UNIT II

Data Link Layer Design Issues

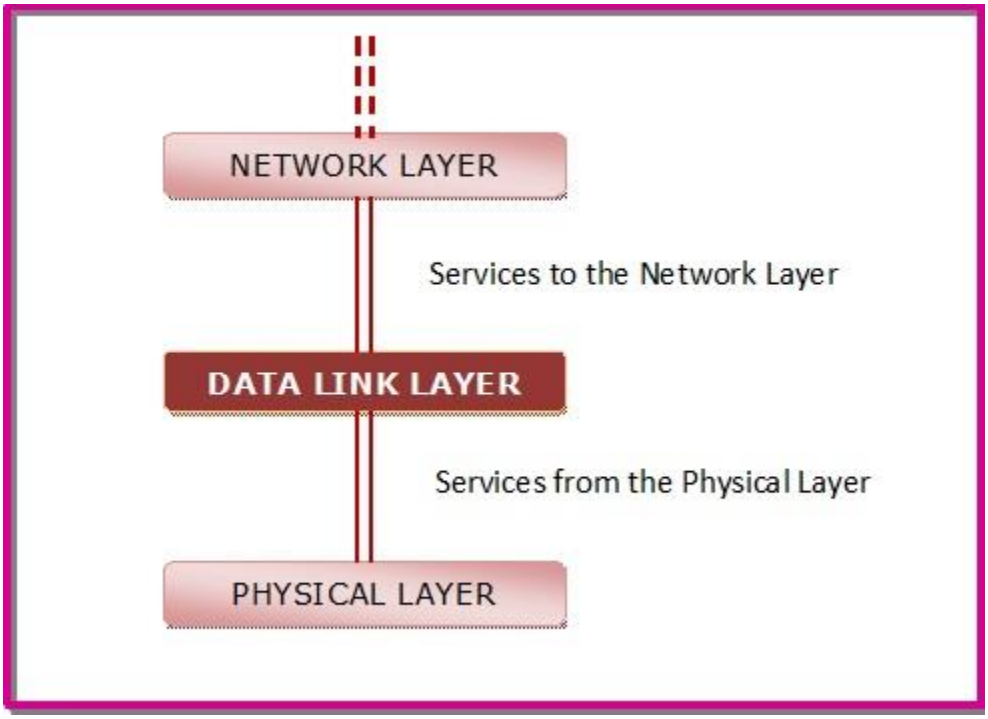
The data link layer in the OSI (Open System Interconnections) Model, is in between the physical layer and the network layer. This layer converts the raw transmission facility provided by the physical layer to a reliable and error-free link.

The main functions and the design issues of this layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

Unacknowledged Connectionless Service (LLC 1) :
Unacknowledged Connectionless Service, as the name suggests, is a service in which data frames are sent or transmitted from destination to source machine without any acknowledgment and without connection established among source and destination machine In this, Unacknowledged Connection service comprises two words i.e. unacknowledged and connectionless service.

- The source machine sends or transmits data frames to the destination machine. But in return, the destination machine does not provide any acknowledgment to the source machine, so this service is known as unacknowledged service. Along with this, there is no connection established between the source and destination machine, therefore it is known as connectionless service. So, combined it is known as unacknowledged connectionless service.

Acknowledged Connectionless Service (LLC 3) :
Acknowledged Connectionless Service, as the name suggests, is a service in which data frames are sent or transmitted from destination to source machine with acknowledgment and without connection established among source and destination machine. In this, Acknowledged Connection service comprises two words i.e., Acknowledged and connectionless service. The source machine sends or transmits data frames to the destination machines and in return, the destination machine provides an acknowledgment to the source machine, so this service is known as acknowledged service. Along with this, there is no connection established between the source and destination machine, therefore it is known as connectionless service. So, combined it is known as acknowledged connectionless service. It does not support any multicast or broadcast addressing. It is a rarely used service.

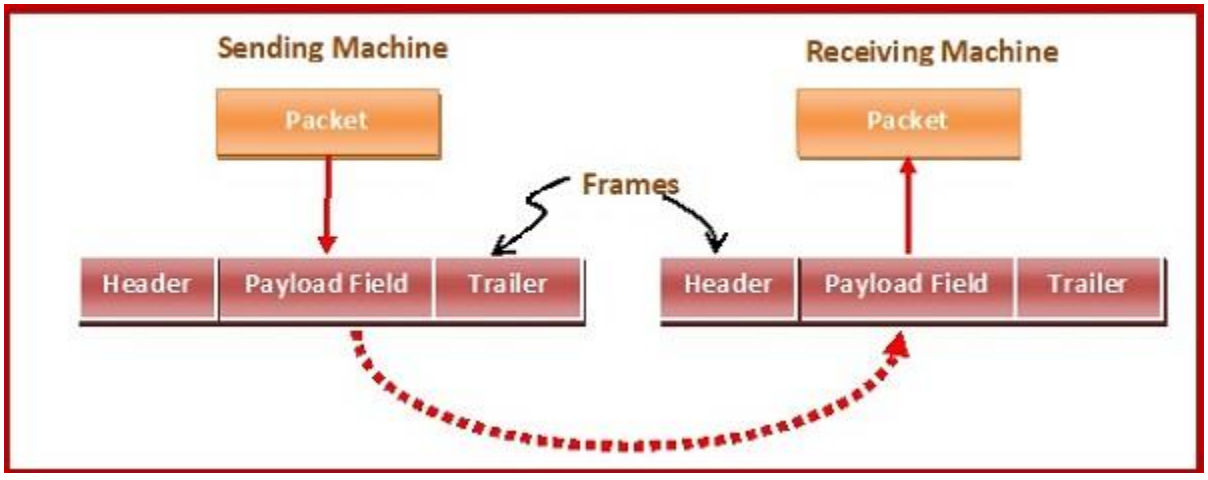
Acknowledged Connection-Oriented Service is basically a technique that is typically used to transport and send data at session layer. The data streams or packets are transferred or delivered to receiver in a similar order in which they have seen transferred by sender. It is actually a data transfer method among two devices or computers in a different network, that is designed and developed after telephone system. Whenever a network implements this service, it sends or transfers data or message from sender or source to receiver or destination in correct order and manner.

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

Feedback – based Flow Control :
In this control technique, sender simply transmits data or information or frame to receiver, then receiver transmits data back to sender and also allows sender to transmit more amount of data or tell sender about how receiver is processing or doing. This simply means that sender transmits data or frames after it has received acknowledgments from user.

Rate – based Flow Control :
In this control technique, usually when sender sends or transfer data at faster speed to receiver and receiver is not being able to receive data at the speed, then mechanism known as built-in mechanism in protocol will just limit or restricts overall rate at which data or information is being transferred or transmitted by sender without any feedback or acknowledgment from receiver

Error Detection and Correction in Data link Layer

Data-link layer uses error control techniques to ensure that frames, i.e. bit streams of data, are transmitted from the source to the destination with a certain extent of accuracy.

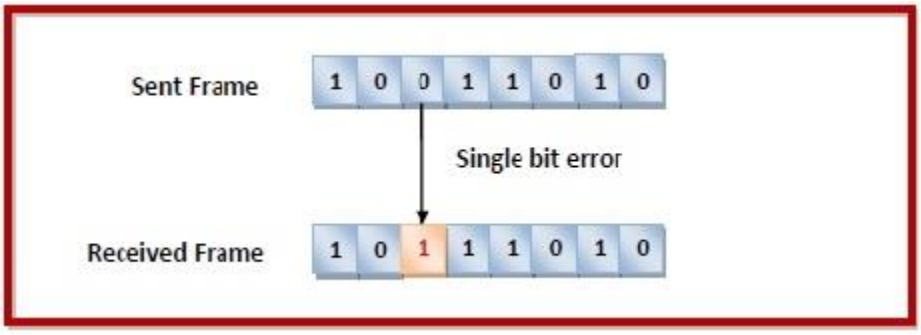
Errors

When bits are transmitted over the computer network, they are subject to get corrupted due to interference and network problems. The corrupted bits leads to spurious data being received by the destination and are called errors.

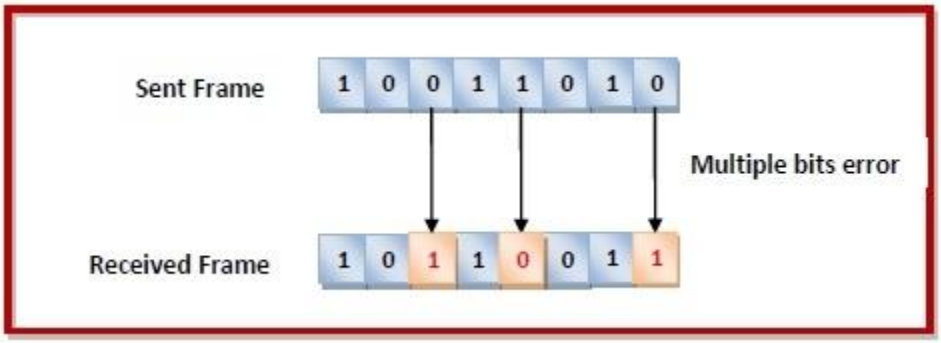
Types of Errors

Errors can be of three types, namely single bit errors, multiple bit errors, and burst errors.

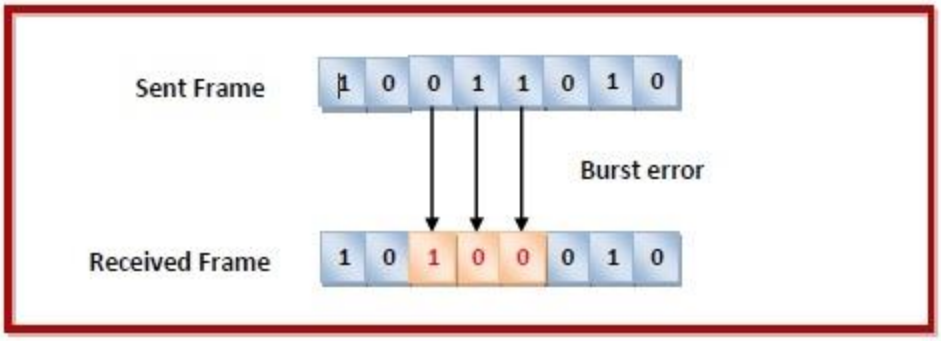
- **Single bit error** − In the received frame, only one bit has been corrupted, i.e. either changed from 0 to 1 or from 1 to 0.



- **Multiple bits error** − In the received frame, more than one bits are corrupted.



- **Burst error** − In the received frame, more than one consecutive bits are corrupted.



Error Control

Error control can be done in two ways

- **Error detection** − Error detection involves checking whether any error has occurred or not. The number of error bits and the type of error does not matter.
- **Error correction** − Error correction involves ascertaining the exact number of bits that has been corrupted and the location of the corrupted bits.

For both error detection and error correction, the sender needs to send some additional bits along with the data bits. The receiver performs necessary checks based upon the additional redundant bits. If it finds that the data is free from errors, it removes the redundant bits before passing the message to the upper layers.

Error Detection Techniques

There are three main techniques for detecting errors in frames: Parity Check, Checksum and Cyclic Redundancy Check (CRC).

Parity Check

The parity check is done by adding an extra bit, called parity bit to the data to make a number of 1s either even in case of even parity or odd in case of odd parity.

While creating a frame, the sender counts the number of 1s in it and adds the parity bit in the following way

- In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
- In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

On receiving a frame, the receiver counts the number of 1s in it. In case of even parity check, if the count of 1s is even, the frame is accepted, otherwise, it is rejected. A similar rule is adopted for odd parity check.

The parity check is suitable for single bit error detection only.

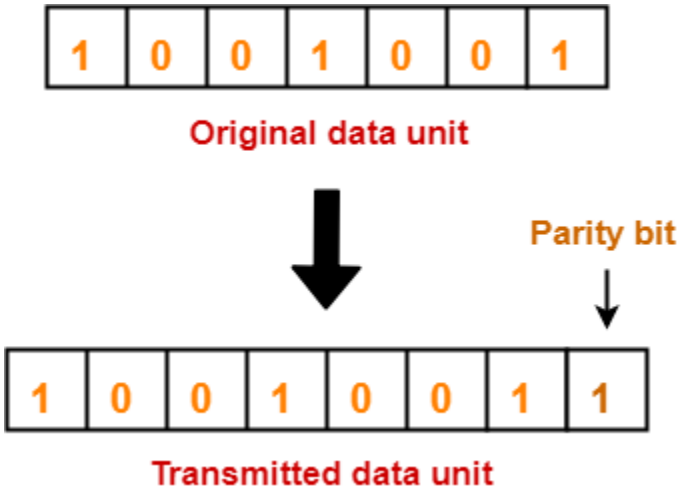
EXAMPLES

Consider the data unit to be transmitted is 1001001 and even parity is used.

Then,

At Sender Side-

- **Total number of 1's in the data unit is counted.**
- **Total number of 1's in the data unit = 3.**
- **Clearly, even parity is used and total number of 1's is odd.**
- **So, parity bit = 1 is added to the data unit to make total number of 1's even.**
- **Then, the code word 10010011 is transmitted to the receiver.**



At Receiver Side-

- **After receiving the code word, total number of 1's in the code word is counted.**
- **Consider receiver receives the correct code word = 10010011.**
- **Even parity is used and total number of 1's is even.**
- **So, receiver assumes that no error occurred in the data during the transmission.**

Checksum

In this error detection scheme, the following procedure is applied

- Data is divided into fixed sized frames or segments.
- The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.
- If the result is zero, the received frames are accepted; otherwise, they are discarded.

EXAMPLE

Consider the data unit to be transmitted is-

10011001111000100010010010000100

Consider 8 bit checksum is used.

Step-01:

At sender side,

The given data unit is divided into segments of 8 bits as-

10011001	11100010	00100100	10000100

Now, all the segments are added and the result is obtained as-

- 10011001 + 11100010 + 00100100 + 10000100 = 1000100011
- Since the result consists of 10 bits, so extra 2 bits are wrapped around.
- 00100011 + 10 = 00100101 (8 bits)
- Now, 1's complement is taken which is 11011010.
- Thus, checksum value = 11011010

Step-02:

- The data along with the checksum value is transmitted to the receiver.

Step-03:

At receiver side,

- The received data unit is divided into segments of 8 bits.
- All the segments along with the checksum value are added.
- Sum of all segments + Checksum value = 00100101 + 11011010 = 11111111
- Complemented value = 00000000
- Since the result is 0, receiver assumes no error occurred in the data and therefore accepts it

Cyclic Redundancy Check (CRC)

Cyclic Redundancy Check (CRC) involves binary division of the data bits being sent by a predetermined divisor agreed upon by the communicating system. The divisor is generated using polynomials.

- Here, the sender performs binary division of the data segment by the divisor. It then appends the remainder called CRC bits to the end of the data segment. This makes the resulting data unit exactly divisible by the divisor.
- The receiver divides the incoming data unit by the divisor. If there is no remainder, the data unit is assumed to be correct and is accepted. Otherwise, it is understood that the data is corrupted and is therefore rejected.

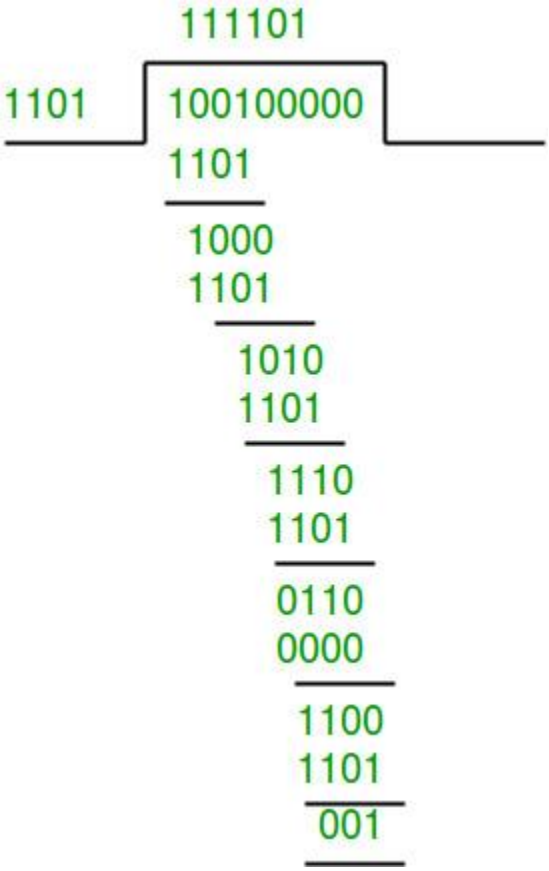
EXAMPLE

Problem-01:

Data word to be sent - 100100

Key - 1101 [Or generator polynomial $x^3 + x^2 + 1$]

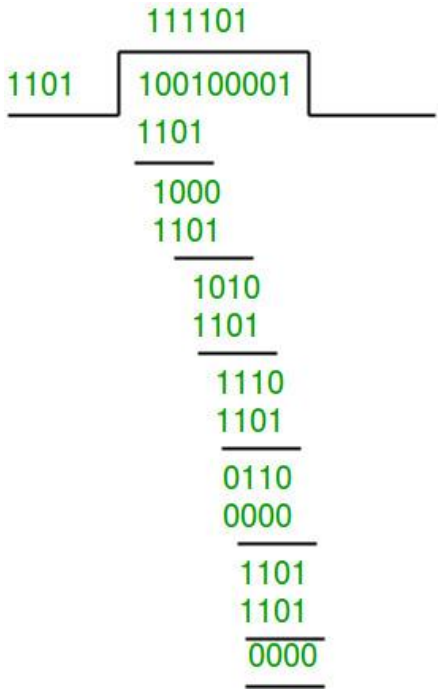
Sender Side:



Therefore, the remainder is 001 and hence the encoded data sent is 100100001.

