Computer Networking Experience gained during and after Disaster Management

A Capstone Project Report by

Sophia Carlone

Department of Computer Science

Submitted in partial fulfillment of the requirements for a

Bachelor of Science Degree with

University Honors

May 2024

Accepted by the Honors Program

2/29/2024

Advisor (Jeanna Matthews) Date

Ronny Bull

Honors Reader/Evaluator (Ronny Bull) Date

Honors Director (Kate Kruger) Date

ABSTRACT

In this capstone project, I will take a non-traditional approach recounting my time as a Lab Director and a member of the Clarkson Open-Source Institute (COSI) during a network collapse. Fixing the network also provided me with an opportunity to experiment with fundamental networking principles in a small-scale network as well as reinforce course material from classes like Computer Networks. This capstone project will present the work during this time as well as the challenges in recreating a network. It represents an opportunity both for me to support my own learning and interests, but also to improve the network of my lab and the network of people in the lab.

ACKNOWLEDGEMENTS

I would like to thank my capstone advisor and lab faculty advisor Professor Jeanna Matthews first and foremost for all the work she put into helping me in the lab and outside of it. Her flexibility, honesty, and hard work also shines through in this paper.

I would also like to thank the Computer Science chair Alexis Maciel for all the times he has helped me and the COSI lab and put up with constant questions from us. I also want to thank Madison Mahady for fighting for COSI. Every past and current COSI member who helped me during my time here at Clarkson also deserves a thanks as they have had a hand in this capstone project, especially those who were my co-lab directors / lab directors at that time, such as Jonathan Nordby, Sydney DeCyllis, Cary Keesler, and Juno Meifert.

Finally, I would like to thank my parents for their support and advice throughout my undergraduate career. More specifically, my mom for the “bee bops” at the end of calls and my dad who actively listened when I brought him into the lab and server room.

TABLE OF CONTENTS

TABLE OF FIGURES

i. INTRODUCTION

1. Inciting Incident

In December 2022, during Clarkson University's winter break, power failures and breakages were occurring at the Collins Hill campus. These caused hindrances to many labs on campus. For example, the Terascale All-Sensing Research Studio was flooded due to a broken water pipe, and they lost 1.2 petabytes of data. During those power failures, there were notifications on the Clarkson Open-Source Institute Discord server (the primary mode of communication within the lab community) that no one could reach the services that the lab hosts. Not only that, but the service that the lab members are most proud of, the Clarkson Mirror, was no longer running.

The lab had worked with outdated hardware for a while. In this case, the fiber switch being used to connect the servers in the server room to our co-location (COLO) and the Internet was showing signs of aging. For example, one of its two power supply units had failed previously. This switch (called F1) was vital to the network infrastructure and the hypothesis is that the power failures and possible power surges killed the last power supply unit, meaning that the switch was no longer operational. Without F1, students had no way to determine the status of the operations of the network.

2. COSI

The Clarkson Open-Source Institute, otherwise known as COSI or the CS labs, is a student-led lab under the Computer Science department. It can be considered a non-traditional lab where students' focus depends on their interests and desires. The lab values exploration of different topics of computer science that cannot be found in most classrooms and practice through programming projects. Students also learn by interacting with our server room, robots, microcontrollers, etc. There is an emphasis on teaching oneself and being open to learning from others. The lab highlights the use of free and open-source software by using/providing computers with Linux operating systems and hosts the Clarkson Mirror for anyone to download free software.

COSI also hosts its own network for its members to learn from. Connection to the Internet is provided by the Office of Information Technology (OIT), but every service vital to a network, such as domain name service (DNS), a firewall, and a dynamic host configuration protocol (DHCP) server has been created and improved overtime by the lab. Professors and students are also given the opportunity to host their research/project servers within the network. These run on physical servers kept in our main location server room on the Hill campus and in a rack in a university colocation facility a few miles away in downtown Potsdam that we call COLO for short.

COLO contains the main data center for Clarkson University and has backup generators and conditioned power (delivers a consistent and proper amount of voltage to servers). It hosts a rack for COSI as well as other local organizations. Compared to the server room on the Hill campus, COLO offers many advantages that prove to have more security in the event of power outages and power surges.

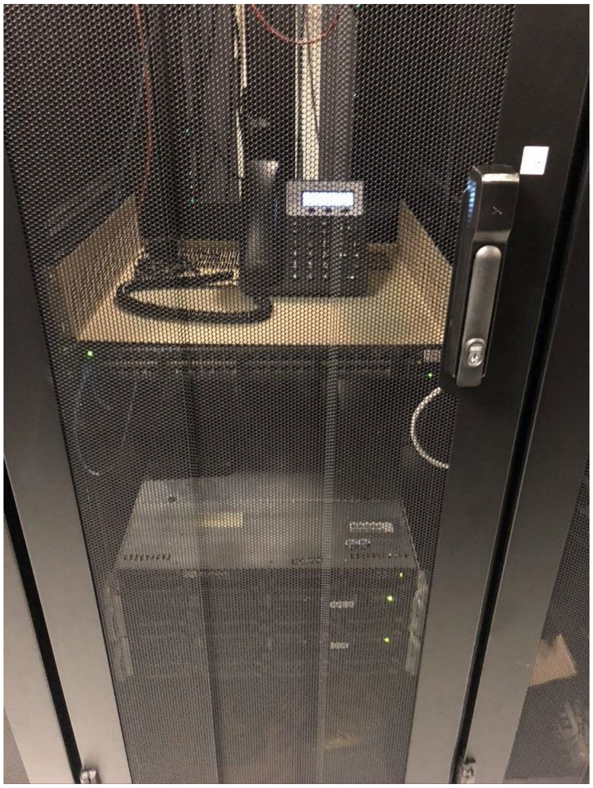


Figure 1. Picture of the COSI rack in COLO before the start of this project

Between these two physical locations, the lab can host physical machines and virtual machines. A physical machine is what most people think of when a server is involved. It is a physical computer that can go in racks, under a desk like a computer tower, or on top of a desk like a laptop. A virtual machine is an emulator of a computer system. It has to live on a physical machine to be able to access the hardware necessary to operate, but besides some sort of virtual machine manager software, it is separate from the computing system of the physical machine. COSI also utilizes other methods of virtualizations, like Docker for containerized software.

3. The Effect of the Power Outage

It was concerning for many of the lab members to not know what was happening back at Clarkson when the power outages occurred. Many people had work that was no longer accessible and the Clarkson Mirror was down. Based on what has been seen previously about the outreach of Mirror, there were an estimated 300 people around the globe downloading something from the website the moment it was disconnected.

Because it was during winter break, it would take a few days for those close to Clarkson to make some emergency adjustments. As the point of the breakage was known, F1 was replaced with another fiber switch the lab owned, relocated from COLO, allowing Mirror to be operational again. It was determined that Mirror was the most important service to restore because it had the most reach, satisfying over two million requests per day.

Many other servers had issues to be addressed as well. With the COLO switch relocated, the servers in COLO had no connection at all. One of the DNS servers was running on a virtual machine that could not be turned on remotely. Adjustments had to be made to the firewall rules to get some SSH access.

The state of the network was concerning, but it also provided new opportunities for change. The layout of the network and the services themselves have vulnerabilities that were apparent because of this disaster. Despite the setback, the ability to restart a network almost from scratch provided a great learning experience.

4. Immediate Actions Taken

After Mirror was back in order, the rest of the network needed attention before the start of the new semester. Along with other lab members, I arrived at Clarkson a few days before the start of the spring semester in order to focus on restoring as many vital components as possible.

Firewall. The operating system of the firewall was reinstalled with Ubuntu because of its user-friendliness [5]. Originally, the firewall rules were created with iptables that filter out ip packets, but this was replaced with nftables as it is very similar to its predecessor, but is better in scalability and was created for the purpose of fixing problems found in iptables [6]. Rules were copied from the previous configuration, with slight modifications to reflect the current accessibility status.

DNS. Authoritative DNS servers maintain the definitive translations of machine names to IP addresses. Recursive name servers iterate through a series of requests on behalf of clients and possibly cache copies of translations. The lab's recursive DNS server was on a server named Talos. The authoritative DNS service was on a virtual machine named Atlas. Reinstalling the operating system and DNS configurations was relatively easy, but there was a problem with Atlas because the host server that the virtual machine lived on was not operational. It was determined that having a non-trivial piece of the network dependent on another server was not optimal. In light of this, both DNS types and a related service, DHCP, were placed on Talos when its operating system was being reinstalled. This meant the lab only had one DNS entry in OIT's own DNS.

