Course Project 2 Report

Soo Yuan Kong and Juan Salazar Cabrera

University of Colorado Colorado Springs

CS4220 001: networkNinja3

Dr. Serena "Sully" Sullivan

May 2nd 2025

Network Design Overview and Justification

For this project, Soo Yuan and Juan designed a hybrid network that connects three main segments: the Main Campus, the Downtown Campus, and a Cloud-based Email Server Network. A hybrid topology was chosen because it effectively integrates star topology (used within each campus for departmental access) and point-to-point topology (used between routers for inter-campus communication) (Sharma, 2025). Each site is connected via point-to-point serial links using subnetted IP ranges for clarity and route management. The Main Campus router connects to both the Cloud router (10.10.10.4/30) and the Downtown Campus router (10.10.10.0/30), serving as the central hub.

We chose to create a university network because we are already studying on campus, and designing such a network enhances our understanding of real-world implementations. At each campus, a 3-layer 3650-24PS switch handles inter-VLAN routing, while departmental switches (2960-24TT) connect end-user devices. The Main Campus supports eight departments, each assigned a unique VLAN (e.g., Admissions: VLAN 10 → 192.168.1.0/24, HR: VLAN 20 → 192.168.2.0/24, etc.), whereas the Downtown Campus supports two departments (Performing Arts and Cybersecurity) on VLANs 90 and 100. The Cloud/School Email Router connects directly to the email server on a separate subnet (20.0.0.0/30). This segmentation improves security and administration.

We implemented RIPv2 for inter-network routing because it provides dynamic route updates and is easier to configure and manage. We deployed DHCP to automatically assign IP addresses and network configuration to devices, which reduces manual errors and improves network efficiency by enabling logical division into subnets. Access Control Lists (ACLs) are

strategically applied to filter traffic between departments (only from VLAN 10 to VLAN 100) and limit access to sensitive data across VLANs (ComputerNetworkingNotes, 2025).

Challenges Faced

The main challenge was the inability to implement an Intrusion Detection System (IDS) due to limitations in Cisco Packet Tracer. Therefore, we chose to implement ACL. During the ACL configuration, several challenges were encountered. Invalid ACL commands were issued, such as using "*access-list 110 deny 192.168.1.0 0.0.0.255*" instead of the correct "*deny ip 192.168.1.0 0.0.0.255 any*". The wrong interface was selected for ACL application, with ACLs mistakenly applied to "*gig0/1*", which was not the correct active subinterface (e.g., "*gig0/0.10*"). Additionally, the ACLs failed to restrict traffic because they were either unbound or attached to inactive interfaces. There was also confusion regarding interfaces, with ACLs attempted on non-existent ports (e.g., "*gig1/0/2*"), indicating a mix-up between router and switch configurations. To troubleshoot, tools like "*ping*", "*show running-config | include access-group*", and error messages such as "Destination host unreachable" were used to verify the functionality of the ACLs.

References

Sharma, D. (2025). *7 types of network topology explained with diagrams.* UniNets. Retrieved May 1, 2025, from https://www.uninets.com/blog/types-of-network-topology#:~:text=The%207%20types%20of%20network,network%20topology%20used%20in%20networking.

ComputerNetworkingNotes. (2025). *Configure standard access control list step by Step Guide*. Retrieved May 1, 2025, from https://www.computernetworkingnotes.com/ccna-study-guide/configure-standard-access-control-list-step-by-step-guide.html