**Assignment 1**

**RITK SINGH 2K19/CO/319**

**Q1**. **Which layer links the network support layers and user support layers?**

**Ans1.**

* The transport layer provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.
* The transport layer is responsible for delivering data to the appropriate application process on the host computers. ... Some transport layer protocols, for example TCP, but not UDP, support virtual circuits, i.e. provide connection-oriented communication over an underlying packet oriented datagram network.
* The transport layer links these layers by segmenting and rearranging the data. It uses protocols like TCP and UDP.

**Q2. What are the concerns of the Physical Layer?**

**Ans2.**

* The physical layer is concerned with actual transfer of data bits across a transmission medium between 2 devices. The physical layer coordinates the functions required to carry a bit stream over a physical medium.
* It deals with the mechanical and electrical specifications of the interface and transmission medium.
* It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur.
* Physical characteristics of interfaces and medium, Representation of bits, data rate, synchronization of bits, line configuration, physical topology, transmission mode.

**Q3.** **What are the responsibilities of Data Link Layer, Network Layer?**

**Ans3.** Theservices provided by Data Link Layer :-

1. Framing
2. Physical Address
3. Flow Control
4. Error Control
5. Access Control

The services which are offered by the network layer :-

1. Packetizing
2. Packet & Forwarding
3. Error Control
4. Flow Control
5. Congestion Control

**Q4.** **What is Bit Stuffing?**

**Ans.** Bit stuffing is the insertion of non information bits into data. Note that stuffed bits should not be confused with overhead bits. Overhead bits are non-data bits that are necessary for transmission (usually as part of headers, checksums etc.).

Applications of Bit Stuffing –

1. synchronize several channels before multiplexing
2. Rate-Match two single channels each other
3. Run length limited coding

**Q5.** **Difference between bit rate and baud rate.**

**Ans.**

| **Bit Rate** | **Baud Rate** |
| --- | --- |
| Bit rate is transmission of number of bits per second. | Baud rate is number of signal units per second. |
| It can be defined as per second travel number of bits. | It can be defined as per second number of changes. |
| Bit rate focusses on computer efficiency. | Baud rate focusses on data transmission. |
| Bit Rate = Baud rate x the number of bit per baud | Baud Rate = Bit rate / the number of bit per baud |

**Q6.** **What is difference between ARP and RARP?**

**Ans.**

|  |
| --- |
|  |
| ARP stands for Address Resolution Protocol. | Whereas RARP stands for Reverse Address Resolution Protocol. |
| Through ARP, (32-bit) IP address mapped into (48-bit) MAC address. | Whereas through RARP, (48-bit) MAC address of 48 bits mapped into (32-bit) IP address. |
| In ARP, broadcast MAC address is used. | While in RARP, broadcast IP address is used. |
| In ARP, ARP table is managed or maintained by local host. | While in RARP, RARP table is managed or maintained by RARP server. |
| In Address Resolution Protocol, Receiver’s MAC address is fetched. | While in RARP, IP address is fetched.  s |
| In ARP, ARP table uses ARP reply for its updation. | While in RARP, RARP table uses RARP reply for configuration of IP addresses . |
| Hosts and routers uses ARP for knowing the MAC address of other hosts and routers in the networks. | While RARP is used by small users having less facilities. |

**ARP**   **RARP**

**Q7.** **What is multicast? What is the motivation for developing multicast?**

**Ans.** **Multicast** is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network.

**Benefits of the multicast technology**

The multicast technology offers great advantages to the success of some advanced applications. A few of these advantages are presented below.

**optimized network performance:**

The intelligent use of network resources avoids unnecessary flow replication. This way, an economy in terms of passing band is achieved through a better architecture to distribute the data.

**support to distributed applications:**

Multicast technology is directed towards distributed applications. Multimedia applications such as distance learning and videoconference can be used in the network in a measurable and effective way.