Receiver Side:

Code word received at the receiver side 100100001



Therefore, the remainder is all zeros. Hence, the

data received has no error.

Error Correction Techniques

Error correction techniques find out the exact number of bits that have been corrupted and as well as their locations. There are two principle ways

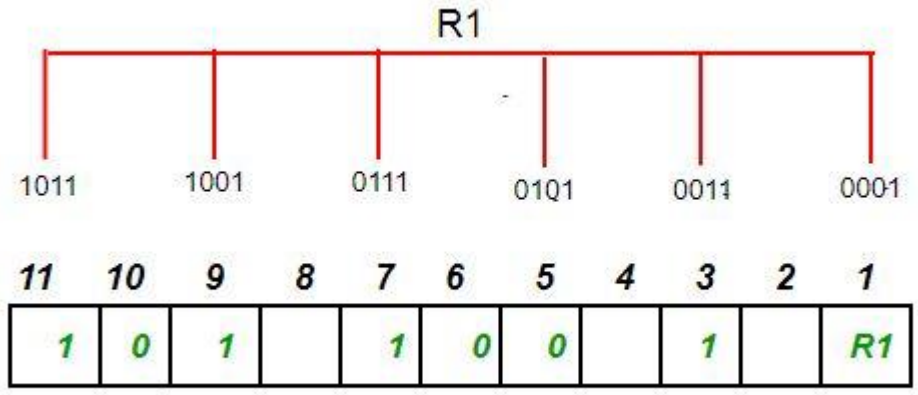
- **Backward Error Correction (Retransmission)** − If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low relative to the requirements of the application.
- **Forward Error Correction** − If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth required for retransmission. It is inevitable in real-time systems. However, if there are too many errors, the frames need to be retransmitted.

The four main error correction codes are

- Hamming Codes

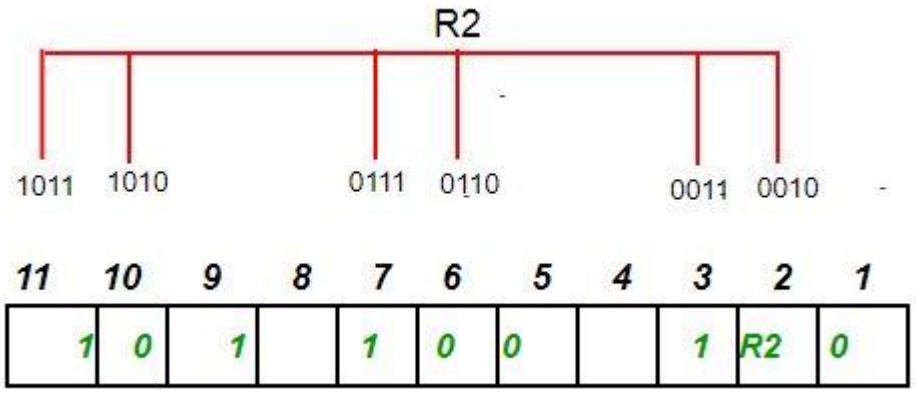
Determining the Parity bits –

1. R1 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the least significant position.
   R1: bits 1, 3, 5, 7, 9, 11



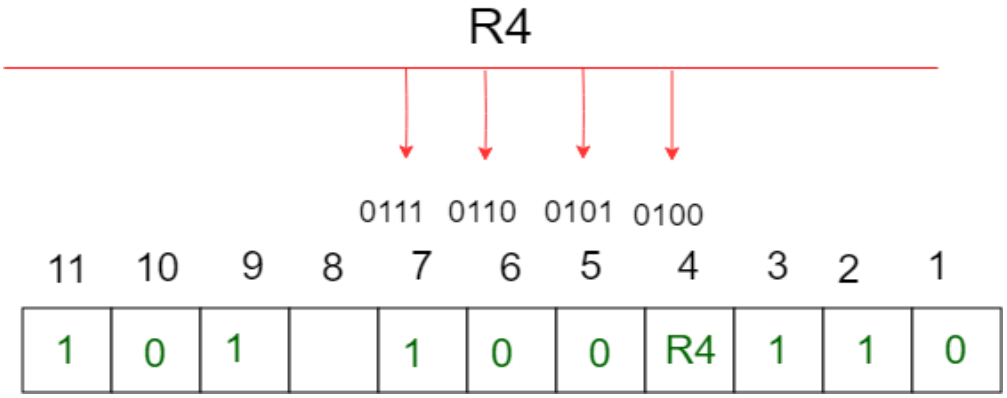
   To find the redundant bit R1, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R1 is an even number the value of R1 (parity bit's value) = 0

2. R2 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the second position from the least significant bit.
   R2: bits 2,3,6,7,10,11



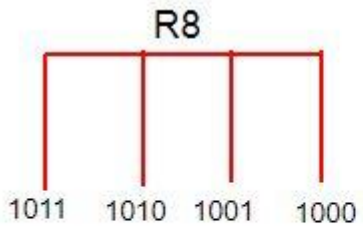
To find the redundant bit R2, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R2 is odd the value of R2(parity bit's value)=1

3. R4 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the third position from the least significant bit.
   R4: bits 4, 5, 6, 7



To find the redundant bit R4, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R4 is odd the value of R4(parity bit's value) = 1

4. R8 bit is calculated using parity check at all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit.
   R8: bit 8,9,10,11



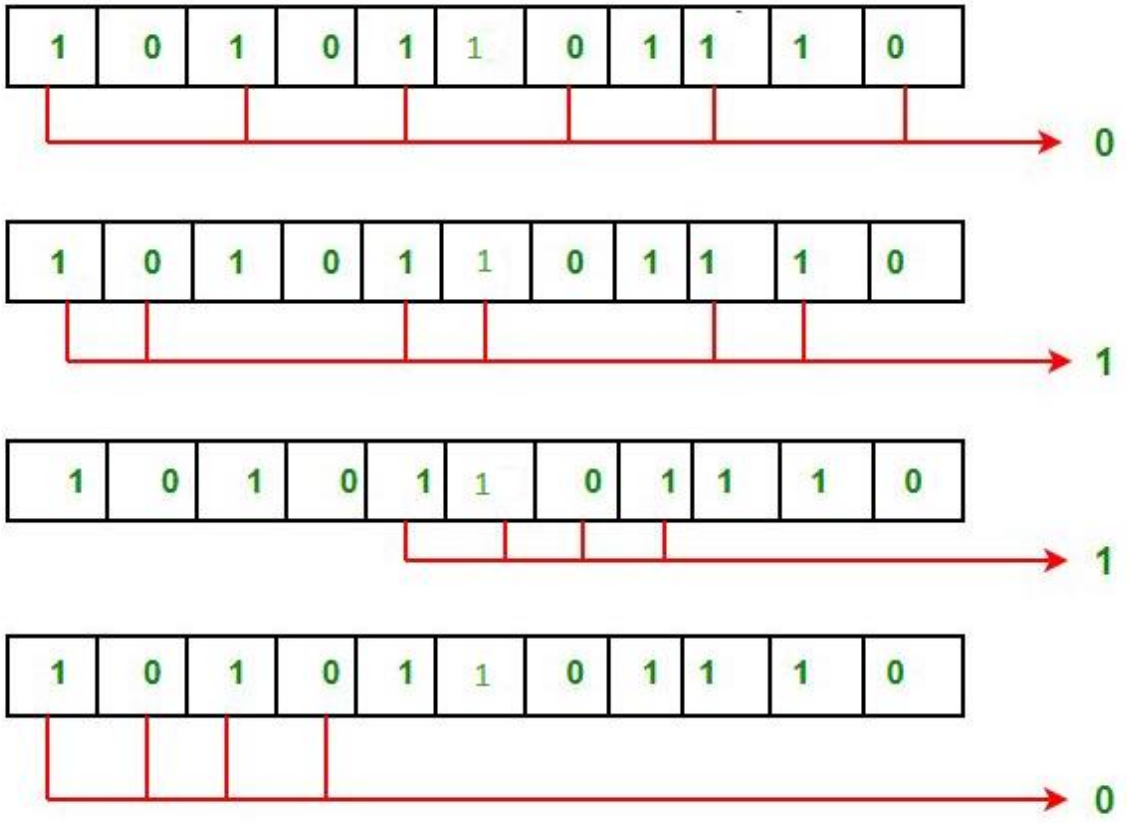
11	10	9	8	7	6	5	4	3	2	1
1	0	1	R8	1	0	0	1	1	1	0

To find the redundant bit R8, we check for even parity. Since the total number of 1's in all the bit positions corresponding to R8 is an even number the value of R8(parity bit's value)=0.

Thus, the data transferred is:

11	10	9	8	7	6	5	4	3	2	1
1	0	1	0	1	0	0	1	1	1	0

Error detection and correction –
Suppose in the above example the 6th bit is changed from 0 to 1 during data transmission, then it gives new parity values in the binary number:



The bits give the binary number as 0110 whose decimal representation is 6. Thus, the bit 6 contains an error. To correct the error the 6th bit is changed from 1 to 0.

- **Binary Convolution Code**

In convolutional codes, the message comprises of data streams of arbitrary length and a sequence of output bits are generated by the sliding application of Boolean functions to the data stream.

In block codes, the data comprises of a block of data of a definite length.

However, in convolutional codes, the input data bits are not divided into block but are instead fed as streams of data bits, which convolve to output bits based upon the logic function of the encoder.

- **Reed – Solomon Code**

Reed - Solomon error correcting codes are one of the oldest codes that were introduced in 1960s by Irving S. Reed and Gustave Solomon.

It is a subclass of non - binary BCH codes.

BCH codes (Bose-Chaudhuri-Hocquenghem codes) are cyclic ECCs that are constructed using polynomials over data blocks.

A Reed - Solomon encoder accepts a block of data and adds redundant bits (parity bits) before transmitting it over noisy channels.

On receiving the data, a decoder corrects the error depending upon the code characteristics.

- **Low-Density Parity-Check Code**

The final error-correcting code we will cover is the **LDPC (Low-Density Parity Check) code.**

LDPC codes are linear block codes that were invented by Robert Gallagher in his doctoral thesis (Gallagher, 1962).

In an LDPC code, each output bit is formed from only a fraction of the input bits.

This leads to a matrix representation of the code that has a low density of 1s, hence the name for the code.

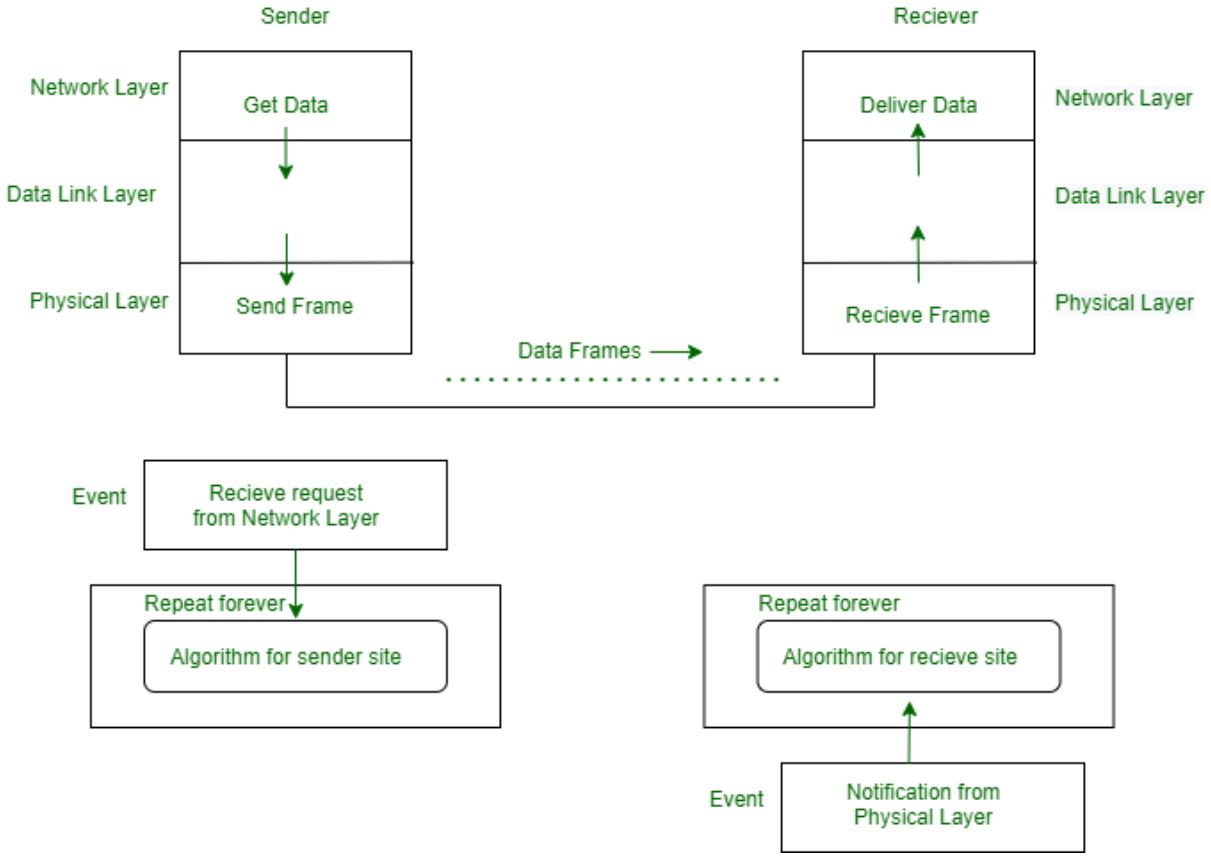
The received codewords are decoded with an approximation algorithm that iteratively improves on a best fit of the received data to a legal codeword.

Simplest Protocol –

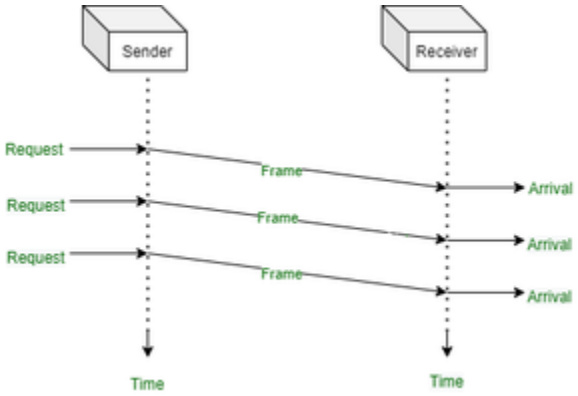
We consider here that the receiver can maintain any frame received with insignificant processing time. The receiver's data link layer immediately removes the header from the frame and assigns the data packet to its network layer, which can also accept the packet immediately. That is to say, the receiver can never be overwhelmed with forthcoming frames.

Design :

The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer(receiver site) receives a frame from its physical layer, extracts data from the frame, and convey the data to its network layer. The data link layers of the sender and receiver provide communication/transmission services for their network layers. The data link layers utilization the services provided by their physical layers for the physical transmission of bits.



- **Flow Diagram :**
  This Flow Diagram shows an example of communication using the simplest protocol. It is very straightforward. The sender sends a series of frames without further consideration about the receiver. Let's take an example, three frames will send from the sender, and three frames received by receivers. Bear in mind the data frames are shown by tilted boxes; the height of the box defines the transmission time difference between the first bit and the last bit in the frame.

