**Q1.Data Link Layer**

1. What is inside an Ethernet Frame?

They are **Ethernet header (Preamble, SFD, Destination, Source and Type), Encapsulated data (Data and Pad), and Ethernet trailer (FCS)**.

1. What is the maximum and minimum payload in Ethernet Frame?

* Maximum payload size in Ethernet II framing (standard Ethernet): 1500 bytes
* Minimum payload size in Ethernet II framing (standard Ethernet): 46 bytes

1. What is a collision ? When does it occur ? How to avoid collisions in the network?

A collision is the result of two devices on the same Ethernet network attempting to transmit data at exactly the same time. When devices attempt to use a medium simultaneously. Change it to full duplex mode.

**Q2.Network layer**

1. **How to determine Network portion and Host portion ?**

Use a 32 bit pattern called subnet mask

1. **Which protocol is in the network layer? What is this protocol used for?**

IP version 4 and IP version 6, these protocols are used to provide end to end connectivity across multiple link layer networks.

1. **How many types of IPV4 address?**

3, unicast address, multicast address, and broadcast address.

1. **How to find network address, usable ip range and broadcast address**

32 - network bits or subnet mask we get an x number, the address for the next network should plus 2^x addresses to the current network. From that we minus 1 address then we get the broadcast address for the current network then minus 1 more for usable ip network addresses.

1. **What is a valid host ip address ?**

A valid host address means no broadcast address and no subnet address can be used and means that not all 9 bits of the host portion can be all 1 or all 0.

1. **How to write IPv6 in abbreviated form and in full unabbreviated form?**

Rule 1: Remove omitting leading 0s

01AB to 1AB

09F0 to 9F0

0A00 to A00

00AB to AB

Rule 2:

Replace single, contiguous string of 1 or more 16 bit segments consisting all 0 with a ::

Double colon “::” can only be used 1

1. **How to find registry/isp/site prefix in ipV6 ?**

registry: /23

isp: /32

site: /48

subnet: /64

**Q3. Transport layer**

1. Sequence number, acknowledgement , window size in TCP

* Sequence Number: Sequence number in TCP is a unique value assigned to each byte of data transmitted, allowing the receiver to reorder and reassemble the data correctly.
* Acknowledgement Number:Acknowledgement (ACK) number in TCP is a value sent by the receiver to indicate the next expected sequence number it is expecting to receive, acknowledging the receipt of the previously received data.
* Window Size: Window size in TCP is the amount of data, in bytes, that a sender can transmit without receiving an acknowledgment from the receiver. It helps regulate the flow of data and prevents congestion in the network.

1. Describe 3 way handshake in TCP

* The first device (the client) sends a SYN (synchronize) packet to the second device (the server).
* The server responds with a SYN-ACK (synchronize-acknowledge) packet, indicating that it has received the SYN packet and is willing to establish a connection.
* The client responds with an ACK (acknowledge) packet, confirming that it has received the SYN-ACK packet.

1. **What is TCP ?**

* TCP is a reliable and connection-oriented communication protocol used in computer networks for ensuring accurate data delivery.

1. **What is UDP ?**

* UDP is a connectionless and unreliable communication protocol used in computer networks for fast data transmission without error checking or flow control.

1. **Difference between TCP and UDP ? What are advantages and disadvantages**

* TCP is reliable, connection-oriented, and has higher overhead, while UDP is unreliable, connectionless, and has lower overhead. TCP is suitable for applications requiring high data integrity, while UDP is faster and more suitable for real-time applications.

1. **How does TCP control flow ?**

* TCP controls flow using a sliding window mechanism. The receiver advertises its window size, indicating available buffer space. The sender adjusts its sending rate based on the window size and receiver's acknowledgments. TCP also includes congestion avoidance mechanisms.

**Q4.Generic networking**

**How is the MAC table built in Switch ?**

* The MAC table in a switch is built through MAC learning, where the switch adds or updates entries based on the source MAC addresses of incoming frames. This allows the switch to efficiently forward frames to the correct destination port based on the MAC address in the table.

**What is ARP used for ?**

* ARP is used to map an IP address to a MAC address in a local network, allowing devices to communicate with each other at the data link layer.

**How is the broadcast message sent ?**

* Broadcast messages are sent to all devices in a network segment using a special MAC address (FF:FF:FF:FF:FF:FF) as the destination. The message is encapsulated into a data link layer frame, transmitted over the network segment, and received by all devices in that segment.

**Router on a stick ?**

* "Router on a stick" is a networking configuration that uses a single router interface to handle multiple VLANs by creating logical subinterfaces. It enables inter-VLAN routing and network segmentation.

**Q5. STP**

**BID,BPDU,path cost ?**

* BID (Bridge ID) is a unique identifier used by bridges in STP.
* BPDU (Bridge Protocol Data Unit) is a special frame used to exchange network topology information.
* Path cost is a value associated with each link used to determine the shortest path to the root bridge in STP.

**What is redundancy ?**

* STP redundancy: Multiple links between switches for fault tolerance and network availability. STP process determines active and standby links. Improves reliability, requires proper configuration.

**How to prevent loops in a switched network ?**

* STP prevents loops in a switched network by selecting a root bridge, calculating shortest paths, blocking redundant paths, and monitoring network changes. Ensures network stability and prevents broadcast storms.

**What is STP used for ?**

* STP prevents loops in Ethernet networks for network stability by selecting a root bridge, calculating shortest paths, blocking redundant paths, and monitoring network changes.

**Q6. Lan design and Link aggregation**

**How many layers in a hierarchical network ?**

3 layers - Access, Distribution, Core

**Main features of each layer?**

* Access Layer: Local network access, port security, VLAN assignment.
* Distribution Layer: Traffic aggregation, interconnection, VLAN routing, policy-based connectivity.
* Core Layer: High-speed switching, high availability, fault tolerance.

**How to find maximum network diameter ?**

* Methods to find maximum network diameter: Physical measurement
* Network documentation
* Network simulation
* Routing protocols (OSPF, RIP)

**Protocol used on etherchannel comparison ?**

* PAgP: Cisco, auto link aggregation, limited to Cisco devices.
* LACP: Open, interoperability, may require manual config.
* Both offer dynamic negotiation, link integrity. Choose based on compatibility, requirements.

**Q7. Ethernet switching and VLAN**

**VLAN, trunk ports and access ports ?**

* VLANs: Logical switch division.
* Trunk ports: Carry traffic from multiple VLANs.
* Access ports: Connect end devices to VLANs.
* Trunk for inter-switch, access for end devices.

**What are best practices when configuring a router on a stick ?**

* Use dedicated VLAN for inter-VLAN routing.
* Configure VLAN tagging on router and switch trunk.
* Use subinterfaces with dot1q encapsulation.

**Q8. Wireless network**

**SSID**

* SSID stands for Service Set Identifier. It is a name used to identify a wireless network.

**Collision on wireless network ?**

* Collisions occur in wireless networks when devices simultaneously transmit, impacting performance. CSMA/CA minimizes collisions.

**How to avoid collisions on wireless networks ?**

* Use CSMA/CA
* Choose clear channel
* Optimize signal strength

**What is CSMA/CA? How does it work ?**

* CSMA/CA is a wireless protocol that avoids collisions by listening for clear channels and using backoff times.

**Security in wireless networks ?**

* Wireless network security: encryption, authentication, access control, monitoring to prevent unauthorized access, data breaches.