**CS3591-COMPUTER NETWORKS**

**PART-C(15 MARKS)**

**UNIT-I INTRODUCTION AND APPLICATION LAYER**

**1.Explain the TCP/IP reference model with neat diagram.**

**TCP/IP Reference Model with Diagram:**

The TCP/IP (Transmission Control Protocol / Internet Protocol) reference model is a set of communication protocols used for the internet and other similar networks. It is the foundation of the modern internet and networking, ensuring data transmission between devices.

The TCP/IP model has four layers:

1. **Application Layer:**
   * Function: This is the highest layer of the TCP/IP model. It directly interacts with the end-user applications and provides protocols that allow software to communicate over the network.
   * Protocols:
     + HTTP (HyperText Transfer Protocol)
     + FTP (File Transfer Protocol)
     + SMTP (Simple Mail Transfer Protocol)
     + DNS (Domain Name System)
   * Services:
     + Email services, file transfer, web browsing, etc.
2. **Transport Layer:**
   * Function: This layer is responsible for end-to-end communication, error handling, and data flow control. It ensures reliable data transfer between host systems.
   * Protocols:
     + TCP (Transmission Control Protocol): Provides reliable, connection-oriented communication.
     + UDP (User Datagram Protocol): Provides faster, connectionless communication but without reliability.
   * Services:
     + Segmentation and reassembly of data packets.
     + Flow control and error detection.
3. **Internet Layer:**
   * Function: This layer is responsible for logical addressing and routing of data packets. It ensures that data packets can travel across networks, regardless of the underlying physical hardware.
   * Protocols:
     + IP (Internet Protocol): Responsible for logical addressing and routing.
     + ICMP (Internet Control Message Protocol): Used for network diagnostic functions like ping.
     + ARP (Address Resolution Protocol): Resolves IP addresses to MAC addresses.
   * Services:
     + Routing of packets from source to destination.
     + Addressing and packet forwarding.
4. **Network Access Layer:**
   * Function: This layer is responsible for the physical transmission of data over the network. It deals with hardware addressing and the actual movement of data through the network infrastructure.
   * Protocols:
     + Ethernet
     + Wi-Fi
     + PPP (Point-to-Point Protocol)
   * Services:
     + Data link and physical transmission of packets.
     + Error detection and physical addressing.

**Diagram of the TCP/IP Model:**

+---------------------------+

| Application Layer | <--- Application Layer

+---------------------------+

| Transport Layer | <--- Transport Layer

+---------------------------+

| Internet Layer | <--- Internet Layer

+---------------------------+

| Network Access Layer | <--- Network Access Layer

+---------------------------+

**2. What is the OSI Model? Explain the Functions, Protocols, and Services of Each Layer.**

The **OSI (Open Systems Interconnection) Model** is a conceptual framework used to understand and design a networking system by dividing it into seven different layers. Each layer performs a specific set of functions and uses various protocols to enable communication between devices.

