DEPARTMENT OF COMPUTER SCIENCE
Question Bank2
Advanced Networking MCA2

QUESTIONS

1. Compare IPv4 and IPv6 in all aspects
2. Explain the Drawbacks of Bellman Fold’s algorithm with Example
3. What are the Limitations of Dijkstra’s algorithm over Bellman’s Ford Algorithm
4. Compare Distance Vector routing and Link state routing algorithms in detail
5. Explain TCP/IP Protocol Architecture
6. Explain the difference between TCP and UDP
7. Explain Socket Programming
8. Explain WLAN
9. What is VLAN? Explain IEEE 802.1Q
10. Explain IEEE 802.11
11. Explain Transmission Media
12. What is an Application Proxy Server and explain how a Proxy firewall works
13. Explain NAT
14. Explain the SDN concept
15. What is Longest Prefix Matching
16. Explain Scheduling mechanisms in routing and forwarding of packets
17. Explain Addressing the internet and what is IP subnetting
18. Explain Intra AS routing in the network with examples
19. Explain BGP
20. Explain MPLS
21. Compare MPLS vs Traditional Network
22. Describe the hidden terminal problem and its solution in wireless LAN
23. Explain how CSMA/CD is used to detect and avoid collision in an Ethernet Network
24. Explain Error detection and correction in data transmission
25. Describe with a diagram the Three-Way-Handshake Mechanism for establishing reliable communication and ensuring Data delivery
26. Explain Classful IP addressing and what is the main drawback of classful addressing
27. Give the meaning of the following terms **(Any 5)**

    I. Sequence number
    II. Window size in tcp
    III. Selective repeat and Go-Back-N
    IV. Subnetting and supernetting
    V. Point-to-point link
    VI. Signal fading
    VII. Multipath
    VIII. Switched LAN

28. Explain SDN in brief
29. Describe How DHCP works
30. Explain ARP in the Data link layer

SOLUTIONS

1. Compare IPv4 and IPv6 in all aspects

Aspect	**IPv4**	**IPv6**
Address Length	32 bits	128 bits
Address Format	Dotted Decimal Notation (e.g., 192.0.2.1)	Hexadecimal Notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334)
Address Space	Limited (4.3 billion addresses)	Huge (3.4 × 10^38 addresses)
Header Format	Fixed-length	Fixed-length with optional extension headers
Header Fields	20 bytes, with 12 fields	40 bytes, with 8 fields
Security	No built-in security features	IPSec support by default for security
Address Configuration	Manual or DHCP	Stateless autoconfiguration or DHCPv6
NAT	Often used due to address exhaustion	Less reliance due to vast address space
Header Checksum	Included in header	Removed to simplify processing

2. Explain the Drawbacks of Bellman Fold’s algorithm with Example

Count to Infinity Problem: One of the main drawbacks of the Bellman-Ford algorithm is the "count to infinity" problem. This occurs when a router incorrectly believes it has discovered a shorter path to a destination and starts to broadcast this information to its neighbors. If the routing information loops back to the original router, it may interpret the loop as a series of shorter paths and update its routing table accordingly, leading to incorrect path selection and potential network instability.

Slow Convergence: The Bellman-Ford algorithm's convergence time can be slow, especially in larger networks or networks with high link churn. Each router iteratively updates its routing table based on information received from neighboring routers, and this process can take multiple iterations to converge to the optimal routing configuration. During this time, network performance may be degraded as routers continue to update and recalculate their routes.

Example:

Consider a network with routers A, B, and C, where A is the source and C is the destination. If there is a link failure between B and C, router B may still advertise routes to C to router A, albeit with a higher cost. Router A, unaware of the link failure, may choose to send packets to C via B, leading to a routing loop. As router A receives updates from router B, each with a slightly higher cost, it continues to update its routing table until it reaches the maximum cost (infinity). This process of counting to infinity can take time and cause unnecessary network overhead.

3. What are the Limitations of Dijkstra’s algorithm over Bellman’s Ford Algorithm

While Dijkstra's algorithm guarantees the shortest path from a single source to all destinations, it requires the network to be free of negative edge weights. Bellman-Ford can handle graphs with negative weights but is slower than Dijkstra's algorithm, especially in dense networks.

