Cole Baty

01187002

CYSE 368 - Fall 2022

Internship as

Student Network Technician

for

Old Dominion University

Internet Technology Services

Table of Contents

1. Introduction

This semester, I began an internship with the Old Dominion University (ODU) Internet Technology Services (ITS) Networks team as a Student Network Technician. I chose to work for this organization because I thought it might be useful in my progress as a cybersecurity professional to develop a working knowledge of the underlying networking technologies that enable our modern society. What attracts me to this job, and more generally to cybersecurity, is that it is a niche field which attracts a certain type of person, but is demonstrably indispensable, with high demand that ensures jobs are likely waiting wherever I decide I want to live after finishing this degree.

There were other factors which contributed to my decision to work for this organization. When I initially interviewed with my supervisor, Bob McCoy, I was very pleased to learn that management places a heavy emphasis on the "student" part of the job title, and so they are flexible about things like scheduling and doing homework on the clock, as long as work isn't being ignored.

The specific learning objectives I hoped to achieve during my internship were

1. To engage in project-related works for projects managed by ODU's Project Management Office (PMO);
2. To conduct an interview with the Security team to learn more about their role;
3. Understand how to implement an Access Control List without a firewall; and
4. To understand and implement Rapid Per-Vlan Spanning Tree (PVST) in Cisco's Packet Tracer

These objectives will be discussed in greater detail in Section 7.

2. Beginning of Internship

The Networks team is a small part of the larger ITS structure at ODU. ITS, as the name implies, is a large operation which "offers faculty, staff, and students a wide range of technology services and support."[1] The Networks team is responsible for maintaining the physical infrastructure that enables networking throughout the ODU footprint on the Norfolk campus and all satellite locations. Initially part of an organization called Telecommunications, which was primarily involved with the telephone systems on campus, the Networking department is the result of many decades of reorganization, segmentation, and realignment in response to adapting the needs of incorporating Internet access into daily professional operations.

[1] https://ww1.odu.edu/its/about

The major products of ITS in general are in the “support of all campus technology needs.”[2] For the Networks team, the major product is providing Internet access on campus wherever it is needed; there is not a “product” as such, but rather a service.

Among the major customers is the President of the University, whose internet access at the Presidential Residence is supported by ITS Networks. Additionally, there is large demand in the residential halls, where students use many internet-related devices to conduct their studies as well as to enjoy free time.

The scope of the operation is quite large. Early in my onboarding process I was given a tour of the ITS data center. I lost count of how many server racks and routers I passed. At one point, my supervisor pointed to a fiber-optic cable, explaining that this was the uplink to the internet service provider (ISP), and it carried 1,000 Gigabits per second (Gibps), which is the most bandwidth I’d ever seen before. I never got an exact count, but there are somewhere between 100-200 Cisco switches and routers on campus, through which all internet traffic must pass, including Wi-Fi.

My onboarding experience was fairly straightforward; there were some forms to fill, and a bit of waiting for access to different accounts and systems. I was very impressed that there was an onboarding document with detailed instructions for every step of the process, including links to other procedure documents for steps which couldn’t be succinctly explained. I came to learn that procedure documentation was a very important priority to the team, which I found to be very comforting. I have previously worked at organizations that have not placed the same importance on continuity and preserving institutional knowledge, and the experience was markedly different. It gave me the impression that this was an organized, structured enterprise, with policies and procedures in place to enforce adherence to a standard.

Onboarding also included some shadowing of the other student workers performing some of the common tasks I would be doing in this position.

