Going Manual: Preparation for a CyberAttack Among Puerto Rico's Electrical Grid System Personnel

Nuria Pacheco, Computer Engineering
Mentor: Dra. Zayira Jordán
Electrical and Computer Engineering & Computer Science, Polytechnic University of Puerto Rico

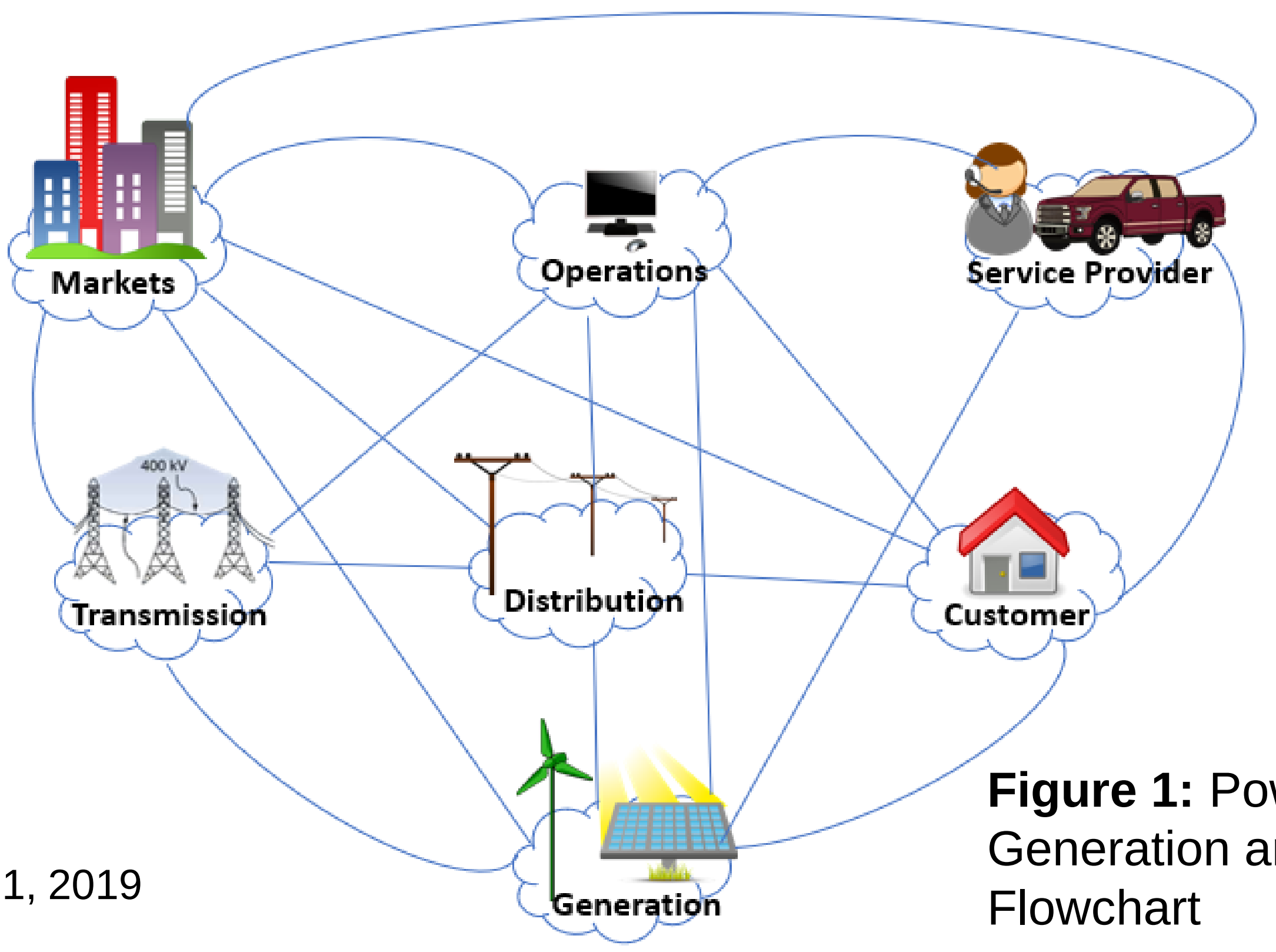
TITLE V STEM
POLYTECHNIC UNIVERSITY OF PUERTO RICO • SAN JUAN
BRIDGES TO STEM SUCCESS
P 0 0 3 1 C 1 6 0 1 4 1

