1)Topology related

Compare Bus and Star topology:

1. Definition: The answer should begin by defining bus and star topology.
2. Network Structure: The answer should compare the network structure of both topologies.
3. Scalability: The answer should explain the scalability of both topologies.
4. Fault Tolerance: The answer should discuss the fault tolerance of both topologies.
5. Cost: The answer should compare the cost of implementing both topologies.

Compare Ring and Star Topology:

1. Definition: The answer should begin by defining ring and star topology.
2. Network Structure: The answer should compare the network structure of both topologies.
3. Scalability: The answer should explain the scalability of both topologies.
4. Fault Tolerance: The answer should discuss the fault tolerance of both topologies.
5. Cost: The answer should compare the cost of implementing both topologies.

Is there any relation between transmission media and topology:

1. Definition: The answer should begin by defining transmission media and topology.
2. Connection: The answer should discuss the connection between transmission media and topology.
3. Distance: The answer should also discuss the distance limitations of different transmission media and their impact on topology.
4. Performance: The answer should explain how the choice of transmission media and topology can impact the performance of the network.
5. Flexibility: Finally, the answer should discuss the flexibility of transmission media and topology in meeting the changing needs of the network.

2)Switching related:

Compare message switching and circuit switching:

1. Definition: The answer should begin by defining message switching and circuit switching.
2. Network Efficiency: The answer should compare the network efficiency of message switching and circuit switching.
3. Delay: The answer should discuss the delay involved in message switching and circuit switching.
4. Scalability: The answer should explain the scalability of message switching and circuit switching.
5. Cost: The answer should compare the cost of implementing message switching and circuit switching.

Differentiate between message switching, circuit switching and packet switching:

1. Definition of each switching method.
2. The process of establishing a connection in each method.
3. The types of data transmitted in each method.
4. The advantages and disadvantages of each method.
5. Real-world examples of each method and where they are commonly used.

3)LAN,MAN,WAN:

Compare LAN, WAN and MAN:

1. Definition: LAN, MAN, and WAN.
2. Size: The range of each type.
3. Ownership: Organization and extent.
4. Connection: Type of connection – connectionless and connection-oriented.
5. Speed: LANs up to 10Gbps or more, while MANs and WANs may offer slower connections due to distance and infrastructure limitations.
6. Topology: Describe topology implemented in each type.
7. Cost: Compare the cost-effectiveness of each type.
8. Security: Compare the level of security provided by each type.
9. Applications: Mention various applications ranging from home applications to world-wide applications.
10. Examples: Give suitable example of each.

Examine the advantages of LAN, MAN, and WAN-

Explanation of LAN, MAN, and WAN in terms of geographic coverage and connectivity

1. Advantages of LAN, MAN, and WAN, such as high-speed connectivity, improved communication, and resource sharing
2. Comparison of the advantages of LAN, MAN, and WAN
3. Importance of network speed, scalability, and business continuity for organizations
4. Role of LAN, MAN, and WAN in improving organizational efficiency and productivity

4)OSI model:

Draw and explain the OSI Reference Model:

1. Definition of the OSI Reference Model and its importance in the field of networking.
2. Draw a detailed diagram of the OSI Reference model with correct order of the layers involved.
3. Brief overview of the seven layers of the OSI Reference Model, highlighting their functions.
4. Detailed explanation of the each layer, their roles in transmitting data between devices, and examples of their implementation.
5. The advantages of the OSI Reference Model, such as the standardization of network communication, the ability to troubleshoot and diagnose network issues, and the compatibility of devices from different manufacturers.
6. Limitations of the OSI Reference Model, such as its complexity and the difficulty of implementing it in real-world networks.
7. Conclusion, summarizing the importance of the OSI Reference Model in networking and emphasizing the need for network administrators to understand it for effective communication and troubleshooting.
8. CRC and checksum:

Generate the CRC code for a data word 110010101. The divisor 10101. Check whether there are errors in the received codeword.:

1) Write the data word and the divisor in binary format.

2) Append the number of zeroes equal to the degree of the divisor (4 in this case) to the data word.

3) Divide the resulting polynomial (110010101000) by the divisor (10101) using binary division.

4) Find the remainder obtained from the division (1100).

5) Append the remainder to the original data word to create the codeword (110010101100).

6) To check for errors in the received codeword, repeat steps 3 and 4 using the received codeword instead of the data word.

7) If the remainder obtained in step 4 is zero, there are no errors in the received codeword. Otherwise, there is an error.

