UNIT-II: Data Link Layer

The Data Link Layer is the second layer in the OSI (Open Systems Interconnection) model and the second layer in the TCP/IP model. It is responsible for the reliable transmission of data over a physical link or network segment. The primary functions of the Data Link Layer include framing, addressing, and error detection and correction. This layer ensures that data packets are delivered without errors and in the correct order between two directly connected nodes in a network.

Some key features and responsibilities of the Data Link Layer are:

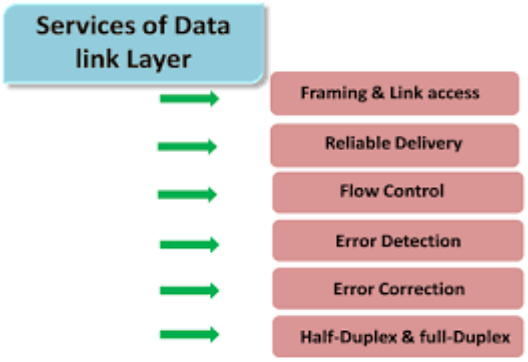
1. Framing: The Data Link Layer takes packets from the Network Layer and encapsulates them into frames, adding start and stop delimiters to define the boundaries of each frame. It also includes other control information for synchronization and flow control purposes.
2. Addressing: Each network interface card (NIC) or network adapter in a network has a unique identifier called a MAC (Media Access Control) address. The Data Link Layer uses MAC addresses to identify devices within the same local network and facilitates the delivery of frames to the correct destination.
3. Error Detection and Correction: The Data Link Layer implements mechanisms to detect and, if possible, correct errors that may occur during data transmission. This ensures the integrity of data being transmitted over the physical medium.
4. Flow Control: The Data Link Layer manages the flow of data between two devices to avoid overwhelming the receiving device with more data than it can handle. It uses various flow control mechanisms to regulate the pace of data transmission.
5. Media Access Control (MAC): The Data Link Layer handles access to the physical transmission medium and determines when devices can transmit data to avoid data collisions in shared networks like Ethernet.
6. Logical Link Control (LLC): The LLC sub-layer of the Data Link Layer is responsible for managing communication between devices on the same network. It offers services to the Network Layer above and handles flow control and error recovery.

Popular Data Link Layer protocols include:

1) Ethernet (IEEE 802.3): Commonly used in local area networks (LANs), Ethernet is a widely adopted standard for wired network connections.
2) Wi-Fi (IEEE 802.11): Used in wireless local area networks (WLANs), Wi-Fi enables wireless communication between devices.
3) Point-to-Point Protocol (PPP): Commonly used for establishing a direct connection between two nodes, such as dial-up connections or point-to-point WAN links.

Data Link Layer Design Issues

Designing the Data Link Layer involves addressing various important issues to ensure the reliable and efficient transmission of data over a network. Let's explore some of the key design issues in more detail:

