CONCEPT OF COMPUTER NETWORK & NETWORK SECURITY SYSTEM (ACtE05)

5.1 INTRODUCTION TO COMPUTER NETWORKS AND PHYSICAL LAYER

Computer Network:

A computer network is a group of interconnected computers and devices that can communicate and exchange data with each other. The network can be formed using different types of connections, such as wired or wireless connections, and can span a small area or a large geographic region. Computer networks allow for sharing resources and information, such as files, printers, and internet access, among connected devices.

The physical layer is the first layer of the OSI (Open Systems Interconnection) model and is responsible for the transmission and reception of unstructured raw data between a device and a physical transmission medium, such as copper wires, optical fibers, or wireless communication channels. The physical layer handles the physical characteristics of the transmission medium, such as data encoding, signaling, and modulation, and ensures that data is transmitted reliably over the network. It defines the physical and electrical specifications, such as cable types, connector types, and data transfer rates, and provides a means for transmitting bits from one device to another.

Protocol & Standard:

In computer networking, a protocol is a set of rules and standards that govern the communication between devices in a network. Protocols define the format, timing, sequencing, and error control of messages exchanged between devices, and provide a common language for devices to communicate with each other.

There are many different protocols used in computer networking, each designed for a specific purpose or function. Examples of common protocols include the Transmission Control Protocol (TCP) and the Internet Protocol (IP) which are used for transmitting data over the Internet, and the Simple Mail Transfer Protocol (SMTP) which is used for sending email messages. Other protocols include the Hypertext Transfer Protocol (HTTP) used for web browsing, the File Transfer Protocol (FTP) used for transferring files, and the Domain Name System (DNS) used for translating domain names into IP addresses.

OSI model:

The OSI (Open Systems Interconnection) model is a conceptual model that defines a standard for communication between different devices in a network. It consists of seven layers, each with a specific function and set of protocols. The OSI model provides a framework for network communication and facilitates the interoperability of different network devices and technologies.

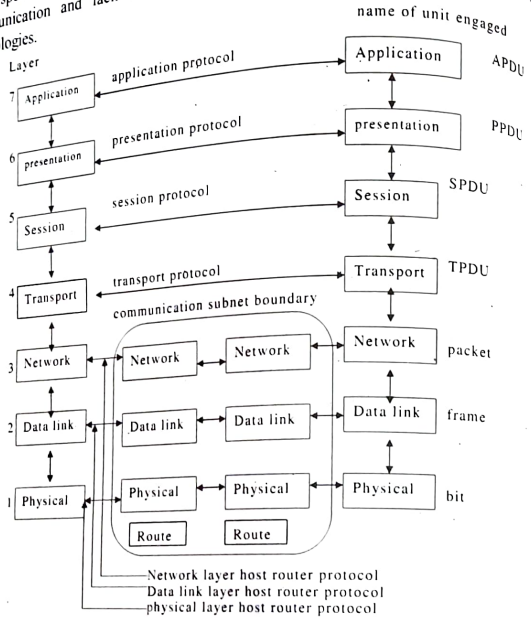

Figure: The OSI Reference Model

The seven layers of the OSI model, from top to bottom, are:

a) **Application Layer:** Provides network services to applications and end-users, such as file transfer and email.

b) **Presentation Layer:** Translates data into a format that can be understood by the application layer, and provides encryption and decryption services.

c) **Session Layer:** Manages and maintains connections between devices and applications, and establishes, manages, and terminates communication sessions.

d) **Transport Layer:** Provides reliable data transport services between devices, and manages flow control and error detection and correction.

e) **Network Layer:** Controls the operation of the subnet and provides routing services to move data across multiple networks.

f) **Data Link Layer:** Transmits data over the physical network and provides error detection and correction services.

g) **Physical Layer:** Transmits and receives raw bit streams over the physical network.

TCP/IP model

The TCP/IP model is a network communication model that is widely used in the Internet and other IP-based networks. It consists of four layers, each with a specific set of protocols and functions:

a) **Application Layer:** This layer contains protocols that support end-user applications, such as email, file transfer, and web browsing. Examples of application layer protocols include HTTP, FTP, and SMTP.

b) **Transport Layer:** This layer provides end-to-end communication services between applications on different devices, and ensures reliable data transfer. The two main protocols in this layer are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

c) **Internet Layer:** This layer provides routing services to move data between different networks, and handles the fragmentation and reassembly of data packets. The Internet Protocol (IP) is the main protocol used in this layer.

d) **Link Layer/Network Access:** This layer is responsible for transmitting data over the physical network, and includes protocols for accessing and controlling the network medium. Examples of link layer protocols include Ethernet, Wi-Fi, and Bluetooth.

***Table:** Difference between TCP/IP and OSI Model*

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.

TCP/IP	OSI
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

Networking Devices (Hubs, Bridges, Switches, and Routers and Transmission media.

Networking devices are hardware devices used to interconnect computers, servers, and other devices to form a network. These devices help in the efficient transfer of data and communication between devices connected to the network. Some common networking devices are:

Switches: A switch is a networking device that connects devices in a network and forwards data between them. It operates at the Data Link Layer (Layer 2) of the OSI model and uses MAC addresses to filter and forward data packets between network segments.

Routers: A router is a networking device that forwards data packets between different computer networks. It operates at the Network Layer (Layer 3) of the OSI model and uses IP addresses to determine the best path for data to reach its destination.

Hubs: A hub is a device that connects devices in a network and sends incoming data packets to all connected devices. It is less efficient than switches because all devices receive all the data, even if it is not intended for them.

Modems: A modem is a device that modulates digital signals into analog signals for transmission over telephone or cable lines, and demodulates analog signals back into digital signals for use by network devices.

Network Interface Cards (NICs): A NIC is a hardware component that connects a device, such as a computer or server, to a network. It provides a physical connection to the network and enables communication between the device and other devices on the network.

Repeaters: A repeater is a device that amplifies and regenerates signals in a network, to extend the distance over which data can be transmitted.

Bridge: A bridge is a networking device that connects two or more network segments or LANs (Local Area Networks) and forwards network traffic between them. It operates at the Data Link Layer (Layer 2) of the OSI model and uses MAC addresses to filter and forward data packets between network segments.

Transmission Media:

Transmission media in computer networks refer to the physical pathways used for transmitting data between devices in a network. There are two types of transmission media:

Guided Media and Unguided media

Guided transmission media are those that provide a physical path along which the data is transmitted. Examples of guided media include:

a) **Twisted pair cables:** Used for connecting devices in a LAN, they consist of pairs of twisted copper wires and are commonly used for Ethernet networks.

b) **Coaxial cables:** Used for cable TV and high-speed Internet connections, they consist of a copper core surrounded by insulation and a metallic shield.

c) **Fiber optic cables:** Used for high-speed data transfer over long distances, they use light to transmit data over glass or plastic fibers.

d) **Leased lines:** A dedicated point-to-point connection between two devices, commonly used for high-speed data transfer over long distances.

Unguided Media

Unguided media, also known as wireless media, refers to a type of transmission medium in communication networks that does not rely on a physical conductor to transmit data. Instead, it uses the air as a medium to carry data between devices. Examples of unguided media include radio waves, microwaves, and infrared radiation.

a) **Radio Waves:** Radio waves are used for wireless communication, such as radio and television broadcasting, cellular networks, and Wi-Fi. They have a wide range of frequencies and are used for both short-range and long-range communication.

b) **Microwaves:** Microwaves are higher frequency electromagnetic waves than radio waves, and are used for point-to-point communication over long distances, such as in satellite communication, and in line-of-sight communication systems such as microwave radio links.

c) **Infrared Radiation:** Infrared radiation is a type of electromagnetic radiation with wavelengths longer than visible light but shorter than radio waves. It is used for short-range communication, such as in remote controls, and in some wireless networking technologies.

d) **Light Waves:** Light waves are a type of electromagnetic radiation used for visible light communication, such as in fiber optic communication. They are also used for some wireless communication systems, such as Li-Fi, which uses light to transmit data.

5.2 DATA LINK LAYER

Data Link Layer:

The Data Link Layer is the second layer of the OSI (Open Systems Interconnection) model and is responsible for providing reliable data transfer between devices on the same physical network. It ensures that data is transmitted error-free and in the correct sequence.

The Data Link Layer is divided into two sublayers: The Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The LLC sublayer provides flow control and error checking, and handles addressing and framing of data packets. The MAC sublayer provides access to the physical network, and handles the transmission of data over the network using a unique MAC address for each device.

