**CS3591-COMPUTER NETWORKS**

**PART-B (13 Marks)**

**UNIT-I INTRODUCTION AND APPLICATION LAYER**

**1.Explain the types of transmission modes.**

o The way in which data is transmitted from one device to another device is known as transmission mode.

o The transmission mode is also known as the communication mode. o Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.

o The transmission mode is defined in the physical layer.

**Types of Transmission mode :**

The Transmission mode is divided into three categories:

o Simplex Mode

o Half-duplex Mode

o Full-duplex mode (Duplex Mode)

**SIMPLEX MODE**

o In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.

o A device can only send the data but cannot receive it or it can receive the data but cannot send the data.

o This transmission mode is not very popular as mainly communications require the two-way exchange of data. The simplex mode is used in the business field as in sales that do not require any corresponding reply.

o The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back. o Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.

o The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission. **Advantage of Simplex mode:**

o In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

**Disadvantage of Simplex mode:**

**o** Communication is unidirectional, so it has no inter-communication between devices.

**HALF-DUPLEX MODE**

o In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.

o Messages flow in both the directions, but not at the same time.

o The entire bandwidth of the communication channel is utilized in one direction at a time.

o In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.

o A Walkie-talkie is an example of the Half-duplex mode. o In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens. Speaking simultaneously will create the distorted sound which cannot be understood.

**Advantage of Half-duplex mode:** o In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

**Disadvantage of Half-Duplex mode:** o In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

**FULL-DUPLEX MODE**

o In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.

o Both the stations can send and receive the message simultaneously. o Full-duplex mode has two simplex channels. One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.

o The Full-duplex mode is the fastest mode of communication between devices.

o The most common example of the full-duplex mode is a Telephone network. When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

**Advantage of Full-duplex mode:**

o Both the stations can send and receive the data at the same time.

**Disadvantage of Full-duplex mode:**

o If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

**2.What is Network Topology? Explain the Different Network Topologies.**

**Network topology** refers to the arrangement or layout of different elements (links, nodes, etc.) in a computer network. It defines the structure of how the devices and components are connected and how data flows between them. Topologies can be physical (the actual physical layout) or logical (the way data is transmitted over the network).

**Types of Network Topologies:**

1. **Bus Topology:**
   * In a bus topology, all devices are connected to a single central cable, known as the bus or backbone. Data is sent from one device to another via this central cable.
   * **Advantages:** Simple and inexpensive to implement, easy to extend.
   * **Disadvantages:** A failure in the central cable can bring down the entire network.
2. **Ring Topology:**
   * Devices are connected in a circular fashion, with each device connected to two other devices. Data travels in one direction or both directions in the ring.
   * **Advantages:** Easy to install and configure, performs well for small networks.
   * **Disadvantages:** A failure in any cable or device can disrupt the entire network.
3. **Star Topology:**
   * In star topology, each device is connected to a central node (usually a hub or switch). All data passes through this central point.
   * **Advantages:** Easy to manage and expand, failure of one device doesn't affect others.
   * **Disadvantages:** The central hub is a single point of failure.
4. **Mesh Topology:**
   * In mesh topology, each device is connected to every other device in the network. This provides multiple paths for data transmission.
   * **Advantages:** Highly reliable, as there are multiple paths for data to reach its destination.
   * **Disadvantages:** Expensive and complex to install due to the large number of connections.
5. **Tree Topology:**
   * Tree topology is a combination of star and bus topologies. Groups of star-configured networks are connected to a linear bus backbone.
   * **Advantages:** Scalable, hierarchical structure makes it easy to manage.
   * **Disadvantages:** Failure in the backbone or central device can bring down large parts of the network.
6. **Hybrid Topology:**
   * A hybrid topology is a combination of two or more different topologies. For example, a network may use a star topology at the local level and a bus topology at the backbone level.
   * **Advantages:** Flexible, can optimize the network performance.
   * **Disadvantages:** More complex to design and manage.

**3. What are the Different Types of Networks? Explain in Detail.**

**Computer networks** can be classified based on their size, scope, and purpose. The following are the different types of networks:

