Christina M. Restauri
Comp Networks for Info Spec 1
April 28, 2021

Data Link Layer: Services

The Data Link Layer is the second layer of the Open Systems Interconnection OSI model. It issues service requests to the physical layer below it and responds to service requests from the network layer above it. Its responsibility is to encode the bits from the physical layer into packets prior to transmission and decode the packets back into bits at the destination. This ensures reliable transmission and delivery of packets across a physical network link from one node (host or router) to another. It also provides the means for detecting transmission errors such as when devices attempt to use the medium simultaneously.

The Data Link Layer is implemented both in software and hardware which is why this layer is divided into two sub-layers called the Logical Link Control LLC and the Media Access Control MAC layers. The Institute of Electrical and Electronics Engineers (IEEE) subdivided the data link layer into two sublayers and each has its own functions. The LLC sublayer places information in the frame that identifies which network layer protocol is being used. This information allows multiple layer 3 protocols, such as IPv4 and IPv6 to utilize the same network interface and media. The MAC sub-layer handles physical addressing and framing. It manages frame access to the network media according to the physical signaling requirements (Englander, Pg. 409).

Together, the MAC and LLC layers are able to provide three (3) levels of service:

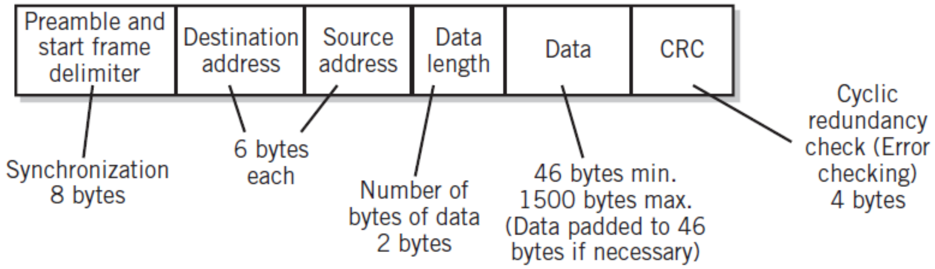
- Unacknowledged connectionless service is when the sender and receiver send frames without any acknowledgment of the receiver.
- Acknowledged connectionless service is when the sender knows a frame has arrived safely or not. If not, it will resend the packet. There is no logical connection established but it uses the time frames for checking acknowledgments.
- Acknowledged connection-oriented service is highly reliable but overhead is very high. Frames are numbered in order and sequence which guarantees the order. Both sender and receiver establish a connection before transmission.

Framing

When framing takes place, both machines must synchronize in order for the transfer to be successful. These frames contain the beginning and end of the packets. They have two address fields provided to identify the source and destination stations and a frame check sequence field for detection of transmission errors. When framing takes place, it breaks up the network layer data stream into small blocks called segmentation, it then adds a header and frame flag to each block to form a frame called encapsulation. The header and trailer in the encapsulation process controls the information to help nodes determine where a frame begins and ends (the delimiters), who is in the communication (physical addresses), and which nodes will communicate next (hop-to-hop links). At the end of the frames are fields that form the trailer. This area is used to detect errors and to mark the end of the message.

FIGURE 13.5

Standard Ethernet Frame


Preamble and start frame delimiter
Destination address
Source address
Data length
Data
CRC
Synchronization 8 bytes
6 bytes each
Number of bytes of data 2 bytes
46 bytes min. 1500 bytes max. (Data padded to 46 bytes if necessary)
Cyclic redundancy check (Error checking) 4 bytes

Note: The above figure 13.5 provided by Englander, 2014. Networks and Data Communications, p. 410.