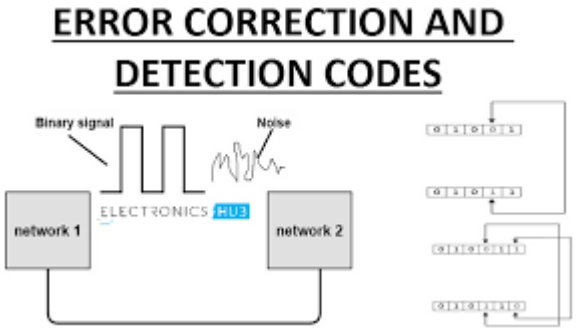


1. **Media Access Control (MAC) Protocols**: The Data Link Layer must determine how devices on a shared network gain access to the transmission medium. Various MAC protocols, such as CSMA/CD (Carrier Sense Multiple Access with Collision Detection) used in Ethernet, or CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) used in Wi-Fi, help manage the access to the channel to prevent collisions and ensure fair distribution of bandwidth.
2. **Error Detection and Correction:** The Data Link Layer is responsible for detecting and, if possible, correcting errors that may occur during data transmission. Techniques like CRC (Cyclic Redundancy Check) or parity bits are used to detect errors in frames. When errors are detected, the layer may request retransmission of the corrupted frames to maintain data integrity.
3. **Framing and Packet Delimitation**: The Data Link Layer needs to define how raw data from the Network Layer is framed into smaller, manageable frames for transmission. The layer must determine the frame boundaries and include control information, such as start and stop flags, to delimit frames accurately.
4. **Flow Control:** Flow control mechanisms are crucial to managing the rate of data transmission between sender and receiver. The Data Link Layer uses techniques like sliding window protocols to ensure that the sender does not overwhelm the receiver with data. Flow control prevents data loss due to buffer overflows.
5. **Link Establishment and Termination:** Before data transmission can occur, the Data Link Layer must establish a link between two devices. This process involves protocols that allow devices to exchange control information and synchronize their communication. Additionally, the layer should handle link termination gracefully.
6. **Addressing and Logical Link Control (LLC)**: The Data Link Layer uses physical addresses, such as MAC addresses, to identify devices on the same network. The Logical Link Control sub-layer is responsible for managing communication between devices and providing services to the Network Layer.

7. **Duplexing**: The Data Link Layer must support different duplex modes, such as half-duplex (one-way transmission at a time) or full-duplex (simultaneous bidirectional communication). The choice of duplex mode affects the efficiency and performance of the communication.
8. **Efficiency and Overhead**: The design of the Data Link Layer should strive to minimize overhead in framing and other control information to maximize the available bandwidth for user data transmission.
9. **Priority and Quality of Service (QoS)**: Some Data Link Layer protocols may support prioritization of data or Quality of Service guarantees to ensure that critical traffic receives preferential treatment over non-critical traffic.
10. **Fragmentation and Reassembly**: When the data received from the Network Layer is larger than the Maximum Transmission Unit (MTU) supported by the Data Link Layer, fragmentation and reassembly mechanisms are necessary to break down and reconstruct data frames.

Error Detection and Correction

Error detection and correction are essential techniques used in data communication to ensure the accuracy and integrity of transmitted data. These techniques help detect and recover from errors that may occur during data transmission over unreliable or noisy communication channels. Let's delve into error detection and correction methods:



Error Detection:

Error detection mechanisms are used to identify whether errors have occurred during the transmission of data. If errors are detected, the receiver can request retransmission of the corrupted data to maintain data accuracy. Common error detection techniques include:

1) **Checksum:** Checksum is a simple method in which the sender adds up all the data bytes and includes the sum (or its complement) in the transmitted message. The receiver recalculates the checksum and verifies it with the received checksum. If they match, the data is assumed to be error-free.
2) **Cyclic Redundancy Check (CRC)**: CRC is a more sophisticated error detection technique. The sender generates a fixed-size CRC code based on the data and appends it to the transmitted message. The receiver performs the same calculation and checks if the calculated CRC matches the received CRC. If they match, the data is considered error-free.
3) **Parity Bit:** Parity is a simple technique used for detecting single-bit errors. A parity bit is added to the transmitted data to make the total number of 1s (or 0s) in the message either even (even parity) or odd (odd parity). The receiver checks if the received data has the correct parity to detect errors.

Error Correction:

Error correction techniques go beyond error detection by not only identifying errors but also recovering the original data without the need for retransmission. These techniques are more complex than error detection and are commonly used in applications where retransmissions are expensive or not feasible. One prominent error correction technique is:

Forward Error Correction (FEC): FEC adds redundant information (error-correcting codes) to the transmitted data, allowing the receiver to correct errors without requesting retransmission. Popular FEC codes include Reed-Solomon codes and Hamming codes. FEC is often used in satellite communication and optical communication systems.

It's important to note that while error detection and correction techniques increase data integrity, they come with a cost of additional overhead. Redundant bits or codes add extra data to the transmitted message, reducing the overall efficiency of data transmission. The choice of error detection and correction methods depends on the specific requirements of the communication system, the expected error rate, and the level of reliability needed.