1. **Personal Area Network (PAN):**
   * **Definition:** A small network typically confined to an individual's workspace. PAN is usually wireless and is used to connect personal devices like smartphones, laptops, and tablets.
   * **Examples:** Bluetooth devices, wireless keyboard and mouse connections.
   * **Range:** Typically up to 10 meters.
2. **Local Area Network (LAN):**
   * **Definition:** A network that connects computers and devices in a limited geographical area like a home, office, or building.
   * **Examples:** Home networks, office networks.
   * **Range:** Typically up to 100 meters.
   * **Features:** High data transfer rate, low latency, often uses Ethernet cables and Wi-Fi.
3. **Wide Area Network (WAN):**
   * **Definition:** A network that spans a large geographical area, such as a country or continent. WANs connect multiple LANs and MANs.
   * **Examples:** The internet, business connections between office locations.
   * **Range:** Can span thousands of kilometers.
   * **Features:** Lower data transfer rates than LANs, uses leased lines, satellites, or other technologies for long-distance connectivity.
4. **Metropolitan Area Network (MAN):**
   * **Definition:** A network that covers a larger geographical area than a LAN but is smaller than a WAN. It connects LANs within a city or large campus.
   * **Examples:** Networks connecting university campuses, or city-wide wireless networks.
   * **Range:** Typically up to 50 kilometers.
   * **Features:** High-speed connections, often used by businesses or local governments.
5. **Campus Area Network (CAN):**
   * **Definition:** A network that connects LANs across multiple buildings within a specific campus area, such as a university campus or a corporate building complex.
   * **Examples:** A university network connecting buildings across a large campus.
   * **Range:** Typically between 1 to 10 kilometers.
   * **Features:** Can be considered a subset of MAN, typically with high-speed internet connectivity.
6. **Storage Area Network (SAN):**
   * **Definition:** A specialized network that provides block-level data storage. It is used to connect servers and storage devices, typically in large data centers.
   * **Examples:** Used in data centers for fast, reliable data storage.
   * **Range:** Covers only the data center or enterprise environment.
   * **Features:** High-performance network designed specifically for storage purposes.
7. **Virtual Private Network (VPN):**
   * **Definition:** A network that allows for secure communication over public or untrusted networks, such as the internet. It uses encryption and tunneling protocols to create a secure connection.
   * **Examples:** Connecting remote workers to a corporate network.
   * **Range:** Global, typically connecting remote users to internal networks.
   * **Features:** Security, remote access, and privacy.

**4. What are the Applications of Computer Networks?**

Computer networks have revolutionized communication, data sharing, and business operations across various sectors. Some of the most prominent applications of computer networks include:

1. **Resource Sharing:**
   * Allows devices and users to share resources such as printers, files, or internet connections. For example, in a LAN, multiple devices can share a single printer, reducing costs and improving efficiency.
2. **Communication:**
   * **Email:** A widely used form of communication within and outside organizations.
   * **Instant Messaging:** Real-time text communication between users.
   * **VoIP (Voice over Internet Protocol):** Allows voice communication over the internet (e.g., Skype, Zoom).
   * **Video Conferencing:** Platforms like Zoom, Microsoft Teams, or Google Meet enable remote video meetings.
3. **File Sharing:**
   * Enables the sharing of documents, media files, and other digital assets across computers. File-sharing platforms, cloud services like Google Drive and Dropbox, allow individuals and businesses to store and share files easily.
4. **Remote Access:**
   * Allows users to access a computer or network remotely, from anywhere in the world, using tools like VPNs or Remote Desktop Protocol (RDP).
5. **E-commerce:**
   * Computer networks facilitate online shopping, payment processing, and other business transactions. Websites, secure payment gateways, and shopping platforms are built on computer networks, allowing global businesses to interact with customers.
6. **Banking and Financial Transactions:**
   * Online banking, mobile payments, stock trading, and cryptocurrency transactions rely heavily on computer networks for secure and real-time operations.
7. **Distributed Computing:**
   * Networks are used to connect multiple computers to share processing power and storage. Technologies like cloud computing and grid computing rely on interconnected systems to provide services like data storage, application hosting, and analytics.
8. **Education and E-Learning:**
   * Educational platforms like MOOCs (Massive Open Online Courses) and online tutorials rely on computer networks to provide education remotely. Students and teachers use virtual classrooms to interact, exchange materials, and conduct examinations.
9. **Social Media and Networking:**
   * Platforms like Facebook, Twitter, LinkedIn, and Instagram are built on computer networks, enabling individuals to share personal updates, communicate, and collaborate across the globe.
10. **Entertainment and Streaming:**
    * Streaming platforms like Netflix, YouTube, and Spotify rely on robust computer networks to provide real-time media access. Video, music, and gaming content are delivered through the internet, with high-quality services enabled by fast, reliable networks.
11. **Health Care:**
    * Telemedicine, electronic health records (EHR), and remote monitoring of patients rely on computer networks for communication between patients, doctors, and healthcare providers.
12. **IoT (Internet of Things):**
    * Computer networks are essential for connecting everyday objects like smart homes, wearables, and industrial equipment to the internet, allowing them to collect data and communicate with each other.
13. **Security and Surveillance:**
    * Computer networks are used for surveillance systems, alarm systems, and security cameras, which can be monitored remotely via the internet. Data from these systems is often transmitted to central servers for analysis.

**5.Explain the OSI reference model with neat diagram.**

The **OSI (Open Systems Interconnection) Reference Model** is a conceptual framework used to understand and standardize the functioning of communication systems. It divides the communication process into seven distinct layers, each responsible for specific tasks in data transmission and reception.