Abstract

This research project was intended to assess the ability for Puerto Rico's power grid administrative authorities to respond to a cyberattack like the one documented in Ukraine in December 2015. The researcher gathered observations during an on site visit as well as interviews with Puerto Rico's Power Electrical Power Authority's (PREPA) personnel. Two simulations were used to replicate possible attack scenarios: 1) a Denial of Service Attack illustrated vulnerabilities in the grid communications infrastructure and 2) informed by the Ukraine scenario, we obtained access to the power networks using spear-phishing emails with BlackEnergy malware. The attack showed that 50% of email receivers opened the email without knowing that their credentials were being potentially revealed to the attacker.

Introduction

- **Smart grids are a great benefit to this generation, but there are also uncertainties over their security.**
- **Ukraine's December 23, 2015 cyberattack is the first publicly acknowledged cybersecurity incident to result in power outages and overhauled infrastructure.**
- **Taking this event into account, a better solution and recommendations need to be implemented to have a viable backup plan so that personnel can respond swiftly and no major effects are experienced by the population served.**



Smart Grid 101, 2019

Figure 1: Power Generation and Delivery Flowchart

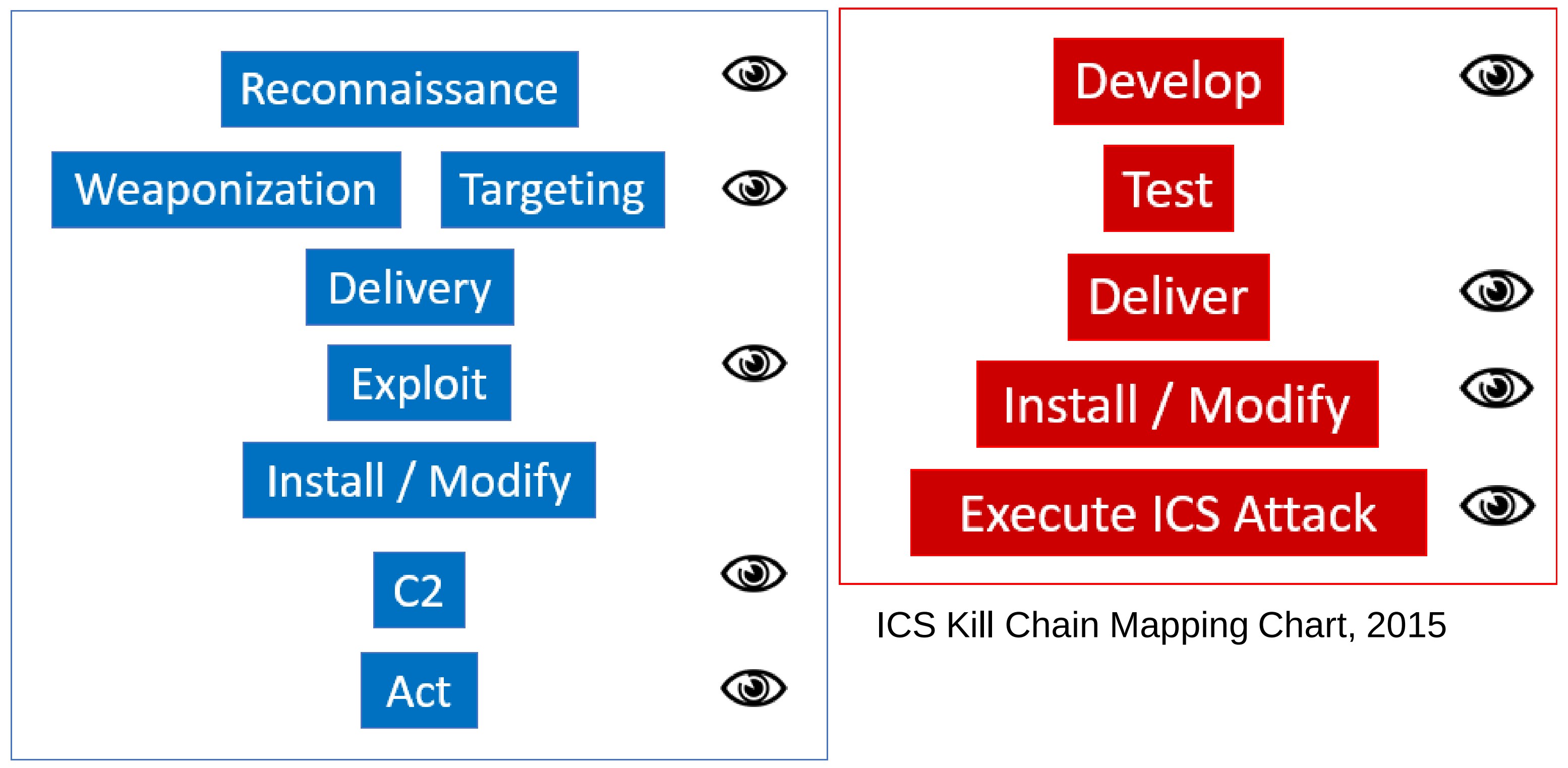
Objectives

- **Address the risk of personnel not being able to prevent, detect or rehabilitate after a power grid has been affected by a cyberattack.**
- **Present different kinds of cyberattacks that could affect a power grid.**
- **Present new alternatives and recommendations to better secure power grid vulnerabilities.**
- **Create a network map simulation and perform a DoS attack to analyze results and reach conclusions.**

Methodology

- **Tactics, techniques and procedures used in Ukraine's power grid attack.**

Figure 2: Stage 1 – Intrusion **Stage 2 –** ICS Attack



ICS Kill Chain Mapping Chart, 2015

- **An exploratory visit was conducted to PREPA command center to learn about power grid architecture components, as well as to analyze security, vulnerabilities, and perform interviews to the personnel.**
- **Lastly, a network map was created representing the PREPA network to create a Denial of Service attack simulation with the components obtained from the visit to PREPA command center.**

