Unit 4
Data Link Layer

Introduction

The data link layer provides reliable transmission of data between two nodes of systems. The primary function of this layer is to combine all bit signals in terms of single unit namely **frame**. It manages transmission circuit established in Layer 1 & send error free data to the above layer (Network layer). The data link layer takes a raw transmission facility and transforms it into a line that appears free of transmission error in the network layer.

A data link protocol performs three functions:

i. Controls when computers transmit (media access control)
ii. Detects and corrects transmission errors (error control)
iii. Identifies the start and end of a message by using a PDU (message delineation)

This datalink layer is further divided into '2' sub layers.

1. **Media Access Control (MAC):** MAC concerns itself with the access control method & determines how physical transmission is controlled. It is concerned with physical address which is a 48-bit address (12 digits hexadecimal number).
2. **Logical Link Control (LLC)**: Establish links between physical and network layer. Multiplex information by splitting it into frames of data, sending the frames across the line and arranging the frames back in order.

Some major responsibilities of Data link Layer are:

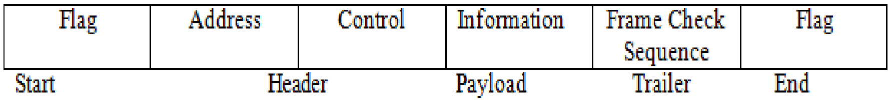
1. **Framing**
   - Combining of single data bits into a frame which is coming from the layer 1.
   - Splitting the data packets into the frames if it is coming from layer 3.
2. **Flow Control**
   - Enforce the flow control mechanism to avoid the overflow & underflow condition
   - Provides the data rate at which receiver can absorb the data.
3. **Error Control**
   - Reliability is added into physical layer by data link layer to detect & re-transmit lost or damaged frames to prevent the duplication of frame.
   - This is achieved through trailer added to the end of the frame.
4. **Access Control**
   - If the multiple nodes are connected to a common network & share common communication medium then there is a high possibility of data collision. To prevent the collision there is a need of Media Access Control.
   - This method defines the procedure a computer follows when it needs to send frames.
5. **Physical Addressing**
   - Data link Layer addresses are called Physical address or MAC Address.
   - These are used to find out the address of next hop in hop to hop delivery.

- 48 bits address is used. i.e. 12 digit Hexadecimal number. E.g. 0F-.2D - 3B - 4A - CD - E8

Framing

The bit stream is combined into an organized format as a single unit called frame. The process of making such type of frame is called **framing**. Framing is the layer 2 encapsulation process.

Structure of Frame



Flag	Address	Control	Information	Frame Check Sequence	Flag
Start	Header		Payload	Trailer	End

Header: A frame header contains information used to process the frame. How the frame is going to deal, such parameters are present there. Particularly, it contains source and destination address.

Payload: it contains actual information to be delivered and is usually much larger than frame header.

Trailer: it contains error detection and error correction bits & methods.

Flag: it marks the beginning and end of frame.

Types of Framing

Framing are of two types:

1. **Variable sized framing**: the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame. This can be done in two ways:
   i. **Length field** – We can introduce a length field in the frame to indicate the length of the frame. Used in **Ethernet (802.3).**
   ii. **End Delimiter (ED)** – We can introduce an ED (pattern) to indicate the end of the frame. Used in **Token Ring**.
2. **Fixed size framing** Here the size of the frame is fixed and so the frame length acts as delimiter of the frame. Consequently, it does not require additional boundary bits to identify the start and end of the frame

Techniques of Framing

Breaking the bit stream into the frame is really the most difficult task. One way to achieve this task is to make the timing gap between the frames or inserting starting and ending points etc.

Following approaches are used:

1. **Character Count**
2. **Flag bytes with byte stuffing (Starting and ending with character stuffing)**
3. **Starting and ending flags with bit stuffing**
4. **Physical Layer Code Violation**

Media Access Control (MAC)

Media access control refers to the need to control when computers transmit. With point-to-point configurations, media access control is unnecessary because there are only two computers on the circuit.

Media access control becomes important when several computers share the same communication circuit, such as a point-to-point configuration with a half-duplex configuration that requires computers to take turns, or a multipoint configuration in which several computers share the same circuit. Here, it is critical to ensure that no two computers attempt to transmit data at the same time—but if they do, there must be a way to recover from the problem.

There are two fundamental approaches to media access control:

1. **Contention:**

   With **contention** computers wait until the circuit is free (i.e., no other computers are transmitting) and then transmit whenever they have data to send. Contention is commonly used in Ethernet LANs. As an analogy, suppose that you are talking with some friends. People listen and if no one is talking they can talk.

2. **Controlled Access**

   Most wireless LANS use **controlled access**. In this case, the wireless access point controls the circuit and determines which clients can transmit at what time. There are two commonly used controlled access techniques: **access requests and polling.**

   With the **access request** technique, client computers that want to transmit send a request to transmit to the device that is controlling the circuit. The controlling device grants permission for one computer at a time to transmit.

   When one computer has permission to transmit, all other computers wait until that computer has finished, and then, if they have something to transmit, they use a contention technique to send an access request.

   (The access request technique is like a classroom situation in which the instructor calls on the students who raise their hands. The instructor acts like the controlling access point. When they want to talk, students raise their hands and the instructor recognizes them so they can contribute. When they have finished, the instructor again takes charge and allows someone else to talk)

   Polling is the process of sending a signal to a client computer that gives it permission to transmit. With polling, the clients store all messages that need to be transmitted. Periodically, the controlling device (e.g., a wireless access point) *polls* the client to see if it has data to send. If the client has data to send, it does so. If the client has no data to send, it responds negatively, and the controller asks another client if it has data to send. It includes

   Roll-call polling & Hub polling

   With **roll-call polling**, the controller works consecutively through a list of clients, first polling client 1, then client 2, and so on, until all are polled. Roll-call polling can be modified to select clients in priority so that some get polled more often than others. For example, one could increase the priority of client 1 by using a polling sequence such as 1, 2, 3, 1, 4, 5, 1, 6, 7, 1, 8, 9.

   With **hub polling** (often called **token passing**), one device starts the poll and passes it to the next computer on the multipoint circuit, which sends its message and passes the poll to the next. That computer then passes the poll to the next, and so on, until it reaches the first computer, which restarts the process again.

Relative Performance

Which media access control approach is best: controlled access or contention? There is no simple answer. The key consideration is throughput—which approach will permit the most amounts of user data to be transmitted through the network.

