**DATA COMMUNIATIONS**

1.What are components of communiation system?

**1)Message**

* Message is the information (or data) to be communicated.
* Message may consist of
* number/text
* picture or
* audio/video

**2) Sender**

* Sender is the device that sends the data-message.
* Sender can be

1. computer and
2. mobile phone

**3) Receiver**

* Receiver is the device that receives the message.
* Receiver can be

1. computer and
2. mobile phone

**4)Transmission Medium**

* Transmission-medium is physical-path by which a message travels from sender to receiver.
* Transmission-medium can be wired or wireless.
* Examples of wired medium:

1. twisted-pair wire (used in landline telephone)
2. coaxial cable (used in cable TV network) →
3. fiber-optic cable

* Examples of wireless medium:

1. radio waves
2. microwaves
3. infrared waves (ex: operating TV using remote control)

**5) Protocol**

* A protocol is a set of rules that govern data-communications.
* In other words, a protocol represents an agreement between the communicating-devices.
* Without a protocol, 2 devices may be connected but not communicating.

2)Explain the OSI Model?

The OSI, or Open System Interconnection, model defines a networking framework for

implementing protocols in seven layers. Control is passed from one layer to the next, starting

at the application layer in one station, proceeding to the bottom layer, over the channel to the

next station and back up the hierarchy.

**Application (Layer 7)**

This layer supports application and end-user processes. This layer provides application

services for file transfers, e-mail, and other network software services. HTTP, E-Mail and

FTP are applications that exist entirely in the application level.

**Presentation (Layer 6)**

This layer provides independence from differences in data representation (e.g., encryption) by

translating from application to network format, and vice versa. The presentation layer works

to transform data into the form that the application layer can accept. It is sometimes called the

syntax layer.

**Session (Layer 5)**

This layer establishes, manages and terminates connections between applications. The session

layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between

the applications at each end. It deals with session and connection coordination.

**Transport (Layer 4)**

This layer provides transparent transfer of data between end systems, or hosts, and is

responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

The two main protocols used in transport layer is TCP (Transmission Control Protocol) and

UDP (User Datagram Protocol). Data is called as segments in transport layer.

**Network (Layer 3)**

This layer provides switching and routing technologies, creating logical paths, known as

virtual circuits, for transmitting data from node to node. Routing and forwarding are

functions of this layer, as well as addressing, internetworking, error handling, congestion

control and packet sequencing. Data is called as packets/ datagram.

**Data Link (Layer 2)**

At this layer, data packets are encoded and decoded into bits. It furnishes transmission

protocol knowledge and management and handles errors in the physical layer, flow control

and frame synchronization. Data is called as frames.

**Physical (Layer 1)**

This layer conveys the bit stream into electrical impulse, light or radio signal. It provides the

hardware means of sending and receiving data on a carrier, including defining cables, cards

and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer

components

3)Explain delay, loss and throughput with formula?

**DELAY**

When the expected data does not arrive on the receiver end at a desired time, the packet is said to be in delay. Based on the purpose of delay, the delay is classified into

1. Processing delay

2. Queueing delay

3. Transmission delay

4. Propagation delay

**TYPES OF DELAY**

**1. Processing Delay**

* + - * The time required to examine the packet’s header and determine where to direct the packet is part of the processing delay.
      * The processing delay can also include other facts, such as the time needed to check for bit-level errors in the packet.
        + A Processing delays in high-speed routers are typically on the order microseconds or less.

**2. Queuing Delay**

* + - * + At the queue, the packet experiences a queuing delay as it waits to be transmitted onto the link.
        + The length of the queuing delay of a specific packet will depend on the number of earlier-arriving packets that are queued and waiting for transmission onto the link.
        + If the queue is empty and no other packet is currently being transmitted, then our packet’s queuing delay will be zero.
        + On the other hand, if the traffic is heavy and many other packets are also waiting to be transmitted, the queuing delay will be long.
* Queuing delays can be on the order of microseconds to milliseconds in practice.

**3. Transmission Delay**

* Assuming that packets are transmitted in a first-come first-serve manner, our packet can be transmitted only after all the packets that have arrive before it have been transmitted.
* Denote the length of the packet by L bits, and denote the transmission rate of the link from router A to router B by R bits/sec.
  + - * + For example, for a 10 Mbps Ethernet link, the rate R = 100 Mbps.
        + Transmission delay = L/R
        + This is the amount of time required to push (that is, transmit) all of the packet’s bits into the link. Transmission delays are typically on the order of microseconds to milliseconds in practice.

**4. Propagation Delay**

* Once a bit is pushed into the link, it needs to propagate to router B. The time required to propagate from the beginning of the link to router B is the propagation delay.
* The bit propagates at the propagation speed of the link.

The propagation speed depends on the physical medium of the link.

The propagation delay is the distance between two routers divided by the

propagation speed. T

Propagation delay = d/s,

where d is the distance between router A and router B and s is the propagation

speed of the link.

* + In wide-area networks, propagation delays are on the order of milliseconds.

**Packet Loss**

Basically this means that when sending a lot of packets in to a queue at a high rate (or at the same time), packet loss will be experienced as the queue will be maxed out and the router will drop packets. A lost packet can be retransmitted on an end-to-end basis in order to ensure that all data are eventually transferred from source to destination.

