June 2023
Q.NO 1

a. List four(4) basic characteristics in network architecture to become a reliable and dynamic network.

Ans:- There are four basic characteristics in network architecture to create a reliable and dynamic network:-

1. Scalability:- The network should be able to accommodate growth in terms of the number of users, devices, and data traffic without significant degradation in performance. It should be easily expandable to meet increasing demands.

2. Resilience:- A reliable network architecture should be resilient to failures and disruptions. Redundancy and failover mechanisms should be in place to ensure continuous operation even in the event of hardware failures or network issues.

3. Security:- Robust security measures should be implemented to protect the network from unauthorized access, data breaches, and malicious activities. This includes encryption, authentication, access control, and intrusion detection/prevention systems.

4. Flexibility:- The network architecture should be flexible and adaptable to changing requirements and technologies. It should support the seamless integration of new devices, applications, and services, as well as accommodate changes in network traffic patterns and user needs over time.

b. Briefly explain the following network components:

Ans:-

i. End device: - An end device refers to any device that originates, consumes, or terminates data within a network. These devices are typically used by end-users to interact with the network and access its resources. Examples of end devices include computers, laptops, smartphones, tablets, printers, IP phones, and IoT (Internet of Things) devices. End devices are the ultimate sources or destinations of data in a network communication process.

ii. Intermediary device:- Intermediary devices are networking devices that facilitate communication between end devices within a network. These devices operate at various layers of the OSI (Open Systems Interconnection) model and perform different functions to ensure data delivery. Examples of intermediary devices include switches, routers, firewalls, hubs, bridges, and gateways. They help in routing, switching, filtering, and managing network traffic, ensuring efficient and secure data transmission.

iii. Network Media:- Network media, also known as network medium, refers to the physical or wireless communication channels used to transmit data signals between devices in a network. It serves as the conduit through which data is transmitted from one device to another. Network media can be categorized into two main types:

> **Guided Media:-** These are physical media that guide the transmission of data signals along a specific path. Examples include twisted-pair copper cables, coaxial cables, and fiber-optic cables.
>
> **Unguided Media:-** Also known as wireless media, these are communication channels that transmit data signals through the air or space without any physical pathway. Examples include radio waves, microwaves, and infrared signals.

c. Briefly explain the THREE (3) main functions of the Physical Layer.

Ans:- The Physical Layer, which is the first layer of the OSI (Open Systems Interconnection) model, serves as the interface between the networking hardware and the transmission medium. It is responsible for the following three main functions:-

1. Encoding and Signaling:- The Physical Layer converts digital data from the data link layer into signals suitable for transmission over the network medium. This process involves encoding the data into electrical, optical, or electromagnetic signals based on the characteristics of the transmission medium. Different encoding schemes, such as amplitude modulation, frequency modulation, and phase modulation, are used to represent binary data as analog signals for transmission.

2. Transmission Rate Management:- Another key function of the Physical Layer is to manage the transmission rate of data over the network medium. It ensures that data is transmitted at a rate compatible with both the transmitting and receiving devices. This involves regulating the timing and speed of data transmission to prevent data loss, signal distortion, or interference. The Physical Layer negotiates the transmission rate during the establishment of a connection, considering factors such as bandwidth, signal-to-noise ratio, and transmission distance.

3. Physical Topology:- The Physical Layer defines the physical layout or topology of the network, including the arrangement of devices and the transmission medium. It determines how devices are connected to each other and how data signals are transmitted between them. Common physical topologies include bus, star, ring, mesh, and hybrid topologies. The Physical Layer also manages the physical addressing of devices, such as MAC (Media Access Control) addresses, which are used for identifying devices on the network.

d. Classify the difference between UTP cabling and Fiber Optic cabling in term of:

Ans:-

i. Range of connection

- UTP Cabling:- UTP cabling typically supports shorter distances compared to fiber optic cabling. Generally, UTP cables can reliably transmit data up to a distance of 100 meters (328 feet) without requiring signal repeaters or amplifiers. Beyond this distance, signal degradation may occur, affecting the quality of data transmission.

