# Q1 - Data link layer

1. What is the job of the data link layer?

* Encapsulate upper layer data into the appropriate frame format for transmission across the physical media.
* Control access to the media to avoid collisions.
* Performing error checking to detect frame corruption.

1. What is the position of the data link layer in the OSI model?

* Data link layer is layer 2. Composed of the LLC (logical link control) and MAC (media access control) sublayers.
* LLC is implemented in software and interfaces the upper layers with the hardware.
* MAC is implemented in software and handles data encapsulation and media access control.

1. What fields are in a data link frame?

* Frame start, frame stop: Bit patterns to signal the start and end of the frame.
* Preamble: Synchronizes the receiver’s clock.
* Addresses: MAC addresses of source and destination nodes.
* Type: The type of layer 3 protocol used in the data payload.
* Quality control: Type of data being transmitted, used to give priority to real time data.
* Frame check sequence: A checksum used to validate the integrity of the frame.
* Data: Data from the upper layer. Minimum is 46 bytes and maximum is 1500 bytes. The minimum exists to ensure that the sending device listens for long enough to detect a potential collision.

1. What are WAN topologies?

* Point-to-point
* Hub and spoke
* Full mesh

1. What are some LAN media access control mechanisms?

* Contention-based: CSMA/CD for Ethernet networks, CSMA/CA for wireless networks. (Any device can send, collisions exist but there are mechanisms to resolve)
* Control-based: Token ring, FDDI (One at a time, no collisions exist, legacy.)

1. What is Ethernet?

Ethernet is a family of network technology for wired communication. It is defined by the protocols in the data link and physical layers.

1. What is a MAC address?

A MAC address is used to identify a layer 2 node. It is uniquely assigned to NICs. A MAC address is 48 bits (or 6 bytes) long. The first 3 bytes is an Organizationally Unique Identifier (OUI) assigned by the IEEE to vendors.

1. What is CSMA/CD?

CSMA/CD is a media access control mechanism used in Ethernet networks to avoid collisions. Devices sharing a media will first have to listen to the media to see if any device is transmitting data. They will wait until the media is clear before sending data. If a collision happens, the sending device that detects this collision will send a jamming signal to ensure that the collision occurs long enough for both ends to pick it up. Then the sending devices each wait for a random period of time before retransmitting.

1. What is CSMA/CA?

CSMA/CA is a media access control mechanism used in wireless networks to avoid collisions. Devices sharing the wireless media will listen to see if the media is clear before sending a notification to a controller expressing their intent to transmit data. They will have to receive a response from the controller before transmitting.

# Q2 - Network layer

1. What is the job of the network layer?

* Provides logical addressing and data routing between hosts on different networks.
* Encapsulation and decapsulation.

1. What is IPv4 and IPv6?

These are both network layer protocols that facilitate communication between devices on different networks. These protocols assign a network unique address to each device to identify them. IPv4 uses 32-bit addresses whereas IPv6 uses 128-bit addresses.

An IPv4 header is 20 bytes long while an IPv6 header is 40 bytes long. However, the IPv6 header is much simpler.

Subnet masks need at least eight 1 bits and at least two 0 bits.

# Q3 - Transport layer

1. What is the job of the transport layer?

* Provides end-to-end communication between applications running on different hosts.
* Ensures data is delivered reliably to end applications.

1. What is TCP?

TCP is a reliable, connection-oriented protocol for communicating between applications. It provides flow control, congestion control, and error checking mechanisms to guarantee correct and ordered delivery. TCP establishes a connection between the source and destination device before transmitting data through a process known as a three-way handshake.

1. What is UDP?

UDP is a best-effort, connectionless protocol for communications prioritizing speed over reliability. It does not establish a connection before transmission and does not guarantee reliable delivery. It is used for applications in which speed is the priority and some data loss is acceptable.

1. What is the sequence number and acknowledgement number?

The sequence number is a 32-bit field in the TCP segment header that identifies the position of the segment. It is used to keep track of the order of segments.

The acknowledgement number is sent by the receiving device to acknowledge delivery to the sender. This value indicates to the sender that the segment has been successfully delivered and what the next sequence number the receiver is expecting.

1. What is the window size?

The window size is the maximum amount of bytes the sender can transmit before having to stop and wait for an acknowledgement. It is dependent on the amount of data the receiver can process at one time and the networking conditions. This number is dynamic and can change during TCP communication.

# Q4 - Generic networking

1. What is subnetting? What is VLSM?

Subnetting is the division of a network into multiple subnetworks for better efficiency and address allocation. Subnetting divides an IP address space into multiple non-overlapping subnetworks, each with its own network address and subnet mask. The subnetworks can be assigned to each group of end devices to logically and physically separate them.

VLSM is a subnetting practice in which each subnet has a variable size. The size of the subnet is determined by the length of the subnet mask, with a longer mask yielding a smaller address range. Having a variable length subnet mask avoids IP address wastage as not all subnets have the same size requirements.

1. What is Inter-VLAN routing? How can it be achieved?

Inter-VLAN routing enables traffic from one VLAN to be forwarded to another. Since layer 2 switches cannot forward traffic from one VLAN to another, a router is needed.