**7 Layers of the OSI Model:**

1. **Application Layer (Layer 7):**
   * **Function:** Provides network services directly to end-user applications. It enables applications to communicate over the network.
   * **Protocols:**
     + HTTP (Hypertext Transfer Protocol)
     + FTP (File Transfer Protocol)
     + SMTP (Simple Mail Transfer Protocol)
     + DNS (Domain Name System)
   * **Services:**
     + File transfer, email services, web browsing, etc.
2. **Presentation Layer (Layer 6):**
   * **Function:** Translates, encrypts, and compresses data between the application and transport layers. It ensures data is in a readable format for the application layer.
   * **Protocols:**
     + SSL/TLS (Secure Sockets Layer / Transport Layer Security)
     + JPEG, GIF (Image compression standards)
   * **Services:**
     + Data translation (e.g., converting EBCDIC to ASCII), encryption, compression.
3. **Session Layer (Layer 5):**
   * **Function:** Manages sessions between applications. It establishes, maintains, and terminates communication sessions between two devices.
   * **Protocols:**
     + NetBIOS (Network Basic Input Output System)
     + RPC (Remote Procedure Call)
   * **Services:**
     + Session establishment, synchronization, and termination.
4. **Transport Layer (Layer 4):**
   * **Function:** Ensures reliable data transfer between two systems. It manages flow control, error correction, and retransmission of lost data.
   * **Protocols:**
     + TCP (Transmission Control Protocol) - Reliable, connection-oriented.
     + UDP (User Datagram Protocol) - Connectionless, fast but unreliable.
   * **Services:**
     + Data segmentation and reassembly, error detection, flow control.
5. **Network Layer (Layer 3):**
   * **Function:** Responsible for routing data between devices across different networks and logical addressing (IP addressing).
   * **Protocols:**
     + IP (Internet Protocol)
     + ICMP (Internet Control Message Protocol)
     + ARP (Address Resolution Protocol)
   * **Services:**
     + Routing, addressing, packet forwarding.
6. **Data Link Layer (Layer 2):**
   * **Function:** Provides error detection and correction in the data transfer process. It also handles physical addressing (MAC addresses).
   * **Protocols:**
     + Ethernet, PPP (Point-to-Point Protocol), Wi-Fi
   * **Services:**
     + Frame delivery, error detection, flow control, MAC addressing.
7. **Physical Layer (Layer 1):**
   * **Function:** Transmits raw data bits over the physical medium (such as electrical signals over cables or wireless signals).
   * **Protocols:**
     + Ethernet, Fiber optics, Wi-Fi, Bluetooth
   * **Services:**
     + Transmission of data bits over physical medium, bit synchronization.

**Diagram of the OSI Model:**

+-------------------+

| Application | <--- Layer 7

+-------------------+

| Presentation | <--- Layer 6

+-------------------+

| Session | <--- Layer 5

+-------------------+

| Transport | <--- Layer 4

+-------------------+

| Network | <--- Layer 3

+-------------------+

| Data Link | <--- Layer 2

+-------------------+

| Physical | <--- Layer 1

+-------------------+

**3. Different Types of Transmission Media in Computer Networks**

Transmission media refers to the physical pathways or channels through which data travels from the source to the destination in a network. It can be categorized into two types: **Guided media** (wired) and **Unguided media** (wireless).

**1. Guided Media (Wired):**

These are physical transmission paths that guide the data along a specific route.

* **Twisted Pair Cable:**
  + **Description:** Consists of pairs of insulated copper wires twisted together to reduce electromagnetic interference.
  + **Types:**
    - **Unshielded Twisted Pair (UTP):** Commonly used in local area networks (LANs) and telephone lines.
    - **Shielded Twisted Pair (STP):** Has shielding to protect against electromagnetic interference, used in high-interference areas.
  + **Data Rate & Distance:** UTP can transmit up to 1Gbps over distances of up to 100 meters.
  + **Advantages:** Inexpensive and easy to install.
  + **Disadvantages:** Prone to interference, lower data rates compared to other media.
* **Coaxial Cable:**
  + **Description:** Consists of a central core wire (usually copper), an insulating layer, a metallic shield, and an outer insulating layer.
  + **Uses:** Traditionally used for cable television, Ethernet networks (in the form of 10BASE2 and 10BASE5).
  + **Data Rate & Distance:** Supports higher speeds (up to 10Gbps) and longer distances than twisted pair cables.
  + **Advantages:** More resistant to electromagnetic interference compared to twisted pair cables.
  + **Disadvantages:** Bulkier, less flexible.
* **Fiber Optic Cable:**
  + **Description:** Transmits data as light pulses through glass or plastic fibers.
  + **Uses:** High-speed, long-distance communication like internet backbone connections and high-performance computing.
  + **Data Rate & Distance:** Can transmit data at speeds up to 100Gbps and over distances up to hundreds of kilometers.
  + **Advantages:** Very high bandwidth, immune to electromagnetic interference, secure.
  + **Disadvantages:** Expensive, installation is more complex.

**2. Unguided Media (Wireless):**

These do not require any physical medium to transmit data. Instead, they rely on electromagnetic waves to propagate through the air.