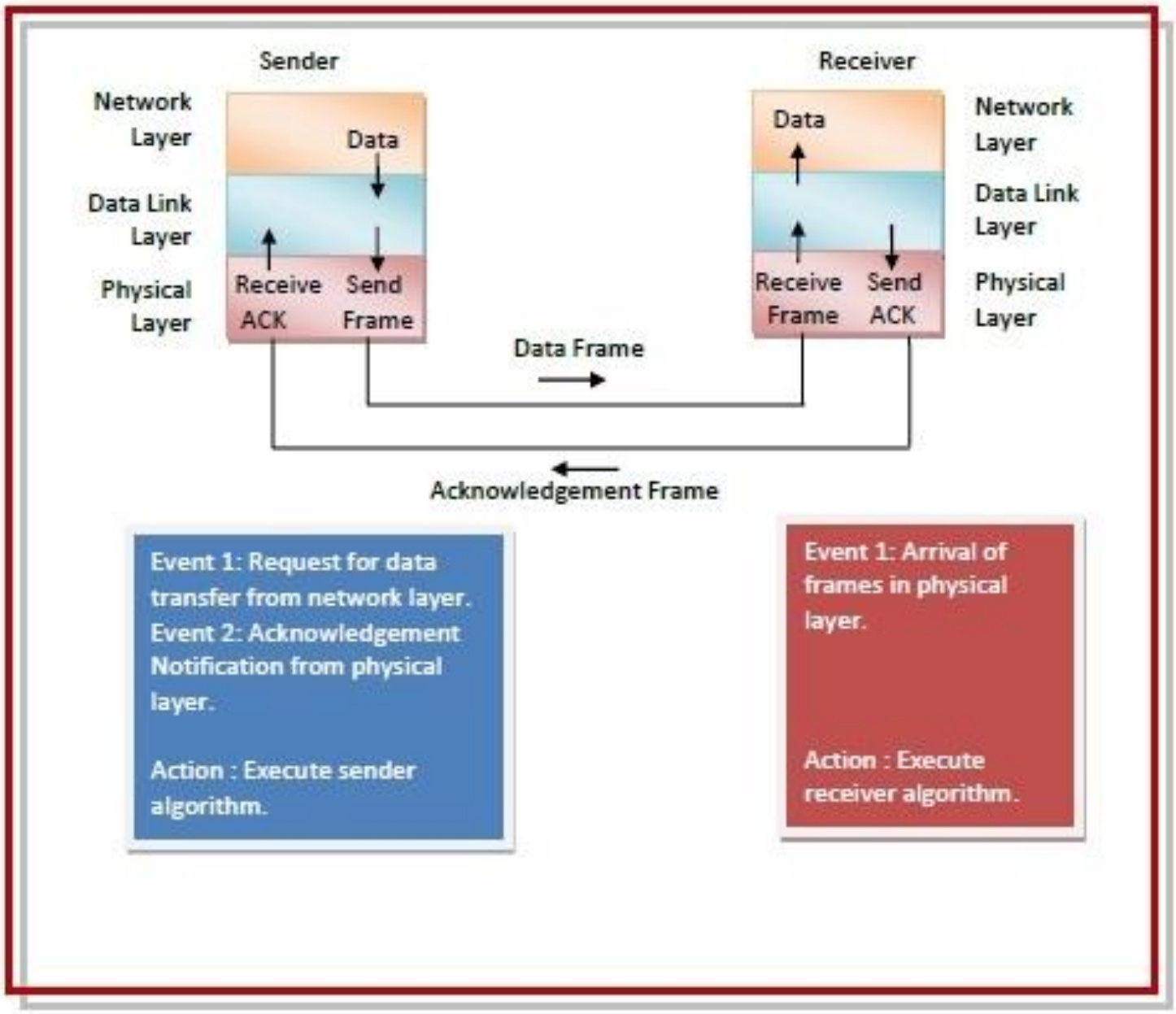


A Simplex Stop-and-Wait Protocol for an Error-Free Channel

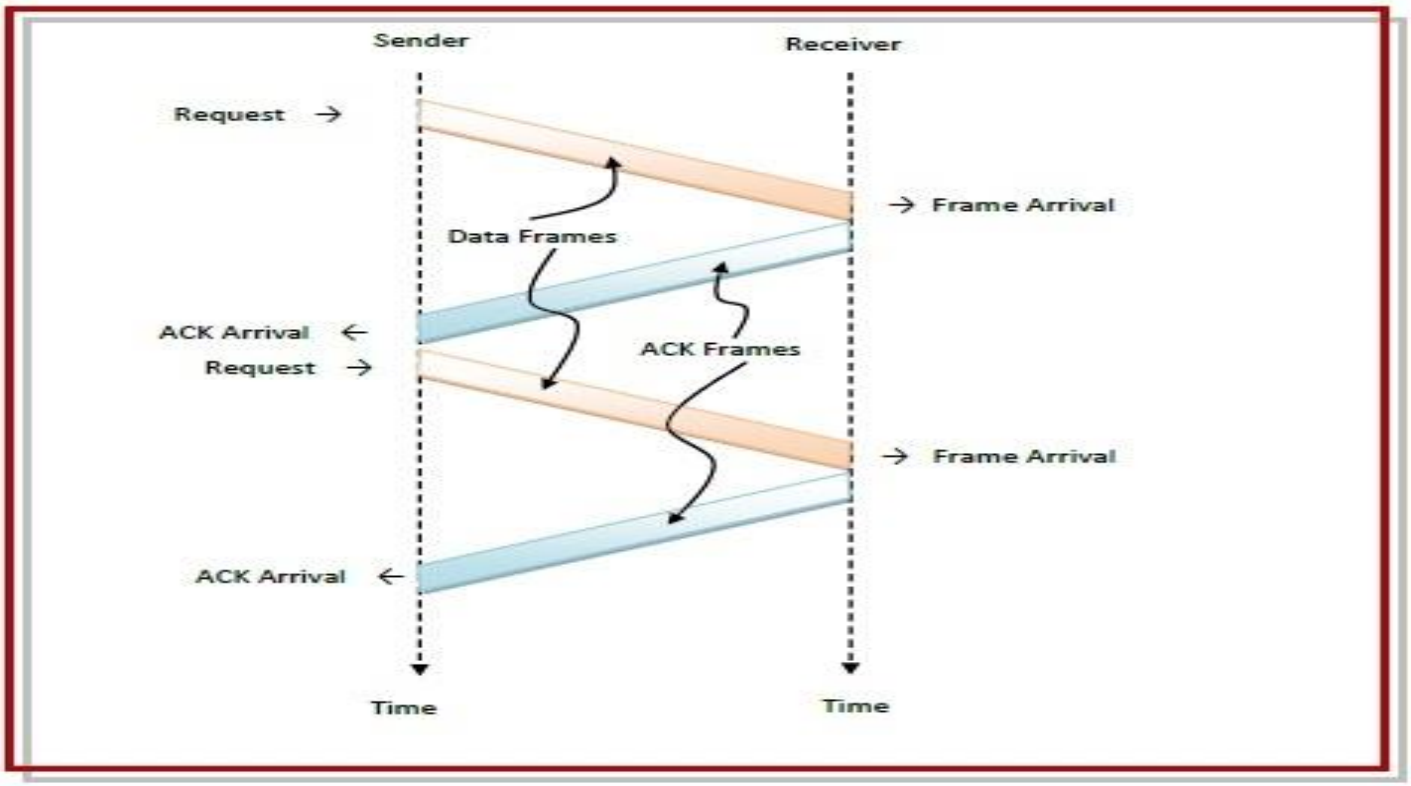
Stop – and – Wait protocol is data link layer protocol for transmission of frames over noiseless channels. It provides unidirectional data transmission with flow control facilities but without error control facilities.

Design

- **Sender Site**: The data link layer in the sender site waits for the network layer for a data packet. It then checks whether it can send the frame. If it receives a positive notification from the physical layer, it makes frames out of the data and sends it. It then waits for an acknowledgement before sending the next frame.
- **Receiver Site**: The data link layer in the receiver site waits for a frame to arrive. When it arrives, the receiver processes it and delivers it to the network layer. It then sends an acknowledgement back to the sender.



Flow Diagram **The following flow diagram depicts communication via simplex stop – and – wait protocol for noiseless channel:**



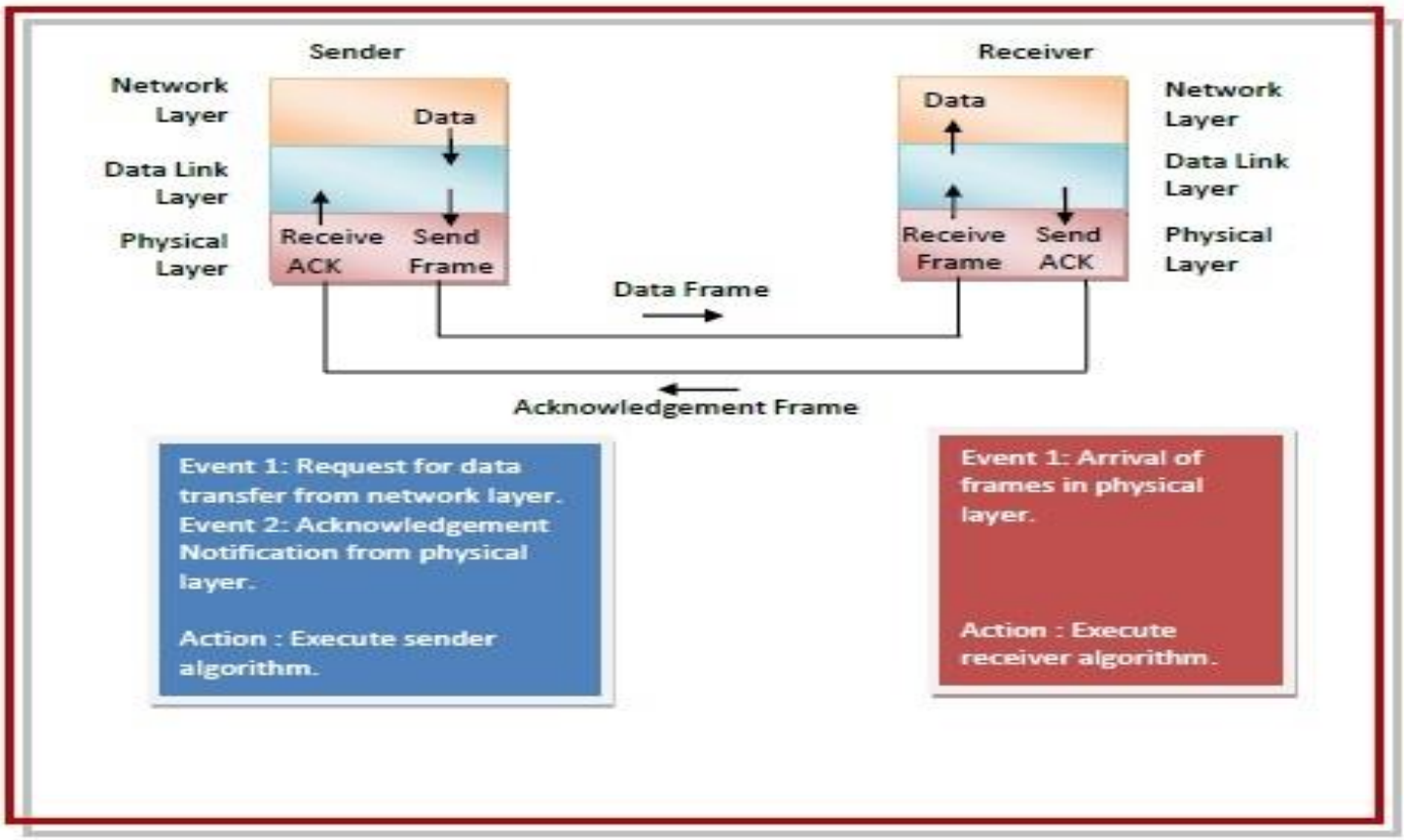
A Simplex Stop-and-Wait Protocol for a Noisy Channel

Simplex Stop – and – Wait protocol for noisy channel is data link layer protocol for data communications with error control and flow control mechanisms. It is popularly known as Stop – and –Wait Automatic Repeat Request (Stop – and –Wait ARQ) protocol. It adds error control facilities to Stop – and – Wait protocol.

This protocol takes into account the facts that the receiver has a finite processing speed and that frames may get corrupted while transmission. If data frames arrive at the receiver's end at a rate which is greater than its rate of processing, frames can be dropped out. Also, frames may get corrupted or entirely lost when they are transmitted via network channels. So, the receiver sends an acknowledgment for each valid frame that it receives. The sender sends the next frame only when it has received a positive acknowledgment from the receiver that it is available for further data processing. Otherwise, it waits for a certain amount of time and then resends the frame.

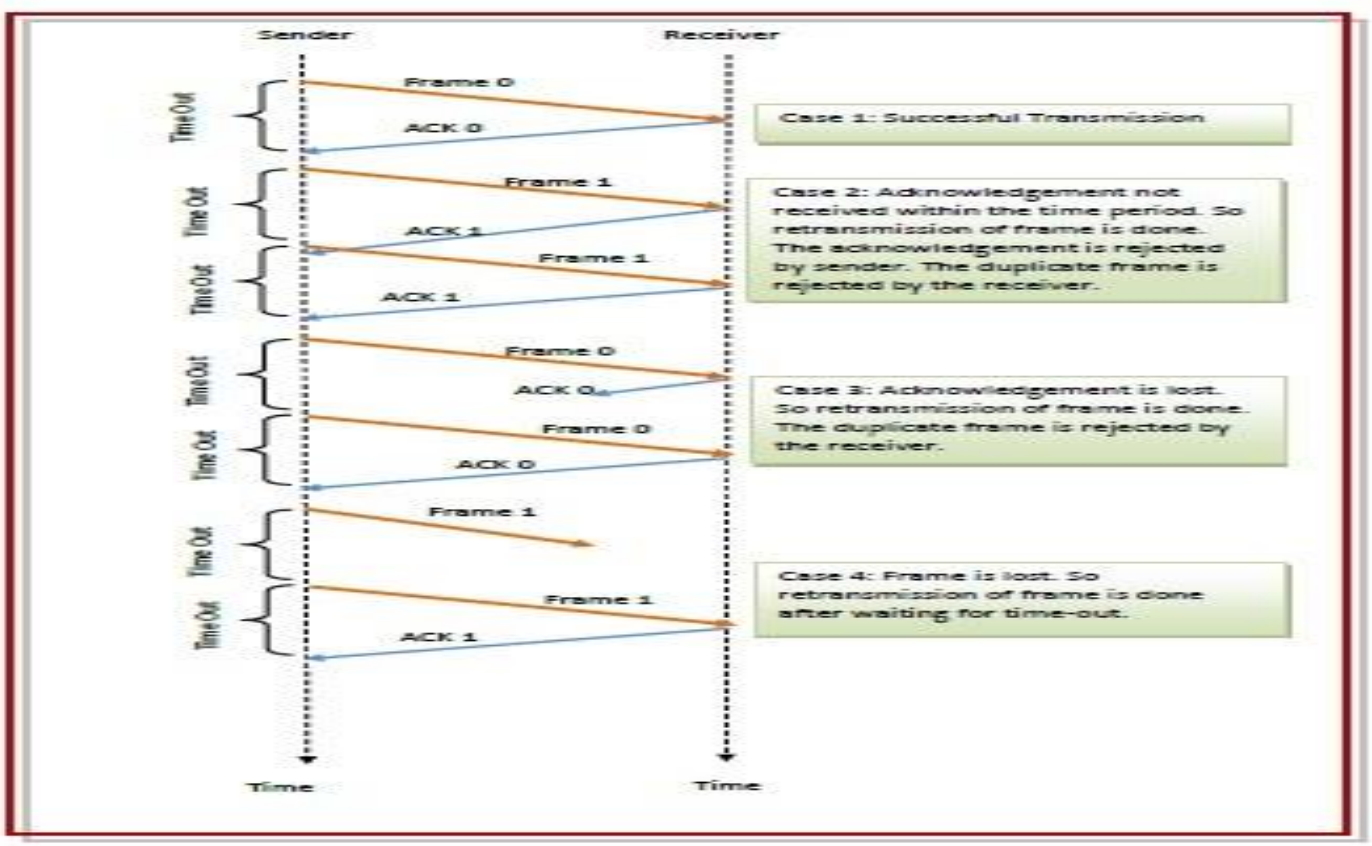
Design

- **Sender Site** − At the sender site, a field is added to the frame to hold a sequence number. If data is available, the data link layer makes a frame with the certain sequence number and sends it. The sender then waits for arrival of acknowledgment for a certain amount of time. If it receives a positive acknowledgment for the frame with that sequence number within the stipulated time, it sends the frame with next sequence number. Otherwise, it resends the same frame.
- **Receiver Site** − The receiver also keeps a sequence number of the frames expected for arrival. When a frame arrives, the receiver processes it and checks whether it is valid or not. If it is valid and its sequence number matches the sequence number of the expected frame, it extracts the data and delivers it to the network layer. It then sends an acknowledgement for that frame back to the sender along with its sequence number



Flow Diagram

The following flow diagram depicts communication via simplex stop – and – wait ARQ protocol for noisy channel −



A One-Bit Sliding Window Protocol

Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol. In these protocols, the sender has a buffer called the sending window and the receiver has buffer called the receiving window.

In one – bit sliding window protocol, the size of the window is 1. So the sender transmits a frame, waits for its acknowledgment, then transmits the next frame. Thus it uses the concept of stop and waits for the protocol. This protocol provides for full – duplex communications. Hence, the acknowledgment is attached along with the next data frame to be sent by piggybacking.