**resource economy:**

The cost of the network resources is reduced through the passing band economy in the links and the processing economy in servers and network equipment. New applications and services can be implanted, without requiring the renovation of network resources.

**scalability:**

The effective use of the network and the reduction of the load in traffic sources permit services and applications to be accessed by a great number of participants. Consequently, services that run on multicast can be easily dimensioned, distributing packages both to few and to a lot of receivers.

**more network availability:**

The economy of network resources associated to the reduction of the load in the applications and servers makes the network less susceptible to jams, and, therefore, more available to be used.

**Q8. Explain ISO/OSI reference model.**

**Ans.**

**The OSI Reference Model:**

This reference model is proposed by International standard organization (ISO) as a a first step towards standardization of the protocols used in various layers in 1983 by Day and Zimmermann. This model is called Open system Interconnection (OSI) reference model. It is referred OSI as it deals with connection open systems. That is the systems are open for communication with other systems. It consists of seven layers.

Layers of OSI Model:

The principles that were applied to arrive at 7 layers:

1. A layer should be created where a different level of abstraction is needed.
2. Each layer should perform a well defined task.
3. The function of each layer should define internationally standardized protocols
4. Layer boundaries should be chosen to minimize the information flow across the interface.
5. The number of layers should not be high or too small.

The ISO-OSI reference model is as shown in figure 2.5. As such this model is not a network architecture as it does not specify exact services and protocols. It just tells what each layer should do and where it lies. The bottom most layer is referred as physical layer. ISO has produced standards for each layers and are published separately.

**Q9. Explain error detection and error correction techniques.**

**Ans.**

**Error Detection**

When data is transmitted from one device to another device, the system does not guarantee whether the data received by the device is identical to the data transmitted by another device. An Error is a situation when the message received at the receiver end is not identical to the message transmitted.

**Types Of Errors**

Errors can be classified into two categories:

1. Single-Bit Error
2. Burst Error

**Error Correction**

Error Correction codes are used to detect and correct the errors when data is transmitted from the sender to the receiver.

Error Correction can be handled in two ways:

* **Backward error correction:** Once the error is discovered, the receiver requests the sender to retransmit the entire data unit.
* **Forward error correction:** In this case, the receiver uses the error-correcting code which automatically corrects the errors.

A single additional bit can detect the error, but cannot correct it.

**Q10. Explain detail about IEEE 802.3 MAC sub-layer.**

**Ans.**

IEEE 802.3 is a set of standards and protocols that define Ethernet-based networks. Ethernet technologies are primarily used in LANs, though they can also be used in MANs and even WANs. IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

**Frame Format of IEEE 802.3**

The main fields of a frame of classic Ethernet are -

**1. Preamble:** The first field of the 802.3 frames, the preamble, contains  
    seven bytes (56 bits) of alternating O's and 1's that alerts the receiving  
    system to the coming frame and enable it to synchronize its input timing.  
**2. Start Frame Delimiter (SFD):** The second field (one byte: 10101011)  
    of the 802.3 frame signals at the beginning of the frame. The SFD tells the receiver that everything that follows is data, starting with the addresses.  
**3. Destination Address (DA):** The Destination Address (DA) field is allotted six bytes and contains the physical address of the packet's next destination. A system's physical address is a bit pattern encoded on its Network Interface Card (NIC).  
**4. Source Address (SA):** The source address (SA) field is also allotted six bytes and contains the physical address of the last device to forward the packet. That device can be the sending station or the most recent router  
to receive and forward the packet.

**5. Length/Type of Protocol Data Unit (PDU):** These next two bytes indicate the number of bytes in the coming PDU. If the length of the PDU is fixed, this field can be used to indicate type, or as the base for other protocols.

