Mock Interview Guide

Linux and Networking

Instructions for Interviewer:

- You are playing the role of **interviewer**. Use this guide as a script.
- Ask each question one at a time. Follow the steps: **Definition → Details → Scenario → Follow-up.**
- If the interviewee struggles, use the **hint**.
- The goal is to keep it conversational and practical. Help the interviewee think and express their learning.
- **colors assigned:** Questions Answers Hint

Freshers - Level

Linux and Networking

(10 Easy Interview Questions)

---

1. **"What is Linux and why is it popular in DevOps?"**

   Expected Answer: Linux is an open-source operating system known for its stability, performance, and flexibility. It's widely used in servers and cloud systems.

   Hint: Think about the OS used in most servers and cloud VMs.

2. **“What is the difference between a process and a service in Linux?”**

Expected Answer: A process is any running program. A service is a background process usually managed by systemd.

Hint: A service is a special kind of process that runs in the background continuously.

3. **“How do you check the current directory you are in?”**

Expected Answer: By running the pwd (print working directory) command.

Hint: It's a simple command to show where you are in the system.

4. **“What does the ls command do?”**

Expected Answer: It lists files and directories in the current working directory.

Hint: Use this command to see what’s in a folder.

5. “How can you find your system’s IP address?”

Expected Answer: Use ip a or ifconfig to display network interface details.

Hint: Look for the address next to your active network interface.

6. “What is a firewall and how does Linux manage it?”

Expected Answer: A firewall controls incoming and outgoing traffic. Linux uses tools like iptables or firewalld.

Hint: Think security and access control.

7. “How do you check system resource usage in Linux?”

Expected Answer: Commands like top, htop, or free show CPU, memory, and processes.

Hint: Use top to see live system activity.

8. “What is the difference between sudo and su?”

Expected Answer: sudo runs commands as another user (default: root), while su switches to another user entirely.

Hint: Use sudo for one-time admin commands.

9. "How do you make a file executable?"

Expected Answer: Use chmod +x filename to give execute permission.

Hint: Change the file's permission to run it like a script.

10. "What is the default port of SSH?"

Expected Answer: Port 22 is the default port used by SSH.

Hint: It's how we remotely access Linux systems.

SCENARIO-BASED INTERVIEW QUESTIONS

---

1. You tried to SSH into a server but got a "Connection refused" error. What could be the reason?

Expected Answer: The SSH service might not be running, the port could be closed by a firewall, or the server might be unreachable.

Hint: Check if sshd is active, and verify port 22 is open.

2. You see high CPU usage on a Linux server. How would you identify the cause?

Expected Answer: Use top or htop to check which process is consuming the most CPU, then investigate that specific service or command.

Hint: Start by observing live system behavior.

3. You cannot ping a remote server, but SSH works fine. What might be happening?

Expected Answer: ICMP packets (used by ping) might be blocked by a firewall, but TCP (used by SSH) is allowed.

Hint: Different protocols, different firewall rules.

4. After editing the /etc/hosts file, hostname resolution still fails. Why?

Expected Answer: There could be a syntax error, DNS is taking precedence, or the system cache needs to be cleared.

Hint: Order in /etc/nsswitch.conf determines lookup priority.

5. **Your cron job is not running as expected. How would you debug it?**

Expected Answer: Check if the cron service is running, review the job syntax, check file permissions, and inspect /var/log/cron.log or journalctl.

Hint: Logs are your first clue with scheduled tasks.

PROJECT-BASED INTERVIEW QUESTIONS

---

1. **How would you configure a Linux server with a static IP, custom hostname, and basic firewall rules?**

Expected Answer:

- **Set static IP in /etc/netplan/ or appropriate network config file**
- **Change hostname with hostnamectl set-hostname**
- **Configure ufw or iptables to allow only required ports**

Hint: Combine networking, system identity, and security setup.

2. You are asked to set up a secure SSH server for a team. What steps would you take?

Expected Answer:

- **Change the default SSH port**
- **Disable root login**
- **Set up key-based authentication**
- **Use fail2ban or firewall to block brute-force attempts**

Hint: Think like a security-focused admin.

3. Describe how you'd automate daily system backups on a Linux server.

Expected Answer:

- **Write a shell script to archive and compress target directories**
- **Use crontab to schedule the script**
- **Store backups locally or remotely (e.g., SCP to backup server)**

Hint: Automate using cron and keep the logic simple.

4. How would you monitor a production Linux server's health and performance?

Expected Answer:

- **Use tools like top, vmstat, iotop, and df for live metrics**
- **Set up cron or systemd timers to log metrics**
- **Optionally configure monitoring tools like Nagios or Prometheus**

Hint: Combine manual checks with automated alerting if needed.