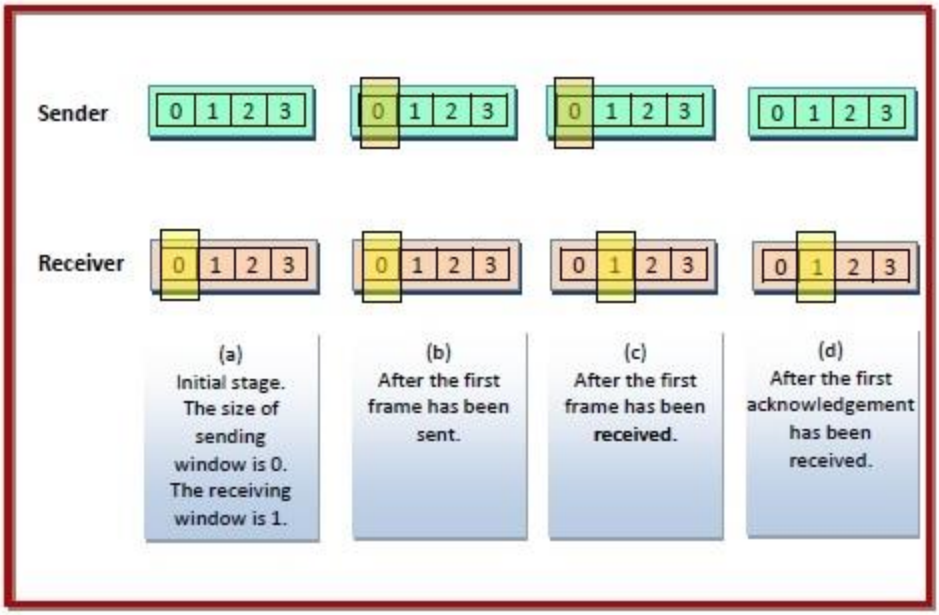
Working Principle

The data frames to be transmitted additionally have an acknowledgment field, *ack* field that is of a few bits length. The *ack* field contains the sequence number of the last frame received without error. If this sequence number matches with the sequence number of the frame to be sent, then it is inferred that there is no error and the frame is transmitted. Otherwise, it is inferred that there is an error in the frame and the previous frame is retransmitted.

Since this is a bi-directional protocol, the same algorithm applies to both the communicating parties.

Illustrative Example

The following diagram depicts a scenario with sequence numbers 0, 1, 2, 3, 0, 1, 2 and so on. It depicts the sliding windows in the sending and the receiving stations during frame transmission.



sliding Window Protocol

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

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

Types of Sliding Window Protocol

Sliding window protocol has two types:

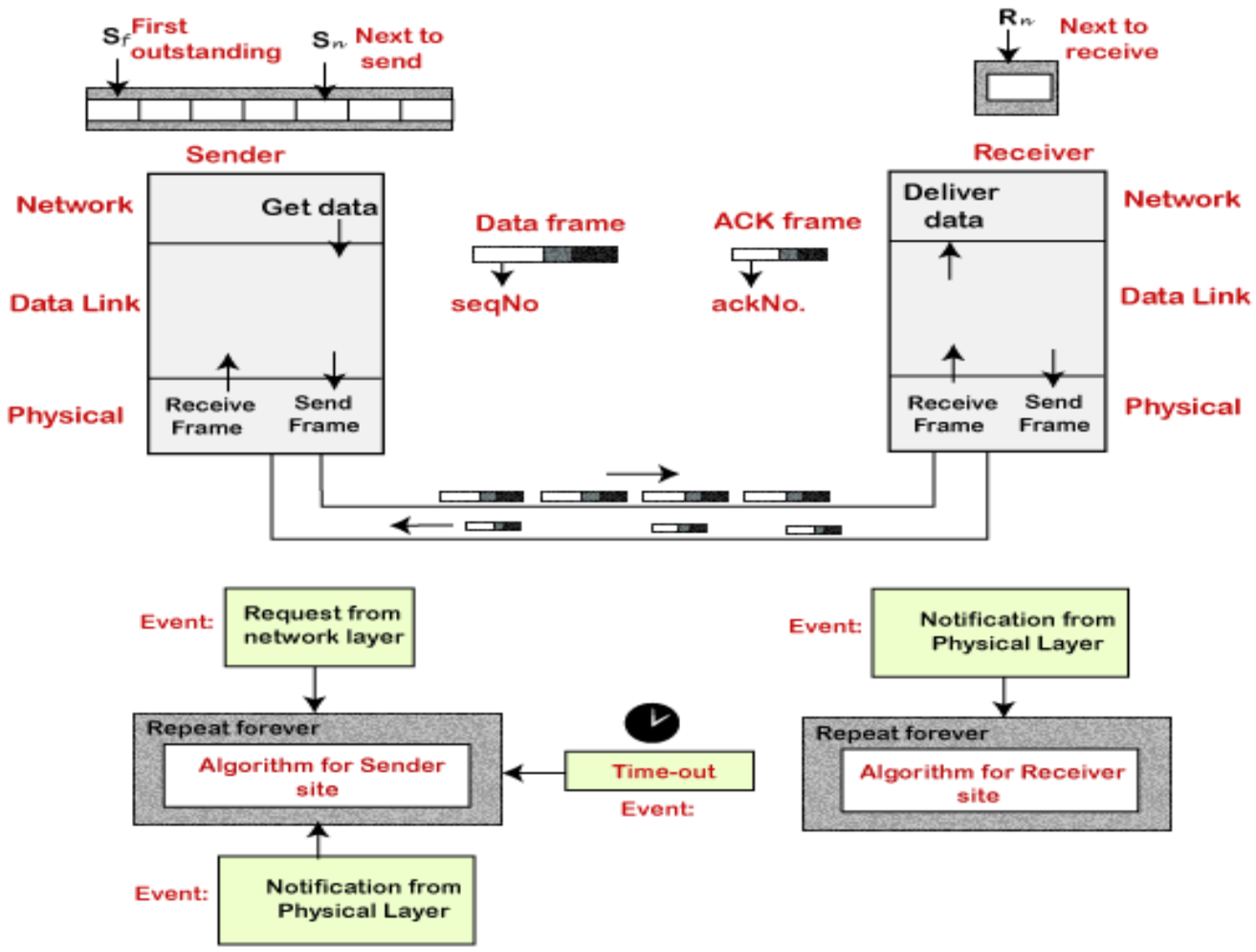
1. Go-Back-N ARQ
2. Selective Repeat ARQ

Go-Back-N ARQ

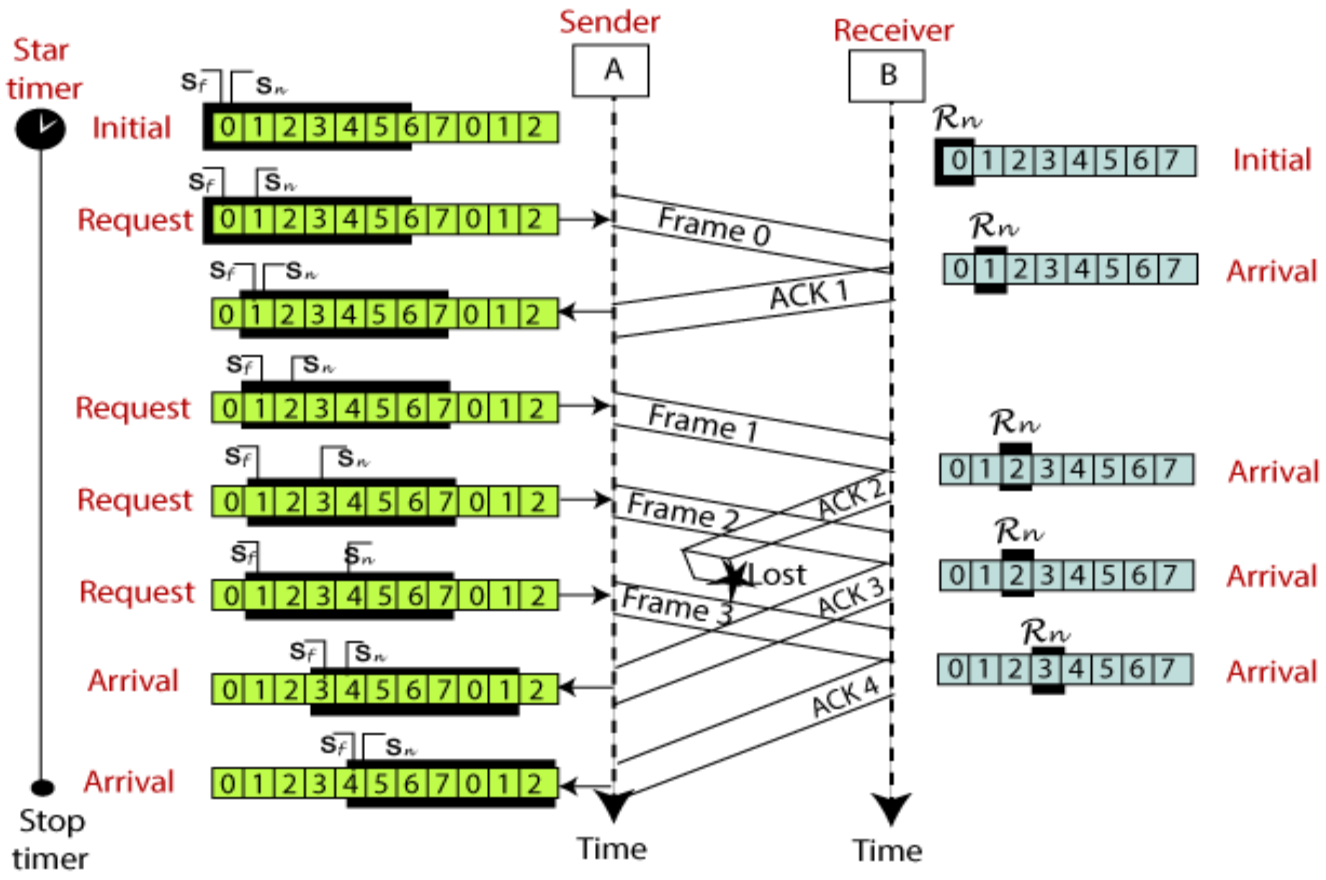
Go-Back-N ARQ protocol is also known as Go-Back-N Automatic Repeat Request. It is a data link layer protocol that uses a sliding window method. In this, if any frame is corrupted or lost, all subsequent frames have to be sent again.

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

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



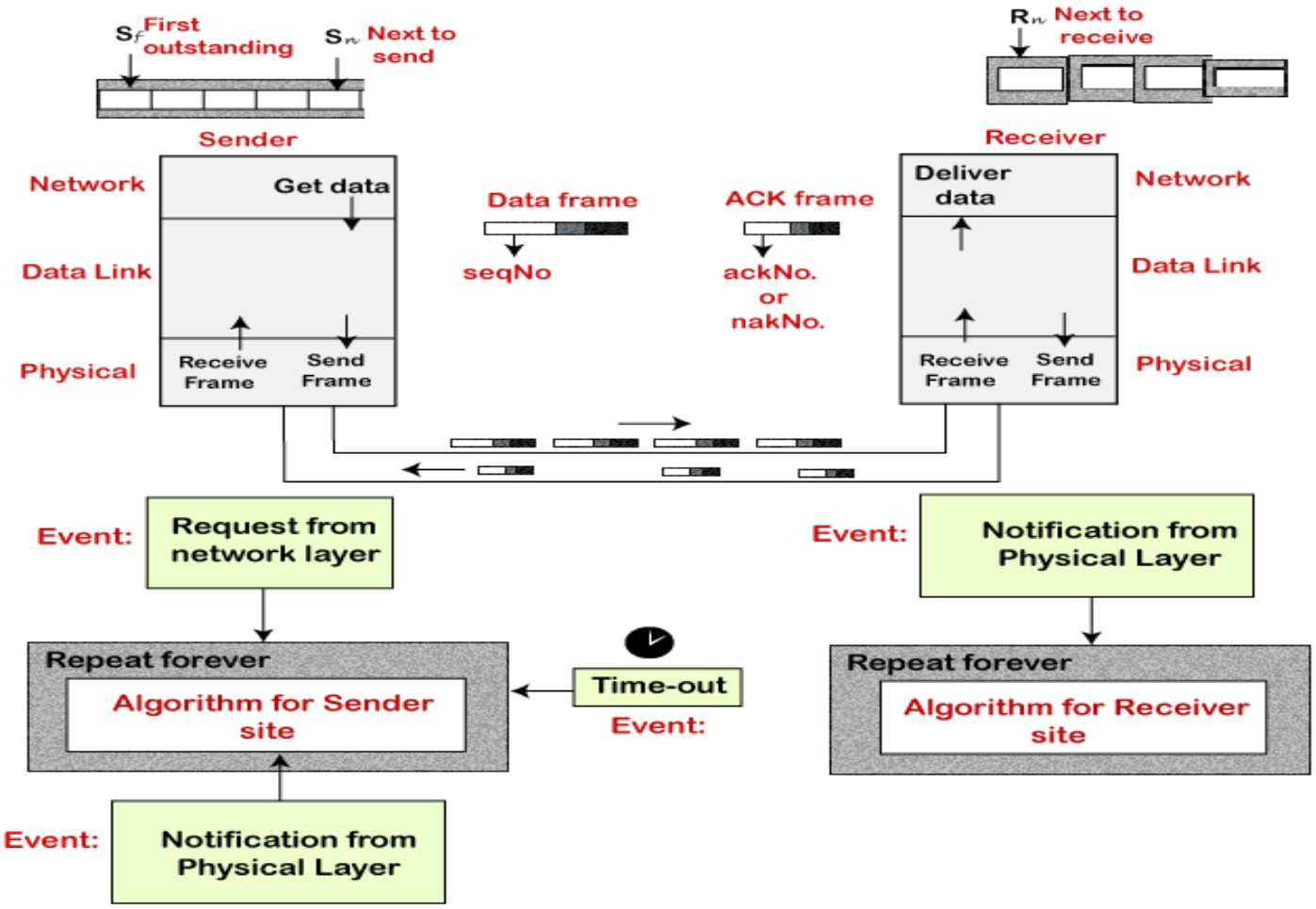
The example of Go-Back-N ARQ is shown below in the figure.



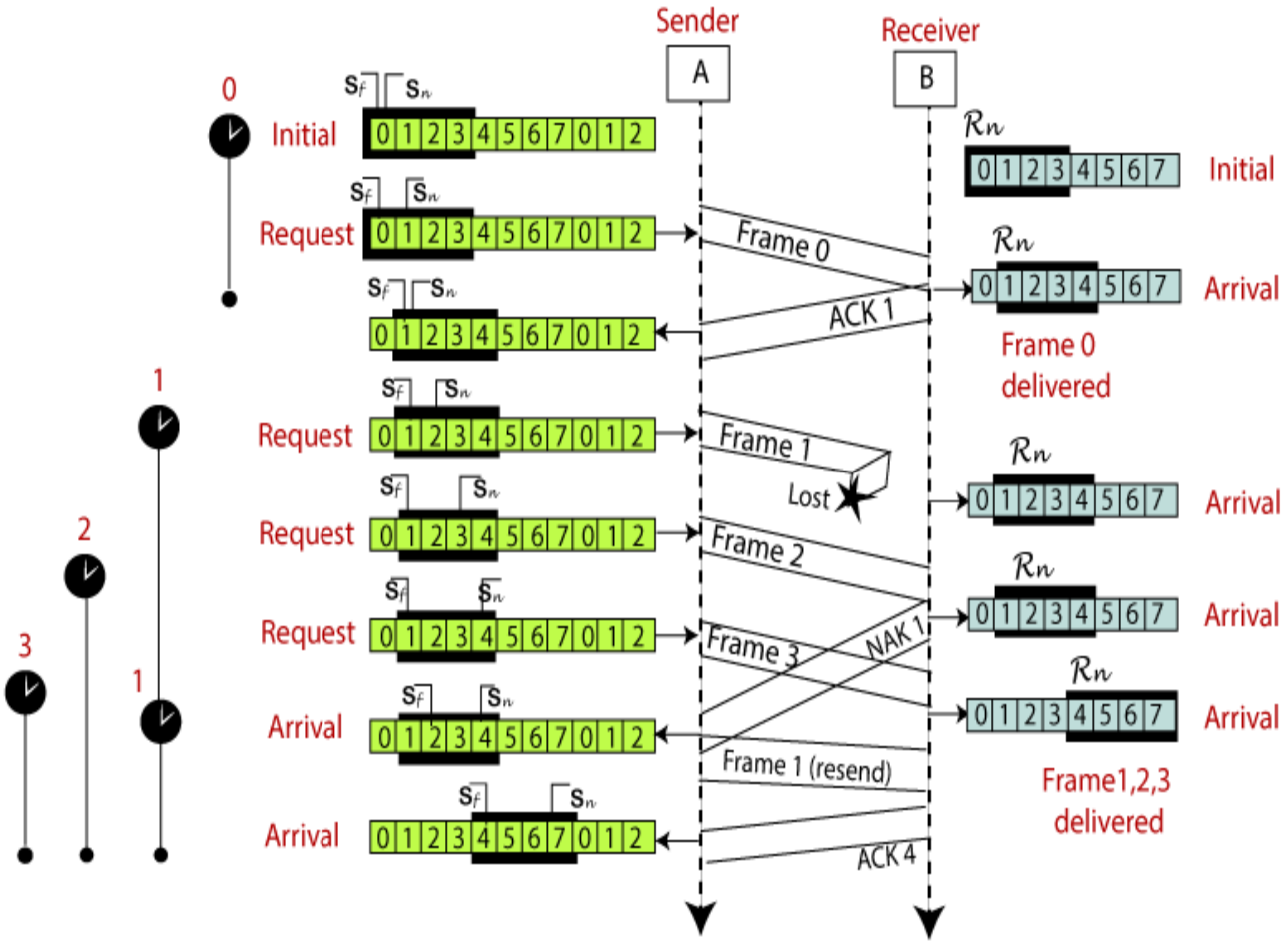
Selective Repeat ARQ

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

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



The example of the Selective Repeat ARQ protocol is shown below in the figure.



