernet has evolved over the years, and its various standards have become the dominant technology for wired LANs in homes, offices, data centers, and other environments. It remains a critical component of modern networking, enabling reliable and high-speed communication between devices in local networks and connecting them to larger networks and the internet.

Physical Layer and Data link layer switching:

Physical Layer Switching and Data Link Layer Switching are two distinct concepts related to network communication and switching technologies. Let's explore each of them:

1. Physical Layer Switching:

Physical Layer Switching, also known as Layer 1 switching, refers to the process of forwarding data at the physical layer of the OSI model. In this context, "switching" is not the same as what is typically associated with network switches. Instead, it involves using hardware-based techniques to directly forward data signals without performing any higher-layer processing.

One example of physical layer switching is in a network switch or bridge that operates purely at the physical layer. In this scenario, the switch simply receives incoming electrical signals (e.g., electrical voltages representing bits on a copper cable or light signals on a fiber optic cable) and regenerates or repeats those signals to transmit them to the appropriate destination port. The switch doesn't examine the content of the data packets; it simply forwards the electrical or optical signals based on the destination port information.

Physical layer switching is relatively simple and fast, but it lacks the intelligence and decision-making capabilities found in higher-layer switches, such as data link layer switches.

2. Data Link Layer Switching:

Data Link Layer Switching, also known as Layer 2 switching, refers to the process of forwarding data frames at the data link layer of the OSI model. This type of switching is commonly associated with network switches that operate at Layer 2.

Data link layer switches are more sophisticated than physical layer switches. They examine the MAC addresses (Layer 2 addresses) in incoming Ethernet frames to make intelligent forwarding decisions. When a frame arrives at the switch, the switch looks up the destination MAC address in its MAC address table to determine which port the frame should be forwarded to. This process is known as MAC address learning.

Data link layer switches use MAC address tables to maintain records of which devices are connected to which switch ports. As frames are received, the switch populates its MAC address table by associating MAC addresses with the corresponding switch ports. This allows the switch to efficiently forward frames directly to the destination port, rather than broadcasting them to all ports like a hub would do.

Data link layer switching provides better performance, reduces network collisions, and improves overall network efficiency compared to physical layer switching or hub-based networks.

In summary, physical layer switching involves basic hardware-based forwarding of electrical or optical signals at the physical layer, while data link layer switching involves intelligent forwarding of Ethernet frames based on MAC addresses at the data link layer. Data link layer switching, performed by modern network switches, is a fundamental technology used in local area networks (LANs) to ensure efficient and reliable data transmission between devices.

Learning bridges:

Learning bridges, also known as Ethernet bridges or MAC bridges, are network devices that operate at the data link layer (Layer 2) of the OSI model. They are used to interconnect multiple network segments within a local area network (LAN) and intelligently forward Ethernet frames

between those segments. Learning bridges are an essential component of modern network switches.

The main function of a learning bridge is to learn the MAC addresses of devices connected to its ports and maintain a MAC address table, also known as a forwarding table or filtering database. When an Ethernet frame arrives at the bridge, it examines the source MAC address in the frame and associates it with the port through which the frame was received. The bridge then updates its MAC address table with this information.

When a frame with a destination MAC address arrives at the bridge, the bridge looks up the destination MAC address in its MAC address table. If the MAC address is found in the table, the bridge knows which port the destination device is connected to and forwards the frame only to that port. This process is known as unicast forwarding.

If the destination MAC address is not found in the MAC address table, the bridge does not know the location of the destination device. In this case, the bridge broadcasts the frame out to all ports (except the port where the frame was received). This is known as flooding. When the destination device responds to the broadcast frame, the bridge learns its MAC address and updates the MAC address table accordingly, allowing subsequent frames to be unicast forwarded to the correct port.

The learning and forwarding process of bridges ensures that frames are efficiently delivered only to the ports where the destination devices are located, reducing unnecessary network traffic and preventing network loops.

Originally, bridges were used to connect separate Ethernet segments to form larger LANs, allowing devices in different segments to communicate with each other transparently. Today, learning bridges are an integral part of network switches, which often include multiple ports and support more advanced features, such as VLANs (Virtual LANs) for network segmentation and Spanning Tree Protocol (STP) for loop prevention.