* **Radio Waves:**
  + **Description:** Used for mobile communication, Wi-Fi, and broadcasting.
  + **Frequency Range:** From 3 kHz to 300 GHz.
  + **Advantages:** Long-range communication, good for broadcasting.
  + **Disadvantages:** Limited bandwidth, subject to interference from weather or other signals.
* **Microwaves:**
  + **Description:** Used for point-to-point communication over long distances.
  + **Frequency Range:** Typically from 1 GHz to 300 GHz.
  + **Uses:** Satellite communication, Wi-Fi networks.
  + **Advantages:** Can carry large amounts of data over long distances.
  + **Disadvantages:** Requires line-of-sight, affected by weather conditions.
* **Infrared (IR):**
  + **Description:** Uses light waves to transmit data between devices over short distances.
  + **Uses:** Remote controls, wireless keyboards, and mice.
  + **Advantages:** Simple and inexpensive.
  + **Disadvantages:** Limited range, cannot pass through walls or other obstructions.
* **Microwave Transmission (Satellite):**
  + **Description:** Uses microwaves for long-distance transmission, primarily for satellite communication.
  + **Advantages:** Provides long-range communication, especially in remote areas.
  + **Disadvantages:** High latency, expensive.

**UNIT-II TRANSPORT LAYER**

PART-C(15 Marks)

**1.Explain the functions of MAC layer present in IEEE 802.11 with necessary diagrams**

**1. Functions of MAC Layer in IEEE 802.11 with Necessary Diagrams**

The MAC (Medium Access Control) layer in the IEEE 802.11 standard is responsible for regulating access to the shared wireless medium. The MAC layer ensures efficient, reliable communication between devices in a wireless local area network (WLAN). It manages access to the wireless channel, frame transmission, and addressing.

**Functions of the MAC Layer in IEEE 802.11:**

1. ***Channel Access:***
   * The MAC layer controls how devices access the wireless medium to prevent collisions and ensure efficient data transmission. It uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) as the access method.
   * CSMA/CA works by listening to the channel before transmitting. If the channel is busy, the device waits until the channel is clear. This method reduces the chance of collision compared to CSMA/CD (used in Ethernet).
2. ***Frame Delimitation:***
   * The MAC layer defines the format of frames that are transmitted over the wireless medium. Each frame consists of several fields, including the header, payload, and trailer, which contain information such as addresses, control information, and error-checking data.
   * The basic frame structure includes:
     + MAC Header: Contains addresses (source and destination) and control information.
     + Payload: Contains the actual data being transmitted.
     + FCS (Frame Check Sequence): Used for error detection.
3. ***Collision Avoidance:***
   * As wireless communication is prone to collisions due to the shared medium, the MAC layer uses mechanisms such as RTS/CTS (Request to Send / Clear to Send) to avoid collisions caused by hidden nodes. If the sender wants to transmit data, it first sends an RTS message to the receiver. If the receiver is ready, it responds with a CTS message. Other devices in the vicinity will defer transmission, reducing the chance of collision.
4. ***Acknowledgment (ACK):***
   * After receiving a frame, the receiver sends an acknowledgment (ACK) to confirm successful reception. If the sender does not receive an ACK, it will retransmit the data.
   * This mechanism ensures reliability in communication.
5. ***Power Management:***
   * The MAC layer allows devices to conserve power by enabling them to go into a low-power mode when they are not actively transmitting or receiving data.
   * This is particularly important for battery-operated devices like laptops and smartphones.
6. ***Quality of Service (QoS):***
   * The MAC layer in IEEE 802.11 supports Quality of Service mechanisms, allowing prioritization of traffic. This is important for applications like VoIP (Voice over IP), video conferencing, or gaming that require low latency and higher bandwidth.