**Throughput in Computer Networks**

Imagine a large file being sent from Host A to Host B across a computer network.

The instantaneous throughput at any instant of time is the rate (in bits/sec) at which Host B is receiving the file.

The average throughput of the file is bits/sec, where the file consists of F bits and the transfer time is T (in seconds)

4)Mention active attacks and passive attacks?

**Passive Attacks**

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

1. ***The release of message contents*** is easily understood We had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.

2. A second type of passive attack, ***traffic analysis*** in If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

**Active Attacks**

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

1. A masquerade takes place when one entity pretends to be a different entity

A masquerade attack usually includes one of the other forms of active attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

2. Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

3. Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect For example, a message meaning “Allow John Smith to read confidential file accounts” is modified to mean “Allow Fred Brown to read confidential file accounts.”

4. The denial of service prevents or inhibits the normal use or management of communications facilities . This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination

5)Explain the components on data communiation depends on?

**Delivery**

* + The system must deliver data to the correct destination.

**2) Accuracy**

* + The system must deliver the data accurately.
  + Normally, the corrupted-data are unusable.

**3) Timeliness**

* + The system must deliver audio/video data in a timely manner.
  + This kind of delivery is called real-time transmission.
  + Data delivered late are useless.

**4) Jitter**

* + Jitter refers to the variation in the packet arrival-time.
  + In other words, jitter is the uneven delay in the delivery of audio/video packets.

6)What is CDN explain?

**CDN – Content Distribution Network or Content Delivery Network** is a solution that provides faster delivery of content to the users distributed worldwide.

What is a CDN?

A CDN is essentially a group of servers that are strategically placed across the globe with the purpose of accelerating the delivery of web content. A CDN

1. Manages servers that are geographically distributed over different locations.

2. Stores the web content in its servers.

3. Attempts to direct each user to a server that is part of the CDN so as to deliver content quickly.

CDN architecture

To minimize the distance between the visitors and your website’s server, a CDN stores a cached version of original content in multiple geographical locations (a.k.a., points of presence/ PoPs). Each PoP contains a number of caching servers known as edge servers that are responsible for content delivery to visitors within its proximity. CDN caches content in many places at once, ensuring quick delivery of content

**1. Origin server** - Actual data is stored

**2. Points of presence**

A point of presence, commonly referred to as a POP, is a single geographical location where a group of CDN edge servers reside. Whereas points of presence, commonly referred to as POPs, is multiple geographical locations that when combined make up the entire network.

**3. Edge servers**

An edge server, which is a server that resides between two networks, are located at each POP. Edge servers are simple proxy caches that work similarly to a web browser cache. They do not generate content for the website, instead, they keep a copy of the content in the cache. The total number of edge servers located at each POP will vary for each CDN provider. The dispersion of POPs will vary from CDN to CDN. Certain providers prefer to cover more ground with small-capacity servers, while other CDNs aim to maintain fewer, high-capacity pops

**How does a CDN work?**

As mentioned, a CDN is a large network made up of various servers located in multiple geographic regions. The POPs are placed close to populated areas, in countries all over the world. For large countries, there may be many different POPs.

The idea is to direct the user to the closest point of presence. When a user requests content from a site that uses a CDN, the request is routed to the closest POP, where a web server sends the requested data. There are several different ways that a request can be routed to a specific POP, one of which is IP anycast.

7) What if the principle and functionally of application layer?

The application layer in the OSI (Open Systems Interconnection) model is the highest layer and is responsible for providing network services directly to end-users. Its primary function is to enable communication between different software applications or processes running on different devices across a network

Functions of application layer

1. Provides services to the user
2. Enables the user to access the network
3. Mail services
4. Directory services
5. File transfer,access,and management

8) What is URL explain?

URL: Uniform resource locator

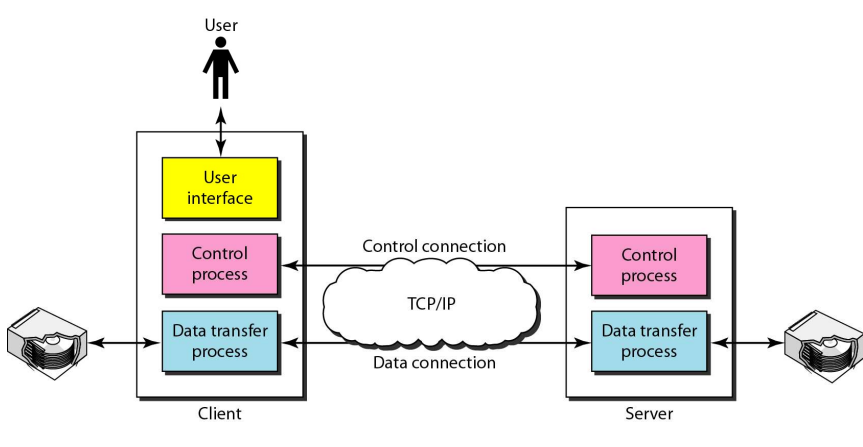
A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet. The URL defines four things: protocol, host computer, port, and path.

9) what is FTP protocol?

FTP :file transfer protocol

Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. As a matter of fact, the greatest volume of data exchange in the Internet today is due to file transfer.

• FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses).Separation of commands and data transfer makes FTP more efficient



**The basic model of FTP**

* The client consist of three components:

User interface, client control process, and the client data transfer process.

* . The server has two components:
* the server control process and the server data transfer process.

The control connection is made between the control processes.

The data connection is made between the data transfer processes

**Communication over control connection**

• Communication is achieved through commands and responses.

• This simple method is adequate for the control connection

• because we send one command (or response) at a time. Each command or response is only one short line

* We want to transfer files through the data connection. File transfer occurs over the data connection under the control of the commands sent over the control connection

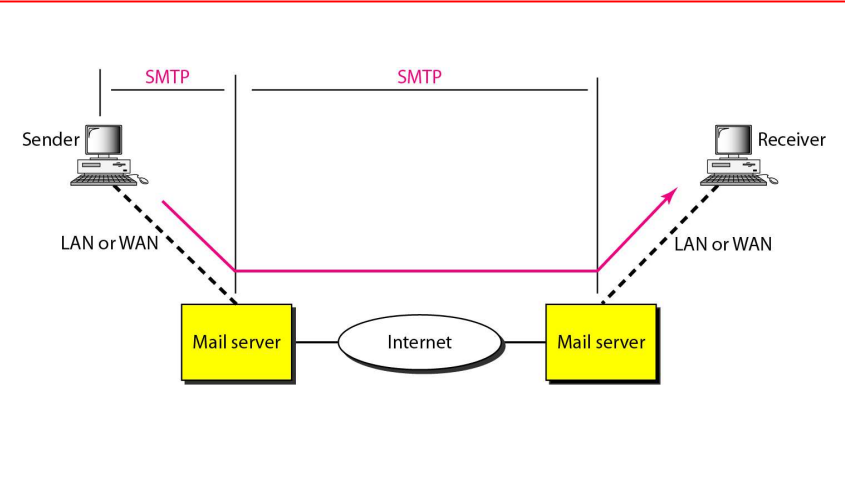
1.RETR command - A file is to be copied from the server to the client.

2. STOR command - A file is to be copied from the client to the server.

3. LIST command - A list of directory or file names is to be sent from the server To the client

10)Explain the protocol used for transfer the emails ?

* The actual mail transfer is done through message transfer agents.
* To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.
* The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP). As we said before, two pairs of MTA client/server programs are used in the most common situation (fourth scenario).



* SMTP is used two times, between the sender and the sender's mail server and between the two mail servers.
* As we will see shortly, another protocol is needed between the mail server and the receiver.
* SMTP simply defines how commands and responses must be sent back and forth

MTA

SERVER

MTA

CLIENT

COMMANDS

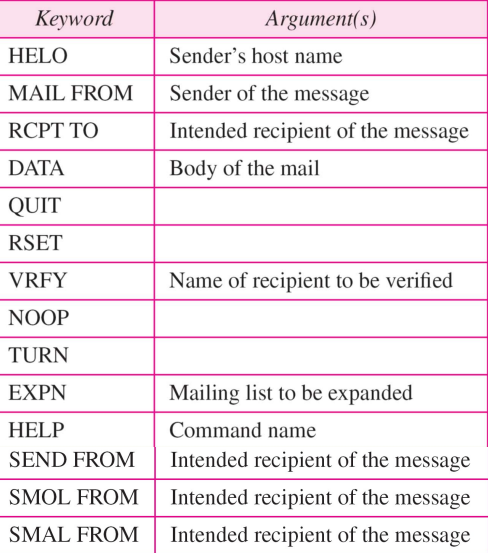
RESPONSES

1.Command format

• Commands are sent from the client to the server.

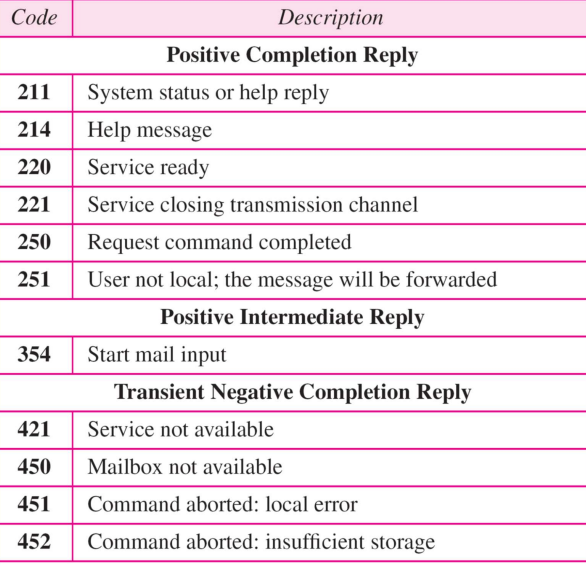
It consists of a keyword followed by zero or more arguments.

• SMTP defines 14 commands. The first five are mandatory; the next three are often used and highly recommended. The last six are seldom



2.RESPONSES

Responses are sent from the server to the client. A response is a three digitcode that may be followed by additional textual information



11)Explain different types of cookies and working their?

**Types of Internet Cookies**

**Essential Cookies**:

* These cookies are necessary for proper website functioning and are placed automatically on your device when you access a website or perform specific actions.
* Examples of essential cookies include:

**Session Cookies**: These remember your activities on a website, such as keeping you logged in to your account while you browse.