4. Compare Distance Vector routing and Link state routing algorithms in detail

Aspect	**Distance Vector Routing**	**Link State Routing**
Information Exchange	Periodic updates of routing tables to neighbors	Exchange of link state packets
Convergence	Slower convergence time	Faster convergence time
Routing Table Size	Smaller routing tables	Larger routing tables
Scalability	Less scalable due to frequent updates	More scalable due to selective updates
Routing Algorithm	Uses Bellman-Ford algorithm	Uses Dijkstra's algorithm

Aspect	**Distance Vector Routing**	**Link State Routing**
Example Protocols	RIP (Routing Information Protocol)	OSPF (Open Shortest Path First)
Loop Prevention	Uses split horizon and poison reverse	Uses sequence numbers and network flooding

5. Explain TCP/IP Protocol Architecture

6. Explain the difference between TCP and UDP

7. **Explain Socket Programming**

Socket Programming: The Backbone of Network Communication

Socket programming is a fundamental concept in network communication, providing a powerful interface for applications to interact with the network layer. It allows applications on different devices to establish connections and exchange data over a network.

Core Idea:

- Sockets act as endpoints for communication, similar to electrical outlets providing a connection point for devices.
- Applications create sockets, specify communication parameters (address, port), and use these sockets to send and receive data.
- The operating system manages the underlying network protocols (e.g., TCP/IP) to ensure data reaches the intended destination.

Here's a breakdown of key concepts in socket programming:

1. Sockets: The Endpoints

Client Socket: Initiates a connection to a server.

Server Socket: Passively listens for incoming connection requests and establishes connections with clients.

2. **Socket Creation and Addressing:**

The **socket()** system call creates a socket on the local machine.

Each socket is identified by a combination of two key elements:

IP Address: Uniquely identifies the device on the network.

Port Number: Identifies a specific application or service on a device (like a door number for a specific room in a building).

3. Socket Types:

There are two primary socket types for different communication patterns:

- **Stream Sockets (TCP):**

Provide a reliable, in-order byte stream for data exchange.

Suitable for applications requiring guaranteed delivery, like file transfers or web browsing.

- **Datagram Sockets (UDP):**

Offer connectionless, best-effort delivery of data packets.

Faster than TCP but lacks guaranteed delivery and ordering. Ideal for real-time applications like online gaming or video streaming where slight delays are acceptable.

4. Establishing Connections (TCP Sockets):

The client socket initiates a connection request using the connect() function, specifying the server's IP address and port number.

The server listens for connection requests on a specific port using the listen() function. Upon receiving a request, it accepts the connection with accept(), creating a new socket for communication with that client.

5. Data Exchange:

Once connected, data can be exchanged between sockets using functions like:

TCP Sockets: **send()** and recv() for sending and receiving data streams, respectively.

UDP Sockets: send () and **recvfrom()** for sending and receiving datagrams, respectively. These functions also specify the target IP address and port for datagrams.

6. Closing Sockets:

When communication is complete, sockets are closed using the **close()** function to release system resources.

8. **Explain WLAN**

WLAN stands for Wireless Local Area Network. It is a type of network that allows devices to connect and communicate wirelessly within a limited geographical area, such as a home, office, or campus.

Components of a WLAN:

Access Points (APs): APs are devices that act as a central hub for wireless connections. They transmit and receive wireless signals to and from client devices, providing access to the WLAN.

Wireless Clients: Wireless clients are devices such as laptops, smartphones, and tablets that connect to the WLAN. They communicate with APs to send and receive data over the wireless network.

Wireless Router: In-home or small office environments, a wireless router combines the functionality of a traditional wired router with that of an AP. It allows both wired and wireless devices to connect to the network and provides Internet access.

9. What is VLAN? Explain IEEE 802.1Q

LAN stands for Virtual Local Area Network. It's a way to segment a physical LAN into multiple logical networks. This creates broadcast domains, which are groups of devices that can see each other's broadcast traffic. With VLANs, you can create separate broadcast domains, so devices in one VLAN only see traffic from other devices in the same VLAN.

IEEE 802.1Q is a networking standard that defines a specific way to implement VLANs. It uses a tag in the Ethernet frame header to identify the VLAN membership of a device. This tag allows switches to forward traffic only to the appropriate VLAN.

10. **Explain IEEE 802.11**

IEEE 802.11, also known by the ubiquitous brand name Wi-Fi, is a set of standards established by the Institute of Electrical and Electronics Engineers (IEEE). These standards define the communication protocols for implementing Wireless Local Area Networks (WLANs). In simpler terms, they're the rules that govern how devices connect to Wi-Fi networks and exchange data wirelessly.

Here's a deeper dive into the key aspects of IEEE 802.11:

1. Medium Access Control (MAC):

- At the core of 802.11 lies the Medium Access Control (MAC) sublayer, responsible for regulating how devices share the wireless medium (radio waves) to avoid collisions.
- It employs a technique called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

2. Physical Layer (PHY):

- The Physical (PHY) layer defines the actual transmission and reception of radio signals over different frequency bands.
- Common IEEE 802.11 standards operate in the 2.4 GHz and 5 GHz bands
- Each band offers different characteristics in terms of range, speed, and capacity. For instance, the 2.4 GHz band provides wider coverage but lower speeds, while the 5 GHz band offers faster speeds but shorter range.