Figure 3: PREPA Corporate Network

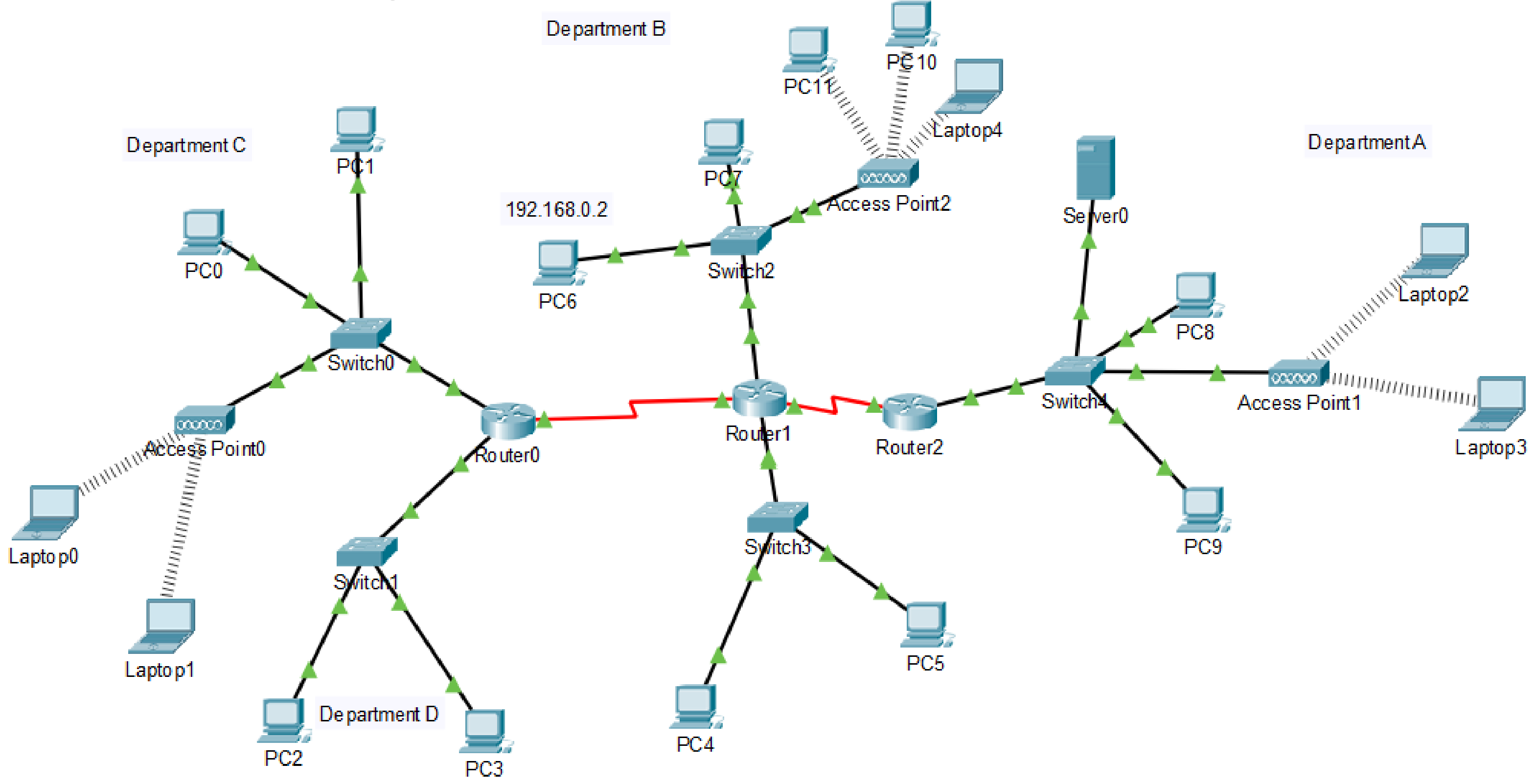