[2] https://ww1.odu.edu/its

3. Management Environment

The management environment was very simple - my direct supervisor was Bob McCoy, Manager, Network Engineering. I learned that Bob had started in ITS as a Student Network Technician, working his way up over the years to his current position. On the same “tier” as Bob (that is, the tier above me), were the full-time engineers and technicians:

- Seth Mcfarland, Senior Network Engineer
- Andy Underwood, Senior Network Engineer
- Aaron Olah, Network Automation Engineer
- Richard Owen, Network Automation Engineer
- James Tate, Cloud Architect
- Rodney Harmon, Communication Systems Technician

Any of the people in this list technically “outranked” me. As we became more familiar with each other and our individual interests and skill sets, the engineers and technicians from the level above me would occasionally “outsource” by tasking me with some part of the task they were working on.

Coordination was conducted through the usual suite of enterprise productivity tools - Zoom for video conferencing, Teams for chat, Sharepoint and OneDrive for file sharing, etc.

I learned that during the Pandemic[3], many of the full-time staff were placed on a remote-work rotation. By the time I joined the organization, the policy was that each person had to be physically in the office one day per week. These were usually worked out so that, at most, only one or two full-time staff were in the office on any given day. Additionally, there was flexibility in my scheduled hours, so it was quite some time before I met everyone in person. Furthermore, I remain completely ignorant of the management tier above my supervisor.

I respond well to a task-oriented management environment, where there are clearly expressed desired end-states and deadlines. Consequently, I really enjoyed the management environment at this internship. While the Pandemic-related challenges made it difficult to get to know everyone in a way I’m accustomed to, I found myself thriving in this environment because of how task-oriented the work is. Additionally, from what I could sense, everyone in our section got along and worked well as a cohesive team, which was a major contributor to the easygoing workplace culture.

[3] I am optimistically hoping that this will not need clarification for many years

4. Major Work Duties

The official position summary of the Student Network Technician reads,

> The Student Network Technician will help provide and maintain a safe and secure computing and communications environment. This position will install and configure network equipment as well as troubleshoot, diagnose, and resolve software or hardware technical issues related to networking systems. They will provide positive and responsive customer service to internal and external users on daily (sic) basis while assisting with handling of incidents, problems, or new requests.[4]

The position is largely help-desk oriented. There is a portal in help-desk ticketing platform Service Now (Fig. 1), which we used to receive service requests from ODU network users.