Other. Backups of all virtual machines and code repositories from Gitea were stored on Mirror. New hardware was researched as replacements for the fiber switches and an initial plan was created as an ideal for when more students arrived at Clarkson.

Documentation is an important part of the sharing of knowledge, and so the documentation of the server room is a continuous effort throughout this project. When a server/service is configured or reconfigured, the lab writes down details that should benefit future lab members. For services such as DNS, what specific software is used and copies of the configuration files are documented, and the operating system and hardware specifications of servers are also written. All of this is stored on the "COSI Book" hosted at book.cosi.clarkson.edu.

5. Initial Plan

The initial plan was more of a "To Do" list while new hardware meant for replacing the broken/old switches was being purchased and delivered. This was an "ideal" plan, meaning that factors of the network recreation were assumed in an idealistic fashion. Assumptions were made about when the new hardware would arrive and how many lab members would be active in executing the plan. Sadly, some expectations were high because of difficulties with delivery. There were also periods of other lab members not showing up after volunteering, as well as limitations on students' schedules.

It should also be noted that in my lab we value teaching as well as learning. For that sake, there have been times where I let others work on a piece of the network as I explained what they should be doing, how what they did/are doing affects the network. There were also improvements by other members that I was not involved with. Those I will recognize, but summarize.

Instead of listing all the “to dos”, I will describe key steps in the plan envisioned at the start of the Spring 2023 semester.

Step 1. While the infrastructure had the vital components to work as a baseline network, it was not at full capacity because there was no connection to COLO. An order would be placed for two new Mikrotik fiber switches as soon as possible. During the wait for them to be delivered, the lab would focus on fixing the broken pieces that were accessible. Figure 1 illustrates what the network looked like at this time. This is called a network topology and indicates the major machines, network segments, and the connections between them. Note that the global Internet is indicated with a cloud. This initial topology only lists what is on the Hill campus since there was no COLO access at that time. F2 is the switch that used to reside in the COLO rack until it replaced F1. The lab has Ziltoid, Mirror, Talos, and a few other servers like our docker container host, Tiamat, but servers are missing compared to later desired topology. The intention here was to get servers like the virtual machine host, Hydra, operational for student projects. Updated DNS entries and firewall rules were expected as this continued. This also planted a perfect opportunity to update software on these machines and reorganize what was needed and where.

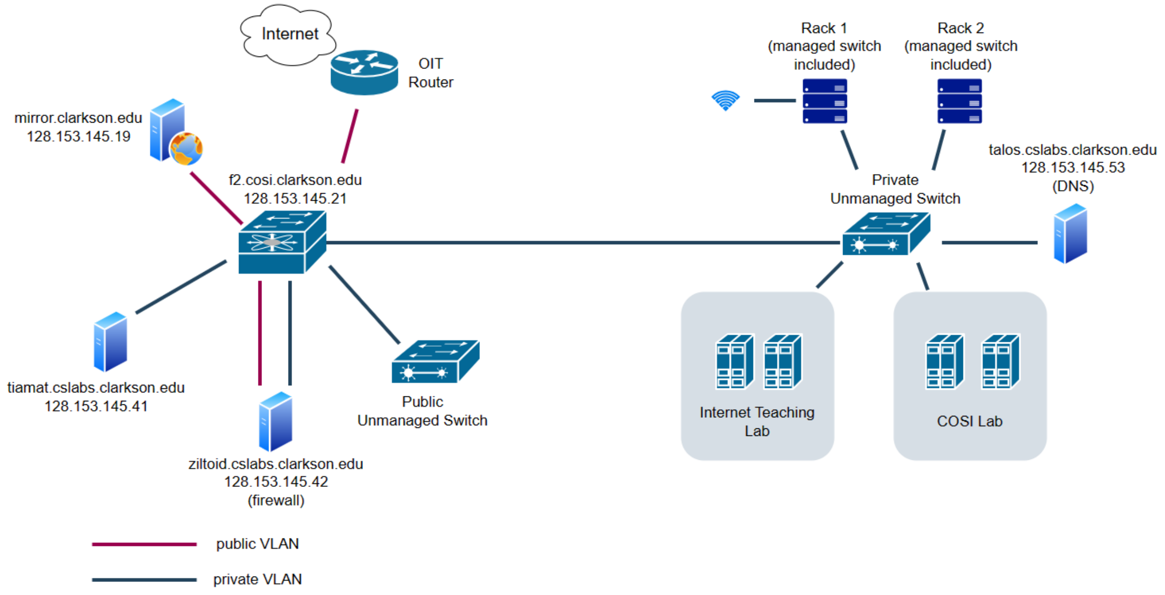


Figure 2. Topology of network at start of the project

Step 2. When new hardware purchased arrives and is installed, that would allow reestablishing a connection to COLO. This connection would need help from OIT. After this, the network would be as it once was in terms of physical space capabilities for running servers, but with some adjustments for security so that the inciting incident would not take down the network again. There was another diagram made for the desired topology of the lab network created by another lab member at the time of the initial planning with minimal feedback. Note that there is now FHILL and FCOLO, representing the fiber switches in the different physical spaces and the connection between them. There are differences from what ended up being the finalized topology, like two different paths to the Internet (represented by the cloud), VLAN allocations, and server placement.

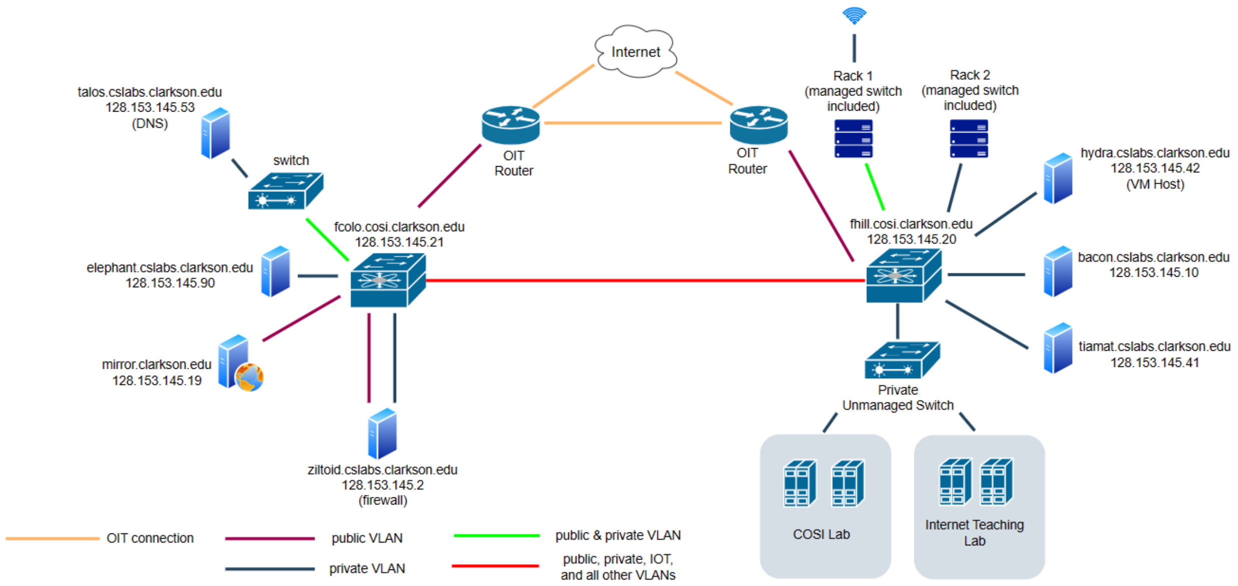

Internet
OIT Router
OIT Router
Rack 1 (managed switch included)
Rack 2 (managed switch included)
talos.cslabs.clarkson.edu 128.153.145.53 (DNS)
switch
fcolo.cosi.clarkson.edu 128.153.145.21
elephant.cslabs.clarkson.edu 128.153.145.90
mirror.clarkson.edu 128.153.145.19
ziltoid.cslabs.clarkson.edu 128.153.145.2 (firewall)
fhill.cosi.clarkson.edu 128.153.145.20
hydra.cslabs.clarkson.edu 128.153.145.42 (VM Host)
bacon.cslabs.clarkson.edu 128.153.145.10
tiamat.cslabs.clarkson.edu 128.153.145.41
Private Unmanaged Switch
COSI Lab
Internet Teaching Lab
OIT connection
public VLAN
private VLAN
public & private VLAN
public, private, IOT, and all other VLANs

Figure 3. First draft of desired topology diagram

Step 3. Keep improving and maintaining the network. There is always room for improvement and many different members had different project and research ideas that could have been used in the network. For example, in the past there have been “Honeypot” servers and a variety of websites to name a few ideas. With each new idea brought in, there were different ways that it could fit into the network and how other services would have to adjust to the new addition. We also hoped to deploy network monitoring as a way to tell lab members sooner rather than later if a service goes down and/or how the network is performing.