3. Different Standards of Wi-Fi:

- The IEEE 802.11 family encompasses a series of standards, each with its own capabilities and improvements:
  - **802.11a, b, and g:** Early standards offering varying speeds and ranges.
  - **802.11n (Wi-Fi 4):** Introduced Multiple-Input Multiple-Output (MIMO) technology for faster speeds and improved performance.
  - **802.11ac (Wi-Fi 5):** Further enhanced speeds and introduced beamforming for more efficient signal direction.
  - **802.11ax (Wi-Fi 6):** Increased efficiency for handling multiple devices and improved performance in congested environments.
  - **802.11axE (Wi-Fi 6E):** Extends Wi-Fi 6 to the 6 GHz band for even greater capacity.

4. Security Measures:.

- IEEE 802.11 standards support various encryption protocols like WEP (deprecated), WPA (Wi-Fi Protected Access), and WPA2 (more secure) to safeguard data transmission from eavesdropping.
- WPA3, the latest standard, offers enhanced security features like stronger encryption and improved resistance against brute-force attacks.

11. Explain Transmission Media

12. What is an Application Proxy Server and explain how a Proxy firewall works

An application proxy server acts as an intermediary between clients and servers for specific applications. It intercepts client requests and forwards them to the appropriate server, and then relays the server's response back to the client. A proxy firewall inspects incoming and outgoing traffic at the application layer, filtering based on application-specific rules. It provides an additional layer of security by hiding the internal network structure from external users.

13. Explain NAT

Network Address Translation (NAT) acts as a translator in your network, translating private IP addresses used within your local network to a single public IP address for accessing the wider internet. Here's a breakdown of its role and significance:

1. The IP Address Crunch:

- The internet relies on unique IP addresses for identifying devices. However, the pool of available public IPv4 addresses is limited.
- NAT steps in to address this scarcity. It allows multiple devices on your internal network (e.g., computers, phones, smart TVs) to share a single public IP address when communicating with the outside world.

2. How NAT Works:

a. When a device on your internal network initiates a connection to an external server, NAT intercepts the outgoing traffic.
b. It replaces the private IP address of the internal device with the public IP address assigned to your router by your internet service provider (ISP).
c. NAT also keeps track of which internal device initiated the connection using ports (think of them as labels for different applications).
d. When the response arrives from the server, NAT uses the port information to route it back to the correct internal device.

3. Benefits and Considerations:

- **Conserves Public IP Addresses:** NAT is a crucial tool for extending the limited pool of public IP addresses to support a growing number of devices.
- **Improves Network Security:** By hiding internal IP addresses, NAT adds a layer of basic security by making it harder for external attackers to directly target devices on your network.

14. Explain the SDN concept

Software-defined networking (SDN) is a revolutionary approach to network management that decouples the control plane from the data plane. Imagine the control plane as the brain, making decisions about how to route traffic, and the data plane as the body, physically forwarding the data. Here's a deeper dive into the SDN concept:

1. Decoupling the Control Plane:

- In traditional networks, each switch or router has its own control plane intelligence built-in. This makes configuration and management complex, especially for large networks.
- SDN disrupts this model by centralizing the control plane in a software-based SDN controller. This controller has a global view of the network and can program forwarding behavior on network devices.

2. OpenFlow Protocol:

- SDN relies on protocols like OpenFlow to communicate between the SDN controller and network devices. OpenFlow allows the controller to program forwarding rules on switches and routers, dictating how to handle different types of traffic.

3. Benefits of SDN:

- **Agility and Flexibility:** SDN empowers network administrators to dynamically adjust network behavior through software. This allows for faster provisioning of new services, easier traffic optimization, and improved security policies.
- **Centralized Control:** Managing the entire network from a single point simplifies configuration and troubleshooting, reducing complexity for large and geographically dispersed networks.
- **Programmability:** With SDN, network behavior can be automated using programming languages, enabling the creation of custom network applications and functionalities.

4. Key Components of an SDN Architecture:

- **SDN Controller:** The central software component that makes decisions about network traffic flow and programs network devices.
- **Southbound Interface:** The communication protocol (e.g., OpenFlow) between the SDN controller and network devices.
- **Northbound Interface:** The API used by applications or network management tools to interact with the SDN controller.
- **OpenFlow Switches:** Network devices that are programmed by the SDN controller to forward traffic according to specific rules.

