MODULE 2

FUNCTION OF THE PHYSICAL LAYER

The Physical Layer is the lowest and most fundamental layer of the OSI (Open Systems Interconnection) model in computer networking. Its primary function is to deal with the physical medium and the transmission of raw binary data over it. This layer is responsible for the following key aspects of network communication:

1. Physical Media: The Physical Layer defines the characteristics of the physical medium used to transmit data. This includes aspects such as the type of cable (e.g., copper, fiber-optic), connectors, and the transmission medium's characteristics (e.g., voltage levels, frequencies). It specifies how data bits are converted into electrical, optical, or radio signals for transmission.

2. Data Encoding and Signaling: It determines how data is encoded into binary signals (0s and 1s) and transmitted over the medium. This includes modulation techniques for analog transmission (e.g., amplitude modulation, frequency modulation) and line coding for digital transmission (e.g., NRZ, Manchester encoding).

3. Data Transmission Rate: The Physical Layer defines the data transmission rate or bandwidth, which is the maximum amount of data that can be transmitted over the medium in a given period. It sets the limits for the speed of data transfer, measured in bits per second (bps) or other units like megabits per second (Mbps) or gigabits per second (Gbps).

4. Physical Topology: It deals with the physical topology of the network, which refers to the arrangement of devices and cables in a network. This includes the layout of cables, connectors, and devices like switches, hubs, and routers.

5. Transmission Modes: The Physical Layer defines transmission modes, such as simplex (one-way communication), half-duplex (two-way communication, but not simultaneously), and full-duplex (two-way communication simultaneously).

6. Signal Quality and Error Handling: It manages signal quality and may include error detection and correction mechanisms to ensure reliable data transmission over the physical medium. Techniques like parity bits and checksums are used for error detection and correction.

7. Physical Addressing: In some cases, the Physical Layer may also include physical addressing schemes, which are used to uniquely identify devices on the network at the hardware level, such as MAC (Media Access Control) addresses in Ethernet.

The Physical Layer of a network is responsible for managing the physical aspects of data transmission. It involves several key components and concepts that are essential for the successful transmission of data over a network medium. Here are the key components involved in the Physical Layer:

COMPONENTS OF THE PHYSICAL LAYER

1. Medium: The medium refers to the physical material or channel through which data is transmitted. It can be one of several types, including:

- Copper Cables: Such as twisted-pair (e.g., Ethernet cables) and coaxial cables (e.g., cable television).

- Fiber-Optic Cables: Transmit data using light signals, offering high bandwidth and long-distance capabilities.

- Wireless: Radio waves or microwaves, used in wireless communication technologies like Wi-Fi, Bluetooth, and cellular networks.

- Satellite: Signals transmitted via communication satellites in geostationary or low Earth orbit for long-distance communication.

2. Connectors and Interfaces: These components are used to physically connect devices to the network medium. Examples include Ethernet RJ-45 connectors, optical fiber connectors, and wireless antenna connectors.

3. Transmitters and Receivers: Transmitters convert digital data into analog or digital signals suitable for transmission over the chosen medium. Receivers, on the other hand, receive and convert these signals back into digital data. These components are crucial for modulation and demodulation in analog transmission and encoding/decoding in digital transmission.

4. Signal Encoding: Signal encoding is the process of converting digital data into electrical, optical, or radio signals that can be transmitted over the medium. It includes techniques like modulation (for analog signals) and line coding (for digital signals).

5. Data Rate or Bandwidth: The Physical Layer defines the data rate or bandwidth, which is the maximum rate at which data can be transmitted over the medium. It is typically measured in bits per second (bps), and it sets the upper limit on the network's transmission speed.

6. Physical Topology: The physical topology of a network describes how devices are physically connected to each other and to the medium. Common topologies include bus, star, ring, and mesh configurations.

7. Transmission Modes: Transmission modes define how data is transmitted between devices. The common modes are:

- Simplex: One-way communication from sender to receiver.
- Half-Duplex: Two-way communication, but only one device can transmit at a time.
- Full-Duplex: Two-way communication where both devices can transmit simultaneously.

8. Signal Quality and Attenuation: The Physical Layer addresses signal quality, ensuring that the signal strength is maintained over the transmission medium and minimizing signal degradation due to attenuation (loss of signal strength over distance).

9. Error Detection and Correction: Some Physical Layer protocols include error detection and correction mechanisms to ensure the integrity of transmitted data. For example, Ethernet uses a frame check sequence (FCS) for error detection.

10. Physical Addressing: In some network technologies like Ethernet, physical addressing is used to uniquely identify devices on the network at the hardware level. MAC (Media Access Control) addresses are an example of physical addresses.

11. Multiplexing: Multiplexing techniques are employed to allow multiple signals to share the same medium efficiently. Examples include time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

12. Transmission Power and Range: In wireless networks, the Physical Layer deals with issues related to transmission power, range, and signal propagation characteristics.

These key components work together to ensure that data can be transmitted reliably and efficiently over the network's physical medium, regardless of whether it's a wired or wireless communication system. The Physical Layer is fundamental to all network communication, serving as the foundation upon which higher-level protocols and layers operate.

ROLE OF TRANSMISSION MEDIA IN PHYSICAL LAYER

Transmission media play a crucial role in the Physical Layer of a network by providing the physical pathway through which data is transmitted from one device to another. They define the characteristics of the medium and affect factors like data transmission speed, distance, and reliability. There are various types of transmission media, each with its own advantages and limitations. Here are examples of different types of transmission media:

1. Twisted-Pair Cable:

- Description: Twisted-pair cables consist of pairs of insulated copper wires twisted together. They are the most common type of cabling used in local area networks (LANs).

- Examples:

  - Unshielded Twisted Pair (UTP): Used in Ethernet networks (e.g., Cat 5e, Cat 6, Cat 7 cables).

  - Shielded Twisted Pair (STP): Offers better noise resistance and is used in environments with higher interference.

2. Coaxial Cable:

- Description: Coaxial cables consist of a central conductor, an insulating layer, a metallic shield, and an outer insulating layer. They are known for their high bandwidth and are used in cable television and broadband internet connections.

- Examples:

  - RG-6 and RG-59: Common types used for cable TV and satellite connections.

  - 10BASE2 and 10BASE5: Older Ethernet standards that used coaxial cables.

3. Fiber-Optic Cable:

- Description: Fiber-optic cables transmit data using pulses of light through thin strands of glass or plastic fibers. They offer high bandwidth, long-distance transmission, and immunity to electromagnetic interference.

- Examples:

  - Single-mode fiber (SMF): Used for long-distance connections, such as in telecommunications and internet backbone networks.

  - Multi-mode fiber (MMF): Commonly used in shorter-distance applications like building-to-building connections in data centers.

4. Wireless Transmission:

- Description: Wireless transmission media use electromagnetic waves to carry data through the air. They provide mobility and flexibility in network connections.

- Examples:

  - Radio Waves: Used in Wi-Fi (802.11) networks, Bluetooth, and some cellular communication.