In general, **contention approaches** work better than controlled approaches for small networks that have low usage. In this case, each computer can transmit when necessary, without waiting for permission. Because usage is low, there is little chance of a collision. In contrast, computers in a controlled access environment must wait for permission, so even if no other computer needs to transmit, they must wait for the poll.

The reverse is true for large networks with high usage: **controlled access works better**. In high-volume networks, many computers want to transmit, and the probability of a collision using contention is high. Collisions are very costly in terms of throughput because they waste circuit capacity during the collision and require both computers to retransmit later. Controlled access prevents collisions and makes more efficient use of the circuit, and although response time does increase, it does so more gradually.

Error Control

Network must be able to transfer data from one device to another with acceptable accuracy. The system must guarantee that the data received are identical to the data transmitted. But during transmission there might occur errors. Some small level errors are tolerable and some are not.

There are two categories of network errors: **corrupted data** (data that have been changed) and **lost data**. Networks should be designed **to (1) prevent, (2) detect, and (3) correct** both corrupted data and lost data.

Sources of Errors

Distortion, attenuation, line outages and **line noise** can cause data communication error.

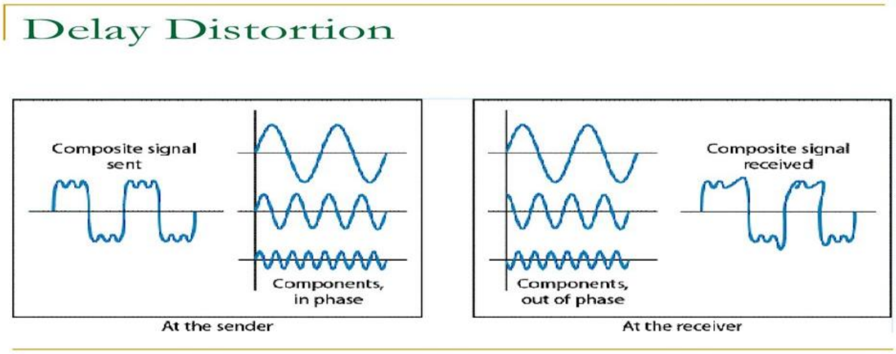
Distortion

It is the change in shape and size of signal. Mostly occurs in case of composite signals made of different frequencies. Due to non uniform velocities of signals of different frequencies, various frequencies of a message signal will arrive at different delay which results in **distortion**.

Delay Distortion

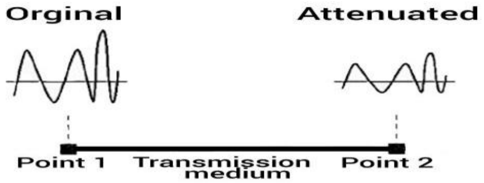
It occurs in case of guided media. For a **band limited signal**, (A band limited signal is a signal with zero energy outside of a defined frequency range.) the velocity tends to be highest near the center frequency and fall off towards the edge of the band. This various frequency components will arrive at receiver at different time resulting the phase shift between the different frequencies. This is called **delay distortion**.

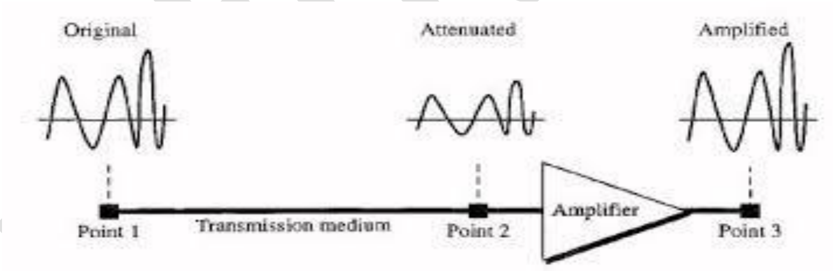
It is critical for digital data because some of the signal components of 1 bit position can spill into another bit position which causes **Inter Symbol Interference (ISI)**.



Attenuation

It is the decrease in strength of signal with the increase in distance. When signal propagates with distance, signal becomes weak. Before the signal vanished, some devices should be kept in between source and destination which makes signal strong.



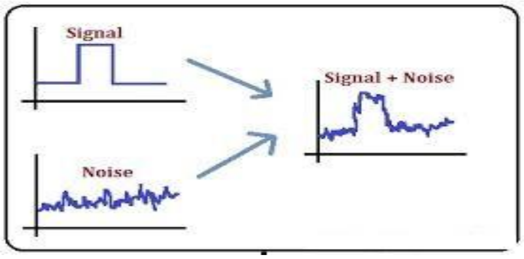


Line Outages

These are catastrophic cause of errors and incomplete transmission. A communication circuit fails for short period of time. This type of failure is caused by loss of carrier signal, storms or any other failure that causes a short circuit.

Noise

It is the addition of unwanted signal on the source sent data signal and received at the receiver side is noise. Received signal consist of transmitted signal plus unwanted signal which are inserted in between transmitter and receiver.



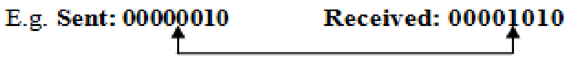
Noise includes the following types:

1. **Thermal Noise/White Noise/ Johnson noise:** It is caused due to thermal agitation of electron and is inescapable. It is present in all electronic devices and transmission media and is function of temperature.
2. **Intermodulation Noise**: When signal at different frequency share common transmission medium, noise signals are produced at frequency (sum or difference or multiple of frequencies) called intermodulation noise. E.g. f_1+ f_2=f_3 (f_1 & f_2 are two signals and f_3 is a new signal which is made from combination of f_1 &f_2)
3. **Crosstalk**: it is unwanted coupling between signal paths. Can occur by the phenomenon in which signal transmitted on one channel of a transmission creates an undesirable effect on other circuit or channel. Crosstalk is experienced during telephone calls when we hear other conversations in the background.
4. **Impulse Noise:** It is the primary source of errors in data communications. It is non-continuous and is generated as sudden scaling of amplitude. Is generated by many causes like electromagnetic disturbances such as lightning, thunder, faults and flaws in communications system etc. it is crated for short period of time.
5. **Echoes:** Echoes are caused by poor connections that cause the signal to reflect back to the transmitting equipment. If the strength of the echo is strong enough to be detected, it causes errors.

Types of errors

The types of error that might occur are:

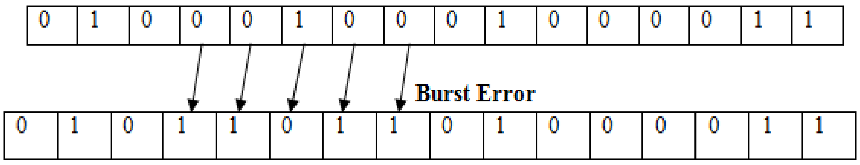
i. **Single bit Error:** Here only one bit of a given data unit is changed. I.e.1 to 0 and vice versa.



