Project Overview

This project involves a university network divided into seven sub-networks, each representing a different college. Some colleges, such as the College of Artificial Intelligence and the Salt Technical College, share the same building.

Additionally, there is a separate network for Salt City, which, along with all university networks, connects to a core switch. This core switch is linked to the university router, which, in turn, connects to the Balqa Governorate router. The Salt City network also connects directly to the Balqa Governorate router.

Moreover, a network in the Amman Governorate hosts a group of servers, including the e-learning server.

Network Restrictions

1. The university network is restricted from communicating with the Salt City network.
2. Certain protocols, such as HTTP and ICMP, are not permitted within the university network.
3. The Salt City network is restricted from accessing the e-learning server.

Technologies Used

1. DHCP: Dynamic Host Configuration Protocol for automatic IP address assignment.
2. Access Lists: To control traffic and enforce network policies.
3. Port Security: To restrict port access and prevent unauthorized devices.
4. DHCP Snooping: To enhance security by monitoring DHCP traffic.
5. OSPF: Open Shortest Path First for efficient routing.
6. VLANs: Virtual Local Area Networks to segment network traffic.
7. Inter-VLANs: Routing between VLANs.
8. SSH: Secure Shell for secure remote connections.
9. Port Management: Disabling all unused ports on switches and placing them in a blackhole VLAN.

10. NAT (PAT): Network Address Translation, specifically Port Address Translation, for efficient IP address usage.

11. DNS: Domain Name System for resolving domain names.

12. Authentication: Ensuring secure access to network resources.