- Fiber Optic Cabling:- Fiber optic cabling offers significantly greater range capabilities compared to UTP cabling. Fiber optic cables can transmit data over much longer distances without experiencing signal loss or degradation. Depending on the type of fiber and network architecture, fiber optic cables can support transmission distances ranging from a few meters to several kilometers without the need for signal repeaters.

ii. Supported bandwidth

- UTP Cabling:- UTP cabling typically supports lower bandwidth compared to fiber optic cabling. The bandwidth capacity of UTP cables depends on factors such as cable category (e.g., Cat 5e, Cat 6, Cat 6a) and the quality of installation. Generally, UTP cables are suitable for moderate to high-speed data transmission rates, such as those required for Ethernet networks (up to 10 Gbps).

- Fiber Optic Cabling:- Fiber optic cabling provides significantly higher bandwidth capabilities compared to UTP cabling. Fiber optic cables can support much greater data transmission rates over longer distances without signal degradation. Depending on the type of fiber (single-mode or multimode) and the network infrastructure, fiber optic cables can support transmission speeds ranging from tens of megabits per second (Mbps) to hundreds of gigabits per second (Gbps), or even terabits per second (Tbps) in advanced fiber optic networks.

Q.No :- 2

a. List Five (5) layer from OSI model.

Ans:- The OSI (Open Systems Interconnection) model consists of seven layers. Here are the first five layers:-

1. Physical Layer:- The lowest layer of the OSI model, responsible for the transmission and reception of raw data bits over a physical medium. It deals with the electrical, mechanical, and functional aspects of the physical connection between devices.

2. Data Link Layer:- The second layer of the OSI model, responsible for the reliable transfer of data between adjacent network nodes. It provides error detection and correction, as well as flow control, to ensure data integrity over the physical link.

3. Network Layer:- The third layer of the OSI model, responsible for the logical addressing, routing, and forwarding of data packets between different networks. It determines the best path for data transmission based on network conditions and addresses.

4. Transport Layer:- The fourth layer of the OSI model, responsible for end-to-end communication between devices across a network. It ensures reliable and orderly delivery of data by providing error detection, flow control, and segmentation/reassembly of data streams.

5. Session Layer:- The fifth layer of the OSI model, responsible for establishing, maintaining, and terminating communication sessions between applications. It manages session setup, synchronization, and teardown, as well as checkpointing and recovery mechanisms.

b. Explain the following process in data transmission:

i. Encoding:- Encoding is the process of converting digital data into a format suitable for transmission over a communication channel. In this process, the binary data (0s and 1s) from the sender's device is transformed into electrical, optical, or electromagnetic signals that can be transmitted over the transmission medium. Different encoding schemes are used depending on the type of transmission medium and the characteristics of the data. Common encoding techniques include amplitude modulation (AM), frequency modulation (FM), phase modulation (PM), and pulse code modulation (PCM). The encoded signals carry the information from the sender's device to the receiver's device, where they are decoded back into digital data for processing.

ii. Segmentation:- Segmentation is the process of dividing a large data stream into smaller segments or packets for transmission over a network. This is done to improve efficiency, reliability, and manageability of data transmission. In segmentation, the data stream is broken down into smaller units called segments, each of which is assigned a sequence number for identification and reassembly at the receiver's end. Segmentation allows for better utilization of network resources by enabling parallel transmission of multiple segments and facilitating error detection and recovery mechanisms, such as checksums and retransmission of lost segments.

iii. Encapsulation:- Encapsulation is the process of adding protocol-specific headers and trailers to data packets as they move through the layers of the OSI (Open Systems Interconnection) model. Each layer in the OSI model adds its own header (at the beginning) and trailer (at the end) to the data payload received from the higher layer, forming a protocol data unit (PDU) at each layer. The encapsulation process ensures that data is properly formatted and organized for transmission over the network. It also provides necessary information for routing, addressing, error detection, and data delivery at the receiving end. At the receiving end, the encapsulation process is reversed, with each layer stripping off its respective header and trailer before passing the data payload to the higher layer for processing. This allows for the proper interpretation and extraction of the original data by the receiving device.

