Illustrate various types of transmission errors with example

ANS : Transmission errors refer to any type of errors that occur during the transmission of data across a network. There are several types of transmission errors, and here are some examples of each type:

Single Bit Error:

A single bit error occurs when a single bit is flipped during transmission. For example, let's say you want to send the binary message 10101010, but during transmission, the first bit is flipped, resulting in 11101010. This error can be caused by electromagnetic interference or noise in the communication channel.

Burst Error:

A burst error occurs when multiple bits in a contiguous block are corrupted during transmission. For example, let's say you want to send the binary message 10101010, but during transmission, a burst of three bits in the middle of the message is corrupted, resulting in 10101111. This error can be caused by interference from other signals or poor quality of the communication channel.

Delayed Error:

A delayed error occurs when the error in transmission is not immediately detected, and the data is stored with errors. For example, let's say you want to send the text message "Hello, how are you?" but during transmission, some characters are corrupted, resulting in "Hello, h@w are you?". If the receiver does not detect the error immediately, the corrupted message will be stored in their system, and the error may not be detected until much later.

Lost Packets:

Lost packets occur when a packet of data is lost during transmission and does not reach its intended destination. For example, let's say you want to send a large file over the internet, but during transmission, some packets are lost due to congestion or network failure. If the lost packets are not retransmitted, the file will be incomplete and unusable.

Duplicate Packets:

Duplicate packets occur when multiple copies of the same packet are received by the receiver. For example, let's say you want to send a packet of data, but due to network congestion, multiple copies of the same packet are sent. If the receiver does not detect the duplicates and removes them, the data may be corrupted, and the receiver may not be able to use it correctly.

Illustrate the process of error detecting using block coding with the help of a neat diagram

Ans..) Block coding is a technique that adds redundant bits to a message to enable the detection and correction of errors. The redundant bits are added to the message at the sender's end and removed at the receiver's end.

Here is a step-by-step process of error detecting using block coding:

Message Encoding:

The sender takes the original message and divides it into fixed-sized blocks, each of which has k bits. The sender then adds n-k redundant bits to each block to form a codeword of n bits. The process of adding redundant bits is called encoding. The resulting codeword is transmitted to the receiver.

Channel Transmission:

The codeword is transmitted over a channel to the receiver. During transmission, the codeword may be corrupted due to noise, interference, or other factors.

Error Detection:

The receiver receives the codeword and checks it for errors. The receiver compares the received codeword with the original codeword to check if any errors occurred during transmission. If there are no errors, the receiver can use the original message. If there are errors, the receiver can request a retransmission of the codeword.

Error Correction:

In some cases, the receiver can correct the errors in the received codeword using error-correcting codes. Error-correcting codes add additional redundancy to the codeword to enable the correction of errors. If the receiver detects errors in the received codeword, it uses the error-correcting codes to correct the errors before using the original message.

Here is a diagram that illustrates the process of error detecting using block coding:

```
 Original Message     +-------------------+

      |          |            |

      v          v            |

   Encoding      Channel        Decoding

      |          |            |

      v          v            |

  Codeword       Received       Detected Errors

                Codeword            |

                  |            |

                  v            v
```

Errors Error Correction

In this diagram, the original message is encoded using block coding to form a codeword, which is then transmitted over the channel. The receiver receives the codeword and checks it for errors. If errors are detected, the receiver requests a retransmission of the codeword. If errors can be corrected, the receiver uses error-correction codes to correct the errors before using the original message.

24) Write a short note on Cyclic codes.

Ans..) Cyclic codes are a type of error-correcting code used in digital communications. They are called cyclic codes because they can be generated by shifting a code word cyclically and then adding it to the original code word. This cyclic shifting property makes cyclic codes very useful in digital communications because they can detect and correct errors that occur during transmission.

Cyclic codes are often represented using a polynomial notation, where the coefficients of the polynomial correspond to the bits of the code word. The polynomial is divided by a generator polynomial, which is a polynomial of degree n-k, where n is the length of the codeword and k is the number of information bits. The remainder of the polynomial division is the cyclic redundancy check (CRC) code, which is added to the original code word to form the transmitted codeword.

Cyclic codes can correct a limited number of errors depending on the length of the codeword and the degree of the generator polynomial. The Hamming distance of a cyclic code is the minimum number of bit positions at which any two distinct code words differ. The larger the Hamming distance, the more errors a cyclic code can detect and correct.

One common type of cyclic code is the cyclic redundancy check (CRC) code, which is widely used in communication systems such as Ethernet and Wi-Fi. CRC codes use a fixed generator polynomial that is agreed upon by the sender and receiver, and the sender adds the CRC code to the original message before transmission.

26) Compare simplest protocol and stop-and-wait protocol for noiseless channels

Ans..) The simplest protocol and the stop-and-wait protocol are both designed to reliably transmit data over a noiseless channel. However, they differ in their efficiency and complexity.