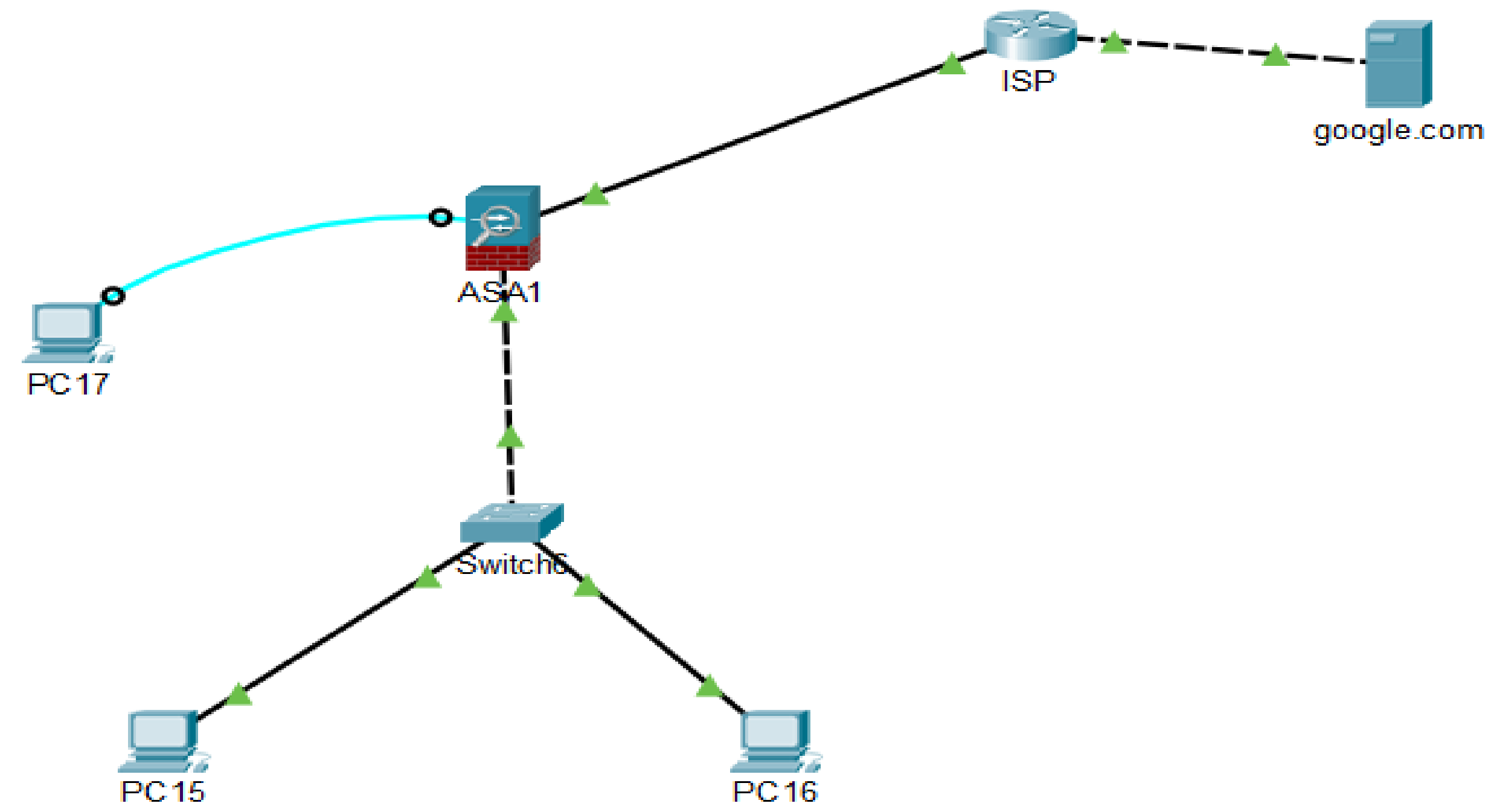