**6. Data:** This field can be split up into two parts Data (0-1500 bytes) and padding (0- 46 bytes.)

**7. CRC:**  The last field in the 802.3 frames contains the error detection information, in this case, a CRC-32.

**Q11.** **Explain about Ethernet.**

**Ans.**

Ethernet is the standard way to connect computers on a [network](https://techterms.com/definition/network) over a [wired](https://techterms.com/definition/wired) connection. It provides a simple [interface](https://techterms.com/definition/interface) and for connecting multiple devices, such computers, [routers](https://techterms.com/definition/router), and [switches](https://techterms.com/definition/switch). With a single router and a few Ethernet cables, you can create a [LAN](https://techterms.com/definition/lan), which allows all connected devices to communicate with each other.

A standard Ethernet cable is slightly thicker than a phone cable and has an [RJ45](https://techterms.com/definition/rj45) connector on each end. Ethernet [ports](https://techterms.com/definition/port) look similar to telephone jacks, but are slightly wider. You can plug or unplug devices on an Ethernet network while they are powered on without harming them.

Like [USB](https://techterms.com/definition/usb), Ethernet has multiple standards that all use the same interface. These include:

* 10BASE-T - supports up to 10 Mbps
* 100BASE-T - supports up to 100 Mbps
* 1000BASE-T (also called "[Gigabit](https://techterms.com/definition/gigabit) Ethernet") - supports up to 1,000 Mbps

Most Ethernet devices are backwards compatible with lower-speed Ethernet cables and devices. However, the connection will only be as fast as the lowest common denominator. For example, if you connect a computer with a 10BASE-T [NIC](https://techterms.com/definition/nic) to a 100BASE-T network, the computer will only be able to send and receive data at 10 Mbps. If you have a Gigabit Ethernet router and connect devices to it using 100BASE-T cables, the maximum [data transfer rate](https://techterms.com/definition/datatransferrate) will be 100 Mbps.

While Ethernet is still the standard for wired networking, it has been replaced in many areas by [wireless](https://techterms.com/definition/wireless) networks. [Wi-Fi](https://techterms.com/definition/wi-fi) allows you to connect your [laptop](https://techterms.com/definition/laptop) or [smartphone](https://techterms.com/definition/smartphone) to a network without being tethered to the wall by a cable. The [802.11ac](https://techterms.com/definition/80211ac) Wi-Fi standard even provides faster maximum data transfer rates than Gigabit Ethernet. Still, wired connections are less prone to interference and are more secure than wireless ones, which is why many businesses and organizations still use Ethernet.

**Q12.** **Explain different error detection and correction mechanisms with examples.**

**Ans.**

**Error Detection:**

When a message is sent, it may be jumbled by noise or the data may be damaged. To avoid this, we employ error-detecting codes, which are bits of extra data appended to a digital message to assist us detect whether an error occurred during transmission.

**Error Detection Techniques:**

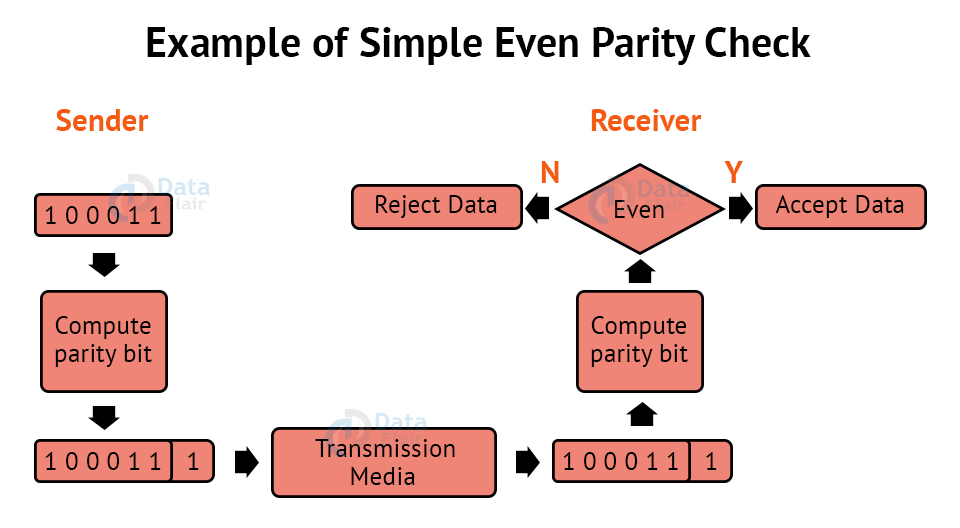
**1. Simple Parity Check:**

One extra bit is transmitted in addition to the original bits to make the number of 1s even in the case of even parity or odd in the case of odd parity.