Overall, learning bridges play a vital role in improving the efficiency and performance of local area networks by intelligently forwarding Ethernet frames based on MAC addresses and dynamically learning the location of devices connected to the network.

spanning tree bridges:

Spanning Tree Bridges, also known as Spanning Tree Protocol (STP) bridges, are network devices that use the Spanning Tree Protocol to prevent loops in Ethernet networks. The Spanning Tree Protocol is a network protocol that allows bridges (or switches) to dynamically create a loop-free logical topology, even when there are redundant paths in the physical network.

The main purpose of the Spanning Tree Protocol is to prevent broadcast storms and data packet duplication that can occur in networks with loops. Without loop prevention, broadcast frames and unknown unicast frames could endlessly circulate in the network, leading to excessive network traffic and performance issues.

Here's how the Spanning Tree Protocol works:

1. Electing the Root Bridge:
In a network with multiple bridges (switches), the first step is to elect a single "Root Bridge." The Root Bridge acts as the central reference point for the entire network. All bridges participate in a root bridge election process, and the bridge with the lowest bridge ID becomes the Root Bridge. The bridge ID consists of a priority value and the bridge MAC address.

2. Determining the Root Ports:
Each non-Root Bridge determines its "Root Port," which is the port that has the shortest path (lowest cost) to the Root Bridge. The cost of a path is typically based on the link speed. Ports with lower path costs are selected as Root Ports.

3. Selecting Designated Ports:
For each network segment (collision domain), one bridge port is designated as the "Designated Port." The Designated Port is the port that offers the shortest path to the Root Bridge. All other non-Root Bridge ports on that segment are put in a blocking state (discarding frames).

4. Creating a Loop-Free Topology:
The Spanning Tree Protocol dynamically places some bridge ports into a "Blocking" state, effectively disabling those ports from forwarding data frames. By blocking redundant paths, a loop-free logical topology is established, ensuring that data frames follow a single path to reach their destination, avoiding the possibility of loops.

5. Handling Changes in the Network:
The Spanning Tree Protocol continuously monitors the network for changes, such as link failures or new bridge additions. If a network change is detected, the bridges run the Spanning Tree Protocol again to recalculate the best paths and reconfigure the forwarding ports accordingly.

Spanning Tree Bridges work together to ensure a stable and loop-free network topology, providing a reliable and efficient communication environment. While Spanning Tree Protocol is effective in preventing loops, it may introduce some convergence delays when topology changes occur. To address this, newer protocols like Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) have been developed to provide faster convergence and better utilization of redundant paths.

repeaters:

Repeaters are network devices used to extend the reach of a network by amplifying and regenerating digital signals. They operate at the Physical Layer (Layer 1) of the OSI model and are primarily used in wired networks to overcome signal attenuation and maintain signal integrity over long distances.

In networking, signals traveling over cables, such as copper twisted pair cables or fiber optic cables, can lose strength (attenuate) as they travel through the transmission medium. This attenuation limits the distance over which data can be reliably transmitted without degradation or errors. Repeaters are deployed strategically along the network to counteract signal loss and extend the effective distance of the network.

Key features and functions of repeaters:

1. Signal Regeneration: When a digital signal weakens due to attenuation, the repeater receives the signal, cleans it up, and regenerates it to its original strength. By doing so, the repeater ensures that the signal remains strong and consistent as it continues its journey across the network.

2. Transparent Operation: Repeaters are transparent devices, meaning they do not modify the data packets or frames passing through them. They only deal with electrical or optical signals at the physical layer, making them agnostic to the higher-layer protocols and data contents.

3. Physical Layer Device: Repeaters work at the lowest layer of the OSI model, which means they operate on raw bits and have no knowledge of the structure or content of data packets. This makes them suitable for any type of data transmission, including Ethernet, Token Ring, or other physical layer protocols.

4. Signal Amplification: Repeaters amplify the signal, increasing its strength, which allows it to travel longer distances before another repeater is required.

5. Placement: Repeaters should be placed strategically to ensure proper signal strength and coverage. Their placement depends on the network's physical layout and the distance limitations of the transmission medium used.