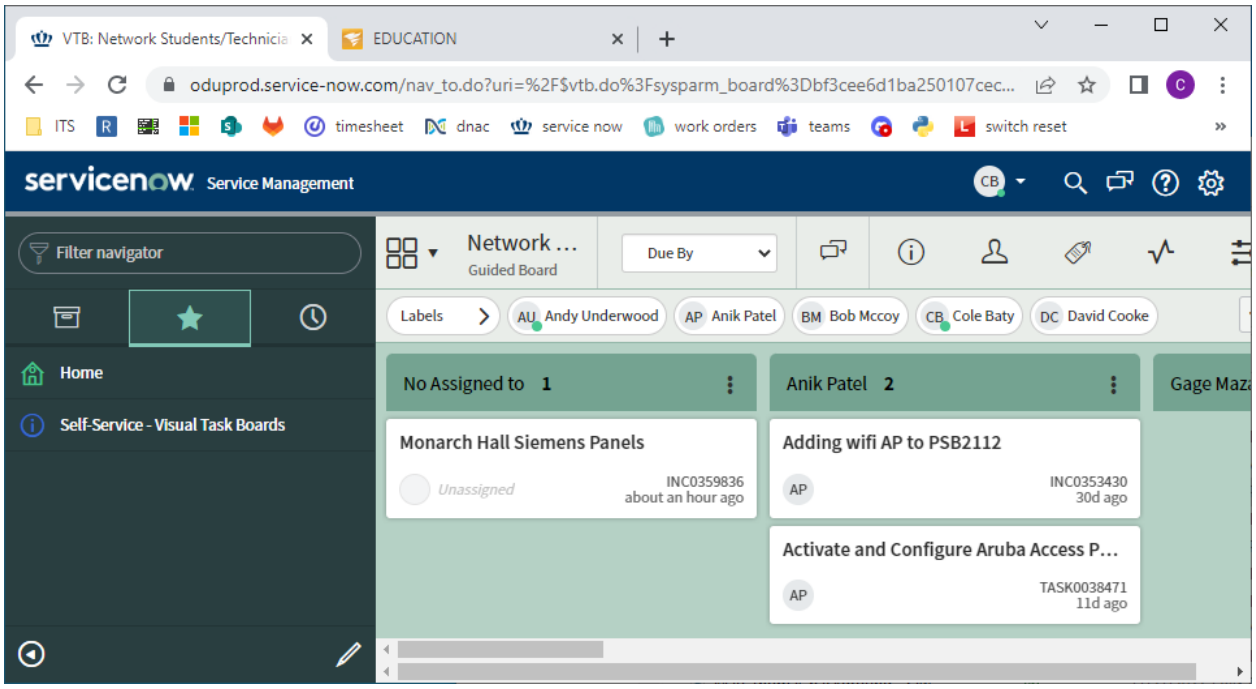


Fig. 1 - Service Now

[4] "Student Network Technician". ODU - ITS - STEP, Appendix A

The typical workflow of a working shift followed this decision tree:

- If there are tickets in the Service Now queue
    - If the ticket can be handled by a Student Network Technician
        - Process the ticket
    - Else, pass it up to the appropriate full-time person
- Else, if there are upcoming large projects (LCR[5], SDA[6] migration, etc)
    - Work on these projects
- Else
    - Work on student projects, homework

The vast majority of tickets I processed were requests to activate or troubleshoot some network port in an office on campus. As people returned to the campus for in-person work, sometimes they would discover the port in their office had been disconnected. This was usually because there had been some sort of equipment upgrade or other action that included evaluating network ports which had not been in use for a long time. These were resolved by the following procedure:

1. Identify the network port label in the office. This corresponds to the port on the “patch panel” in the network closet
2. Ensure the connection from the patch panel to the port in the office is intact
3. Select and configure an available switch port on the network switch
4. Make the connection from the patch panel to the network switch - “cross-connecting”
5. Test the connection in the office to ensure the desired connectivity

This is a very straightforward procedure, and often the most challenging part is simply tracing a cable from one port to another. Over time, as many cross-connects are made, the cables can become quite tangled, and with an average of 288 ports per network switch[7], it can sometimes feel like a futile exercise in topology to arrange them all neatly (Fig. 2).

[5] Life-cycle replacement of aging equipment “in production”
[6] Software Defined Access - ODU is in the process of incorporating all network equipment into the Cisco SDA fabric
[7] 48 ports per line card * 6 line cards (avg) per installed switch