**MAC Frame Structure in IEEE 802.11:**

+-------------------+-------------------+------------------+------------------+------------------+------------------+

| Frame Control | Duration/ID | Address 1 | Address 2 | Address 3 | Sequence Control |

+-------------------+-------------------+------------------+------------------+------------------+------------------+

| Address 4 (optional) | Frame Body | Frame Check Sequence (FCS) |

+------------------------+----------------------------------------+

* Frame Control: Defines the type of frame (Data, RTS, CTS, ACK, etc.) and the protocol version.
* Duration/ID: Specifies the time duration or a unique identifier for a particular frame.
* Addresses: Source and destination addresses; in the case of a basic 802.11 frame, it involves addresses for the sender, receiver, and access point (if applicable).
* Frame Body: Contains the data or control information.
* FCS: A checksum that detects errors in the frame during transmission.

**Diagram: IEEE 802.11 MAC Frame Structure**

+-------------------+-------------------+------------------+------------------+

| Frame Control | Duration/ID | Address 1 | Address 2 |

+-------------------+-------------------+------------------+------------------+

| Address 3 | Sequence Control | Address 4 | Frame Body |

+-------------------+-------------------+------------------+------------------+

| FCS (Frame Check Sequence) |

+---------------------------------------------------------------------+

**2.Discuss in detail about the Bit- oriented Protocols.**

**Bit-Oriented Protocols:**

Bit-oriented protocols are communication protocols where the data is transmitted as a continuous stream of bits rather than in fixed-length frames. These protocols are widely used for efficient and flexible communication, especially in environments where the overhead of frame-based protocols is not desirable.

**Key Features of Bit-Oriented Protocols:**

1. **Bit-level Control:**
   * These protocols provide control over the bit stream, meaning that the sender and receiver can manipulate bits directly, without predefined frame boundaries.
2. **Framing and Data Link Layer Management:**
   * Bit-oriented protocols need to define methods for identifying the start and end of the data. Special characters or sequences of bits are often used to signal the beginning and end of a message (for example, flags, or bit stuffing).
3. **Efficiency:**
   * As bit-oriented protocols do not require headers or large data units, they are typically more efficient in terms of bandwidth utilization than byte-oriented protocols, particularly for high-speed or low-latency communication.
4. **Error Detection and Correction:**
   * These protocols often incorporate error detection techniques like Cyclic Redundancy Check (CRC) to ensure reliable communication by detecting and possibly correcting errors in the bit stream.

**Common Bit-Oriented Protocols:**

1. **HDLC (High-Level Data Link Control):**
   * HDLC is a bit-oriented protocol used for point-to-point and point-to-multipoint communication.
   * It uses a flag (01111110) to mark the beginning and end of a frame.
   * It incorporates bit stuffing, which involves adding extra bits to avoid the flag pattern appearing within the frame.
2. **SDLC (Synchronous Data Link Control):**
   * A predecessor to HDLC, it also uses a bit-oriented frame format for communication over synchronous links.
3. **PPP (Point-to-Point Protocol):**
   * While PPP is primarily byte-oriented, it uses a form of bit-level framing (using flag sequences and escaping bytes) in certain instances for efficient communication.

**Diagram of Bit-Oriented Protocol (HDLC Frame):**

+-------------------+-------------------+-------------------+-----------------+

| Flag (01111110) | Address | Control | Data |

+-------------------+-------------------+-------------------+-----------------+

| FCS (CRC) | Flag (01111110) |

+-------------------+-------------------+-------------------+-----------------+

* Flag: Marks the start and end of the frame.
* Address: Specifies the address of the recipient.
* Control: Defines the control information for managing communication.
* Data: Contains the payload being transmitted.
* FCS (Frame Check Sequence): CRC-based error detection field.

**3.How frame order and flow control is achieved using the data link layer? (May 14)**

**Frame Order and Flow Control in Data Link Layer**

Frame order and flow control are essential mechanisms for ensuring efficient, reliable communication between devices in a network. The data link layer is responsible for handling these aspects, ensuring that data is delivered in order and that devices do not overwhelm each other with too much data at once.

**Frame Ordering:**

* Frame ordering ensures that the sequence of frames is maintained during transmission. In some protocols, such as TCP (which operates at the transport layer), the frames are numbered to ensure that they can be reordered at the receiver if they arrive out of order.
* Data Link Layer ensures that the frames are transmitted in a manner that avoids errors due to lost or misordered frames. The order is important in protocols that require a continuous stream of data (e.g., video or audio streams).