It's important to note that modern network technologies, such as Ethernet, commonly use switches instead of repeaters for signal regeneration and extending network coverage. Switches operate at higher layers of the OSI model (Data Link Layer), allowing them to process and forward data based on MAC addresses. Switches provide better performance, security, and segmentation capabilities compared to repeaters.

Repeaters were more prevalent in older networks, such as legacy Ethernet networks or Token Ring networks, where switches were not widely available or practical. With the advancement of network technology and the widespread adoption of switches, repeaters have become less common in modern network infrastructures.

hubs:

Hubs are network devices used to connect multiple devices in a local area network (LAN). They operate at the Physical Layer (Layer 1) of the OSI model and are designed to receive data signals from one port and broadcast those signals to all other ports, effectively sharing the incoming data with all connected devices. Hubs were commonly used in older Ethernet networks but have largely been replaced by more advanced devices like switches.

Key features and functions of hubs:

1. Signal Broadcasting: When a data signal arrives at any port of the hub, the hub repeats or regenerates the signal and sends it out to all other ports. This broadcast-based approach means that all connected devices receive the transmitted data, regardless of whether they are the intended recipients or not.

2. Shared Bandwidth: Hubs operate in a shared bandwidth environment, meaning that the total available bandwidth is shared among all connected devices. This can lead to performance issues, especially as the number of connected devices and network traffic increases.

3. Collision Domain: In a hub-based network, all connected devices are part of the same collision domain. This means that data collisions can occur when two or more devices try to transmit data simultaneously, leading to inefficiencies and reduced network throughput.

4. Limited Network Segmentation: Hubs do not provide network segmentation. All devices connected to a hub are part of the same LAN and share the same broadcast domain. This lack of segmentation can lead to increased broadcast and multicast traffic, resulting in higher network congestion.

5. Hub vs. Switch: Compared to switches, which operate at the Data Link Layer (Layer 2), hubs lack the intelligence to make forwarding decisions based on MAC addresses. Switches selectively

forward data only to the port where the intended recipient is located, leading to better network performance and reduced unnecessary network traffic.

It's important to note that hubs have largely become obsolete in modern network infrastructure due to their limitations and inefficiencies. Network switches, which are widely used today, provide a much more efficient and intelligent way of connecting devices in a LAN. Switches offer dedicated bandwidth to each connected device, facilitate network segmentation through Virtual LANs (VLANs), and significantly reduce the likelihood of collisions, leading to improved network performance and better data transmission capabilities. As a result, hubs have been largely replaced by switches in most networking applications.

bridges:

Bridges are network devices that operate at the Data Link Layer (Layer 2) of the OSI model and are used to interconnect multiple network segments or LANs (Local Area Networks). Bridges are designed to improve network efficiency and reduce network collisions by selectively forwarding data frames between different network segments.

Key features and functions of bridges:

1. Segmentation: Bridges segment a LAN into multiple collision domains. Each network segment connected to a bridge operates as a separate collision domain, which means that data collisions are limited to the devices within that segment. This segmentation reduces the likelihood of network collisions and improves overall network performance.

2. Filtering: Bridges use the MAC (Media Access Control) addresses in Ethernet frames to make intelligent forwarding decisions. When an Ethernet frame arrives at a bridge, the bridge examines the destination MAC address in the frame and checks its forwarding table to determine which network segment the destination device is located. The bridge then forwards the frame only to the appropriate segment, reducing unnecessary network traffic.

3. Learning MAC Addresses: Bridges dynamically learn the MAC addresses of devices connected to each of their network segments. As frames are received, the bridge associates the source MAC addresses with the corresponding network segments in its forwarding table. This learning process enables the bridge to make more efficient forwarding decisions in the future.

4. Loop Prevention: Bridges use the Spanning Tree Protocol (STP) to prevent loops in the network. The Spanning Tree Protocol dynamically creates a loop-free logical topology by selectively blocking redundant paths in the network.

5. Transparent Operation: Bridges are transparent devices that operate at the Data Link Layer. They do not modify the content of data frames but focus on making decisions based on MAC addresses.

6. Extending the Network: Bridges enable the extension of LANs beyond their physical limitations by connecting multiple segments together. They facilitate communication between devices in different network segments as if they were part of the same LAN.