The main functions of the Data Link Layer are:

a) **Framing**: The Data Link Layer divides data received from the Network Layer into manageable frames, and adds a header and a trailer to each frame to identify the source and destination devices.

b) **Addressing**: The Data Link Layer uses the Media Access Control (MAC) address to identify each device connected to the network. This allows devices to communicate directly with each other on the same network.

c) **Flow Control**: The Data Link Layer provides flow control mechanisms to manage the flow of data between devices, and to prevent buffer overflow and data loss.

d) **Error Detection and Correction:** The Data Link Layer checks each frame for errors during transmission and uses error detection and correction mechanisms, such as cyclic redundancy check (CRC), to ensure that data is transmitted error-free.

e) **Access Control**: The Data Link Layer provides access control mechanisms to regulate access to the physical network, and to prevent collisions and data loss in shared media networks.

f) **Media Conversion:** The Data Link Layer provides media conversion mechanisms to enable different types of devices to communicate with each other, and to ensure that data is transmitted in the correct format over the network.

Error Detection and Correction:

Error detection and correction is an important function of the Data Link Layer, which is responsible for ensuring that data is transmitted error-free over a network. There are several mechanisms used for error detection and correction in the Data Link Layer, including:

a) **Parity Check:** Parity check is a simple error detection mechanism that adds an extra bit, called the parity bit, to each byte of data. The parity bit is set to 1 or 0, depending on the number of 1s in the data byte, and is used to detect errors during transmission.

b) **Checksum:** Checksum is a more advanced error detection mechanism that calculates a checksum value for each data packet, based on the contents of the packet. The receiving device calculates its own checksum value and compares it to the checksum value in the packet to detect errors.

c) **Cyclic Redundancy Check (CRC):** CRC is a more sophisticated error detection mechanism that uses a mathematical algorithm to generate a checksum value for the data packet. The receiving device performs the same calculation and compares its result to the checksum value in the packet to detect errors.

d) **Forward Error Correction (FEC):** FEC is an error correction mechanism that adds redundant data to the transmitted data to enable the receiving device to correct errors in the data. It is commonly used in satellite communication and other communication systems where data loss is common.

Flow Control:

Flow control is an important service provided by the Data Link Layer, which is responsible for managing the flow of data between devices on the same physical network. The main purpose of flow control is to ensure that data is transmitted at a rate that is manageable for the receiving device, and to prevent buffer overflow and data loss.

There are two types of flow control: stop-and-wait flow control and sliding window flow control.

a) **Stop-and-wait flow control:** In stop-and-wait flow control, the transmitting device sends a frame of data to the receiving device and waits for an acknowledgement (ACK) before sending the next frame. This ensures that the receiving device can process each frame before receiving the next one, and prevents buffer overflow and data loss.

b) **Sliding window flow control:** In sliding window flow control, the transmitting device sends a series of frames to the receiving device, and the receiving device sends back an acknowledgement that indicates the number of frames that it is ready to receive. This allows the transmitting device to send multiple frames before waiting for an ACK, and ensures that the receiving device can process the data at a rate that is manageable.

Data Link Protocol:

A data link protocol is a set of rules and procedures used by the Data Link Layer to ensure reliable data transfer between devices on the same physical network. The data link protocol defines the format and structure of data frames, as well as the mechanisms used for addressing, flow control, error detection and correction, and access control.

Multiple Access Protocols:

Multiple Access Protocols are used in the Data Link Layer of computer networks to allow multiple devices to share a single communication channel. These protocols are used to regulate the access to the channel and prevent collisions between data frames transmitted by different devices.

There are several types of Multiple Access Protocols, including:

a) **Carrier Sense Multiple Access with Collision Detection (CSMA/CD):** In CSMA/CD, each device listens for carrier signals on the communication channel to determine if the channel is busy or available. If the channel is available, the device can transmit a frame of data. If two or more devices attempt to transmit data at the same time and a collision occurs, the devices stop transmitting and wait for a random time before trying again.

b) **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA):** In CSMA/CA, devices must request permission from the access point before transmitting data. The access point determines which device has access to the channel and issues a transmission grant. This protocol is commonly used in wireless networks, such as Wi-Fi.

c) **Time Division Multiple Access (TDMA):** In TDMA, the communication channel is divided into time slots, and each device is assigned a specific time slot during which it can transmit data. This protocol is commonly used in satellite communication and some cellular networks.

d) **Frequency Division Multiple Access (FDMA):** In FDMA, the communication channel is divided into frequency bands, and each device is assigned a specific frequency band during which it can transmit data. This protocol is commonly used in some cellular networks.

e) **Code Division Multiple Access (CDMA):** In CDMA, each device is assigned a unique code, and the communication channel is shared by all devices simultaneously. The receiving device uses the assigned code to separate the data from each device. This protocol is commonly used in some cellular networks.

LAN addressing and ARP (Address Resolution Protocol):

In computer networking, LAN (Local Area Network) addressing is the process of assigning unique addresses to each device on a local area network. The LAN address is used by devices to communicate with each other on the same network.

There are two types of LAN addressing: MAC addressing and IP addressing.

a) **MAC Addressing:** The Media Access Control (MAC) address is a unique identifier assigned to each network interface card (NIC) on a device. This address is used by the Data Link Layer to identify devices on the same network. The MAC address is a 48-bit number, usually represented as six pairs of hexadecimal digits separated by colons (for example, 00:11:22:33:44:55).

b) **IP Addressing:** The Internet Protocol (IP) address is a unique identifier assigned to each device on a network. The IP address is used by the Network Layer to identify devices on the same network or on different networks. The IP address is a 32-bit number, usually represented as four decimal numbers separated by dots (for example, 192.168.0.1).

ARP (Address Resolution Protocol):

The Address Resolution Protocol (ARP) is a protocol used in computer networking to map a network address (such as an IP address) to a physical address (such as a MAC address). ARP is used by devices to determine the MAC address of another device on the same network, which is necessary for communication over the Data Link Layer.

Types of Address Resolution Protocol:

a) **Reverse ARP (RARP):** Reverse ARP is used to map a data link layer address to a network layer address. It is used by diskless workstations to obtain their IP address from a RARP server.

b) **Inverse ARP (IARP):** Inverse ARP is used to map a network layer address to a data link layer address on Frame Relay networks.

c) **Proxy ARP:** Proxy ARP is used by a device (such as a router) to answer ARP requests for a device on a different network. The device with the IP address being requested is not on the same network as the requesting device, but the requesting device sends an ARP request to the local network anyway. The device that receives the ARP request responds with its own MAC address, allowing the requesting device to forward data to the device with the requested IP address.

Ethernet:

Ethernet is a standard communication protocol used in computer networks for wired local area networks (LANs). It is used in the Data Link Layer of the OSI model, and provides a way for devices to communicate with each other over a shared physical medium, such as a coaxial cable or twisted pair cable.

Ethernet defines the format and structure of data frames, as well as the mechanisms used for addressing, flow control, error detection and correction, and access control. Ethernet frames consist of a header and a trailer, which contain information about the source and destination devices, as well as the type of data being transmitted.

IEEE 802.3(Ethernet):

IEEE 802.3 is a set of standards for Ethernet, a protocol used in computer networking to connect devices on a local area network (LAN). The IEEE 802.3 standard defines the physical layer and the data link layer of the OSI model, and provides a standardized way for devices to communicate with each other over a shared physical medium, such as a twisted pair or coaxial cable.

The IEEE 802.3 standard specifies the format and structure of Ethernet frames, including the preamble, header, and trailer. It also defines the mechanisms used for addressing, flow control, error detection and correction, and access control.

There are several types of Ethernet networks, each with different characteristics and capabilities. Some of the most common types of Ethernet networks include:

a) **10BASE-T Ethernet:** This is the original Ethernet standard, which uses a twisted pair cable and provides a data transfer rate of 10 megabits per second (Mbps).

b) **Fast Ethernet (100BASE-T):** This standard uses a twisted pair cable and provides a data transfer rate of 100 megabits per second (Mbps).

c) **Gigabit Ethernet (1000BASE-T):** This standard uses a twisted pair cable and provides a data transfer rate of 1 gigabit per second (Gbps).

d) **10 Gigabit Ethernet (10GBASE-T):** This standard uses a twisted pair cable or fiber optic cable and provides a data transfer rate of 10 gigabits per second (Gbps).

e) **40 Gigabit Ethernet (40GBASE-T):** This standard uses a fiber optic cable and provides a data transfer rate of 40 gigabits per second (Gbps).

f) **100 Gigabit Ethernet (100GBASE-T):** This standard uses a fiber optic cable and provides a data transfer rate of 100 gigabits per second (Gbps).

g) **Ethernet over Power (EoP):** This standard uses existing electrical wiring to transmit Ethernet signals, and provides a data transfer rate of up to 1 gigabit per second (Gbps).

h) **Power over Ethernet (PoE):** This standard allows devices to be powered through the Ethernet cable, eliminating the need for a separate power source.