**Flow Control:**

* Flow control prevents a sender from overwhelming a receiver with data faster than it can process. The data link layer uses flow control techniques to manage data transmission between devices.

**Types of Flow Control:**

1. Stop-and-Wait:
   * The sender sends one frame and waits for an acknowledgment from the receiver before sending the next frame.
   * This method is simple but can be inefficient, as the sender must wait for each frame to be acknowledged.
2. Sliding Window Protocol:
   * More efficient than stop-and-wait, the sliding window protocol allows the sender to send multiple frames before waiting for an acknowledgment.
   * The receiver can control the flow by providing the window size, which determines how many frames the sender can send without receiving an acknowledgment.
   * Window Size: Determines how many frames can be in transit before requiring acknowledgment.
   * Flow Control Mechanism: The receiver sends back a "window size" field, which tells the sender how many frames can be sent without waiting for an acknowledgment.

**Diagram of Sliding Window Flow Control:**

Sender: [ Frame 1 | Frame 2 | Frame 3 ] ----> Receiver: [ ACK 1 | ACK 2 | ACK 3 ]

Window Size: 3

* The sender can send 3 frames before waiting for an acknowledgment.
* The receiver sends an acknowledgment for the first frame (ACK 1), and the sender can then send more frames.

**Frame Order in Data Link Layer:**

* Data link layer protocols like HDLC and PPP can use sequence numbers to maintain the order of frames.
* In protocols where retransmission of frames occurs (like ARQ (Automatic Repeat reQuest)), sequence numbers are used to identify frames and ensure they are processed in the correct order.

**UNIT-III NETWORK LAYER**

PART-C(15 Marks)

**1.Explain Multicast Routing features and explain DVMRP(Nov 15)**

**Multicast Routing Features:**

Multicast routing refers to the method used for transmitting a message to multiple receivers (group communication) efficiently. It is used to send data to multiple recipients simultaneously without duplicating the data for each recipient.

Key features of **Multicast Routing** include:

1. **Efficient Use of Bandwidth:**
   * Multicast routing sends a single copy of data across a network and replicates it only when necessary. This is much more efficient than broadcasting data to every single host on the network, which wastes bandwidth.
2. **Group Communication:**
   * Multicast routing allows for group communication, where a sender sends data to a specific group of receivers (identified by a multicast IP address). This is ideal for applications like live video streaming, conference calls, and online gaming.
3. **Scalability:**
   * Multicast routing is scalable, as it allows a large number of receivers to join a multicast group without requiring separate streams from the sender for each receiver. The data travels only to the routers on the path to the multicast group members.
4. **Multicast Groups:**
   * A multicast group is identified by a specific **Multicast IP Address** in the range **224.0.0.0 to 233.255.255.255**. Receivers that want to receive the multicast traffic must join the group.
5. **Routing Protocols:**
   * Multicast routing requires special protocols designed for multicast delivery. Some of these protocols include:
     + **DVMRP (Distance Vector Multicast Routing Protocol)**
     + **PIM (Protocol Independent Multicast)**
     + **MOSPF (Multicast Open Shortest Path First)**
6. **Reverse Path Forwarding (RPF):**
   * Multicast routing uses **RPF** to ensure that packets are forwarded along the reverse path from the source. It helps prevent loops and ensures that multicast packets are forwarded efficiently.

**DVMRP (Distance Vector Multicast Routing Protocol):**

**DVMRP** is a **distance-vector protocol** for multicast routing that is based on the routing algorithm used by the RIP protocol (RIP's distance-vector routing). It is used to manage multicast groups and deliver multicast traffic efficiently across the network.