Medium - Level

Linux and Networking

(Interview Questions- 1 to 2 Years Experience)

---

1. **"How do you check open ports on a Linux system?"**

   Expected Answer: Use netstat -tuln or ss -tuln to list listening ports and associated services.

   Hint: Want to see what's running and listening on your machine?

2. **"Explain the difference between a hard link and soft link."**

   Expected Answer: A hard link points directly to the file data; a soft link (symbolic link) points to the file name or path.

   Hint: One is a clone, the other is a shortcut.

3. **"How would you add a new user in Linux?"**

Expected Answer: Use useradd username and set a password with passwd username.

Hint: Think basic user management commands.

4. “What is the /etc/hosts file used for?”

Expected Answer: It maps IP addresses to hostnames locally before DNS is used.

Hint: A simple way to resolve names without a DNS server.

5. “How do you schedule a task to run daily in Linux?”

Expected Answer: Use crontab -e and add a line like 0 0 * * * /path/to/script.

Hint: Think of automating a daily script run.

6. “How do you permanently assign a static IP in Linux?”

Expected Answer: Edit the network config file under /etc/netplan/ or /etc/sysconfig/network-scripts/ depending on distro.

Hint: Static IP setup depends on distro, but config files are key.

7. “What is the use of /var/log directory?”

Expected Answer: It stores system logs like boot logs, authentication logs, and service logs.

Hint: Where would you check if something failed?

8. “Explain ping and traceroute.”

Expected Answer: ping tests connectivity; traceroute shows the path packets take to reach a host.

Hint: One checks connection, the other maps the route.

9. “What is the difference between TCP and UDP?”

Expected Answer: TCP is reliable and connection-based; UDP is faster but connectionless.

Hint: Think about reliability vs speed.

10. **“How do you kill a running process?”**

Expected Answer: Use kill <PID> or killall <process-name> to stop a process.

Hint: Find the PID with ps or top.

SCENARIO-BASED INTERVIEW QUESTIONS

---

1. **You added a new user, but they can't SSH into the server. What might be wrong?**

Expected Answer: The user's home directory or .ssh folder might have incorrect permissions, or their public key is missing in authorized_keys.

Hint: SSH requires proper directory permissions and key setup.

2. **After rebooting a server, the static IP configuration is lost. What could be the issue?**

Expected Answer: The configuration may not have been saved in the right persistent config file or applied using netplan or systemctl.

Hint: Temporary changes are lost after reboot — make them permanent.

3. You see 'permission denied' when trying to execute a script. What steps would you take to fix it?

Expected Answer: Check if the script has execute permission using ls -l, then run chmod +x script.sh to fix it.

Hint: Linux blocks execution unless permission is explicitly set.

4. You can ping an external IP but not a domain name. What's likely the problem?

Expected Answer: DNS is likely misconfigured or the /etc/resolv.conf file is missing the correct DNS server.

Hint: It's a name resolution issue, not a network issue.

5. Your team reports slow SSH logins to a Linux server. How would you troubleshoot this?

Expected Answer: Check DNS resolution delays, UseDNS setting in sshd_config, or authentication method delays.

Hint: SSH login latency is often DNS or auth related.

PROJECT-BASED INTERVIEW QUESTIONS

1. **You need to set up a Linux server for a staging environment. What are your steps?**

Expected Answer:

- **Install necessary packages (e.g., web server, DB)**
- **Configure network settings and hostname**
- **Create service accounts and directories**
- **Set up firewall rules and monitoring**

Hint: Treat staging like a mini-production setup.

2. **How would you automate the creation of users and their home directories on multiple servers?**

Expected Answer:

- **Write a shell script or use Ansible to automate useradd, passwd, and mkdir operations**
- **Use a loop for multiple users**

Hint: Think repeatable and scriptable.

3. **You are asked to monitor disk usage on critical directories. How do you implement this?**

Expected Answer:

- **Use df -h, du -sh, or custom scripts**
- **Schedule regular checks with cron**
- **Send alerts via mail or log them**

Hint: Automate checks before disks fill up.

4. **You want to restrict access to a service to only specific IP addresses. How do you achieve that?**

Expected Answer:

- **Use firewall rules (iptables, firewalld, or ufw)**
- **Or configure the service (e.g., NGINX, SSH) to bind to allowed IPs only**

Hint: Layered access control is the goal.

Hard - Level

Linux and Networking

(Interview Questions - 3+ Years Experience)

---

1. **“Explain how DNS works when resolving a domain name.”**

   Expected Answer: The system queries a resolver, which contacts root → TLD → authoritative name servers to resolve the IP.