E.g. Sent: 00000010 Received: 00001010

ii. **Burst Error:** Here 2 or more bits in the data unit have changed. In burst error **three** kinds of error can occur:

   a. The bits in the frame can be inverted, anywhere within the frame including the data bits or the frame's control bits.
   b. Bits can be deleted from the frame.
   c. Additional bits can be inserted into the frame, before the frame or after the frame.



0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1
0	1	0	1	1	0	1	1	0	1	0	0	0	0	1	1

iii. **Erasure (Ambiguity):** the signal that arrives at a receiver ambiguous (data not clear, either logical 1 or a logical 0).

Error Prevention

Error prevention is very important. There are many techniques to prevent errors (or at least reduce them), depending on the situation. Some techniques are:

- **Shielding** (protecting wires by covering them with an insulating coating) is one of the best ways to prevent impulse noise, cross-talk, and intermodulation noise. Many different types of wires and cables are available with different amounts of shielding. In general, the greater the shielding, the more expensive the cable and the more difficult it is to install.
- **Moving cables** away from sources of noise (especially power sources) can also reduce impulse noise, cross-talk, and intermodulation noise. For impulse noise, this means avoiding lights and heavy machinery. Locating communication cables away from power cables is always a good idea. For cross-talk, this means physically separating the cables from other communication cables.
- Cross-talk and intermodulation noise is often caused by improper multiplexing. Changing multiplexing techniques (e.g., from FDM to TDM) or changing the frequencies or size of the guardbands in FDM can help.
- **Many types of noise** (e.g., echoes, white noise) can be caused by poorly maintained equipment or poor connections and splices among cables. This is particularly true for echo in fiber-optic cables, which is almost always caused by poor connections. The solution here is obvious: Tune the transmission equipment and redo the connections.
- To avoid attenuation, telephone circuits have **repeaters** or **amplifiers** spaced throughout their length. For **analog signal amplifier** can be used, for **digital signal repeaters** can be used.

Error Detection

It is possible to develop data transmission methodologies that give very high **error-detection** performance. The only way to do error-detection is to send **extra data** with each message. These error-detection data are added to each message by the data link layer of the sender on the basis of some mathematical calculations performed on the message (in some cases, error-detection methods are built into the hardware itself). The receiver performs the same mathematical calculations on the message it receives and matches its results against the error-detection data that were transmitted with the message. If the two match, the message is assumed to be correct. If they don't match, an error has occurred. Three well-known **error-detection methods** are: **Parity Check, Cyclic Redundancy Check & Checksum.**

(In your Copy)

Error Correction

Once error has been detected, it must be corrected. The simplest, most effective, least expensive, and most commonly used method for error correction are retransmission. With retransmission, a receiver that detects an error simply asks the sender to retransmit the message until it is received without error. It includes:

1. Automatic Repeat reQuest (ARQ)

Once error has been detected, it must be corrected. The simplest, most effective, least expensive, and most commonly used method for error correction is retransmission. With retransmission, a receiver that detects an error simply asks the sender to retransmit the message until it is received without error. This is often called **Automatic Repeat reQuest (ARQ).** There are three versions of ARQ. They are:

1) **Stop and wait ARQ**
2) **Go back 'N'ARQ**
3) **Selective-Repeat ARQ (retransmission)**

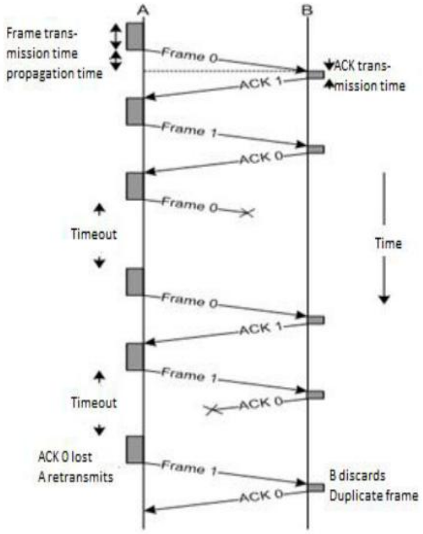
Stop and wait ARQ

It is a technique used to retransmit the data in case of damaged or lost frames. The source station transmits a single frame and then most awaits an acknowledgement from the destination station.

There are two possible errors:

First, the frame that arrive at the destination would be damaged which is detected by receiver by using error detection techniques and discard the frame. After a frame is transmitted a source station waits for an ACK. If no ACK is received by the time that the timer expires and the same frame is send again. The transmitter always maintains a copy of transmitted frame until the time out or ACK is received.

The second type of error is the damage ACK. For the successful reception of frame, if the acknowledgment is damaged in transit which is therefore time out and resend the same frame. To avoid the duplication of frame they are alternatively labeled with ‘0’ and ‘1’ and positive ACK are of the form ACK0 and ACK1. As in sliding window convention, an ACK0 acknowledgement receipt of a frame numbered ‘1’ and indicates that the receiver is ready for a frame number ‘0’. This system is simple but inefficient.



Go Back N ARQ

In this protocol multiple numbers of frames can be transmitted without waiting of ACK. A copy of each transmitted is maintained until the receptive ACK is received.

This is based on the sliding window protocol. If the receiver detects any error in the frame, it sends negative ACK (REJ) for that frame. The receiver will discard all the future incoming frames until the frame error is correctly received. Thus source transmitter must go back and retransmit that frame and all subsequent frames.

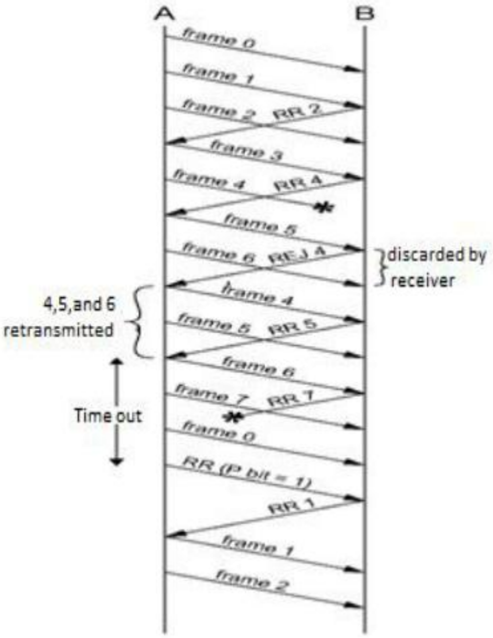
Advantages

1. Sender can send multiple frame at a time
2. More efficient than stop and wait ARQ

Disadvantages

1. Buffer requirement

2. If negative ACK is lost, there will be unnecessary transmission of frames until time out which requires retransmission of such frames.