Elementary Data Link Control Protocols

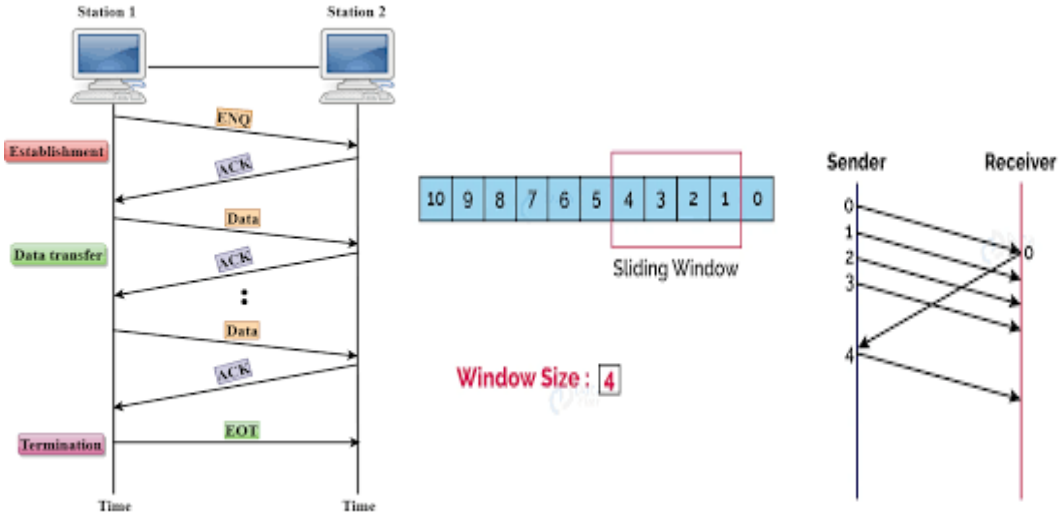
Elementary Data Link Control (EDLC) protocols are simple and basic protocols used in the Data Link Layer to provide reliable communication between two devices over a point-to-point link. These protocols are typically used in scenarios where the underlying physical link is relatively error-free and does not require complex error recovery mechanisms. Here are two common Elementary Data Link Control protocols:

Stop-and-Wait Protocol:

The Stop-and-Wait protocol is one of the simplest EDLC protocols, and it works as follows:

- Sender: The sender sends a data frame to the receiver and waits for an acknowledgment (ACK) from the receiver before sending the next frame. If the sender doesn't receive an ACK within a specified timeout period, it retransmits the same frame.
- Receiver: The receiver waits for a frame from the sender. Upon receiving a frame, it sends an ACK back to the sender to confirm successful reception. If the frame is corrupted or lost, the receiver discards it, and the sender will automatically retransmit the same frame.

The Stop-and-Wait protocol is straightforward to implement but can be inefficient in terms of bandwidth utilization since the sender must wait for ACKs after every frame transmission.



Sliding Window Protocol:

The Sliding Window protocol is a more efficient EDLC protocol that allows multiple frames to be in transit simultaneously. It works as follows:

- Sender: The sender can transmit multiple frames without waiting for individual ACKs for each frame. The sender maintains a "window" of frames that it can transmit before receiving acknowledgments. The window size determines the number of frames that can be sent consecutively.
- Receiver: The receiver keeps track of the frames it expects to receive. Upon receiving a frame correctly, it sends an ACK back to the sender, indicating the next expected frame. If a frame is lost or corrupted, the receiver discards it and waits for the sender to retransmit it.

The Sliding Window protocol significantly improves the efficiency of data transmission, as multiple frames can be in transit simultaneously, reducing the impact of propagation delays. Different variations of the Sliding Window protocol exist, such as Go-Back-N and Selective Repeat, which determine the behavior of the sender and receiver regarding retransmissions and acknowledgments.

Both the Stop-and-Wait protocol and the Sliding Window protocol are examples of half-duplex protocols, meaning that data can only flow in one direction at a time. Full-duplex communication, where data can flow in both directions simultaneously, can also be achieved using similar concepts and techniques.

Sliding Window Protocols

Sliding Window protocols are a family of data link layer protocols that enable efficient and reliable data transmission over a point-to-point communication link. These protocols use a "sliding window" mechanism to manage the flow of data between the sender and receiver. The sliding window allows the sender to transmit multiple data frames consecutively without waiting for individual acknowledgments, improving the utilization of the communication link. The receiver uses the sliding window to keep track of the frames it expects to receive and to provide feedback to the sender.