While creating a frame, the sender counts the amount of 1s in it. If even parity is utilised and the number of 1s is even, one bit with the value 0 is added. In this manner, the number of 1s remains even. If the number of 1s is odd, a value 1 is added to make it even.

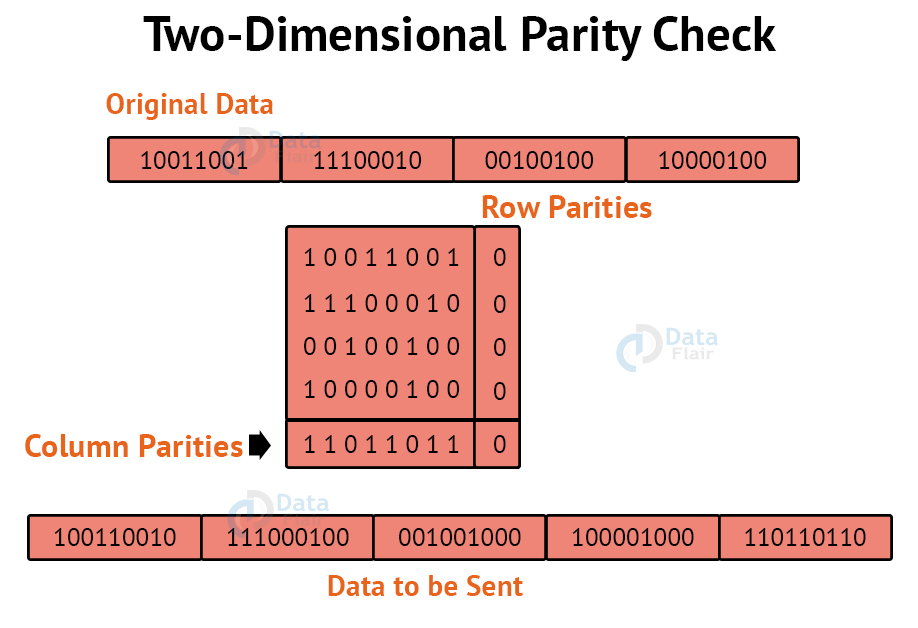
The receiver just counts how many 1s are in a frame. If the number of 1s is even and even parity is utilised, the frame is regarded as uncorrupted and approved. Even if the number of 1s is odd and odd parity is utilised, the frame is not damaged.

The receiver can identify a single bit flip in transit by counting the number of 1s. However, when more than one bit is incorrect, it is extremely difficult for the receiver to identify the problem.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/simple-parity-check.jpg)

**2. Two-Dimensional Parity Check:**

For each row, parity check bits are calculated, which is identical to a basic parity check bit. For each column, parity check bits are computed and transmitted together with the data. These are compared with the parity bits calculated on the received data at the receiving end.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/two-dimensional-parity-check.jpg)