The OSI model helps in ensuring interoperability between different networking systems and devices, providing a guideline for the development of networking protocols and ensuring data flows smoothly from one device to another.

**7 Layers of the OSI Model**

Here’s a detailed explanation of each layer:

1. **Physical Layer (Layer 1):**
   * **Function:** Responsible for the transmission and reception of raw data bits over a physical medium (like cables, fiber optics, etc.).
   * **Responsibilities:**
     + Defines the electrical, mechanical, and procedural characteristics of the transmission medium.
     + Deals with hardware devices such as cables, switches, and network interface cards (NICs).
   * **Example:** Ethernet cables, Wi-Fi, and Bluetooth.
2. **Data Link Layer (Layer 2):**
   * **Function:** Ensures error-free transfer of data frames between devices on the same network.
   * **Responsibilities:**
     + Provides error detection and correction (e.g., CRC).
     + Handles MAC (Media Access Control) addressing to identify devices on the local network.
     + Manages flow control and physical addressing.
   * **Example:** Ethernet, Wi-Fi, PPP (Point-to-Point Protocol).
3. **Network Layer (Layer 3):**
   * **Function:** Responsible for routing data packets between devices across different networks.
   * **Responsibilities:**
     + Logical addressing (IP addressing).
     + Routing and forwarding of data packets.
     + Determines the best path for data transmission.
   * **Example:** IP (Internet Protocol), routers.
4. **Transport Layer (Layer 4):**
   * **Function:** Ensures reliable data transfer between two devices.
   * **Responsibilities:**
     + Provides error detection and correction.
     + Segments and reassembles data for transmission.
     + Manages end-to-end communication and flow control.
   * **Example:** TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
5. **Session Layer (Layer 5):**
   * **Function:** Manages sessions between applications, establishing, maintaining, and terminating communication.
   * **Responsibilities:**
     + Controls dialogues (connections) between systems.
     + Synchronizes data exchange and ensures that data is properly synchronized.
     + Manages full-duplex, half-duplex, or simplex communication.
   * **Example:** NetBIOS, RPC (Remote Procedure Call).
6. **Presentation Layer (Layer 6):**
   * **Function:** Translates, encrypts, and compresses data between the application and transport layers.
   * **Responsibilities:**
     + Data encoding, data compression, and encryption.
     + Converts data from one format to another (e.g., from EBCDIC to ASCII).
   * **Example:** SSL/TLS (Secure Sockets Layer / Transport Layer Security), JPEG, GIF, and encryption algorithms.
7. **Application Layer (Layer 7):**
   * **Function:** The closest layer to the user, this layer interacts directly with the end-user application and provides network services.
   * **Responsibilities:**
     + Provides interfaces for end-user applications.
     + Manages network services like email, file transfer, web browsing, etc.
   * **Example:** HTTP, FTP, SMTP, DNS, POP3.

**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

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

**UNIT-II TRANSPORT LAYER**

PART-B(13 Marks)

**1.Discuss in detail about the Ethernet. (May 12,15)(Nov 15)**

**1. Ethernet – Detailed Explanation**

Ethernet is a widely used technology for Local Area Networks (LANs). It was first developed by Xerox in the 1970s and has evolved to become the dominant LAN standard, primarily due to its simplicity, low cost, and scalability. Ethernet is used to connect devices like computers, printers, switches, and routers within a limited geographical area, such as a building or campus.

**Key Features of Ethernet:**

* Media Type: Ethernet can operate over different physical media, including twisted pair cables (Cat5e, Cat6), coaxial cables, and fiber-optic cables.
* Topology: Traditionally, Ethernet used a bus topology, but modern Ethernet networks usually use a star topology, with switches at the center connecting multiple devices.
* Data Link Layer (Layer 2): Ethernet works at the data link layer and uses MAC (Media Access Control) addresses for communication. Each Ethernet device is identified by a unique 48-bit MAC address.
* Frame Format: Ethernet frames consist of:
  + Preamble: 7 bytes (used for synchronization).
  + Start Frame Delimiter (SFD): 1 byte (indicates the start of the frame).
  + Destination MAC Address: 6 bytes.
  + Source MAC Address: 6 bytes.
  + Length/Type: 2 bytes.
  + Data: 46 to 1500 bytes (contains the payload).
  + Frame Check Sequence (FCS): 4 bytes (used for error detection).

**Ethernet Speeds and Standards:**

* 10 Mbps (Ethernet): The original Ethernet speed.
* 100 Mbps (Fast Ethernet): An upgrade in the early 1990s.
* 1 Gbps (Gigabit Ethernet): Common in modern LANs.
* 10 Gbps (10 Gigabit Ethernet): Used in high-speed networks and data centers.