**Key Features of DVMRP:**

1. **Flood and Prune Mechanism:**
   * DVMRP uses a **flood-and-prune** mechanism to determine the best path for sending multicast data. Initially, all multicast packets are flooded throughout the network. The routers then "prune" the paths that are not part of the multicast group, ensuring that only the routers that need the data will receive it.
2. **Reverse Path Forwarding (RPF):**
   * DVMRP uses RPF to prevent routing loops and ensure that packets follow the most efficient path based on the source's IP address. It ensures that multicast traffic is forwarded only along the path that would be used to reach the source.
3. **Multicast Tree Construction:**
   * DVMRP constructs a **Source-Specific Multicast Tree (SSM)** for each multicast group. It builds a tree for each source, making it efficient to deliver data to multiple receivers.
4. **Routing Table Updates:**
   * DVMRP routers periodically exchange routing updates to maintain and update their multicast routing tables. These updates contain information about the multicast sources, the path to reach them, and the routers that need to forward the multicast traffic.
5. **Compatibility with RIP:**
   * DVMRP is based on the same principles as RIP, which means it is relatively easy to implement in existing RIP-based networks. However, it is less scalable than other multicast routing protocols like PIM.
6. **Pruning of Non-Interest Routers:**
   * If a router does not have any multicast receivers for a particular group, it sends a prune message to stop forwarding the multicast traffic for that group. This pruning mechanism ensures that unnecessary multicast traffic does not traverse the entire network.

**Diagram of DVMRP:**

[Source]

|

[Router1] -----> [Router2] -----> [Receiver1]

| |

[Router3] -------------> [Receiver2]

|

[Receiver3]

* **Flooding**: Initially, multicast data is flooded across the network.
* **Pruning**: Routers that do not have any receivers prune their paths to stop receiving the multicast traffic.
* **RPF**: Ensures that the multicast traffic follows the optimal path to each receiver.

**2.Explain the working of Protocol Independent Multicast (PIM) in detail. (May 17)**

**Protocol Independent Multicast (PIM)** is a family of multicast routing protocols that allows the forwarding of multicast traffic without relying on a specific unicast routing protocol. It is designed to work in both **dense** and **sparse** networks and is independent of the unicast routing protocols (such as OSPF, RIP, or BGP) in use.

**Key Features of PIM:**

1. **Protocol Independence:**
   * PIM is independent of the unicast routing protocol, which means it can work with any unicast routing protocol (e.g., OSPF, RIP, BGP). It uses the unicast routing table for routing multicast packets, allowing PIM to be deployed in various network topologies.
2. **Two Modes of Operation:**
   * PIM has two major operating modes: **PIM Sparse Mode (PIM-SM)** and **PIM Dense Mode (PIM-DM)**.
   * **PIM Sparse Mode (PIM-SM):**
     + Used in networks with sparse receivers (i.e., receivers are spread out over the network). It requires a **Rendezvous Point (RP)**, a central point where multicast sources and receivers join the multicast distribution tree.
     + Multicast traffic is only forwarded to routers that have requested the data via an **explicit join** to the RP.
     + After the join, the source’s data is forwarded through a shared multicast tree rooted at the RP.
   * **PIM Dense Mode (PIM-DM):**
     + Used in networks with many receivers (i.e., dense networks). It is a **flood-and-prune** mechanism similar to DVMRP. All routers in the network receive multicast traffic by default, and routers that don’t have receivers **prune** their paths to avoid unnecessary traffic.
3. **Rendezvous Point (RP):**
   * In **PIM-SM**, the RP is a central point where multicast sources and receivers meet. The RP receives multicast traffic from sources and forwards it to receivers. The RP simplifies the multicast routing decision process.
   * Routers that need to receive multicast traffic send a **Join message** to the RP. The RP then sends the data through a shared multicast tree.
4. **Multicast Distribution Trees:**
   * PIM builds two types of trees:
     + **Shared Tree**: In **PIM-SM**, the multicast traffic initially flows through a shared tree rooted at the RP.
     + **Source Tree**: Once a receiver joins a multicast group, the router may switch to a source-specific tree (known as an **SPT**) to improve efficiency.
5. **Forwarding:**
   * Once the multicast group membership is established and the tree is built, routers forward multicast traffic along the tree. PIM uses the unicast routing table to forward multicast packets along the path from the source to the receivers.