**User-input Cookies** (Session-ID): They track items that users input, like answers in an online form or items in a shopping cart.

**Authentication Cookies**: These identify users through login credentials, confirming their identity and remembering account information.

**User-centric Security Cookies**: Detect authentication errors and track incorrect login attempts.

**Load-balancing Cookies**: Connect information between a user’s web server and the website’s server

**Non-Essential Cookies**:

* These cookies are not strictly necessary for website functionality but enhance user experience.
* Examples include:

**Preferences Cookies**: Also known as “functionality” cookies, they store user preferences (e.g., language settings).

**Statistics Cookies**: These track performance metrics, helping website owners analyze user behavior.

**Marketing Cookies**: Advertisers use them to track online activity and deliver relevant ads to users2.

**Supercookies:**

* Supercookies are more persistent and harder to remove than regular cookies.
* They can store extensive data, including browsing history, and are often used for tracking purposes.
* Unlike regular cookies, supercookies are not easily managed by users and can pose privacy risks1.

***How Cookies Work***

Setting Cookies:

1. When you visit a website, it sends a small text file (the cookie) to your browser.
2. The cookie contains information about your visit, preferences, or session data.
3. Your browser stores this cookie locally.

Sending Cookies Back:

1. Whenever you revisit the same website, your browser sends the stored cookies back to the server.
2. The website uses this data to personalize your experience, remember your login status, and more.

Expiration and Persistence:

1. Some cookies expire when you close your browser (session cookies).
2. Others persist across sessions (persistent cookies) and have an expiration date set by the website.

Privacy Considerations:

1. While cookies enhance functionality, they also raise privacy concerns.
2. Users can manage cookies through browser settings, clearing or blocking them as desired.

12)Explain virtual circuits mentions its advantages and disadvantages?

Virtual circuits are a communication paradigm used in computer networks, particularly in packet-switched networks like the Internet. They offer a middle ground between the two extremes of circuit-switched and datagram (connectionless) networks.

***Advantages of Virtual Circuits***

* **Predictable Performance**: Once the virtual circuit is established, subsequent data packets follow the same path, which can lead to more predictable performance characteristics compared to datagram networks.
* **Efficient Routing**: Because the path is predetermined, routing decisions don't need to be made for each packet, reducing overhead and potentially improving efficiency.
* **Connection-Oriented Communication**: Virtual circuits provide a connection-oriented communication model, where both ends of the communication link are aware of each other's presence. This can simplify error handling and flow control.
* **Less Overhead**: Virtual circuits typically involve less overhead compared to circuit-switched networks because resources are allocated dynamically rather than dedicated for the entire duration of the communication session

***Disadvantages of Virtual Circuits:***

* **Setup Overhead**: Before any data transfer can occur, a virtual circuit must be established between the sender and receiver. This setup process incurs overhead, which can be significant, especially for short-lived or sporadic communication sessions.
* **Less Flexibility**: Once a virtual circuit is established, the route is fixed for the duration of the communication session. This lack of flexibility can be a disadvantage in dynamic network environments where routes may need to change due to congestion, failures, or other factors.
* **Resource Allocation**: Virtual circuits require network resources to be allocated for the duration of the communication session, even if those resources are not fully utilized. This can lead to inefficient resource utilization, especially in cases where the network experiences varying levels of traffic.
* **State Maintenance**: Network devices must maintain state information for each established virtual circuit, which can consume memory and processing resources. Additionally, failure to properly release resources after a virtual circuit is terminated can lead to resource wastage.

14)Explain Datagram network?

**Datagram Networks**

* + This is analogous to postal system.
  + Each packet is routed independently through the network.
  + Each packet has a header that contains source and destination addresses.
  + Each switch examines the header to determine the next hop in the path to the destination.
  + If the transmission line is busy then the packet is placed in the queue until the line becomes free.
  + Packets are referred to as datagrams.
  + Datagram switching is normally done at the network layer. • In Internet, switching is done by using the datagram switching.

***• Advantage***:

1) High utilization of transmission-line can be achieved by sharing among multiple packets.

***• Disadvantages:***

1) Packets may arrive out-of-order, and re-sequencing may be required at the destination

2) Loss of packets may occur when a switch has insufficient buffer

**Data gram network with four switches**

* All four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination.
* This is so because the links may be involved in carrying packets from other sources and do not have the necessary bandwidth available to carry all the packets from A to X.
* This approach can cause the datagrams of a transmission to arrive at their destination out-of- order with different delays between the packets.
* Packets may also be lost or dropped because of a lack-of-resources.
* It is the responsibility of an upper-layer protocol to

1. reorder the datagrams or
2. ask for lost datagrams.

* The datagram-networks are referred to as connectionless networks. This is because

1) The switch does not keep information about the connection state.

2) There are no setup or teardown phases.

3) Each packet is treated the same by a switch regardless of its source or destination.

15)Explain the architerture of router?

***Input Port***: This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at the router, this is done by the leftmost part in the below diagram, and the middle part does the work of interoperating with the link-layer like decapsulation, in the last part of the input port the forwarding table is looked up and is used to determine the appropriate output port based on the destination address.