There are two primary variations of the Sliding Window protocol:

1. Go-Back-N (GBN) Protocol:

In the Go-Back-N protocol, the sender can transmit a continuous sequence of frames, each identified by a sequence number. The receiver acknowledges correctly received frames by sending cumulative acknowledgments (ACKs) indicating the highest sequence number received successfully.

Sender's Perspective:

- The sender maintains a window of frames that it can send, typically ranging from the last acknowledged frame to the last unacknowledged frame plus a predefined window size.
- The sender continuously sends frames within the window and starts a timer for the first unacknowledged frame.
- If the sender receives an ACK for the first unacknowledged frame within the timeout period, it advances the window, acknowledging all frames up to the newly acknowledged frame.
- If the sender does not receive an ACK within the timeout period, it retransmits all the frames in the window, starting from the first unacknowledged frame.

Receiver's Perspective:

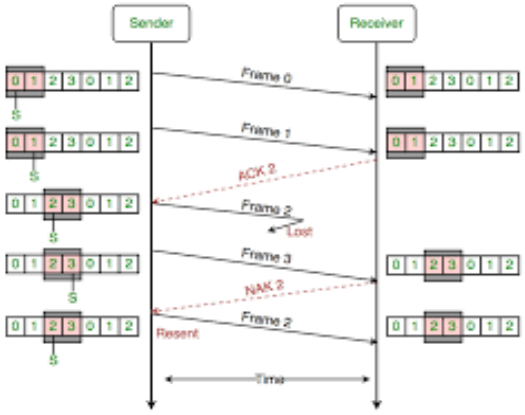
- The receiver expects to receive frames with specific sequence numbers. Upon receiving a frame correctly, it sends an ACK for the highest consecutive frame received (cumulative acknowledgment).
- If a frame is missing or corrupted, the receiver discards it, and the sender will eventually retransmit the missing frames.

Selective Repeat (SR) Protocol:

In the Selective Repeat protocol, the sender can transmit a continuous sequence of frames, each identified by a sequence number, similar to Go-Back-N. However, the receiver individually acknowledges correctly received frames rather than sending cumulative acknowledgments.

Sender's Perspective:

- The sender maintains a window of frames that it can send, typically ranging from the last acknowledged frame to the last unacknowledged frame plus a predefined window size.



- The sender continuously sends frames within the window and starts individual timers for each frame in the window.
- If the sender receives an ACK for a specific frame within the timeout period, it advances the window, acknowledging the successful receipt of that frame.
- If the sender does not receive an ACK for a specific frame within the timeout period, it retransmits only the missing frame (not the entire window).

Receiver's Perspective:

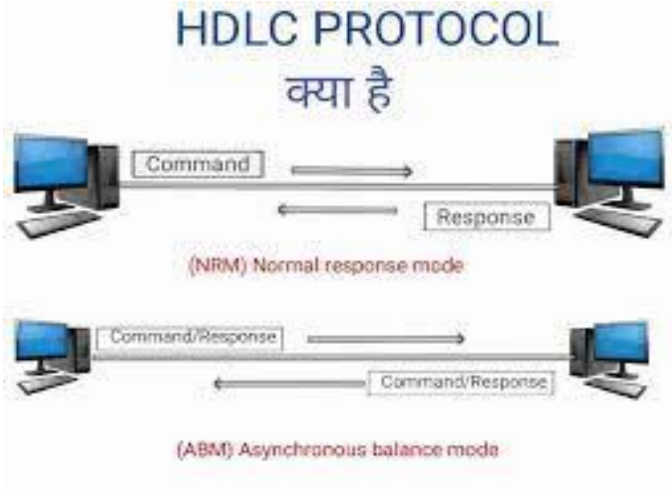
- The receiver expects to receive frames with specific sequence numbers. Upon receiving a frame correctly, it sends an ACK for that specific frame, indicating its successful receipt.
- If a frame is missing or corrupted, the receiver discards it, and the sender will eventually retransmit the missing frame.

Selective Repeat offers better efficiency compared to Go-Back-N, as it allows the sender to avoid unnecessary retransmissions of frames that have been successfully received. However, it requires additional complexity at both the sender and receiver sides to maintain individual timers and acknowledge specific frames.