The simplest protocol is also known as the "naive" or "send-and-wait" protocol. In this protocol, the sender simply sends a packet and waits for an acknowledgment from the receiver before sending the next packet. If the sender does not receive an acknowledgment within a certain time period, it assumes that the packet was lost and retransmits it. This process continues until the receiver acknowledges receipt of the packet.

The stop-and-wait protocol, on the other hand, is a more sophisticated protocol that reduces the number of retransmissions required. In this protocol, the sender sends a packet and waits for an acknowledgment from the receiver. If the sender receives an acknowledgment, it sends the next packet. However, if the sender does not receive an acknowledgment within a certain time period, it assumes that the packet was lost and retransmits it. In addition, the sender waits for an acknowledgment before sending any further packets, which prevents the receiver from becoming overwhelmed with packets.

In terms of efficiency, the stop-and-wait protocol is more efficient than the simplest protocol because it reduces the number of retransmissions required.

27) Compare Stop-and-wait ARQ with Go-back-n ARQ for noisy channel

Ans..) Stop-and-wait ARQ (Automatic Repeat reQuest) and Go-Back-N ARQ are two common error control protocols used in communication systems for transmitting data over noisy channels. They both use a form of retransmission to recover from errors, but they differ in their efficiency and effectiveness in noisy channels.

Stop-and-wait ARQ sends a single packet at a time and waits for an acknowledgment from the receiver before sending the next packet. If the sender does not receive an acknowledgment within a timeout period, it retransmits the packet. This protocol is simple to implement and works well in low-noise channels, but it can be inefficient in noisy channels as it requires waiting for an acknowledgment for each packet.

Go-Back-N ARQ, on the other hand, sends multiple packets at once and uses a sliding window to keep track of the packets. The receiver sends an acknowledgment for the packets it has received, and the sender only retransmits the packets that have not been acknowledged. This protocol is more efficient than Stop-and-wait ARQ as it allows for multiple packets to be in transit at once, but it can be less effective in noisy channels as a single lost packet can cause the retransmission of many packets.

In summary, Stop-and-wait ARQ is simple to implement but can be inefficient in noisy channels, while Go-Back-N ARQ is more efficient but can be less effective in noisy channels.

28) Define logical address and explain how it is different from MAC Address

Ans..) A logical address is a network layer address that is used to identify a device on a network, while a MAC address is a data link layer address that is used to identify the physical address of a device on a network.

A logical address, also known as an IP address, is assigned to a device by the network administrator or by a dynamic host configuration protocol (DHCP) server. It is used to identify the device on the network and to enable communication between devices on different networks. Logical addresses are hierarchical, with the most significant bits identifying the network and the least significant bits identifying the host.

In contrast, a MAC address, also known as a physical address, is hard-coded into a device's network interface card (NIC) and uniquely identifies the device on the local network. MAC addresses are used by the data link layer protocols, such as Ethernet, to enable communication between devices on the same network segment. Unlike logical addresses, MAC addresses are not hierarchical and are assigned by the manufacturer of the NIC.

The main difference between logical addresses and MAC addresses is that logical addresses are used to identify devices on a network regardless of their physical location, while MAC addresses are used to identify devices on the local network segment

29) Illustrate various classes of IP

Ans...) IP (Internet Protocol) addresses are divided into several classes based on their network architecture. The IP address classes are:

Class A:

Class A IP addresses have the highest order bit set to 0 and are used for networks with a large number of hosts. The first octet of a Class A IP address is used to identify the network, while the remaining three octets are used to identify the host. Class A IP addresses range from 0.0.0.0 to 127.255.255.255, with 0.0.0.0 and 127.0.0.1 being reserved.

Class B:

Class B IP addresses have the first two bits set to 10 and are used for medium-sized networks. The first two octets of a Class B IP address identify the network, while the remaining two octets identify the host. Class B IP addresses range from 128.0.0.0 to 191.255.255.255.

Class C:

Class C IP addresses have the first three bits set to 110 and are used for small networks. The first three octets of a Class C IP address identify the network, while the last octet identifies the host. Class C IP addresses range from 192.0.0.0 to 223.255.255.255.

Class D:

Class D IP addresses have the first four bits set to 1110 and are used for multicasting. Class D IP addresses range from 224.0.0.0 to 239.255.255.255.

Class E:

Class E IP addresses have the first five bits set to 11110 and are reserved for future use. Class E IP addresses range from 240.0.0.0 to 247.255.255.255.

34) Explain IPV4 datagram format

Ans...) The IPv4 datagram is the basic unit of data in an IPv4 network. It is a packet of information that is sent from one device to another over a network. Here is a breakdown of the IPv4 datagram format:

Version (4 bits): This field identifies the version of the Internet Protocol being used, which is usually set to 4 for IPv4.