**Ethernet Switches and Hubs:**

* Hubs: A hub broadcasts data to all devices on the network, leading to collisions in a shared medium environment.
* Switches: Ethernet switches provide a more efficient method by learning the MAC addresses of devices and forwarding frames only to the appropriate device, reducing collisions.

**Ethernet and Full Duplex Communication:**

Modern Ethernet supports full-duplex communication, meaning data can be sent and received simultaneously, which improves network performance and eliminates collisions, a problem in half-duplex communication (which occurs in older Ethernet).

**2.Explain CSMA in detail. Describe the CSMA/CD protocol and comment on its performance for medium access.**

**CSMA (Carrier Sense Multiple Access) :**

CSMA (Carrier Sense Multiple Access) is a protocol used in Ethernet networks to control access to the shared communication medium, avoiding collisions between multiple devices trying to send data simultaneously.

**CSMA Operation:**

1. Carrier Sense: Before transmitting, each device "listens" to the network to determine if it is idle (i.e., no other device is transmitting).
2. Transmit Data: If the channel is idle, the device begins transmitting its data.
3. Collision Detection: If another device simultaneously transmits, a collision occurs, and both devices stop transmitting.

CSMA operates in the following methods to avoid collisions:

**Types of CSMA:**

1. **1-Persistent CSMA:**
   * Devices continuously listen to the channel.
   * If the channel is idle, the device transmits immediately.
   * If the channel is busy, the device keeps listening until it becomes idle.
   * Problem: High collision rate, as multiple devices transmit when the channel is free.
2. **Non-Persistent CSMA:**
   * If the channel is busy, the device waits for a random amount of time before checking again.
   * If idle, it transmits immediately.
   * Advantage: Reduces the likelihood of collisions compared to 1-persistent CSMA.
3. **P-Persistent CSMA:**
   * In this method, when the channel is idle, the device transmits with a probability PPP, and if it doesn't transmit, it waits for a random amount of time.
   * Advantage: Balances the collision rate and channel utilization.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – Protocol and Performance:

CSMA/CD is a protocol used in Ethernet networks to handle collisions in a shared communication medium. It's an extension of CSMA, specifically designed for half-duplex networks.

**CSMA/CD Protocol:**

1. Carrier Sense: A device first listens to the channel to check if it's idle or busy.
2. Transmit Data: If the channel is idle, the device begins transmitting its data.
3. Collision Detection: While transmitting, the device simultaneously listens for any collisions. If a collision is detected (via signal interference), the transmission is immediately halted.
4. Backoff Mechanism: After a collision, the devices involved must wait for a random backoff time before attempting to transmit again. This random delay helps avoid repeated collisions.

**Performance of CSMA/CD:**

* Efficiency: CSMA/CD works efficiently under low traffic conditions. However, as the number of devices increases, the likelihood of collisions increases, leading to a decrease in performance.
* Collisions: When a collision occurs, both devices must retransmit, causing delays and reducing the throughput of the network.
* Throughput: The throughput decreases as more devices are added to the network due to increased collisions and the backoff process.
* Limitations: In modern Ethernet networks using full-duplex communication, CSMA/CD is no longer needed, as the devices can send and receive data simultaneously, eliminating collisions.

**4.Explain the functioning of wireless LAN in detail. (Nov 10,12,15)(May 15)**

**Wireless LAN (WLAN) – Detailed Explanation**

A Wireless Local Area Network (WLAN) is a type of network that allows devices to communicate wirelessly within a limited geographic area, such as a home, office, or campus. WLANs use radio frequency (RF) technology to transmit data.

**Components of WLAN:**

* Access Points (AP): Devices that provide connectivity between wireless devices and the wired network.
* Wireless Clients: Devices such as laptops, smartphones, and tablets that connect to the wireless network via an AP.
* Wireless Router: A device that combines routing, switching, and wireless access point functions.

**WLAN Operation:**

1. RF Communication: Wireless devices communicate over radio frequencies, typically using the 2.4 GHz or 5 GHz bands.
2. IEEE 802.11 Standard: WLANs are based on the IEEE 802.11 standards, which define the protocols for data transmission, security, and media access control in wireless networks.
3. Access Control: WLANs use a form of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to control access to the channel and avoid collisions.

**IEEE 802.11 Protocol Stack:**

* Physical Layer (PHY): Defines the transmission medium, including modulation and data rate (e.g., 802.11a/b/g/n/ac).
* MAC Layer: Manages access to the wireless medium, including channel allocation, error detection, and frame synchronization.

**WLAN Advantages:**

* Mobility: Users can move freely within the coverage area without losing connectivity.
* Flexibility: Easier to install and scale compared to wired networks.
* Cost-effective: Reduces cabling and hardware costs.

**WLAN Challenges:**

* Interference: Wireless networks are subject to interference from other devices (e.g., microwaves, Bluetooth devices).
* Security: WLANs are more vulnerable to unauthorized access and attacks (e.g., eavesdropping, spoofing).