This plan was a great start in order to get the network back to where it started, but the situation evolved over time. Packages arrived at times unknown to the lab and there were changes to ideas and timelines along the way. Therefore, it was determined that the best documentation for this project would be a “development log” to act as a journal to document what was learned and experienced along the way. The aim was to help in this capstone project as well as to be a sort of fun history for the lab.

6. Defining Success

First and foremost, a sign of success was checking the boxes of the initial “to do” list to get ready for the hardware to be ordered. Afterwards, another sign of success was having a connection to COLO with all the servers there operational.

Also, the desired topology presented before was a great starting point, but there seemed to be places of redundancy and places where it could be much simpler for the lab members. Not to mention, there was a lack of security and resiliency for the servers the lab values most to keep running. An implemented topology where all this is accomplished would be another form of success in terms of presenting what has been learned. This new topology would need the approval of the lab.

If there is time for improvement, other signs of success could be in balancing the loads on switches. For example, can there be better through-put, or ping latency compared to the start of this project? Comparing this to the network before will be biased as there is none of this data from the previous state of the network, but if there is a determination of improvement in some way, that would be a success. Having the most updated documentation for the network will also be solid proof of improvement. There is also room for improvement in the idea of software creation, but that is dependent on time and resources of the lab and its members.

Last but not least, an element of success is how much the lab members learned during this process. Those interested in networking have a great chance of learning something new during this process. Even those who have worked with the server room before or have taken a class should be constantly learning or teaching others.

ii. LITERATURE REVIEW

This project will build on a foundation of knowledge in computer networking (e.g. courses such as Computer Networks) and information about the pre-existing COSI lab network that was taught from previous COSI members and throughout my time at Clarkson. In this section, there will be an overview of the major activities and best practices in network management to provide additional context.

1. Network Management Definition

First, there should be a definition of network management. An article by Hari Subedi, "Network management best practices for businesses" is helpful. As Subedi writes that "Network management refers to a system consisting of processes, tools, and applications that help in the administration, operations, and maintenance of a network infrastructure" [10].

This same source mentions that networking involves four main functions of provisioning, configuration, security, and network management and five functional areas of network management being fault management, configuration management, performance management, accounting management, and security management [10]. Most of these functions align with other sources on the topic of efficient network management even if the exact names differ [8] [3].

2. What needs to be done for COSI then?

When applying these general best practices to the COSI lab, it is important to consider how the needs of the lab may be unique. For example, many articles are geared towards businesses and may not include the educational function of our lab. Most network management attempts to keep network resources stable, secured, and unmodified unless necessary. The COSI lab wants to encourage student learning and experimentation, therefore it is better to keep in mind that the network will be modified to the ideas of the lab members. Also, the network is relatively small and some large-scale or highly automated systems might be inefficient. With that in mind, here is how COSI compares in each of the five functional areas recommended by Subedi [10].

Fault management. COSI is a group of people who frequently use and work on the lab network. It is a plus that knowledge is aimed to be passed down so that at least some lab members can identify problems and either have the knowledge or know where the resources are to fix the issue. Within the accumulated knowledge lies the fault management as students come and go.

Configuration management. In a time where the network is not broken, the configurations are all up to date and working. These configurations are documented in code repositories or on sites such as book.cosi.clarkson.edu. If this is not the case, all software used is free and open-source, and therefore should have documentation online. The lab also uses webhooks for configurations like that for the DNS entries.

Accounting management. The lab likes to give server accounts to those who have any interest, but limit those with full administrative privileges. Users are not tracked for the sake of privacy unless alerted to someone not following the conditions of having the agreed upon accounts.

Security management. COSI has a firewall up and running that was created by members and can be adjusted anytime. There is also help from OIT’s firewall for services like Mirror because if that was exposed to any malicious intent, those around the globe that use it can be at risk of malware.

Performance management. The lab members have performance management for Mirror only.

Based on this assessment, this project should also look into improvement of network performance management. This could be done by using very simple means that tells members when something like a server is not working properly.

Performance management, also known as network monitoring [9], as its name suggests, involves monitoring how the network is running and each of the devices in order to know sooner when something is wrong. “A network management solution typically works by collecting key network performance indicators in real-time from the network and sending it to a centralized server, which can be on-premises or in the cloud. The collected data is then analyzed by a control application to give meaningful information to the engineers who can then make necessary changes to network devices such as switches, routers, access points, etc.” [10]

The primary goal of this project is restoring network functionality lost as a result of a power failure in December 2022, but additional performance management is a secondary goal. In other words, getting the network back up is the main goal, but there is also a desire to improve it in some way. There could be a proposal of some novel management strategies such as using a Discord bot (Discord being where the lab communication happens) that tells members when a device no longer has a connection. This idea can be advanced to do more than detect connections. It can send signals of faulty behavior.

3. Network Monitoring

Many network monitoring applications are not open-source [9], but the COSI lab prefers to use open-source software. With most organizations who have networks also having money to spare, it seems a common practice to do as described: “An organization may outsource some or all aspects of network management to a managed services provider (MSP)...” [3]. Luckily, the

Open-Source community this lab gets its namesake from has come to the rescue with their own network monitoring applications [1]. These will all be useful for this capstone, especially, the Simple Network Management Protocol and the tool Telemetry.

4. Simple Network Management Protocol

All sources mentioned a Simple Network Management Protocol. “Simple Network Management Protocol (SNMP) – an open standard protocol that queries each network element and sends responses to the system for analysis” [3]. Because it is a relatively old protocol, it can work on a multitude of devices, but like most less updated protocols, there are still some implementation issues across different platforms. [11].

There is some uncertainty as to if an implementation of SNMP to its full potential is wise for the labs because it can fix nodes on its own, which we would prefer the students to do, but it would still be useful to know when something is down. The lab would have the option to have unidirectional (read-only) access to node information which may be preferable [11].

5. Telemetry

Another option the lab has is telemetry. “Streaming telemetry – a protocol that transmits key performance indicators from network devices to the system in real-time” [3]. The idea of a streaming service could be a wonderful tool in network management. Looking for a definition, what is found is that “telemetry is the collection of measurements or other data at remote or inaccessible points and their automatic transmission to receiving equipment for monitoring” and it has the main points of being a data exporter, collector, and analyzer [4]. This seems to also be helpful with my idea for alerting lab members.

6. Which of these two are better?

Something researched while comparing the two is that "SNMP is used best when retrieving relatively static data, such as inventory or neighboring devices. Its polling mechanism makes collecting high-volume, high-resolution performance data a challenge" [7]. The same source also says, "Streaming telemetry is better for collecting high-resolution performance data, such as high-speed network interface statistics" [7].

Telemetry seems to have implemented solutions that are problems in SNMP [12], but also might not be supported by older devices [7]. It was a Google project and is meant to replace SNMP [12]. It has been made for more use cases as SNMP works on UDP while Telemetry uses both UDP and TCP [12]. Though, another bright side for the old protocol, SNMP allocates memory more efficiently than telemetry [7].

It is not surprising that there are tradeoffs. Something taught in the computer science major is that there are tradeoffs for most things; protocols, data structures, algorithms, etc. These tradeoffs must be analyzed in the context of this particular use case. There is a debate between wanting something that is new and hopefully will be more supported and/or have less bugs, versus SNMP that most devices can use and memory can be used more efficiently. There are capabilities to combine the two tools though. A network can use a combination of both when there is old and new hardware [7]. That may be more complicated, but something that is worth a try.

iii. METHODOLOGY

1. Identification of Malfunctions

The bulk of the knowledge of what is malfunctioning in the lab network at a single point in time is from something referred to as “scream testing.” That means most of the malfunctions that occurred are known because someone tried to use a server/service, and when they could not, they told the lab directly. An example of this is the first time the lab members found that no one could connect to the network during winter break. It is also how the network maintainers now know that while the servers can reach the Internet, users cannot SSH into said servers.

