**Differentiate between Connection oriented and connection-less services**

|  |  |  |
| --- | --- | --- |
| S. N | Connection Oriented Services | Connection-less Services |
| 1 | Connection Oriented Service is related to the telephone system. | Connection-less service is related to the postal system. |
| 2 | It is feasible | It is not feasible |
| 3 | In its congestion is not possible | In its congestion is possible |
| 4 | In connection-oriented service packets follow the same route. | In connection-less service packets doesn't follow in different route. |
| 5 | It is more reliable | It is less reliable |
| 6 | It requires authentication | It doesn't require authentication |
| 7 | Example:  TCP (Transmission Control Protocol) | Example:  UDP (User Datagram Protocol |

**What is computer network? Explain OSI model.**

Ans. Computer network is the group of devices which are connected to each other through transmission medium such as wired, cables and wireless. The devices may be computers, printers, fax machines etc. The main purpose of having computer network is to send and receive the data stored in other computers through the network.

protocols

Protocols

Message

Sender

Receiver

Transmission Medium

Fig. Basic Components of computer networks.

**OSI Model:**

**OSI** Model stands for Open-Source Inter-connection which is developed by ISO (International Organization of Standardization) in 1984. OSI model has seven layers with unique functionality performed by hardware and software. Each layer of sender is connected to the corresponding layer of receiver end. Every layer has separate protocol and interface between them.

The seven layers of OSI models are as follows:

1. Application layer
2. Presentation layer
3. Session layer
4. Transport layer
5. Network layer
6. Data link layer
7. Physical layer

**Application Layer:**  
 This is the top layer of OSI model and it is able to perform application and end-user processes. Every process or task done by this layer are application specific. It follows HTTP, SMTP and POP3 protocols.

**Presentation Layer:**

This layer is responsible for data encryption, compression, translation etc. and the date is changed by the sender end and in the receiver end it performs decryption, decompression on the data.

**Session Layer:**

This layer is responsible for the establishing or opening and end or closing the communication between two devices. It allows for complete data transfer and also checks the interruptions of the session.

**Transport Layer:**

This layer divides the data into smaller segments and as well as add header to the segments.

It is responsible for end-to-end delivery of the data.

**Network Layer:**

This layer further divides those segments into packets and packets hold the address of source and destination which helps to identify from where the data is and where to go. It also provides routing and it helps to identify the shortest route for data and to handle the traffic.

**Data Link Layer:**

Data link layer is responsible for transferring the data between two nodes. It also performs the error and flow control of the nodes. It converts the packets into the frames and frames holds the MAC addresses which are physical addresses of devices.

**Physical Layer:**

Physical layer establishes physical connection between two devices. The data in this layer is in the form of bites and bites are converted into voltage signals using different line coding techniques.

**Explain IEEE 802.3 and IEEE 802.4. Explain CSMA/CD Protocol.**

Ans.

**IEEE 802.3:**

IEE 802.3 is widely used standard which implements at physical layer and data link layer of OSI model. It handles data frames and employee line coding to transmit data through the twisted-pair. It has different transmission speed of 10Mbps, 100Mbps, 1000Mbps. 100Mbps ethernet is called fast ethernet and 1000Mbps ethernet is called gigabit ethernet. Fast ethernet and gigabit ethernet used full duplex transmission. Ethernet uses CSMA/CD to identify the data collision.

**IEEE 802.4:**

IEE 802.4 is the known as token bus. It is a token passing standard used in LAN. The LAN use tree or bus topologies where a virtual ring is established. The token is passed from one user to another in a sequence. Every node knows the address of the station to its left or right. A co-axial cable carries data when a node receives the token and requested transmission.

**CSMA/CD:**

CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection. It is the media access control method used in ethernet technology.

It is mostly used in co-axial cable which connect the bus topology. It is used when multiple nodes want to transmit the data on the shared link. If two devices transmit data at the same time collision occurs. It causes error and data corruption. CSMA/CD is used to stop the data collision it follows following steps:

**Step 1:** It checks the sender is ready to transmit or not.

**Step 2:** It checks if the transmission line is idle by sending the dummy data and checks for the collision signal.

**Step 3:** If it senses the link is idle the data transmission occurs on the link if the signal successfully travels to the receiver there will be no collision signal. Otherwise, collision signal will be received. Here transmission is stopped and waits for a random time before it resends the data frame. This process repeated until the data is transferred.