15. What is an IP prefix? Describe Longest Prefix Matching

1. IP Prefix: A Subnet Address

An IP prefix, also known as a subnet address, It defines a specific network segment within a larger IP network.

- **IP Address:** A unique identifier for a device on the internet.
- **Subnet Mask:** A series of 1s followed by 0s in a 32-bit (IPv4) or 128-bit (IPv6) address. The 1s define the network portion, and the 0s define the host portion of the IP address.

Example:

- IP Address: 192.168.1.10
- Subnet Mask: 255.255.255.0 (This mask has 24 leading 1s)

The IP prefix in this example is 192.168.1.0/24. This indicates that all IP addresses from 192.168.1.1 to 192.168.1.254 belong to the same network segment.

2. Longest Prefix Matching: The Routing Algorithm.

How it Works:

a. The router compares the destination IP address of the packet with the prefixes in its routing table.
b. It selects the prefix that matches the most leading bits (the longest prefix) of the destination IP address.
c. The router then forwards the packet to the next hop (usually another router) associated with the chosen prefix.

16. Explain Scheduling mechanisms in routing and forwarding of packets

Scheduling mechanisms in routing and forwarding of packets determine the order in which packets are transmitted through a network. They include techniques such as FIFO (First-In-First-Out), priority queuing, weighted fair queuing, and round-robin scheduling. These mechanisms help optimize network performance by managing packet transmission based on factors like packet priority, available bandwidth, and congestion levels.

17. Explain Addressing the internet and what is IP subnetting

Addressing the Internet involves assigning unique IP addresses to devices connected to the Internet to enable communication. IP subnetting is the process of dividing a larger IP network into smaller subnetworks, or subnets, to improve network efficiency and manageability. It involves creating a subnet mask to determine the network and host portions of an IP address and allocating IP addresses accordingly

18. Explain Intra AS routing in the network with examples

Intra AS (Autonomous System) routing refers to routing within a single autonomous system, typically managed by a single organization or service provider. Examples include Interior Gateway Protocols **(IGPs)** such as **OSPF** (Open Shortest Path First) and **IS-IS** (Intermediate System to Intermediate System), which are used to exchange routing information within an AS and determine the best paths between routers within the AS.

19. Explain BGP

BGP (Border Gateway Protocol) is an exterior gateway protocol used to exchange routing information between different autonomous systems on the Internet. It is the protocol that routers in different ASes use to communicate and make routing decisions. BGP enables routers to dynamically learn and advertise routes to reach networks outside their own AS, facilitating global Internet connectivity.

20. Explain MPLS

MPLS: Speeding Up Traffic Flow with Labels

Multiprotocol Label Switching (MPLS) is a networking technology that prioritizes speed and efficiency in data forwarding across wide area networks (WANs). It works by utilizing labels instead of traditional IP addresses for routing packets.

Beyond IP Addresses:

- Traditional IP routing relies on IP addresses embedded in each packet header. Routers need to analyze these addresses at each hop to determine the next destination. This can be time-consuming, especially in large networks.
- MPLS introduces a layer of abstraction by assigning short labels to packets at the ingress (entry) point of the network. These labels are independent of IP addresses and remain constant throughout the MPLS domain (a network segment using MPLS).

Label Switching vs. IP Routing:

- Think of IP routing as looking up a complete address in a directory (routing table) at each stop. MPLS is like using a reference number (label) associated with the address, allowing for a faster lookup and forwarding process.

Benefits of MPLS:

- **Speed:** By using labels instead of IP addresses, MPLS streamlines packet forwarding, leading to faster data transfer.
- **Scalability:** MPLS scales well for large networks as label switching is faster than complex IP address lookups.
- **Traffic Engineering:** MPLS allows pre-configuring paths (MPLS tunnels) for specific traffic types, ensuring quality of service (QoS) for critical applications.
- **VPN-like Functionality:** MPLS can provide isolation between different network users, similar to a VPN, but without encryption overhead.

How MPLS Works:

- **Label Distribution Protocol (LDP):** MPLS relies on LDP, a signaling protocol, to distribute label information between MPLS routers. Routers exchange reachability information and agree on labels for specific destinations.
- **Label Stacking:** MPLS labels can be stacked in a header, allowing for traffic forwarding across multiple MPLS domains. Each router removes the top label and forwards the packet based on the remaining label.