Both Go-Back-N and Selective Repeat are widely used in point-to-point communication scenarios, such as satellite links or high-speed networks, to achieve reliable and efficient data transmission. The choice between these protocols depends on factors such as link characteristics, error rates, and the required level of performance and reliability.

HDLC (High-Level Data Link Control):

HDLC (High-Level Data Link Control) is a data link layer protocol used for point-to-point and multipoint communication over synchronous communication channels. It is a bit-oriented protocol, meaning it operates at the bit level, and it is widely used in various networking technologies and applications.



Here are some key features and characteristics of HDLC:

1. **Frame Structure:** HDLC frames consist of a header, data, and a trailer. The header and trailer contain control information necessary for frame synchronization, addressing, error detection, and flow control.
2. **Synchronous Communication:** HDLC operates synchronously, meaning it requires both the sender and receiver to be synchronized in terms of bit timing. This synchronization is achieved using special bit patterns called flags (01111110) that delimit the start and end of each frame.
3. **Unnumbered Mode**: HDLC operates primarily in unnumbered mode, where frames are not explicitly numbered for sequencing. Instead, frames are identified by the type of frame they represent (e.g., information, acknowledgment, or supervisory).
4. **Asynchronous Balanced Mode (ABM)**: HDLC's ABM is a mode of operation where both endpoints can act as either the primary or secondary station, allowing bidirectional communication. Each station can initiate the data transfer.

5. **Asynchronous Response Mode (ARM)**: In ARM, one endpoint acts as the primary station, initiating communication, while the other acts as the secondary station, responding to requests from the primary.
6. **Transparency:** HDLC provides transparency for data transmission, which means that certain bit patterns in the data will not be interpreted as control characters. To achieve transparency, HDLC uses a technique called "bit stuffing," where an extra "0" bit is inserted into the data stream whenever five consecutive "1" bits are encountered in the original data.
7. **Error Detection:** HDLC employs a cyclic redundancy check (CRC) for error detection. The CRC helps to detect errors that may occur during data transmission over the communication link.
8. **Link Management:** HDLC includes mechanisms for link establishment, termination, and maintenance. It manages the link between two connected devices and provides the necessary control procedures for reliable data transfer.

HDLC has served as a fundamental protocol in various networking technologies, including ISDN (Integrated Services Digital Network), X.25 networks, and Frame Relay. Its simple and efficient design, along with its ability to handle both point-to-point and multipoint configurations, has made it a widely used protocol in telecommunications.

PPP (Point-to-Point Protocol)

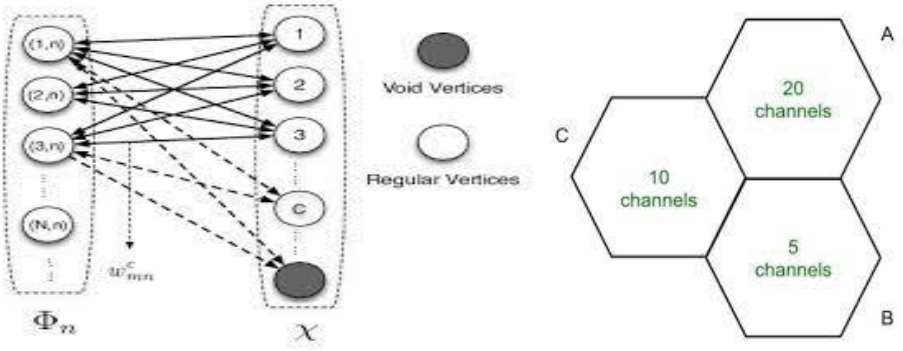
PPP (Point-to-Point Protocol) is a widely used data link layer protocol that provides a method for establishing a direct connection between two network nodes over various physical mediums, such as serial cables, dial-up connections, or dedicated leased lines. PPP is designed to facilitate point-to-point communication, and it offers features for authentication, compression, and error detection. It is highly flexible and extensible, allowing the encapsulation of multiple higher-layer protocols within PPP frames.