**What are transmission media? Explain any two types. Discuss flow control in data link layer.**

Ans.:

Transmission media refers to the physical pathways through which data, signals, or information are transferred from one location to another in a communication system. The pathways can be wired and wireless and are essential for the successful transfer of data between devices or networks.

Here I'll explain two types of transmission media:

1. Twisted Pair Cables:
2. Fiber Optics

**Twisted Pair Cables:**

Twisted pair cables are one of the most common and traditional form of transmission media. They consist of pair of insulated copper wires twisted together to reduce electromagnetic interference and signal degradation. There are two main types of twisted pair cables:

1. Unshielded twisted Pair (UTP): UTP cables are widely used for networking applications, such as Ethernet connection. They consist of multiple pairs of insulated copper wires, with each pair twisted to minimize crosstalk and electromagnet interference.
2. Shielded Twisted Pair Cables (STP): STP cables include additional shielding, such as a metal foil or braided mesh, around the twisted pairs.

**Fiber Optics:**

Fiber optics cables are advanced transmission media that use light signal to transmit data. They consist of thin strands of glass or plastic fibers that carries data through reflection and refraction of light. Fiber Optics cables of different advantages over traditional copper-based cables including:

1. High bandwidth
2. Low Signal Loss
3. Immunity to interference
4. Security

**Flow control in data link layer:**

Flow control mechanisms manages the rate at which data is transmitted from the sender to receiver to prevent data overload or loss due to speed mismatches between the sender and receiver. Flow control ensures that the receiver can process and store the incoming data at a pace it can handle. Two common flow control methods are:

1. **Stop-and-Wait:** In stop-and-wait flow control, the sender sends a data frame and then waits for an acknowledgement from the receiver before sending the next frame. This method ensures that the receiver has successfully received the previous frame before sending next one.
2. **Sliding Window:** Sliding window flow control allows the sender to transmit multiple frames before waiting for acknowledgements. The receiver acknowledges the receipt of frames and specifies the next frame it expects to receive. This allows for more efficient utilization of the communication channel.

**Error control in data link layer:**  
 Error control mechanisms are put in place to detect and correct errors that may occur during the transmission of data. Errors can be introduced due to various factors, such as noise, signal attenuation, or interference. Error control techniques aim to ensure that the received data matches the original transmitted data. Two common error control methods are:

1. **Parity checking:** Parity checking is a simple error detection technique. A parity bit is added to each transmitted data unit to make the total number of 1s (or 0s) in the unit even or odd. The receiver then checks the parity of the received data and compares it to the expected parity. If they do not match, an error is detected.

1. **Checksum**: Checksum involve the computation of a checksum value based on the data being sent. The sender attaches this checksum to the data. The receiver performs the same computation on the received data and compares the calculated checksum with the received checksum. If they differ, an error is deected.

**What is channel bandwidth? Explain the concept of sub-netting. Define inter-network.**

**Ans.**

1. **Channel Bandwidth:**

Channel bandwidth refers to the range of frequencies that a communication channel or transmission medium can carry. It represents the capacity of the channel to transmit data and is typically measured in hertz (Hz). A wider channel bandwidth allows for the transmission of higher frequencies and, consequently, higher data rates.

In practical terms, channel bandwidth determines how much data can be transmitted over a communication link within a given period. For example, in wired or wireless communication systems, a larger channel bandwidth enables higher data transfer rates, which is essential for applications such as streaming video, voice communication, and internet browsing. Channel bandwidth is a critical factor in determining the overall performance and capacity of a communication system.

2. **Subnetting:**

Subnetting is a technique used in computer networking to divide a larger IP address space into smaller, more manageable subnetworks or subnets. It allows for efficient utilization of IP addresses and helps in organizing and managing a network infrastructure. Subnetting involves splitting a single network into multiple smaller networks, each with its own unique network address and subnet mask.

The concept of subnetting helps improve network efficiency, security, and management. It allows network administrators to:

- Allocate IP addresses more effectively.

- Contain and manage broadcast traffic within smaller segments.

- Implement security measures at a more granular level.

- Isolate different departments, sections, or functions of a network.

Subnetting involves manipulating the subnet mask of an IP address to create smaller subnets with their own unique ranges of IP addresses. The subnet mask defines the portion of an IP address that represents the network and the portion that represents the host. By modifying the subnet mask, administrators can define the boundaries of subnets within a larger IP address space.