Physical Addressing (MAC)

The MAC addresses are the physical addresses of the nodes. The data frames sent across a local area network must use these physical addresses to identify the source and destination addresses. When a network card is installed in a computer, it immediately has its own data link layer address that uniquely identifies it from every other computer in the world. This physical address is used for identifying the source of all frames being transmitted. The MAC address and physical address are often used interchangeably. Nonetheless, this physical address is how the packets navigate to their destination. A protocol called Address Resolution Protocol ARP is used to discover the relationship between an IP address and its corresponding physical address or MAC address. It performs IP address-to-physical address translation (Englander, Pg. 410).

Because there are different types of medium such as copper wires, microwaves, optical fibers, and satellite links, there are also different standards to correspond with each physical medium and signaling method. The data link layer prepares the information by using timers and sequence numbers to check for errors assuring the correct sequencing of data. It provides protocols like Ethernet to enable the data to pass successfully to the next layer. There are other layer 2 protocols such as PPP, High-Level Data Link Control (HDLC), Frame Relay, and Asynchronous Transfer Mode (ATM), but Ethernet is the predominant medium-access protocol for local area networks LANs (Englander, Pg. 409).

Media Access Control (MAC continued…)

The MAC or media access control is also the name of the sublayer and controls how data is placed and received from the various types of media. It is defined by the Institute of Electrical and Electronic Engineers (IEEE) 802.3 subcommittee. There are different methods for controlling this access and it depends on how the nodes share the media and what type of topology (Point-to-Point, Multiaccess, Ring) or how the connections appear to the data link. The two basic methods for shared media are Controlled and Contention-based (Dye, 2008).

- Controlled is when each node has its own time to use the medium. This makes the network predictable and eliminates collisions as well. This type of control is mostly implemented in wide area networks where there are large amounts of data traveling long distances. The frames moving through WANs are also exposed to the more detrimental environments than those of LANs.

- In the contention-based method, all nodes are competing to use the medium. These networks usually have plenty of bandwidth and shorter geographical distances like LANs because their access methods do not have the overhead for controlled methods.

There are two forms of control in a contention-based network, Carrier Sense Multi-access Collision Detection (CSMA/CD) for Ethernet networks and Carrier Sense Multi-access Collision Avoidance CSMA/CA generally used in wireless networks (Dye, 2008). These controls both monitor the media for a data signal called the "carrier" and if there is no signal, then the data is transmitted. The only difference between the two are CSMA/CA transmits that it is about to send data to let the other devices know to keep the airways free thus avoiding collisions. In CSMA/CD, it will check for the carrier and if present, will wait until no carrier is active, then it will transmit. CSMA/CD does not prevent the occurrence of collisions that might occur, it only detects (listens) if the channel is free and then transmits the frame to the access point and then to the destination node (Englander, 412).

Flow Control

In this service of the Data Link Layer, flow control deals with the hop-to-hop transmission between the source and destination stream of communication patterns between nodes. It is basically a speed matching mechanism between the sender and the receiver to establish a smooth communication without loss. It accomplishes this by managing how much data can be sent by the sender before receiving an acknowledgement from the sender which is the indication for the sender to send the next set of packets. There are two type of mechanisms that can be used called Stop and Wait and Sliding Window. Stop and Wait forces the sender to stop and wait until an acknowledgement is received after it has sent its data. In Sliding Window, both the sender and receiver agree on the number of frames after which the acknowledgement should be sent. In flow control, error control can influence it, both work closely together (Azahari, 2013).

Error Control

Error control in computer networks is typically achieved by detecting errors. The data link layer deals with errors that occur in transmission and there are numerous chances for transmission errors that can affect the frames. The information that is transferred from one hop to another in a steady stream can be exposed to interference such as White or Gaussian noise, Impulse noise, Crosstalk, Echo, Jitter, Attenuation, and Distortion. These channel interferences change the structure of the signal which causes errors (ITU, 1996). There are two types of errors, single-bit and burst. A single-bit error changes only one bit from either a 1 to a 0 or a 0 to a 1. Even though it is only one bit, it changes the whole meaning of the data being transmitted. The second type of error is a burst error. This type of error is when multiple bits in the data unit have changed (Azahari, 2013).