c. Describe the following services that can be integrated in Broadband multi-services network:

i. IPTV (Internet Protocol Television):- IPTV delivers television content over an IP-based network, like the internet, instead of traditional satellite or cable formats. It enables access to

live TV channels, on-demand content, and interactive features via broadband. This service uses multicast or unicast streaming protocols and supports various devices like smart TVs, set-top boxes, computers, and mobile devices.

ii. VOD (Video-on-Demand):- VOD allows users to select and watch video content at their convenience from a library of movies, TV shows, and documentaries. The content is stored on servers and streamed upon user request. VOD platforms offer features like pause, rewind, fast forward, and offline viewing. It enhances entertainment options and user experience by providing personalized on-demand content.

iii. VoIP (Voice over Internet Protocol):- VoIP enables voice communication over IP networks using packet-switched protocols. It supports voice calls, video conferences, and multimedia messaging over broadband connections. VoIP services offer traditional telephone features like call forwarding, caller ID, and voicemail, along with advanced functionalities such as unified communications and mobility support. It provides cost-effective and feature-rich communication solutions for both residential and business users.

Q. No:- 3

a. What is the networking protocol?

Ans:- A networking protocol is a set of rules and conventions that govern the communication between devices on a computer network. These protocols define how data is formatted, transmitted, received, and interpreted across the network. They ensure that devices can exchange information reliably and efficiently, regardless of differences in hardware, operating systems, or software.

b. List any Five (5) network related protocols.

Ans:- Here are five network-related protocols:

1. Internet Protocol (IP):- IP is a core protocol responsible for addressing and routing data packets between devices on a network. It provides the foundation for communication on the internet and other IP-based networks.

2. Transmission Control Protocol (TCP):- TCP is a connection-oriented protocol that ensures reliable, ordered, and error-checked delivery of data packets between devices. It establishes and manages communication sessions, handling flow control and retransmission of lost packets.

3. User Datagram Protocol (UDP):- UDP is a connectionless protocol that provides a lightweight and fast way to transmit data packets between devices. Unlike TCP, UDP does not guarantee delivery or sequencing of packets, making it suitable for real-time applications like streaming media and online gaming.

4. Ethernet:- Ethernet is a widely used networking protocol that defines the rules for transmitting data packets over wired local area networks (LANs). It specifies the physical and data link layers of the OSI model, including standards for framing, addressing, and collision detection.

5. Domain Name System (DNS):- DNS is a protocol used to translate human-readable domain names (e.g., www.example.com) into numerical IP addresses that computers can understand. It enables users to access websites and other internet services using easy-to-remember domain names, rather than numerical IP addresses.

c. ARP spooling is a kind of network attack that manipulate the vulnerabilities in ARP Protocols. Explain how attackers can manipulate the ARP broadband message for the gateway.

Ans:- ARP (Address Resolution Protocol) spoofing, also known as ARP poisoning or ARP cache poisoning, is a type of network attack where an attacker exploits vulnerabilities in the ARP protocol to associate their own MAC (Media Access Control) address with the IP address of a legitimate network device, such as the gateway router. This manipulation allows the attacker to intercept, modify, or redirect network traffic intended for the legitimate device.

The way attackers can manipulate the ARP broadband message for the gateway:-

1. ARP Spoofing Setup:- The attacker begins by running software tools specifically designed for ARP spoofing. These tools allow the attacker to send forged ARP packets onto the local network, impersonating the IP address of the gateway router. The attacker's goal is to convince other devices on the network that their MAC address corresponds to the IP address of the gateway router.

2. Sending ARP Broadcasts:- The attacker's machine sends out forged ARP packets, typically ARP requests or replies, broadcasted across the local network. These packets contain the attacker's MAC address and the IP address of the gateway router, falsely claiming to be the legitimate gateway.

3. Spoofed ARP Responses:- When other devices on the network receive the forged ARP packets, they update their ARP cache tables with the MAC address provided by the attacker. As a result, these devices start sending network traffic intended for the gateway router to the attacker's machine instead.

4. Intercepting and Manipulating Traffic:- With the ARP spoofing attack successful, the attacker can intercept and manipulate network traffic passing through their machine. They can analyze the traffic for sensitive information, modify data packets, or launch further attacks, such as a man-in-the-middle attack.