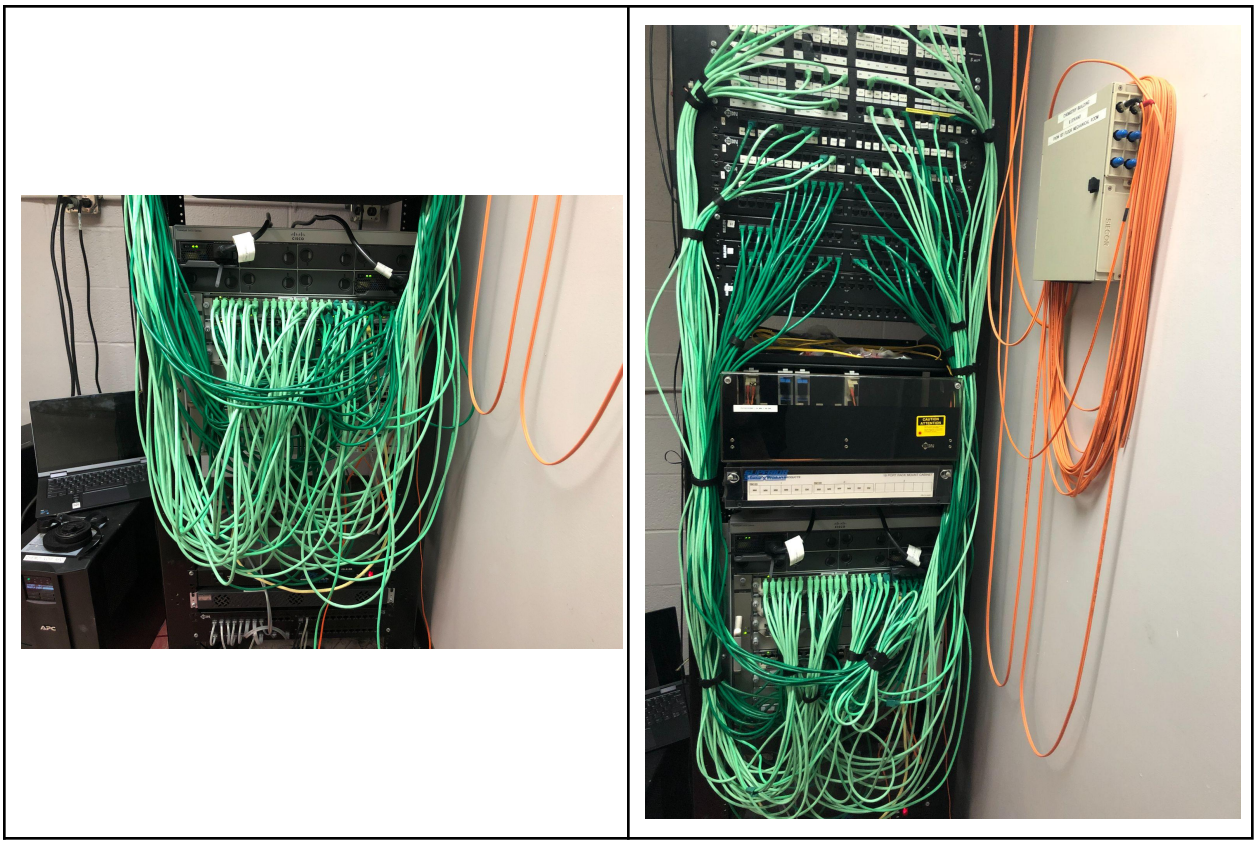


Fig. 2 - examples of cable management
Left - poor; right - better

This task is important to the organization because without internet connectivity, it becomes impossible for ODU network users to get work done. There are many different systems used all over campus, many of which have very specific network access requirements, and if the physical link to these networks doesn't work, it may prevent an office or an entire building from getting any work done while the link is down.

Other common help desk tasks were addressing tickets: assigning or removing static IP address reservations from specific devices. This was a simple matter of adding or removing a DHCP reservation in the IP Address Management (IPAM) software InfoBlox (Fig. 3).