21. Compare MPLS vs Traditional Network

Feature	**MPLS**	**Traditional IP Routing**
Routing Mechanism	Label Switching	IP Address lookup
Speed	Faster	Slower
Scalability	Scales well for large networks	Scales well for large networks
Traffic Engineering	Scales well for large networks	Scales well for large networks
Complexity	Scales well for large networks	Scales well for large networks
Cost	Scales well for large networks	Scales well for large networks

22. Describe the hidden terminal problem and its solution in wireless LAN

The hidden terminal problem is a challenge that occurs in wireless local area networks (WLANs) when two or more devices (terminals) cannot directly detect each other's transmissions, but they can communicate with a common access point (AP). This situation arises because wireless transmissions can be obstructed or attenuated by physical obstacles, leading to one terminal being hidden from another.

Here's a scenario to illustrate the hidden terminal problem:

Imagine three devices, A, B, and C, all connected to the same access point. Device A wants to communicate with Device B, and Device C wants to communicate with the access point. However, A and C are out of range of each other, so they cannot detect each other's transmissions. If both A and C transmit simultaneously to their intended recipients, their signals might interfere with each other, leading to packet collisions and data loss at both B and the access point.

The hidden terminal problem can cause degraded network performance, increased latency, and decreased throughput due to collisions and retransmissions.

One solution to the hidden terminal problem is the use of the Request to Send/Clear to Send (RTS/CTS) mechanism, which is a part of the IEEE 802.11 MAC protocol. Here's how it works:

1. **Request to Send (RTS)**: Before sending a data packet, the sender (device A) sends a short RTS frame to the access point, indicating its intention to transmit data to another device (device B).

2. **Clear to Send (CTS)**: Upon receiving the RTS frame, the access point responds with a CTS frame, confirming that the channel is clear for the intended transmission.
3. **Data Transmission**: Once device A receives the CTS frame, it can transmit the data packet to device B. Other devices within range, including device C, will defer their transmissions during the specified duration, preventing collisions.

23. Explain how CSMA/CD is used to detect and avoid collision in an Ethernet Network

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a protocol used in Ethernet networks to manage access to the shared communication medium, typically a coaxial cable or twisted pair cable. CSMA/CD helps to detect and mitigate collisions that can occur when multiple devices attempt to transmit data simultaneously on the network.

Working:

1. **Carrier Sense (CS):** Before transmitting data.
   i. A device listens to the communication medium to detect if it is idle.
   ii. If the medium is busy (another device is currently transmitting), the device waits until it becomes idle before attempting to transmit.
2. **Multiple Access (MA):** Once the medium is sensed as idle. The device begins transmitting its data frame onto the network. However, multiple devices may attempt to transmit simultaneously, especially if they sense the medium as idle at the same time.
3. **Collision Detection (CD):** While transmitting data, the device continues to monitor the network for collisions. Collisions occur when two or more devices transmit data simultaneously, causing their signals to interfere with each other and become garbled.
4. **Collision Detection Process:**
   i. If a device detects a collision during its transmission, it stops transmitting immediately and:
   ii. Sends a jamming signal to ensure all other devices on the network are aware of the collision. After sending the jamming signal, the device enters a backoff algorithm.
5. **Backoff Algorithm:** Upon detecting a collision, the device waits for a random amount of time before attempting to retransmit the data frame. The purpose of this backoff algorithm is to reduce the likelihood of another collision occurring when the device retransmits. The random backoff time helps to minimize the chance of multiple devices choosing the same time to retransmit, thereby reducing the probability of collisions.

24. Explain Error detection and correction in data transmission

Error detection and correction techniques are fundamental in ensuring the integrity and reliability of data transmission in communication systems. Here's a brief explanation of error detection and correction:

1. **Error Detection**: Error detection techniques allow the receiver to determine whether the received data contains any errors. If errors are detected, the receiver can request retransmission of the data or take corrective action based on the specific error detection method used. **Common error detection techniques include parity checking, checksums, and cyclic redundancy check (CRC).**
2. **Error Correction**: Error correction techniques go beyond error detection by not only identifying errors but also correcting them automatically. Error correction codes, such as Reed-Solomon codes and Hamming codes, are examples of error correction techniques used in various communication systems.