What could also be used is connecting to each server or service, and either manually or using some type of program, making sure each is running, fully functional, and has the connectivity that desired. This method would be time consuming for the students.

2. Comparing to Best Practices

As mentioned in the literature review, there are some best practices or key areas of a network that the lab network should follow. The performance management is the area where COSI lacks in the network. There is currently no monitoring besides what was implemented for Mirror. If maintainers are able to know when something malfunctions as soon as possible, the number of “scream tests” would decrease and problems would be solved much more quickly.

3. Suggested Improvements

Because of this lack of performance monitoring, part of this project is enhancing our network monitoring abilities. To do this, the lab could have a Discord bot. The purpose of this is to create a small application that alerts if a server can be “pinged” (can be reached by the bot) so that lab network maintainers know sooner when something has gone wrong. This may work best because it is a relatively easy program to create and understand, meaning it can be modified in the future. It would also appear where all members of the lab, even if they work directly with the network or not, could see what is currently happening and stay up to date. Many lab members have notifications for Discord and would see it much faster than if it was hosted on some type of service people would have to remember to check. For the large network monitor, it's just the process of utilizing a server to host the monitoring program and build it based on research conducted previously. This would be a time permitting and engagement depending task.

4. Overall

It is hard to place into writing all that is needed to do throughout this project because the possibilities of what may happen are endless. Different services and tasks require different methodologies themselves. For example, reinstalling an operating system is much different than setting up nftables for a firewall. There will also be breakage in software and hardware that no one prepares for beforehand. The skill here is the flexibility to save time to fix whatever comes the lab’s way. People who have more experience will be able to understand a problem, fix, and teach solutions sooner, while other issues may be new and have to take some time looking through documentation. The precedence here is to find the source of the problem, determine if it can be solved, and if so either use someone’s current knowledge and learn from it, or teach oneself the concepts needed to get the job done.

iv. PRELIMINARY RESULTS

Since the beginning of writing this proposal, progress has already been made. Not everything can be done as the lab waits for hardware and other materials to be delivered, and so the focus has been to get up the more important servers for the students and faculty.

1. Hydra

This server is the virtual machine host. There was no connectivity to this server while the network was down. Since the semester started, members were able to back up all the virtual machine files, update the operating system, rerun the virtual machines, and keep it connected to the students who have projects on it. This last point is important as there was a time of no connectivity after the virtual machines were set up, and after an investigation it was determined that the UFW or uncontrolled firewall each Ubuntu server has was blocking the SSH port.

2. Ziltoid

This server is the firewall. During the first few weeks of the Spring 2023 semester, the lab had to learn about and implement nftables. The firewall would be able to accept packets from the ip addresses and ports chosen for different servers, as well as allow paths for students to SSH into servers in order to adjust and work.

3. DNS

The lab also runs its own DNS (Domain Name System) server. There are two types of DNS servers: recursive and authoritative. Before this semester, each was hosted on a different machine. One was a virtual machine that could not be used while Hydra was down. In order to have less dependencies on Hydra, the labs moved both the recursive and authoritative DNS protocols onto one server that is called Talos. Talos also had its operating system updated and it also functions as the DHCP server for the network. Both the DNS and DHCP protocols were reconfigured.

4. Miscellaneous

The lab has also worked hard to reconfigure and manage the physical network. This means more organization and labeling in the server room, setting up managed switches to have the correct VLAN (Virtual Local Address Network) configurations, and simple cable management.

v. DEVELOPMENT LOG

This section of the paper will be a journal-like writing of what was worked on, when, and what problem solving and ideas were thought of. The writing will be paraphrased for conciseness. For the full development log, please refer to the appendix for the website that it is hosted on.

The summary of this log is as follows. There were problems with the switches ordered and they did not arrive until the start of the Fall 2023 semester. During that time, the servers on the Hill campus were all updated and operational. Students were able to host their virtual machines and websites as needed for personal and class purposes. There were many issues with server hardware failing, including Ziltoid and Talos. Replacement of parts or entire servers were made to counteract this. Some of this hardware failure allowed the labs to create some safety systems in the network such as a primary and secondary DNS server with both recursive and authoritative properties so that one could be a back up if the other fails.

What I am most proud of is the creation of a new topology I created. This was approved by the lab members that came to participate in a meeting for feedback. It went through different versions, but it was made with simplicity and security in mind. There is only one point of access to the Internet to reduce the different pathways and make the network simpler. It moves our firewall, Mirror, and DNS with room for other servers (like ones used for management bots) down to COLO which is backed by a generator. Only the VLANs currently used are part of the network, with the private VLAN being the only one reaching the main lab. The simplicity has tradeoffs, but was liked for its understandability for future new lab members.

This topology was put into place in February 2024. Led by myself and the lab directors, seven people in total came to help as we split up into two teams. One team was focused on the server room to move servers around, and the other in COLO to place Mirror, TalDOS, and Kasper into the rack there. Though there were connectivity issues at first, the problems were solved by the next day. The organization of the servers also met with conflicts, but was done as well. The topology has been implemented and working.

January 2023

- COSI network not working properly. Some people went up to get Mirror running. Afterwards, I came up early to the semester to get DNS, DHCP, ziltoid OS, and Talos OS reinstalled.
- Working on getting the virtual machines (VM) on Hydra running after reinstalling the operating system with two lab members, one of which has never done so before. I must be able to challenge my assumptions. Qemu was not working out this time, but I can always try again in root because that was needed when transferring the backups. Plus, it may have groups that can use Qemu and my user may not be in that group.
- I was able to transfer VM files correctly, but there were differences on what I expected the operating systems of the VMs could be (Ubuntu 22.08) vs what they had to be (Ubuntu 20.08).
- I could not SSH into Mirror. I tried checking my SSH configuration, and from different entry points. The problem was the SSH-keys used to get on the mirror were for my windows machine and not my arch-linux machine. The only way you can get on the mirror is if your keys were added.
- There seems to be a bottleneck problem in which all network packets go through our private VLAN which share a 1GB connection.

February 2023

- Hydra: I had to redo the partitions (add filesystem then mount) which did not work before because we were one letter off in making them before. We then created pools with zpools (had to also write nothing to all partitions)
- Learned what a "scream test" is. It is when you do not know something is broken until someone complains or talks about it. A research student with their servers Red Dwarf and Prometheus being hosted by COSI could not reach those two to obtain research. I tried to see if it was a faulty ethernet connection, but then saw that the switches on top of the racks they were in were not connected to our private switch. After connecting them to the private switch again, I tried to ping, but got a "Destination Host Unreachable" error. My ideas: plug my laptop directly into those machines and use the nmap command to look at the results. Or a user on those machines may be needed.
- My fellow lab director, Jonathan, and I went down to COLO to talk with OIT. We explained the situation and said they will get a connection ready for us in COLO.
- Going back to Red Dwarf, I tried testing cables again. I learned how to test ethernet cables and was advised that should always be my first course of action. Because that still did not work out, the plan is also to have a direct connection to the switches these servers connect to in order to obtain the webGUI. This is something I learned to do when trying to get our firewall connected.
- Trying to run the newly restored VMs on Hydra, I learned that I could SSH in a way to get the virt-manager application on my screen: "ssh -X hydra virt-manager". This is nice, but also very slow and volatile. The SSH connection was closing on me just from using the backspace button too many times.
- Time to reorganize cables for less mess!

March 2023

- I have ideas to make a Discord bot to help students know what a server goes down. It would also be nice to show data such as throughput on a visualization.
- The firewall went down. I could not help due to a personal family event.
- First time making a VM for one of my class projects. There needs to be a network bridge in the VM server host to have the VMs and the host talk to each other. You can also SSH into a VM if you are one the host no problem.
- I learned that we could not SSH into COSI from outside the COSI wifi. This included the introduction of two things, holes in the firewall for users to get in.
- I learned from a presentation from a NASA employee, as soon as someone is in a network, it is so easy to move through it.
- The fiber switches needed to connect to COLO will not be in for another 11 weeks.