  - Microwaves: Used for point-to-point long-distance connections, such as in microwave relay systems.

  - Infrared (IR): Used in some remote controls and short-range data transmission.

5. Satellite Communication:

- Description: Satellites in geostationary or low Earth orbit are used as transmission media for long-distance communication. Signals are transmitted to and from satellites in space.

- Examples:

  - Geostationary Satellites: Used for television broadcasting, global positioning systems (GPS), and satellite internet.

- Low Earth Orbit (LEO) Satellites: Used for satellite phone services like Iridium and Starlink.

6. Power Line Communication (PLC):

- Description: PLC uses existing electrical power lines to transmit data signals. It is often used for home networking and smart grid applications.

- Examples: HomePlug AV and IEEE P1901 standards for power line communication.

7. Underwater Fiber-Optic Cables:

- Description: Specialized fiber-optic cables designed for underwater applications, such as underwater research, offshore oil and gas exploration, and telecommunications between continents.

The choice of transmission medium depends on various factors, including data transmission speed, distance, cost, and environmental conditions. Each type of medium has its own advantages and trade-offs, and network designers select the most suitable medium based on the specific requirements of the network and its intended use cases.

MODULATION TECHNIQUE IN THE PHYSICAL LAYER

Encoding and modulation techniques are fundamental processes in the Physical Layer of computer networking that facilitate the conversion of digital data into analog or digital signals for transmission over a physical medium. These techniques are crucial for ensuring that data can be transmitted reliably and efficiently. Here's a summary of encoding and modulation techniques, along with examples:

1. Encoding Techniques:

- Digital Encoding: In digital transmission, data is represented directly as binary digits (0s and 1s). There are different methods for encoding digital data, including:

- Non-Return-to-Zero (NRZ): In NRZ, a high voltage represents one bit (e.g., +5V), and a low voltage represents the other bit (e.g., 0V). For example, +5V for '1' and 0V for '0'.

- Manchester Encoding: In Manchester encoding, each bit is represented by a transition in the middle of the bit period. A rising transition represents '0' and a falling transition represents '1'.

- Differential Manchester Encoding: Similar to Manchester encoding, but the transition in the middle represents '1' and no transition represents '0'.

- Analog Encoding: In analog transmission, digital data is converted into analog signals. Common analog encoding methods include:

- Amplitude Modulation (AM): In AM, the amplitude of a carrier wave is varied based on the digital data. For example, a high amplitude represents '1,' and a low amplitude represents '0.'

- Frequency Modulation (FM): In FM, the frequency of the carrier wave is varied to represent digital data.

- Phase Modulation (PM): PM varies the phase of the carrier wave based on digital data.

2. Modulation Techniques:

- Amplitude Modulation (AM): In AM modulation, the amplitude of a carrier wave is varied according to the digital signal. For instance, in AM radio broadcasting, the strength of the carrier wave is modified to carry audio signals. A stronger signal represents a '1,' and a weaker signal represents a '0.'

- Frequency Modulation (FM): FM modulation involves changing the frequency of a carrier wave based on the digital signal. It's commonly used in FM radio broadcasting, where different frequencies represent different audio signals or data.

- Phase Modulation (PM): PM modulates the phase of the carrier wave to encode digital data. Changes in phase represent digital bits. PSK (Phase Shift Keying) is a common form of phase modulation.

FREQUENCY MODULATION IN DETAIL

Frequency Modulation (FM) is a modulation technique used in telecommunications and broadcasting to transmit information, such as audio signals or data, by varying the frequency of a carrier wave in proportion to the instantaneous amplitude of the signal being sent. FM is primarily used in applications where signal quality and resistance to amplitude noise or interference are critical, such as in FM radio broadcasting and some forms of wireless communication. Here's a detailed explanation of FM:

1. Carrier Wave: FM begins with a carrier wave, which is a high-frequency, continuous sinusoidal waveform. This carrier wave is used to carry the information or signal.

2. Modulating Signal: The information to be transmitted, referred to as the modulating signal, is typically an analog signal, such as an audio waveform from a microphone, musical instrument, or other sources. This signal contains the information you want to convey, such as music, speech, or data.

3. Frequency Deviation: In FM, the frequency of the carrier wave is varied in response to the instantaneous amplitude of the modulating signal. This variation is known as frequency deviation. When the modulating signal's amplitude is high, the frequency deviation is large, and when the amplitude is low, the frequency deviation is small.

4. Interpretation at the Receiver: At the receiver end, the incoming FM signal is demodulated to extract the original modulating signal. This involves reversing the frequency modulation process to obtain the original information signal.

5. Advantages of FM:

- Resistance to Amplitude Noise: FM is less susceptible to amplitude noise and interference compared to amplitude modulation (AM). This makes it suitable for high-fidelity audio transmission.

- Wide Frequency Range: FM signals can carry audio, video, and data over a wide frequency range, making it versatile for various applications.

- Good Signal Quality: FM provides excellent signal quality, making it ideal for applications where audio fidelity is crucial, such as FM radio broadcasting.

6. Applications:

- FM Radio Broadcasting: FM is widely used for radio broadcasting, providing high-quality audio transmission.

- Wireless Communication: Some wireless communication systems, including analog and digital radio communication, use FM modulation.

- Frequency Modulated Continuous Wave (FMCW) Radar: FMCW radar systems use FM techniques to measure distances and velocities, commonly used in automotive radar and weather radar.

DIFFERENCE BETWEEN HUB AND REPEATER

Hubs and repeaters are both networking devices used at the Physical Layer of a network, but they serve different purposes and have distinct characteristics. They are primarily used to extend the reach of a network, but they do so in different ways. Here's a differentiation between hubs and repeaters and how they extend network reach:

Hub:

1. Function:

- A hub is a basic networking device that operates at the Physical Layer (Layer 1) of the OSI model.

- Its primary function is to connect multiple network devices in a shared network segment, such as a local area network (LAN).

2. Operation:

- A hub operates as a multi-port, broadcast device. When it receives data on one of its ports, it broadcasts that data to all other ports, regardless of the destination.

- It doesn't have any intelligence to determine the source or destination of the data.

3. Extending Network Reach:

- Hubs do not extend the reach of a network in the traditional sense. Instead, they act as signal repeaters within a single network segment.

- Data sent to a hub is simply rebroadcast to all devices within the same network segment, which can lead to network congestion and inefficient use of bandwidth.

4. Limitations:

- Hubs are not suitable for larger or more complex networks because they do not segment or filter traffic, leading to network collisions and reduced performance as the number of connected devices increases.

Repeater:

1. Function:

- A repeater is a networking device designed to amplify and retransmit signals to extend the reach of a network.

- It operates at the Physical Layer and is used to overcome signal degradation over long distances.

2. Operation:

- A repeater receives signals from one network segment, amplifies them to boost their strength, and then retransmits them to another network segment.

- Repeaters are typically used to connect two network segments and ensure that data can travel farther without significant signal loss.