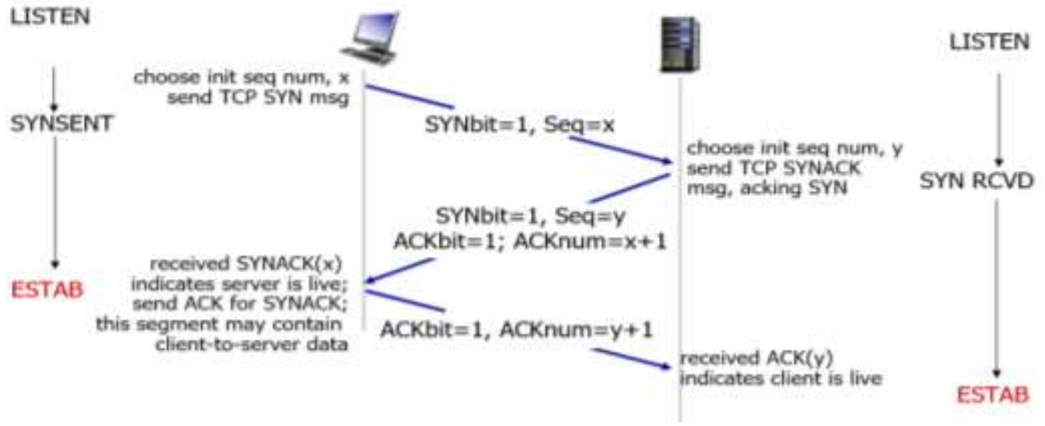
25. Describe with a diagram the Three-Way-Handshake Mechanism for establishing reliable communication and ensuring Data delivery

The most common method for establishing a reliable connection.

1. Initiated by the client sending a SYN (synchronize) message.
2. The server responds with a SYN-ACK (synchronize acknowledgment) message.
3. The client acknowledges the server's SYN with an ACK message.

This exchange synchronizes sequence numbers and acknowledges readiness to communicate

TCP 3-way handshake



26. **Explain Classful IP addressing and what is the main drawback of classful addressing**

Classful IP addressing is an addressing scheme used in the early days of the Internet, before the introduction of Classless Inter-Domain Routing (CIDR). In the classful addressing scheme, IP addresses are divided into classes, each designated for specific purposes and with predetermined address ranges.

The main classes used in classful addressing are:

Class	**Leading Bits**	**Range of First Octet**	**Network Portion**	**Host Portion**
Class A	0	0.0.0.0 to 127.255.255.255	First Octet	Last three octets
Class B	10	128.0.0.0 to 191.255.255.255	First two octets	Last two octets
Class C	110	192.0.0.0 to 223.255.255.255	First three octets	Last octet
Class D	1110	224.0.0.0 to 239.255.255.255	Reserved for multicast	-
Class E	1111	240.0.0.0 to 255.255.255.255	Reserved for experimental use	-

The main drawback of classful addressing is its inefficiency in address allocation and utilization. This inefficiency stems from several factors:

1. **Fixed Address Space**: This leads to the wastage of IP addresses, especially in networks where the number of hosts is much smaller than the maximum capacity allowed by the class.
2. **Address Exhaustion**: This issue became particularly problematic as the Internet grew, leading to the development and adoption of CIDR to address the scarcity of available IP addresses.

27. Give the meaning of the following terms
    I. Sequence number
    II. Window size in tcp
    III. Selective repeat and Go-Back-N
    IV. Subnetting and supinating
    V. Point-to-point link
    VI. Signal fading
    VII. Multipath
    VIII. Switched LAN

I. **Sequence Number**:

- In networking, a sequence number is a unique identifier assigned to each packet sent from a source to a destination. It helps in sequencing and reordering packets at the receiver's end to ensure data integrity and proper delivery.

II. **Window Size in TCP**:

- The window size in TCP (Transmission Control Protocol) refers to the maximum number of unacknowledged bytes that a sender can transmit before requiring an acknowledgment from the receiver. It plays a crucial role in flow control, determining the amount of data that can be in transit at any given time.

III. **Selective Repeat and Go-Back-N**:

- Selective Repeat and Go-Back-N are two error recovery techniques used in data communication protocols, particularly in sliding window protocols like TCP.
    - **Selective Repeat**: In selective repeat, the receiver individually acknowledges each correctly received packet and requests retransmission only for the missing or damaged packets.
    - **Go-Back-N**: In Go-Back-N, If an acknowledgment is not received within a certain time frame, the sender retransmits all unacknowledged packets from the beginning of the window.

IV. **Subnetting and Supernetting**:

- **Subnetting**: Subnetting is the process of dividing a single network into smaller, more manageable subnetworks. It helps in improving network efficiency
- **Supernetting**: Supernetting, also known as route aggregation, is the opposite of subnetting. It involves combining multiple smaller network addresses into a larger address block, thereby reducing the number of routing table entries and simplifying routing in large-scale networks.

V. **Point-to-Point Link**:

- A point-to-point link is a communication link between two devices, allowing data to be transmitted directly from one device to another without any intermediate devices or network segments. It provides a dedicated communication channel between the sender and receiver, ensuring efficient and reliable data transfer.