802.4(Token Bus):

IEEE 802.4, also known as Token Bus, is a communication protocol for local area networks (LANs). It was developed in the early 1980s as an alternative to the more popular Ethernet standard. Token Bus is a bus-based network topology, in which all devices are connected to a

shared communication medium (a coaxial cable) and data is transmitted serially from one device to the next. The Token Bus protocol is based on a token-passing mechanism, in which a token is passed between devices to control access to the communication medium. Only the device that holds the token is allowed to transmit data, which ensures that data is transmitted in an orderly and controlled manner, avoiding collisions and other types of interference.

802.5(Token Ring):

IEEE 802.5, also known as Token Ring, is a communication protocol for local area networks (LANs). It was developed as an alternative to the more popular Ethernet standard in the 1980s. Token Ring is a ring-based network topology, in which all devices are connected to each other in a circular fashion, forming a logical ring. The Token Ring protocol is based on a token-passing mechanism, in which a token is passed between devices to control access to the communication medium. Only the device that holds the token is allowed to transmit data, which ensures that data is transmitted in an orderly and controlled manner, avoiding collisions and other types of interference.

CSMA/CD:

The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol is used to detect collisions in the media access control (MAC) layer of a network. When a collision is detected, the protocol stops transmission and sends a jam signal to prevent the sender from wasting time and resources. If multiple stations detect a collision, the protocol waits for a random amount of time before attempting to transmit again. The CSMA/CD protocol ensures efficient transmission and prevents wasted bandwidth in a network.

Advantages of CSMS/CD:

a) The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol has several advantages, including the ability to detect collisions quickly on a shared channel.

b) CSMA/CD is an improvement over CSMA for collision detection, and it helps prevent wasted transmission by ensuring that each station shares bandwidth fairly.

c) CSMA/CD has lower overhead than CSMA/CA and allows for more efficient use of available bandwidth. Overall, CSMA/CD is a cost-effective and flexible protocol for local area networks.

Wireless LANs:

A Wireless Local Area Network (WLAN) allows a mobile user to connect to a Local Area Network (LAN) using a wireless connection. WLANs use the IEEE 802.11 group of standards to define their technologies, which include the Ethernet protocol and the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for path sharing. WLANs also use the Wired Equivalent Privacy (WEP) algorithm for encryption.

WLANs provide high-speed data communication in small areas such as offices and buildings, allowing users to move around while staying connected to the network. Wireless LAN technology can be a cost-effective alternative to laying cables, and it is sometimes the only option for providing high-speed internet access. As a result, wireless solutions are becoming increasingly popular.

PPP (Point to Point Protocol):

The Point-to-Point Protocol (PPP) is a data link protocol used to establish a direct connection between two network nodes. It is commonly used in dial-up connections and Virtual Private Networks (VPNs) to provide secure and reliable transmission of data over the internet.

The Point-to-Point Protocol (PPP) is designed to work with a variety of physical network media, including serial cables, phone lines, trunk lines, cellular telephones, and fiber optic links such as SONET. Because PPP is a data link layer protocol that identifies the source and destination of transmissions, it is commonly used by Internet Service Providers (ISPs) to provide dial-up access to the internet.

Overall, PPP is a flexible protocol that can support a wide range of network topologies and media, making it an important component of modern networking technologies.

Wide Area Protocol (WAP)

Wide area protocols are a set of protocols used in wide area networks (WANs) to establish communication between geographically dispersed devices. These protocols are designed to enable devices to communicate over long distances, often across different network technologies and architectures.

Some of the commonly used wide area protocols include:

a) X.25: A protocol used to transmit data over public packet-switched networks.

b) Frame Relay: A protocol used to transmit data between devices over a high-speed digital connection.

c) ATM (Asynchronous Transfer Mode): A protocol used to transfer data between devices over a cell-based network.

d) MPLS (Multiprotocol Label Switching): A protocol used to direct data traffic between devices over a wide area network.

e) TCP/IP: A suite of protocols used to connect devices to the internet and to establish communication between them.

5.3 NETWORK LAYER

Network Layer:

The Network Layer is a layer in the OSI model and the TCP/IP protocol suite that provides logical addressing and routing services for data packets as they are transmitted across a network. The Network Layer is responsible for moving data between networks, and it is the layer where routing takes place.

At the Network Layer, data packets are encapsulated with IP addresses, which allow them to be directed to their destination across different networks. The Network Layer provides several key services, including addressing, routing, and fragmentation.

Addressing (Internet address, classful address):

Internet Address: An Internet address, also known as an IP address, is a unique identifier assigned to every device connected to the internet. An IP address is a numerical label that

identifies the device's location on a network, allowing it to send and receive data over the internet.

There are two main versions of IP addresses: IPv4 and IPv6. IPv4 addresses are 32 bits in length and are represented in decimal form, while IPv6 addresses are 128 bits in length and are represented in hexadecimal form. IP addresses are divided into two parts: the network ID and the host ID. The network ID identifies the network to which the device is connected, while the host ID identifies the specific device on that network.

Classful address

Classful IP addressing is a method of dividing IP addresses into classes based on the range of their network ID. Under classful addressing, IP addresses are divided into five classes: A, B, C, D, and E.

a) **Class A:** IP addresses in Class A have their first octet in the range of 1-126. The first octet represents the network ID, while the remaining three octets represent the host ID. Class A addresses are typically used for large networks, as they provide a large number of hosts.

b) **Class B:** IP addresses in Class B have their first octet in the range of 128-191. The first two octets represent the network ID, while the remaining two octets represent the host ID. Class B addresses are typically used for medium-sized networks.

c) **Class C:** IP addresses in Class C have their first octet in the range of 192-223. The first three octets represent the network ID, while the remaining octet represents the host ID. Class C addresses are typically used for small networks.

d) **Class D:** IP addresses in Class D are used for multicast addresses, which allow a single packet to be sent to multiple devices at the same time. Class D addresses have their first octet in the range of 224-239.

e) **Class E:** IP addresses in Class E are reserved for experimental use and are not used for normal network communication. Class E addresses have their first octet in the range of 240-255.

Subnetting:

Subnetting is a technique used in IP networking to divide a larger network into smaller, more manageable sub-networks, or subnets. This allows network administrators to create more efficient and secure networks by reducing broadcast traffic and isolating network segments.

Subnetting is based on the concept of the network ID and the host ID in an IP address. In a classful network, the network ID and host ID are fixed based on the class of the IP address. However, with subnetting, a portion of the host ID is used to create the subnet ID, which allows a single network to be divided into multiple subnets.

For example, if a network has an IP address of 192.168.0.0 and a subnet mask of 255.255.255.0, the first three octets (192.168.0) represent the network ID, while the last octet (0) represents the host ID. The subnet mask indicates that the first 24 bits (or 3 octets) of the IP address are used for the network ID, while the last 8 bits (or 1 octet) are used for the host ID. This allows the network to be divided into up to 256 different subnets, each with its own range of host addresses.

Routing Protocols (RIP, OSPF, BGP, Unicast and multicast routing protocols):

A routing protocol is a protocol used by routers to exchange information with other routers in order to determine the best path for forwarding network traffic. Routing protocols are used in IP networks to create and maintain a routing table, which contains information about the network topology and the best path to reach each destination on the network.

There are several types of routing protocols, including:

Routing Information Protocol (RIP) is a distance-vector routing protocol used in IP networks. RIP is one of the oldest routing protocols still in use, and it is designed to support small to medium-sized networks.

Routing Information Protocol (RIP)

RIP stands for Routing Information Protocol. RIP works by broadcasting routing information to all routers in a network. Each router then uses the received information to update its routing table, which contains information about the best path to reach each destination on the network. RIP uses a hop count metric to determine the best path to a destination, with the goal of minimizing the number of hops required to reach the destination.

RIP has a number of limitations, including a limited hop count of 15, which means that it cannot be used for large networks or networks with complex topologies. RIP also has a slow convergence time, which can lead to network instability in the event of a topology change.