It's important to note that modern network switches have largely replaced bridges in today's network infrastructure. Switches offer similar functionality to bridges, but with additional benefits, such as faster data forwarding, better scalability, and support for advanced features like VLANs (Virtual LANs) for network segmentation. While bridges were common in older Ethernet networks, switches have become the primary choice for interconnecting network segments in

modern LANs due to their superior performance and capabilities.

switches:

Switches are network devices that operate at the Data Link Layer (Layer 2) of the OSI model and are used to connect multiple devices within a local area network (LAN). They intelligently forward data frames based on their destination MAC addresses, making data transmission more efficient and reducing network collisions. Switches are a fundamental component of modern networking and have largely replaced hubs and bridges in local area networks.

Key features and functions of switches:

1. MAC Address Learning: When an Ethernet frame arrives at a switch, the switch examines the source MAC address in the frame and associates it with the port through which the frame was received. The switch maintains a MAC address table (also known as a forwarding table) that maps MAC addresses to their corresponding switch ports. This learning process allows the switch to build an efficient forwarding database.

2. Forwarding Decision: When a switch receives a data frame with a destination MAC address, it looks up the destination MAC address in its MAC address table. If the MAC address is found, the switch knows which port the destination device is connected to and forwards the frame only to that specific port. This process is called unicast forwarding and is one of the key features that make switches more efficient than hubs.

3. Broadcast and Multicast Handling: If the destination MAC address is not found in the MAC address table, the switch will broadcast the frame out to all ports (except the incoming port). This ensures that the frame reaches all devices on the network. Additionally, switches handle multicast traffic by forwarding frames only to the ports where devices have requested to receive multicast traffic.

4. Collision Domains: Each switch port operates as a separate collision domain. This means that devices connected to different switch ports can transmit data simultaneously without causing collisions. Unlike hubs, which have a single collision domain for all connected devices, switches provide dedicated bandwidth for each connected device, improving overall network performance.

5. VLAN Support: Many switches support Virtual LANs (VLANs), which allow the network to be logically segmented into multiple virtual networks. VLANs provide greater network security, improved network management, and enhanced traffic isolation.

6. Full-Duplex Communication: Switches enable full-duplex communication between devices. Full-duplex communication allows devices to transmit and receive data simultaneously, effectively doubling the available bandwidth for each connection.

Overall, switches offer significant advantages over hubs and bridges, including better network performance, reduced network collisions, improved security, and support for advanced network features. They have become the standard choice for interconnecting devices in local area networks and are essential components in modern networking infrastructure.

routers:

Routers are network devices that operate at the Network Layer (Layer 3) of the OSI model. They are essential for connecting multiple networks together, directing data traffic between them, and determining the optimal paths for data packets to reach their destinations. Routers are critical components in both local area networks (LANs) and wide area networks (WANs), including the

internet.

Key features and functions of routers:

1. Network Interconnection: Routers are responsible for interconnecting multiple networks, such as LANs or different segments of the internet. They receive data packets from one network and forward them to the appropriate destination network based on the destination IP address.

2. IP Addressing: Routers use IP (Internet Protocol) addresses to identify and route data packets. Each connected network segment has its unique IP address range, and routers maintain a routing table that maps IP addresses to the corresponding network interfaces.

3. Routing Decisions: When a router receives a data packet, it examines the destination IP address and searches its routing table to determine the best path to forward the packet. Routers use various routing protocols, such as RIP (Routing Information Protocol), OSPF (Open Shortest Path First), and BGP (Border Gateway Protocol), to exchange routing information with other routers and make informed routing decisions.

4. Path Selection: Routers select the most efficient path for data packets to reach their destinations. The path is determined based on factors like hop count, link speed, network congestion, and administrative distance. The process of determining the best path is known as routing.

5. Network Segmentation: Routers provide network segmentation, ensuring that data traffic is contained within its appropriate network boundaries. This segmentation improves network security and isolates potential network issues from spreading across the entire network.

6. Network Address Translation (NAT): Routers can perform Network Address Translation, allowing private IP addresses used within a local network to be translated to a single public IP address when communicating with external networks like the internet. NAT enables multiple devices within a private network to share a single public IP address.

7. Firewall and Security: Many routers include built-in firewall capabilities, providing network security by filtering and controlling incoming and outgoing traffic based on predefined rules.