Short note on CRC and checksum:

1. Definition: Briefly explain what CRC (Cyclic Redundancy Check) and checksum are, and how they are used in data communication.
2. Computation: Explain how CRC and checksum are calculated. Describe the mathematical algorithms involved in generating the checksum and CRC values for a given data block.
3. Error Detection: Explain how CRC and checksum are used for error detection. Describe how errors can be detected by comparing the checksum or CRC value computed at the receiver end with the one transmitted by the sender.
4. Strength: Discuss the strengths and limitations of both CRC and checksum. Explain why CRC is considered to be a more powerful and reliable error detection technique compared to checksum.

5) Applications: Provide examples of applications where CRC and checksum are used. Explain why one technique may be preferred over the other in certain applications based on their specific requirements.

1. ALOHA related:

Explain ALOHA and Slotted ALOHA:

1. Introduction to ALOHA and Slotted ALOHA as two early methods for sharing a single communication channel among multiple users.
2. Explanation of how ALOHA works by allowing users to transmit data at any time, but also risking data collisions if multiple users transmit at the same time.
3. Discussion of the advantages and disadvantages of ALOHA, including its simplicity but also its high collision rate.
4. Explanation of how Slotted ALOHA improves upon ALOHA by dividing time into discrete slots and allowing users to transmit data only at the beginning of each slot.
5. Discussion of the advantages and disadvantages of Slotted ALOHA, including its reduced collision rate but also its potential for idle slots if no user has data to transmit.
6. Conclusion, summarizing the key points about ALOHA and Slotted ALOHA and highlighting their historical significance as early methods for shared communication channel access.

Examine different types of ALOHA:

1. Introduction to ALOHA as a method for shared communication channel access among multiple users.
2. Explanation of pure ALOHA as the original version of ALOHA, in which users can transmit data at any time and risk data collisions if multiple users transmit at the same time.
3. Discussion of slotted ALOHA as an improved version of ALOHA, in which time is divided into discrete slots and users can transmit data only at the beginning of each slot.
4. Explanation of adaptive ALOHA as a further improvement over slotted ALOHA, in which the number of slots is dynamically adjusted based on the network load and the number of active users.
5. Comparison of the different types of ALOHA, highlighting the advantages and disadvantages of each approach in terms of collision rate, throughput, and complexity.
6. Conclusion, summarizing the key points about the different types of ALOHA and their relative strengths and weaknesses.

What is pure ALOHA and slotted ALOHA, what is efficiency, justify your answer.

1. Explanation of pure ALOHA as a method for shared communication channel access among multiple users, in which users can transmit data at any time and risk data collisions if multiple users transmit at the same time.
2. Description of slotted ALOHA as an improvement over pure ALOHA, in which time is divided into discrete slots and users can transmit data only at the beginning of each slot.
3. Explanation of efficiency in the context of ALOHA, as the ratio of the number of successfully transmitted frames to the total number of frames transmitted.
4. Justification of why slotted ALOHA is more efficient than pure ALOHA, by highlighting that the probability of collision in slotted ALOHA is reduced since users can only transmit at the beginning of each time slot, whereas in pure ALOHA users can transmit at any time and collisions are more likely to occur.
5. Conclusion, summarizing the key points about pure ALOHA and slotted ALOHA, and highlighting the relative advantages and disadvantages of each approach in terms of efficiency and other factors.

Compare pure and slotted ALOHA:

1. Definition of pure ALOHA and slotted ALOHA as two methods for shared communication channel access among multiple users.
2. Explanation of how pure ALOHA allows users to transmit data at any time, while in slotted ALOHA, time is divided into discrete slots and users can only transmit data at the beginning of each slot.
3. Comparison of the efficiency of pure ALOHA and slotted ALOHA, highlighting that pure ALOHA has lower efficiency due to a higher probability of data collisions, while slotted ALOHA has higher efficiency due to a lower probability of data collisions.
4. Discussion of the advantages and disadvantages of pure ALOHA and slotted ALOHA. For example, pure ALOHA is simpler to implement and requires less coordination among users, but has lower efficiency and a higher probability of collisions. Slotted ALOHA, on the other hand, has higher efficiency and a lower probability of collisions, but requires more coordination and synchronization among users.
5. Conclusion, summarizing the key differences between pure ALOHA and slotted ALOHA and highlighting the factors that could influence the choice of one method over the other in different network scenarios.
6. Transmission media:

Compare wired and wireless media-

1. Definition of wired and wireless media and their importance in network communication.
2. Comparison of the physical characteristics of wired and wireless media, including the use of cables or airwaves to transmit data.
3. Discussion of the advantages of wired media, such as higher bandwidth, reliability, and security due to the physical connection.
4. Discussion of the advantages of wireless media, such as mobility, flexibility, and ease of installation.
5. Comparison of the limitations of wired and wireless media, including potential cable damage or interference for wired media, and signal loss, interference, or security concerns for wireless media.
6. Conclusion, summarizing the differences and similarities between wired and wireless media, and emphasizing the importance of choosing the appropriate medium based on the specific network requirements and constraints.