   Hint: Think about the step-by-step resolution path.

2. **“How do you analyze a system’s performance bottleneck?”**

   Expected Answer: Use tools like top, iotop, vmstat, and sar to identify CPU, memory, disk, or I/O issues.

   Hint: Identify which resource is being overused.

3. **“What is a runlevel? How is it used in Linux?”**

Expected Answer: A runlevel defines system states (e.g., multi-user, graphical). Managed via systemctl or init.

Hint: Think boot stages and modes.

4. **"How would you troubleshoot a 'network unreachable' error?"**

Expected Answer: Check IP config, default gateway, DNS, firewall, and use tools like ping, traceroute, ip r.

Hint: Start from your machine and trace out.

5. **"What is SELinux and how does it work?"**

Expected Answer: Security-Enhanced Linux enforces access controls through contexts and policies.

Hint: It restricts services beyond normal file permissions.

6. **"Explain the Linux boot process."**

Expected Answer: BIOS → Bootloader (GRUB) → Kernel → init/systemd → Target/runlevel.

Hint: Sequence of startup from hardware to userland.

7. "What are bonding and teaming in Linux networking?"

Expected Answer: They combine multiple network interfaces for redundancy or performance.

Hint: Used in production to avoid link failure.

8. "How would you trace a DNS issue in a Linux system?"

Expected Answer: Use dig, nslookup, or host to trace resolution steps and DNS server responses.

Hint: Try to isolate whether the issue is local or DNS provider related.

9. "How do you secure an SSH server?"

Expected Answer: Change default port, disable root login, use key-based auth, and enable firewalls or fail2ban.

Hint: Think defense layers for remote access.

10. **"What is the difference between iptables and firewalld?"**

Expected Answer: iptables is the legacy firewall tool; firewalld is a dynamic manager using zones and services.

Hint: Old vs modern approach in managing firewall rules.

SCENARIO-BASED INTERVIEW QUESTIONS

---

1. **A critical service randomly crashes on a production server. How do you investigate and fix it?**

Expected Answer: Check logs in /var/log, inspect memory usage with top/journalctl, and analyze systemctl status or dmesg output. Use ulimit if resource limits are exceeded.

Hint: Use logs, process info, and memory checks.

2. **You discover a rogue process consuming high CPU and memory. How do you deal with it without crashing the system?**

Expected Answer: Use top/ps to identify the process, gracefully stop it using kill, and investigate the cause before restarting.

Hint: Kill smartly — avoid abrupt shutdown unless necessary.

3. **You made a firewall change and locked yourself out of the remote server. What now?**

Expected Answer: Use out-of-band console access (cloud console or physical access) to revert changes or disable firewall temporarily.

Hint: Always plan for rollback or remote access fallback.

4. **An automated script fails due to environment variable issues. How do you troubleshoot this?**

Expected Answer: Check if the variable is correctly exported, persistent across sessions, and sourced in scripts (.bashrc, .profile, etc.).

Hint: Login shell vs non-login shell behavior matters.

5. **Your system experiences intermittent DNS resolution failures. How do you investigate and fix it?**

Expected Answer: Analyze /etc/resolv.conf, DNS server availability, and consider switching to a reliable public DNS. Check logs and latency.

Hint: Look at both system config and external DNS health.

PROJECT-BASED INTERVIEW QUESTIONS

---

1. **Design a high-availability Linux server cluster for a production app. What would you include?**

Expected Answer:

- **Use load balancers, redundant nodes, and shared storage**
- **Configure heartbeat, failover, and auto-recovery**
- **Automate configuration with Ansible**

Hint: Think availability, fault tolerance, and automation.

2. **You're asked to secure a Linux server for external exposure. What measures do you take?**

Expected Answer:

- **Harden SSH (change port, disable root, keys only)**
- **Enable firewalls and intrusion prevention (e.g., fail2ban)**
- **Apply security updates and remove unused packages**

Hint: Defense in depth — think layered security.

3. **You need to migrate a Linux server with multiple services to a new machine with minimal downtime. How do you plan it?**

Expected Answer:

- **Document existing configs**
- **Set up and test new server**
- **Use rsync for data sync**
- **Schedule a cut-over window with DNS switch**

Hint: Minimize downtime with prep and testing.

4. **Implement centralized logging for a fleet of Linux servers. How would you do it?**

Expected Answer:

- **Use syslog or rsyslog to send logs to a central server**
- **Parse and visualize logs using ELK stack or Graylog**

Hint: Central logs = easier audits and faster debugging.