Key features and characteristics of PPP include:

1) **Frame Structure:** PPP frames consist of a header and a trailer, with the data payload containing the encapsulated higher-layer protocol packets. The frame's header includes control fields for frame synchronization and error detection.
2) **Link Control Protocol (LCP):** LCP is a crucial component of PPP and is responsible for establishing, configuring, and terminating the PPP link. It negotiates link parameters between the two endpoints, such as authentication methods, compression algorithms, and maximum frame size.
3) **Network Control Protocols (NCPs)**: NCPs are used to configure and manage the higher-layer protocols that are carried within the PPP frames. Examples of NCPs include IPCP (IP Control Protocol) for IP address negotiation and IP packet configuration and IPCP for IPX packet configuration.
4) **Authentication:** PPP supports various authentication methods, such as PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). These methods allow the two communicating nodes to verify each other's identity before allowing data transmission.
5) **Multilink PPP (MLPPP):** MLPPP allows the bundling of multiple physical links to create a single logical link with increased bandwidth. This technique is especially useful for improving data rates in situations where individual links have limited bandwidth.
6) **Error Detection and Correction:** While PPP itself does not provide built-in error correction mechanisms like HDLC, it can work in conjunction with higher-layer protocols like TCP/IP, which handle error detection and recovery.
7) **Dynamic IP Address Assignment**: PPP supports the dynamic assignment of IP addresses to network nodes, making it suitable for dial-up connections, where IP addresses can be assigned on-demand from a pool of available addresses.

Channel Allocation problem

The Channel Allocation problem, also known as the Multiple Access problem, is a fundamental issue in computer networks and telecommunications. It involves the efficient sharing of a communication channel among multiple users or devices to transmit data without interference or collisions. The goal is to allocate the channel's bandwidth and time slots effectively to ensure fair and reliable communication.



There are several types of channel allocation problems, depending on the communication medium and the network architecture:

1. **Multiple Access Channel Allocation:**

In shared communication channels, multiple devices or users need access to the channel to transmit data. The challenge is to determine how these devices share the channel without causing data collisions. Examples of multiple access channel allocation include Ethernet in a local area network (LAN) or Wi-Fi in a wireless network.

- Fixed Channel Allocation: In this method, the channel is divided into fixed time slots, and each device is assigned a specific time slot to transmit data. The disadvantage is that unused time slots cannot be utilized by other devices, leading to inefficiency.
- Dynamic Channel Allocation: This approach dynamically assigns time slots to devices based on their current demand. Various algorithms like Carrier Sense Multiple Access (CSMA) or its variations, like CSMA/CD (Collision Detection) and CSMA/CA (Collision Avoidance), are used to manage access to the channel in an adaptive and more efficient manner.

2. **Frequency Channel Allocation:**

- In wireless communication, multiple frequency channels are available for devices to transmit data. The challenge is to allocate these frequency channels efficiently to minimize interference and maximize data throughput. Frequency Division Multiple Access (FDMA) and Frequency Hopping Spread Spectrum (FHSS) are examples of frequency channel allocation methods.

3. **Time Division Channel Allocation:**

In time division multiplexing (TDM) scenarios, a single channel is divided into time slots, and different devices take turns to use the channel during their allocated time slot. This method is commonly used in digital voice communication and T1/E1 lines for digital data transmission.

4. **Code Division Channel Allocation:**

Code Division Multiple Access (CDMA) is used in mobile cellular networks, where each device is assigned a unique code to transmit data simultaneously over the same frequency channel. CDMA allows multiple users to share the same channel while keeping their data separated through the use of different codes.

IEEE standards for Local Area Networks

The Institute of Electrical and Electronics Engineers (IEEE) has developed several standards for Local Area Networks (LANs) to ensure interoperability, reliability, and performance in networking technologies. Here are some of the most notable IEEE standards for LANs:

1) IEEE 802.3 Ethernet:

This is one of the most widely used LAN standards and defines the specifications for wired Ethernet networks. It covers various data rates, including 10 Mbps (10BASE-T), 100 Mbps (100BASE-T), 1 Gbps (1000BASE-T), 10 Gbps (10GBASE-T), and higher. Ethernet is used in various settings, from home and small office networks to large enterprise networks.

2) IEEE 802.11 Wi-Fi:

Also known as Wi-Fi, this standard defines wireless LAN (WLAN) technologies. It specifies different wireless frequencies, modulation techniques, and security protocols for wireless communication. Various versions of Wi-Fi have been developed, including 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax (Wi-Fi 6 and Wi-Fi 6E).

3) IEEE 802.1Q VLANs:

This standard defines Virtual LANs (VLANs), which allow logical segmentation of a physical LAN into multiple virtual LANs. VLANs enable network administrators to group devices logically, regardless of their physical location, enhancing network security and efficiency.

4) IEEE 802.1X Port-Based Network Access Control:

This standard specifies port-based network access control, often used in conjunction with VLANs for securing access to network resources. It provides a framework for authentication and authorization of devices trying to connect to the network.

5) IEEE 802.3af and IEEE 802.3at PoE:

These standards define Power over Ethernet (PoE) technologies, enabling network devices like IP phones, wireless access points, and IP cameras to receive power and data over a single Ethernet cable.

6) IEEE 802.3ad Link Aggregation (LAG) / IEEE 802.1AX Link Aggregation Control Protocol (LACP):

These standards define link aggregation techniques that allow multiple Ethernet links to be bundled together to increase bandwidth and provide redundancy.

7) IEEE 802.1D Spanning Tree Protocol (STP) / IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) / IEEE 802.1s Multiple Spanning Tree Protocol (MSTP):

These standards provide mechanisms to prevent loops in Ethernet networks and enable redundant paths without causing network instability.

8) IEEE 802.1Q-2018 Time-Sensitive Networking (TSN):

TSN is a set of standards that address real-time communication requirements in industrial and automotive applications, ensuring deterministic and low-latency data transmission.

WLAN, Bluetooth

WLAN (Wireless Local Area Network) and Bluetooth are two wireless communication technologies commonly used for short-range wireless connections. Both technologies enable devices to communicate without the need for physical cables, making them convenient for various applications. However, they differ in their use cases, range, data rates, and intended applications.

WLAN (Wireless Local Area Network):

- Definition: WLAN is a wireless network technology based on IEEE 802.11 standards that allows devices to connect to a local network or the internet without the need for wired connections. It is commonly used in homes, offices, public places, and other locations to provide wireless internet access and local network connectivity.
- Range: WLAN typically covers a range of several tens to a few hundred meters, depending on factors like the type of access point and environmental conditions.
- Data Rates: WLAN supports various data rates, depending on the specific IEEE 802.11 standard used. The most common ones are 802.11n (up to 600 Mbps), 802.11ac (up to several Gbps), and the latest 802.11ax (Wi-Fi 6) standard with even higher data rates.
- Applications: WLAN is used for connecting laptops, smartphones, tablets, IoT devices, and other devices to the internet or local networks. It is commonly used for web browsing, video streaming, file sharing, and other data-intensive applications

Bluetooth:

- Definition: Bluetooth is a short-range wireless technology that allows devices to establish low-power, ad-hoc connections and communicate with each other. It operates on the 2.4 GHz ISM band.
- Range: Bluetooth has a relatively shorter range compared to WLAN, typically up to 10 meters (Bluetooth Classic) or up to 100 meters (Bluetooth Low Energy - BLE).
- Data Rates: Bluetooth data rates vary based on the version of Bluetooth. Bluetooth 3.0 and 4.0 have data rates of up to 24 Mbps, while Bluetooth 5.0 and newer versions support up to 2 Mbps.
- Applications: Bluetooth is commonly used for connecting devices such as smartphones, wireless headphones, speakers, fitness trackers, smartwatches, and IoT devices. It is ideal for short-range connections, like wirelessly transferring files, streaming audio, or exchanging small amounts of data between devices.

Comparison:

- WLAN provides higher data rates and longer range compared to Bluetooth, making it more suitable for data-intensive applications and connecting devices over larger distances.
- Bluetooth excels in short-range communication, and its low power consumption makes it ideal for battery-operated devices like wearables and IoT sensors.
- WLAN requires access points for network connectivity, while Bluetooth devices can directly communicate with each other without the need for intermediate infrastructure.