**Diagram of PIM-Sparse Mode:**

less

Copy

[Source] -----> [RP] -----> [Router1] -----> [Receiver1]

|

[Router2] -----> [Receiver2]

|

[Router3] -----> [Receiver3]

* **PIM-SM Process:**
  1. Source sends multicast traffic to the RP.
  2. Routers that need the multicast traffic join the shared tree at the RP.
  3. Once receivers are joined, traffic is forwarded to them.

**Advantages of PIM:**

* **Scalability**: PIM is scalable and can handle large networks with many receivers.
* **Flexibility**: It works in both dense and sparse networks, making it suitable for various topologies.

**4. i) Explain IPv4 classful and classless addressing. (10) (Nov 19) ii) Assume that you are given a network ID 165.121.0.0. You are responsible for creating subnets on the network and each subnet must provide at least 900 host IDs. What subnet mask meets the requirement for the minimum number of host IDs and provide the greatest number of subnets ?**

**Classful Addressing:**

IPv4 classful addressing divides IP addresses into classes based on the first few bits of the address. The classes are:

* **Class A** (1.0.0.0 - 127.255.255.255): Supports 128 networks, each with up to 16 million hosts.
* **Class B** (128.0.0.0 - 191.255.255.255): Supports 16,384 networks, each with up to 65,000 hosts.
* **Class C** (192.0.0.0 - 223.255.255.255): Supports 2 million networks, each with up to 254 hosts.
* **Class D** (224.0.0.0 - 239.255.255.255): Used for multicast addresses.
* **Class E** (240.0.0.0 - 255.255.255.255): Reserved for future use.

**Classless Addressing (CIDR):**

Classless Inter-Domain Routing (CIDR) eliminates the fixed boundaries of classful addressing and allows for more flexible IP address allocation. CIDR uses a **prefix length** to indicate the number of bits used for the network portion of the address, written in the format **IP address/Prefix length** (e.g., 192.168.1.0/24).

**ii) Subnetting a Network (5 Marks)**

Given the network ID **165.121.0.0** and the requirement that each subnet must provide at least **900 host IDs**, we can calculate the subnet mask as follows:

* To accommodate **900 hosts**, we need at least **10 bits** for the host portion, since 210−2=1024−2=9002^{10} - 2 = 1024 - 2 = 900210−2=1024−2=900 (subtracting 2 for the network and broadcast addresses).
* The original network is **165.121.0.0** (Class B), with a default subnet mask of **255.255.0.0** or **/16**.
* To create subnets that accommodate at least 900 hosts, we need to extend the subnet mask from **/16** to **/22**.
  + **/22** subnet mask provides **1024 hosts**, which is more than enough for the required 900 hosts.

**Subnet Mask:**

* **Subnet Mask**: **255.255.252.0** or **/22**
* This allows for **1024 hosts** per subnet, and the network will be divided into **64 subnets** (since 2^6 = 64).

**UNIT-IV ROUTING**

**Q1: Explain the Working of Distance Vector Routing with an Example.**

**1. Working of Distance Vector Routing:**

* Each router maintains a **routing table** with distance to all networks.
* Routers share updates **periodically**.
* Uses the **Bellman-Ford Algorithm** for route calculation.

**2. Example:**

Consider three routers: **A, B, and C**

* **A → B (cost = 2), B → C (cost = 3), A → C (cost = 5)**.
* Using distance vector, **A updates route to C via B** (2+3 = 5).

**3. Advantages:**

✔ Simple to implement.  
✔ Works well in small networks.

**4. Disadvantages:**

❌ **Slow convergence**.  
❌ **Routing loops (solved using split horizon and hold-down timers).**

**Q2: Compare Link-State Routing (OSPF) and Distance Vector Routing (RIP).**

| **Feature** | **Distance Vector (RIP)** | **Link State (OSPF)** |
| --- | --- | --- |
| **Algorithm** | Bellman-Ford | Dijkstra's |
| **Metric** | Hop count | Cost (bandwidth-based) |
| **Convergence** | Slow | Fast |
| **Updates** | Periodic | Only when needed |
| **Scalability** | Small networks | Large networks |
| **Example** | Small office networks | Large enterprise networks |

**3. Conclusion:**

* **RIP** is easy to set up but not scalable.
* **OSPF** is complex but more efficient.