There are various techniques for error control and they have their advantages and disadvantages as does flow control but together they help ensure frames are received in order and without errors. When detecting errors, the receiver decides whether the received data is correct or not without having to copy the original message. It accomplishes this by using redundancy which adds extra bits for detecting errors at the destination. There are two factors to determine error detection, the bit error rate (BER) and the type of error: random single-bit errors or groups of continuous bit errors or burst errors. The most widely used error detection schemas are: Parity Checks, Cyclic Redundancy Checks (CRC), and Checksums (Azahari, 2013).

Parity Checks

A parity check is the more common method for detecting bit errors with asynchronous character and character-oriented synchronous transmission. It involves adding a parity bit to each block of data bits either even or odd. For even (odd) parity, the sender sets the parity bit so that the total number of 1 bits is even (1) parity bit and odd (0) parity bit. However, this method is suitable for single bit error detection only. The problem is if there are an even number of errors, it will not detect it and cannot tell which bit is in the error. Therefore, it has a one bit error detection capability but no error correction capability.

Cyclic Redundancy Checks

This method can detect more errors without increasing the amount of additional information within the packet. The hardware necessary to perform this task is a shift register circuit. CRC is based on binary division using a predetermined divisor so if the remainder is the same as the value on the added CRC, the data will be received. CRC is good at detecting single-bit and double-bit errors, as well as odd number errors and bust errors.

Checksums

A Checksum is a type of redundancy check used to detect errors. It calculates the binary values in a packet and stores the results with the data. On the other end, the new checksum is calculated and compared with the existing checksum. A non-match indicates an error. Checksum detects all errors involving an odd number of bits as well as even number of bits. Traditional checksum has performance issues in detecting errors due to values in words incrementing and decrementing the same number of times causing the checksum value to remain the same even though there are errors. However, the Fletcher and later Adler checksums are both created to have detection capabilities almost as good as CRCs (Azahari, 2013).

Summary

The Data Link Layer is responsible for making the physical links reliable for the various shared types of communications. This paper discussed the data link layer’s characteristics and responsibilities. This paper also covered the logical link control sub-layer which handles flow control (controlling the flow of packets in the network), error control (controlling errors during transmission), and media access control (controlling the nodes accessing the channel).

The areas covered specifically were namely, framing which encapsulates the data into frames, then adds error checking bits, flow control, and correction methods. Consequently, the receiving side in turn looks for errors, flow control, and extracts the datagram. While not all methods for error detection and correction were presented in this paper, the most popular techniques and widely used error detection schemas and their functions were presented.

References

Azahari, A. (. 1.)., et al. “Review of Error Detection of Data Link Layer in Computer Network.” ARPN Journal of Engineering and Applied Sciences, vol. 9, no. 1, pp. 1–4. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=edselc&AN=edselc.2-52.0-84894293827&site=eds-live. Accessed 7 Apr. 2021.

Conard, J. W. “Services and Protocols of the Data Link Layer.” Proceedings of the IEEE, Proc. IEEE, vol. 71, no. 12, Dec. 1983, pp. 1378–1383. EBSCOhost, doi:10.1109/PROC.1983.12781.

Englander, I. (2014). “The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach.” John Wiley & Sons, Inc. Bentley University. Fifth Edition.

Institute of Electrical and Electronics Engineers. (2021). “IEEE GET Program.” Retrieved from https://ieeexplore.ieee.org/browse/standards/get-program/page/series?id=68.

International Telecommunication Union (ITU). (1996). Handbook Digital Radio-Relay Systems. Retrieved from https://www.itu.int/dms_pub/itu-r/opb/hdb/R-HDB-24-1996-PDF-E.pdf.

Dye M., McDonald R., & Rufi A. W. (2008). Network Fundamentals, CCNA Exploration Companion Guide. Cisco Press, Cisco Systems, Inc., Indianapolis, IN.