3. Extending Network Reach:

- Repeaters extend the reach of a network by regenerating and amplifying signals, allowing data to traverse longer distances without becoming too weak or distorted.

- They are especially useful in situations where the distance between network segments exceeds the limitations of the network's original signaling capabilities.

4. Limitations:

- Repeaters are relatively simple devices and do not have the intelligence to filter or segment traffic. They simply amplify and repeat signals.

- They cannot address issues related to network congestion or collisions.

ETHERNET PROTOCOL IN PHYSICAL LAYER

Ethernet is a fundamental and widely used protocol at the Physical Layer (Layer 1) and the Data Link Layer (Layer 2) of the OSI model in computer networking. It plays a pivotal role in wired networks, such as local area networks (LANs), by defining the rules and standards for transmitting data over various types of wired transmission media.

Here's the significance of the Ethernet protocol in the Physical Layer and how it handles data transmission in wired networks:

1. Standardization and Interoperability:

- Ethernet provides a standardized framework for transmitting data over various physical media, including twisted-pair copper cables, fiber-optic cables, and coaxial cables. This standardization ensures that devices from different manufacturers can communicate and interoperate seamlessly within Ethernet networks.

2. Media Access Control (MAC) Addressing:

- Ethernet uses MAC addressing at the Data Link Layer (Layer 2) to uniquely identify network devices at the hardware level. MAC addresses are crucial for directing data packets to their intended destinations within a LAN.

3. Data Framing:

- Ethernet frames data into packets that can be transmitted over the network. These frames contain source and destination MAC addresses, as well as other control and error-checking information.

4. Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

- In traditional Ethernet, such as 10BASE-T (Ethernet over twisted-pair cables), CSMA/CD is used to manage access to the shared network medium. Devices listen for a clear channel before transmitting data. If a collision is detected (i.e., two devices transmit simultaneously), they wait for a random backoff period before retransmitting.

5. Ethernet Speeds and Types:

- Ethernet supports various speeds, including 10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), 10 Gbps (10 Gigabit Ethernet), 40 Gbps, and 100 Gbps, to accommodate different network requirements.

- Ethernet has evolved over the years to support different types of physical media, including twisted-pair (e.g., Ethernet over CAT5e, CAT6), fiber-optic (e.g., Ethernet over single-mode and multi-mode fibers), and copper coaxial cables.

6. Switching and Segmentation:

- Ethernet switches, operating at the Data Link Layer, use MAC addresses to intelligently forward data frames only to the devices that need them, reducing network collisions and improving overall network efficiency.

- This segmentation of the network into smaller collision domains allows Ethernet to scale effectively for larger LANs and support higher data transfer rates.

7. Reliability and Error Handling:

- Ethernet includes error-checking mechanisms like Frame Check Sequence (FCS) to ensure data integrity. Frames with errors are discarded and, if necessary, retransmitted.

IMPORTANCE OF DATA FRAMING IN THE PHYSICAL LAYER

Data framing, within the context of data transmission at the Physical Layer, refers to the process of organizing and structuring raw data into manageable packets or frames before it is transmitted over a network medium. This structuring is crucial for several reasons:

1. Data Segmentation: Data framing divides a continuous stream of data into discrete, manageable chunks or frames. These frames have headers and, in some cases, trailers that provide information about the frame itself. This segmentation makes it easier to transmit and receive data in smaller, more organized units.

2. Addressing and Routing: Frames often include information like source and destination addresses, which are essential for routing data to its intended recipient. By including this addressing information, data can be directed to the appropriate destination within a network.

3. Error Detection and Correction: Data framing allows for the inclusion of error-checking mechanisms like Frame Check Sequence (FCS). These mechanisms help detect and sometimes correct errors that may occur during transmission, ensuring data integrity.

4. Flow Control: Framing can also include control information for managing the flow of data between sender and receiver. This helps prevent data overload and congestion on the network.

5. Protocol Compatibility: Data framing adheres to specific standards and protocols, ensuring that different devices and systems can understand and interpret the structured data. This compatibility is vital for the interoperability of devices from different manufacturers.

DATALINK LAYER

Switches and bridges both operate at the Data Link Layer (Layer 2) of the OSI model and serve similar functions in network communication, but there are differences in their capabilities and scale. Here's an outline of the functions of switches at the Data Link Layer and how they differ from bridges, along with examples of their usage in a network:

Switches at the Data Link Layer:

1. MAC Address Learning: Switches maintain a MAC address table, also known as a MAC address forwarding table. They learn the MAC addresses of devices connected to their ports by examining the source MAC address of incoming frames.

2. Frame Forwarding: When a frame arrives at a switch, it uses the MAC address table to determine which port to forward the frame to based on the destination MAC address. This allows switches to send frames only to the port where the destination device is located, reducing network congestion.

3. Broadcast Handling: Switches do not forward broadcast frames (destined for all devices on the network) to all ports. Instead, they forward broadcast frames to all ports except the one on which they were received.

4. Collision Domains: Switches create individual collision domains for each port, which means that devices connected to different switch ports can transmit simultaneously without causing collisions.

5. Segmentation: Switches segment a network into multiple collision domains, improving network efficiency and reducing collisions compared to hubs or bridges.

6. VLAN Support: Many switches support Virtual LANs (VLANs), which allow network administrators to logically segment a single physical switch into multiple isolated virtual networks.

7. High Port Density: Switches come in various port configurations, from small switches with a few ports to large switches with dozens or even hundreds of ports, making them suitable for networks of various sizes.

Bridges at the Data Link Layer:

1. MAC Address Filtering: Bridges filter and forward frames based on MAC addresses, just like switches. However, bridges generally have fewer ports and simpler forwarding capabilities compared to switches.

2. Segmentation: Like switches, bridges segment a network into multiple collision domains, reducing network collisions and improving network performance. However, they are typically used in smaller-scale networks.

3. Legacy Devices: Bridges are sometimes used in older or simpler network configurations where the network does not require the advanced features of modern switches.

Differences:

- Scale: Switches are designed for larger networks and come with more ports and advanced features, making them suitable for modern, complex LANs. Bridges are typically used in smaller networks or in legacy setups.

- Functionality: Switches are more advanced and can perform additional tasks like VLAN support, QoS (Quality of Service) management, and more granular control over traffic. Bridges are simpler and have fewer features.

Examples of Usage:

- Switches: Switches are used in various scenarios, including corporate LANs, data centers, and carrier networks. For example, they are used to interconnect computers, servers, and other networked devices within a large office building.

- Bridges: Bridges are less commonly used today but can still be found in legacy or simpler network configurations. For example, a bridge might be used to connect two separate LANs in a small office or to extend a network over a short distance.

OPERATION OF BRIDGES IN COMPUTER NETWORKS

Learning bridges, also known as learning switches or MAC bridges, are networking devices designed to operate at the Data Link Layer (Layer 2) of the OSI model. They play a critical role in Ethernet-based computer networks by efficiently managing network traffic and preventing network loops. Here's a description of the purpose and operation of learning bridges in computer networks:

Purpose of Learning Bridges:

The primary purpose of learning bridges is to improve the efficiency and reliability of Ethernet networks by:

1. Reducing Collision Domains: Learning bridges segment a network into multiple collision domains. Each port on a learning bridge creates a separate collision domain, allowing devices connected to different ports to transmit data simultaneously without causing collisions.