Difference between the Go-Back-N ARQ and Selective Repeat ARQ?

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

Example data link protocols

Packet over SONET

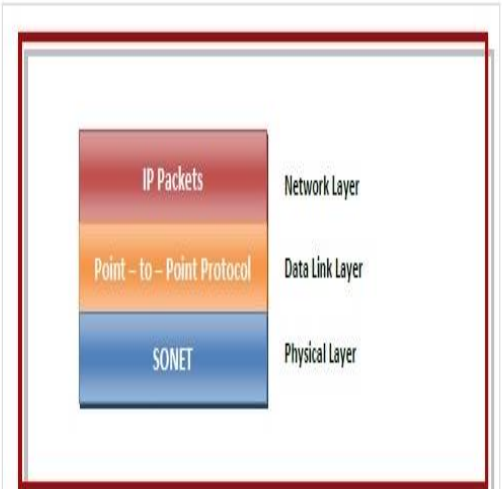
SONET , is the physical layer protocol that is most commonly used over the wide-area optical fiber links that make up the backbone of communications networks, including the telephone system

Packet-over-SONET (POS) is a standard that maps IP packets into SONET frames.

To implement this mechanism, Point – to – Point Protocol (PPP) runs on IP routers. Point – to – Point Protocol (PPP) is a data link layer protocol that is used to transmit data between two directly connected (point-to-point) computers.

It is a byte-oriented protocol that is widely used in broadbandcommunications having heavy loads and high speeds.

The following diagram shows the protocol stack of Packet over SONET (POS) −



Features provides by PPP in POS

Framing − It encapsulates the datagram in a frame so that it can be transmitted over the specified physical layer.

It delineates the beginning and end of the frames and provides for error detection.

Link Control Protocol (LCP) − It is responsible for establishing, configuring, testing, maintaining and terminating links for transmission.

It also imparts negotiation for set up of options and use of features by the two endpoints of the links.

Network Control Protocols (NCPs) − These protocols are used for negotiating the parameters and facilities for the network layer. For every higher-layer protocol supported by PPP, one NCP is there.

Application of POS

For sending a large amount of network traffic over the Internet.

For transmitting IP packets over Wide Area Networks (WANs).

In resilient packet ring (RPR) standard.

High-level Data Link Control (HDLC)

is a group of communication protocols of the data link layer for transmitting data between network points or nodes.

Since it is a data link protocol, data is organized into frames.

A frame is transmitted via the network to the destination that verifies its successful arrival.

It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

The main difference between High-level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) is that High-level Data Link Control is the bit-oriented protocol, on the other hand, Point-to-Point Protocol is the byte-oriented protocol.

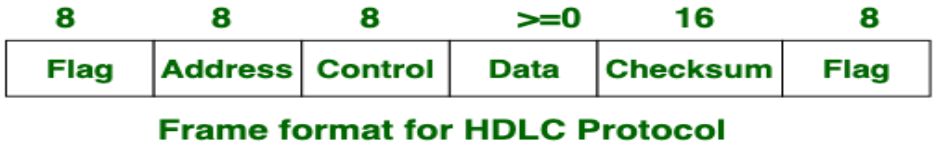
Another difference between HDLC and PPP is that HDLC is implemented by Point-to-point configuration and also multi-point configurations on the other hand While PPP is implemented by Point-to-Point configuration only.

Address field – It is used to describe the terminal.

Control field – The bits in the control field is intended for the sequence number and acknowledgements.

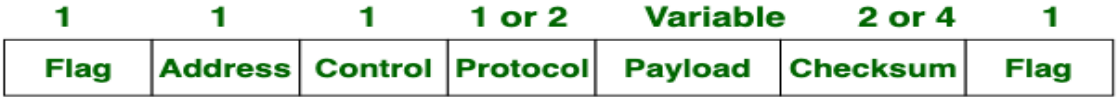
Data field – This field is used to hold the information.

Checksum field -In this field, the bits are reserved for the performing the cyclic redundancy code



Frame format for HDLC Protocol

Click to enlarge



Frame format for PPP Protocol

The PPP frame contains two flag fields, a **protocol filed** to determine the type of packet residing in the payload, and a payload field which can variate.

However, the rest of the fields are the same as the HDLC protocol.

ADSL (Asymmetric Digital Subscriber Loop)

Asymmetric digital subscriber line (ADSL) is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide.

• ADSL (Asymmetric Digital Subscriber Line) is a technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses.

Unlike regular dialup phone service, ADSL provides continuously-available, "always on" connection.

• ADSL differs from the less common symmetric digital subscriber line (SDSL).

• In ADSL, Bandwidth and bit rate are said to be asymmetric, meaning greater toward the downstream than upstream.

• ADSL is generally offered at downstream data rates from 512 Kbps to about 6 Mbps.

• Providers usually market ADSL as a service for consumers for Internet access for primarily downloading content from the Internet, but not serving content accessed by others.

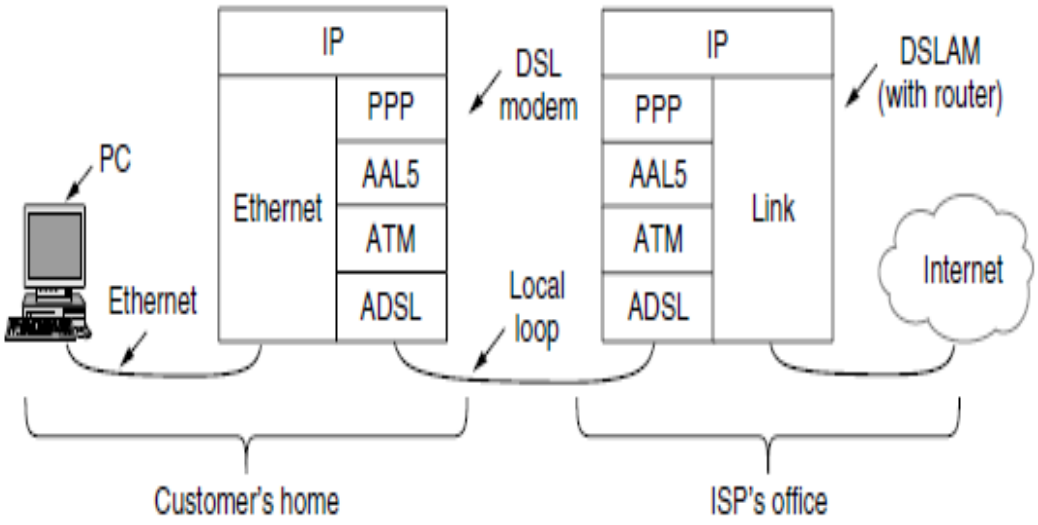


Figure 3-26. ADSL protocol stacks.

Near the top of the stack, just below the IP network layer, is PPP. This protocol is the same PPP that we have just studied for packet over

SONET transports.

It works in the same way to establish and configure the link and carry IP packets.

In between ADSL and PPP are ATM and AAL5. These are new protocols that ATM (Asynchronous Transfer Mode) was designed in the early 1990s

It promised a network technology that would solve the world's telecommunications problems by merging voice, data, cable television, telegraph, by strings, and everything else into an integrated system

To send data over an ATM network, it needs to be mapped into a sequence of cells.

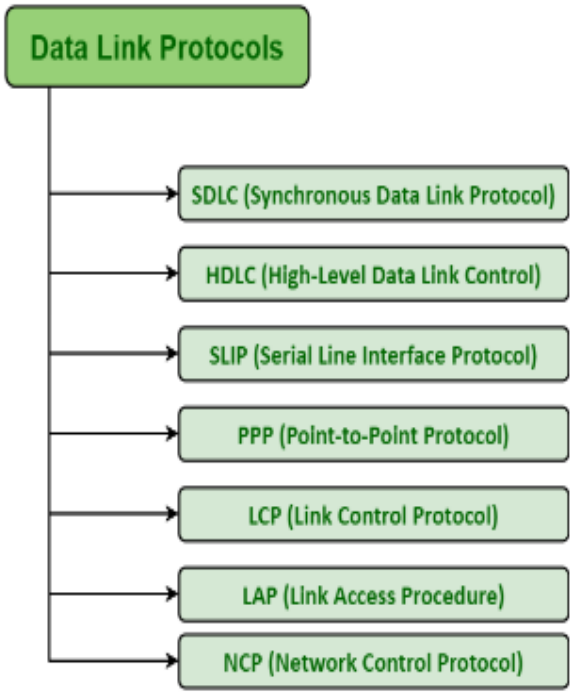
This mapping is done with an ATM adaptation layer in a process called segmentation and reassembly.

Several adaptation layers have been defined for different services, ranging from periodic voice samples to packet data.

The main one used for packet data is AAL5 (ATM Adaptation Layer 5).

An AAL5 frame Instead of a header, it has a trailer that gives the length and has a 4-byte CRC for error detection.

Naturally, the CRC is the same one used for PPP and IEEE 802 LANs like Ethernet.



SDLC is basically a communication protocol of computer.

It usually supports multipoint links even error recovery or error correction also.

It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC.

It is also designed and developed by IBM in 1975.

It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. I

t is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet.

It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link.

It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication.

It is some limitations like it does not provide mechanisms such as error correction or error detection.

Link Access Procedure (LAP) –

LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links.

It also includes some reliability service features.

There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services).

It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

Medium Access Control Sublayer (MAC sublayer)

he medium access control (MAC) is a sublayer of the data link layer of the open system interconnections (OSI) reference model for data transmission. It is responsible for flow control and multiplexing for transmission

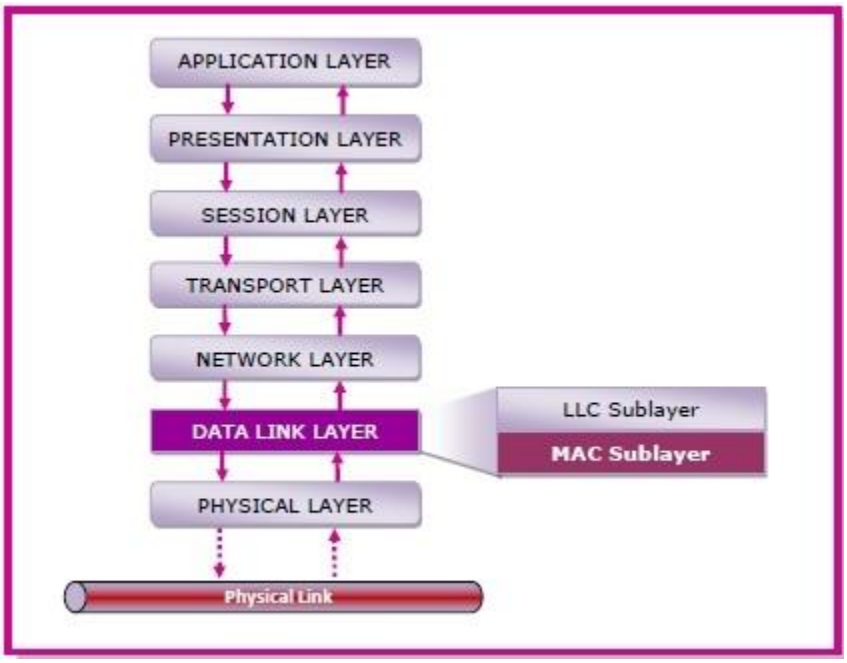
medium. It controls the transmission of data packets via remotely shared channels. It sends data over the network interface card.

MAC Layer in the OSI Model

The Open System Interconnections (OSI) model is a layered networking framework that conceptualizes how communications should be done between heterogeneous systems. The data link layer is the second lowest layer. It is divided into two sublayers −

- The logical link control (LLC) sublayer
- The medium access control (MAC) sublayer

The following diagram depicts the position of the MAC layer –



Functions of MAC Layer

- It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
- It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
- It resolves the addressing of source station as well as the destination station, or groups of destination stations.
- It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.
- It also performs collision resolution and initiating retransmission in case of collisions.
- It generates the frame check sequences and thus contributes to protection against transmission errors.

MAC Addresses

MAC address or media access control address is a unique identifier allotted to a network interface controller (NIC) of a device. It is used as a network address for data transmission within a network segment like Ethernet, Wi-Fi, and Bluetooth.

MAC address is assigned to a network adapter at the time of manufacturing. It is hardwired or hard-coded in the network interface card (NIC). A MAC address comprises of six groups of two hexadecimal digits, separated by hyphens, colons, or no separators. An example of a MAC address is 00:0A:89:5B:F0:11.

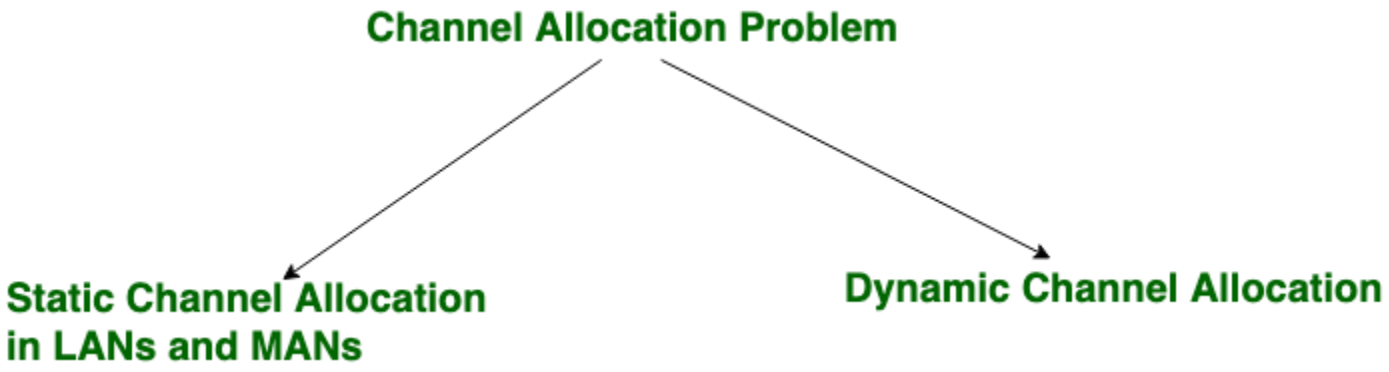
Channel Allocation Problem in Computer Network

Channel allocation

- is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks.
- There are user's quantity may vary every time the process takes place.
- If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion.
- If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.

Channel allocation problem can be solved by two schemes:

1. Static Channel Allocation in LANs and MANs,
2. Dynamic Channel Allocation.



These are explained as following below.

- **Static Channel Allocation in LANs and MANs:**
  It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM).
- if there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion.
- since each user has a private frequency band, there is no interface between users.

It is not efficient to divide into fixed number of chunks.

T = 1/(U*C-L)

T(FDM) = N*T(1/U(C/N)-L/N)
Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

2. Dynamic Channel Allocation:

Possible assumptions include:

1. **Station Model:**
   Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.
2. **Single Channel Assumption:**
   In this allocation all stations are equivalent and can send and receive on that channel.
3. **Collision Assumption:**
   If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must retransmitted. Collisions are only possible error.
4. **Time** can be divided into Slotted or Continuous.
5. **Stations** can sense a channel is busy before they try it.

Protocol Assumption:

- N independent stations.
- A station is blocked untill its generated frame is transmitted.
- probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- **Carrier Sense:** A station can sense if a channel is already busy before transmission.
- **No Carrier Sense:** Time out used to sense loss data.

.