3. **Inter-network:**

An inter-network, often abbreviated as "internet," refers to a collection of multiple interconnected networks that use a common set of communication protocols to enable devices from different networks to communicate with each other. The term "internet" is not exclusive to the World Wide Web but describes any network of networks.

In the context of computer networking, an inter-network involves the connection of distinct local area networks (LANs) or wide area networks (WANs) to create a larger network infrastructure. This allows devices and systems on different networks to share information and resources seamlessly. The most notable example of an inter-network is the global internet, which connects millions of networks worldwide.

The inter-network concept is fundamental to modern communication, as it enables data and information to be transmitted between disparate networks, facilitating global connectivity, information exchange, and collaborative efforts across diverse geographic locations.

**Explain propagation and transmission line.**

**Ans**

Propagation and transmission lines are concepts related to the transfer of signals and electromagnetic waves in communication systems and electrical circuits. Let's explore each of these concepts:

1. \*\*Propagation\*\*:

Propagation refers to the process by which electromagnetic waves (or signals) travel through a medium or space. It involves the transmission of energy and information from a source to a destination. Electromagnetic waves include various types of waves, such as radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays, and gamma rays. Propagation characteristics vary based on the frequency of the waves and the properties of the medium they pass through.

When electromagnetic waves propagate through a medium, they may experience effects like attenuation (weakening of the signal), reflection (bouncing off surfaces), refraction (bending of the wave as it enters a different medium), and diffraction (spreading of waves as they encounter obstacles or openings). Understanding propagation is crucial in designing communication systems, antennas, and other technologies that rely on the transmission of electromagnetic waves.

2. \*\*Transmission Line\*\*:

A transmission line is a physical pathway or conductor used to transfer electrical signals or energy from one point to another. Transmission lines are commonly used in electrical circuits and communication systems to carry high-frequency signals with minimal distortion and loss. They are essential for efficient signal propagation over a distance. Transmission lines are characterized by parameters such as impedance, capacitance, and inductance.

Key features and types of transmission lines include:

- \*\*Coaxial Cable\*\*: A coaxial cable consists of an inner conductor surrounded by an insulating layer, a metallic shield, and an outer insulating layer. Coaxial cables are widely used in television, networking, and other applications that require the transmission of high-frequency signals with minimal interference.

- \*\*Microstrip Line\*\*: Microstrip lines are used in printed circuit boards (PCBs) and integrated circuits. They consist of a conductive strip on a dielectric substrate, with a ground plane on the opposite side of the substrate. Microstrip lines are compact and suitable for high-frequency applications.

- \*\*Waveguides\*\*: Waveguides are hollow metal tubes or structures that guide electromagnetic waves, typically at microwave frequencies. They are often used in radar systems, satellite communications, and other applications where precise control of wave propagation is essential.

- \*\*Open-Wire Lines\*\*: Open-wire lines consist of two parallel conductors separated by insulators. They were historically used for long-distance telecommunication before coaxial cables became more popular.

- \*\*Twisted Pair Cable\*\*: Twisted pair cables are a type of transmission line used for balanced signal transmission, commonly used in Ethernet networking.

Transmission lines are designed to match the impedance of the source and load to minimize signal reflections and maximize power transfer. They play a crucial role in maintaining signal integrity and minimizing signal degradation as signals travel from one point to another within a circuit or communication system.

Explain flow control, congestion control in transport layer.

Ans.

Flow control and congestion control are two important mechanisms in the transport layer of the OSI (Open Systems Interconnection) model that manage the efficient and reliable transfer of data between two communicating devices over a network. While they both aim to regulate the flow of data, they address different aspects of data transfer.

1. \*\*Flow Control\*\*:

Flow control is a mechanism that ensures that a sender does not overwhelm a receiver with data at a rate that the receiver cannot process. It prevents buffer overflow at the receiver's end and maintains a balance between the sender's transmission rate and the receiver's processing capacity. Flow control is particularly relevant when there is a speed or capacity mismatch between the sender and receiver.

Two common flow control methods are:

- \*\*Stop-and-Wait\*\*: In this method, the sender sends a data packet and then waits for an acknowledgment from the receiver before sending the next packet. This ensures that the receiver has successfully received the previous packet before more data is sent.