2. Filtering Traffic: Learning bridges filter network traffic by forwarding frames only to the port where the destination device is located, reducing unnecessary traffic on other segments of the network. This filtering is based on the MAC (Media Access Control) addresses of devices.

3. Preventing Network Loops: One of the key functions of learning bridges is to prevent network loops, which can cause broadcast storms and severely degrade network performance. By maintaining a MAC address table and intelligently forwarding frames, learning bridges ensure that frames do not endlessly circulate within a network.

Operation of Learning Bridges:

Learning bridges operate using the following mechanisms:

1. MAC Address Learning: Learning bridges maintain a MAC address table (also called a forwarding table or CAM table) that associates MAC addresses with specific switch ports. When a frame arrives at a port, the bridge examines the source MAC address of the frame and records it in the MAC address table, associating it with the port on which it arrived.

2. Frame Forwarding Decision: When a frame arrives at a learning bridge, the bridge uses the destination MAC address of the frame to determine which port to forward the frame to. It checks the MAC address table to find the port associated with the destination MAC address. If the port is known, the frame is forwarded only to that port.

3. Broadcast Handling: Broadcast frames (destined for all devices on the network) are broadcast to all ports except the one on which they were received. This prevents broadcast storms from occurring by limiting the broadcast domain to a single collision domain.

4. Address Aging: To ensure that the MAC address table remains up-to-date, learning bridges implement address aging. Entries in the table have a limited lifetime, typically in the range of 300 to 1,000 seconds. If a device does not communicate within this timeframe, its entry is removed from the table.

5. Dynamic Updating: The MAC address table is dynamically updated as devices communicate on the network. As devices join the network and send frames, the bridge learns their MAC addresses and associates them with the corresponding ports.

Spanning tree Bridge

The Spanning Tree Bridge algorithm, often simply referred to as the Spanning Tree Protocol (STP) or IEEE 802.1D, is a network protocol that plays a crucial role in ensuring the stability and reliability of Ethernet networks. Its primary

purpose is to prevent network loops and create a loop-free topology in bridged or switched networks. Here's an explanation of the Spanning Tree Bridge algorithm and why it is essential in network communication:

Spanning Tree Bridge Algorithm:

The Spanning Tree Bridge algorithm operates at the Data Link Layer (Layer 2) of the OSI model and is used in Ethernet networks with bridges or switches. Its key objectives are:

1. Loop Prevention: The primary function of the Spanning Tree Protocol is to detect and prevent network loops, which can occur when there are redundant network paths in a bridged or switched network.

2. Loop-Free Topology: The algorithm aims to create a loop-free logical topology within a network. This means that even though there may be physical redundancy (multiple paths between switches or bridges), only one path is designated as active, while others are blocked to prevent loops.

3. Failover and Redundancy: While STP blocks some paths to prevent loops, it also ensures that alternate paths can be activated in case of network failures. This failover mechanism allows for network redundancy and improved network reliability.

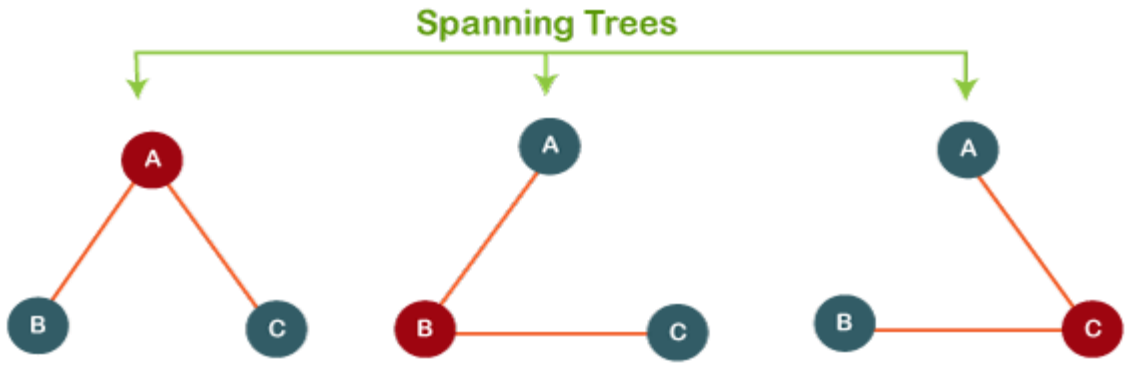

Fig 2.0

1. A is directly connected to B and C, while B and C are indirectly connected through A. In this spanning tree, A is a central point and all the points are connected without any formation of loops.
2. B is directly connected to A and C, while A and C are connected through B. B is a bridge between A and C, or we can say that B is a central point. In this case, also, all the points are connected without any formation of loops.
3. C is directly connected to both A and B, while A and B are connected through C. Therefore, C is a bridge between A and B, and C is a central point. In this case, all the points are connected without any formation of loops.

Till now, we have observed two basic features of spanning-tree:

- ✓ It does not contain any loop.
- ✓ It is minimally connected.

OPERATION OF THE SPANNING TREE BRIDGE ALGORITHM:

The operation of the Spanning Tree Bridge algorithm involves the following steps:

1. Bridge Election: In a network with multiple bridges or switches, one of them is elected as the root bridge. The root bridge becomes the reference point for the rest of the network and is used as a basis for determining the designated and non-designated ports on other bridges.

2. Path Cost Calculation: Each bridge calculates the cost of the path from itself to the root bridge. This cost is based on the number of hops (bridges or switches) between them. Bridges use Bridge Protocol Data Units (BPDUs) to exchange information about path costs.

3. Port State Transitions: Based on the path cost calculations, each bridge determines the state of its ports. Ports can be in one of the following states:

- Blocking: Ports that are in blocking state do not forward data frames but are listening to BPDUs to monitor the network topology.

- Listening: Ports in listening state are preparing to transition to the forwarding state. They still do not forward data frames.

- Learning: Ports in learning state are transitioning to the forwarding state. They start learning MAC addresses but still do not forward data frames.

- Forwarding: Ports in forwarding state are actively forwarding data frames.

4. Loop-Free Topology: The algorithm ensures that only one path (the best path) to the root bridge is designated as forwarding, while other paths are placed in a blocking state. This loop-free topology is crucial in preventing network loops.

Importance in Network Communication:

The Spanning Tree Bridge algorithm is essential in network communication for several reasons:

1. Loop Prevention: It prevents network loops, which can lead to broadcast storms and severe network congestion. Without STP, loops can render a network unusable.

2. Network Stability: By creating a loop-free topology and managing redundant paths, STP ensures network stability and prevents unpredictable network behavior.