***Switching Fabric***: This is the heart of the Router, It connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in several ways some of the prominent ones are:

1. **Switching via memory**: In this, we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional CPU with input and output ports acting as input and output devices.
2. **Switching via bus**: In this implementation, we have a bus that connects all the input ports to all the output ports. On receiving a packet and determining which output port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus. All output ports can see the packets but they will be delivered to the output port whose token has been put in, the token is then scraped off by that output port and the packet is forwarded
3. **Switching via interconnection network**: This is a more sophisticated network, here instead of a single bus we use a 2N bus to connect n input ports to n output ports.

***Output Port***: This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions, and finally transmits the packets to an outgoing link.

***Routing Processor***: It executes the routing protocols, and it works like a traditional CPU. It employs various routing algorithms like the link-state algorithm, distance-vector algorithm, etc. to prepare the forwarding table, which is looked up to determine the route and the output port.

16)Explain the frame structure of ABI6?

The ABI6 frame structure is a carefully arranged system of beams, columns, and slabs designed to withstand significant stresses and moments generated by both gravity and lateral loads. Let’s delve into the details:

***Components of the Frame Structure:***

**Beams:** These are linear elements that form the framework. Beams resist bending and flexing, contributing to the overall rigidity of the structure.

**Columns**: Vertical supports that provide stability and transmit loads from the beams to the ground.

**Slabs**: Horizontal surfaces that distribute loads and provide a platform for the structure.

***Types of Walls:***

**Load-Bearing Walls**: These walls carry the vertical loads of the structure. They are essential for stability and support.

**Non-Load-Bearing Walls**: These walls do not carry significant loads and are primarily used for partitioning or aesthetic purposes.

***Shear Walls***: In framed buildings, shear walls play a crucial role as load-bearing walls. They resist lateral forces such as wind or seismic loads. Typically, diagonal bracing elements strengthen the system against these lateral forces.

***Rigid Frame System***:

A rigid frame structure is composed of beams, columns, and slabs that work together to form a robust framework. Rigidity prevents bending or flexing.

**Static Indeterminacy**: Rigid frames lack pinned joints between individual members, resulting in static indeterminacy.

**Stiffness**: Beams and columns with rigid connections give the frame its stiffness, making it resistant to vertical and lateral stresses.

**Analysis Techniques**: Structural analysis methods, such as the portal method, virtual work, Castigliano’s theorem, force method, and stiffness method, help determine internal forces and support reactions.

***Types of Rigid Frames***:

**Fix-Ended Rigid Frame**: Both ends are fixed, providing stability and continuity.

**Pin-Ended Rigid Frame:** Held together by pins, it loses rigidity if the pins are removed.

**Braced Frame Structure**: Diagonal bracing between beams and columns enhances resistance to lateral forces, making it suitable for earthquake and wind pressures.

17)Explain the frame format of ICMP and working?

ICMP (Internet Control Message Protocol) is a network layer protocol used in IP networks to send error messages and operational information between network devices. ICMP operates on top of the Internet Protocol (IP) and is used primarily for diagnostic and control purposes

**IP Header**: Every ICMP message is carried within an IP packet. The IP header contains information such as source and destination IP addresses, version number, header length, Type of Service (ToS), Time-to-Live (TTL), protocol number (which is set to 1 for ICMP), and header checksum.

**ICMP Header**: Within the IP payload, the ICMP header contains specific information about the ICMP message. The structure of the ICMP header typically includes the following fields:

1. ***Type***: Specifies the type of ICMP message. Common types include echo request/reply, destination unreachable, time exceeded, parameter problem, etc.
2. ***Code***: Further refines the type of ICMP message. For example, for an ICMP Destination Unreachable message, the code field may indicate the reason for the unreachable destination (e.g., host unreachable, port unreachable, protocol unreachable, etc.).
3. ***Checksum:*** Provides error-checking for the ICMP message.
4. ***Identifier and Sequence Number***: Used primarily in echo request/reply messages for diagnostics. The sender includes a unique identifier and sequence number in the echo request, and the receiver echoes them back in the reply message.
5. ***Data***: Depending on the ICMP message type, additional data may be included in the ICMP payload. For example, in echo request/reply messages, this field typically contains arbitrary data sent by the sender for diagnostic purposes.

***Working of ICMP***:

ICMP messages serve various purposes in IP networks, including error reporting, network troubleshooting, and diagnostic purposes. Here's a brief overview of how ICMP works:

1. **Error Reporting**: When a router or host encounters an error while processing an IP packet (e.g., destination unreachable, time exceeded), it generates an ICMP error message and sends it back to the source IP address specified in the original packet.
2. **Network Troubleshooting**: ICMP echo request/reply messages (commonly known as "pings") are used for network troubleshooting and diagnostics. A sender sends an ICMP echo request message to a destination host, and if the host is reachable and operational, it responds with an ICMP echo reply message.
3. **Path MTU Discovery**: ICMP messages are used for Path MTU Discovery, a mechanism to determine the Maximum Transmission Unit (MTU) size along a path between two hosts. This helps prevent IP fragmentation and improves network performance.
4. **Router Advertisement and Solicitation:** ICMP messages such as Router Advertisement and Router Solicitation are part of the ICMPv6 protocol and are used in IPv6 networks for router discovery and configuration.

18)Explain all the four digital to digital ,analog to digital, digital to analog. Analog to digital conversions?

