**During the division of work, Erik Ádám Hegyi is responsible for the preparation of the documentation, the detailed description of the network topology, the specifications of the devices and the recording of the progress of the project.**

**József Márk Görgényi was responsible for configuring network devices, setting up VLANs, ensuring the proper functioning of the Internet and VPN settings, as well as configuring the firewall, Márk carried out the simulation, debugging and testing of the network using Cisco Packet Tracer.**

**During the cooperation, we both actively participated in the planning and fine-tuning of the network, we constantly communicated with each other and made suggestions if we found a mistake in the other's task or if we could somehow help the other's efficiency. We have created a stable, safe and reliable network system for coordinated work.Network Design and Implementation Presentation**

**Part 1 – Network Infrastructure and Planning**

The goal of this project was to establish a **reliable, scalable, and secure network infrastructure** connecting three locations. The process began with designing the **network topology**, considering the company’s operational needs, expected traffic load, and potential future expansions.

To enhance network efficiency and security, **VLANs** were implemented, ensuring logical segmentation and improved data management across departments. **Dynamic routing protocols** were utilized to enable optimal route selection and smooth data flow.

Security was a primary focus, so **firewalls and access control lists (ACLs)** were configured to prevent unauthorized traffic. Additionally, an **intrusion detection system (IDS)** was integrated to monitor potential threats. To ensure **secure communication between locations**, **VPN technology** was deployed, providing data encryption and protecting against unauthorized access.

Finally, to guarantee **business continuity**, **redundant devices and failover protocols** were included in the design. These measures help minimize service downtime and mitigate the impact of unexpected network failures.

**Part 2 – Implementation, Testing, and Security Solutions**

During the **implementation phase**, network devices, including **switches, routers, and firewalls**, were configured based on the initial design. VLANs were carefully set up to ensure proper network segmentation across different departments.

Dynamic routing protocols were deployed and tested to ensure **optimal data traffic flow**. Secure **VPN connections** were established to facilitate **encrypted communication** between locations.

Once the network was set up, rigorous **testing procedures** were conducted. **Stress tests** were performed to assess network load capacity, and **simulated cyber-attacks** were executed to evaluate security system effectiveness. Firewalls and the **intrusion detection system** were extensively tested to identify and address potential vulnerabilities.

In the final stage, **comprehensive documentation** was created, outlining all configurations and best practices. Recommendations for **ongoing monitoring and maintenance** were also provided to ensure the long-term stability and security of the network.

The result is a **high-performance, secure, and easily scalable network** that effectively supports the company's current operations while allowing for future growth.