3. Redundancy and Failover: STP allows for network redundancy and rapid failover. If a link or switch fails, the protocol can quickly activate an alternative path to maintain network connectivity.

4. Efficient Use of Resources: The algorithm optimizes network resource utilization by selecting the best path while blocking redundant paths that are not needed for normal traffic.

HUBS, BRIDGES, SWITCHES, ROUTERS, AND GATEWAYS

Repeater, Hub, Bridge, Switch, Router, and Gateway are all networking devices that play distinct roles within a network. Here's a comparison and contrast of their functionalities:

1. Repeater:

- Functionality: Repeats or regenerates incoming signals to extend the reach of a network. It operates at the Physical Layer.

- Use Case: Used to overcome signal degradation over long distances in wired or wireless networks.

- Intelligence: Minimal to no intelligence; operates at the physical layer without knowledge of data.

- Broadcast Handling: Broadcasts and forwards all incoming signals.

2. Hub:

- Functionality: Connects multiple network devices in a shared network segment. It operates at the Physical Layer.

- Use Case: Rarely used today due to their inefficiency. Mostly seen in legacy networks.

- Intelligence: Minimal intelligence; simply broadcasts incoming data to all connected devices.

- Broadcast Handling: Broadcasts all incoming data to all connected devices.

3. Bridge:

- Functionality: Segments a network into multiple collision domains and filters traffic based on MAC addresses. It operates at the Data Link Layer.

- Use Case: Used to reduce collisions in Ethernet networks and improve network efficiency.

- Intelligence: Moderate intelligence; maintains a MAC address table for filtering.

- Broadcast Handling: Broadcasts are forwarded to all ports except the one on which they were received.

4. Switch:

- Functionality: Similar to a bridge but with higher port density and advanced features. Segments networks, filters traffic, and forwards frames based on MAC addresses. It operates at the Data Link Layer.

- Use Case: Used extensively in modern LANs for efficient and scalable network communication.

- Intelligence: High intelligence; maintains a MAC address table and can perform VLANs, QoS, and more.

- Broadcast Handling: Broadcasts are forwarded only to ports where the destination device is located.

5. Router:

- Functionality: Connects multiple networks, routes data between them based on IP addresses, and makes routing decisions based on network layer information (Layer 3). Operates at the Network Layer.

- Use Case: Used to connect different networks (e.g., LAN to WAN) and direct traffic between them.

- Intelligence: High intelligence; understands IP addresses and can perform routing, NAT, and firewall functions.

- Broadcast Handling: Does not forward broadcasts by default, isolating broadcast domains.

6. Gateway:

- Functionality: Translates data between different network protocols or architectures. It operates at various layers, depending on the specific gateway type.

- Use Case: Used for interoperability between different networks with different protocols or technologies.

- Intelligence: High intelligence; translates and manages data between disparate networks.

- Broadcast Handling: Depends on the specific gateway type and its role in the network.

MAC ADDRESS PROCESS

Switches make forwarding decisions based on MAC (Media Access Control) addresses, and this process plays a crucial role in enhancing network performance by efficiently directing network traffic to its intended destination. Here's an explanation of how switches make forwarding decisions based on MAC addresses and how it improves network performance:

1. Learning MAC Addresses:

- When a switch is powered on or when a new device is connected to one of its ports, the switch begins the process of MAC address learning.

- The switch examines the source MAC addresses of incoming Ethernet frames. Each frame contains a source MAC address in its header, which identifies the device that sent the frame.

- The switch associates the source MAC address with the port on which it received the frame and adds this information to its MAC address table, also known as a MAC address forwarding table. The table keeps track of which MAC addresses are reachable through which switch ports.

2. MAC Address Table:

- The MAC address table is a critical component of a switch's operation. It maps MAC addresses to specific switch ports.

- As the switch learns MAC addresses, it updates the table. Over time, the table becomes a database of MAC addresses and their corresponding ports.

3. Forwarding Decision:

- When a frame arrives at a switch, the switch examines the destination MAC address in the frame's header.

- It checks its MAC address table to determine if it knows which port is associated with the destination MAC address.

- If the destination MAC address is found in the table, the switch forwards the frame only to the port where the destination device is located. This is known as unicast forwarding.

- If the destination MAC address is not found in the table (indicating that the device is not yet known to the switch), the switch broadcasts the frame to all its ports (except the port on which it was received). This is known as broadcast forwarding.

How Switches Enhance Network Performance:

1. Efficient Traffic Handling: By forwarding frames based on MAC addresses, switches ensure that data is sent only to the specific port where the destination device resides. This eliminates unnecessary traffic on the network, reducing congestion and improving network efficiency.

2. Collision Domain Segmentation: Switches segment the network into multiple collision domains, meaning that devices on different switch ports can transmit simultaneously without causing collisions. This segmentation improves the overall network performance.

3. Reduced Broadcast Domain: Switches significantly reduce the size of broadcast domains. Broadcast frames are only sent to ports where the destination device is unknown, limiting the scope of broadcast traffic.

4. Faster Data Delivery: Switches make forwarding decisions in hardware, which is much faster than the software-based decisions made by bridges or routers. This results in faster data delivery and lower latency.

5. Improved Scalability: Switches can handle a large number of connected devices and efficiently manage traffic, making them suitable for networks of various sizes.

6. Enhanced Security: By forwarding frames based on MAC addresses, switches provide a level of security by not broadcasting data to all devices on the network. This isolation helps in network segmentation and access control

WHAT IS CHECKSUM?

The checksum is a network method to check for any error or damage to the data transmitted to the sender side from the sender side. The checksum method applies the bit addition and bit complement method to perform the checksum implementation.

Working Steps for Checksum

Steps involved in the checksum error-detection method:

Step 1: At the Sender Side,

Divide the original data into the ‘m’ number of blocks with ‘n’ data bits in each block.

Adding all the ‘k’ data blocks.

The addition result is complemented using 1’s complement.

The obtained data is known as the Checksum.

Step 2: Data Transmission

Integrate the checksum value to the original data bit.

Begin the transmission of data to the receiver side.

Step 3: At the Receiver Side,

Divide the received data into the ‘k’ number of blocks.

Adding all the ‘k’ data blocks along with the checksum value.

The addition result is complemented using 1’s complement.

Two possible cases after 1’s complement:

Case 1: If the result is 0.

No errors in the received data from the sender side.

The receiver accepts the data.

Case 2: If the result is not 0.

Errors in the received data from the sender side.

The receiver discards the data and requests for retransmission of data.

Solved Example

Let’s use an example to implement the checksum method and consolidate our understanding of the network principle.

For the given data value 11001100 10101010 11110000 11000011, perform the checksum method.

1. The first step is to perform the bit addition of the given data bits at the sender side.

Sender Side:

1	0	0	1	1	0	0	1
1	1	1	0	0	0	1	0
0	0	1	0	0	1	0	0
1	0	0	0	0	1	0	0
0	0	1	0	0	0	1	1
						1	**0**
0	0	1	0	0	1	0	1

Note: The extra carry bits are added to the summation result.

