PROJECT REPORT

Networking Academy
Virtual Internship Program 2025

CYBER SHIELD:
DEFENDING THE NETWORK

By

Levin Johith A

Sathyabama Institute of Science and Technology

CSE DEPARTMENT

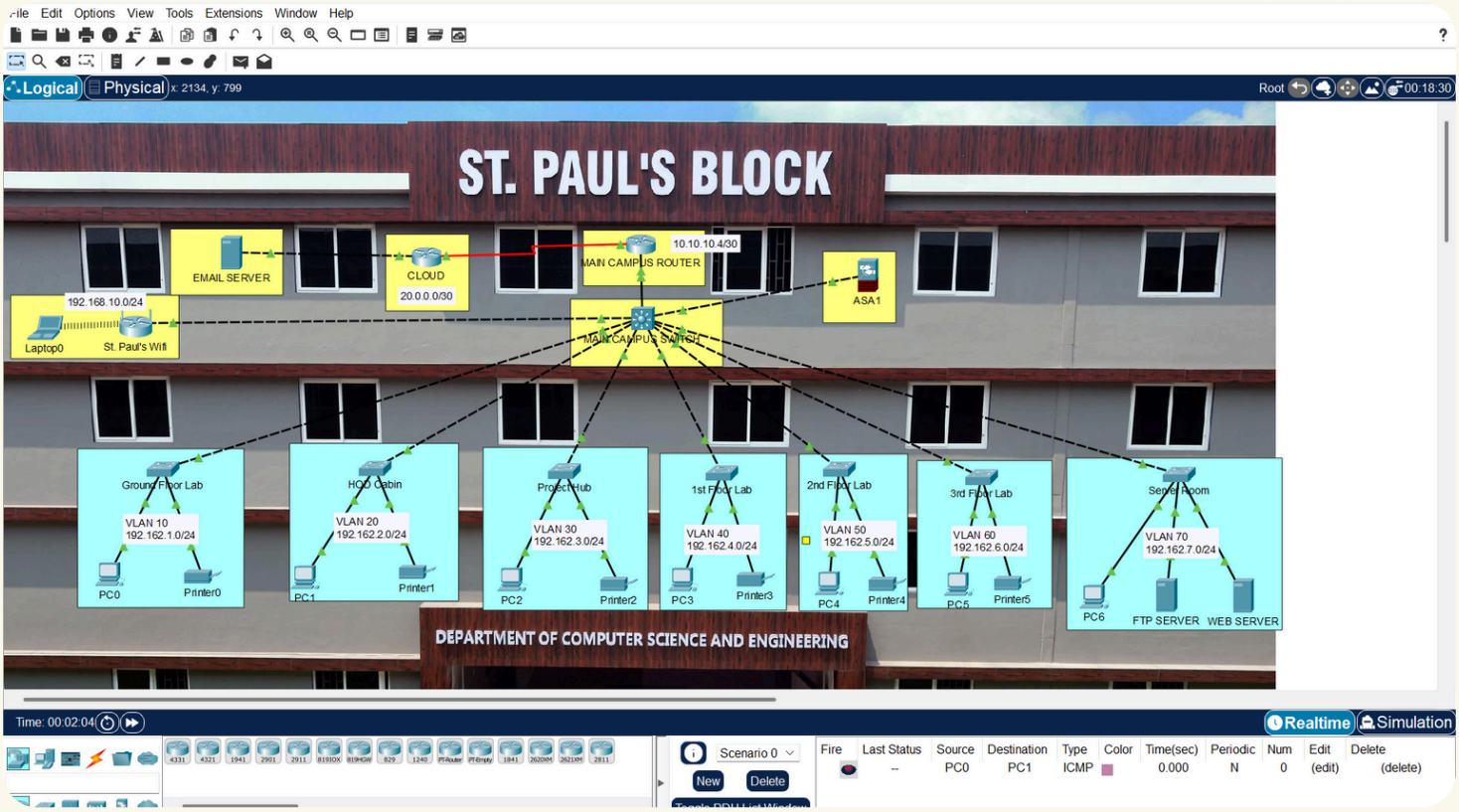
INTRODUCTION

This project, developed as part of the Cisco Virtual Internship Program 2025, focuses on addressing these challenges through the lens of cybersecurity.