April 2023

- It would be a good idea to reset some of the root passwords for servers.
- I may have brought Hydra down (destroyed its connection) when I worked on it last month. I tried to rewrite the bridge from the month prior, but that did not work. After a while, we noticed it had no route to a computer in COSI or mirror, but it could connect to Google. This is nice as it can download updates, but something is still clearly wrong.
- Another thing I noticed on Hydra was that it did have a hole in the firewall, but it was on a non-standard port (not port 22 usually used for SSH). Hydra's SSH configuration file still uses port 22, which could be another reason why it is not working. We try to have a standard port for SSH in our lab that is not port 22 which is commonly used. Connected to the firewall from Hydra worked.

- A lab member, Peter, told me about the "syslog" or more importantly, that you can use the command "tail -f /var/log/syslog". The syslog is the system log that lists what is going on in your operating system. I knew about this, but now how it could apply to network debugging. The command specifically will allow the end of the log to automatically refresh. This is nice in order to watch in real time how the system responds when you do things like SSH, place it in a flash drive, etc. This is where I noticed something called UFW BLOCK that was blocking the port for SSH. Turns out, Ubuntu has an integrated firewall for the server you are getting the operating system on. It is called "Ubuntu firewall" (UFW) and it is automatically enabled and blocking ports including the one I needed. All that time, all I had to do was use the command "ufw allow port X" and now everything works. I applied this UFW knowledge to VMs I could not get to previously.
- I was trying to get the switch connected to Red Dwarf out for over an hour. It was physically stuck and those I asked for help could not even get it. The sides of the server (called "ears") that allow the us to screw the server into the rack are stripped.
- I inserted a replacement switch and configured its VLAN settings for our public and private VLANS. We are now able to ping Red Dwarf.
- I learned a little bit about types of cables from another COSI member. Most importantly, ethernet cables use rj-45, but they are not rj-45. This means the ethernet cables have 8 pins for their wires to go in a certain configuration, but other types of cables could have the same 8 pins.
- During some more cable management and clean up, we had to unplug the firewall and DNS server. I stepped out for a bit and came back to see that those I left were still working on getting DNS backup. I took a look and the service that runs the authoritative DNS (called nsd for network service discovery) was disabled. All that I needed to do was restart the service.

July 2023

- Talos is breaking down over the summer. Which means our DNS was going down. For a bit, we need someone who was on campus to physically reboot the server.
- It seems nsd.service is failing on boot. I learned about “systemd” for services on the system in order to get the configuration file for the nsd.service. I was able to change it so that when powered on, Talos will try more times to restart the nsd service. In the process of this, I also learned that crontab, which is a job scheduler for processes on the system.
- The problem was the nsd.service was failing on boot with error saying it was "restarting too quickly" through some research of the problem in systemd, turns out that package has files in /etc/systemd/system/multi-user.target.wants in which you can adjust how systemd interacts with the service. Since it was being restarted too quickly, you can find that among all other commands allowed and not there by default, there is StartLimitBurst=x where x is an int that represents how many tries to restart the service, and StartLimitInterval=x where x is an int that sets how long in between each restart attempt.
- Before that, there was an error on Talos for saying the network was unreachable. The cause of that error was not determined and seemed to go away after fixing nsd.service.

September 2023

- The new fiber switches that are needed for a COSI-COLO connection finally arrived about a week before the start of this new fall semester. I invited people to join me in setting up those switches. More people than I expected came and it was hard to fit in the server room and I didn’t know what to do with everyone who showed up.
- I learned a command: “ip address add <ip address> broadcast + dev <connection medium>” because I need to be on the same network via IP address on a direct

connection to the new fiber switch in order to configure it.

- I learned a bit about the Mikrotik routerOS. This includes terminal commands as well as differences for this new way to configure a router. For example, I could not make a VLAN with multiple ports like I am used to. I must make a bridge that connects the ports and place a VLAN on that bridge.

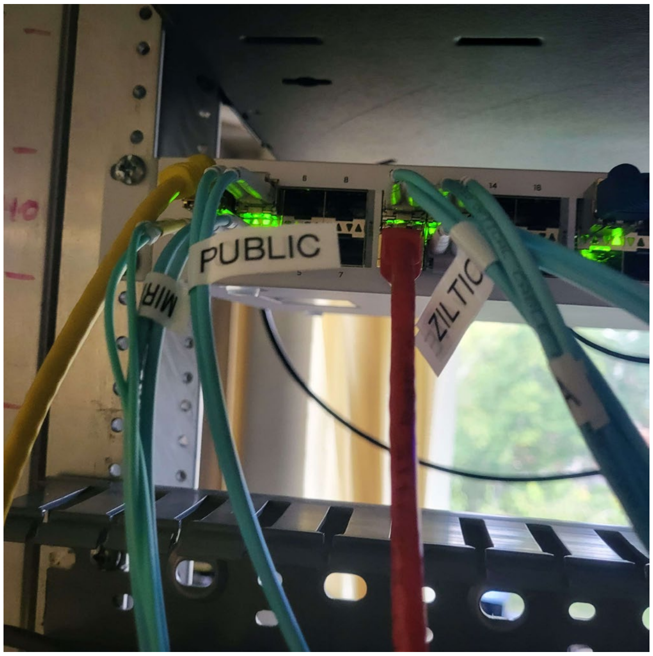


Figure 4. Image of new fiber switch (FHILL)

- I had some trial and error with the configuration of the new switch. It may have been due to the extra elements in VLAN configuration that I filled out, but now they seem to be unnecessary. Myself and my fellow (new) lab director noticed that there was an error in the firewall for packets to go to this new device. After changing the IPtables used for our firewall, we actually took down more of the network, including our weekly meeting tool: talks.cosi.clarkson.edu. We also made sure that we were using the correct transceivers for each port/connection used.

- After changing the PVIDs of the VLANs and the ip address of the switch in order to get it to comply with the firewall, it seems everything was fine except for the connection to Hydra. I realized that the difference was that before this new switch, Hydra expected to be on the private and public VLAN, but now it was only set on private. I asked if there was anyone who wanted Hydra to stay on the public VLAN, and after setting it to only have access to the private VLAN which made everything simpler and work. There was then no longer a bridge on Hydra.
- Talos stopped working because of a hardware issue. More specifically, a memory stick issue. Sadly, this is not too uncommon because our hardware is getting old. Thankfully, we had a more recent server (from 2011) donated by a COSI alum. I named that new server TalDOS and was able to get DHCP, and both types of DNS on it. Because the hardware was still old, it could not recognize Ubuntu 22.04, so we had to get an older version of an operating system. Another lab member took over at this point to finish the job. They changed the operating system again and reinstalled everything needed.
- During my discovery that TalDOS' kernel was outdated, I did poke around in the grub configuration for the first time.

October 2023

- I created a new network topology in the labs to reduce redundancy, place the more vital servers where there is a backup generator, and make it all more easily understood. Each time I received feedback from others. There are some servers that may or may not be moved due to spacing in both COLO and Hill locations.