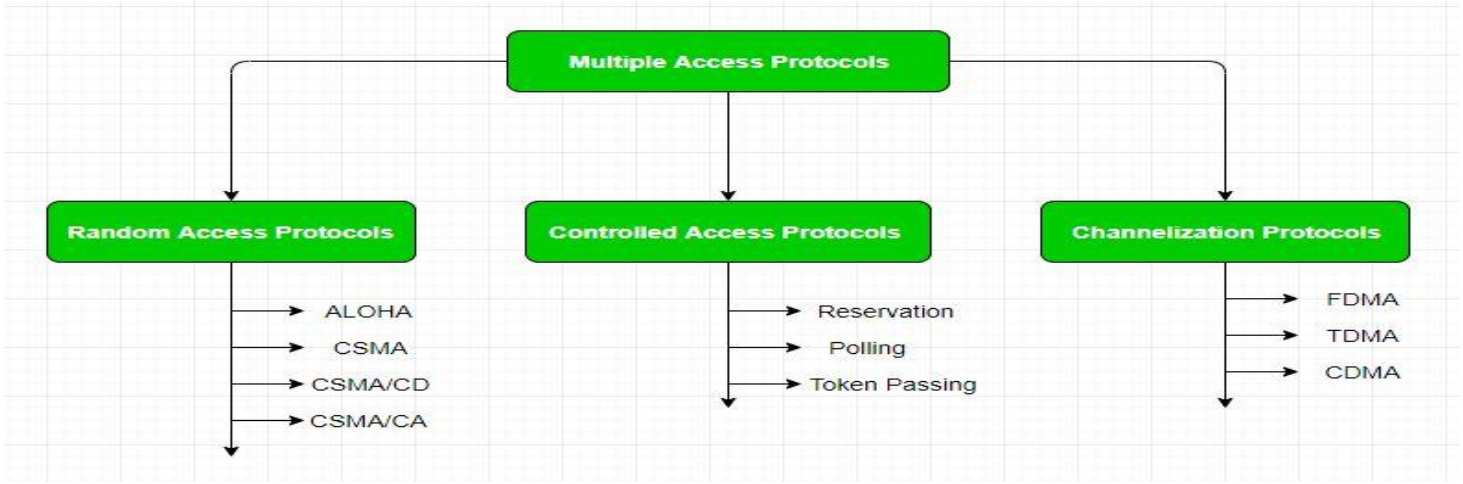
Multiple Access Protocols in Computer Network

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

- Data Link Control
- Multiple Access Control

Data Link control –
The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control. **Multiple Access Control –**
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient,

- however if there is no dedicated link present then multiple stations can access the channel simultaneously.
- Hence multiple access protocols are required to decrease collision and avoid crosstalk. Multiple access protocols can be subdivided further as –



1. Random Access Protocol: In this, all stations have same superiority that is no station has more priority than another station.
Any station can send data depending on medium's state(idle or busy). It has two features:
1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

(a) ALOHA – It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

- **Pure Aloha:**
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

- Vulnerable Time = 2* Frame transmission time
- Throughput = G exp{-2*G}

  Maximum throughput = 0.184 for G=0.5

- **Slotted Aloha:**
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.
- Vulnerable Time = Frame transmission time
- Throughput = G exp{-*G}

  Maximum throughput = 0.368 for G=1

For more information on ALOHA refer – LAN Technologies

(b) CSMA – Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data.
If it is idle then it sends data, otherwise it waits till the channel becomes idle.
However there is still chance of collision in CSMA due to propagation delay.
For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data.
However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data.
This will result in collision of data from station A and B.

CSMA access modes-

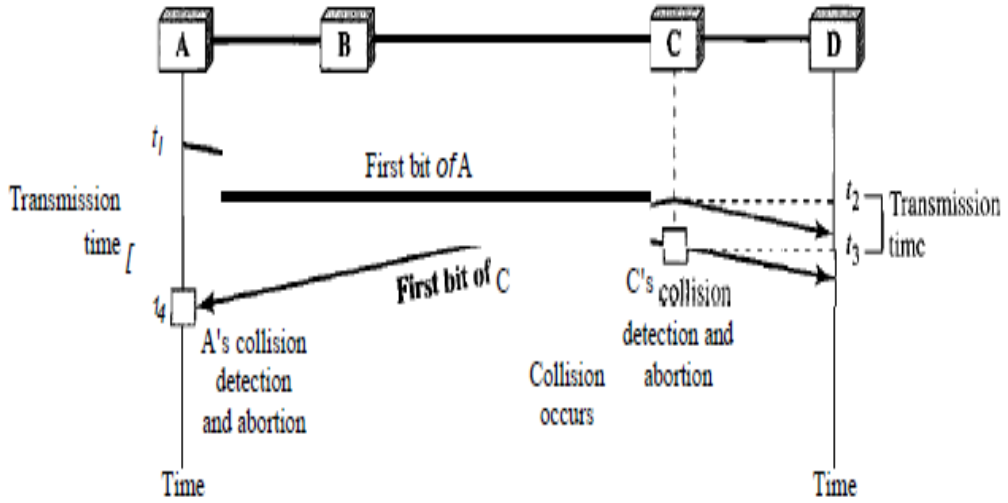
- **1-persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

(c) CSMA/CD – Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected

- The CSMA method does not specify the procedure following a collision.
- Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision.
- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful.

- If so, the station is finished. If, however, there is a collision, the frame is sent again.To better understand CSMA/CD, let us look at the first bits transmitted by the two stations involved in the collision
- Although each station continues to send bits in the frame until it detects the collision, we show what happens as the first bits collide.
- In Figure 12.12, stations A and C are involved in the collision

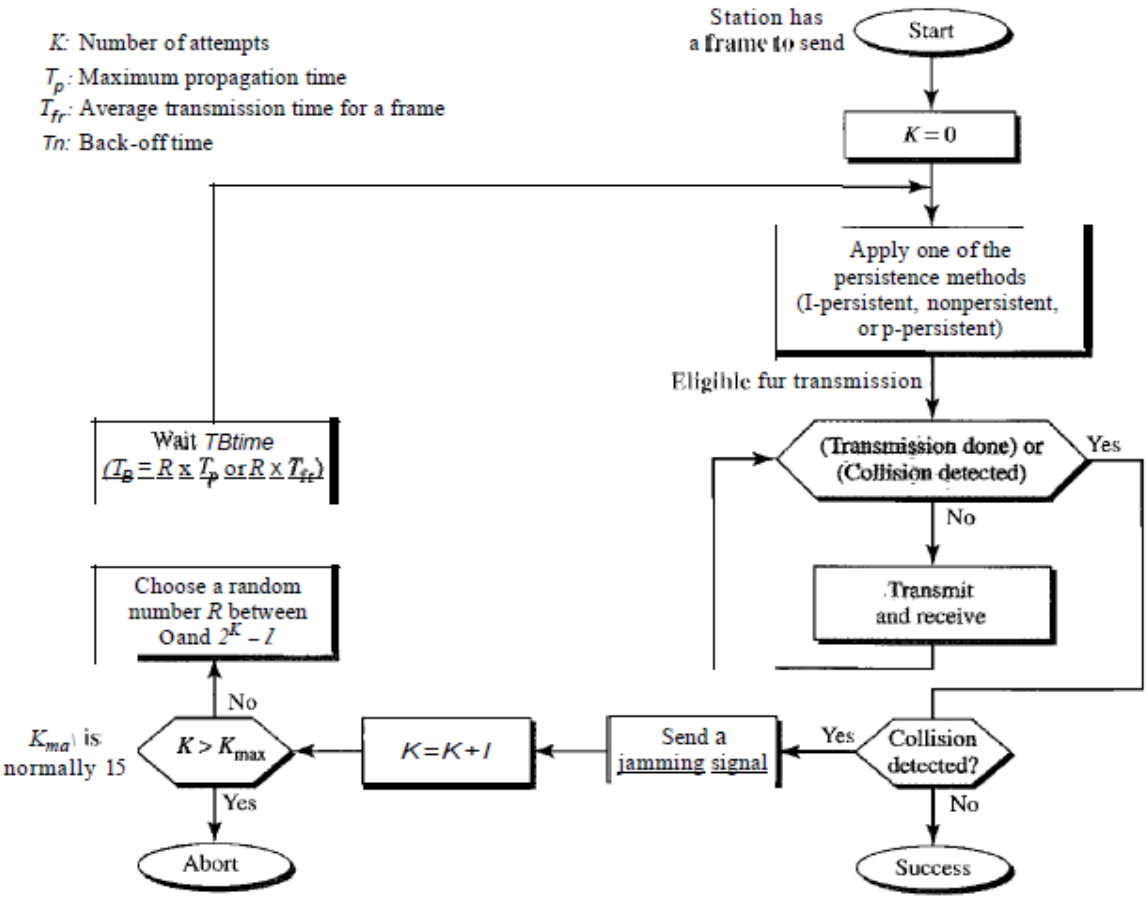
Figure 12.12 *Collision of the first bit in CSMA/CD*



- At time t 1, station A has executed its persistence procedure and starts sending the bits of its frame.
- At time t2, station C has not yet sensed the first bit sent by A.
- Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right.
- The collision occurs sometime after time t2' Station C detects a collision at time t3 when it receives the first bit of A's frame.
- Station C immediately aborts transmission.
- Station A detects collision at time t4 when it receives the first bit of C's frame;
- it also immediately aborts transmission.
- Looking at the figure, we see that A transmits for the duration t4 - tl; C transmits for the duration t3 - t2‘
- **Minimum Frame Size**
- For CSMA/CD to work, we need a restriction on the frame size.
- Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection.
- Therefore, the frame transmission time Tfr must be at least two times the maximum propagation time Tp.
- **Energy Level**
- We can say that the level of energy in a channel can have three values: zero, normal, and abnormal.

- At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame.
- At the abnormal level, there is a collision and the level of the energy is twice the normal level.
- A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.
- Figure 12.15 shows the situation.

Figure 12.14 *Flow diagramfor the CSMAlCD*



Throughput

The throughput of CSMAlCD is greater than that of pure or slotted ALOHA.
The maximum throughput occurs at a different value of G and is based on the persistence method and the value of p in the p-persistent approach.
For I-persistent method the maximum throughput is around 50 percent when G =1.
For nonpersistent method, the maximum throughput can go up to 90 percent when G is between 3 and 8.

(d) CSMA/CA – Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals.
If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred.
To distinguish between these two cases, collision must have a lot of impact on received signal.

However it is not so in wired networks, so CSMA/CA is used in this case.
CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access:
In this, the data is sent by that station which is approved by all other stations
3. Channelization:
In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no to bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
  For more details refer – Circuit Switching
- **Code Division Multiple Access (CDMA) –** One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly data from different stations can be transmitted simultaneously in different code languages.

.

Collision-Free Protocols

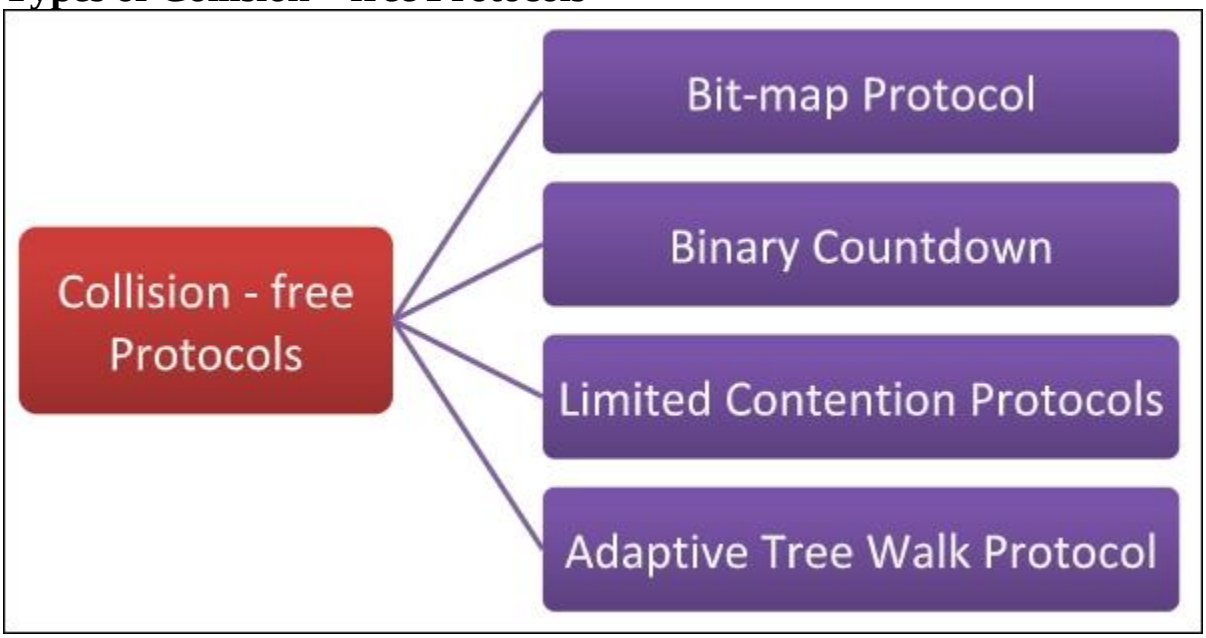
In computer networks, when more than one station tries to transmit simultaneously via a shared channel, the transmitted data is garbled.

This event is called collision. The Medium Access Control (MAC) layer of the OSI model is responsible for handling collision of frames.

Collision – free protocols are devised so that collisions do not occur. Protocols like CSMA/CD and CSMA/CA nullifies the possibility of collisions once the transmission channel is acquired by any station.

However, collision can still occur during the contention period if more than one stations starts to transmit at the same time. Collision – free protocols resolves collision in the contention period and so the possibilities of collisions are eliminated.

Types of Collision – free Protocols



Bit – map Protocol

In bit map protocol, the contention period is divided into N slots, where N is the total number of stations sharing the channel.

If a station has a frame to send, it sets the corresponding bit in the slot. So, before transmission, each station knows whether the other stations want to transmit.

Collisions are avoided by mutual agreement among the contending stations on who gets the channel.

Binary Countdown

This protocol overcomes the overhead of 1 bit per station of the bit – map protocol. Here, binary addresses of equal lengths are assigned to each station.

For example, if there are 6 stations, they may be assigned the binary addresses 001, 010, 011, 100, 101 and 110.

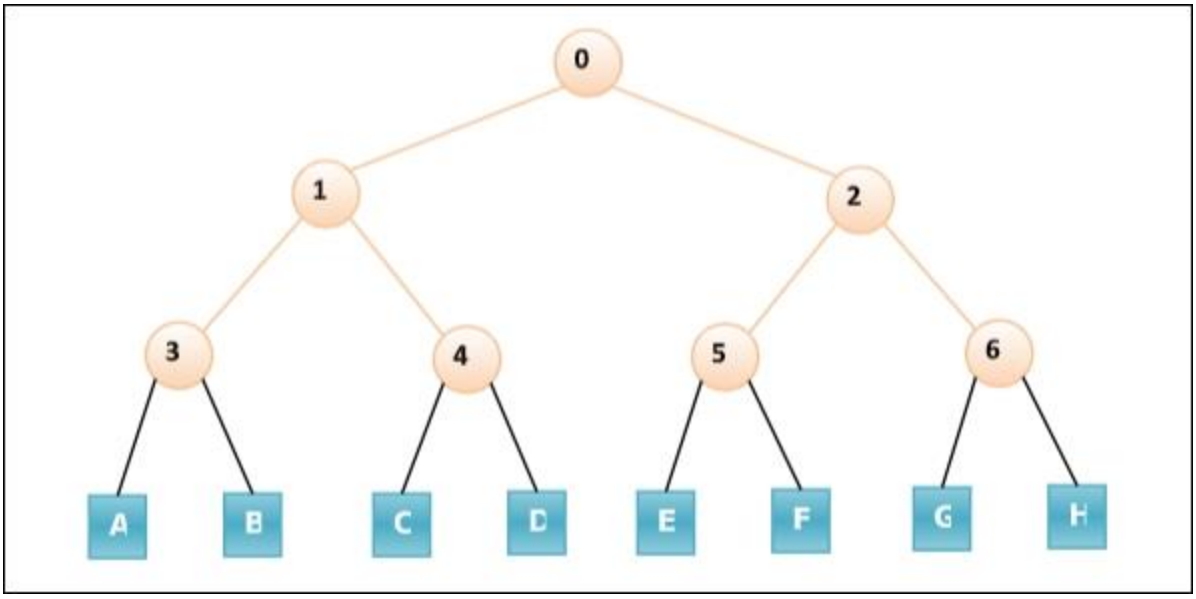
All stations wanting to communicate broadcast their addresses. The station with higher address gets the higher priority for transmitting.

Limited Contention Protocols

These protocols combines the advantages of collision based protocols and collision free protocols. Under light load, they behave like ALOHA scheme. Under heavy load, they behave like bitmap protocols.

Adaptive Tree Walk Protocol

In adaptive tree walk protocol, the stations or nodes are arranged in the form of a binary tree as follows -



Initially all nodes (A, B ……. G, H) are permitted to compete for the channel. If a node is successful in acquiring the channel, it transmits its frame. In case of collision, the nodes are divided into two groups (A, B, C, D in one group and E, F, G, H in another group). Nodes belonging to only one of them is permitted for competing. This process continues until successful transmission occurs.

WIRELESS LANS

- Wireless LANs (WLANs) are wireless computer networks that use high-frequency radio waves instead of cables for connecting the devices within a limited area forming LAN (Local Area Network)
- The main wireless LAN standard is 802.11
- **802.11 ARCHITECTURE AND PROTOCOL STACK**
- 802.11 networks can be used in two modes
- **Infrastructure Mode** − Mobile devices or clients connect to an access point (AP) that in turn connects via a bridge to the LAN or Internet.

The client transmits frames to other clients via the AP.