Header length (4 bits): This field specifies the length of the IP header in 32-bit words.

Type of Service (8 bits): This field is used to define the quality of service required for the packet.

Total Length (16 bits): This field specifies the total length of the IPv4 datagram in bytes.

Identification (16 bits): This field is used for fragmentation and reassembly of packets.

Flags (3 bits): These bits are used to control fragmentation of the packet.

Fragment Offset (13 bits): This field is used to indicate the position of the data in the original packet.

Time to Live (8 bits): This field specifies the number of hops the packet can take before it is discarded.

Protocol (8 bits): This field specifies the type of data carried in the payload of the packet, such as TCP or UDP.

Header Checksum (16 bits): This field is used to check the integrity of the header.

Source IP Address (32 bits): This field specifies the IP address of the sender.

Destination IP Address (32 bits): This field specifies the IP address of the receiver.

Options (variable): This field is used to provide additional information, such as security or routing information, in the header.

37) Explain multi-casting basics in details

Ans..) Multicasting is a method of sending data to multiple receivers in a network. Instead of sending a copy of data to each receiver individually, a single copy of data is sent to a multicast address, which is then distributed to all the receivers who have subscribed to that address. This method is more efficient than unicast (one-to-one) or broadcast (one-to-all) transmissions, especially in networks with a large number of receivers.

Multicasting is widely used in applications such as video conferencing, online gaming, and content delivery networks. To understand multicasting in more detail, let's look at some of the basics of how it works.

Multicast Addressing:

In multicasting, the destination address is a multicast address, which is a special class of IP address that represents a group of receivers. Multicast addresses start with the prefix "224." and are followed by three octets that identify the multicast group. For example, the address 224.0.0.1 represents all hosts on the network.

Multicast Group Membership:

To receive multicast data, a host must be a member of the multicast group. This is accomplished through a membership protocol, such as the Internet Group Management Protocol (IGMP), which allows hosts to join or leave multicast groups dynamically. When a host joins a multicast group, it sends an IGMP message to the multicast router indicating its interest in receiving data for that group. The multicast router then adds the host's address to the list of members for that group.

Multicast Routing:

Multicast routing is the process of distributing multicast traffic across a network. In a multicast-enabled network, there are multicast routers that maintain information about multicast groups and their members. When a source sends data to a multicast address, the multicast router receives the data and forwards it only to the members of the group. This is done using multicast routing protocols such as Protocol Independent Multicast (PIM) or Multicast Source Discovery Protocol (MSDP).

Multicast Trees:

Multicast trees are used to efficiently deliver multicast data to all members of a multicast group. In a multicast tree, the source node is at the root of the tree, and each branch of the tree represents a path to a multicast group member. The branches of the tree are created dynamically as hosts join or leave the multicast group, and multicast routers use multicast routing protocols to build the tree and distribute data to all members of the group.

38) Explain Multicasting with example

Ans..) Let's say you have a group of users who want to watch a live video stream of a conference, but they are located in different parts of the world. Instead of sending a separate stream to each user, which would consume a large amount of bandwidth, you can use multicasting to deliver the stream to all of them simultaneously.

The live video stream would be sent from the conference location to a multicast router on the network. The multicast router would then replicate the stream and send it only to the members of the multicast group who have expressed interest in receiving the stream.

For example, let's say there are 100 users who want to watch the video stream. Each user would join the multicast group by sending an IGMP message to the multicast router indicating their interest in receiving the video stream. The multicast router would then add the user's address to the list of members for that group.

As the live video stream is being sent, the multicast router replicates the data and sends it to all the members of the multicast group, who can then watch the video stream in real-time.

This method of multicasting saves a lot of bandwidth and network resources, as the video stream is sent only once and then replicated to all members of the multicast group. It also ensures that all members receive the same quality of video, as the stream is not affected by network congestion or delays caused by sending multiple copies of the data to each individual user.

39) Write a short note on OSPF and IGMP protocols

Ans...) OSPF (Open Shortest Path First) and IGMP (Internet Group Management Protocol) are two important protocols used in computer networks.

OSPF is a link-state routing protocol that is used to determine the shortest path for data to travel between two points on a network. OSPF routers exchange information about network topology to build a complete map of the network. This information is used to calculate the shortest path to a destination network. OSPF is a scalable protocol that can be used in networks of all sizes, from small office networks to large enterprise networks. OSPF is widely used in enterprise networks, including those of service providers.

IGMP is a network-layer protocol that is used to manage multicast group memberships. When a device wants to receive multicast traffic, it sends an IGMP join message to its local router, which in turn sends an IGMP query to the multicast group. Devices that are members of the multicast group respond to the query, allowing the router to determine which devices are interested in receiving the multicast traffic. IGMP is used to optimize the distribution of multicast traffic and prevent unnecessary traffic on the network.