Open Shortest Path First (OSPF):

Open Shortest Path First (OSPF) is a link-state routing protocol used in IP networks. It is designed to support larger networks with complex topologies and provides faster convergence and more efficient use of network bandwidth than distance-vector protocols such as Routing Information Protocol (RIP).

OSPF works by exchanging link-state advertisements (LSAs) between routers to build a complete map of the network topology. Each router then uses the map to calculate the shortest path to each destination on the network. OSPF uses a cost metric based on the bandwidth of each link to determine the shortest path, with the goal of minimizing the overall cost of the path.

Border Gateway Protocol (BGP):

Border Gateway Protocol (BGP) is a routing protocol used in IP networks to exchange routing information between different Autonomous Systems (AS). An Autonomous System is a network that is controlled by a single entity and has a unique identifier, known as an AS number.

BGP is designed to support large-scale networks with complex topologies, and it uses a path-vector algorithm to determine the best path for forwarding network traffic. BGP takes into account several path attributes, such as AS path length, local preference, and MED (Multi-Exit Discriminator), to determine the best path to a destination.

BGP is used primarily in the Internet to exchange routing information between different Internet Service Providers (ISPs) and large enterprise networks. BGP allows each ISP or enterprise to maintain its own routing policies and preferences, while still ensuring that network traffic is routed in the most efficient and reliable way possible.

BGP has several advanced features, such as:

a) Policy-based routing: BGP allows network administrators to define complex routing policies based on factors such as cost, bandwidth, and performance.

b) Route aggregation: BGP allows multiple network prefixes to be combined into a single route, which can reduce the size of the routing table and improve network performance.

c) Load balancing: BGP allows network traffic to be distributed across multiple paths, which can improve network performance and reliability.

Unicast Routing Protocol:

Unicast routing protocol is a type of routing protocol used in computer networks to forward packets from a single source to a single destination. Unicast routing protocols are designed to provide efficient and reliable routing for point-to-point communication, and they are commonly used in small to medium-sized networks.

There are several types of unicast routing protocols, including:

a) Distance-vector routing protocol: This type of protocol calculates the best path to a destination based on the number of hops required to reach the destination. Examples of distance-vector routing protocols include Routing Information Protocol (RIP) and Interior Gateway Routing Protocol (IGRP).

b) Link-state routing protocol: This type of protocol builds a complete map of the network topology by exchanging link-state information between routers. Each router then uses the map to calculate the shortest path to each destination. Examples of link-state routing protocols include Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS).

c) Path-vector routing protocol: This type of protocol uses a vector of AS numbers to determine the best path to a destination. Path-vector routing protocols are commonly used in large-scale networks such as the Internet, and examples include Border Gateway Protocol (BGP).

Multicast Routing Protocol (MRP):

Multicast Routing Protocol (MRP) is a type of routing protocol used in computer networks to forward data packets to multiple recipients at the same time. MRP is designed to support one-to-many and many-to-many communication, and it is commonly used in applications such as video streaming, online gaming, and content distribution.

There are several types of MRP, including:

Distance-vector multicast routing protocol: This type of protocol calculates the best path to a multicast group based on the number of hops required to reach the group. Examples of distance-vector multicast routing protocols include Distance Vector Multicast Routing Protocol (DVMRP) and Multicast Open Shortest Path First (MOSPF).

Source-specific multicast routing protocol: This type of protocol is designed to optimize the delivery of multicast traffic by using the source address to determine the best path to the multicast group. Examples of source-specific multicast routing protocols include Protocol-Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP).

Any-Source Multicast (ASM) routing protocol: This type of protocol is designed to deliver multicast traffic from any source to a multicast group. Examples of ASM routing protocols include PIM-SM (Sparse Mode) and PIM-DM (Dense Mode).

***Routing algorithms* (shortest path algorithm, flooding, distance vector routing, link state routing):**

Routing algorithms are used in computer networks to determine the best path for routing data packets from a source node to a destination node. There are several types of routing algorithms, including:

Distance-vector routing algorithm: This type of algorithm calculates the shortest path to a destination based on the number of hops required to reach the destination. The most well-known example of a distance-vector routing algorithm is the Routing Information Protocol (RIP).

Link-state routing algorithm: This type of algorithm builds a complete map of the network topology by exchanging link-state information between routers. Each router then uses the map to calculate the shortest path to each destination. The most well-known examples of link-state routing algorithms are Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS).

Path-vector routing algorithm: This type of algorithm uses a vector of AS numbers to determine the best path to a destination. Path-vector routing algorithms are commonly used in large-scale networks such as the Internet, and the most well-known example is the Border Gateway Protocol (BGP).

Flooding: Flooding is a type of routing algorithm used in computer networks to forward data packets to all connected nodes. In a flooding algorithm, each node that receives a packet broadcasts the packet to all of its neighbors, except for the node from which the packet was received. The process is repeated until all nodes in the network have received the packet.

Flooding algorithms are simple to implement and are effective in small networks where the overhead of broadcasting packets is relatively low. However, they can be highly inefficient in large networks, as the number of packets transmitted can grow exponentially as the network size increases. In addition, flooding algorithms are susceptible to broadcast storms, where a single packet can trigger a large number of additional packets, leading to network congestion and reduced performance.

To address the limitations of flooding algorithms, several modifications have been developed, including:

a) Randomized flooding: This modification introduces randomness into the flooding algorithm to reduce the likelihood of broadcast storms.

b) Reverse path forwarding: This modification uses the knowledge of the shortest path back to the source to avoid unnecessary flooding.

c) Selective flooding: This modification limits the scope of flooding to a specific subset of the network, rather than flooding the entire network.

Routing Protocols (ARP, RARP, IP, ICMP):

Routing protocols are used in computer networks to determine the best path for forwarding data packets from a source to a destination. There are several types of routing protocols including:

a) **Address Resolution Protocol**: The Address Resolution Protocol (ARP) is a protocol used in computer networks to map a network address (such as an IP address) to a physical address (such as a MAC address). ARP is used by network devices to identify the MAC address of another device on the same network when communicating.

b) **Reverse Address Resolution Protocol (RARP):** It is a protocol used in computer networks to map a physical (MAC) address to an IP address. Unlike the Address Resolution Protocol (ARP), which maps an IP address to a MAC address, RARP maps a MAC address to an IP address.

RARP is typically used in diskless workstations, which do not have permanent storage such as a hard drive, and therefore cannot store their own IP address configuration. Instead, the workstation sends its own MAC address to a RARP server, which returns the corresponding IP address. The workstation can then use this IP address to communicate on the network. RARP has been largely superseded by other protocols, such as Dynamic Host Configuration Protocol (DHCP), which can provide more flexible and dynamic IP address allocation. However, RARP is still used in some legacy systems and can be useful in certain niche applications.

c) **Internet Protocol (IP):**

The Internet Protocol (IP) is a protocol used in computer networks to route data packets between devices. IP is responsible for providing logical addressing, fragmentation and reassembly, and error checking for data packets, and is used by virtually all communication on the internet.

IP operates at the network layer of the TCP/IP protocol suite, and is responsible for providing a unique logical address to every device on the network. This logical address is known as an IP address, and is typically represented as a 32-bit binary number, although newer versions of IP, such as IPv6, use larger address spaces.

d) **The Internet Control Message Protocol (ICMP):**

The Internet Control Message Protocol (ICMP) is a protocol used in computer networks to report error conditions and provide diagnostic information. ICMP is an integral part of the Internet Protocol (IP) suite, and is used by network devices such as routers to communicate error information to other devices on the network.

ICMP is typically used for two main purposes: error reporting and network management. For example, if a router receives an IP packet that it cannot forward, it will send an ICMP message to the source IP address to indicate that the packet has been dropped. ICMP is also used to perform diagnostic functions, such as ping, which uses ICMP echo requests and replies to test network connectivity between devices.

Some of the most common ICMP message types include:

a) Echo request/reply: Used to test network connectivity using the ping command.

b) Destination unreachable: Sent by a router to indicate that a packet cannot be forwarded.

c) Time exceeded: Sent by a router to indicate that a packet has exceeded its time-to-live (TTL) value.

d) Redirect: Sent by a router to indicate that a better next-hop address is available for a particular destination.

IPv6 (Packet formats, Extension headers, Transition from IPv4 to IPv6, and Multicasting).

IPv6 (Internet Protocol version 6) is the latest version of the Internet Protocol (IP) and is designed to replace the earlier IPv4 protocol. IPv6 is intended to solve many of the problems that IPv4 has faced, such as address exhaustion, limited quality of service capabilities, and security issues.

