**🎤 Slide 3: Network Layout & Topology**

“Let’s begin with the comparison of the network layout and topology.

In the old design, the network used a flat topology, where all devices were connected through a single layer of switches. This made the network simple but caused issues like broadcast traffic overload and poor scalability.

In the new design, we’ve adopted a hierarchical topology with segmentation. This means traffic is more organized, and different departments or functions are separated using VLANs.

For example, VLAN 99 is used for the server room, while VLAN 40 is for office users. This reduces congestion, improves troubleshooting, and makes the network easier to scale as the organization grows.”

**🎤 Slide 4: Network Devices Used**

“Next, we’ll look at the network devices used.

The old setup used three unmanaged switches and a single basic router. This limited the control over traffic and prevented advanced configurations.

The new design upgrades to three **managed switches**, which allow us to use features like VLAN tagging, QoS, and centralized management.

Instead of one router, we now have **multiple routers** – for example, a router for the shop, one for the office, and one for general routing. This setup improves both performance and reliability.

We’ve also added an **ASA firewall** to filter malicious traffic and apply security policies.

Finally, server functions are no longer centralized. We now have **multiple dedicated servers** – for HTTP, DNS, and DHCP – improving redundancy and ensuring better service availability.”

**🎤 Slide 5: Network Security Comparison**

“Security has been a major focus of the new network design.

In the old setup, there was **no firewall**, which left the internal network vulnerable to external threats. In the new design, a **Cisco ASA firewall** has been added to filter and inspect incoming and outgoing traffic.

Additionally, VLANs are now being used to separate departments such as Shop, Office, Manager, and Stock Room. This limits the movement of threats within the network and reduces the overall attack surface.

Access control is also enforced through routing and VLAN rules, ensuring that only authorized users and devices can access sensitive resources like internal servers.”