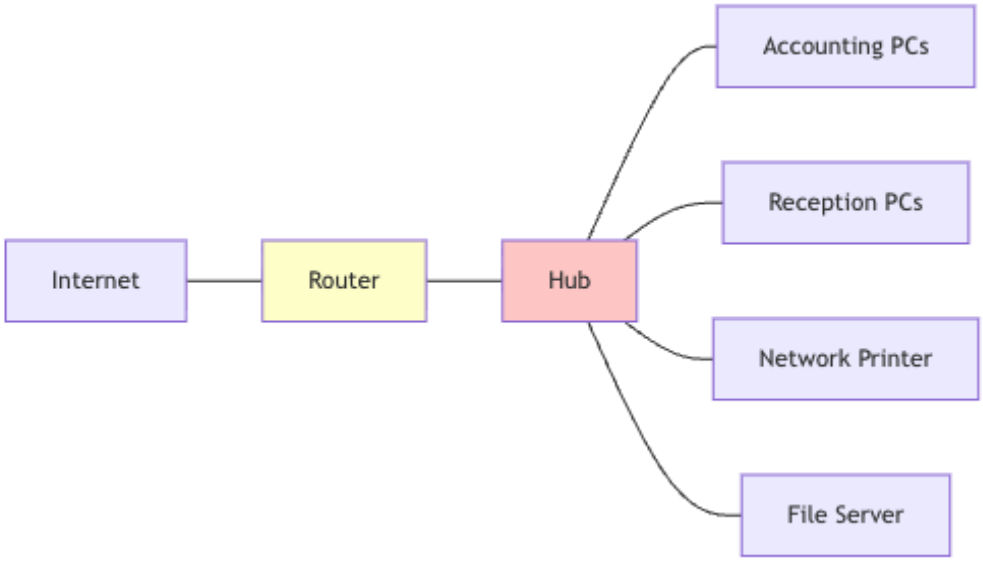
Problem 1: Network Troubleshooting Analysis (50 points)
For each scenario below, analyze the network diagram and suggest improvements.

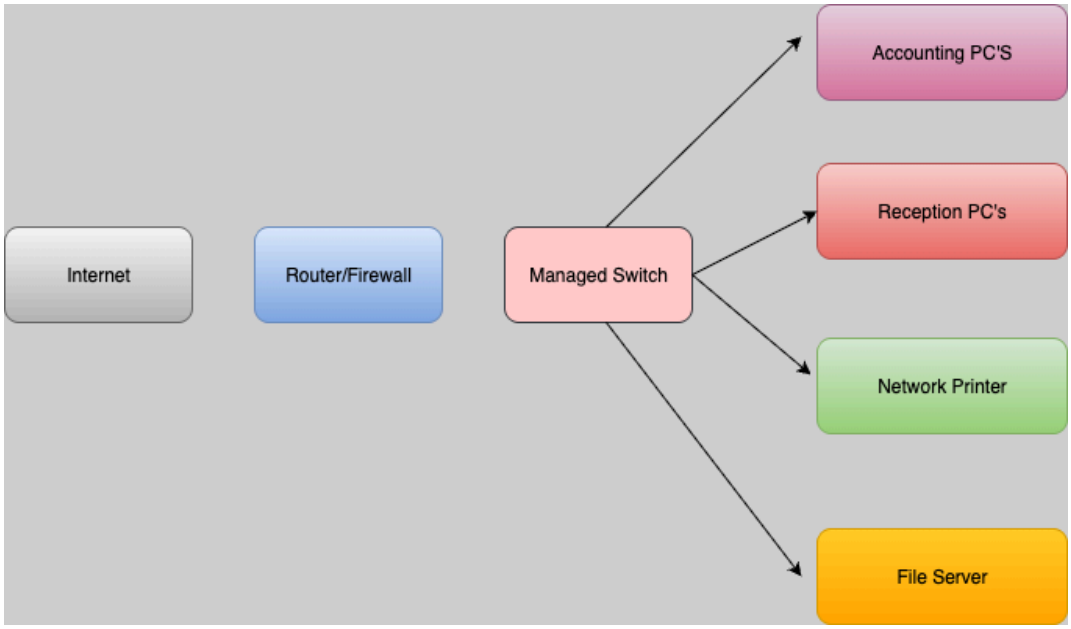
Your response should:
1.Identify and explain inefficiencies or issues with the current design.
2.Provide a corrected diagram showing your solution.
3.Justify your choices with specific reasoning.

- Scenario A: Office Network Performance Issues:

Situation: A small accounting firm has the following network setup in their main office
Current:



Suggested:



Summary: Why did I choose router/firewall and Managed switch?