2. Perform the 1's Complement for the bit addition result, thus obtaining the checksum value.

Sender Side:

0	0	1	0	0	1	0	1

1's Complement

Checksum	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**0**

3. Integrate the checksum value and the original data bit and begin the data transmission to the receiver.

11011010	10011001	11100010	00100100	10000100

4. The receiver side will begin the Checksum Checker method, repeat the bit addition, and perform the 1's complement.

Receiver Side:

1	0	0	1	1	0	0	1
1	1	1	0	0	0	1	0
0	0	1	0	0	1	0	0
1	0	0	0	0	1	0	0
1	**1**	**0**	**1**	**1**	**0**	**1**	**0**
1	1	1	1	1	1	0	1
						1	**0**
1	1	1	1	1	1	1	1

5. If the complement result is 0, the data received is correct and without any error.

Receiver Side:

1	1	1	1	1	1	1	1

1's Complement

Checksum	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Result: No error in the data received from the sender side.

Gain experience via a remote internship opportunity and obtain an internship certificate by choosing our unique Advanced Executive Program in Cybersecurity. Grab your seat now and enhance your resume in just 6 months. Contact our team today!

STRATEGIES USED TO ACHIEVE ERROR CORRECTION IN DATALINK LAYER.

Error correction, in the context of the Data Link Layer (Layer 2) of the OSI model, refers to the process of detecting and correcting errors that may occur during the transmission of data over a network. The Data Link Layer plays a crucial role in ensuring the reliability of data transfer between directly connected devices. Error correction strategies aim to identify and rectify errors, improving the integrity of transmitted data. Here are some strategies used to achieve error correction in networks:

1. Automatic Repeat reQuest (ARQ):

- ARQ is a common error correction technique where the sender retransmits data frames that are suspected to be corrupted or lost during transmission.

- The recipient detects errors using techniques like checksums or cyclic redundancy checks (CRCs) and requests retransmission of the corrupted frames.

- Popular variations of ARQ include Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ.

2. Forward Error Correction (FEC):

- FEC is a proactive error correction method that involves adding extra redundant data (error-correcting codes) to the transmitted message.

- These codes are designed in such a way that the recipient can use them to detect and correct errors without the need for retransmission requests.

- Examples of FEC codes include Reed-Solomon codes and Hamming codes.

3. Automatic Repeat reQuest with Forward Error Correction (ARQ-FEC):

- This approach combines ARQ and FEC techniques to enhance error correction capabilities.

- The sender adds FEC information to the data before transmission, and if errors are detected at the receiver, it requests retransmission of only the corrupted parts using ARQ.

4. Hybrid Error Correction:

- Some networks use a combination of error correction methods to achieve higher reliability.

- For instance, a network might employ FEC for moderate error correction and ARQ for handling more severe errors.

5. Retransmission Strategies:

- ARQ-based methods often involve different retransmission strategies, including:

  - Selective Retransmission: Only the frames with errors are retransmitted.

  - Go-Back-N: If any frame is found to have errors, all subsequent frames are retransmitted.

  - Selective Repeat: Only the frames with errors are retransmitted, but out-of-sequence frames are also retained and acknowledged.

6. Timeouts and Acknowledgments:

- ARQ mechanisms rely on timeouts and acknowledgments (ACKs) to manage retransmissions.

- The sender sets a timeout for receiving an acknowledgment from the receiver. If an ACK is not received within the specified time, the sender assumes that the frame was lost or corrupted and retransmits it.

7. Flow Control:

- Flow control mechanisms at the Data Link Layer, such as sliding window protocols, help prevent network congestion and reduce the chances of errors due to congestion-related packet loss.

8. Quality of Service (QoS):

- In some networks, QoS mechanisms are used to prioritize certain types of data traffic, ensuring that critical data is less likely to be affected by errors or packet loss.

SLIDING WINDOW PROTOCOL

The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol).

In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocol

Sliding window protocol has two types:

1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

The size of the sender window is N in this protocol. For example, Go-Back-8, the size of the sender window, will be 8. The receiver window size is always 1.

If the receiver receives a corrupted frame, it cancels it. The receiver does not accept a corrupted frame. When the timer expires, the sender sends the correct frame again. The design of the Go-Back-N ARQ protocol is shown below.

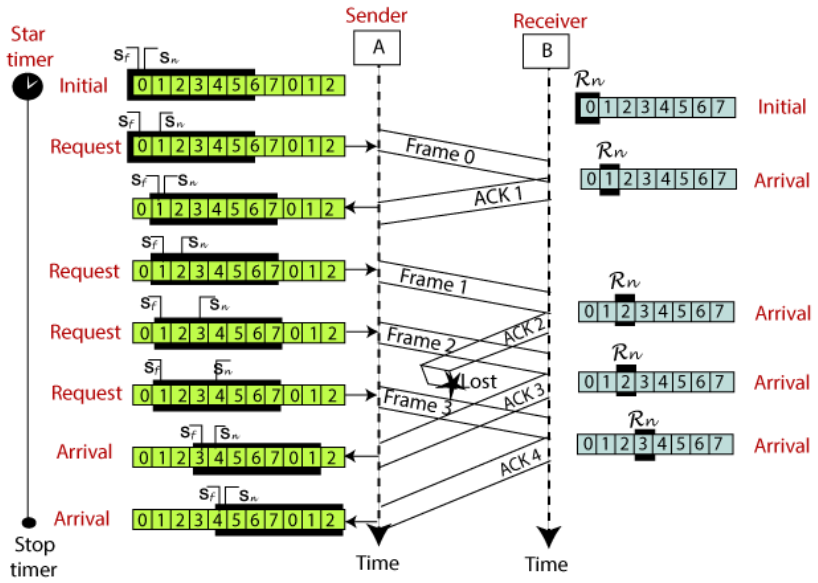

Fig 2.1 SLIDING WINDOW GO BACK N ARQ

Selective Repeat ARQ

Selective Repeat ARQ is also known as the Selective Repeat Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. The Go-back-N ARQ protocol works well if it has fewer errors. But if there is a lot of error in the frame, lots of bandwidth loss in sending the frames again. So, we use the Selective Repeat ARQ protocol. In this protocol, the size of the sender window is always equal to the size of the receiver window. The size of the sliding window is always greater than 1.

If the receiver receives a corrupt frame, it does not directly discard it. It sends a negative acknowledgment to the sender. The sender sends that frame again as soon as on the receiving negative acknowledgment. There is no waiting for any time-out to send that frame. The design of the Selective Repeat ARQ protocol is shown below.

