**Explain the difference between static and dynamic IP addressing.**

* **Static IP Addressing** assigns a fixed IP address to a device manually. It does not change over time and is ideal for servers or devices that need consistent access.
* **Dynamic IP Addressing** uses DHCP (Dynamic Host Configuration Protocol) to automatically assign IP addresses from a pool. These addresses can change over time and are commonly used for client devices.

**How do you monitor network traffic in Linux?**  
You can monitor network traffic using tools such as:

* iftop – displays bandwidth usage on an interface
* nload – shows incoming and outgoing traffic separately
* iptraf – provides real-time network statistics
* tcpdump – captures and analyzes network packets
* wireshark – GUI-based packet analyzer

**What are the differences between TCP and UDP?**

* **TCP (Transmission Control Protocol)** is connection-oriented, reliable, and ensures data integrity with error checking and retransmission.
* **UDP (User Datagram Protocol)** is connectionless, faster, and used for applications where speed is more critical than reliability (e.g., video streaming, DNS).

**Explain the process of configuring a network interface in Linux.**  
You can configure a network interface by:

* Editing configuration files like /etc/sysconfig/network-scripts/ifcfg-<interface> (RHEL) or /etc/network/interfaces (Debian)
* Using commands like ip addr add, ip link set, or nmcli
* Restarting the network service using systemctl restart network or nmcli connection up <name>

**What tools are available for diagnosing DNS issues?**  
Common tools include:

* dig – queries DNS servers
* nslookup – resolves domain names
* host – simple DNS lookup
* Checking /etc/resolv.conf for correct DNS server entries
* ping and traceroute to test connectivity

**Check for any SELinux file problems**  
Use the following commands:

* ls -Z – shows SELinux context of files
* restorecon -Rv /path – restores default SELinux context
* audit2why and audit2allow – analyze audit logs for SELinux denials
* Check logs in /var/log/audit/audit.log

**You are trying to ping a server by hostname and you get an error message, “ping: unknown host …”. What could be the reason and how to solve the problem so you can ping it by hostname?**  
Possible reasons:

* DNS server is unreachable or misconfigured
* Hostname is not resolvable
* /etc/resolv.conf is missing or incorrect  
  Solutions:
* Check DNS settings in /etc/resolv.conf
* Use nslookup or dig to test resolution
* Add hostname to /etc/hosts if DNS is not available

**Explain the different commands to start, stop, restart, enable and disable firewall services.**  
Using firewalld:

* systemctl start firewalld
* systemctl stop firewalld
* systemctl restart firewalld
* systemctl enable firewalld
* systemctl disable firewalld  
  Using iptables:
* service iptables start/stop/restart
* chkconfig iptables on/off (for older systems)