8. Dynamic Host Configuration Protocol (DHCP): Routers often offer DHCP services, automatically assigning IP addresses to devices within the local network, simplifying network setup and management.

Routers play a critical role in directing data traffic between networks, ensuring that data packets reach their intended destinations efficiently and securely. In larger networks, multiple routers work together to form a complex network topology, facilitating global connectivity and enabling internet communication as we know it today.

gateways.

Gateways are network devices or software components that serve as entry and exit points between different networks or network protocols. They operate at various layers of the OSI model, depending on their functionality and the type of networks they connect. Gateways play a crucial role in enabling communication between networks with different architectures, protocols, or addressing schemes.

Key features and functions of gateways:

1. Protocol Translation: Gateways can perform protocol translation, converting data from one network protocol to another. For example, a TCP/IP to IPX/SPX gateway can enable communication between networks using different networking protocols.

2. Network Address Translation (NAT): Similar to routers, some gateways provide Network Address Translation (NAT) capabilities, allowing devices in a private network with private IP addresses to access the internet using a single public IP address.

3. Network Interconnection: Gateways interconnect networks that use different communication protocols or have incompatible addressing schemes. They act as bridges between these networks, facilitating data exchange.

4. Application Layer Translation: Some gateways perform application-layer translation, allowing communication between applications that use different data formats or communication methods.

5. Security: Gateways often include security features, such as firewalls and proxy servers, to control and filter network traffic for improved security and protection against unauthorized access.

6. Internet Gateways: Internet gateways connect private networks to the internet. They handle the translation of private IP addresses to public IP addresses, allowing devices within the private network to access the internet.

7. Email Gateways: Email gateways process and forward email messages between different email systems, such as exchanging messages between SMTP (Simple Mail Transfer Protocol) and non-SMTP networks.

8. Voice Gateways: Voice gateways enable communication between traditional telephony systems (PSTN) and Voice over IP (VoIP) networks, allowing voice traffic to be transmitted over IP-based networks.

9. Multi-Protocol Support: Some gateways are capable of supporting multiple protocols simultaneously, enabling seamless communication between different network types.

10. Transparent Operation: Gateways are designed to be transparent to end-users and applications, providing a seamless integration between connected networks.

Gateways are essential in enabling communication and data exchange between diverse networks and systems. They play a crucial role in today's interconnected world, facilitating the smooth operation of various technologies and enabling seamless communication between different networks and protocols.

Data Link Layer -
Design issues:

Design issues in the Data Link Layer of the OSI model involve various challenges and considerations related to efficient and reliable data transmission between directly connected devices over a shared medium. Some of the key design issues in the Data Link Layer include:

1. Framing: One of the primary design issues is how to frame data packets for transmission over the physical medium. Designers must decide on a framing technique that allows the receiver to detect the beginning and end of each frame and accurately extract the data payload.

2. Addressing: The Data Link Layer requires a mechanism for addressing devices on the local network. The choice of addressing scheme, such as MAC addresses, needs to be carefully considered to ensure uniqueness and efficient data delivery.

3. Error Detection and Correction: Designers must implement error detection and correction mechanisms to ensure reliable data transmission. Techniques like CRC (Cyclic Redundancy Check) are commonly used to detect errors in received frames.

4. Flow Control: The Data Link Layer must handle flow control to regulate the rate at which data is sent and received to prevent overwhelming the receiver. Flow control mechanisms like Sliding Window Protocol or Stop-and-Wait Protocol need to be designed and implemented.

5. Medium Access Control (MAC) Protocols: For shared transmission mediums, such as Ethernet, designers must decide on the appropriate MAC protocol to control access to the medium and avoid data collisions. Different MAC protocols, such as CSMA/CD or CSMA/CA, have different characteristics and performance implications.

6. Collision Handling: In shared transmission mediums, data collisions can occur when multiple devices attempt to transmit data simultaneously. Designers need to handle collision scenarios efficiently, such as through collision detection and backoff algorithms.

7. Efficiency and Throughput: Efficient use of available bandwidth is essential for maximizing network throughput. Designers must consider the overhead introduced by framing, addressing, and error checking to optimize data transmission efficiency.