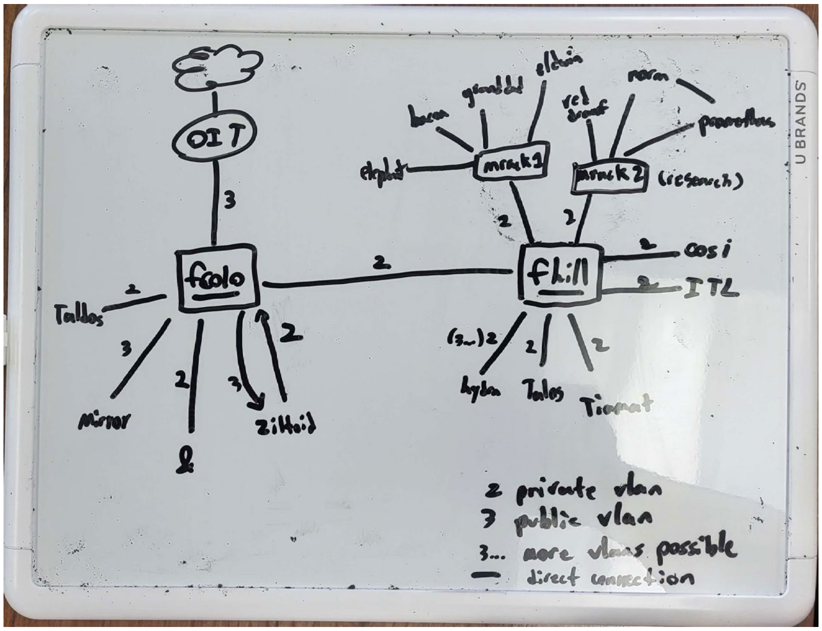


Figure 5. Newly Created Topology Version 1

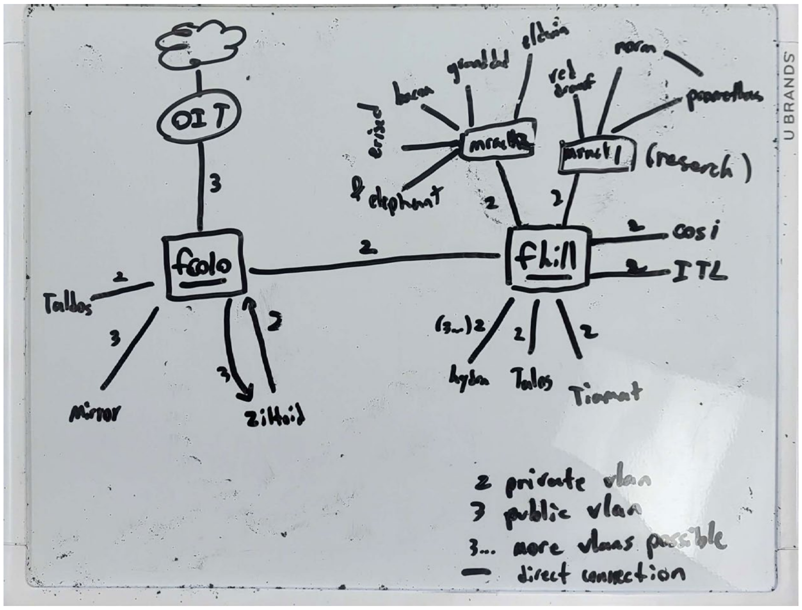


Figure 6. Newly Created Topology Version 2

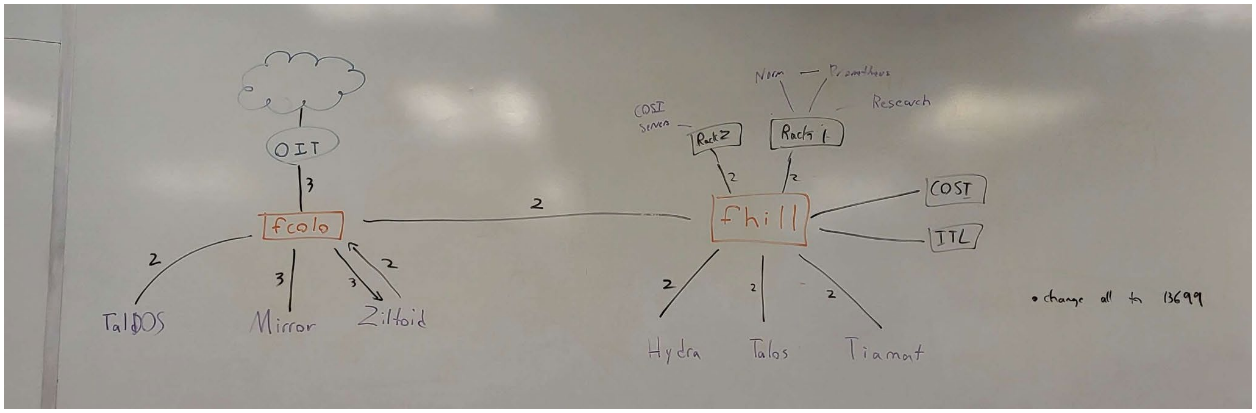


Figure 7. Finalized Topology

- One concern about the topology was the accessibility to the servers in COLO since only three people can access that location at the moment. One possible solution to this would be using a KVM over IP. This is a device that would allow us to connect to COLO even if the Internet went down at the hill. This would be a project after the topology is implemented and could either be bought or made ourselves using a raspberry pi. The information about this I was using was written by Don Hui in 2021 on Tom's Hardware website [2].
- We have had some big developments this month. My fellow lab director was trying to get a connection to COLO, which broke our network for a weekend. We had to wait for OIT's help since it was a connection to one of their switches. OIT said the problem was with the transceiver used.
- Even after that was fixed, we still could not get a connection to COLO. It is most likely that it is our fiber optic cables that are broken. More will need to be bought. When purchasing these items, I learned that there are different types of fiber optic cables. There is a multi-mode or single-mode type that determines the width of the passage the light can travel through the connector. There is also LC UPC and SC UPC. UPC means there

is Ultra-Physical Contact and LC vs SC is another size determination. For COSI, we needed LC UPC to SC UPC, duplex singlemode cables.

November 2023

- Before Thanksgiving break, we finally got the fiber optic cables in. The old cables were switched out for these new ones. Connection has been established between COSI and COLO.

January 2024

- Getting right back into the school year, it has been a long time since someone regenerated the passwords for our devices. One of the new switches has a password of "password" for convenience and was never switched to something else. It would be better to change most of those that have been used for many years. Also, the lockbox that the lab directors are able to unlock that hosts these root passwords is very outdated and messy. I created a new password template with an emphasis on marking the date it was made, so that there would be no mistake on which information is the most modern.
- I created a plan on how a server moving day (now being named THE GREAT COSI MOVE OF 2024) could be organized. It involves two teams, with one at COLO and one at COSI. Presented it to interested members after a lab meeting.
- Went to COLO to clean out the rack so that everything could be moved when everything was ready. Universal rails are wanted before we proceed. A heads up to OIT should also be sent so that they can move our point of Internet access to COLO.
- I learned how to create a Discord bot for pinging our services to find if anything went down. It was having many problems with spamming the lab members overnight, but it

was able to detect Hydra being unreachable. More improvements can be made.

February 2024

- My so-called “ping bot” is having issues because it is running on a Raspberry Pi in my room. The connection has been going out so it will not be able to reach the servers, and it will send too many messages to the Discord server when back online. Since the idea is for this to be in COLO, it should not happen once officially deployed, but for now it is shut off for repairs. During times that it was tested, improvements over when it should ping ip addresses rather than web addresses were made.
- The COSI server room got a new rack and universal rails donated by OIT. The hope is to schedule a time this month for THE GREAT COSI MOVE OF 2024.
- Working with OIT, I and one other lab member went down to COLO where we tested the uplink to the Hill campus. At first there was a problem with the transceiver with OIT’s end, but an uplink has now been installed and the COSI move can proceed.
- THE GREAT COSI MOVE OF 2024 has started. There was a total of seven people who came to help out. We split into two groups with one going to COLO (including me) and another staying in the server room. We took out Mirror, Kasper, and TalDOS to transport down to COLO, and corrected mis-labeled cables. Everything seemed to go smoothly until Mirror could not be pinged, which meant it had no connection, and later we discovered that DNS went down again. Those who stayed behind organized the racks in the server room. Not everything was complete on this day as hoped.
- On another day, a lab member went down to COLO to check on what went wrong. TalDOS did not boot properly and the cables for the bridge on Kasper to filter out packets were switched. Everything was then fine.
- The things not finished was the movement of servers in the main server room. I, with

help of my friend Peter later the first day and Cary on the second, moved the servers to not what was imagined. Turns out that different types of server racks have different holds/holes that can be used for server racks, therefore certain servers can only be placed in one rack. This meant that there could be no separation between racks of what is research and what is the students. What was done instead was separating them by mounting research machines on the bottom of racks and student servers at the top. Sadly, not all were mounted since more purchased rails are still waiting to be delivered.

- With this, the move was complete.

vi. CURRENT RESULTS

1. Network Status

At this point in time, the network is running as stated in the preliminary report. Everything vital to the structure of the network is running well. The firewall, domain name service, domain host configuration protocol service, and more are working fine. There were a few mishaps with the server running the DNS and DHCP, but those have been solved and security has been made through having a primary and secondary server (TalDOS and Talos respectively) running DNS and DHCP so that one can fail and it is not as hard as a blow. Much of the hardware in COSI is getting old and with modern servers being expensive and budgeting requirements with the lab, there were some compromises made. Servers donated to us by an alum are slightly more modern (still around 10 years old) and when hardware fails, those new servers are being placed into use.