Three ways to achieve:

* Traditional: Assign each VLAN an interface on the router. This is easy to set up and use but is not scalable and becomes expensive quickly.
* Router-on-a-stick: Divides a physical router interface into logical subinterfaces associated with each VLAN. Only one interface is needed to carry traffic from all VLANs. Suitable for small to medium networks. Less expensive but requires more configuration.
* Layer 3 switches: Uses SVI (Switch Virtual Interfaces) to retag the frame. These act as router interfaces.

1. What are VLANs used for?

VLAN divides a switch into multiple virtual switches with different broadcast domains. Different groups of users can be allocated to different VLANs for better security and management.

VLANs help to cut costs because otherwise each work group would require a different physical switch and a router interface. Members of the same work group would also be confined to the same physical proximity to the switch. Without VLANs, administrators would have to limit the number of work groups, which results in more devices per broadcast domain, or spend more resources installing switches and routers.

# Q5 - Spanning tree protocol

1. What is redundancy and what problem does it cause?

Redundancy is a method of providing fault tolerance to the network by having more than one path from source to destination devices. Redundancy minimizes the impact of single-point errors.

With more than one path between two devices, loops can happen, leading to phenomena such as broadcast storm, unicast duplication and MAC address inconsistency.

1. What is STP?

The Spanning Tree Protocol is a mechanism to prevent Layer 2 loops by blocking redundant paths in the network. STP ensures that only one path between a source and destination device is active at a time. It does so by nominating a switch as a root and choosing the best path from other switches to the root, disabling the rest.

1. How does the root bridge get elected?

Switches assume themselves to be the root initially. They forward BPDU frames containing their Bridge ID and root ID to adjacent switches every 2 seconds. Upon receiving the frame, other switches will look at the root ID and update their own as necessary. They then forward the lower root ID to adjacent switches.

The bridge ID is 8 bytes in length and comprises a 2-byte bridge priority and 6-byte MAC address. The bridge with the lowest bridge priority becomes the root. If there is a tie, the switch with the lower MAC address becomes the root.

1. Port role assignment:

Root ports: Ports with the cheapest path to the root become root ports. The path cost is calculated by summing up the cost of all links. (10Gb/s = 2, 1Gb/s = 4, 100Mb/s = 19, 10Mb/s = 100). If there is a tie, the next hop bridge ID, then the next hop’s interface ID will be used to break the tie.

Designated ports: All ports on the root bridge are designated ports. If one end of a link is a root port, the other end is a designated port. If a link does not have a root port, one end will be a designated port. The end on the switch with the lowest cost to the root, then lowest bridge ID will be the designated port.

Non-designated ports: All ports that are not root ports or designated ports will become non-designated ports. These ports only send and receive BPDU frames.

1. What is STP convergence?

Convergence is the total amount of time needed for the STP process to nominate the root bridge and put ports in the correct roles.

1. STP port states: Blocking, listening, learning, forwarding, disabled.

# Q6 - LAN design and link aggregation

1. How many layers in a hierarchical network? What are their features?

Three layers: Access, distribution, core.

Access: Provides end devices access to the network. Control access to the network through port security.

Distribution: Aggregates data from the access layer before passing it to the core layer for routing. Can control network flow with access control lists and delineates broadcast domains.

Core: High-speed backbone of the network, aggregates traffic from the distribution layer. Must be highly available, highly redundant, and capable of handling large amounts of traffic.

In a collapsed model, the distribution and core layers are combined into one.

1. Advantages of hierarchical network?

Advantages: scalable, redundant, performant, secure, manageable since devices have predefined roles.

1. What is network diameter?

The number of intermediary devices a packet needs to traverse to get from source to destination. This number is predictable in a hierarchical network.

1. What is redundancy?

Increasing the number of links and/or devices to prevent single-point errors from halting the entire network, thus making it more available. Unlikely to be implemented at access layer.

1. What is bandwidth aggregation/link aggregation?

Bundling multiple physical links together to increase bandwidth.

1. What is link aggregation?

Link aggregation allows the creation of logical links from multiple physical links. EtherChannel is a form of link aggregation in switched networks.

Advantages:

* Configurations applied on port channel also apply to constituent physical ports.
* Relies on existing ports, no need for upgrades.
* STP views the port channel as one logical link.
* Load-balances between physical link.
* If one member physical link in the port channel goes down, the logical link will still operate -> redundancy.

Disadvantages:

* An Ethernet frame will only be transmitted on one physical link.
* Full throughput happens only when there are enough packets to use all physical connections concurrently.
* Serialization delay is the same as that of a single connection.

1. Link aggregation protocols: PAgP and LACP

PAgP is Cisco proprietary, not recommended.

LACP is open standard, recommended.

To establish a port channel with PAgP, one end must be set to desirable mode. This protocol is identified by the use of desired/auto mode.

To establish a port channel with LACP, one end must be set to active mode. This protocol is identified by the user of active/passive mode.

1. Requirements for configuring EtherChannel:

* EtherChannel must be supported on both devices.
* Ports on both ends must operate with the same speed and duplex settings.
* Interfaces must be in the same VLAN.