5. Potential Impacts:- ARP spoofing attacks can lead to various security threats, including eavesdropping on sensitive data, session hijacking, or denial-of-service attacks. By controlling the flow of network traffic, attackers can execute malicious activities without detection.

6. Countermeasures:- To mitigate ARP spoofing attacks, network administrators can implement security measures such as ARP spoofing detection software, port security features on network switches, static ARP entries, and cryptographic network protocols like IPsec.

d. Briefly explain the following Ethernet frame forwarding methods of Cisco Switches:

i. Store-Forward:- Store-forward switching involves the switch receiving the entire Ethernet frame before it forwards it to the destination device. The switch verifies the integrity of the frame, including error checking with CRC (Cyclic Redundancy Check). After verification, the switch makes a forwarding decision based on the destination MAC address and then forwards the frame out of the appropriate port.

ii. Cut-Through:- Cut-through switching begins forwarding the frame as soon as it reads the destination MAC address in the frame's header. Unlike store-forward switching, cut-through switching does not wait for the entire frame to be received and stored before forwarding begins. This method offers lower latency but may forward corrupt or incomplete frames if errors are detected after forwarding starts.

e. List the FOUR (4) advantages of Packet Switching over Circuit Switching used in the Wide Area Networks. (WAN)

Ans:- Packet switching offers several advantages over circuit switching in Wide Area Networks (WANs):

1. Efficient Resource Utilization:- Packet switching allows for more efficient use of network resources as it dynamically allocates bandwidth on a per-packet basis, enabling multiple packets from different sources to share the same transmission medium simultaneously.
2. Flexible Routing and Path Selection:- Packet switching networks offer flexibility in routing and path selection, enabling packets to be routed dynamically based on network conditions and congestion levels. This allows for adaptive routing schemes that optimize network performance and reliability.
3. Scalability and Redundancy:- Packet-switched networks are scalable and support the addition of new nodes and devices without significant reconfiguration. They can incorporate redundancy and fault tolerance mechanisms, such as redundant paths and alternate routes, to ensure high availability and reliability.
4. Support for Various Data Types:- Packet switching is well-suited for transmitting different types of data, including voice, video, and multimedia content, over the same network infrastructure. Quality of service (QoS) mechanisms can prioritize packets to ensure that real-time and delay-sensitive applications receive adequate bandwidth and performance.

Q.NO:- 4

a. You have a block of IP addresses to be used to configure the networks in your organization. The available IP starts with 172.150.64.0/21. The IP should be distributed to following group:

- **Group A needs 400 IP currently with 100 IP to be reserved for future expansion**
- **Group B needs 250 IP currently with 150 IP to be reserved for future expansion**
- **Group C needs just 80 IP currently with 20 IP to be reserved for future expansion.**

State for each network group:

i. **The suitable network ID and subnet masks for each department with the consideration of current and future needs.**
ii. **The range of IP can be used for all the hosts in each department with assumption that the first available IP to be assigned as default gateway for each connection.**

You need to do the IP assignment effectively and give some reserve spaces to be used in case of company expansion.

Ans:-Let's go through each group:

Group A:

- Current requirement: 400 IP addresses + 100 reserved = 500 IP addresses
- Subnet size: 512 (2^9) - Sufficient to accommodate current and future needs
- Network ID: 172.150.64.0/23
- Subnet mask: 255.255.254.0
- Usable IP range: 172.150.64.1 to 172.150.65.254 (First IP reserved for default gateway)

Group B:

- Current requirement: 250 IP addresses + 150 reserved = 400 IP addresses
- Subnet size: 512 (2^9) - Sufficient to accommodate current and future needs
- Network ID: 172.150.66.0/23
- Subnet mask: 255.255.254.0
- Usable IP range: 172.150.66.1 to 172.150.67.254 (First IP reserved for default gateway)

Group C:

- Current requirement: 80 IP addresses + 20 reserved = 100 IP addresses
- Subnet size: 128 (2^7) - Sufficient to accommodate current and future needs
- Network ID: 172.150.68.0/25