The COSI network now has a connection to COLO and the movement of servers based on the topology made was implemented. This means that the COSI network has all the functionality as it did before the inciting incident of the power outages. Not only that, but since then there have been power outages at the school that did not affect any of the lab infrastructure or services. There has also been much improvement when it comes to the reliability of the servers staying functional and the simplicity on the Hill campus for lab members. What is left to do in terms of the implementation of the new topology is mounting some servers to racks, which is dependent on the delivery of purchased equipment.

2. Improvements

There are two significant improvements that were implemented into the network. One is creating a primary and secondary DNS server for Talos because of hardware failures. The creation of a new server called "TalDOS" has been made to be the primary server on newer hardware.

The second significant improvement was a remapping of the topology. The idea behind this was better organization and to move important servers down to our co-location which has a backup generator.

It should be noted that before the start of the Spring 2024 semester, there was once again power outages happening frequently at the school. However, with the new fiber switches and moving vital services to the most up to date hardware, there was no repeat of the inciting incident that started this project. Some other parts of the university however were not so fortunate. Research in chemistry and other disciplines was again lost. The university President and Provost have expressed disappointment in the repeated power outage and committed to installing better backup power going forward.

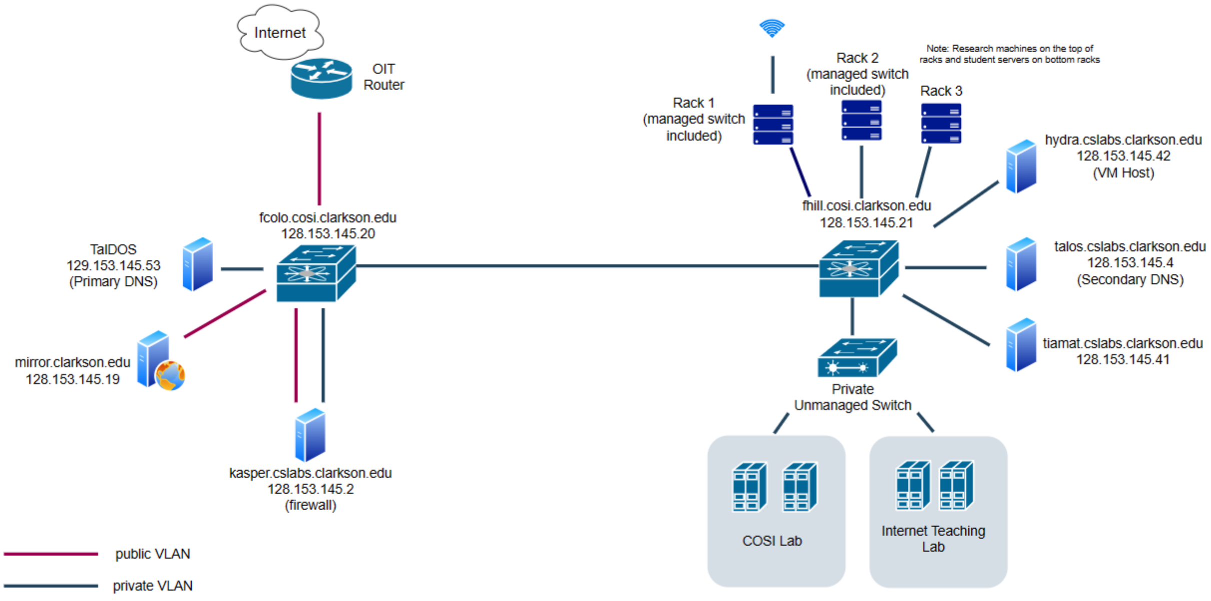


Figure 8. Finalized Topology Diagram.

This topology was created with the idea of having one point of access to the Internet (represented by the cloud) to decrease redundancy, be simpler for lab members to understand, keep the most important servers in a place where they are more likely to not be powered off, and be more organized. This topology has gotten feedback from multiple parties and this figure above is the implemented topology. The only difference from the approved topology is the new rack and organization of research and student servers, due to accounting for rack mounting holds.

Having two points of access to the Internet through OIT was changed. The thought behind it was that even though there were two points of access, there was still one COSI-made firewall planned to filter out those packets. Also, if the Hill server room suddenly lost power, the point of access would be in COLO being backed up by a generator. Reducing to one point of access made it much simpler and the one picked was the one more secure.

There can be some fear in jumping into a project like this because of a mental block originating from the feeling that because something is very complex, it should be left to those with more experience. This has been heard many times around COSI. That is why simplicity was also a factor for this topology. That is shown with the fact of having two VLANs total and VLAN 2 (private) being the only one used in FHILL currently. The reason for this is to not be bogged down by different VLANs going to different servers. At this point in time, these are the only two VLANs being used and VLAN 3 is only used by the firewall and Mirror. With VLAN 2 being the only one on the Hill leaves less complexity with where packets from servers are going to, leaving one less hurdle for newcomers. This does not mean that newer lab members would not interface with navigating multiple VLANs, because if they use Mirror or look at this topology or documentation, they should be able to trace how these are separate. There is also room for more VLANs to be made and sent up FHILL as it is deemed fit, as done in the past.

Mirror, TalDOS, and Ziltoid have been moved to COLO because as some of the more important services, the lab wants them to be connected to a generator if the power goes out. There would be less worry about the access to the Clarkson Mirror because of outages. Lab members would be always able to edit the DNS and firewall entries.

Lastly, there is a natural organization of the most important servers in COLO, and even more organization on the Hill. There is a separation between research servers owned by professors that need permission to be touched, versus a space for student project servers.

3. Network Management

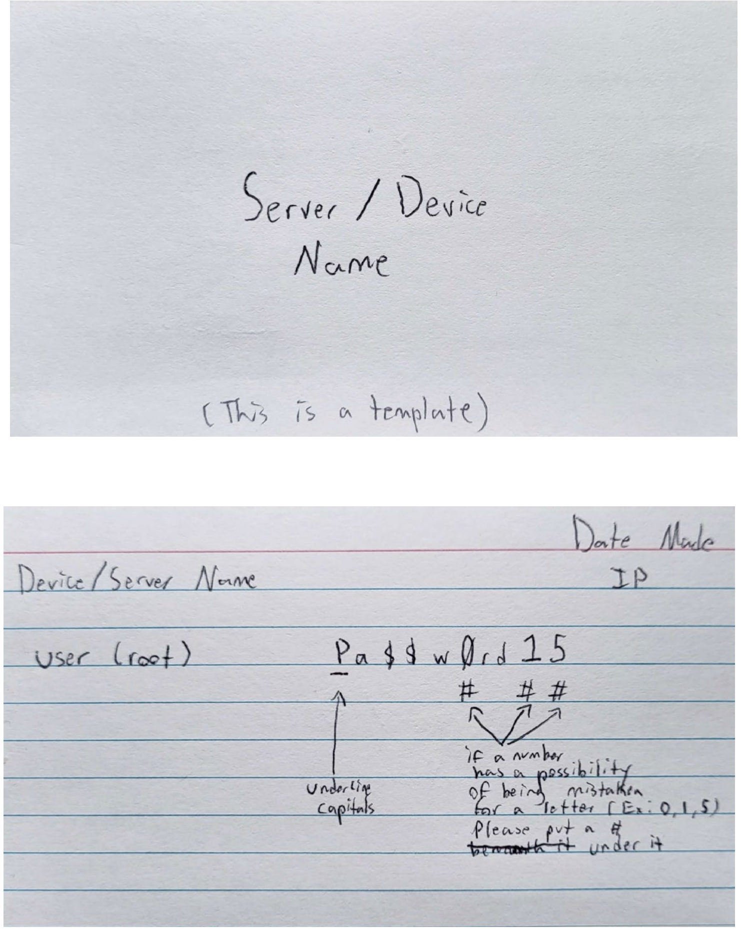
A Discord bot was made for the COSI Discord server. It was a simple python script, but it opened the door to learning about python virtual environments. It is not set up yet and it is planned to be installed on a server in COLO to have connectivity and power security.

The ping bot first tries to reach the DNS server TalDOS. If the response is positive (meaning a connection has been made) that means the ping bot can use the human-readable machine name (e.g. mirror.clarkson.edu) of COSI servers to determine what is running. If the response is negative (no connection has been made), only the IP addresses (e.g. 128.153.145.19) of servers will work, so that is what the bot will try.