**3. Checksum:**

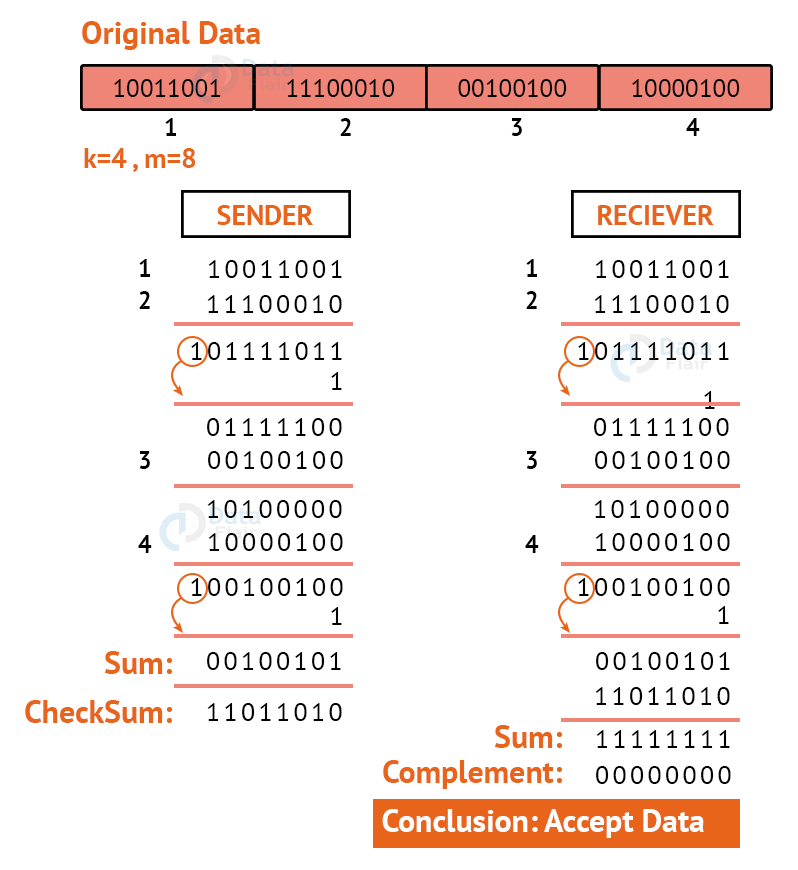
The data is split into k segments of m bits each in the checksum error detection technique.

To get the total, the segments are summed at the sender’s end using 1’s complement arithmetic. To obtain the checksum, a complement of the sum is taken.

The checksum segment is sent with the data segments.

To obtain the total, all received segments are summed using 1’s complement arithmetic at the receiver’s end. The sum is then calculated.

If the result is 0, the data is accepted; otherwise, it is rejected.

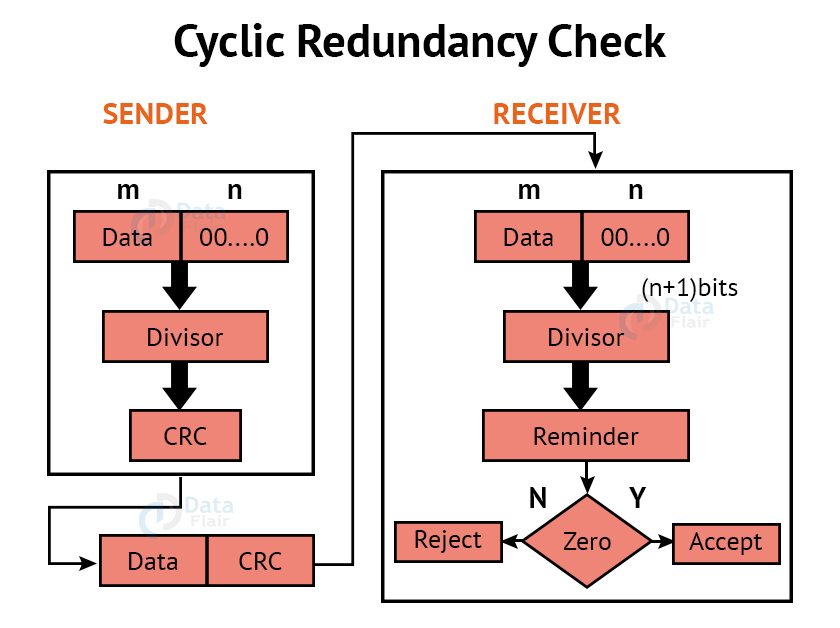
[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/checksum.jpg)

**4. Cyclic Redundancy Check:**

CRC is an alternative method for determining whether or not a received frame includes valid data. The binary division of the data bits being delivered is used in this approach. Polynomials are used to generate the divisor.