Selective Repeat ARQ (retransmission)

In this protocol only the rejected frames are transmitted. Suppose F4 is rejected then the subsequent frames are accepted by the receiver and store in the buffer until the valid F4 is received.

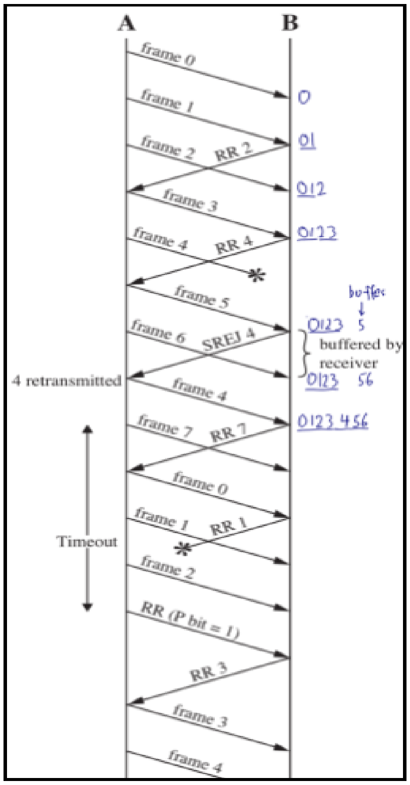
This is more efficient than go back N ARQ because it minimizes the amount of retransmission. But the receiver must maintain the buffering capacity large enough to save the frame until the frame in error is retransmitted and must contain logic for re-inserting that frame in the proper sequence.

Advantage

More efficient than go back NARQ (minimization of retransmission)

Disadvantage

Receiver requires larger buffer size.

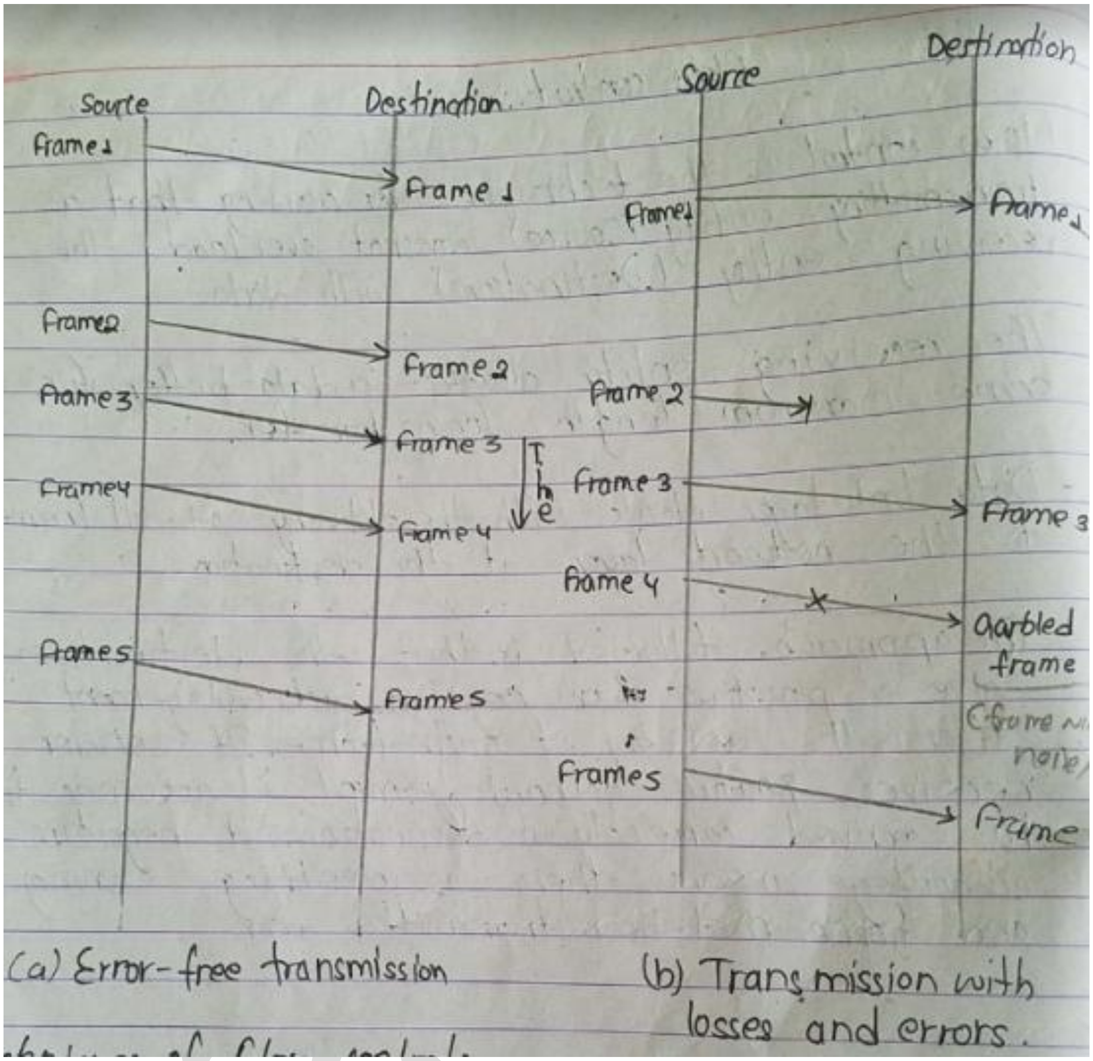


2. **Forward Error Correction**
   Consult your book for this topic

Flow Control

Flow control is the technique for assuring that a transmitting entity (source) does not overload the receiving entity (destination) with data. The receiving entity allocates a data buffer for some maximum length for a transfer. Data link layer deals with the delivery of all frames to the network layer at the destination.

The approach followed is that the destination gives a positive or negative acknowledgement after the delivery of each frame. If sender receives positive ACK, it assumes frame has arrived correctly at destination. A negative ACK means there is something wrong and frame must be re-transmitted.



(a) Error-free transmission

(b) Transmission with losses and errors.