The chosen model for this project is the St. Paul's Block of Sathyabama University, which represents a typical academic building with multiple labs, faculty offices, and server rooms. The objective is to analyze and secure its network using Cisco Packet Tracer while applying the principles learned in the Cisco Networking Academy Cybersecurity course. The project is divided into three parts:

- Part 1 - Red Team Audit of the existing block network.
- Part 2 - Hybrid Secure Access Design for faculty and students.
- Part 3 - Web Access Policy Framework for controlled, monitored usage.

Part 1: Red Team Audit



1.1 Network Layout (from Packet Tracer model)

- Main Campus Router and Switch connecting the block to the backbone.
- ASA Firewall securing external connectivity.
- Email Server connected via block LAN.
- Wi-Fi Network (St. Paul's Wi-Fi) with range 192.168.10.0/24.
- VLANs configured per lab/floor:
  - VLAN 10: Ground Floor Lab (192.162.1.0/24)
  - VLAN 20: HOD Cabin (192.162.2.0/24)
  - VLAN 30: Project Hub (192.162.3.0/24)
  - VLAN 40: 1st Floor Lab (192.162.4.0/24)
  - VLAN 50: 2nd Floor Lab (192.162.5.0/24)
  - VLAN 60: 3rd Floor Lab (192.162.6.0/24)
  - VLAN 70: Server Room (FTP + Web servers, 192.162.7.0/24)