8. Broadcasting and Multicasting: The Data Link Layer needs to handle broadcast and multicast frames appropriately. Broadcast frames are sent to all devices on the network, while multicast frames are directed to a specific group of devices.

9. Network Topology: The Data Link Layer should be designed to support various network topologies, such as point-to-point, bus, ring, or star. The choice of topology impacts factors like data collision likelihood and ease of network management.

10. Security: Designers should consider security aspects, such as MAC address spoofing prevention and data confidentiality, to ensure the integrity of data transmitted at the Data Link Layer.

11. Interoperability: When designing Data Link Layer protocols, interoperability with existing networking technologies and devices is essential to ensure seamless communication between different network elements.

12. Protocol Overhead: Designers must strike a balance between necessary protocol overhead for framing, addressing, and error checking and the available bandwidth to avoid excessive data overhead.

Addressing these design issues in the Data Link Layer requires a deep understanding of network protocols, transmission mediums, and the specific requirements of the network environment. A well-designed Data Link Layer ensures efficient, reliable, and secure data transmission within the local network.

Error Detection & Correction:

Error detection and correction are essential functionalities in the Data Link Layer of the OSI model. They help ensure the accurate and reliable transmission of data over a communication link. Several techniques are used in the Data Link Layer to detect and, in some cases, correct errors that may occur during data transmission. Some common error detection and correction methods in the Data Link Layer include:

Error Detection:

1. Parity Check: Parity check is a simple error detection technique where an extra bit (parity bit) is added to each data unit. The parity bit is set in such a way that the total number of 1s (for even parity) or 0s (for odd parity) in the data unit, including the parity bit, becomes even or odd, respectively. The receiver checks the parity bit to detect single-bit errors. However, it can only detect odd numbers of errors and is not suitable for detecting burst errors.

2. Checksum: Checksum is a more robust error detection technique commonly used in the Data Link Layer. It involves generating a checksum value based on the data being sent. The sender appends the checksum to the data before transmission. The receiver recalculates the checksum based on the received data and checks if it matches the transmitted checksum. If not, an error is detected.

Error Correction:

1. Automatic Repeat Request (ARQ): ARQ is a reactive error correction technique used in the Data Link Layer. When an error is detected, the receiver sends a negative acknowledgment (NAK) to the sender, requesting the retransmission of the corrupted frame. The sender responds by retransmitting the requested frame. This process continues until the receiver successfully receives the error-free frame and sends a positive acknowledgment (ACK) to the sender.

2. Forward Error Correction (FEC): FEC is a proactive error correction technique used to correct errors without requiring retransmissions. In FEC, redundant bits (error-correcting codes) are added to the data before transmission. The receiver uses these redundant bits to identify and correct errors in the received data. Reed-Solomon codes and Hamming codes are common examples of FEC.

3. Hybrid ARQ: Hybrid Automatic Repeat Request is a combination of ARQ and FEC. It initially uses FEC for error correction, but if errors remain after FEC, it switches to ARQ for retransmission.

4. Go-Back-N and Selective Repeat: These are specific ARQ protocols that define how multiple frames are handled during retransmission. Go-Back-N ARQ requires the retransmission of multiple frames from a damaged frame onward, while Selective Repeat ARQ only requests retransmission of the damaged frame.

The choice of error detection and correction techniques depends on factors like the communication channel's characteristics, the desired level of reliability, and the overhead considerations. Implementing effective error detection and correction mechanisms in the Data Link Layer ensures data integrity and helps maintain efficient and reliable data transmission over communication links.

Data Link Layer Protocols:

The Data Link Layer in the OSI model is responsible for reliable data transmission over a

communication link between directly connected devices. It includes several protocols that govern how data is framed, addressed, transmitted, and error-checked. Some of the commonly used Data Link Layer protocols are:

1. Ethernet: Ethernet is one of the most widely used Data Link Layer protocols in wired local area networks (LANs). It defines the framing format, MAC addressing, and CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism for access control in shared media Ethernet networks.

2. IEEE 802.11 (Wi-Fi): The IEEE 802.11 protocol family, commonly known as Wi-Fi, is used for wireless LANs. It defines the MAC layer protocol for wireless communication, including channel access methods like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

3. Point-to-Point Protocol (PPP): PPP is used for point-to-point links, such as dial-up connections and leased lines. It provides a standard method for encapsulating multiple network layer protocols, such as IP and IPv6, over a single serial link.