The sender divides the bits that are being transferred and calculates the remainder. The sender inserts the remainder at the end of the original bits before sending the actual bits. A codeword is made up of the actual data bits plus the remainder. The transmitter sends data bits in the form of codewords.

The receiver, on the other hand, divides the codewords using the same CRC divisor. If the remainder consists entirely of zeros, the data bits are validated; otherwise, it is assumed that some data corruption happened during transmission.

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/cyclic-redundancy-check.jpg)

**Error Correction:**

Error Correction codes are used to detect and repair mistakes that occur during data transmission from the transmitter to the receiver.

**There are two approaches to error correction:**

**1. Backward Error Correction:**

When a backward mistake is detected, the receiver requests that the sender retransmit the complete data unit.

**2. Forward Error Correction:**

In this scenario, the error-correcting code is used by the receiver, which automatically corrects the mistakes.

A single extra bit can identify but not repair the mistake.

To correct the mistakes, the specific location of the error must be known. If we wish to compute a single-bit mistake, for example, the error correcting algorithm will identify which one of seven bits is incorrect. We will need to add some more redundant bits to do this.

The number of redundant bits is calculated using the following formula:

2r>=d+r+1

The above formula is used to compute the value of r. For example, if the value of d is 4, the least possible number that fulfils the above relation is 3.

**Error Correction Techniques:**

**1. Hamming Code:**

**Parity bits:** A bit that is added to the original binary data to make sure the total number of 1s is even or odd (in case of even or odd parity respectively).

Even parity: To check for even parity, if the total number of 1s is even, the parity bit value is 0. If the total number of occurrences of 1s is odd, the parity bit value is 1.

**Odd Parity:** To test for odd parity, if the total number of 1s is even, the parity bit value is 1. If the total number of 1s is odd, the parity bit value is 0.

To produce d+r, an information of ‘d’ bits is added to the redundant bits ‘r’.

Each (d+r) digit’s position is assigned a decimal value.

The ‘r’ bits are assigned to locations 1, 2,….2k-1.

The parity bits are recalculated at the receiving end. The position of an error is determined by the decimal value of the parity bits.

**Example: If the data to be transmitted is 1011001**

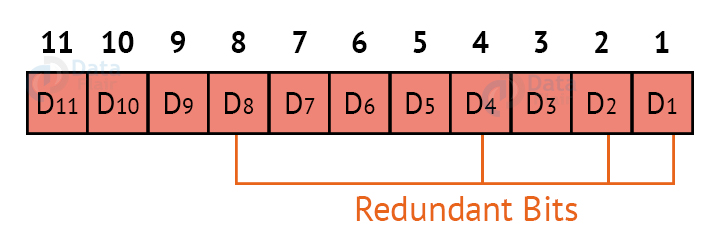
Number of data bits = 7

Thus, number of redundancy bits = 4

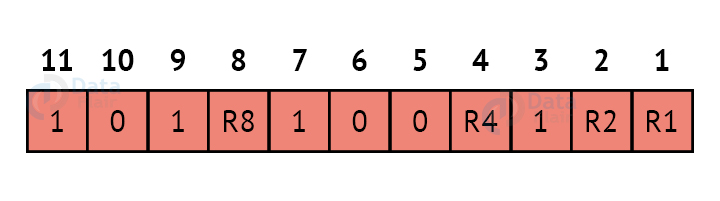
Total bits = 7+4 = 11

Redundant bits are always placed at positions that correspond to the power of 2, so the redundant bits will be placed at positions: 1,2,4 and 8.