Explain the different transmission media in networking:

1. Definition of transmission media and its importance in network communication
2. Overview of the two main types of transmission media, wired and wireless.
3. Explanation of the physical characteristics of wired transmission media, such as twisted-pair cables, coaxial cables, and fibre-optic cables, and their respective advantages and limitations.
4. Explanation of the physical characteristics of wireless transmission media, such as radio waves, microwaves, and infrared signals, and their respective advantages and limitations.
5. Comparison of the advantages and limitations of wired and wireless transmission media, including factors such as bandwidth, range, reliability, and security.

Explain guided transmission media in detail:

1. Definition of guided transmission media and its importance in network communication.
2. Overview of the different types of guided transmission media with diagrams of each, including twisted-pair cables, coaxial cables, and fiber-optic cables.
3. Explanation of the physical characteristics and advantages of each type of guided transmission media, including bandwidth, distance, and immunity to noise and interference.
4. Comparison of the advantages and limitations of each type of guided transmission media.
5. Discussion of common applications for guided transmission media, including LANs, WANs, and the internet.

8)IPV4

Header format:

1. Brief introduction to IPv4 protocol and the importance of its header in network communication.
2. Overview of the structure of an IPv4 packet header.
3. Explanation of the Version, Header Length, Total Length, Time to Live, Protocol, Source IP Address, Destination IP Address, and Header Checksum fields and their respective roles in the header.
4. Conclusion, summarizing the function and significance of each field in the IPv4 header.

9)TCP and UDP

Compare TCP and UDP:

1. Definition and basic functionality of TCP and UDP.
2. Differences in their communication model, such as connection-oriented vs. connectionless.
3. Differences in their reliability and error-checking mechanisms.
4. Applications and use cases for TCP and UDP, including common protocols and services that use each.
5. Advantages and disadvantages of TCP and UDP, such as speed, resource utilization, and suitability for specific types of data transmission.

10)Routing:

What is routing in network , explain shortest routing path routing protocol?

1) Definition of routing in computer networking

2) Explanation of why routing is important in computer networks

3) Types of routing protocols (e.g. distance-vector, link-state, path-vector)

4) Brief overview of shortest path routing protocol

5) Explanation of how shortest path routing protocol works

6) Advantages and disadvantages of shortest path routing protocol

7) Real-world examples of shortest path routing protocol (e.g. OSPF, IS-IS)

8) Comparison of shortest path routing protocol with other routing protocols.

What are three main functions of network layer?What is routing ?What is shortest path routing?

1) Network layer: Definition and overview of its functions

2) Three main functions of network layer: forwarding, routing, and addressing

3) Forwarding: Transmitting a packet from one interface to another interface within the same network

4) Routing: The process of finding a path for the packet to reach its destination network

5) Shortest path routing: Overview and definition of the concept

6) Routing protocols: Definition and examples

7) Link-state routing protocols: Definition and examples

8) Distance-vector routing protocols: Definition and examples

9) Shortest path routing protocol: Explanation of its operation

10) Dijkstra's algorithm: Explanation of its use in finding the shortest path routing

11)congestion related:

What is congestion and what are its causes? Explain Token bucket algorithm:

1. Introduction to congestion and its causes, including the impact of congestion on network performance.
2. Explanation of the Token Bucket algorithm, which is a popular method for controlling network traffic and avoiding congestion.
3. Discussion of how the Token Bucket algorithm works to regulate traffic and prevent congestion.
4. Explanation of the advantages and disadvantages of using the Token Bucket algorithm for congestion control.
5. Conclusion, summarizing the key points about congestion and the Token Bucket algorithm, and emphasizing the importance of effective congestion control mechanisms in network design.

How congestion is controlled in TCP:

1. Explanation of the role of TCP congestion control mechanisms in preventing network congestion and improving network performance.
2. Discussion of the main TCP congestion control mechanisms, including slow start, congestion avoidance, and fast retransmit/fast recovery.
3. Explanation of how TCP slow start works to gradually increase the amount of data sent by a TCP connection until the network capacity is reached.
4. Discussion of how TCP congestion avoidance works to prevent network congestion by dynamically adjusting the sending rate based on the network congestion level.
5. Conclusion, summarizing the key points about TCP congestion control mechanisms and highlighting their importance in ensuring efficient and reliable data transmission in networks.