4. High-Level Data Link Control (HDLC): HDLC is a synchronous data link protocol used for communication over point-to-point and multipoint links. It provides reliable and error-checked data transmission and is widely used in telecommunications and network connections.

5. Asynchronous Transfer Mode (ATM): ATM is a cell-based switching and multiplexing technology used in wide area networks (WANs). It provides connection-oriented and connectionless data transmission and is commonly used in telecommunications and backbone networks.

6. Frame Relay: Frame Relay is a WAN protocol used for high-speed data transmission over a wide area network. It operates on permanent virtual circuits (PVCs) and provides reliable data transmission with error-checking mechanisms.

7. Token Ring: Token Ring is a LAN protocol that uses a token-passing mechanism for access control. It defines how devices access the network in a ring topology and has been largely replaced by Ethernet in modern networks.

8. Serial Line Internet Protocol (SLIP): SLIP is a simple protocol used for point-to-point serial connections, commonly used for dial-up Internet connections. It does not provide error-checking or error-correction mechanisms.

9. Point-to-Point Protocol over Ethernet (PPPoE): PPPoE is a protocol used to establish a PPP session over Ethernet connections. It is commonly used by Internet Service Providers (ISPs) for DSL (Digital Subscriber Line) connections.

These are just a few examples of Data Link Layer protocols. Different protocols are used for specific networking technologies, and their characteristics vary based on the network's requirements, transmission medium, and topology. The choice of the appropriate Data Link Layer protocol depends on the specific application and network environment.

Sliding window protocols.

Sliding window protocols are a class of data link layer protocols used for reliable and efficient data transmission over a communication channel, especially in point-to-point or point-to-multipoint links. These protocols allow multiple data frames to be in transit simultaneously, providing

improved link utilization and minimizing delays caused by waiting for acknowledgments. Sliding window protocols use a window of frames to keep track of transmitted and received data, and they employ various mechanisms for flow control and error recovery. Two popular sliding window protocols are the Go-Back-N and Selective Repeat protocols.

1. Go-Back-N (GBN) Protocol:
   - In the Go-Back-N protocol, the sender is allowed to transmit multiple frames before receiving acknowledgments. The receiver acknowledges correctly received frames using cumulative acknowledgments. If the receiver detects an error in a frame or a frame is lost, it discards all subsequent frames until the error is resolved.
   - The sender maintains a sending window of size N, which means it can have N unacknowledged frames in transit. Once the sender has sent N frames, it waits for the corresponding acknowledgments before sending more frames. If an acknowledgment for a specific frame is not received within a timeout period, the sender retransmits all the frames starting from the unacknowledged frame.

2. Selective Repeat Protocol:
   - The Selective Repeat protocol is an improvement over the Go-Back-N protocol that allows the sender to retransmit only the lost or damaged frames, rather than retransmitting all the subsequent frames. The receiver uses individual acknowledgments for each correctly received frame.
   - The sender maintains a sending window of size N, like in Go-Back-N. However, unlike Go-Back-N, when the sender receives acknowledgments, it only removes the acknowledged frames from the window and continues sending new frames. If the sender receives a negative acknowledgment (NACK) or a timeout occurs, it retransmits only the specific unacknowledged frames.

Advantages of Sliding Window Protocols:
- Sliding window protocols provide increased throughput and efficiency by allowing multiple frames to be in transit simultaneously, maximizing link utilization.
- They enable selective retransmission of lost or damaged frames, reducing unnecessary retransmissions and improving network efficiency.
- Sliding window protocols provide flow control, ensuring that the sender does not overwhelm the receiver with data.

Limitations of Sliding Window Protocols:
- Both Go-Back-N and Selective Repeat protocols require the receiver to maintain buffer space to temporarily store out-of-order frames until they can be delivered to the network layer.
- Sliding window protocols introduce additional overhead due to the need for sequence numbers, acknowledgments, and timers.

Overall, sliding window protocols are valuable tools in achieving reliable data transmission and efficient flow control in point-to-point and point-to-multipoint communication links. The choice between Go-Back-N and Selective Repeat depends on the specific requirements and characteristics of the network environment.