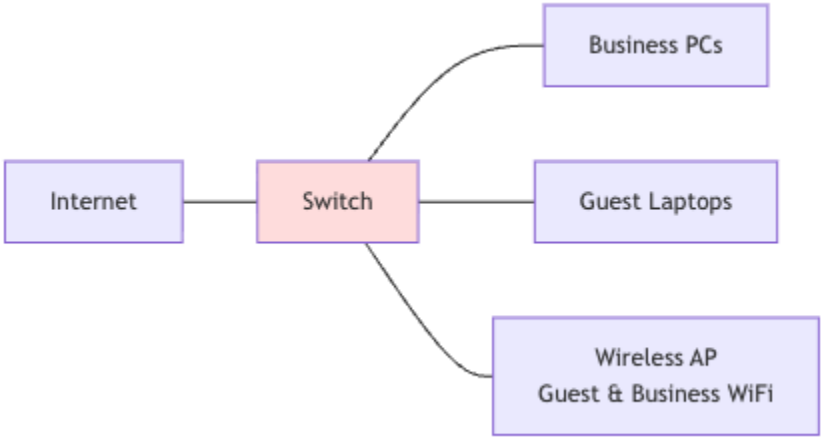
Router/Firewall: The Router/Firewall (Blue) provides Internet access, security, and NAT. Also the router/firewall makes sure that inter-VLAN routing and security regulations are followed (for example, it stops receptionists or guests from getting to accounting resources). Without it, devices from distinct logical networks cannot be segregated or filtered.

Managed Switch: The Managed Switch (Peach) distributes wired connections to PCs and servers. As we see in the reference where The office faces delayed file transfers, particularly when numerous employees utilize the file server at the same time. Which is the most common reason to replace the hub with a Managed switch. However, A hub broadcasts each frame to all ports, resulting in collision on the other side Switch forward frames just to the destination ports. Which means It helps to Stop the collisions and shares bandwidth more fairly than a hub.

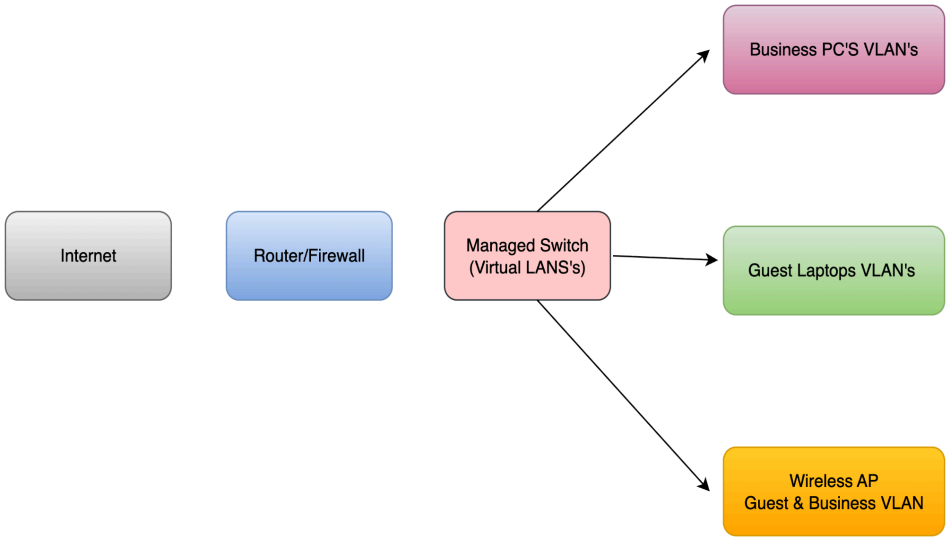
- Scenario B: Network Security Concerns (25points)

Situation: A consulting company wants to separate their guest network from their internal business network but currently has this setup:

Current:



Suggested:



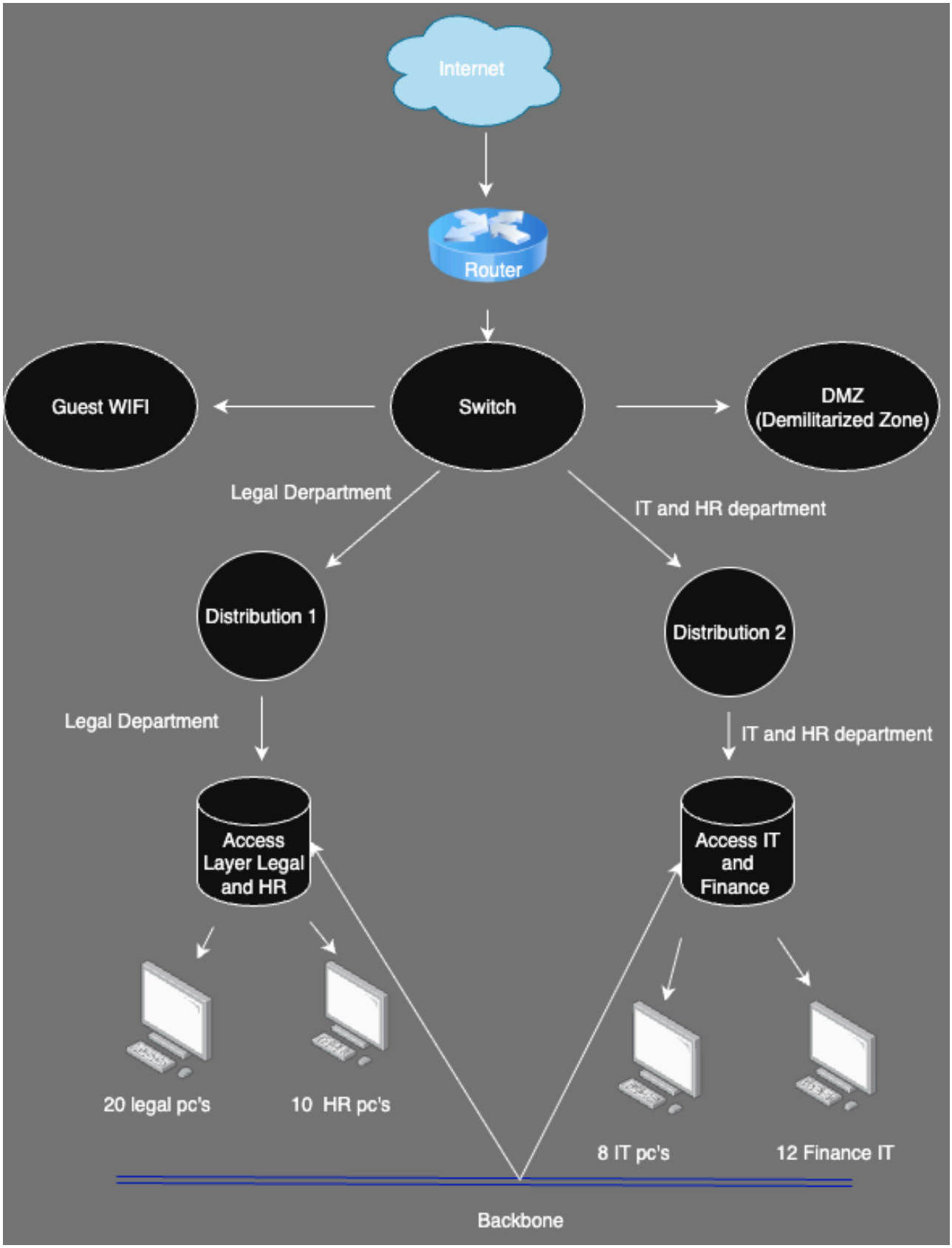
Summary: Why did I choose router/firewall and Managed switch?

The Internet is connected through the router/firewall which is next connected to the Managed switch VLAN's. The connectivity is disturbed by the switch is PC's for Business, Laptop's for Guest, Wireless access point which host both by guest and business VLAN's. As you can see in the first Diagram that there is a security issue which is very risky because guests can use and share the resources including the company pc's. In order to avoid that risky factor we will be

separating both networks via wireless AP Guest & Business wifi to Wireless AP Guest & Business VLAN. The right separation solution is Use the Managed Switch's VLANs (Virtual LANs). One VLAN for internal resources and business PC's. A single VLAN for visitor devices. Different wireless AP Connect the business WiFi to the business VLAN. As well as by Putting the guest WiFi into the guest VLAN. However, by doing this it's help's the Business systems to be secured and completely separated from guest devices.

Problem 2: Small Business Network Design (50 points)
Scenario: You are consulting for a growing law firm that needs to expand and reorganize their network infrastructure. They are moving to a larger office space and adding significant staff.

Summary: The company is growing from 10 to 50 PCs in four departments and has to keep the networks of each department separate for privacy and compliance. The suggested design includes a three-tier topology (Access / Distribution / Backbone) with VLAN-based segmentation, inter-VLAN routing that is managed by a firewall, and perimeter security (firewall + DMZ). However, This design helps to facilitate the expansion as well as streamlines the administration which helps to uphold the department-specific security regulations.


Internet
Router
Guest WIFI
Switch
DMZ
(Demilitarized Zone)
Legal Derpartment
IT and HR department
Distribution 1
Distribution 2
Legal Department
IT and HR department
Access
Layer Legal
and HR
Access IT
and
Finance
20 legal pc's
10 HR pc's
8 IT pc's
12 Finance IT
Backbone