**4.Explain how hidden node and exposed node problem is solved in IEEE 802.11.(Nov 13)**

**Hidden Node and Exposed Node Problem in IEEE 802.11**

**Hidden Node Problem:**

* Issue: Occurs when two devices are within range of the Access Point (AP) but are not within range of each other. This can lead to collisions, as one device cannot sense the transmission of the other, even though they are both communicating with the same AP.
* Solution: IEEE 802.11 uses a Request to Send (RTS) and Clear to Send (CTS) handshake to avoid collisions. When a device wants to transmit, it sends an RTS to the AP. If the AP grants permission, it responds with a CTS. Devices hearing the CTS are forbidden from transmitting, preventing collisions.

**Exposed Node Problem:**

* Issue: Occurs when a device (A) is trying to transmit but detects that another device (B) is transmitting, even though they are not sharing the same channel. Device A may unnecessarily defer its transmission, thus reducing network efficiency.
* Solution: The use of RTS/CTS can also help mitigate this problem, as devices only defer transmission if they are in the actual transmission range of the device transmitting to the AP.

**UNIT-III NETWORK LAYER**

PART-B(13 Marks)

**1.Discuss about Link-state routing and routers. (Nov 12,20)(May 15,21)**

**Link-State Routing and Routers (13 Marks)**

**Link-State Routing** is a type of routing protocol where each router maintains a map of the entire network and determines the best path based on this information. It is different from distance-vector routing, where each router only knows its neighbors and the distance to them.

**Key Characteristics of Link-State Routing:**

1. **Link-State Advertisements (LSAs):**
   * Routers in a link-state protocol send **LSAs** to all other routers in the network. Each LSA contains information about the router’s directly connected neighbors and their status.
   * LSAs are broadcast or multicast to all routers in the network, and each router keeps a database of these LSAs.
2. **Network Topology:**
   * Each router builds a **Link-State Database (LSDB)** that contains the topology of the network. This database is identical across all routers in the network.
   * From this LSDB, each router creates a **shortest path tree (SPT)** using Dijkstra’s algorithm.
3. **Routing Table Generation:**
   * Once the shortest path tree is built, the router generates its routing table, which contains the best paths to all destinations.
   * This routing table is updated periodically based on the LSAs received from neighbors.

**Advantages of Link-State Routing:**

1. **Faster Convergence:**
   * Link-state routing algorithms typically converge faster than distance-vector protocols because routers have complete network topology information.
2. **Scalability:**
   * Link-state protocols can handle large networks better than distance-vector protocols, as they reduce the amount of routing information exchanged by sending only LSAs rather than complete routing tables.
3. **More Accurate Routing Information:**
   * Since each router has the entire map of the network, it can make more accurate routing decisions compared to distance-vector protocols.

**Popular Link-State Routing Protocols:**

1. **OSPF (Open Shortest Path First):**
   * OSPF is the most widely used link-state routing protocol. It is designed to work within a single autonomous system and uses **Dijkstra’s algorithm** for computing the shortest path.
2. **IS-IS (Intermediate System to Intermediate System):**
   * Similar to OSPF, IS-IS is used in large-scale networks like service providers’ networks.

**Routers:**

* **Routers** are devices that forward data packets between different networks. Routers use routing protocols (like Link-State, Distance-Vector) to determine the best path for data transmission.
* They maintain **routing tables**, which contain information about the network's topology, and use algorithms to choose the optimal route for packets based on criteria such as the shortest path, least cost, or highest reliability.

**2. Explain about the inter domain routing (BGP) routing algorithms. (Nov 20)(May 21 )**

**Inter-Domain Routing (BGP) Algorithms:**

**BGP (Border Gateway Protocol)** is the inter-domain routing protocol used to exchange routing information between different autonomous systems (ASes) on the internet. Unlike interior gateway protocols (IGPs), which operate within an AS, BGP operates between ASes, making it an essential protocol for internet routing.

**Key Features of BGP:**

1. **Path Vector Protocol:**
   * BGP is a **path vector protocol**, meaning it maintains a list of ASes that a route has traversed. Each BGP router advertises the path to a destination, and other routers use this information to avoid routing loops and select the best path.
2. **Route Selection:**
   * BGP selects routes based on a set of attributes, including **AS Path**, **Next Hop**, **Local Preference**, **MED (Multi-Exit Discriminator)**, and **Weight**. The AS Path attribute is one of the most important in BGP, as it prevents routing loops and helps in determining the best route.
3. **Inter-Domain Routing:**
   * BGP is used to route traffic between different ISPs (Internet Service Providers) or large networks. It ensures that traffic is efficiently routed between diverse networks on the internet.
4. **Full Routing Table:**
   * BGP routers maintain a **full routing table** that contains paths to all reachable destinations in the internet, with information about the ASes that lead to those destinations.
5. **Policy-Based Routing:**
   * BGP supports **policy-based routing**, which allows network administrators to define policies on routing decisions. For example, an administrator can configure a preference for certain routes based on cost, reliability, or performance.