Types of flow control

A. Stop and Wait Flow Control

B. Sliding Window Flow Control

Stop and Wait Flow Control

Stop and wait flow control works under the following assumption:

- Data transmission in one direction only.
- Channel is error free.

The simple form of flow control is known as stop and wait flow control.

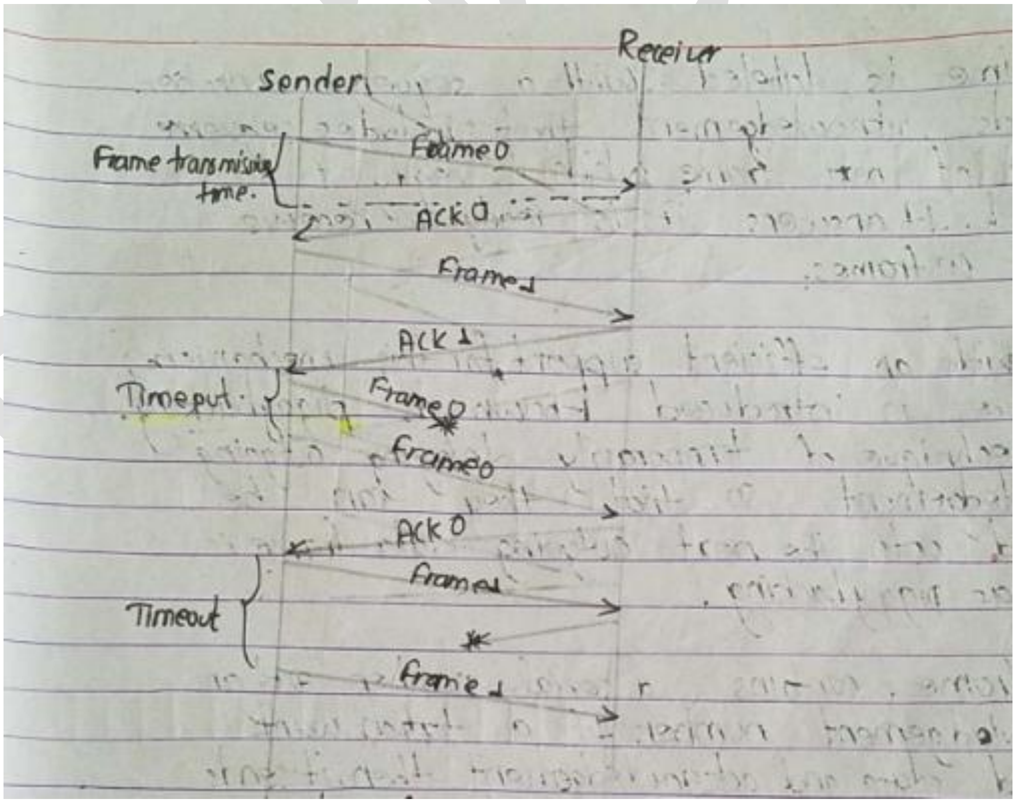
Process

- A source transmit a frame at first, after the destination receives the frame, it indicates its willingness to accept another frame of data by sending back an acknowledgement to the frame just arrived. The source must wait until it receives the acknowledgement before sending the next frame of data. The destination can stop the flow of data simply by holding ACK.

- Receiver sends a positive ACK to sender to transmit the next data frame. Error free channel is assumed. Data frames are transmitted in one direction where each frame is individually acknowledged by the receiver by a separate ACK frame.
- The sender transmits one frame, starts a timer and waits for an ACK from receiver before sending further frames. A time out period is used where frames are not acknowledged by the receiver and are retransmitted automatically by the sender.
- Frames received which are damaged are not acknowledged and are retransmitted by the sender when time out.
- A one bit sequence 0 or 1 is used to distinguish between original data frames and duplicate retransmitted frames which are to be discarded.

Disadvantages

- At a time only one frame can be transmitted.
- No full utilization of the particular channel.
- Single message is sent in different frames so there is the higher chance of error.
- If only one frame collides then again whole frame has to be transmitted.

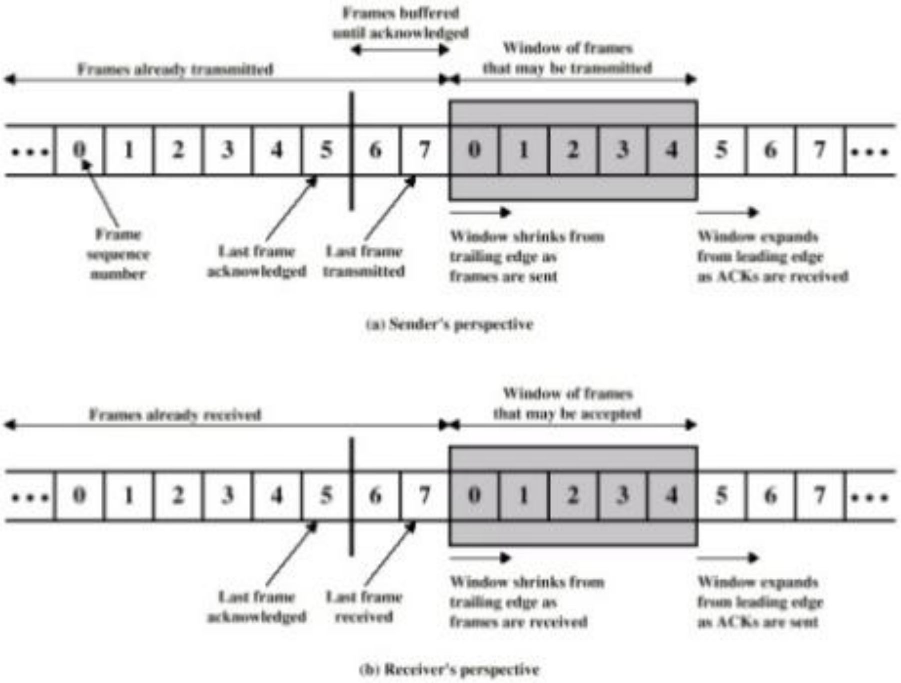


Sliding Window Flow Control

In this mechanism of flow control, the system is full duplex and can transmit multiple frames at a same time.