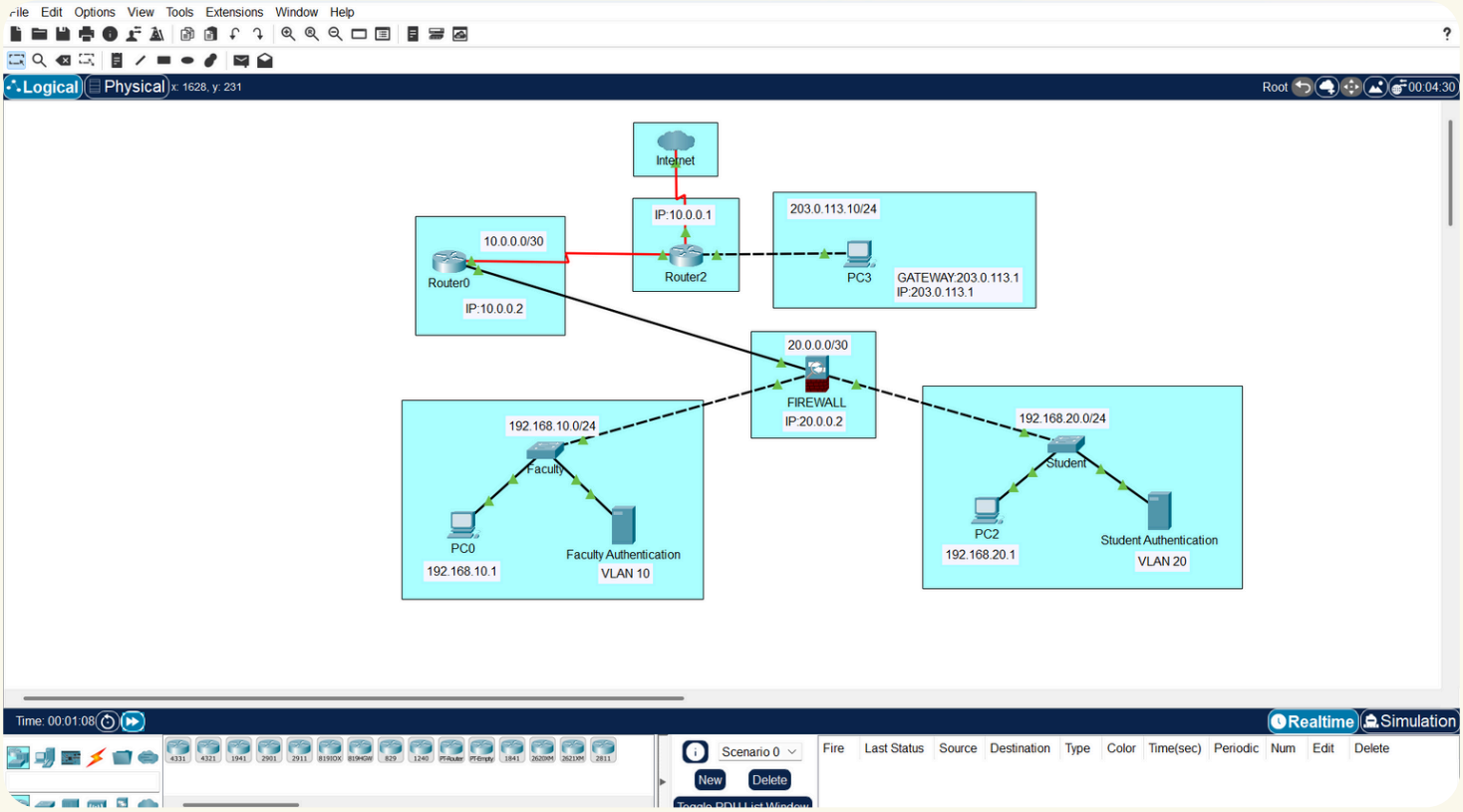
1.2 Identified Weaknesses

- Wi-Fi access uses shared credentials.
- VLANs exist but not all traffic between them is restricted.
- Firewall provides perimeter security but lacks deep packet inspection.
- Servers in VLAN 70 are still reachable from student VLANs.
- No SIEM/logging for activity monitoring.

1.3 Recommendations

- Enforce ACLs between VLANs to block unnecessary access.
- Apply role-based authentication via RADIUS.
- Strengthen firewall with IDS/IPS policies.
- Isolate server VLAN (70) with restricted access only from Faculty VLAN.
- Centralize logging with Syslog server for incident tracking.

Part 2: Hybrid Secure Access Design



2.1 Network Layout (from Packet Tracer model)

- Two routers simulate internal and external connections.
- Firewall (20.0.0.2/30) filters campus traffic.
- VLAN 10: Faculty Network (192.168.10.0/24) with authentication server.
- VLAN 20: Student Network (192.168.20.0/24) with authentication server.
- Remote access via VPN and role-based authentication.

2.2 Design Highlights

- Faculty VLAN (10): Full research/academic access with RADIUS-based authentication.
- Student VLAN (20): Restricted portal and lab access, controlled by authentication.
- Firewall: Segregates external traffic from VLANs.
- VPN Access: Allows faculty to connect securely from off-campus.