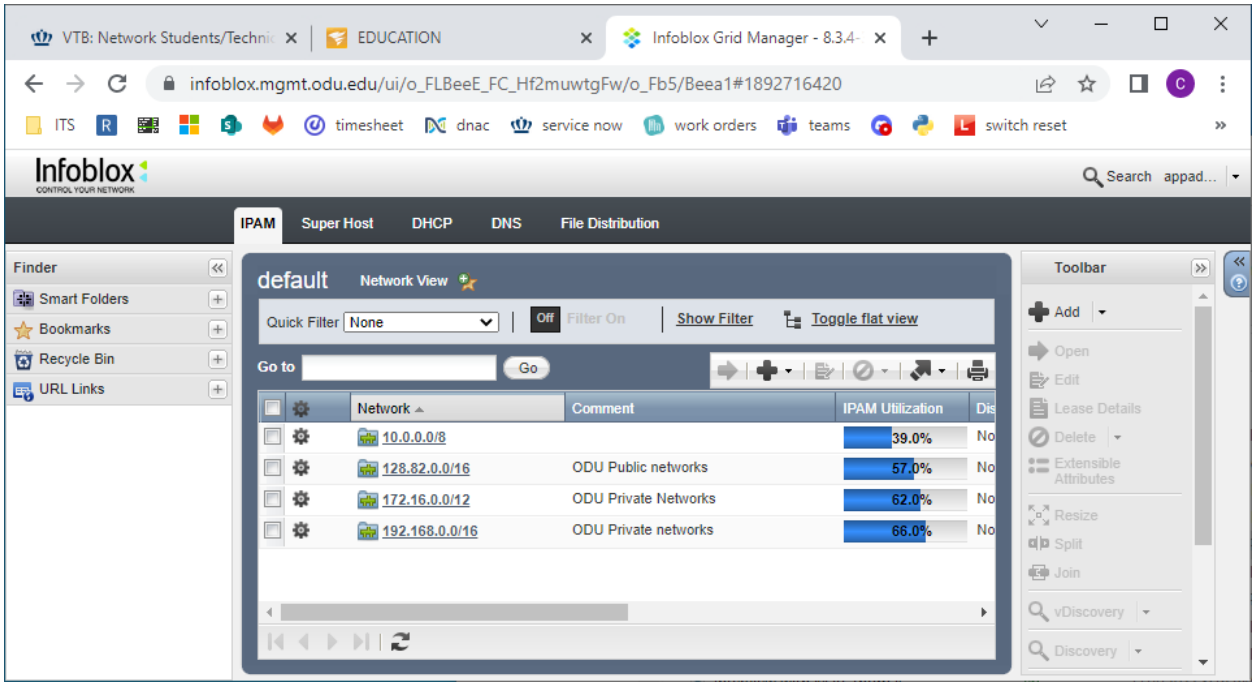


Fig. 3 - Infoblox, IPAM platform

This was important because, within a given network, there may be a specific machine that hosts an important database, for which custom automation scripts and tools have been written. These scripts often rely on the target machine having a fixed address, so without a static IP reservation the address of the target machine may change and disrupt the entire system.

The major project I completed during this internship was to migrate five switches from “traditional” network switching into the Cisco Software Defined Access (SDA) fabric being implemented on ODU. Details of this project can be found in Reflection Paper 1. Samples of work from this project are included in Appendix B. This project is overseen by the ITS Project Management Office (PMO), and the desired end-state is to have all routers and switches within the footprint incorporated into the SDA fabric.

SDA is a higher level abstraction of packet switching than the traditional method. In traditional packet switching, the routing table for each switch/router is implemented per-device in the control plane. In SDA, the control plane for all devices is managed centrally by a designated control node within the fabric site, which coordinates routing for the entire control plane for the given fabric site. Additionally, the software used to manage the SDA fabric provides a robust RESTful Application Programming Interface (API) which can be used for further automation.

As with any project involving a major change to equipment already “in production”, there was a lengthy procedure document outlining three phases of executing this migration: pre-execution, execution, and post-execution. The procedure document was compiled by Senior Engineer Seth Mcfarland. Pre-execution involved collecting data on the target switches, including stakeholders whose devices would be affected by the change to the network (Fig. 4). This must

occur far enough in advance so that stakeholders can assess the potential impact and notify the Networks team of any necessary changes they will need to make.