- \*\*Sliding Window\*\*: Sliding window flow control allows the sender to transmit multiple packets before waiting for acknowledgments. The receiver acknowledges received packets and specifies the next expected packet. This mechanism optimizes data transfer by allowing the sender to maintain a certain number of unacknowledged packets in transit.

2. \*\*Congestion Control\*\*:

Congestion control, on the other hand, focuses on preventing network congestion, which occurs when the network's resources (such as bandwidth or router buffers) are insufficient to handle the volume of data being sent. Congestion can lead to performance degradation, increased packet loss, and reduced quality of service.

Congestion control aims to detect and alleviate congestion by controlling the rate at which data is sent into the network. It involves adjusting the sending rate dynamically based on the network conditions. Some congestion control methods include:

- \*\*Traffic Policing and Shaping\*\*: These methods involve controlling the rate of incoming and outgoing traffic to match a predefined rate. Traffic shaping can smooth out bursty traffic patterns, while traffic policing can drop or mark packets that exceed a certain rate.

- \*\*Queue Management\*\*: Routers and switches often use queue management algorithms to prioritize and drop packets during periods of congestion. Examples include Random Early Detection (RED) and Weighted Random Early Detection (WRED).

- \*\*Explicit Congestion Notification (ECN)\*\*: ECN is a mechanism that allows routers to notify senders of impending congestion. When a router's buffer is close to being full, it marks packets with an ECN bit instead of dropping them. The sender detects these marks and can react accordingly by reducing its sending rate.

In summary, flow control manages the pacing of data transmission between sender and receiver to avoid overwhelming the receiver, while congestion control prevents network congestion by dynamically adjusting the sending rate based on network conditions. Both mechanisms contribute to the smooth and efficient operation of data transfer in the transport layer of a communication network.

Explain how CIA helps in computer network security.

Ans.

CIA, in the context of computer network security, refers to the three core principles of information security: Confidentiality, Integrity, and Availability. These principles form the foundation of a comprehensive approach to ensuring the security and protection of data and resources within a computer network. Let's explore how each aspect of CIA contributes to network security:

1. \*\*Confidentiality\*\*:

Confidentiality ensures that information is only accessible to authorized individuals or entities. In a network security context, confidentiality mechanisms prevent unauthorized access to sensitive data. This is achieved through various measures:

- \*\*Encryption\*\*: Data is encrypted before transmission and can only be decrypted by authorized recipients. This prevents eavesdropping and unauthorized access to the data while it's in transit or storage.

- \*\*Access Control\*\*: Access controls, such as passwords, authentication protocols, and role-based access, restrict data access to authorized users only.

- \*\*Virtual Private Networks (VPNs)\*\*: VPNs create encrypted tunnels between remote users and a network, ensuring that data transmitted over public networks remains confidential.

2. \*\*Integrity\*\*:

Integrity ensures that data remains accurate and unaltered during transmission and storage. Maintaining data integrity is crucial to prevent unauthorized modification or tampering. Mechanisms to ensure integrity include:

- \*\*Hashing\*\*: Data is hashed using cryptographic algorithms, and the hash value is compared at the receiving end to verify that the data has not been tampered with during transit.

- \*\*Checksums\*\*: Checksums are used to detect errors or changes in data by adding a unique value to the data and verifying it at the destination.

- \*\*Digital Signatures\*\*: Digital signatures provide authentication and integrity by using encryption to associate a digital signature with a piece of data. Any alteration to the data can be detected through the signature verification process.

3. \*\*Availability\*\*:

Availability ensures that resources and services are accessible and operational when needed. Network security measures to ensure availability include:

- \*\*Redundancy\*\*: Implementing redundant components or backup systems to ensure that services remain operational even if one component fails.

- \*\*Load Balancing\*\*: Distributing network traffic across multiple servers to prevent overloading and ensure consistent availability.

- \*\*Distributed Denial of Service (DDoS) Mitigation\*\*: Deploying mechanisms to detect and mitigate DDoS attacks, which attempt to overwhelm network resources to disrupt services.

- \*\*Disaster Recovery\*\*: Establishing plans and procedures to recover from unexpected events or disasters that could disrupt network operations.

By adhering to the principles of CIA, organizations can establish a strong foundation for network security. This holistic approach helps protect sensitive information, maintain the integrity of data, and ensure that network resources and services are available and reliable, thereby reducing the risk of unauthorized access, data breaches, and service disruptions.