Working Mechanism

- Two work station ‘A’ and ‘B’ are connected by full duplex link. If two station exchange data they need to maintain two windows; one for transmitting the frame and another for receiving the frame. ‘B’ allocates space for W frames and ‘A’ sends W frames without getting acknowledged.
- To keep the track of which frame has been acknowledged each frame is labeled with a sequence number. ‘B’ sends acknowledgement that includes sequence number of next frame which is ready to be received. It answers ‘B’ is ready to receive next W frames.
- To provide an efficient support for the mechanism, a feature is introduced known as piggybacking. The technique of temporarily delaying outgoing acknowledgement so that they can be backed onto the next outgoing data frame is known as piggybacking.
- Each frame contains a serial number and an acknowledgement number. If a station wants to send data and acknowledgment then it sends both frames so that communication capacity can be saved and utilized. If the station has acknowledgement but not the data, it sends separate acknowledgement frames as RR (Ready to Receive) and RNR (Received Not Ready). If the station has to send the data but no new acknowledgement, then it must repeat ACK sequence number.


Frames buffered until acknowledged
Frames already transmitted
Window of frames that may be transmitted
••• 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 •••
Frame sequence number
Last frame acknowledged
Last frame transmitted
Window shrinks from trailing edge as frames are sent
Window expands from leading edge as ACKs are received
Frames already received
Window of frames that may be accepted
••• 0 1 2 3 4 5 6 7 0 1 2 3 4 5 6 7 •••
Last frame acknowledged
Last frame received
Window shrinks from trailing edge as frames are received
Window expands from leading edge as ACKs are sent

(a) Sender's perspective

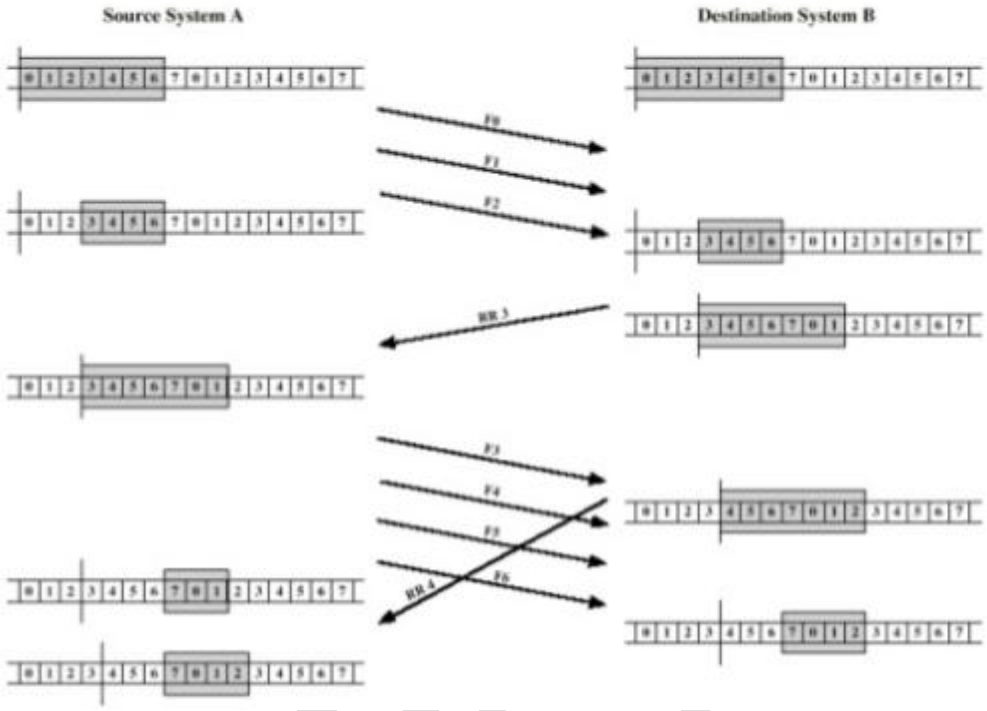
(b) Receiver's perspective

Advantages

- Multiple frames sent at a time
- Better than stop and wait flow control.

Disadvantages

- The system is very complex.

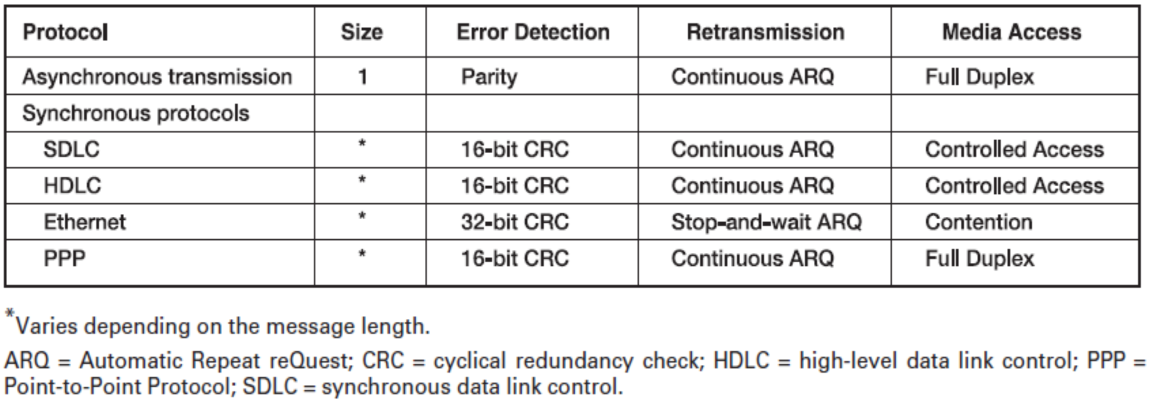


Explanation

1. Initially ‘A’ and ‘B’ have windows indicating that ‘B’ can receive 7 frames and ‘A’ may transmit 7 frames
2. After transmitting three frames F_0, F_1 and F_2 without acknowledgement, ‘A’ has shrunk (reduce) its window to four frames and maintains a copy of three transmitted frames (F_0, F_1 and F_2).
3. The window indicates that ‘A’ can transmit four frames beginning with frame F_3.
4. ‘B’ then transmits RR3 (Receive Ready Frame 3) which mean I have received all frames up to F_2 and I am ready to receive F_3 i.e. I am prepared to receive seven frames beginning with F_3
5. With this acknowledgement, ‘A’ is backup to transmit seven frames beginning with F_3 and ‘A’ discard the buffer frame which has been discarded.
6. A proceed to transmit F_3, F_4, F_5 and F_6.
7. B acknowledge F_3 by sending RR4 and allows transmission of F_4 by the time RR4 reaches A, it has already transmitted F_4, F_5 and F_6 and therefore A open its window to permit sending four frames beginning with F_7.