Redundant bits will be placed here:

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-01.jpg)

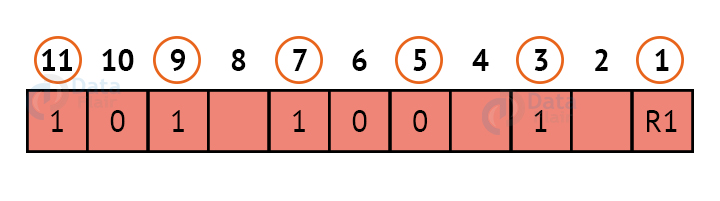
Thus now, all the 11 bits will look like this:

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-02.jpg)

Here, R1, R2, R4 and R8 are the redundant bits.

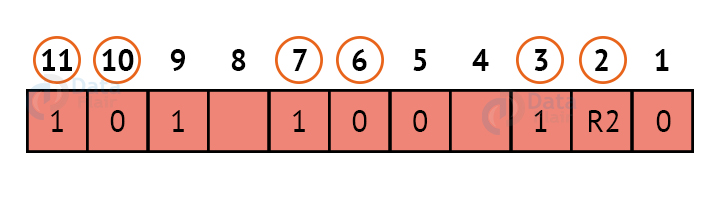
Determining the parity bits:

**R1:**

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-03.jpg)

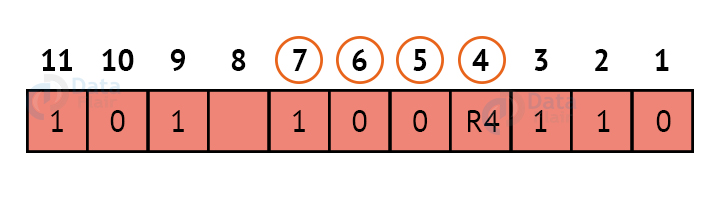
We look at bits 1,3,5,7,9,11 to calculate R1. In this case, because the number of 1s in these bits together is even, we make the R1 bit equal to 0 to maintain even parity.

**R2:**

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-04.jpg)

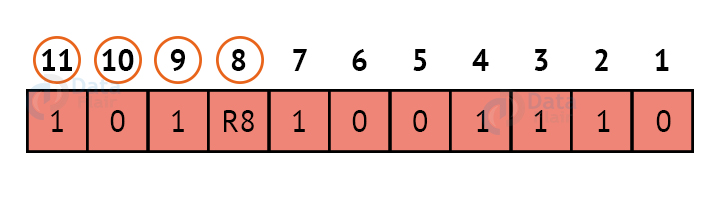
We look at bits 2,3,6,7,10,11 to calculate R2. In this case, because the number of 1s in these bits together is odd, we make the R2 bit equal to 1 to maintain even parity.

**R4:**

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-05.jpg)

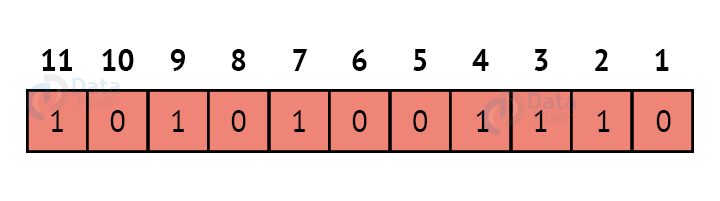
We look at bits 4,5,6,7 to calculate R4. In this case, because the number of 1s in these bits together is odd, we make the R4 bit equal to 1 to maintain even parity.

**R8:**

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-06.jpg)

We look at bits 8,9,10,11 to calculate R8. In this case, because the number of 1s in these bits together is even, we make the R8 bit equal to 0 to maintain even parity.

Thus, the final block of data which is transferred looks like this:

[](https://data-flair.training/blogs/wp-content/uploads/sites/2/2021/09/hamming-code-07.jpg)

**Q13.** **Explain different flow control mechanisms used in brief.**

**Ans.**

Flow control is basically technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgment from receiver.