IPv6 uses a 128-bit address format, which provides a much larger address space than the 32-bit format used in IPv4. This means that IPv6 can support a much larger number of devices on the internet, as well as provide improved quality of service and security features.

The packet format of IPv6 (Internet Protocol version 6) is designed to be more efficient than the packet format of IPv4, while also providing support for new features such as flow labeling and larger address space. The IPv6 packet format consists of the following fields:

a) Version: This 4-bit field indicates the version of the IP protocol being used. For IPv6, this field is set to 6.

b) Traffic Class: This 8-bit field is used to classify packets based on the type of traffic they carry, such as real-time traffic or bulk data.

c) Flow Label: This 20-bit field is used to mark packets with a flow label, which can be used to provide quality of service (QoS) guarantees or other types of processing.

d) Payload Length: This 16-bit field indicates the length of the packet payload, in octets.

e) Next Header: This 8-bit field indicates the type of header that follows the IPv6 header. For example, it could indicate a TCP header or an ICMP header.

f) Hop Limit: This 8-bit field is similar to the TTL field in IPv4, and is used to limit the number of hops a packet can travel before being discarded.

g) Source Address: This 128-bit field contains the source IPv6 address.

Destination Address: This 128-bit field contains the destination IPv6 address.

Extension Headers:

In IPv6 (Internet Protocol version 6), extension headers are additional headers that can be added to the basic IPv6 packet format to provide additional functionality or features. Extension headers are placed after the IPv6 header and before the packet payload, and are identified by the Next Header field in the IPv6 header.

There are several different types of extension headers in IPv6, each with its own specific purpose:

a) Hop-by-Hop Options Header: This header is used to carry optional information that must be processed by every router along the packet's path.

b) Destination Options Header: This header is similar to the Hop-by-Hop Options Header, but is only processed by the final destination.

c) Routing Header: This header is used to specify a list of intermediate nodes that the packet should pass through.

d) Fragment Header: This header is used to support packet fragmentation and reassembly, allowing large packets to be broken up into smaller pieces for transmission.

e) Authentication Header: This header is used to provide data authentication and integrity, ensuring that packets have not been modified in transit.

f) Encapsulating Security Payload Header: This header is used to provide confidentiality and integrity protection for packet payloads.

Transition from IPv4 to IPv6:

a) The transition from IPv4 (Internet Protocol version 4) to IPv6 (Internet Protocol version 6) is a necessary process due to the depletion of the available IPv4 address space. IPv6 provides a larger address space, improved security, and additional features that make it a necessary upgrade for the internet. The transition from IPv4 to IPv6 can be accomplished in several ways:

b) Dual-stack: In a dual-stack approach, both IPv4 and IPv6 are supported on a network. This allows devices to communicate using either protocol, and is the most common approach to transition to IPv6.

c) Tunneling: Tunneling involves encapsulating IPv6 packets within IPv4 packets, allowing them to traverse an IPv4-only network. This approach is useful when connecting isolated IPv6 networks across an IPv4 network.

d) Translation: Translation involves converting IPv6 packets to IPv4 packets, allowing them to be transmitted across an IPv4 network. This approach is useful when the network infrastructure is unable to support IPv6 natively.

e) The transition from IPv4 to IPv6 is a gradual process that will take time to complete. It is important for network administrators to plan for the transition and ensure that their network infrastructure is capable of supporting both IPv4 and IPv6. This may require upgrading network hardware, software, and applications to support the new protocol.

In summary, the transition from IPv4 to IPv6 is necessary to support the growth of the internet and provide new features and capabilities. The transition can be accomplished through a variety of approaches, including dual-stack, tunneling, and translation. Network administrators should plan for the transition and ensure that their network infrastructure is capable of supporting both protocols during the transition period.

5.4 TRANSPORT LAYER

The Transport Layer is the fourth layer in the OSI (Open Systems Interconnection) reference model, and is responsible for providing reliable end-to-end communication between applications running on different devices. The Transport Layer ensures that data is transmitted from the source to the destination in a reliable and efficient manner.

The Transport Layer is divided into two protocols: Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). These protocols provide different levels of reliability and are used for different types of applications.

TCP provides reliable, connection-oriented communication between applications. TCP breaks data into smaller segments and uses a three-way handshake to establish a connection between the source and destination devices. TCP provides error checking and flow control to ensure that data is transmitted reliably.

UDP, on the other hand, is a connectionless protocol that provides fast, unreliable communication between applications. UDP does not provide error checking or flow control, but is useful for applications that require fast, real-time communication such as video streaming and online gaming.

The Transport Layer also provides multiplexing and demultiplexing services, allowing multiple applications to use the same network connection. This is accomplished by using port numbers to identify different applications running on the same device.

In summary, the Transport Layer is responsible for providing reliable end-to-end communication between applications running on different devices. TCP and UDP are the two protocols used at this layer, providing different levels of reliability and are used for different types of applications. The Transport Layer also provides multiplexing and demultiplexing services to allow multiple applications to use the same network connection.

Transport Services:

The transport service is a set of protocols and functions that provide end-to-end communication between processes running on different hosts. The transport layer receives data from the application layer and prepares it for transmission over the network. It establishes a logical connection between the sender and receiver and ensures that the data is delivered reliably, in the correct order, and without errors. The transport service can also provide flow control, congestion control, and multiplexing of multiple connections over a single network connection. Examples of transport layer protocols include TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).

Port and Socket:

a) In the Transport Layer of computer networking, ports and sockets are used to facilitate communication between applications running on different devices.

b) A port is a number used to identify a specific application running on a device. Ports are assigned to applications to ensure that data sent to the device is correctly directed to the correct application. The Transport Layer uses port numbers to identify the application and

the destination device, allowing multiple applications to use the same network connection. Port numbers are divided into three ranges: well-known ports, registered ports, and dynamic or private ports.

c) A socket is a combination of an IP address and a port number that identifies a unique endpoint in a network. A socket is used to establish a connection between two applications running on different devices. A socket is created by the Transport Layer when an application requests a connection, and is used to send and receive data between the two endpoints.

d) When an application requests a connection, the Transport Layer creates a socket that includes the source IP address and port number and the destination IP address and port number. This socket is used to establish a virtual circuit between the two applications, allowing them to communicate with each other.

Connection establishment and connection release:

In the Transport Layer of computer networking, connection establishment and connection release are two important processes that are used to establish and terminate connections between applications running on different devices.

a) Connection establishment is the process of establishing a virtual circuit between two applications running on different devices. This process is used by connection-oriented protocols such as TCP. During the connection establishment process, the two devices exchange control messages to agree on the initial sequence numbers, window sizes, and other parameters that are needed to ensure reliable data transmission. Once the parameters have been agreed upon, data can be transmitted over the virtual circuit. The connection establishment process is also used to establish security mechanisms such as encryption and authentication.

b) Connection release is the process of terminating a virtual circuit between two applications running on different devices. This process is used by connection-oriented protocols such as TCP to ensure that the virtual circuit is properly released and that resources used for the connection can be freed. During the connection release process, the two devices exchange control messages to signal that they have finished transmitting data and that the virtual circuit can be released. Once the virtual circuit has been released, the resources used for the connection can be freed for use by other applications.

Flow control & buffering

In the Transport Layer of computer networking, flow control and buffering are two important mechanisms used to manage the transmission of data between applications running on different devices.

Flow control is the process of regulating the amount of data sent by the sender to ensure that the receiver can process the data at the rate it is being sent. Flow control prevents the receiver from being overwhelmed by data it cannot process, which can lead to dropped packets, network congestion, and other issues. Flow control mechanisms include techniques such as windowing, where the receiver sends messages to the sender indicating the amount of data it can accept.

Buffering is the process of temporarily storing data in a buffer before it is transmitted to the receiver. Buffers are used to smooth out fluctuations in network traffic and to ensure that data is transmitted at a constant rate. Buffers are used by the sender and receiver, and can be implemented in hardware or software. Buffers are sized according to the amount of data that needs to be transmitted, and are used to prevent data loss due to network congestion or other issues.

Multiplexing and de-multiplexing

Multiplexing and de-multiplexing are techniques used in the Transport Layer of computer networking to allow multiple applications to share a single network connection.