- Subnet mask: 255.255.255.128
- Usable IP range: 172.150.68.1 to 172.150.68.126 (First IP reserved for default gateway)

With this allocation, each group has enough IP addresses for current use and reserves for future expansion, along with defined network IDs, subnet masks, and usable IP ranges.

b. List the FOUR (4) reasons why we need the IPv6.
Ans:- Here are four reasons why IPv6 is needed:
1. Address Space Exhaustion:- IPv4 addresses are running out due to the rapid growth of internet-connected devices. IPv6 provides a much larger address space compared to IPv4, allowing for an almost unlimited number of unique addresses. This ensures that every device can have its own globally unique IP address, supporting the proliferation of internet-connected devices such as IoT devices, smartphones, and smart appliances.
2. Addressing Efficiency:- IPv6 simplifies address assignment and management by using a more hierarchical and efficient addressing structure. It eliminates the need for techniques like Network Address Translation (NAT) used in IPv4, which can complicate network configurations and introduce performance overhead. With IPv6, every device can have a globally routable IP address, leading to simpler and more scalable network architectures.
3. Improved Security:- IPv6 includes built-in support for IPsec (Internet Protocol Security), a suite of protocols for securing IP communications. IPsec provides authentication, integrity, confidentiality, and anti-replay protection for network traffic, enhancing the overall security of IPv6-based networks. Additionally, IPv6 addresses some vulnerabilities present in IPv4, such as address spoofing and header manipulation, leading to improved network security.
4. Support for New Technologies:- IPv6 introduces several features and enhancements that support emerging technologies and applications. These include features like stateless address autoconfiguration, multicast addressing, and mobility support, which enable efficient and seamless communication in modern network environments. IPv6 also facilitates the deployment of new services and protocols, such as VoIP (Voice over Internet Protocol), video streaming, and cloud computing, by providing a robust and scalable networking foundation.

c. One PC with NIC MAC address 0001:4257:3844 is set to join the network. This node will get the auto-assigned IPv6 address using SLAAC mechanism. Determine the 64 bit Interface ID for this PC.
Ans:- To determine the 64-bit Interface ID for the PC using the SLAAC (Stateless Address Autoconfiguration) mechanism in IPv6, we need to follow these steps:

Given the MAC address: 0001:4257:3844
1. Convert the MAC address to binary format:
- 0001:4257:3844
- 0000 0000 0001 0100 0010 0101 0111 0011 1000 0100
2. Invert the U/L bit:
- The U/L bit is the 7th bit in the first byte of the MAC address. In this case, it's 0 (indicating a globally unique address), so we need to set it to 1 (indicating a locally administered address).
- After inversion: 0001 0000 0001 0100 0010 0101 0111 0011 1000 0100

3. Insert FFFE in the middle:
- Inserting FFFE in the middle of the MAC address: 0001:0000:0001:4257:3844
- In binary: 0000 0000 0001 0000 0000 0001 0100 0010 0101 0111 0011 1000 0100

4. Convert the modified MAC address to hexadecimal:

- 1000:1000:0101:0000:0111:0010:0101:1110:0011:1000:0100

5. Append the modified MAC address to the IPv6 prefix assigned by the network:
- Assuming the network prefix is 2001:db8:abcd:1234::/64:
- The Interface ID would be: 2001:db8:abcd:1234:1000:1000:0105:0000

So, the 64-bit Interface ID for the PC using the SLAAC mechanism is: 1000:1000:0105:0000

Q.NO:- 5

a. Explain the IPv6 Link-Local Unicast Address.

Ans:- IPv6 Link-Local Unicast Address is an automatically assigned address used for communication within a local network segment. It does not require manual configuration or external services like DHCP. These addresses are only valid within the local link and cannot be routed outside of it. Link-Local addresses have a specific address range defined in the fe80::/10 prefix. They are automatically generated for each interface based on the device's MAC address or randomly generated identifiers. These addresses play a crucial role in neighbor discovery, address resolution, and other network operations within the local subnet.

b.