* **Digital to Digital**

The conversion involves three techniques: line coding,, block coding ,scrambling. Line coding is always needed ;block coding and scrambling may or may not be needed

Line coding is the process of converting digital data to digital signals

1. Unipolar :NRZ
2. Polar :NRZ, RZ, and BIPHASE
3. Bipolar: AMI and Pseudotrenary
4. Multilevel: 2B/1Q, 8B/6T,and 4D -PAMS
5. Multitransition: MLT-3

In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below.

**NRZ (Non-Return-to-Zero):** Traditionally, a unipolar scheme was designed as a non-return-to-zero (NRZ) scheme in which the positive voltage defines bit I and the zero voltage defines bit O. It is called NRZ because the signal does not return to zero at the middle of the bit.

1. Bit 0-0V
2. Bit 1-postive V

In polar schemes, the voltages are on the both sides of the time axis

**1.NRZ-L (Non Return to Zero – Level) :** the level of the voltage determines the value of the bit

**2.NRZ-I (Non Return to Zero - Invert):** the change or lack of change in the level of the voltage determines the value of the bit. If there is no change, the bit is 0; if there is a change, the bit is 1.

**3.RZ (Return to zero):** There is transition in the middle of each bit

***NRZ Scheme***: Bit 0-positive V

Bit 1 -Negative V

***RZ Scheme***: Bit 0-NegativeV +0V

Bit 1-PositiveV +0V

**Biphase** : Two types are Manchester and Differential Manchester.

• *Manchester encoding* - the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half.

• *Differential Manchester* - There is always a transition at the middle of the bit, but the bit values are determined at the beginning of the bit.

If the next bit is 0, there is a transition; if the next bit is 1, there is none

Bit 0-Positive to Negative V

Bit 1-Negative to Positive V

In bipolar encoding (sometimes called multilevel binary), there are three voltage levels: positive, negative, and zero.

The voltage level for one data element is at zero, while the voltage level for the other element alternates between positive and negative voltages. Types are AMI and Pseudoternary

***1. AMI***: It means alternate I inversion. A neutral zero voltagerepresents binary 0. Binary 1 are represented by alternating positive and negative voltages.

***2. Pseudoternary***: A variation of AMI encoding is called pseudoternary in which the 1 bit is encoded as a zero voltage and the 0 bit is encoded as alternating positive and negativevoltages

* **Analog to Digital**

Two methods are

1. Pulse Code Modulation (PCM)

2. Delta Modulation (DM)

**PULSE CODE MODULATION**

The most common technique to change an analog signal to digital data (digitization) is called pulse code modulation (PCM).

A PCM encoder has three processes

1. The analog signal is sampled.

2. The sampled signal is quantized.

3. The quantized values are encoded as streams of bits

***SAMPLER:***

The first step of PCM is sampling. Sampling of the signal is based on Nyquist Theorem. It states that “the sampling frequency fsshould be always greater than or equal to twice the maximum frequency content in the message signal fm.

fs >= 2 fm

***QUANTIZING:***

We approximate the value of the sample amplitude to the quantized values.

***ENCODER:***

The last step in PCM is encoding. After each sample is quantized and the number of bits per sample is decided, each sample can be changed to an n-bit code word.

**DELTA MODULATION**

PCM is a very complex technique. Other techniques have been developed to reduce the complexity of PCM. The simplest is delta modulation.

***Modulator***

The modulator is used at the sender site to create a stream of bits from an analog signal. The process records the small positive or negative changes, called delta O. If the delta ispositive, the process records a I; if it is negative, the process records a O.

***Demodulator***

The demodulator takes the digital data and, using the staircase maker and the delay unit, creates the analog signal. The created analog signal, however, needs to pass through a low-pass filter for smoothing

* **Digital to Analog**

Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal (carrier signal) based on the information in digital data

Types of digital to analog

1. Amplitude shift keying
2. Frequency shift keying
3. Phase shift keying

**Modulation :**

process (or result of the process) of translation the message signal to modulated carrier signal at frequencies that are very high compared to the baseband frequencies.

• **Demodulation** is the process of extracting the message back the modulated carrier

*Amplitude shift keying (ASK)*

In ASK the amplitude of the carrier signal is varied to representbinary 1 or 0.

* Carrier signal is a high frequency signal that acts as a basis for the information signal.
* Both frequency and phase remain constant while the amplitude changes.

**Pros:**

* ASK transmitter and receiver are simple to design.
* ASK needs less bandwidth than FSK.

**Cons:**

* ASK transmission can be easily corrupted by noise.

**Application:**

* Early telephone modem (AFSK).
* ASK is used to transmit digital data over optical fiber

*FSK (Frequency Shift Keying) •*

* The frequency of the carrier signal is varied to represent binary1 or 0. •
* Both peak amplitude and phase remain constant while thefrequency changes. •
* The frequency of the signal during each bit duration is constant,and its value depends on the bit (0 or 1)

*FSK Modulator*

* One way to think about binary
* **Analog to Digital**

Analog-to-analog conversion is the representation of analog information by an analog signal

Types Analog to Analog conversion

1. Amlitude modulation
2. Frequency modulation
3. Phase modulation

*Amplitude Modulation*

* A carrier signal is modulated only in amplitude value
* The modulating signal is the envelope of the carrier
* The required bandwidth is 2B, where B is the bandwidth of the modulating signal
* Since on both sides of the carrier freq. fc the spectrum is identical, we can discard one half, thus requiring a smaller bandwidth for transmission

Frequency Modulation

* The modulating signal changes the freq. fc of the carrier signal
* The bandwidth for FM is high
* It is approx. 10x the signal frequency

*Phase Modulation (PM)*

* The modulating signal only changes the phase of the carrier signal.
* The phase change manifests itself as a frequency change but the instantaneous frequency change is proportional to the derivative of the amplitude.
* The bandwidth is higher than for AM.