**BGP Attributes:**

* **AS Path**: A list of ASes that the route has passed through.
* **Next Hop**: The next-hop IP address to reach a destination.
* **Local Preference**: Indicates the preferred path for outgoing traffic within an AS.
* **MED (Multi-Exit Discriminator)**: A metric used to prefer one entry point to an AS over another.
* **Weight**: A Cisco-specific attribute that is used to prefer one route over another.

**BGP Message Types:**

* **Open**: Establishes a session between two BGP routers.
* **Update**: Advertises new routes or withdraws old ones.
* **Notification**: Indicates an error condition.
* **Keep-Alive**: Maintains the BGP session.

**Advantages of BGP:**

* **Scalability**: BGP can handle large networks with complex routing tables.
* **Control**: BGP allows for fine-grained control over routing decisions, which is essential for managing internet traffic.

**3.Explain about IPV6?Compare IPV4 and IPV6 (May 16)**

**IPv6 and Comparison with IPv4**

**IPv6** (Internet Protocol version 6) is the most recent version of the Internet Protocol, designed to replace **IPv4**. IPv6 offers a larger address space, improved security features, and better support for modern internet applications.

**Key Features of IPv6:**

1. **Larger Address Space:**
   * IPv6 uses a 128-bit address (represented as eight groups of four hexadecimal digits), allowing for a theoretical address space of 340 undecillion addresses (3.4 × 10^38). This is a significant increase compared to IPv4’s 32-bit address space (approximately 4.3 billion addresses).
2. **Simplified Header:**
   * IPv6 headers are simpler than IPv4 headers, with fewer fields and no need for checksum calculation. This reduces processing overhead in routers.
3. **Autoconfiguration:**
   * IPv6 supports **stateless address autoconfiguration (SLAAC)**, allowing devices to automatically configure their IP address without the need for a DHCP server.
4. **Improved Security:**
   * IPv6 was designed with **IPsec** (a security protocol) as a fundamental part of the standard, ensuring confidentiality, integrity, and authentication for IP communications.
5. **No NAT (Network Address Translation):**
   * With the larger address space, IPv6 eliminates the need for NAT, allowing for end-to-end connectivity between devices.

**Comparison of IPv4 and IPv6:**

| **Feature** | **IPv4** | **IPv6** |
| --- | --- | --- |
| **Address Length** | 32-bit | 128-bit |
| **Address Space** | 4.3 billion addresses | 340 undecillion addresses |
| **Header Size** | 20-60 bytes | 40 bytes |
| **Address Configuration** | Manual or DHCP | Stateless or DHCPv6 |
| **Security** | Optional (IPsec) | Mandatory (IPsec) |
| **Routing Complexity** | More complex due to NAT | Simplified due to large address space |
| **Broadcast Support** | Yes | No (uses multicast instead) |

**4. Explain the Routing Information protocol/Distance vector routing in detail. (Nov 13,15,19,21)(May 15,16,21)**

**Routing Information Protocol (RIP) / Distance Vector Routing (13 Marks)**

**Routing Information Protocol (RIP)** is one of the oldest distance-vector routing protocols. It uses hop count as its metric to determine the best path. RIP is a part of the **Distance Vector Routing** family, where each router shares its routing table with neighbors periodically.

**Key Features of RIP:**

1. **Distance Vector Protocol:**
   * In distance-vector routing, routers share their routing table with neighboring routers. Each router knows the distance (usually in terms of hop count) to reach various destinations.
2. **Metric (Hop Count):**
   * RIP uses hop count as its metric, where each hop between routers is counted as one. The maximum allowed hop count in RIP is 15, and any destination more than 15 hops away is considered unreachable.
3. **Periodic Updates:**
   * RIP routers send updates every 30 seconds to all neighboring routers, allowing them to maintain an up-to-date view of the network.
4. **Routing Loops:**
   * RIP is susceptible to routing loops, but it uses techniques like **split horizon** and **poison reverse** to mitigate this problem.

**Advantages of RIP:**

* **Simplicity**: RIP is simple to configure and deploy.
* **Compatibility**: It is supported by most routers and can work well in small to medium-sized networks.

**Disadvantages of RIP:**

* **Limited Scalability**: RIP is not suitable for large networks due to its 15-hop limit.
* **Slow Convergence**: RIP has slow convergence times, meaning it takes longer to recover from network changes.

**5. Explain in detail i) ICMP ii) ARP (Nov 19) iii) RARP.**

**i) ICMP (Internet Control Message Protocol):**

ICMP is used for error reporting and diagnostic functions in IP networks. It is part of the Internet Protocol suite.