Multiplexing is the process of combining multiple data streams from different applications into a single data stream that can be transmitted over a single network connection. Multiplexing allows multiple applications to share a single network connection, which can improve the efficiency of the network and reduce the cost of network infrastructure. Multiplexing can be done at different layers of the network stack, including the Transport Layer, where it is used to combine multiple application data streams into a single data stream.

There are several techniques for multiplexing in the Transport Layer of computer networking. The main multiplexing techniques are as follows:

a) **Time Division Multiplexing (TDM):** TDM is a technique in which multiple signals are combined into a single signal by assigning each signal a specific time slot. During the time slot, the signal is transmitted over the network, and then the next signal is transmitted in the next time slot. TDM is commonly used in digital communication systems and is an efficient way to use bandwidth.

b) **Frequency Division Multiplexing (FDM):** FDM is a technique in which multiple signals are combined into a single signal by assigning each signal a specific frequency band. Each signal is then transmitted at its assigned frequency band, and the signals are separated at the receiving end based on their frequency band. FDM is commonly used in analog communication systems and is an efficient way to use bandwidth.

c) **Statistical Multiplexing**: Statistical multiplexing is a technique in which multiple signals are combined into a single signal based on the bandwidth requirements of each signal. During periods of low bandwidth usage, signals can share the available bandwidth, while during periods of high bandwidth usage, the signals are given priority based on their requirements.

d) **Wavelength Division Multiplexing (WDM):** WDM is a technique used in optical communication systems in which multiple signals are combined into a single signal by assigning each signal a specific wavelength. Each signal is then transmitted at its assigned wavelength, and the signals are separated at the receiving end based on their wavelength.

e) **Code Division Multiplexing (CDM):** CDM is a technique in which multiple signals are combined into a single signal by assigning each signal a specific code. Each signal is then transmitted using its assigned code, and the signals are separated at the receiving end based on their code. CDM is commonly used in wireless communication systems and is an efficient way to use bandwidth.

De-multiplexing is the process of separating a single data stream into multiple data streams for different applications. De-multiplexing is done at the receiving end of the network connection, where the data stream is separated into different data streams for different applications. De-multiplexing is necessary to ensure that the data is correctly directed to the correct application, and to prevent data corruption or loss.

Congestion control algorithm:

In computer networking, congestion occurs when there is a higher demand for network resources than the available capacity can accommodate. When congestion occurs, packets of data may be delayed, lost, or dropped, resulting in degraded network performance and reduced throughput. Congestion can occur at various points in a network, including the sender, receiver, or intermediate network nodes such as routers or switches.

Congestion can be caused by various factors, such as an increase in traffic volume, network failures, or a misconfiguration of network devices. Congestion can also occur when the network is not designed to handle the traffic load, such as when the network topology does not provide enough bandwidth for the traffic demand.

There are two congestion control algorithm which are as follows:

a) **The leaky bucket algorithm:**

The leaky bucket algorithm is commonly used in the context of network traffic shaping or rate-limiting. It is designed to control the rate at which traffic is sent to the network and shape burst traffic to a steady traffic stream. Along with token bucket execution, it is commonly used for traffic shaping algorithms.

One of the disadvantages of the leaky bucket algorithm is that it can result in inefficient use of available network resources, including bandwidth. The algorithm may not effectively use all available network resources, resulting in wasted capacity. In contrast, the token bucket algorithm may be more efficient in utilizing network resources.

b) **Token Bucket Algorithm:**

The leaky bucket algorithm has a fixed output rate and cannot accommodate bursts of traffic. In situations where bursts of traffic occur, a more flexible algorithm is required. The token bucket algorithm is commonly used in network traffic shaping or rate-limiting because it is a more flexible algorithm that does not lose information.

In the token bucket algorithm, the tokens in the bucket are used to determine when traffic should be sent. The bucket contains a predefined number of tokens, and each token represents a packet of a certain size. When a packet is sent, tokens are removed from the bucket. When there are no more tokens, the algorithm restricts the flow of traffic.

The token bucket algorithm can accommodate bursts of traffic, up to the number of tokens in the bucket. When there are tokens in the bucket, the traffic can flow up to the peak burst rate. However, if there are no tokens, the traffic flow is restricted.

5.5 APPLICATION LAYER

The Application layer is the topmost layer of the OSI reference model and is responsible for providing network services to user applications. This layer interacts directly with the end-user application and supports a wide range of communication services and applications, including email, file transfer, and web browsing. The Application layer supports various protocols, including HTTP, SMTP, FTP, DNS, Telnet, and others. These protocols define how data is transferred and presented to the user application.

Web (HTTP & HTTPS):

HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) are application-layer protocols used for transmitting data over the internet.

HTTP is a protocol used for transmitting web pages, images, and other content over the internet. It is a stateless protocol, meaning it does not maintain any session or connection information between the client and server. Instead, each request and response are treated as separate transactions. HTTP uses port 80 as its default port and is widely used for accessing web pages.

HTTPS is a secure version of HTTP, which uses encryption to protect the data being transmitted over the internet. HTTPS uses Secure Sockets Layer (SSL) or Transport Layer Security (TLS) to encrypt the data, making it more difficult for unauthorized parties to intercept and read the data. HTTPS uses port 443 as its default port and is used for transmitting sensitive information such as login credentials, credit card numbers, and personal information.

File Transfer (FTP, PuTTY, Win SCP):

File Transfer Protocol (FTP), PuTTY, and WinSCP are all file transfer protocols used for transferring files over a network.

FTP is a client-server protocol used for transferring files over the internet. It uses two separate channels: a command channel for sending commands and a data channel for sending data. FTP is commonly used for uploading and downloading files to and from web servers.

PuTTY is a free and open-source terminal emulator and network file transfer application. It supports various network protocols, including SSH (Secure Shell), Telnet, rlogin, and serial connections. PuTTY is primarily used for remote terminal access and file transfers over the network.

WinSCP is a free and open-source SFTP (Secure File Transfer Protocol) and SCP (Secure Copy Protocol) client for Windows. It is used for securely transferring files between local and remote computers over the internet. WinSCP supports various authentication methods, including passwords, public key authentication, and Kerberos.

Overall, FTP, PuTTY, and WinSCP are all useful tools for transferring files over the network. FTP is commonly used for transferring files to and from web servers, while PuTTY and WinSCP are primarily used for remote terminal access and secure file transfers.

Electronic Mail (E-Mail):

a) Electronic mail, commonly known as email, is a method of exchanging digital messages between individuals and organizations over the internet. Email was one of the earliest applications of the internet, and it continues to be one of the most widely used communication methods today.

b) Email messages can contain text, images, and attachments such as files and documents. Email systems typically consist of a mail server, which stores and manages the email messages, and a mail client, which is used by the user to send and receive email messages.

c) Email is based on the Simple Mail Transfer Protocol (SMTP), which is responsible for sending email messages between mail servers, and the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP), which are used by mail clients to retrieve email messages from the mail server.

d) Email can be used for a variety of purposes, including personal and business communication, marketing, and customer support. Email is also widely used for email marketing campaigns, which involve sending promotional messages and advertisements to large numbers of email subscribers.

DNS (Domain Name System):

DNS (Domain Name System) is a system used to translate human-readable domain names into IP addresses, which are used by computers to identify and communicate with each other over the internet.

Every device connected to the internet is assigned an IP address, which is a numerical label used to identify the device on the network. However, IP addresses are not easy to remember, so DNS is used to map domain names to IP addresses. When a user enters a domain name into their web browser, the DNS resolver on their computer sends a query to a DNS server, asking for the IP address associated with that domain name. The DNS server then looks up the IP address in its database and returns it to the DNS resolver, which can then connect to the website using the IP address.

P2P (peer-to-peer) applications are software programs that allow users to share files and resources directly with each other, without the need for a central server or intermediary. In a P2P network, each node (or peer) acts both as a client and a server, allowing files to be shared between users without the need for a dedicated server.

P2P applications

Some of the most common P2P applications include:

a) BitTorrent: a popular file-sharing protocol that allows users to download and share large files, such as movies and music, over the internet.

b) Skype: a communication tool that allows users to make voice and video calls, send instant messages, and share files with other Skype users.

c) Napster: a file-sharing program that was one of the first popular P2P applications, but was shut down due to copyright infringement issues.

d) Bitcoin: a digital currency that uses a P2P network to validate transactions and maintain the blockchain ledger.

e) FileZilla: a file transfer protocol (FTP) client that allows users to upload and download files to and from FTP servers.

P2P applications have both advantages and disadvantages. On the one hand, P2P networks allow users to share files and resources without the need for a central server, which can be more efficient and cost-effective. On the other hand, P2P networks can be used for illegal file sharing and can also be vulnerable to security threats and malware.