19)Explain any two error detection techniques?

Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination

Detection Methods

1. VRC
2. LRC
3. CRC
4. Checksum

***VRC: Vertical Redundancy Check***

* It can detect single bit error
* It can detect burst errors only if the total number of errors is odd

***LRC: Longitudinal Redundancy Check***

* LRC increases the likelihood of detecting burst errors.
* If two bits in one data units are damagedand two bits in exactly the same positions inanother data unit are also damaged, the LRC checker will not detect an error

***Checksum:***

***At the sender***

* The unit is divided into k sections, each of n bits.
* All sections are added together using one’s complement to get the sum.
* The sum is complemented and becomes the checksum.
* The checksum is sent with the data

***At the receiver***

* The unit is divided into k sections, each of nbits.
* All sections are added together using one’s complement to get the sum.
* The sum is complemented.
* If the result is zero, the data are accepted: otherwise, they are rejected.

***Performance***

* The checksum detects all errors involving an odd number of bits.
* It detects most errors involving an even number of bits.
* If one or more bits of a segment are damaged and the corresponding bit or bits of opposite value in a second segment are also damaged, the sums of those columns will not change and the receiver will not detect a problem.

***II - Error Correction***

It can be handled in two ways:

1) receiver can have the sender retransmit the entire data unit **– Retransmission (Backward Error Correction BEC)**

2) The receiver can use an error-correcting code, which automatically corrects certain errors – **Forward Error Correction (FEC)**

20)Explain MPLS protocol with frame format?

**Multi Protocol Label Switching (MPLS)** is an IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets. MPLS uses layer 3 service i.e, Internet Protocol, and uses router as forwarding device. The traffic of different customers is separated from each other because MPLS works somewhat like VPN. It does not work like regular VPN that encrypts the data but it ensures packet from one customer cannot be received by another customer. An MPLS header is added to packet that lies between layers 2 and 3. Hence, it is also considers to be Layer 2.5 protocol.

**MPLS Header** – The MPLS Header is 32 bit long and is divided into four parts –

1. **Label** – This field is 20 bit long and can take value b/w 0 & 220 – 1.
2. **Exp** – They are 3 bits long and used for Quality of Service(QoS).
3. **Bottom of stack (S)** – It is of size 1 bit. MPLS labels are stacked one over other. If there is only one label remained in MPLS header, then its value is 1 otherwise 0.
4. **Time to Live (TTL**) – It is 8 bit long and its value is decreased by one at each hop to prevent packet to get stuck in network.

21) Explain frame format and working of ARP?

*Frame Format of ARP (Address Resolution Protocol):*

ARP operates at the data link layer (Layer 2) of the OSI model and is used to map IP addresses to MAC (Media Access Control) addresses in a local network. ARP messages are encapsulated within Ethernet frames, which are commonly used in Ethernet networks. Here's the frame format of ARP:

1. **Ethernet Header:**

**Destination MAC Address**: Broadcast (FF:FF:FF:FF:FF:FF) or unicast MAC address of the recipient.

**Source MAC Address**: MAC address of the sender's network interface.

**EtherType**: Indicates the type of payload, typically set to 0x0806 to indicate an ARP frame.

1. **ARP Header:**

**Hardware Type**: Specifies the type of hardware (e.g., Ethernet) used on the local network. For Ethernet, the value is 1.

**Protocol Type**: Indicates the type of protocol being resolved (e.g., IPv4). For IPv4, the value is 0x0800.

**Hardware Address Length**: Specifies the length of MAC addresses, typically 6 for Ethernet.

**Protocol Address Length**: Specifies the length of IP addresses, typically 4 for IPv4.

**Operation Code:** Indicates the type of ARP message (e.g., request or reply).

**Sender Hardware Address**: MAC address of the sender.

**Sender Protocol Address**: IP address of the sender.

**Target Hardware Address**: MAC address being requested (only present in ARP requests).

**Target Protocol Address**: IP address being resolved.

***Working of ARP:***

*ARP Request*:

1. When a device needs to send data to another device on the same local network but does not have the recipient's MAC address, it broadcasts an ARP request message containing its own IP address and MAC address and the IP address of the intended recipient.
2. The ARP request is broadcasted to all devices on the local network.
3. Upon receiving the ARP request, the device with the matching IP address sends an ARP reply containing its MAC address to the sender.

*ARP Reply*:

1. When a device receives an ARP request for its IP address, it responds with an ARP reply containing its MAC address.
2. The ARP reply is unicast back to the sender of the ARP request.

*Caching:*

1. Once a device receives an ARP reply, it caches the IP-to-MAC address mapping in its ARP table (also known as the ARP cache). This caching helps avoid repetitive ARP requests for frequently accessed destinations and improves network efficiency.
2. ARP cache entries typically have a timeout period, after which they expire and need to be refreshed through ARP resolution.