Data Link Protocols

The different types of protocols used in Datalink layer are listed in the figure below. The figure includes the information about protocol, error detection technique, retransmission technique and media access:



Protocol	Size	Error Detection	Retransmission	Media Access
Asynchronous transmission	1	Parity	Continuous ARQ	Full Duplex
Synchronous protocols				
SDLC	*	16-bit CRC	Continuous ARQ	Controlled Access
HDLC	*	16-bit CRC	Continuous ARQ	Controlled Access
Ethernet	*	32-bit CRC	Stop-and-wait ARQ	Contention
PPP	*	16-bit CRC	Continuous ARQ	Full Duplex

*Varies depending on the message length.

ARQ = Automatic Repeat reQuest; CRC = cyclical redundancy check; HDLC = high-level data link control; PPP = Point-to-Point Protocol; SDLC = synchronous data link control.

Fig: Data Link Layer Protocol Summary

Asynchronous Transmission

Asynchronous transmission is often referred to as *start-stop transmission* because the transmitting computer can transmit a character whenever it is convenient, and the receiving computer will accept that character. It is typically used on point-to-point full-duplex circuits (i.e., circuits that have only two computers on them), so media access control is not a concern.

It is a mode of serial transmission in which the data is transmitted as a continuous stream of bytes separated by starts and stop bits. Data is transmitted from source to destination frame by frame (character by character). Each frames/ character begins with a **start bit** which is binary '**0**' and end with **stop bit** which is binary **'1'**.Data bits are usually followed by **parity bit** for **error checking** .

In asynchronous communication, only about 80 percent of the transmitted bits actually contain data, while the other 20 percent contain signaling information in the form of start bit and stop bit and parity bit. An 8-bit character requires 3 bits of control information (start, stop, and parity bits).The bit of the character are transmitted beginning with LSB (Least Significant Bit)

The transmission is asynchronous at frame level (character level) but is still synchronized at bit level during the reception of data.

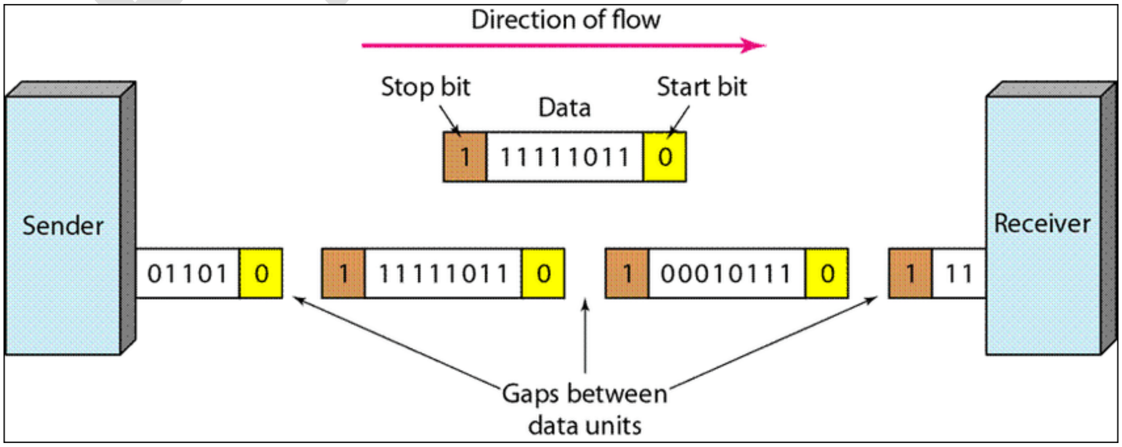
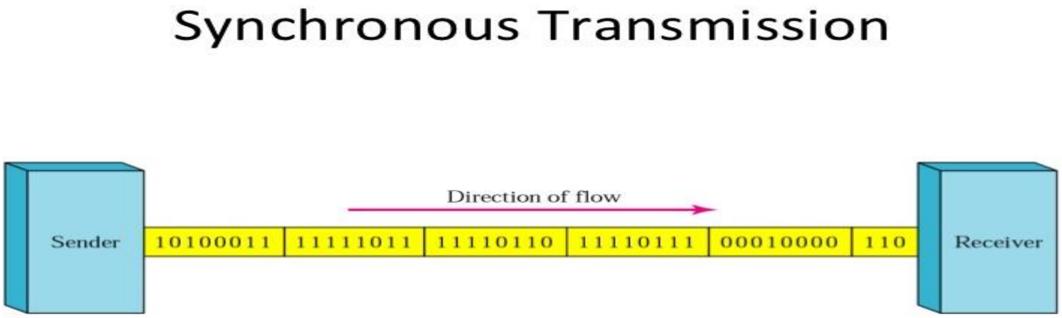


Fig: Asynchronous Transmission

Synchronous Transmission

It is a mode of serial transmission in which continuous stream of data in the form of signal is transmitted accompanied by regular timing signals which are generated by some external clocking mechanism which ensures both sender and receiver are synchronized with each other. The block of data is in the form of bit stream and is transferred without start and stop bit. The transmission is good over short distance communication. It uses preamble and postamble each of 8 bits to leave sufficient space between the blocks.It is more efficient than asynchronous transmission.

The advantage of synchronous transmission is **speed.** With no extra bits or gaps introduced at the source end and remove at the receiving end and by extension with fewer bits to move across the link, synchronous transmission is faster than asynchronous transmission. Thus it is used in high speed applications.

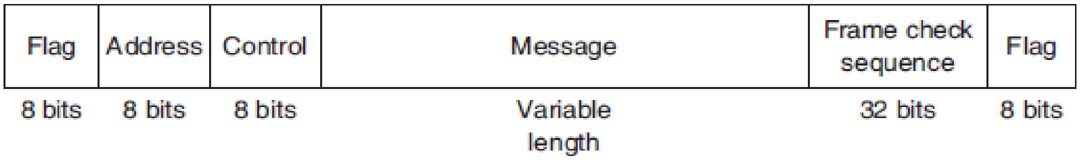


There are many protocols for synchronous transmission. Some of them are:

1) **Synchronous Data Link Control (SDLC)**
2) **High – Level Data Link Control (HDLC)**
3) **Ethernet**
4) **Point-to point Protocol (PPP)**

Synchronous Data Link Control (SDLC)

Synchronous data link control *(SDLC)* is a mainframe protocol developed by IBM in 1972 that is still in use today. It uses a controlled-access media access protocol. Each SDLC frame begins and ends with a special bit pattern (01111110), known as the **flag**. The **address field** identifies the destination. The length of the address field is usually 8 bits but can be set at 16 bits; all computers on the same network must use the same length. The **control field** identifies the kind of frame that is being transmitted, either information or supervisory. An **information frame** is used for the transfer and reception of messages, frame numbering of contiguous frames, and the like. A **supervisory frame** is used to transmit acknowledgments (ACKs and NAKs). The **message field** is of variable length and is the user's message. The **frame check sequence field** is a 32-bit CRC code.