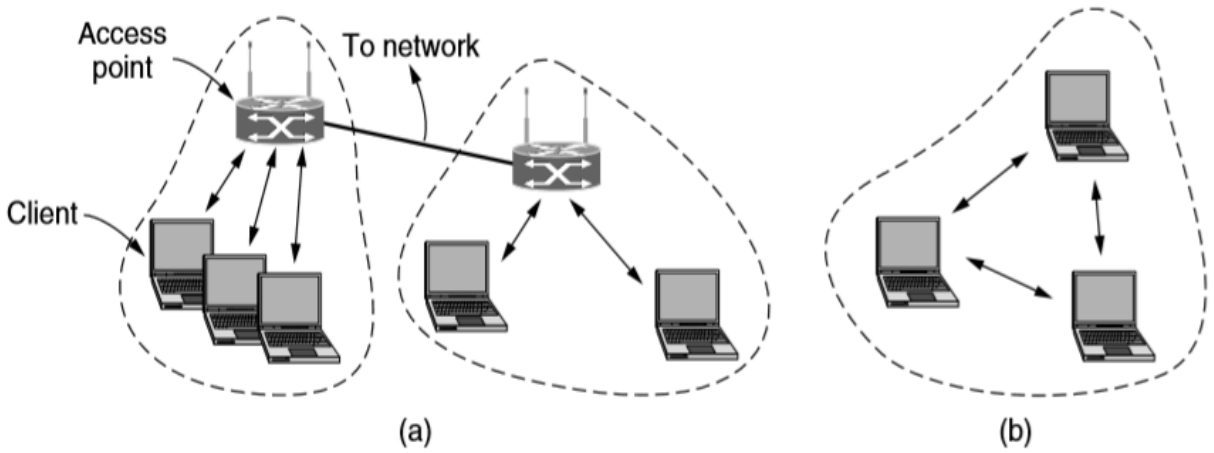


Figure 4-23. 802.11 architecture. (a) Infrastructure mode. (b) Ad-hoc mode.

- **Ad Hoc Mode** − Clients transmit frames directly to each other in a peer-to-peer fashion
- This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point
- The 802.11 physical layer corresponds to the OSI physical layer, but the data link layer is split into multiple sublayers.
- in 802.11 the MAC sub layer determines which channel gets to transmit next.
- The sub layer above, the LLC (Logical Link Layer), hides the differences between the varying 802.11 versions for the network layer

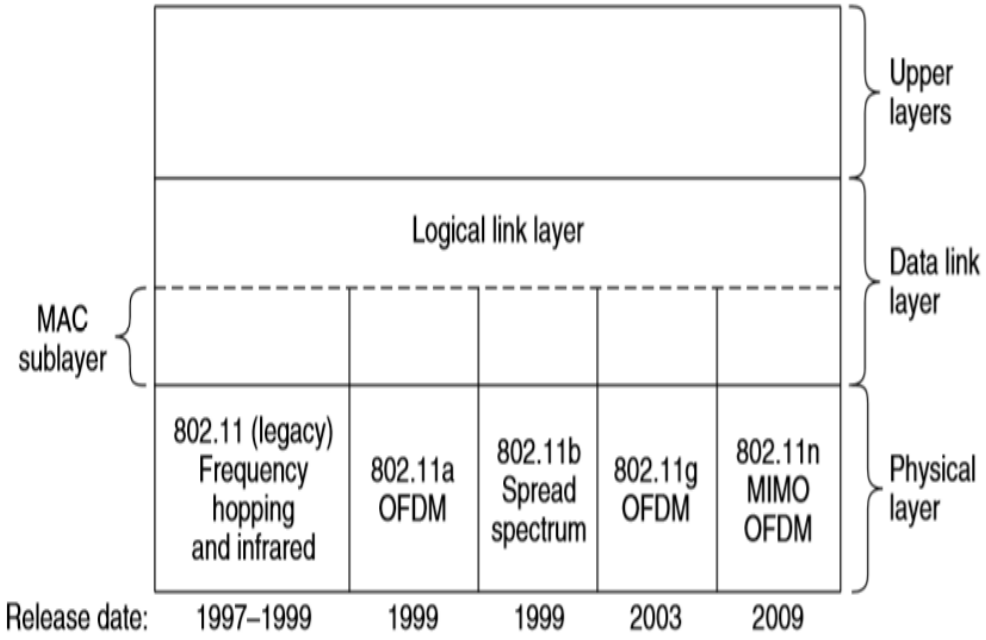


Figure 4-24. Part of the 802.11 protocol stack.

- **The 802.11 physical layer**
- "All 802.11 techniques use short-range radios to transmit signals in either 2.4-GHz or 5-GHz ISM frequency bands".
- These bands are unlicensed, and so are shared by many other devices such as garage door openers, or microwave ovens.
- Fewer applications tend to use the 5-GHz band, so 5-GHz can be better for some applications despite shorter range due to higher frequency
- All 802.11 transmission methods define multiple rates.
- Different rates can be used depending on the current conditions.
- If the signal is weak, a low rate is used. If the signal is clear, the highest rate is used. The process of adjustment is called rate adaption.
- **802.11b**
- 802.11b is a spread-spectrum method. It supports rates of 1, 2, 5.5, and 11Mb/s
- 802.11b is similar to the CDMA system, except that one spreading code is shared between all users. 802.11b uses a spreading sequence called the Barker Sequence.
- The autocorrelation of the Barker Sequence is low except when sequences are aligned.
- This allows a receiver to lock onto the start of a transmission. The Barker sequence is "used with BPSK modulation to send 1 bit per 11 chips"

- **802.11a**
- 802.11a was standardized after 802.11b. It supports rates up to 54Mb/s in the 5-GHz ISM band
- 802.11a is based on OFDM (Orthogonal Frequency Division Multiplexing).
- Bits are sent over 52 subcarriers in parallel. 48 carry data, and 4 are used for synchronization. A symbol lasts 4μs, and sends either 1, 2, 4, or 6 bits. "The bits are coded for error correction with a binary convolutional code first so only 1/2, 2/3, or 3/4 of the bits are not redundant"
- 802.11a can run at different rates using the different combinations . The rates range from 5 to 55Mb/s.
- **802.11g**
- 802.11g uses the OFDM modulation methods of 802.11a, but operates in 2.4GHz ISM band
- It has the same rates as 802.11a, as well as compatibility with 802.11b devices
- **802.11n** was ratified in 2009. The aim of 802.11n was throughput of 100Mb/s after transmission overheads were removed
- To meet the goal:
- Channels were doubled from 20MHz to 40MHz.
- Frame overhead was reduced by allowing a group of frames to be sent together.
- Up to four streams could be transmitted at a time using four antennas.
- **The MAC sublayer protocol**
- The 802.11 MAC sublayer is different from the Ethernet MAC sublayer for two reasons:
- Radios are almost always half duplex
- Transmission ranges of different stations might be different
- 802.11 uses the CSMA/CA (CSMA with Collision Avoidance) protocol.
- CSMA/CA is similar to ethernet CSMA/CD.
- It uses channel sensing and exponential backoff after collisions, but instead of entering backoff once a collision has been detected, CSMA/CA uses backoff immediately
- The algorithm will backoff for a number of slots, for example 0 to 15 in the case of the of the OFDM physical layer.
- The station waits until the channel is idle by sensing that there is no signal for a short period of time.
- It counts down idle slots, pausing when frames are sent. When its counter reaches 0, it sends its frames
- Acknowledgements "are used to infer collisions because collisions cannot be detected" [1, P. 303]
- This way of operating is called DCF (Distributed Coordination Function). in DCF each station is acting independently, without a central control.
- The other problem facing 802.11 protocols is transmission ranges differing between stations.

- It's possible for transmissions in one part of a cell to not be received in another part of the cell, which can make it impossible for a sender to sense a busy channel, resulting in collisions
- 802.11 defines channel sensing to consist of physical and virtual sensing. Physical sensing "checks the medium to see if there is a valid signal"
- With virtual sensing, each station keeps a record of what channel is in use.
- It does this with the NAV (Network Allocation Vector). Each frame includes a NAV field that contains information on how long the sequence that the frame is part of will take to complete

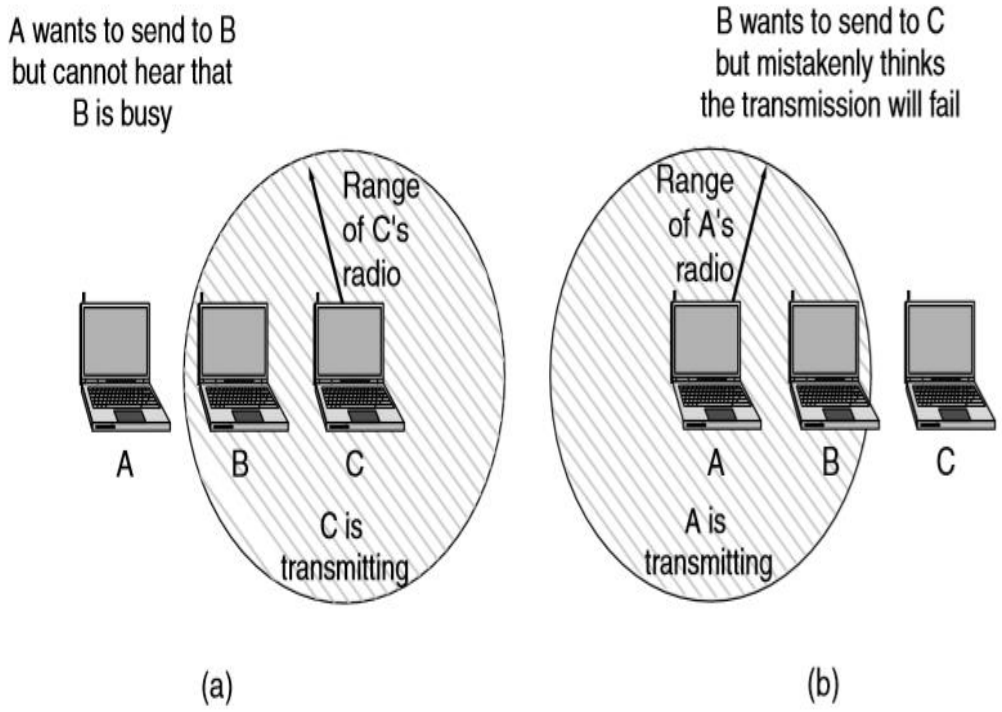


Figure 4-26. (a) The hidden terminal problem. (b) The exposed terminal problem.

- 802.11 is designed to:
- Be reliable.
- Be power-saving.
- Provide quality of service.
- The main strategy for reliability is to lower the transmission rate if too many frames are unsuccessful.
- Lower transmission rates use more robust modulations. If too many frames are lost, a station can lower its rate.
- If frames are successfully delivered, a station can test a higher rate to see if should upgrade

- Another strategy for successful transmissions is to send shorter frames. 802.11 allows frames to be split into fragments, with their own checksum.
- The fragment size can be adjusted by the AP.
- Fragments are numbered and sent using a stop-and-wait protocol
- 802.11 uses beacon frames. Beacon frames are broadcast periodically by the AP.
- The frames advertise the presence of the AP to clients and carry system parameters, such as the identifier of the AP, the time, how long until the next beacon, and security settings"
- Clients can set a power-management bit in frames that are sent to the AP to alert it that the client is entering power-save mode.
- In power-save mode, the client rests and the AP buffers traffic intended for it.
- The client wakes up for every beacon, and checks a traffic map that's sent with the beacon.
- The traffic map tells the client whether there is buffered traffic.
- If there is, the client sends a poll to the AP, and the AP sends the buffered traffic
- 802.11 provides quality of service by extending CSMA/CA with defined intervals between frames.
- Different kinds of frames have different time intervals.
- The interval between regular data frame is called the DIFS (DCF InterFrame Spacing). Any station can attempt to acquire a channel after the channel has been idle for DIFS
- The shortest interval is SIFS (Short InterFrame Spacing).
- **802.11 frame structure**
- There are three different classes of frames used in the air:
- Data
- Control
- Management
- The first part of frame is the *Frame Control* field, made up of 11 subfields:
- *Protocol Version*: set to 00 for current versions of 802.11.

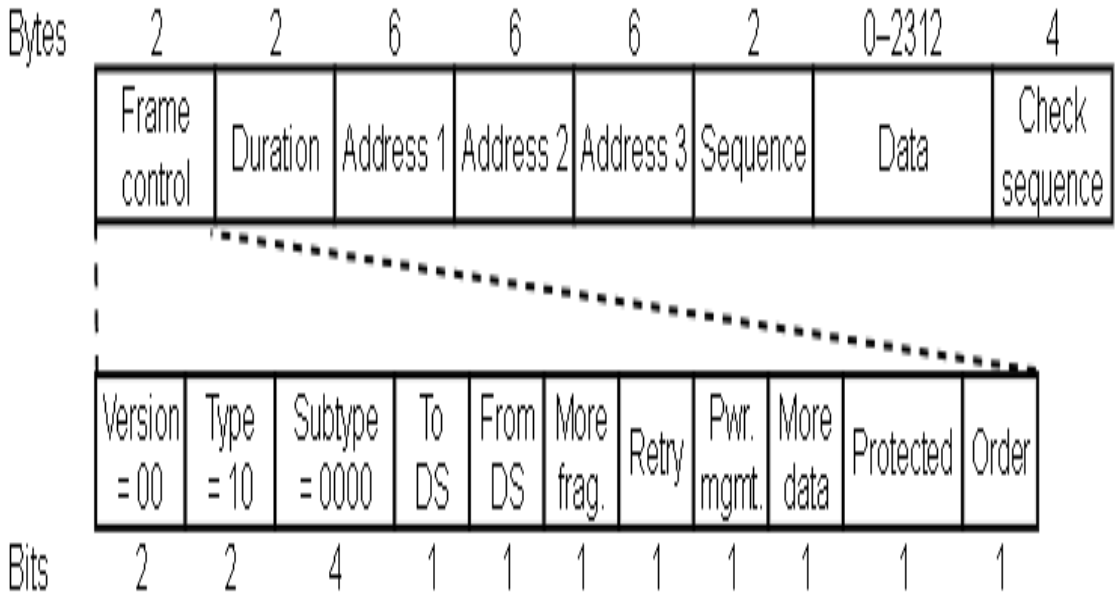


FIGURE: FORMAT OF THE 802.11 DATA FRAME [1, P. 310]

- *Type*: can be one of data, control, or management, and the *Subtype* (e.g RTS or CTS). These are set to 10 and 0000 in binary for a normal data field.
- *To DS* and *From DS*: these bits indicate whether frames are coming or going from a network connected to the AP (the network is called the distribution system).
- *More Fragments*: this bit means that more fragments will follow.
- *Retry*: this bit "marks a retransmission of a frame sent earlier".
- *Power Management*: this bit indicates that the sender is going into power-save mode.
- *More Data*: this bit indicates that the sender has additional frames for the receiver.
- *Protected Frame*: this bit indicates that the frame body has been encrypted for security.
- *Order*: this "bit tells the receiver that the higher layer expects the sequence of frames to arrive strictly in order".
- The second field in the data frame is the *Duration* field.
- This describes how long the frame and its acknowledgements will occupy the channel (measured in microseconds).
- It's included in all frames, including control frames
- The addresses to and from an AP follow the standard IEEE 802 format.

- The *Address 1* is the receiver, *Address 2* is the transmitter, *Address 3* is the address of the endpoint that originally sent the frame via the AP
- The *Sequence* 16-bit field numbers frames so that duplicates can be detected.
- The first 4 bits identify the fragment, the last 12 contain a number that's incremented on each transmission
- The *Data* field contains the payload. It can be up to 2312 bytes.
- The first bytes of the payload are for the LLC layer to identify the higher-layer protocol that the data is a part of
- The final part of the frame is the *Frame Check Sequence* field, containing a 32-bit CRC for validating the frame
- "Management frames have the same format as data frames, plus a format for the data portion that varies with the subtype (e.g., parameters in beacon frames)"
- Control frames contain *Frame Control*, *Duration*, and *Frame Check Sequence* fields, but they might only have one address and no *Data* section.
- **Services**
- 802.11 defines a number of services that must be provided by conformant wireless LANs.
- Mobile stations use the association service to connect to APs.
- Usually, the service is used just after a station has moved within range of an AP.
- When the station is within range, it learns the identity and capabilities of the AP through either beacon frames, or by asking the AP directly.
- The station sends a request to associate with the AP, which the AP can either accept or reject
- The reassociation service is used to let a station change its preferred AP.
- If correctly used, there should be no data loss between the handover.
- The station or the AP can also disassociate. The station should use this before shutting down
- Stations should authenticate before sending frames via the AP. Authentication is handled differently depending on the security scheme.
- If the network is open, anyone can use it. Otherwise credentials are required. WPA2 (WiFi Protected Access 2) is the recommended approach that implements security defined in the 802.11i standard.
- With WPA2, the AP communicates with an authentication server that "has a username and password database to determine if the station is allowed to access the network". A password can also be configured (known as a pre-shared key)
- The distribution service determines how to route frames from the AP.