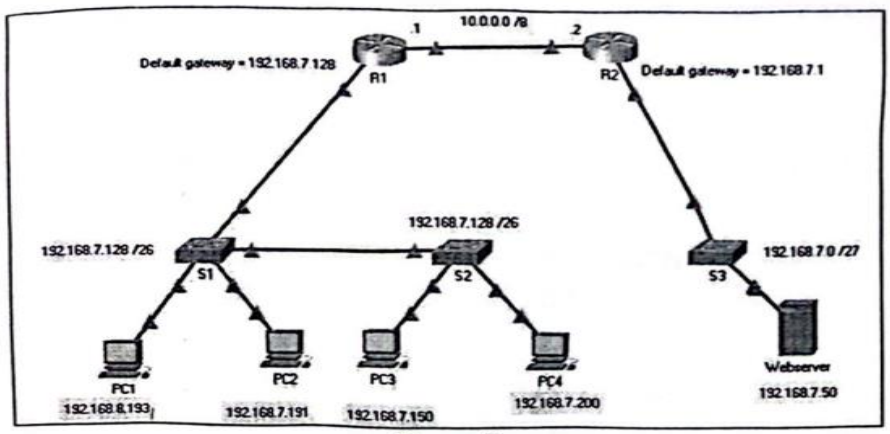

Figure 1

The network as in the figure 1 has been constructed with the IP for all end devices as stated in the figure.

i. Identify the FOUR (4) mistakenly set IP.
ii. Identify the TWO (2) networks that consider as the remote network of PC3.

Ans:- To identify the mistakenly set IP addresses and the remote networks of PC3, let's analyze the given network configuration:

i. Mistakenly Set IP Addresses:

1. The default gateway for R1 is mistakenly set as 192.168.7.1 instead of 192.168.7.128.
2. The IP address configured on R1 is 10000/8, which seems to be incorrect. It should be in the format of an IP address followed by a subnet mask, such as 192.168.7.1/8.
3. The IP address configured on PC2 is given as 192.168.7.191 192 1687.150, which seems to have formatting errors and is not a valid IP address.
4. The IP address configured on PC4 is given as 192.168.7.50 192.168.7.200, which also seems to have formatting errors and is not a valid IP address.

ii. Remote Networks of PC3:

1. The network with the IP range 192.168.7.128/26 is considered as a remote network of PC3.
2. The network with the IP range 192.168.7.192/27 is also considered as a remote network of PC3.

So, the identified mistakenly set IP addresses are:

1. Default gateway for R1: 192.168.7.1
2. IP address configured on R1: 10000/8
3. IP address configured on PC2: 192.168.7.191 192 1687.150
4. IP address configured on PC4: 192.168.7.50 192.168.7.200

And the remote networks of PC3 are:

1. 192.168.7.128/26
2. 192.168.7.192/27

c. Explain the three-way TCP handshake process.

Ans:- The three-way TCP handshake process is used to establish a connection between a client and a server in a TCP/IP network.

The process involves three steps: SYN, SYN-ACK, and ACK.

- First, the client sends a SYN (synchronize) packet to the server, indicating its intention to establish a connection.
- The server responds with a SYN-ACK (synchronize-acknowledgment) packet, acknowledging the client's request and indicating its readiness to establish a connection.
- Finally, the client sends an ACK (acknowledgment) packet back to the server, confirming the receipt of the server's response. At this point, the connection is established, and data transfer can begin.

d. Explain the Three Transport layer functions.

Ans:- The transport layer in the OSI model provides three primary functions: segmentation, multiplexing/demultiplexing, and error detection/correction.

1. Segmentation:- The transport layer breaks data from the session layer into smaller units called segments or datagrams before transmission over the network. Segmentation helps in efficient transmission and reassembly of data at the receiving end.

2. Multiplexing/Demultiplexing:- Multiplexing is the process of combining multiple data streams from different applications or sessions into a single stream for transmission over the network. Demultiplexing is the reverse process, where incoming data streams are separated and directed to the appropriate application or session.

3. Error Detection/Correction:- The transport layer includes mechanisms for error detection and correction to ensure the integrity of data transmission. This may involve checksums, acknowledgment/retransmission mechanisms, and error recovery algorithms to detect and correct errors that occur during data transmission.