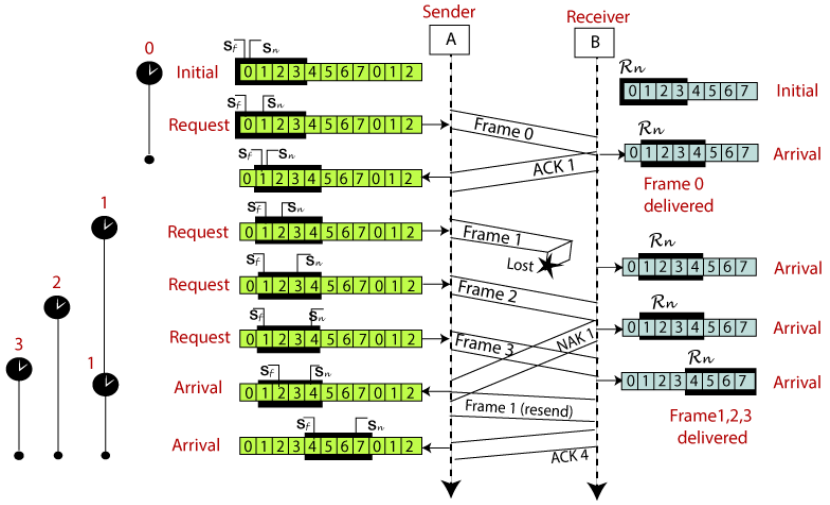

Fig 2.3 SLIDING WINDOW SELECTIVE REPEAT

Go-Back-N ARQ	Selective Repeat ARQ
If a frame is corrupted or lost in it,all subsequent frames have to be sent again.	In this, only the frame is sent again, which is corrupted or lost.
If it has a high error rate,it wastes a lot of bandwidth.	There is a loss of low bandwidth.
It is less complex.	It is more complex because it has to do sorting and searching as well. And it also requires more storage.
It does not require sorting.	In this, sorting is done to get the frames in the correct order.
It does not require searching.	The search operation is performed in it.
It is used more.	It is used less because it is more complex.

TABLE 2.0 Difference Between Go-back-ARQ and Selective Repeat

What is Stop and Wait protocol?

Here stop and wait means, whatever the data that sender wants to send, he sends the data to the receiver. After sending the data, he stops and waits until he receives the acknowledgment from the receiver. The stop and wait protocol is a flow control protocol where flow control is one of the services of the data link layer.

It is a data-link layer protocol which is used for transmitting the data over the noiseless channels. It provides unidirectional data transmission which means that either sending or receiving of data will take place at a time. It provides flow-control mechanism but does not provide any error control mechanism.

The idea behind the usage of this frame is that when the sender sends the frame then he waits for the acknowledgment before sending the next frame.

Primitives of Stop and Wait Protocol

The primitives of stop and wait protocol are:

Sender side

Rule 1: Sender sends one data packet at a time.

Rule 2: Sender sends the next packet only when it receives the acknowledgment of the previous packet.

Therefore, the idea of stop and wait protocol in the sender's side is very simple, i.e., send one packet at a time, and do not send another packet before receiving the acknowledgment.

Receiver side

Rule 1: Receive and then consume the data packet.

Rule 2: When the data packet is consumed, receiver sends the acknowledgment to the sender.

Therefore, the idea of stop and wait protocol in the receiver's side is also very simple, i.e., consume the packet, and once the packet is consumed, the acknowledgment is sent. This is known as a flow control mechanism.

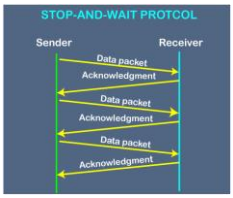

Fig 2.4.1 stop-and-wait ARQ

the above figure shows the working of the stop and wait protocol. If there is a sender and receiver, then sender sends the packet and that packet is known as a data packet. The sender will not send the second packet without receiving the acknowledgment of the first packet. The receiver sends the acknowledgment for the data packet that it has received. Once the acknowledgment is received, the sender sends the next packet. This process continues until all the packet are not sent. The main advantage of this protocol is its simplicity but it has some disadvantages also. For example, if there are 1000 data packets to be sent, then all the 1000 packets cannot be sent at a time as in Stop and Wait protocol, one packet is sent at a time.

Disadvantages of Stop and Wait protocol

The following are the problems associated with a stop and wait protocol:

1. Problems occur due to lost data

Fig 2.4.2 stop-and-wait ARQ case 1

Suppose the sender sends the data and the data is lost. The receiver is waiting for the data for a long time. Since the data is not received by the receiver, so it does not send any acknowledgment. Since the sender does not receive any acknowledgment so it will not send the next packet. This problem occurs due to the lost data.

In this case, two problems occur:

- ✓ Sender waits for an infinite amount of time for an acknowledgment.
- ✓ Receiver waits for an infinite amount of time for a data.

2. Problems occur due to lost acknowledgment

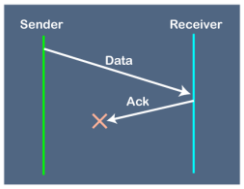

Fig 2.4.3 stop-and-wait ARQ case 2

Suppose the sender sends the data and it has also been received by the receiver. On receiving the packet, the receiver sends the acknowledgment. In this case, the acknowledgment is lost in a network, so there is no chance for the sender to receive the acknowledgment. There is also no chance for the sender to send the next packet as in stop and wait protocol, the next packet cannot be sent until the acknowledgment of the previous packet is received.

3. Problem due to the delayed data or acknowledgment

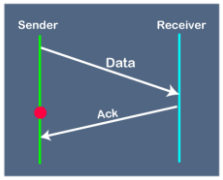

Fig 2.4.4 stop-and-wait ARQ case 3

Suppose the sender sends the data and it has also been received by the receiver. The receiver then sends the acknowledgment but the acknowledgment is received after the timeout period on the sender's side. As the acknowledgment is received late, so acknowledgment can be wrongly considered as the acknowledgment of some other data packet.

Difference

Key	Stop and Wait protocol	Go-Back-N protocol	Selective Repeat protocol
Sender window size	The Sender window size in the Stop and Wait protocol is 1.	The Sender window size in the Go-Back-N protocol is N.	The Sender window size in the Selective Repeat technique is N.
Receiver Window size	The Receiver window size in the Stop and Wait protocol is 1.	The Receiver window size in the Go-Back-N protocol is 1.	The Receiver window size in the Selective Repeat technique is N.
Minimum Sequence Number	The minimum sequence number in the Stop and Wait procedure is 2.	The Minimum Sequence Number in the Go-Back-N protocol is N+1, where N is the number of packets sent.	The Minimum Sequence Number in the Selective Repeat protocol is 2N, where N is the number ofpackets transmitted.

Efficiency	In Stop and Wait protocol, Efficiency formular is 1/(1+2*a) where a is ratio of propagation delay vs transmission delay.	In Go-Back-N protocol, Efficiency formular is N/(1+2*a) where a is ratio of propagation delay vs transmission delay and N is number of packets sent.	In Selective Repeat protocol, Efficiency formular is N/(1+2*a) where a is ratio of propagation delay vs transmission delay and N is number of packets sent.
Acknowledgement Type	In Stop and Wait protocol, Acknowledgement type is individual.	In Go-Back-N protocol, Acknowledgement type is cumulative.	In Selective Repeat protocol, Acknowledgement type is individual.
Supported Order	At the receiver end of the Stop and Wait protocol, no specific order is required.	Only in-order delivery is accepted at the receiver end of the Go-Back-N protocol.	In Selective Repeat protocol, out-of-order deliveries can also be accepted at receiver end.
Retransmissions	In Stop and Wait protocol, in case of packet drop, number of retransmission is 1.	In Go-Back-N protocol, in case of packet drop, number of retransmission is N.	In Selective Repeat protocol, in case of packet drop, number of retransmission is 1.