VI. **Signal Fading**:

- Signal fading refers to the attenuation or weakening of a transmitted signal as it travels through a communication medium, such as air or cables. Fading can occur due to factors like distance, obstacles, interference, and environmental conditions, leading to fluctuations in signal strength and quality.

VII. **Multipath**:

- Multipath refers to the phenomenon in which a transmitted signal reaches the receiver through multiple paths, resulting in signal reflections, phase shifts, and interference.

VIII. **Switched LAN**:

- A switched LAN (Local Area Network) is a network configuration in which network devices, such as computers, servers, and printers, are interconnected using network switches. Unlike traditional hub-based LANs, where all devices share the same broadcast domain and collision domain, switched LANs offer dedicated bandwidth and collision domains for each connected device, leading to improved performance and security.

28. Explain SDN in brief

Software-defined networking (SDN) is a networking architecture that decouples the network control plane from the data plane and supports network programmability. This allows for more centralized and flexible network management. SDN is particularly well-suited for campus, hospitality, and mobile networks, where there is a need to support a wide range of devices and services.

Data-plane switches:

- fast, simple, commodity switches implementing generalized data-plane forwarding in hardware
- flow (forwarding) table computed, installed under controller supervision
- API for table-based switch control (e.g., OpenFlow)

SDN controller (network OS):

- maintain network state information
- interacts with network control applications “above” via northbound API
- interacts with network switches “below” via southbound API
- implemented as a distributed system for performance, scalability, fault-tolerance, robustness

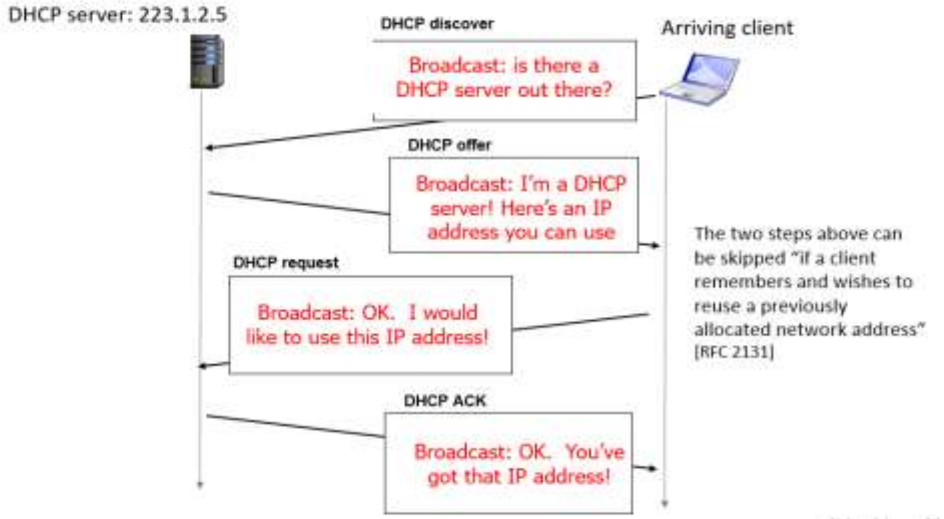
29. Describe How DHCP works

- host dynamically obtains an IP address from the network server when it “joins” the network
- can renew its lease on the address in use
- allows reuse of addresses (only hold address while connected/on)
- support for mobile users who join/leave the network

DHCP overview:

- host broadcasts DHCP discover msg
- DHCP server responds with DHCP offer msg
- host requests IP address: DHCP request msg
- DHCP server sends address: DHCP ack msg

DHCP client-server scenario



DHCP server: 223.1.2.5

Arriving client

DHCP discover

Broadcast: is there a DHCP server out there?

DHCP offer

Broadcast: I'm a DHCP server! Here's an IP address you can use

DHCP request

Broadcast: OK. I would like to use this IP address!

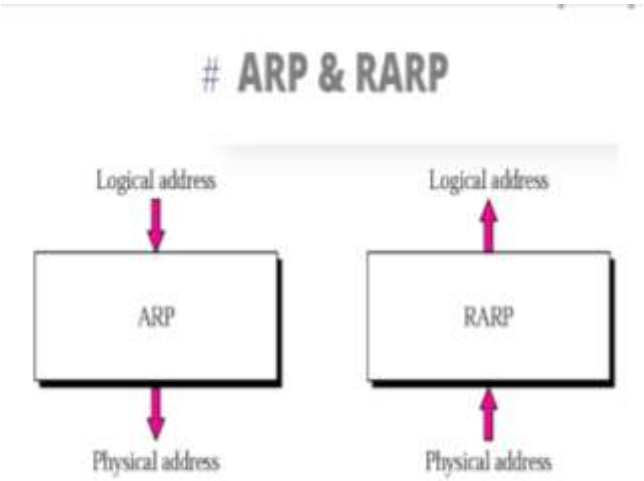
DHCP ACK

Broadcast: OK. You've got that IP address!