Flag	Address	Control	Message	Frame check sequence	Flag
8 bits	8 bits	8 bits	Variable length	32 bits	8 bits

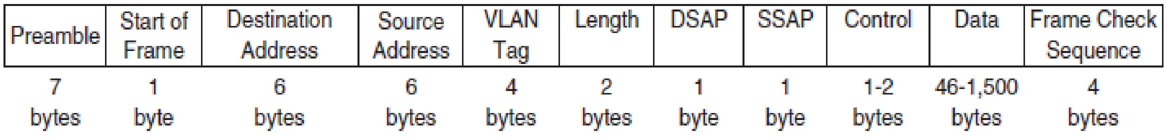
High – Level Data Link Control (HDLC)

High-level data link control (HDLC) is a formal standard developed by the ISO often used in WANs. The current standard for HDLC is ISO 13239. HDLC is essentially the same as SDLC, except that the address and control fields can be longer. HDLC also has several additional benefits such as a larger sliding window for continuous ARQ. It uses a controlled-access media access protocol. HDLC provides both connection-oriented and connectionless service.

Ethernet

Ethernet is a very popular LAN protocol, conceived by Bob Metcalfe in 1973 and developed jointly by Digital, Intel, and Xerox in the 1970s. Since then, Ethernet has been further refined and developed into a formal standard called **IEEE 802.3**ac. There are several versions of Ethernet in use today. Ethernet uses a **contention media access** protocol.

There are several standard versions of Ethernet. Figure below shows an Ethernet 803.3ac frame. The frame starts with a **7-byte preamble** which is a repeating pattern of ones and zeros (10101010). This is followed by a **start of frame delimiter**, which marks the start of the frame. The **destination address** specifies the receiver, whereas the **source address** specifies the sender. The **length** indicates the length in 8-bit bytes of the message portion of the frame. The *VLAN tag* field is an optional 4-byte address field used by virtual LANs (VLANs). The **DSAP destination service access point** and **SSAP source service access point** are used to pass control information between the sender and receiver. These are often used to indicate the type of network layer protocol the packet contains. The **control field** is used to hold the frame sequence numbers and ACKs and NAKs used for error control, as well as to enable the data link layers of communicating computers to exchange other control information. In most cases, the control field is 1-byte long. The maximum length of the message is about 1,500 bytes. The frame ends with a CRC-32 **frame check sequence** used for error detection.

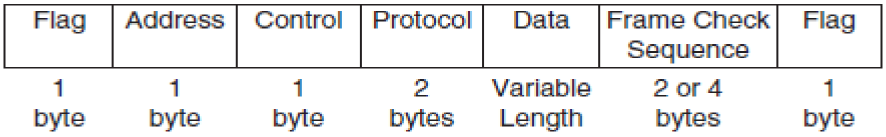


Preamble	Start of Frame	Destination Address	Source Address	VLAN Tag	Length	DSAP	SSAP	Control	Data	Frame Check Sequence
7 bytes	1 byte	6 bytes	6 bytes	4 bytes	2 bytes	1 byte	1 byte	1-2 bytes	46-1,500 bytes	4 bytes

Fig: Ethernet 802.3 frame layout

Point-to point Protocol (PPP)

Point-to-Point Protocol (PPP) was developed in the early 1990s and is often used in WANs. It is designed to transfer data over a point-to-point circuit but provides an address so that it can be used on multipoint circuits. Figure below shows the basic layout of a PPP frame, which is very similar to an SDLC or HDLC frame. The frame starts with a **flag**, and has a one-byte address (which is not used on point-to-point circuits). The **control field** is typically not used. The **protocol field** indicates what type of data packet the frame contains (e.g., an IP packet). The **data field** is variable in length and may be up to 1,500 bytes. The **frame check sequence** is usually a CRC-16, but can be a CRC-32. The frame ends with a **flag**.



Flag	Address	Control	Protocol	Data	Frame Check Sequence	Flag
1 byte	1 byte	1 byte	2 bytes	Variable Length	2 or 4 bytes	1 byte

Fig: PPP frame layout

Transmission Efficiency.

The objective of a data communication network is to move the highest possible volume of accurate information through the network. The higher the volume, the greater the resulting network’s efficiency and the lower the cost. Network efficiency is affected by characteristics of the circuits such as error rates and maximum transmission speed, as well as by the speed of transmitting and receiving equipment, the error-detection and control methodology, and the protocol used by the data link layer. Each protocol we discussed uses some bits or bytes to delineate the start and end of each message and to control error. These bits and bytes are necessary for the transmission to occur, but they are not part of the message. They add no value to the user, but they count against the total number of bits that can be transmitted. Each communication protocol has both information bits and overhead bits. **Information bits** are those used to convey the user’s meaning. **Overhead bits** are used for purposes such as error checking and marking the start and end of characters and packets.

Transmission efficiency is defined as the total number of information bits (i.e., bits in the message sent by the user) divided by the total bits in transmission (i.e., information bits plus overhead bits).

For example, let’s calculate the transmission efficiency of asynchronous transmission. Assume we are using 7-bit ASCII. We have 1 bit for parity, plus 1 start bit and 1 stop bit. Therefore, there are 7 bits of information in each letter, but the total bits per letter is 10 (7 + 3). The efficiency of the asynchronous transmission system is 7 bits of information divided by 10 total bits, or 70%. We can improve efficiency by reducing the number of overhead bits in each message or by increasing the number of information bits. For example, if we remove the stop bits from asynchronous transmission, efficiency increases to 7/9, or 77.8%.

The same basic formula can be used to calculate the efficiency of synchronous transmission. For example, suppose we are using SDLC. The number of information bits is calculated by determining how many information characters are in the message. If the message portion of the frame contains 100 information characters and we are using an 8-bit code, then there are 100×8=800 bits of information. The total number of bits is the 800 information bits plus the overhead bits that are inserted for delineation and error control. Figure of SDLC above shows that SDLC has a beginning flag (8 bits), an address (8 bits), a control field (8 bits), a frame check sequence (assume we use a CRC-32 with 32 bits), and an ending flag (8 bits). This is a total of 64 overhead bits; thus, efficiency is 800/(800 + 64) = 92.6%. This example shows that synchronous networks usually are more efficient than asynchronous networks and some protocols are more efficient than others.

The general rule is that the larger the message field, the more efficient the protocol.