Technical Assessment for IT engineer

- ## PC Configuration & Maintenance

Scenario 1: New Employee Onboarding

First, I install the operating system Windows or Linux. Then I install all updates.

Next, I install company software: browser, antivirus, VPN and communication tools Teams or Slack.

I create a new user account with the employee's name.

I connect the laptop to the company network and test Internet access.

Finally, I check everything works and give the laptop to the new employee.

Scenario 2: Troubleshooting

First, I ask the user when the problem started.

I check if the laptop is full or has many programs open. I clean temporary files and close background apps.

Then, I check Wi-Fi signal and try to connect to another network.

If Wi-Fi is still bad, I restart the router and update the network driver.

If it is still slow, I test with another device to see if the problem is from the laptop or network. After fixing, I test again to confirm everything is working.

- ## Cloud Migration & Management (Scaleway / Cloudflare)

Scenario 3: Scaleway Migration

First, I check what data we have on the local file server. Then I create a Scaleway Object Storage bucket.

I copy the files to Scaleway using the console or a sync tool (like rclone). I test that all files are in the cloud and users can access them.

After that, I remove old data if needed and make sure backups are enabled. Finally, I inform the team how to connect to the new cloud storage.

Scenario 4: Cloudflare Configuration

1. Migrate DNS records

- Log in to the Cloudflare dashboard.
- Add the company's domain name.
- Cloudflare will scan and import most DNS records automatically.

- Check all records (A, CNAME, MX, TXT, etc.) to make sure they match the old DNS provider.
- Change the nameservers at the domain registrar to the ones given by Cloudflare.
- Wait for the DNS to update (it may take a few hours).

2. Set up a reverse proxy with SSL

- In Cloudflare, turn on the orange cloud icon for the records you want to proxy.
- This means traffic will go through Cloudflare before reaching your servers.
- Go to the SSL/TLS tab and select “Full” or “Full (Strict)” mode.
- Cloudflare will now handle HTTPS traffic safely.

3. Configure secure remote access with Cloudflare Zero Trust

- Go to the Zero Trust Dashboards.
- Create an Access Application for each internal app
- Choose the domain
- Add login rules (Google, Microsoft, etc.) so only approved users can connect.
- Use Cloudflare Tunnel to link internal apps without opening firewall ports.
- Now employees can securely access internal tools from anywhere.

- ## Global IT Support

Scenario 5: Remote Assistance

Steps:

a. Communicate
   - Send a message or call them to understand the issue.
   - Ask what error message they see.
   - Stay calm and polite.

b. Help with VPN
   - Ask them to restart the computer and try again.
   - Check if their Internet connection works.
   - Guide them to open the VPN app and verify login details.
   - If needed, reset their VPN credentials or check the VPN server status.

c. Help with the printer
   - Use remote desktop software
   - Check if the printer is online and has paper/ink.
   - Reinstall the printer driver if necessary.

d. Follow up
   - Confirm everything is working again.

- Thank them for their patience and report the issue in the IT log.

Scenario 6: IT Inventory & Standarlization

a. Create a central inventory system
   - Use a cloud tool like ManageEngine, GLPI, or a shared Google Sheet at first.
   - List each device: serial number, user, model, location, and status.
b. Use standard configurations
   - Create a company “gold image”
   - Apply this image to all new computers.
c. Keep inventory updated
   - Add or remove items when new devices arrive or old ones are replaced.
   - Do monthly or quarterly checks to verify everything is correct.
d. Security and backups
   - Store the inventory securely with access for IT staff only.
   - Back it up regularly to the cloud.

- ## Automation & Scripting

```
#!/bin/bash

# Update the system

echo "Updating system..."

sudo apt update -y

sudo apt upgrade -y

# Make a backup of important folders

echo "Creating backup..."

tar -czf /tmp/backup.tar.gz /home

# Upload the backup to Scaleway

echo "Uploading to Scaleway..."

aws s3 cp /tmp/backup.tar.gz s3://my-scaleway-bucket/

# Clean up

rm /tmp/backup.tar.gz

echo "All done!"
```