* **Types of ICMP Messages:**
  + **Echo Request and Echo Reply**: Used for pinging and testing connectivity.
  + **Destination Unreachable**: Sent when a destination cannot be reached.
  + **Time Exceeded**: Used in traceroute, indicating that the time-to-live (TTL) has expired.

**ii) ARP (Address Resolution Protocol):**

ARP is used to map a 32-bit IPv4 address to a MAC address in local networks.

* **ARP Process:**
  + When a device wants to send data to another device on the same network, it sends out an ARP request asking for the MAC address corresponding to an IP address.
  + The device with the matching IP address replies with its MAC address.

**iii) RARP (Reverse Address Resolution Protocol):**

RARP is used to map a MAC address to an IP address. It is typically used by diskless workstations to obtain their IP address from a central server when booting.

**UNIT-IV ROUTING**

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

PART-A

**1. Why do we need a Domain Name System? What role does the DNS Resolver play in the DNS system? (Nov 12)**

Domain Name System can map a name to an address and conversely an address toname. The Domain Name System converts domain names into IP numbers. IP numbersuniquely identify hosts on the Internet: however they are difficult to remember. Wetherefore need a memorable way of identifying hosts.

**2. What are the four main properties of HTTP?**

* Global Uniform Resource Identifier
* Request-response exchange
* Statelessness
* Resource metadata.

**3. What are the TCP connections needed in FTP?**

FTP establishes two connections between the hosts. One connection is used for datatransfer, the other for control information.

The control connection uses very simple rules of communication. The data connectionneeds more complex rules due to the variety of data types transferred.

**4. What is WWW and SMTP? (Nov 10,15)( May 15)**

* World Wide Web is an internet application that allows user to view pages and move from one web page to another.
* It helps to store and share data across varied distances. The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer (SMTP).
* It is a system for sending messages to other computer users based on e-mail addresses.

**5. What are the four groups of HTTP Headers? What are the two methods of HTTP?(May 15) (Nov 15)**

The four groups of HTTP headers are

* General headers
* Entity Headers
* Request Headers
* Response Headers.

Two methods of HTTP are

GetMethod( ) PostMethod( )

**6. What is PGP? (Nov 10)(May 12)**

Pretty Good Privacy (PGP) is used to provide security for electronic mail. It providesauthentication, confidentiality, data integrity, and non-repudiation. It is a programusing public key encryption popularly used with email. Pretty Good Privacy uses avariation of the public key system. In this system, each user has an encryption key thatis publicly known and a private key that is known only to that user. PGP comes in twopublic key versions -- Rivest-Shamir-Adleman (RSA) and Diffie-Hellman.

**7. What are the transmission modes of FTP? (Nov 21)**

* Stream mode: Default mode and data is delivered from FTP to TCP as acontinuous stream of data.
* Block mode: Data is delivered from FTP to TCP in terms of blocks. Each data blockfollows the three byte header.
* Compressed mode: File is compressed before transmitting if size is big. Runlength encoding method is used for compression.

**8. Why is an application such as POP needed for electronic messaging? (May 12)**

Workstations interact with the SMTP host, which receives the mail on behalf of everyhost in the organization, to retrieve messages by using a client-server protocol such asPost Office Protocol. Although POP3 is used to download messages from the server, theSMTP client still needed on the desktop to forward messages from the workstation user

to its SMTP mail server.

**9. What is the use of MIME Extension?**

Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol thatallows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data atthe sender site to NVT ASCII data and deliverers it to the client SMTP to be sent throughthe Internet. MIME converts binary files, executed files into text files. Then only it canbe transmitted using SMTP.

**10. What is IMAP?**

Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mailfrom your local server. IMAP is a client/server protocol in which e-mail is received andheld for you by your Internet server. MAP can be thought of as a remote file server.POP3 can be thought of as a "store-and-forward" service.

**UNIT-IV ROUTING**

**Q1: Explain Unicast Routing and Its Importance.**

**Definition:**

Unicast routing is the process of forwarding data packets from a **single source to a single destination** across a network.

**Importance of Unicast Routing:**

1. **Efficient Packet Delivery** → Ensures reliable communication.
2. **Path Optimization** → Determines the best route.
3. **Error Handling** → Detects and handles failed links.
4. **Scalability** → Supports large networks.

**Example:**

* **Google Search** → The request sent by a user follows a unicast route to Google's servers, which then respond with results.

**Q2: Describe Distance Vector Routing and Explain RIP.**

**1. Distance Vector Routing:**

* A routing algorithm where each router updates its table based on **distance** (number of hops) to reach a destination.
* Uses the **Bellman-Ford algorithm**.
* **Drawback:** Slow convergence.

**2. Routing Information Protocol (RIP):**

* **Type:** Distance vector protocol.
* **Metric:** Hop count (max **15 hops**).
* **Update Interval:** Every **30 seconds**.
* **Drawback:** Not suitable for large networks.