4. Documentation

The documentation for COSI, which is hosted publicly at book.cosi.clarkson.edu is being kept up to date by members of the lab. Using this “book”, future members should be able to know what each server does, where it is, configurations documents, and the specifications of the hardware. It also contains what resources are available to students in the lab. This documentation is very important to the continuation of the labs because the contents are specific to COSI and cannot be found from other public sources online. This contradicts something like Mirror, in which the content can be found and updated by public sources. Knowing this, the documentation of COSI needs to be kept up-to-date and backed up.

Some standards were also created for documentation as well. Specifically for root passwords. During this time, new passwords were randomly generated for all devices and presented a template on how those passwords should be kept.



Server / Device
Name

(This is a template)

Date Made

Device/Server Name IP

user (root) Pa$$wØrd15

# # #

underline capitals

if a number has a possibility of being mistaken for a letter (Ex: 0, 1, 5) Please put a # ~~beneath it~~ under it

Figure 9. Front and back of password documentation template

vii. CHALLENGES

During this project, many challenges faced COSI and the students here. Some of those are easily understood. Power outages, loose cables, students not available because of work, and more were all normal and understandable setbacks, but the major ones came from the changes of the university and other external forces.

When students came back early at the start of the Spring 2023 semester, the purchase of the two new fiber switches was proposed to replace the one that broke and the other that was removed from COLO. It was approved at the first meeting and an order was sent out. No one is at fault for the time it took to have those switches delivered and they came at the beginning of the Fall 2023 semester. There was no dedicated person to place these orders in for a month, and when it was placed, the delivery was projected to be long. It was a consequence of the COVID-19 pandemic that parts of the fiber switch model ordered were backed up in supply. Each update, the seller kept pushing back the time it would arrive. Without these switches, it took longer to get access to COLO and move servers around to the finalized topology.

At the time of writing this (Spring 2024), Clarkson University is going through rapid change, and that is derived from the budget cuts that had to be made. Though it has taken the spotlight more towards the end of 2023 and now into 2024, budget restrictions were in motion for a longer period of time. COSI has not seen major cuts to our budget yet, but during the Fall 2023 semester, much of our hardware started to fail. Talos was mentioned before as an example, but even our server for Ziltoid failed and was replaced by a new server called Kasper by a lab member. The most modern servers COSI owns may be around 10 years old and were donated by an alum. The lab would like to buy new modern servers. The problem is that the person who was taking the orders changed jobs within the university, and the person who was supposed to help (the assistant to the Dean of Arts and Sciences) lost her job as that school was being dissolved.

With no one to place these orders, it impacted the activities of the lab.

Besides budgeting and orders, it would only be fair to look at the challenges for COSI that were an impact of the COVID-19 pandemic. The lab prides itself on the way its members learn and teach. Members start COSI learning from those more experienced in the labs. Later, that knowledge passed on is bestowed to others when a member is more experienced. Because of the lull of activity in 2020 and into 2021, it was hard to obtain some knowledge and traditions of the lab. For example, it was unknown by members that entered during the pandemic that there was another documentation page previously for COSI called “undocs”, which is a wiki for the lab members. Another example is in lab culture, like going on a hike to Mt. Ampersand. I was able to have knowledge passed down to me, and I am thankful for that, but now another problem has arisen with lack of motivation for incoming students to join organizations. Between what I have heard about other clubs, and seeing myself as COSI lab director and a president of another club, commitments overall have gone down. Some clubs did not make the transition through COVID at all (e.g. Clarkson Golden Knotes or APO). COSI has survived as a vibrant community of people, but it has been hard at times. We have tried to focus on passing knowledge down and this emphasizes the importance of documentation even more.

viii. CONCLUSION

Despite the challenges, the lab is in a good place. The network will be at its full capacity by the end of Spring 2024. Documentation is being kept up to date. Many people have had some active role in this undertaking, and hopefully they all learned something new.

For myself, it was great to implement some of the concepts I learned in classes to this capstone. There were many tiny pieces of information that I would have never learned if I did not go through this process. From combing through system logs and the different types of cables, it will benefit me greatly. There is also the matter of leadership. How to pull people together, how to know when you have done your best, how to cope with forces outside your control hindering productivity, and after one steps down from a position how to find the balance of leading in order to make a team the most productive it can be.

ix. REFERENCES

[1] J. Cirelly. (2023, March. 7). “5 best open-source network monitoring tools for 2023 with links.” Comparitech. https://www.comparitech.com/net-admin/open-source-network-monitoring-tools/ (accessed March 9, 2023).

[2] D. Hui. (2021, March 6). “How to build a KVM over IP with Raspberry Pi.” Tom’s Hardware. https://www.tomshardware.com/how-to/kvm-over-ip-raspberry-pi (accessed March 9, 2023).

[3] “What is network management?” IBM. https://www.ibm.com/topics/network-management (accessed March 8, 2023).

[4] Noaa. (2022, February 14). “Network telemetry - an IT executive's guide.” Netreo. https://www.netreo.com/blog/network-telemetry-it-executive-guide/ (accessed March 8, 2023).

[5] Qasim. (2024, January 31). “Ubuntu vs windows 11: The ultimate battle of 5 elements.” RedSwitches. https://www.redswitches.com/blog/ubuntu-vs-windows/#:~:text=Ubuntu%20offers%20a%20user%2Dfriendly,for%20tech%20novices%20and%20professionals (accessed March 8, 2023).

[6] E. Simard. (2020, October 22). “Iptables vs nftables: What’s the difference?” Linux Handbook. https://linuxhandbook.com/iptables-vs-nftables/ (accessed March 8, 2023).

[7] T. Slattery. (2020, June 9). “Telemetry vs. SNMP: Is One better for network management?” TechTarget. https://www.techtarget.com/searchnetworking/answer/Telemetry-vs-SNMP-Is-one-better for-network-management (accessed March 8, 2023).

[8] Staff Contributor. (2021, April 19). “Network Management Guide: How To, best practices, &amp; tools.” DNSstuff. https://www.dnsstuff.com/network-management (accessed March 8, 2023).

[9] Staff Contributor. (2022, November 30). “Best Network Monitoring Software.” DNSstuff. https://www.dnsstuff.com/network-monitoring-software (accessed March 8, 2023).

[10] H. Subedi. (2022, May 11). “Network management best practices for businesses.” Jones IT. https://www.itjones.com/blogs/2022/1/8/network-management-best-practices-for-businesses (accessed March 8, 2023).

[11] Wikimedia Foundation. (2023, February 3). “Simple Network Management protocol.” Wikipedia. https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol (accessed March 8, 2023).

[12] Würzburg. (2022, September 28). “The similarities and differences between SNMP and telemetry.” Infosim. https://www.infosim.net/stablenet/blog/the-similarities-and-differences-between-snmp-an d-telemetry/ (accessed March 8, 2023).

x. APPENDIX

1. Glossary

Mirror: A software mirror is a website for people to obtain free and open-source software. In this case, “Mirror” means the specific software mirror created and run by the Clarkson Open-Source institute. Can be accessed by the public at mirror.clarkson.edu to obtain free and open-source software

SSH: Secure Shell protocol. Allows users to access other services in a network for things like remote logins

Iptables: A program to configure the IP packet filter used in a firewall. Used for Linux, it allows a system administrator to set rules on what packets can go through a firewall

Nftables: A packet classification program used in a firewall

Talos: COSI lab’s server for recursive and authoritative Domain Name Service

Gitea: A platform that hosts software development version control that utilizes git

COSI Book: Found at book.cosi.clarkson.edu or book.cslabs.clarkson.edu, it is COSI’s documentation website. Created using a free and open-source software called “mdbook”, lab members can find detailed information about services in the lab and make edits through the Github repository. It resides in a docker container on Tiamat

Docker: Free and Open-source software used to deploy containerized software

Tiamat: COSI lab’s server used primarily for hosting student and COSI websites

Hydra: COSI lab's default virtual machine host server

Webhook: A callback function that allows communication between two applications based on specified events

2. Links

Development Log: carlone-capstone.cslabs.clarkson.edu or carlone-capstone.cosi.clarkson.edu

COSI "Book" Documentation: book.cslabs.clarkson.edu or book.cosi.clarkson.edu

Clarkson Mirror: mirror.clarkson.edu

Discord "Ping" bot: https://github.com/sophiacarlone/PingBot

Docker: https://www.docker.com