Socket programming

Socket programming is a way for applications to communicate with each other over a network using sockets, which are endpoints for sending and receiving data between two or more computers.

Sockets are created by a program and then bound to a network port, allowing other programs to connect to it and communicate with the program. The communication can be either TCP (Transmission Control Protocol) or UDP (User Datagram Protocol), both of which are used for different types of applications.

In socket programming, the program creates a socket and then establishes a connection to another program on the network using the IP address and port number of the other program. Once the connection is established, the two programs can send and receive data between each other.

Socket programming is widely used for a variety of applications, such as web servers, email clients, and file transfer protocols. It provides a flexible and efficient way for applications to communicate over a network, making it an essential part of modern computer networking.

Socket programming can be done in many programming languages, including C, C++, Java, Python, and many more. There are also many libraries and frameworks available that make socket programming easier and more accessible for developers.

Application server concept:

An application server is a type of server that provides a runtime environment for web and enterprise applications. It provides an infrastructure for developing, deploying, and managing web-based applications that can be accessed by multiple users simultaneously over a network.

An application server typically includes software components that are responsible for managing the life cycle of applications, including components for load balancing, session management, security, and database connectivity. These components allow applications to run efficiently and securely, with high availability and scalability.

Application servers are used for developing and deploying a wide range of web and enterprise applications, such as e-commerce websites, banking applications, customer relationship management systems, and supply chain management systems. They are particularly useful for large-scale and complex applications that require high levels of performance, reliability, and security.

Concept of traffic analyzer (MRTG, PRTG, SNMP, Packet tracer, Wireshark).

A traffic analyzer is a tool used to capture and analyze network traffic in order to monitor and manage network performance. It allows network administrators to identify and diagnose network problems, optimize network performance, and ensure the reliability and security of network services.

There are several types of traffic analyzers available, including MRTG, PRTG, SNMP, Packet Tracer, and Wireshark. Each of these tools has its own features and capabilities, but they all provide a way to monitor network traffic and analyze network performance.

a) MRTG (Multi Router Traffic Grapher) is a free and open-source tool that provides a way to monitor the traffic load on network links. It can be used to generate graphs that show the amount of traffic flowing through network links over time.

b) PRTG (Paessler Router Traffic Grapher) is a commercial network monitoring tool that can be used to monitor bandwidth usage, network availability, and network performance. It provides a web-based interface for monitoring and analyzing network traffic and can be used to generate reports and alerts.

c) SNMP (Simple Network Management Protocol) is a protocol that is used to manage and monitor network devices. It provides a way to monitor network performance, track network usage, and diagnose network problems.

d) Packet Tracer is a network simulation tool that is used to design, configure, and troubleshoot network topologies. It provides a way to simulate network traffic and test network configurations before deploying them in a production environment.

e) Wireshark is a free and open-source packet analyzer that is used to capture and analyze network traffic. It provides a way to view network traffic at the packet level, allowing network administrators to diagnose network problems and optimize network performance.

5.6 NETWORK SECURITY

Network Security:

Network security refers to the process of protecting computer networks and their associated infrastructure from unauthorized access, use, modification, or destruction. It involves the use of various technologies, tools, and techniques to safeguard networks and their data from a range of threats, including hackers, malware, viruses, and other malicious attacks.

The primary goal of network security is to ensure the confidentiality, integrity, and availability of network resources and data.

a) Confidentiality refers to the protection of sensitive information from unauthorized access, use, or disclosure.

b) Integrity refers to the accuracy, completeness, and reliability of data,

c) While availability refers to the ability to access network resources and services when needed.

Computer security

Computer security refers to the protection of computer systems, networks, software, and data from unauthorized access, theft, damage, and other types of attacks. It involves the use of various security technologies, protocols, policies, and practices to ensure the confidentiality, integrity, and availability of computer systems and data.

The goal of computer security is to prevent or mitigate the impact of security breaches, such as data theft, malware infections, hacking attacks, and other types of cyber threats. Effective computer security requires a multi-layered approach that addresses various aspects of security, including physical security, network security, application security, information security, operational security, and disaster recovery and business continuity planning

Computer security can be broadly classified into several types based on the aspect of security being addressed. Some of the commonly recognized types of computer security are:

a) Physical security: This type of security is concerned with the physical protection of hardware, software, and data from unauthorized access, theft, or damage. Examples of physical security measures include security guards, access control systems, video surveillance, and fire suppression systems.

b) Network security: Network security involves the protection of network infrastructure and communication systems from unauthorized access, misuse, or attack. This includes technologies like firewalls, intrusion detection systems, and virtual private networks (VPNs).

c) Application security: Application security focuses on the protection of software applications from external and internal threats, including malicious code, malware, and hacking attacks. This type of security is typically implemented using secure coding practices, software testing, and vulnerability scanning.

d) Information security: Information security refers to the protection of data from unauthorized access, disclosure, alteration, or destruction. This includes the use of encryption, access control, and other security technologies to safeguard data at rest and in transit.

Types of Security Attack:

There are several types of security attacks that can compromise the security of computer systems, networks, and data. Some of the most common types of security attacks include:

a) Malware attacks: Malware is malicious software that is designed to disrupt, damage, or gain unauthorized access to computer systems and data. Examples of malware include viruses, worms, Trojans, and ransomware.

b) Phishing attacks: Phishing is a type of social engineering attack that involves tricking users into revealing sensitive information or downloading malicious software by posing as a legitimate entity. Phishing attacks are usually carried out through email or other forms of electronic communication.

c) Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks: These attacks are designed to overwhelm a computer system, network, or server with traffic, making it unavailable to legitimate users.

d) Password attacks: Password attacks involve attempting to guess or steal user passwords to gain unauthorized access to computer systems and data. Examples of password attacks include brute-force attacks, dictionary attacks, and phishing attacks.

e) Man-in-the-middle (MitM) attacks: MitM attacks involve intercepting communication between two parties in order to eavesdrop, steal information, or modify the communication.

f) SQL injection attacks: SQL injection attacks are a type of web application attack that involves exploiting vulnerabilities in web applications to gain unauthorized access to data stored in a back-end database.

g) Cross-site scripting (XSS) attacks: XSS attacks are a type of web application attack that involves injecting malicious code into a web page, which is then executed by users who visit the page.

Principles of Cryptography:

Cryptography is the practice of securing communication and data from unauthorized access or modification by transforming it into an unreadable format. The following are some of the principles of cryptography:

a) Confidentiality: This principle ensures that the information is accessible only to authorized users or entities. The information is encrypted or scrambled using a secret key or algorithm, which only the authorized users or entities can access.

b) Integrity: This principle ensures that the information is not altered or modified during transmission. Cryptographic algorithms are used to detect any unauthorized modification of the information.

c) Authentication: This principle ensures that the identities of the communicating parties are verified. Cryptography is used to ensure that the parties are who they claim to be, and that the data being transmitted is authentic.

d) Non-repudiation: This principle ensures that the sender cannot deny having sent a message or data. Cryptography is used to provide digital signatures, which can be used to prove the authenticity of the data and the sender.

e) Availability: This principle ensures that the information is available to authorized users when they need it. Cryptography can be used to provide access controls, which ensure that only authorized users can access the information.

f) Overall, the principles of cryptography provide a framework for securing communication and data, and they are essential to ensuring the confidentiality, integrity, authenticity, non-repudiation, and availability of information.

The RSA algorithm

The RSA algorithm is a widely used encryption algorithm for secure data transmission over the internet. It is named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman.

The RSA algorithm is based on the mathematical concept of prime factorization. It works by using two large prime numbers and combining them in a way that makes it difficult for anyone to determine the original numbers. This combination produces a public key and a private key.

The public key can be shared with anyone who wants to send encrypted data to the recipient, while the private key is kept secret by the recipient for decryption of the data.

To use the RSA algorithm for encryption, the sender encrypts the data using the recipient's public key. The recipient can then use their private key to decrypt the data. This process ensures that only the recipient can decrypt the data, as they are the only one with access to the private key.