**Example:**

* A small office network with multiple routers using **RIP v2** for communication.

**Q3: What is Link State Routing? Explain OSPF.**

**1. Link State Routing:**

* Each router **broadcasts its link status** to all other routers.
* Uses **Dijkstra’s algorithm** to compute the shortest path.

**2. Open Shortest Path First (OSPF):**

* **Type:** Link-state routing protocol.
* **Metric:** Cost (based on bandwidth).
* **Updates:** Only when network changes occur (**efficient**).
* **Divides networks into Areas** to optimize performance.

**Example:**

* Large enterprises use **OSPF** for better scalability than RIP.

**Q4: Explain Path-Vector Routing and Describe BGP.**

**1. Path-Vector Routing:**

* Used in inter-domain routing (between networks).
* Stores the **entire path** to prevent loops.

**2. Border Gateway Protocol (BGP):**

* **Type:** Path-vector routing protocol.
* **Metric:** Path attributes (AS Path, Next Hop, etc.).
* **Uses:** Internet routing between ISPs.
* **Advantage:** Prevents routing loops.

**Example:**

* The internet’s backbone is managed by **BGP** between different ISPs.

**Q5: Describe the Concept of Multicast Routing.**

**Definition:**

Multicast routing delivers packets **from one sender to multiple receivers** using **efficient routing trees**.

**Challenges:**

✔ Maintaining group membership.  
✔ Preventing duplicate packets.

**Protocols Used:**

1. **Distance Vector Multicast Routing Protocol (DVMRP)**
   * Uses **reverse path forwarding (RPF)**.
   * Builds a **source-based tree**.
2. **Protocol Independent Multicast (PIM)**
   * Works in **dense and sparse networks**.
   * Uses **shared trees** for efficiency.

**UNIT-V DATALINK AND PHYSICAL LAYER**

**Q1: Explain Framing in the Data Link Layer.**

**1. Definition:**

Framing is the process of dividing a stream of data into **smaller, manageable units** (frames) for transmission over a network.

**2. Types of Framing:**

1. **Character-based Framing:**
   * Uses **special characters** to mark frame boundaries (e.g., **SOH, EOT**).
   * **Issue:** Character corruption may cause errors.
2. **Bit-based Framing:**
   * Uses **bit patterns** (e.g., **01111110 in HDLC**).
   * Prevents errors with **bit stuffing** (inserting extra bits when needed).

**3. Example:**

* Ethernet frames have headers and footers with MAC addresses and checksums.

**Q2: Describe Flow Control Mechanisms in the Data Link Layer.**

**1. Definition:**

Flow control ensures that a **fast sender does not overwhelm a slow receiver**.

**2. Techniques:**

1. **Stop-and-Wait Protocol:**
   * Sender waits for an **ACK** after each frame.
   * **Issue:** Low efficiency.
2. **Sliding Window Protocol:**
   * Uses **window size** to allow multiple frames before requiring an ACK.
   * More efficient.

**3. Example:**

* TCP uses **sliding window** for better performance.

**Q3: Explain Error Control in the Data Link Layer.**

**1. Definition:**

Error control detects and corrects errors in transmitted frames.

**2. Techniques:**

1. **Error Detection:**
   * **Parity Check** → Adds an extra bit.
   * **Checksum** → Sums all bits and appends to the frame.
   * **CRC (Cyclic Redundancy Check)** → Uses polynomial division.
2. **Error Correction:**
   * **Hamming Code** → Adds redundancy bits.
   * **ARQ (Automatic Repeat reQuest)** → Retransmits corrupted frames.

**3. Example:**

* Wi-Fi uses **CRC** for error detection.

**Q4: What is CSMA/CD? Explain its Working in Ethernet.**

**1. Definition:**

Carrier Sense Multiple Access with Collision Detection (**CSMA/CD**) is used in **Ethernet networks** to avoid data collisions.

**2. Steps in CSMA/CD:**

1. **Carrier Sensing:** Device checks if the channel is **idle**.
2. **Transmission:** If idle, it **sends data**.
3. **Collision Detection:** If a collision occurs, devices send a **jam signal**.
4. **Backoff Algorithm:** Devices **wait** before retransmitting.

**3. Example:**

* Used in **wired Ethernet (IEEE 802.3)** networks.

**Q5: Explain Virtual LAN (VLAN) and Its Benefits.**

**1. Definition:**

A Virtual LAN (**VLAN**) is a **logical segmentation** of a physical network, allowing devices to communicate as if they were on the same network, even if physically separated.

**2. Benefits of VLANs:**

✔ **Improved Security** → Isolates sensitive data.  
✔ **Better Network Management** → Reduces broadcast domains.  
✔ **Enhanced Performance** → Reduces congestion.  
✔ **Flexibility** → Devices can move without reconfiguring the network.

**3. Example:**

* A company **separates HR and IT departments** using VLANs to improve security.