- If the destination is local, the frames are sent over the air. If they are not, they are forwarded over the wired network.
- The integration service handles translation for frames to be sent outside the 802.11 LAN
- The data delivery service lets stations transmit and receive data using the protocols outlined in this section
- A privacy service manages encryption and decryption.
- The encryption algorithm for WPA2 is based on AES (Advanced Encryption Standard).
- The encryption keys are determined during authentication
- The QOS traffic scheduling is used to handle traffic with different priorities.
- "The transmit power control service gives stations the information they need to meet regulatory limits on transmit power that vary from region to region"
- "The dynamic frequency selection service give stations the information they need to avoid transmitting on frequencies in the 5-GHz band that are being used for radar in the proximity"

Data Link Layer Switching

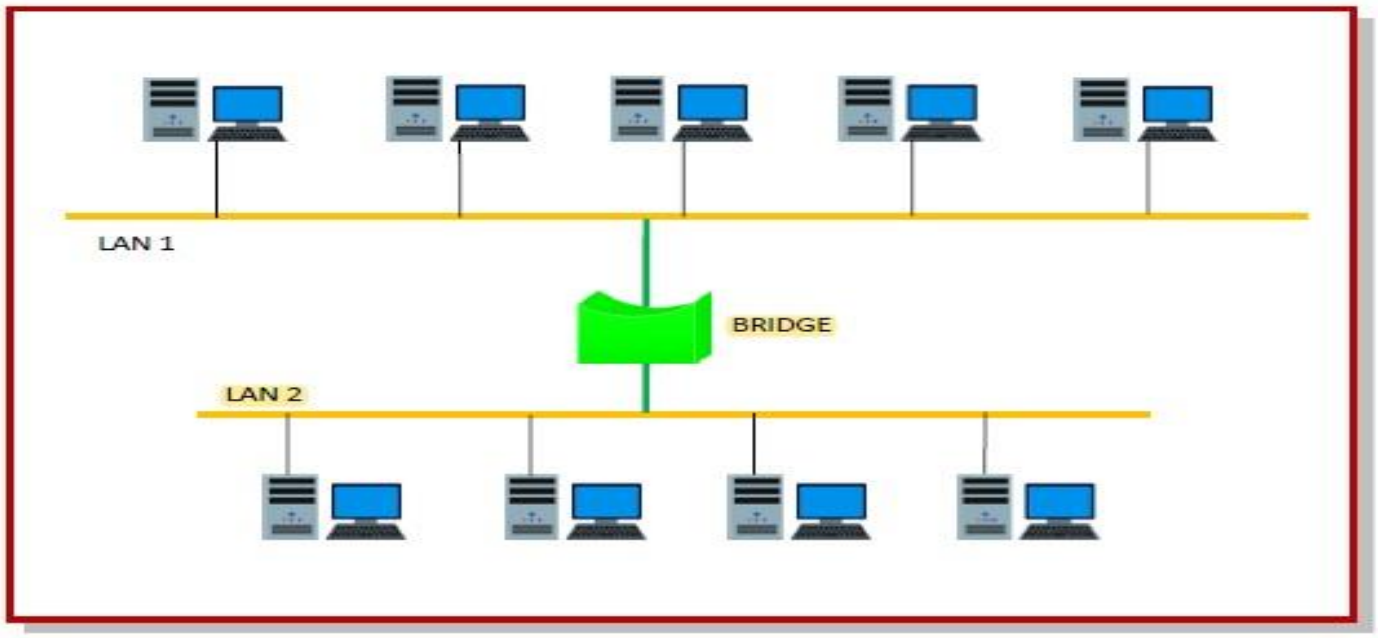
Network switching is the process of forwarding data frames or packets from one port to another leading to data transmission from source to destination

Switching in data link layer is done by network devices called **bridges**.

Bridges

A data link layer bridge connects multiple LANs (local area networks) together to form a larger LAN. This process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network.

The following diagram shows connection by a bridge −



Switching by Bridges

When a data frame arrives at a particular port of a bridge, the bridge examines the frame's data link address, or more specifically, the MAC address. If the destination address as well as the required switching is valid, the bridge sends the frame to the destined port. Otherwise, the frame is discarded.

The bridge is not responsible for end to end data transfer. It is concerned with transmitting the data frame from one hop to the next. Hence, they do not examine the payload field of the frame. Due to this, they can help in switching any kind of packets from the network layer above.

Bridges also connect virtual LANs (VLANs) to make a larger VLAN.

If any segment of the bridged network is wireless, a wireless bridge is used to perform the switching.

There are three main ways for bridging −

- simple bridging
- multi-port bridging
- learning or transparent bridging

- **Uses of bridges**
- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them
- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
    - If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.
- If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- .
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above.
- This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- Learning Bridges

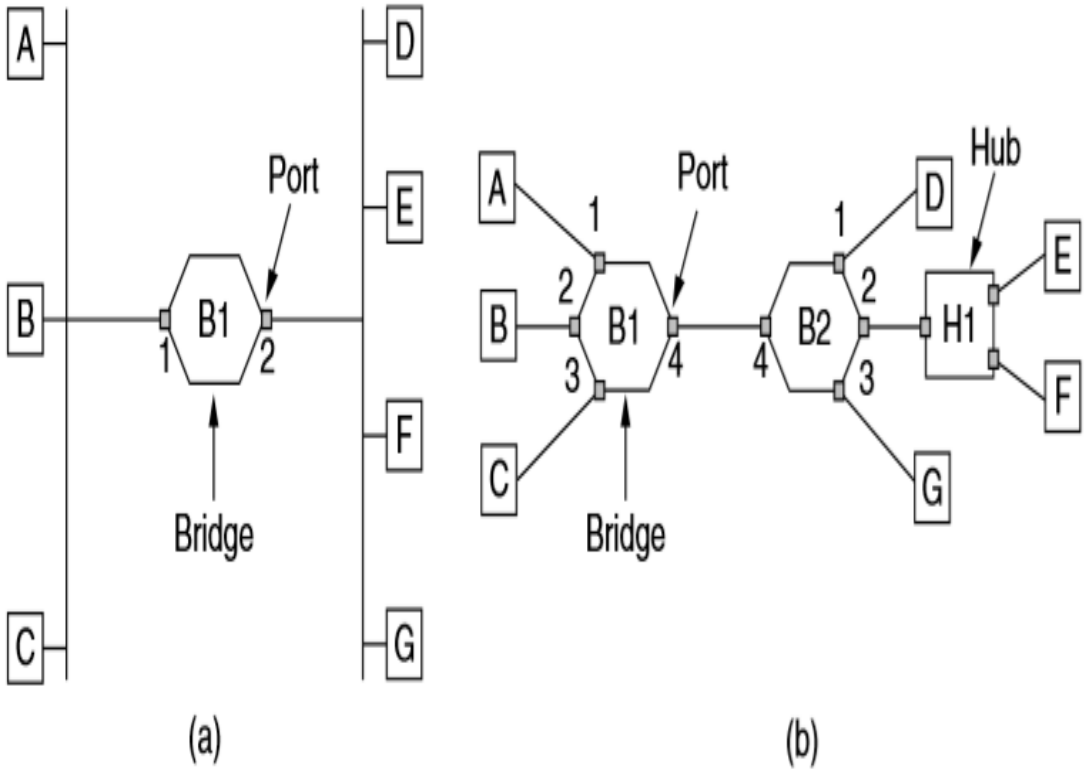


Figure 4-41. (a) Bridge connecting two multidrop LANs. (b) Bridges (and a hub) connecting seven point-to-point stations.

- The topology of two LANs bridged together is shown in Fig for two cases
- 1 two multidrop LANs, such as classic Ethernets, are joined by a special station—the bridge
- 2 LANs with point-to-point cables, including one hub, are joined together.
- The bridges are the devices to which the stations and hub are attached.

- If the LAN technology is Ethernet, the bridges are better known as Ethernet switches.
- All of the stations attached to the same port on a bridge belong to the same collision domain, and this is different than the collision domain for other ports.
- Different kinds of cables can also be attached to one bridge.
- For example, the cable connecting bridge B1 to bridge B2 might be a long-distance fiber optic link, while the cable connecting the bridges to stations might be a short-haul twisted-pair line.
- This arrangement is useful for bridging LANs in different buildings.
- **Operations of a bridge**
- Each bridge operates in promiscuous mode, that is, it accepts every frame transmitted by the stations attached to each of its ports.
- The bridge must decide whether to forward or discard each frame, and, on which port to output the frame. This decision is made by using the destination address.
- As an example, consider the topology of Fig. 4-41(a).
- If station A sends a frame to station B, bridge B1 will receive the frame on port 1.
- This frame can be immediately discarded because it is already on the correct port.
- However, in the topology of Fig. 4-41(b) suppose that A sends a frame to D.
- Bridge B1 will receive the frame on port 1 and output it on port 4.
- Bridge B2 will then receive the frame on its port 4 and output it on its port 1.
- To know that which device is present on which port a bridge maintains a big hash table which carries all the related information
- These values are inserted into the table when the bridge is connected for the first time
- It uses the flooding algorithm to get the information of devices present on various ports
- a flooding algorithm: every incoming frame for an unknown destination is output on all the ports to which the bridge is connected except the one it arrived on.
- The algorithm used by the bridges is backward learning.
- the bridges operate in promiscuous mode, so they see every frame sent on any of their ports. By looking at the source addresses, they can tell which machines are accessible on which ports.
- For example, if bridge B1 in Fig. 4-41(b) sees a frame on port 3 coming from C, it knows that C must be reachable via port 3, so it makes an entry in its hash table.
- Any subsequent frame addressed to C coming in to B1 on any other port will be forwarded to port 3.
- To handle dynamic topologies, whenever a hash table entry is made, the arrival time of the frame is noted in the entry.
- Whenever a frame whose source is already in the table arrives, its entry is updated with the current time.

- Thus, the time associated with every entry tells the last time a frame from that machine was seen.
- The routing procedure for an incoming frame depends on the port it arrives on (the source port) and the address to which it is destined (the destination address).
- The procedure is as follows.
- 1. If the port for the destination address is the same as the source port, discard the frame.
- 2. If the port for the destination address and the source port are different, forward the frame on to the destination port.
- 3. If the destination port is unknown, use flooding and send the frame on all ports except the source port.
- As each frame arrives, this algorithm must be applied,
- **Spanning tree bridges**
- Bridges are genarally used in between pairs of LANs to enhance the reliability of a site
- such enhancements some times cause additional overhead due to the occurrence of loops in topology
- The problem can be solved by representing the topology in the form of a spanning tree that traverse every LAN present in the network
- For example, in Fig. 4-44 we see five bridges that are interconnected and also have stations connected to them. Each station connects to only one bridge.
- There are some redundant connections between the bridges so that frames will be forwarded in loops if all of the links are used.
- This topology can be thought of as a graph in which the bridges are the nodes and the point-to-point links are the edges.
- The graph can be reduced to a spanning tree, which has no cycles by definition, by dropping the links shown as dashed lines in Fig. 4-44.
- Using this spanning tree, there is exactly one path from every station to every other station.
- Once the bridges have agreed on the spanning tree, all forwarding between stations follows the spanning tree.
- Since there is a unique path from each source to each destination, loops are impossible.

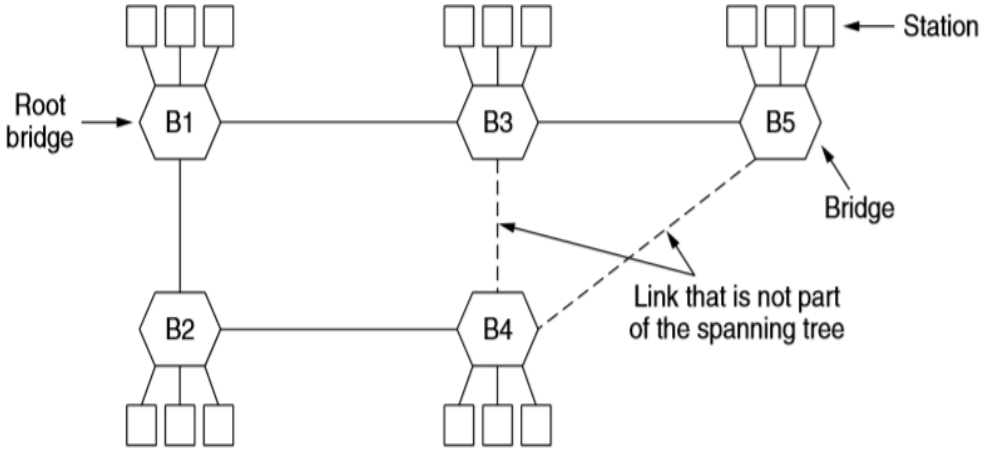


Figure 4-44. A spanning tree connecting five bridges. The dashed lines are links that are not part of the spanning tree.

REPEATERS,HUBS,BRIDGES,SWITCHES,ROUTERS AND GATEWAYS

- **Repeater** – A repeater operates at the physical layer.
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- An important point to be noted about repeaters is that they do not amplify the signal.
- When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength.
- It is a 2 port device.

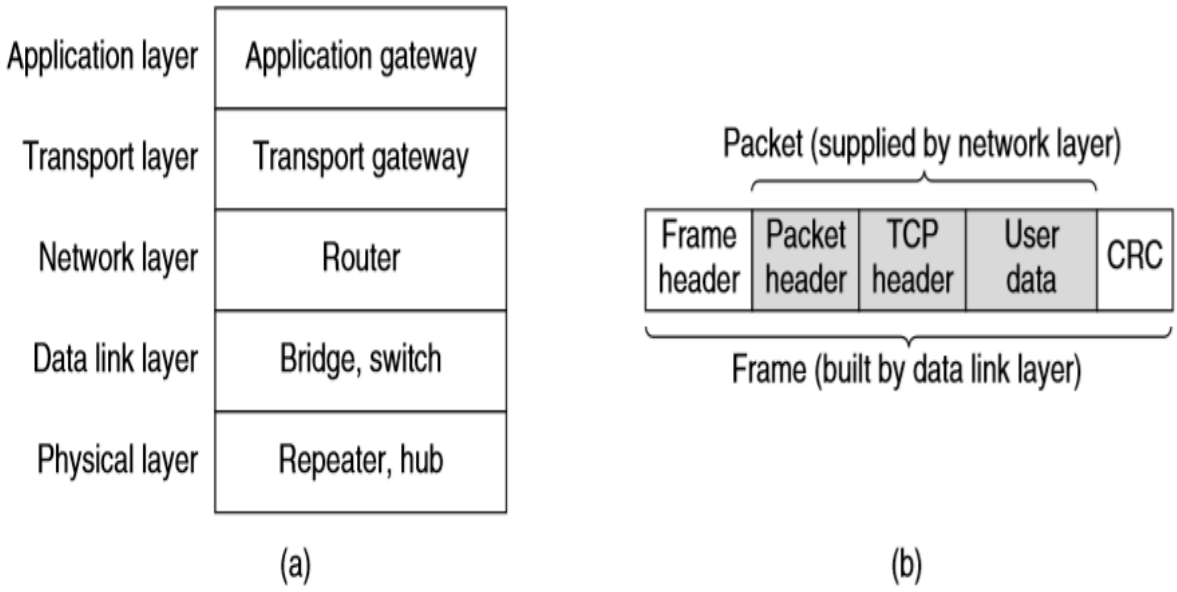
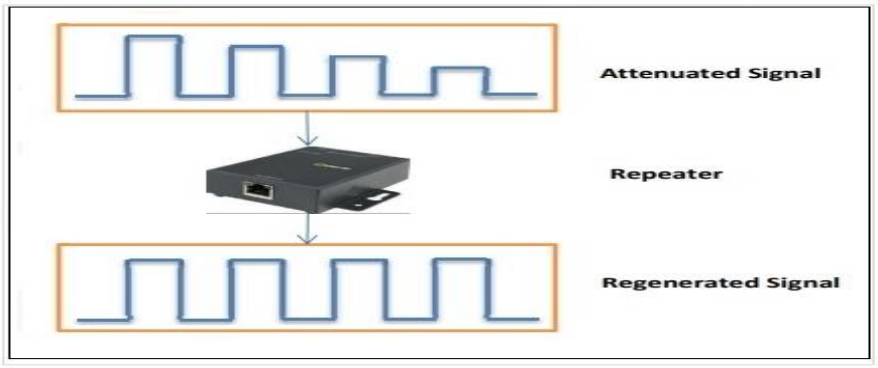


Figure 4-45. (a) Which device is in which layer. (b) Frames, packets, and headers.



- **Hub** – A hub is basically a multiport repeater.
- A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Normally, it is used for Peer to Peer small Home Network.
-
- Types of Hub
- **Active Hub**:- These are the hubs which have their own power supply and can clean, boost and relay the signal along with the network..
- These are used to extend the maximum distance between nodes.

- **Passive Hub** :- These are the hubs which collect wiring from nodes and power supply from active hub.
- These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub** :- It work like active hubs and include remote management capabilities.
- They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.
- **Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination.
- It is also used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, thus making it a 2 port device.
- **Types of Bridges**
- **Transparent Bridges**:- These are the bridge in which the stations are completely unaware of the bridge's existence
- i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary.
- These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- **Source Routing Bridges**:- In these bridges, routing operation is performed by source station and the frame specifies which route to follow.
- The host can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.
- **Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance
- A switch is a data link layer device.
- The switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.
-
- **routers** A router is a device like a switch that routes data packets based on their IP addresses.
- Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets.
- Router divide broadcast domains of hosts connected through it
- **Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.

- They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called protocol converters and can operate at any network layer.
- Gateways are generally more complex than switch or router.