12)Stop and wait protocol:

Suppose you develop an error recovery protocol for a link that is unreliable and delay-sensitive, which of the following protocol you would choose - 1)stop and wait, 2) selective repeat, 3)Go back

1. If the link is unreliable and delay-sensitive, the best error recovery protocol to choose would be the Stop-and-Wait protocol.
2. This is because the Stop-and-Wait protocol is a simple protocol that only transmits one packet at a time, waits for an acknowledgment before transmitting the next packet, and retransmits a packet if an acknowledgment is not received within a specified time.
3. Selective Repeat and Go-Back-N protocols are more complex and transmit multiple packets before waiting for an acknowledgment, making them less suitable for a link that is delay-sensitive.
4. In contrast, Stop-and-Wait is a more conservative approach, which would be better suited to an unreliable and delay-sensitive link.

What is difference between stop and wait and sliding window protocol ? Explain selective repeat protocol?

1. Definition of Stop-and-Wait and Sliding Window protocols.
2. Key difference between Stop-and-Wait and Sliding Window protocols.
3. Explanation of how Selective Repeat protocol works.
4. Advantages of Selective Repeat protocol over Stop-and-Wait and Sliding Window protocols.
5. Real-world examples of where Selective Repeat protocol is commonly used.

13)CSMA

CSMA/CD:

1. CSMA/CD is a media access control protocol used in Ethernet networks.
2. It helps to avoid collisions when multiple nodes try to transmit data simultaneously on a shared medium.
3. Before transmitting, a node listens for any ongoing transmission. If the medium is idle, it starts transmitting immediately.
4. If multiple nodes transmit at the same time and a collision occurs, they stop transmission, wait for a random amount of time, and then retransmit.
5. CSMA/CD is used in half-duplex Ethernet networks and has been replaced by CSMA/CA in wireless networks.

What is p-persistent CSMA?

1. Explanation of the medium access control sublayer.
2. Explanation of multiple access protocol with diagram.
3. Also, you need to explain about the random access protocol along with CSMA under which p-persistent falls.
4. Draw the CSMA flowchart.
5. Explain the p-persistent and conclude how it can reduce the chance of collision and improves the efficiency.

14)HDLC

What is HDLC, compare frame formats, I frame, S frame, and U frame.  
OR  
Explain HDLC protocol along with its frame structure:

1. HDLC is a protocol used for communication between network equipment in a network.
2. HDLC uses three different frame types: I, S, and U.
3. I frames are for data transfer, S frames are for supervisory functions, and U frames are for unnumbered functions.
4. Each frame type has a different format, with I frames having a fixed-length format that includes sequence numbers and data payloads, S frames having a variable-length format that includes sequence numbers and control functions, and U frames having a variable-length format that includes control functions and optional information.
5. The different frame types are used for different purposes in network communication, and have their own advantages and disadvantages depending on the specific network scenario.

15)IP address and subnet mask

Explain IP address and subnet mask:

1. An IP address is a unique numerical identifier assigned to each device on a network that uses the Internet Protocol (IP) for communication.
2. IP addresses are 32-bit numbers, typically represented in dotted decimal notation, such as 192.168.1.1.
3. IP addresses are divided into two parts: network and host. The network part identifies the network to which the device belongs, while the host part identifies the specific device within that network.
4. A subnet mask is a 32-bit number that separates the network and host portions of an IP address.
5. The subnet mask is used to determine the network portion of an IP address, which is used for routing and communication between networks.

What is IP addressing?How it is classified?How is subnet addressing performed ?

1. IP Addressing: A unique numerical identifier assigned to each device connected to a network that uses the Internet Protocol for communication.
2. IP Address Classification: IP addresses are classified into different classes, A, B, C, D, and E, based on the range of the first octet.
3. Subnet Addressing: Subnet addressing is the process of dividing a network into smaller subnetworks, called subnets, to improve network efficiency and security.
4. Subnet Mask: A subnet mask is a 32-bit number that helps to identify the network and host portions of an IP address.
5. Subnet Address Calculation: Subnet addresses are calculated by performing a bitwise AND operation between the IP address and the subnet mask to identify the network portion, and the remaining bits are used to identify the host portion.

|  |  |  |
| --- | --- | --- |
| ## Most Probable Questions |  |  |
| 1)OSI model 👍 |  |  |
| 2)ALOHA |  |  |
| 3)Transmission media |  |  |
| 4)IPV4 |  |  |
| 5)Congestion control |  |  |
| 6)HDLC |  |  |
| 7)IP address and subnet mask |  |  |
|  |  |  |