22)Explain PPP with frame format and working?

**Frame Format of PPP:**

1. **PPP Header:**

* **Flag:** A unique bit pattern (01111110) used to indicate the start and end of the frame.
* **Address:** Typically set to 11111111 (broadcast) for point-to-point connections.
* **Control: Specifies** the type of frame. For data frames, it's typically set to 00000011.
* **Protocol:** Indicates the type of network layer protocol being encapsulated (e.g., IPv4, IPv6, IPX). It allows PPP to support multiple network layer protocols.

1. **Payload:**

* The payload contains the encapsulated network layer packet (e.g., IP packet).

1. **Frame Check Sequence (FCS):**

* A CRC (Cyclic Redundancy Check) value calculated over the entire frame (header and payload). It is used for error detection.

1. **Flag:**

* Another occurrence of the flag pattern (01111110), indicating the end of the frame.

**Working of PPP:**

**Link Establishment and Authentication:**

* Before data transmission can occur, the PPP link must be established between the two devices. This involves negotiation and authentication phases.
* During the negotiation phase, the two devices exchange configuration parameters (such as maximum frame size, supported network layer protocols, etc.) using LCP (Link Control Protocol).
* Once negotiation is successful, the devices authenticate each other using authentication protocols such as PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).

**Data Transmission**:

* After link establishment and authentication, the devices can start transmitting data frames over the PPP link.
* Network layer packets (e.g., IP packets) are encapsulated within PPP frames and transmitted between the two devices.

**Error Detection and Correction**:

* PPP uses the Frame Check Sequence (FCS) field to detect errors in received frames. If the calculated CRC value does not match the received FCS value, it indicates that the frame may have been corrupted during transmission.
* If errors are detected, the frame is discarded, and the receiver may request retransmission using the Automatic Repeat reQuest (ARQ) mechanism.

**Link Termination:**

* When communication is complete, or if either device wishes to terminate the connection, the PPP link is terminated gracefully. This involves sending LCP termination packets to signal the end of the PPP session.

23)What is ethernet and working of it?

Ethernet is a widely used networking technology for connecting devices within a local area network (LAN). It defines the physical and data link layer specifications for wired network communication. Ethernet networks typically use twisted-pair copper cables or fiber-optic cables to transmit data between devices. Here's an explanation of Ethernet along with its working:

***Working of Ethernet:***

Ethernet Frame Format:

Ethernet frames are the basic units of data transmission in Ethernet networks. The frame format typically consists of the following components:

**Preamble:** A sequence of alternating 1s and 0s used for synchronization between sender and receiver.

**Start Frame Delimiter (SFD)**: Marks the end of the preamble and the beginning of the frame.

**Destination MAC Address**: Specifies the MAC (Media Access Control) address of the intended recipient device.

**Source MAC Address:** Indicates the MAC address of the sending device.

**EtherType or Length Field**: Indicates the type of payload encapsulated within the frame (e.g., IPv4, IPv6, ARP, etc.) or specifies the length of the payload.

**Payload**: Contains the actual data being transmitted, such as IP packets, ARP requests, or user data.

**Frame Check Sequence (FCS)**: A CRC (Cyclic Redundancy Check) value calculated over the entire frame (excluding preamble and SFD), used for error detection.

Media Access Control (MAC) Sublayer:

1. The MAC sublayer is responsible for controlling access to the physical network medium and transmitting frames between devices.
2. Ethernet uses a contention-based access method known as Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Before transmitting data, a device checks the network to ensure it is not already in use by another device. If the network is idle, the device sends its frame. If collisions occur (i.e., two or more devices attempt to transmit simultaneously), each device stops transmitting and waits for a random backoff period before reattempting transmission.
3. Full-duplex Ethernet, which allows devices to transmit and receive data simultaneously, does not use CSMA/CD.

Physical Layer:

1. The physical layer of Ethernet defines the electrical, mechanical, and functional specifications for transmitting data over the network medium (e.g., copper cables, fiber-optic cables).
2. Ethernet supports various physical layer standards, including 10BASE-T (twisted-pair copper cables), 100BASE-TX (Fast Ethernet), 1000BASE-T (Gigabit Ethernet), and 10GBASE-T (10 Gigabit Ethernet).
3. Each physical layer standard specifies characteristics such as cable type, maximum cable length, signaling rate, and encoding scheme.

Switching and Routing:

1. In Ethernet networks, switches and routers play crucial roles in forwarding frames between devices and connecting multiple LAN segments or networks.
2. Ethernet switches use MAC addresses to make forwarding decisions, forwarding frames only to the intended recipient devices.
3. Ethernet routers operate at the network layer (Layer 3) and use IP addresses to route packets between different LANs or subnets.

24)What are VLANs?

We can roughly define a virtual local area network

(VLAN) as a local area network configured by software ,not by physical wiring

***VLAN Configuration***

**Manually** – network admin uses VLAN software to manually assign the station. hanging from one VLAN to other can also be done manually

**Automatic** – station automatically connected or disconnected

**Semiautomatic** – initialization is done manually and migration is done automatically

***VLAN: Advantages***

1. Cost and time reduction
2. Creating Virtual Work Groups
3. Security