The two steps above can be skipped “if a client remembers and wishes to reuse a previously allocated network address” [RFC 2131]

30. Explain ARP in the Data link layer

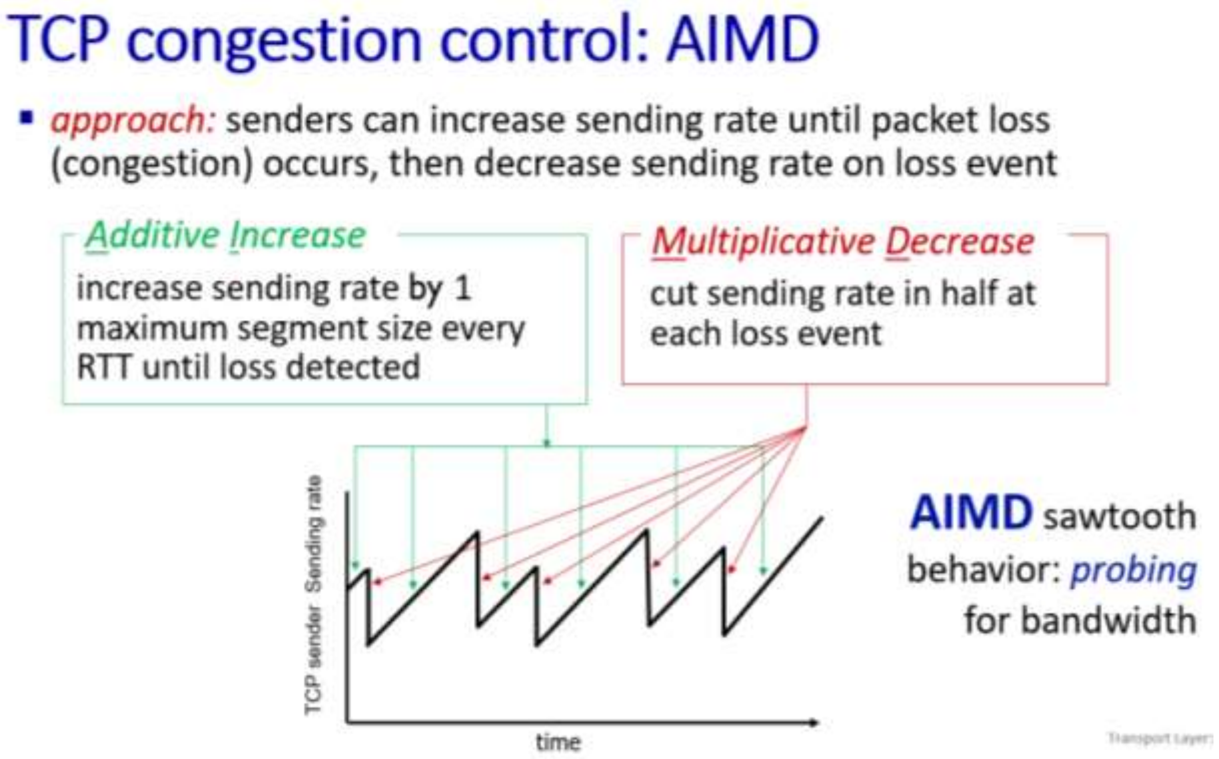
- **A Logical Address** is an Internet address. Its jurisdiction is universal, a logical address is unique universally.
- **A Physical address** is a local address. Its jurisdiction is a local network, it should be unique locally.
- **The Address Resolution Protocol(ARP)** maps a logical address to a physical address.



The ARP process

- The sender knows the IP address of the target.
- IP asks ARP to create an ARP request packet.
- The packet is encapsulated in a frame using the physical broadcast address(All FFs MAC address) as the destination address.
- All machines except the one targeted drop the packet.
- The target machine replies with an ARP Reply Packet containing its physical address. This packet is unicast.
- The sender receives the reply packet.
- The IP datagram is now encapsulated in a frame and is unicast to the target machine.

31. Explain Congestion Control Additive Increase and Multiplicative Decrease (AIMD)



TCP congestion control: AIMD

- *approach:* senders can increase sending rate until packet loss (congestion) occurs, then decrease sending rate on loss event

Additive Increase

increase sending rate by 1 maximum segment size every RTT until loss detected

Multiplicative Decrease

cut sending rate in half at each loss event

AIMD sawtooth behavior: *probing* for bandwidth

Transport Layer: