The Data Link Layer is the second layer of the OSI Layered Model. It ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It is responsible for converting a data stream to signals bit by bit and sending them over the underlying hardware. At the receiving end, the data link layer picks up data from the hardware, which is in the form of electrical signals, assembles them into a recognizable frame format, and hands them over to the upper layer. To detect errors efficiently and easily, transmitting a small-size data is a better approach.

The data link layer has two sub-layers: Logical Link Control (LLC) and Media Access Control (MAC). The LLC deals with protocols, flow-control, and error control. It provides an interface to the upper layer, flow control, error control, and management functions. The MAC sub-layer deals with the actual control of media, constructing headers and trailers, assembling frames, addressing, error checking, and accessing the medium.

The data link layer performs several functions, including framing, addressing, synchronization, error control, flow control, and multi-access. Framing involves taking packets from the network layer and encapsulating them into frames, then sending each frame bit-by-bit on the hardware. At the receiver's end, the data link layer picks up signals from the hardware and assembles them into frames. Addressing is provided through a layer-2 hardware addressing mechanism, with a unique hardware address encoded into the hardware at the time of manufacturing. Synchronization ensures that both machines are synchronized when data frames are sent on the link. Error control detects and attempts to recover actual data bits when errors occur in transition. Flow control ensures that stations on the same link, which may have different speeds or capacities, can exchange data at the same speed. Multi-access mechanisms such as CSMA/CD are used to equip systems with the capability of accessing a shared media.

The frame is formed by breaking down a stream of packets into smaller, digestible chunks. It typically includes synchronization features that indicate to the receiver the beginning and end of the payload data within the stream. In the OSI model, a frame is the protocol data unit at the data link layer, representing the final encapsulation before transmission over the physical layer. A frame consists of a link-layer header followed by a packet, separated by an interframe gap. Examples include Ethernet frames, PPP frames, Fiber Channel frames, and V.42 modem frames. Frames can have fixed or variable sizes. Fixed-size frames, such as those in the ATM wide-area network, do not require boundary definitions, as the size itself acts as a delimiter. Variable-size frames require start and end specifications and are prevalent in local area networks.

Variable-size framing approaches include the Character-Oriented and Bit-Oriented methods. The Character Count method uses a field in the header to specify the number of characters in the frame but can fail if the count is distorted in transit. Bit stuffing allows frames to contain an arbitrary number of bits and character sizes. Each frame begins and ends with a special bit pattern called a flag byte. When five consecutive 1s are encountered in the data, a '0' bit is stuffed into the outgoing bit stream. Byte stuffing, or Character Stuffing, recognizes frame boundaries using flag bytes, inserting an escape byte before any flag byte in the data. Physical Layer Coding Violations apply to networks where data encoding on the physical medium contains redundancy.

Error detection and correction mechanisms are used to ensure accurate transmission. Errors can be of three types: single-bit errors, multiple-bit errors, and burst errors. Error detection allows the receiver to check whether the received data is corrupted and may request retransmission. Error correction allows the receiver to reconstruct the original information when errors occur. Common error detection methods include Parity Check and Cyclic Redundancy Check (CRC). Parity Check adds an extra bit to make the number of 1s even or odd, while CRC involves binary division of the data bits, using a divisor generated by polynomials. The checksum method divides data into sections, adds them using one's complement arithmetic, and complements the result to create a checksum.

Error control mechanisms include Automatic Repeat Request (ARQ), where data retransmission occurs in case of damaged frames, lost frames, or lost acknowledgements. Retransmission is triggered by three cases: damaged frames, lost frames, and lost acknowledgements. ARQ techniques include Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ. Stop-and-Wait ARQ sends a frame and waits for an acknowledgment before transmitting the next frame. If no acknowledgment is received in time, the sender retransmits the frame. Piggybacking is used in bidirectional communication, where acknowledgements are placed in data frame headers to save bandwidth. Go-Back-N ARQ allows the sender to send multiple frames without receiving acknowledgments for each. If a frame is lost, all subsequent frames are retransmitted. Selective Repeat ARQ improves efficiency by retransmitting only the frames that were not acknowledged.

Flow control manages the rate of data transmission to prevent a fast sender from overwhelming a slow receiver. It can be achieved through feedback-based flow control, where the receiver informs the sender of its status, and rate-based flow control, where data transfer occurs at a rate agreed upon in pre-communication. Methods include Stop-and-Wait and Sliding Window. The Sliding Window mechanism allows multiple frames to be transmitted before an acknowledgment is required, improving efficiency over Stop-and-Wait.

HDLC is a data link layer transmission protocol developed by IBM, ensuring successful data transmission through frames containing address, control, data, and checksum fields. HDLC supports three types of frames: Information frames (I-frames) carrying user data, Supervisory frames (S-frames) carrying control information, and Unnumbered frames (U-frames) for session management and control. PPP is a data link protocol for direct connections between nodes, commonly used for dial-up internet access. It provides connection authentication, transmission encryption, and data encapsulation. PPP supports multiple network layer protocols and is widely used for LAN-to-WAN connections.

The Media Access Control (MAC) layer handles shared physical connections among multiple computers. It is responsible for addressing, channel access control, and managing collisions. Ethernet, IEEE 802.3, is a widely used MAC protocol employing Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Other MAC protocols include ALOHA, CSMA, and Token Ring. The channel allocation problem involves managing shared broadcast channels among multiple users. Static channel allocation methods like Frequency Division Multiplexing (FDM) and Time Division Multiplexing (TDM) waste bandwidth in dynamic environments. Dynamic allocation methods like ALOHA and CSMA are more efficient.

Multiple Access Protocols regulate transmission on shared broadcast channels. These include Random Access Protocols (e.g., ALOHA, CSMA), Channel Partitioning Protocols (e.g., TDMA, FDMA, CDMA), and Controlled Access Protocols. Ethernet technology is widely used in LANs and MANs, defined by IEEE 802.3 standards. Token Ring (IEEE 802.5) uses token passing for network access control, while Token Bus (IEEE 802.4) combines Ethernet and Token Ring characteristics.

VLANs (Virtual Local Area Networks) logically group devices within a network, improving security, reducing broadcast traffic, and enhancing management. VLANs can be configured statically or dynamically using VLAN Membership Policy Servers (VMPS). WLAN (Wireless LAN), based on IEEE 802.11 standards, enables wireless networking through infrastructure or ad-hoc modes. Wireless networks offer mobility, cost-effectiveness, and flexibility in various environments.