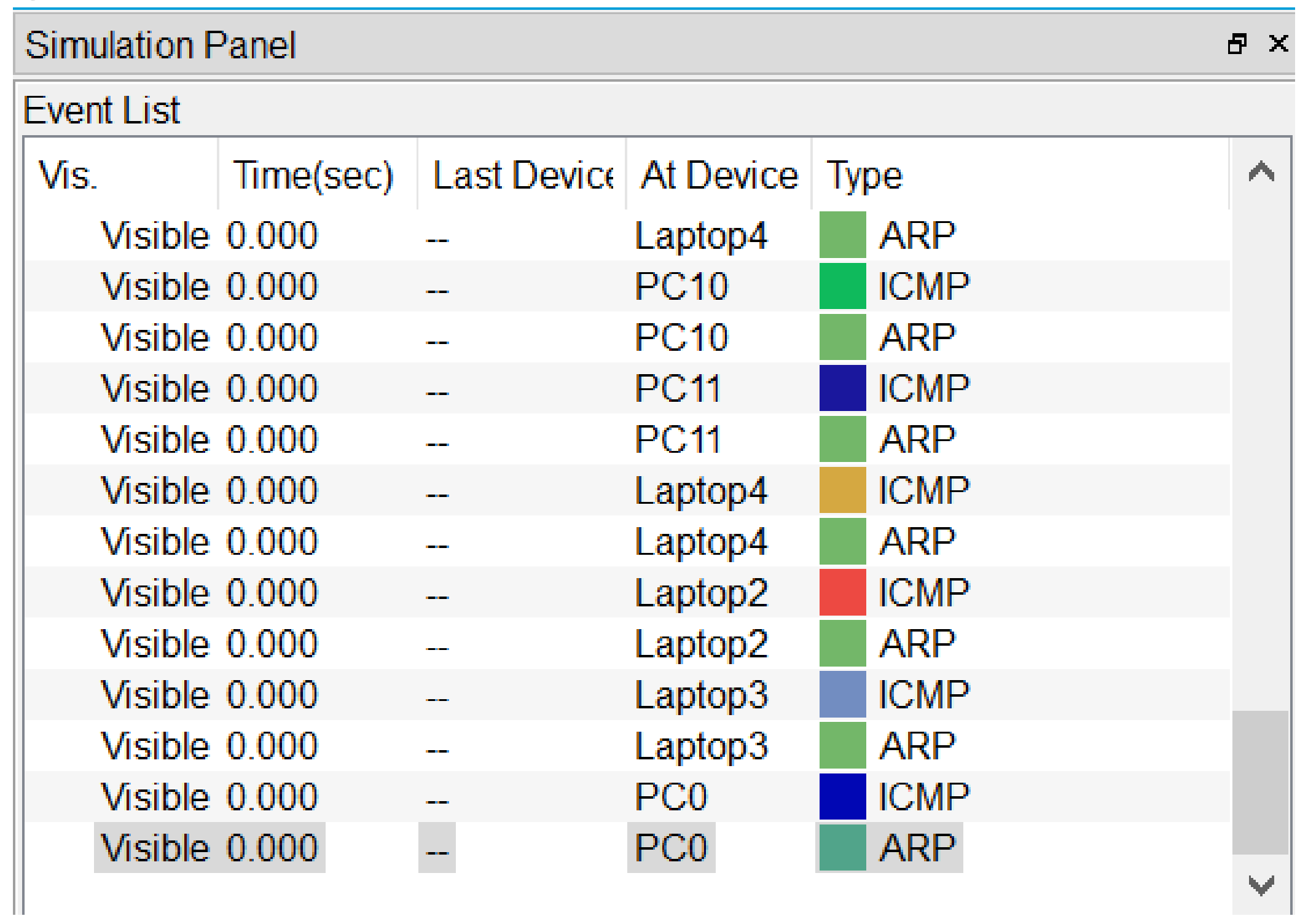
Figure 4: Attacker



Analysis & Results

- **During our visit to PREPA's command center some of the vulnerabilities found were: 1) having server cabinets open, 2) having only one person in charge of the network, 3) using computers with outdated OS versions, 4) having low physical security.**
- **As a next step, the simulation from Cisco Packet Tracer was completed. By targeting one user successfully, all network traffic could potentially be affected as well as other major confidential areas.**

Figure 5: Packet Traffic from Attacker Network



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
Visible	0.000	--	Laptop4	ARP
Visible	0.000	--	PC10	ICMP
Visible	0.000	--	PC10	ARP
Visible	0.000	--	PC11	ICMP
Visible	0.000	--	PC11	ARP
Visible	0.000	--	Laptop4	ICMP
Visible	0.000	--	Laptop4	ARP
Visible	0.000	--	Laptop2	ICMP
Visible	0.000	--	Laptop2	ARP
Visible	0.000	--	Laptop3	ICMP
Visible	0.000	--	Laptop3	ARP
Visible	0.000	--	PC0	ICMP
Visible	0.000	--	PC0	ARP

Conclusions

- **Taking these results into account, it is imperative to demonstrate the risk to PREPA workers, to improve their network against future attacks, as well as implementing more efficient solutions and training.**
- **To avoid any future danger, personnel needs to become more aggressive in security and provide more training to staff as well as recruiting more personnel to be in charge of the SCADA cybersecurity department.**
- **Lastly, some of the recommendations that can be given to enforce the security at the command center are: 1) update computer software, 2) disable all ports from computers, 3) prohibit the entry of foreign devices to the installations, and 4) upgrade entrance security and registration.**

Acknowledgements

- **Thanks to Dr. Zayira Jordan and the entire UPRHS faculty for your support and for being able to assist us students with numerous technical workshops and professional development opportunities.**