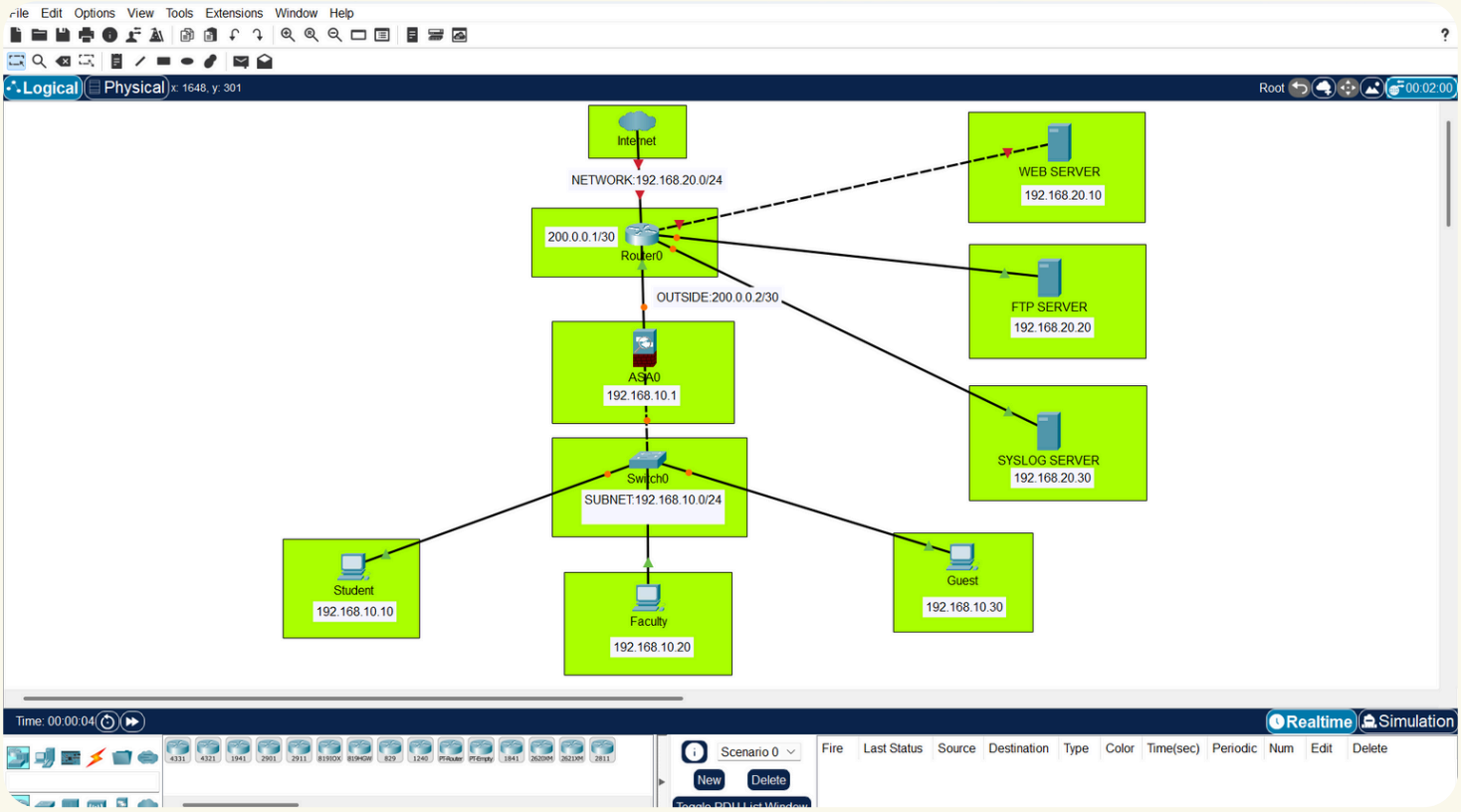
2.3 Risks & Fallback

- VPN overload → fallback to split tunneling.
- Authentication server downtime → backup local accounts.

Part 3: Web Access Policy Framework

3.1 Network Layout (from Packet Tracer model)

- Router and ASA firewall manage traffic flow.
- VLAN 10 Subnet: Students, Faculty, Guests.
- Servers:
    - Web Server (192.168.20.10)
    - FTP Server (192.168.20.20)
    - Syslog Server (192.168.20.30)



3.2 Policy Design

- Students: Block social media, torrents, gaming during class hours.
- Faculty: Full access, but log all activities.
- Guests: Only HTTP/HTTPS internet access.
- Time-based enforcement: Strict during working hours, relaxed evenings/weekends.

3.3 Technology Used

- DNS Filtering: Prevents access to blocked categories.
- Layer 7 Firewall: Stops application-based misuse.
- Syslog Server: Central logging of all events.

3.4 Enforcement Logic

- IF (User = Student) AND (Time = Class hours) → Block [Social Media, Torrents, Gaming].
- IF (User = Faculty) → Allow all, log activity.
- IF (User = Guest) → Allow HTTP/HTTPS only.