The following are the steps involved in the RSA algorithm:

a) **Key generation:**
The first step in the RSA algorithm is to generate a public key and a private key. This is done by selecting two large prime numbers, p and q, and multiplying them together to get n. The value of n is used to generate the public and private keys.

b) **Public key distribution:**
The public key is then made available to anyone who needs to send an encrypted message to the owner of the private key.

c) **Encryption:**
To encrypt a message using RSA, the message is first converted into a numerical value. The sender then uses the recipient's public key to encrypt the numerical value.

d) **Decryption:**
To decrypt the encrypted message, the recipient uses their private key. The recipient converts the encrypted numerical value back into the original message.

e) **Signing:**
In addition to encryption, the RSA algorithm can also be used for digital signatures. A digital signature is created by using the sender's private key to encrypt a message, and the recipient can verify the signature using the sender's public key.

f) **Verification:**
To verify the signature, the recipient uses the sender's public key to decrypt the signature. If the decrypted signature matches the original message, then the signature is valid.

Digital Signature:

A digital signature is a mathematical technique used to validate the authenticity and integrity of digital messages or documents. It provides a way to verify that a message or document was created by a particular person or entity, and that it has not been tampered with or altered since it was signed.

Digital signatures are created using public key cryptography, where the person or entity creating the signature uses their private key to encrypt a hash of the message or document. The recipient can then use the sender's public key to decrypt the signature and verify that the message or document has not been tampered with and was in fact sent by the claimed sender.

Digital signatures are commonly used in electronic transactions, online contracts, and other digital documents where authenticity and integrity are important. They provide a way to establish trust between parties and ensure that digital messages and documents are secure and reliable.

The main features of digital signatures are:

a) Authentication: Digital signatures provide a way to verify the identity of the signer and ensure that the message or document was not tampered with during transmission.

b) Integrity: Digital signatures provide assurance that the message or document has not been modified in any way since it was signed.

c) Non-repudiation: Digital signatures provide proof that the sender cannot deny having sent the message or document.

d) Security: Digital signatures use encryption to protect the signature and ensure that only the intended recipient can read it.

e) Efficiency: Digital signatures can be applied quickly and easily to large volumes of documents, making them a more efficient way to manage document signing and verification.

Securing e-mail (PGP):

PGP (Pretty Good Privacy) is a software program that provides encryption and digital signature capabilities for email and other electronic communications. It allows users to encrypt the content of their email messages so that only the intended recipient can read them, and also provides a way to digitally sign messages to ensure their authenticity.

The PGP encryption process involves generating a public key and a private key for each user. The public key can be shared with anyone who wants to send an encrypted message, while the private key is kept secret and only used by the owner of the key to decrypt messages that have been encrypted with their public key. To send an encrypted email message, the sender would use the recipient's public key to encrypt the message, and then send the encrypted message through regular email channels. The recipient would then use their private key to decrypt the message and read its contents.

Securing TCP connections (SSL)

SSL (Secure Sockets Layer) is a protocol used to secure communications over the internet by encrypting data transferred between two systems. It is used to establish secure connections between web browsers and servers, email clients and servers, and other types of applications that require secure communication.

When a connection is made between a client and server, the SSL protocol is used to negotiate a secure connection, which involves establishing a set of shared cryptographic keys that are used to encrypt and decrypt data. This process is commonly referred to as the SSL handshake.

During the SSL handshake, the server presents a digital certificate to the client, which contains information about the server's identity and public key. The client verifies the certificate, and if it is trusted, generates a session key that is used to encrypt and decrypt data transmitted during the session.

Once the secure connection is established, all data transmitted between the client and server is encrypted, which provides protection against eavesdropping and other forms of cyber-attacks.

Network layer security (IPsec, VPN):

Network layer security involves securing communication at the network layer (layer 3) of the OSI model. IPsec and VPN are two common technologies used for network layer security.

IPsec (Internet Protocol Security) is a protocol suite used for securing internet protocol (IP) communications. It provides security services, such as authentication, encryption, and data integrity, to protect network traffic. IPsec can be used to secure communication between two systems or between a remote user and a network.

A Virtual Private Network (VPN) is a secure connection between two or more devices or networks over the internet. VPNs can be used to securely connect a remote worker to a corporate network or to create a secure connection between two networks. VPNs typically use encryption to ensure the confidentiality of data transmitted over the internet.

IPsec and VPNs can be used together to provide comprehensive network layer security. IPsec provides security for individual network connections, while VPNs provide a secure connection between two networks or devices. This combination of technologies can be used to provide secure remote access to a corporate network, secure communication between two networks, or to provide a secure connection between devices in a distributed network.

Securing wireless LANs (WEP):

Wired Equivalent Privacy (WEP) is a security protocol used to protect wireless networks. It was introduced in 1999 as part of the original 802.11 wireless network standard.

WEP uses a shared secret key to encrypt data transmitted between wireless devices. The key can be 64 bits or 128 bits in length. WEP encryption can provide a basic level of security for wireless networks, but it is not considered a strong security solution.

WEP has several vulnerabilities that make it relatively easy for attackers to bypass its security features. For example, WEP keys can be easily cracked using widely available software tools. WEP also has weaknesses in its initialization vector (IV) generation process, which makes it vulnerable to certain types of attacks.

Due to its weaknesses, WEP has been largely replaced by newer and more secure wireless security protocols such as Wi-Fi Protected Access (WPA) and WPA2. These protocols use stronger encryption algorithms and provide better security features than WEP. It is highly recommended to use the latest security protocols and to keep wireless network hardware and software updated with the latest security patches to ensure a secure wireless network.

Firewalls:

A firewall is a security device or software that is designed to monitor and control network traffic to and from an organization's network. The main purpose of a firewall is to protect the network from unauthorized access and to prevent malicious traffic from entering the network.

Firewalls can be hardware or software-based, and they typically work by examining packets of data as they pass through the network. They use a set of predefined rules to determine whether a packet should be allowed to pass through the network or be blocked.

There are several types of firewalls that are commonly used in network security. These include:

a) **Packet-filtering firewalls:** These are the simplest and most basic type of firewall. They work by examining each packet of data that passes through the network and determining whether to allow or block the packet based on a set of predefined rules.

b) **Stateful inspection firewalls:** These firewalls are more advanced than packet-filtering firewalls. They not only examine each packet of data but also keep track of the state of network connections. This allows them to identify and block suspicious traffic that may be part of a larger attack.

c) **Application-level gateways:** These firewalls operate at the application layer of the network and are designed to monitor specific types of traffic, such as email or web traffic. They are often used in conjunction with other types of firewalls to provide additional layers of protection.

d) **Circuit-level gateways:** These firewalls operate at the transport layer of the network and are designed to monitor the flow of traffic between two hosts. They are often used in conjunction with other types of firewalls to provide additional layers of protection.

e) **Next-generation firewalls:** These are advanced firewalls that combine several different types of firewall technologies and security features. They are designed to provide a high level of security and are often used in large enterprise environments.

MULTIPLE CHOICE QUESTIONS

1. **_____ is not true in case of OSI and TCP/IP model.**
   A. The OSI Model is a logical and conceptual model that defines how communication needs to be done
   B. TCP/IP model depends on standard protocols that assigns the network of hosts over the Internet.
   C. Both OSI and TCP/IP models are protocol independent
   D. None of these

2. **A computer has just been installed on the Ethernet LAN but it is not communicating with the network, then what should be done at first?**
   A. Update the NIC driver
   B. Verify the IP address configuration on the workstation
   C. Verify the connectivity on the computer's network card
   D. All of the above

3. **Which of the following commands is not used in the troubleshooting of computer networks?**
   A. Ping B. Tracert
   C. Ipconfig D. Chkdsk

4. **In network troubleshooting, which of the following commands is used?**
   A. Netstat B. Nslookup
   C. Tracert D. All of the above

5. **Which server maintains a directory of domain names and translate them to Internet Protocol (IP) addresses.**
   A. DNS Server
   B. DHCP Server
   C. Web Server
   D. Database Server

6. **Which data link sub-layer carries out data link functions that depend upon the type of medium?**
   A. Logical link control
   B. Media access control
   C. Network interface control
   D. Error Control

7. **When connected to the Internet, the device used to perform modulation and demodulation is called**
   A. Trans receiver B. Modem
   C. Repeater D. All of the above

8. **An web-site is a collection of**
   A. Components of internet
   B. Web-pages
   C. Web links
   D. All of the above

9. **In web applications, _____ is the correct order to form URLs.**
   A. Protocol name, File name, DNS name
   B. DNS name, Protocol name, File name
   C. Protocol name, DNS name, File name
   D. Protocol name, File name, DNS name

10. **In computer networking, MAN lies in between LAN and WAN in terms of**
    A. Area coverage
    B. Data transfer rate
    C. Both of the above
    D. None of these