There are basically two types of techniques being developed to control the flow of data :-

**1. Stop-and-Wait Flow Control :**This method is the easiest and simplest form of flow control. In this method, basically message or data is broken down into various multiple frames, and then receiver indicates its readiness to receive frame of data. When acknowledgment is received, then only sender will send or transfer the next frame.

This process is continued until sender transmits EOT (End of Transmission) frame. In this method, only one of frames can be in transmission at a time. It leads to inefficiency i.e. less productivity if propagation delay is very much longer than the transmission delay.

**Advantages –**

This method is very easiest and simple and each of the frames is checked and acknowledged well.

It can also be used for noisy channels.

This method is also very accurate.

**Disadvantages –**

This method is fairly slow.

In this, only one packet or frame can be sent at a time.

It is very inefficient and makes the transmission process very slow.

**2. Sliding Window Flow Control :**This method is required where reliable in-order delivery of packets or frames is very much needed like in data link layer. It is point to point protocol that assumes that none of the other entity tries to communicate until current data or frame transfer gets completed. In this method, sender transmits or sends various frames or packets before receiving any acknowledgment.

In this method, both the sender and receiver agree upon total number of data frames after which acknowledgment is needed to be transmitted. Data Link Layer requires and uses this method that simply allows sender to have more than one unacknowledged packet “in-flight” at a time. This increases and improves network throughput.

**Advantages –**

It performs much better than stop-and-wait flow control.

This method increases efficiency.

Multiples frames can be sent one after another.

**Disadvantages –**

The main issue is complexity at the sender and receiver due to the transferring of multiple frames.

The receiver might receive data frames or packets out the sequence.

**Q14.** What is framing? Explain different types of framing protocols with their format.

**Ans.** Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy. Frame is continuously used in Time Division Multiplexing process.

Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

**Types of framing** – There are two types of framing:

**1. Fixed size** – The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.

Drawback: It suffers from internal fragmentation if the data size is less than the frame size

Solution: Padding

**2. Variable size** – In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish. This can be done in two ways: 

1. Length field – We can introduce a length field in the frame to indicate the length of the frame. Used in Ethernet(802.3). The problem with this is that sometimes the length field might get corrupted.
2. End Delimiter (ED) – We can introduce an ED(pattern) to indicate the end of the frame. Used in Token Ring. The problem with this is that ED can occur in the data. This can be solved by:

* Character/Byte Stuffing: Used when frames consist of characters. If data contains ED then, a byte is stuffed into data to differentiate it from ED.

Let ED = “$” –> if data contains ‘$’ anywhere, it can be escaped using ‘\O’ character.   
–> if data contains ‘\O$’ then, use ‘\O\O\O$'($ is escaped using \O and \O is escaped using \O).

**Disadvantage** – It is very costly and obsolete method.

1. Bit Stuffing: Let ED = 01111 and if data = 01111   
   –> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data = 011101.   
   –> Receiver receives the frame.   
   –> If data contains 011101, receiver removes the 0 and reads the data.

**Q15. Explain how network software is implemented in networks.**

**Ans.** Network software encompasses a broad range of software used for design, implementation, and operation and monitoring of computer networks. Traditional networks were hardware based with software embedded. With the advent of Software – Defined Networking (SDN), software is separated from the hardware thus making it more adaptable to the ever-changing nature of the computer network.

A software defined network uses a centralized SDN controller to deliver software-based network services. A network administrator can manage network policies from a central control plane without having to handle individual switches.

SDN architecture has three layers that communicate via northbound and southbound application programming interfaces (APIs). Applications can use a northbound interface to talk to the controller. Meanwhile, the controller and switches can use southbound interfaces to communicate.

**The layers include:**

* Application layer — SDN applications communicate behaviors and needed resources with the SDN controller.
* Control layer — Manages policies and traffic flow. The centralized controller manages data plane behavior.
* Infrastructure layer — Consists of the physical switches in the network.