**Q3: Explain Multicast Routing Protocols: DVMRP and PIM.**

**1. Distance Vector Multicast Routing Protocol (DVMRP):**

* Uses **reverse path forwarding (RPF)**.
* Builds a **source-based tree**.
* Floods packets initially, then prunes unnecessary branches.

**2. Protocol Independent Multicast (PIM):**

* Works in **both dense and sparse networks**.
* Builds **shared trees** instead of flooding.
* **Types:**
  + **PIM-DM (Dense Mode):** Best for networks with many receivers.
  + **PIM-SM (Sparse Mode):** Best for wide-area multicast.

**Comparison:**

| **Feature** | **DVMRP** | **PIM** |
| --- | --- | --- |
| Flooding | Yes | No |
| Network Type | Dense | Sparse |
| Complexity | High | Low |

**UNIT-V DATA LINK AND PHYSICAL LAYER**

**Q1: Explain HDLC and PPP Protocols in Detail.**

**1. High-Level Data Link Control (HDLC):**

✔ **Bit-oriented** protocol.  
✔ **Frame Structure:**

* **Flag (01111110)** → Identifies frame boundaries.
* **Address Field** → Identifies the recipient.
* **Control Field** → Defines frame type.
* **Data Field** → Contains actual data.
* **CRC Field** → Error detection.

✔ **Modes:**

* **Normal Response Mode (NRM)** → Master-Slave.
* **Asynchronous Balanced Mode (ABM)** → Peer-to-peer.

**2. Point-to-Point Protocol (PPP):**

✔ Used for **dial-up and broadband connections**.  
✔ **Components:**

* **Link Control Protocol (LCP)** → Establishes the link.
* **Network Control Protocol (NCP)** → Configures IP, IPv6, etc.  
  ✔ **Advantages:**
* Supports multiple protocols.
* Error detection using CRC.

**Example:**

* PPP is used in **DSL and VPN connections**.

**Q2: Explain Wireless LAN (802.11) and Its Features.**

**1. Introduction to 802.11 (Wi-Fi):**

✔ IEEE **802.11** standard defines **Wireless Local Area Networks (WLANs)**.  
✔ Uses **radio waves** instead of cables.

**2. Key Features:**

1. **Physical Layer:**
   * Uses **DSSS, FHSS, and OFDM** for transmission.
   * Operates at **2.4 GHz and 5 GHz**.
2. **Media Access Control (MAC):**
   * Uses **CSMA/CA (Collision Avoidance)**.
3. **Wi-Fi Modes:**
   * **Infrastructure Mode:** Devices connect via **access points**.
   * **Ad-Hoc Mode:** Devices communicate **directly**.

**3. Advantages:**

✔ Mobility.  
✔ Cost-effective.  
✔ Easy installation.

**4. Example:**

* Home **Wi-Fi networks** use 802.11 standards.

**Q3: Compare Circuit Switching and Packet Switching.**

| **Feature** | **Circuit Switching** | **Packet Switching** |
| --- | --- | --- |
| **Definition** | Dedicated path established before communication | Data divided into packets and sent independently |
| **Example** | Telephone networks | Internet (TCP/IP) |
| **Efficiency** | Less efficient | Highly efficient |
| **Latency** | Low latency once established | Higher due to routing delays |
| **Flexibility** | Rigid, fixed path | Dynamic path selection |

**1. Circuit Switching:**

✔ **Dedicated connection** → Reserves a path for the entire session.  
✔ **Phases:**

* **Setup Phase** → Establishes a connection.
* **Data Transfer Phase** → Continuous transmission.
* **Teardown Phase** → Connection is released.  
  ✔ **Example:** **Traditional telephone networks**.

**2. Packet Switching:**

✔ **Data is divided into packets**, each with headers and trailers.  
✔ **Types:**

* **Datagram Packet Switching:** Packets take **independent routes**.
* **Virtual Circuit Switching:** A **predefined route** is set up.  
  ✔ **Example:** **Internet (TCP/IP, VoIP, Streaming services)**.