Role of Datalink layer

Data Link Layer protocols ensure reliable data delivery in the presence of errors and packet loss through various techniques and mechanisms. Here's a summary of how these protocols achieve this:

1. Error Detection:

- Data Link Layer protocols often use error-detection techniques like checksums and cyclic redundancy checks (CRCs) to identify errors in transmitted data frames.

- When a frame arrives at the receiver, it checks the checksum or CRC to detect any errors. If errors are detected, the frame is discarded, and an acknowledgment for the previous error-free frame is sent.

2. Acknowledgments:

- Protocols like Automatic Repeat reQuest (ARQ) and Sliding Window Protocols use acknowledgments (ACKs) to confirm the successful reception of data frames.

- If the sender does not receive an ACK within a specified time, it assumes that the frame was lost or corrupted and retransmits it.

3. Retransmission:

- In ARQ-based protocols, if a frame is not acknowledged or is acknowledged with errors, the sender retransmits the frame to ensure its successful delivery.

- The retransmission process continues until the frame is successfully received or until a maximum number of retransmission attempts is reached.

4. Sequence Numbers:

- Data frames often include sequence numbers to ensure that they are received in the correct order. If frames arrive out of order, they can be reordered at the receiver before higher-layer processing.

5. Selective Repeat:

- Some protocols, like Selective Repeat ARQ, allow the receiver to request retransmission of only the frames that have errors, reducing unnecessary retransmission of correctly received frames

6. Forward Error Correction (FEC):

- Some protocols, such as those used in wireless communication or satellite links, employ FEC codes that add redundancy to data frames. The receiver can use this redundancy to correct errors without requesting retransmission.

7. Flow Control:

- Flow control mechanisms help manage the rate of data transmission between sender and receiver. Sliding Window Protocols are an example, where the sender waits for acknowledgments before sending additional data, preventing congestion and packet loss.

8. Buffering:

- Receivers often employ buffers to temporarily store out-of-order frames until they can be reordered correctly. This prevents packet loss due to frame reordering.

9. Timeout and Retransmission Timer:

- A timeout mechanism is used to determine when a frame is considered lost and needs to be retransmitted. Protocols set retransmission timers to trigger retransmissions if acknowledgments are not received within a specific time frame.

10. Automatic Repeat reQuest with Forward Error Correction (ARQ-FEC):

- Some protocols combine ARQ with FEC, where error correction is performed at the receiver using FEC, and if errors persist, ARQ-based retransmissions are used.

Difference between Router and Gateway

The following table highlights the major differences between a router and a gateway.

Router	Gateway
It is capable of dynamic routing.	It is not capable of dynamic routing.
It's a piece of hardware that's in charge of receiving, processing, and forwarding data packets to other networks.	It is a gadget that allows networks with various protocols to communicate with one another.
The OSI model's layer 3 and layer 4 are used by routers.	The OSI model's layer 5 is where a gateway functions.
A router's primary job is to transport traffic from one network to another.	A gateway's primary role is to convert one protocol to another.
It is only available in specialized applications.	Dedicated apps, physical servers, or virtual applications are used to host it.
A router's main function is to store routing information for various networks and route traffic based on the destination.	A gateway's main function is to distinguish between what is within and what is outside the network.
Wireless networking, static routing, NAT, and DHCP server are some of the extra services provided by a router.	A gateway's further functions include network access control, protocol conversion, and so on.

Conclusion

From the above discussion, we can conclude that Routers are the network devices that can connect multiple networks together. Routers examine the data packets and verify their path to the destination PC. A gateway, on the other hand,

is a network device or piece of hardware that functions as a "gate" between two networks. It may also be characterized as a node that serves as a gateway to the network's other nodes.

What Is Address Resolution Protocol?

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet..

Working of ARP

- ✓ At the network layer, when the source wants to communicate with the destination. Firstly, the source needs to find out the MAC address (Physical Address) of the destination. For this, the source will check the ARP cache and ARP table for the MAC address of the destination. If the MAC address of the destination is present in the ARP cache or ARP table, then the source uses that MAC address for the communication.
- ✓ If the MAC address of the destination is not in the ARP cache or ARP table, then the Source generates an ARP Request message. The ARP Request message consists of the MAC address and the IP address of the source. It also contains the IP address and MAC address of the destination. The MAC address of the destination left null because the user has requested this.
- ✓ The ARP Request message will be broadcasted to the local network by the source computer. All the devices in the LAN network receive the broadcast message. Now, each device compares its own IP address with the IP address of the destination. If the IP address of the device match with the IP address of the destination, then that device will send an ARP to reply message. If the IP address of the device does not match the IP address of the destination, then the device will automatically drop the packet.
- ✓ The destination sends an ARP reply packet when the destination address matches the device. That ARP Reply packet consists of the MAC address of the device. The destination device automatically updates the table and stores the source's MAC address because this address will be required for the communication from the source.
- ✓ Now the source acts as a target for the destination device, and the destination device sends the ARP Reply message.
- ✓ The ARP Reply message is unicast instead of broadcast. This is because the device (destination) that is sending the ARP Reply message knows the MAC address of the device (source) to which the ARP Reply message is sent.
- ✓ When the source device receives the ARP Reply message, then it will know the MAC address of the destination because the ARP Reply packet contains the MAC address of the destination along with the other addresses. The source will update the MAC address of the destination in the ARP cache. Now the sender is able to communicate directly to the destination.

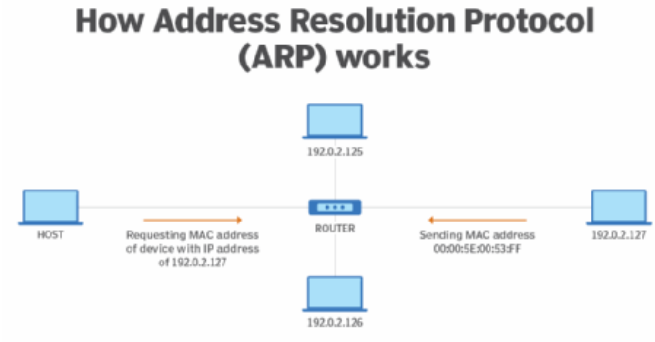

Fig 2.5 ARP Protocol

Advantages of using ARP

- ✓ We can easily find out the MAC address of the device if we know the IP address of that device.
- ✓ It is not necessary to configure the address of the end nodes for the MAC address. We can find it when needed.

Disadvantages of using ARP

- ✓ ARP attacks such as ARP spoofing and ARP denial of service may occur.