- What is localhost and why would ping localhost fail?
    - Localhost it's the internal interface in Linux, that some programs can use to talk to each other inside the server. The ping will fail if the lo interface is down, or if we don't resolve localhost in our /etc/hosts file or some firewall rule is dropping ICMP packets or blocking lo interface.
- What is the similarity between "ping" & "traceroute" ? How is traceroute able to find the hops.
    - Both use ICMP (Internet control message protocol) packets to archive their proposes, but traceroute sends the packets gradually increasing the TTL value, starting with TTL 1. The first router receives the packet, decrements the TTL value and drops the packet because the TTL has zero. The router sends an ICMP Time Exceeded message back to the source.
- What is the command used to show all open ports and/or socket connections on a machine?
    - lsof -i
    - netstat -a
    - ss -a
- Is 300.168.0.123 a valid IPv4 address?
    - no
- Which IP ranges/subnets are "private" or "non-routable" (RFC 1918)?
    - 10.0.0.0/8
    - 192.168.0.0/16
    - 172.16.0.0/16
- What is a VLAN?
    - It's a virtual lan created to separate networks inside a switch, making the broadcast domain shorter, and for security proposes. Works in the network layer (OSI Layer 2)
- What is ARP and what is it used for?
    - It's a layer 2 protocol that maps IP address to MAC address.
- What is the difference between TCP and UDP?
    - TCP (Transmissions control protocol) and UDP (User Datagram Protocol), both works in the layer 3 of the OSI model, and are different methods to send information across networks, or Internet. TCP is used in scenarios when reliability is important, and is used by the majority of layer 7 protocols, like HTTP, FTP, SMTP. TCP is connection-oriented (after estabilishes the connection between two devices, maintains until the transfer process finishes), and uses a process called three-way handshake (SYN, SYN-ACK, ACK)..

    - UDP it's a connectionless protocol (doesn't estabilish a connection before hand) it's much simple and used in situations when data loss is acceptable, because doesn't guarantee all data is successfully transferred.
- What is the purpose of a default gateway?
    - The default gateway it's the way to get in other networks.
- What is command used to show the routing table on a Linux box?
- route
- netstat -r
- ip route list
- ip r
- A TCP connection on a network can be uniquely defined by 4 things. What are those things?
- remote-ip-address
- remote-port
- source-ip-address
- source-port
- When a client running a web browser connects to a web server, what is the source port and what is the destination port of the connection?
    - source port it's dynamic based on net.ipv4.ip_local_port_range defined between 32768 - 61000, destination port 80 or 443.
- How do you add an IPv6 address to a specific interface?
    - using ip -6 addr command, or using ifconfig ip inet6, or editing the OS file for network interfaces.
- You have added an IPv4 and IPv6 address to interface eth0. A ping to the v4 address is working but a ping to the v6 address gives yout the response sendmsg: operation not permitted. What could be wrong?
    - can be a firewall rule
- What is SNAT and when should it be used?
    - SNAT stands for Source Network Address Translation - changes the source address in IP header of a packet. The typical usage is to change the private address/port to a public address/port for packets leaving the network.
- Explain how could you ssh login into a Linux system that DROPs all new incoming packets using a SSH tunnel.
    - We could login using some DRAC interface if the machine it's physical, or we can use the libvirt, or vmware console if virtual, or aws console.
- How do you stop a DDoS attack?

    - You try to block the source address of the attack, or we use some CDN.
- How can you see content of an ip packet?
    - capturing the packet with tcpdump, and opening with wireshark.