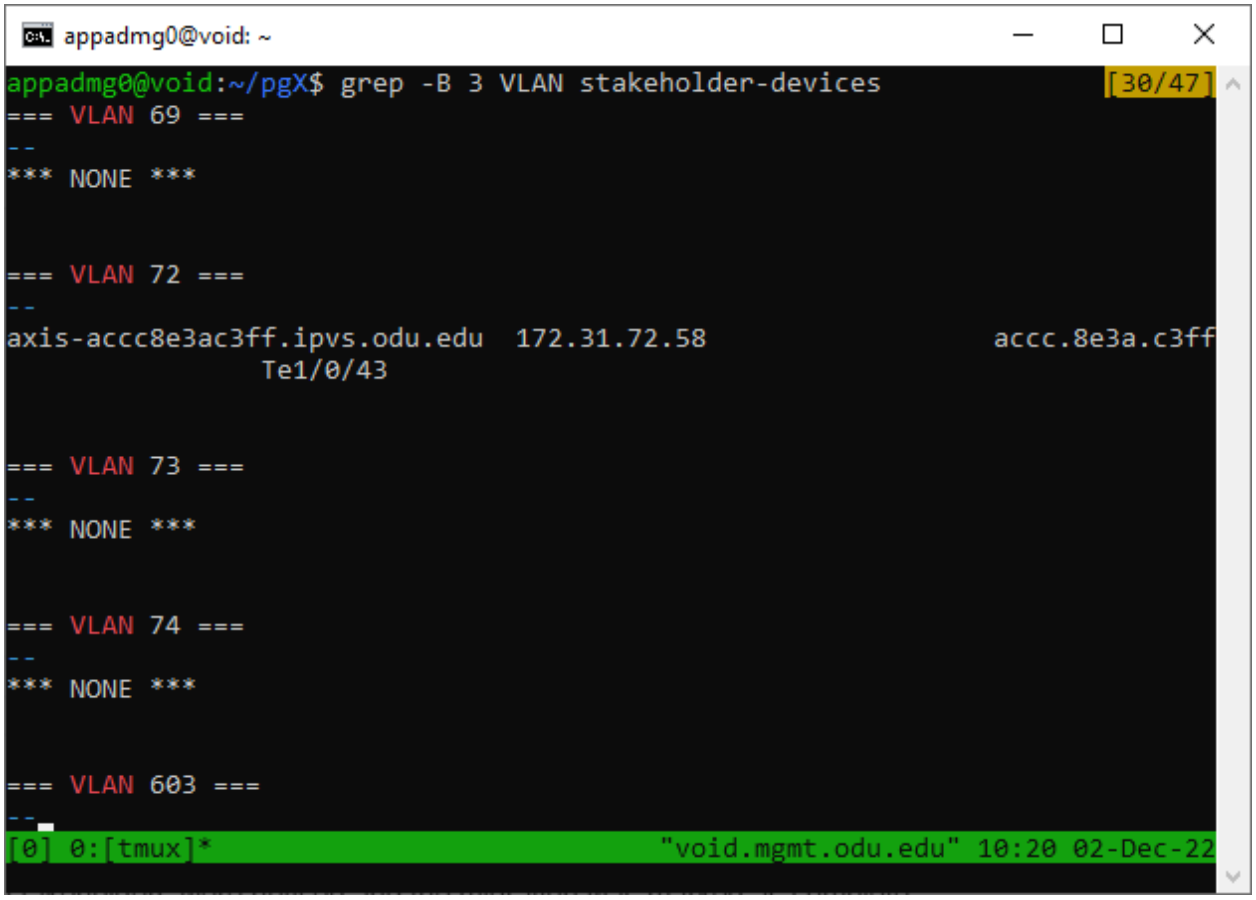


Fig. 4 - sample of stakeholder devices affected by SDA migration

Execution involved running some scripts, both provided by the Cisco SDA software and some which were custom-written by Aaron Olah, Network Automation Engineer. Additionally, there were some fiber-optic cables that had to be physically moved from one port to another. All in all, the execution did not involve a lot of work.

Post-execution involved running some more scripts to collect more information that was used to update static IP reservations for stakeholder devices. Finally, when everything was finished, the stakeholders were noticed and the migration was marked as complete.

5. Specific use of cybersecurity skills and knowledge

At this internship, I made heavy use of my knowledge of Linux. Student Network Technicians are granted user accounts to a CentOS machine on the network, through which the management ports for all network switches can be accessed (Fig. 5)[8]. I used many common command line tools daily, such as `ssh`, `nslookup`, and `ping`.

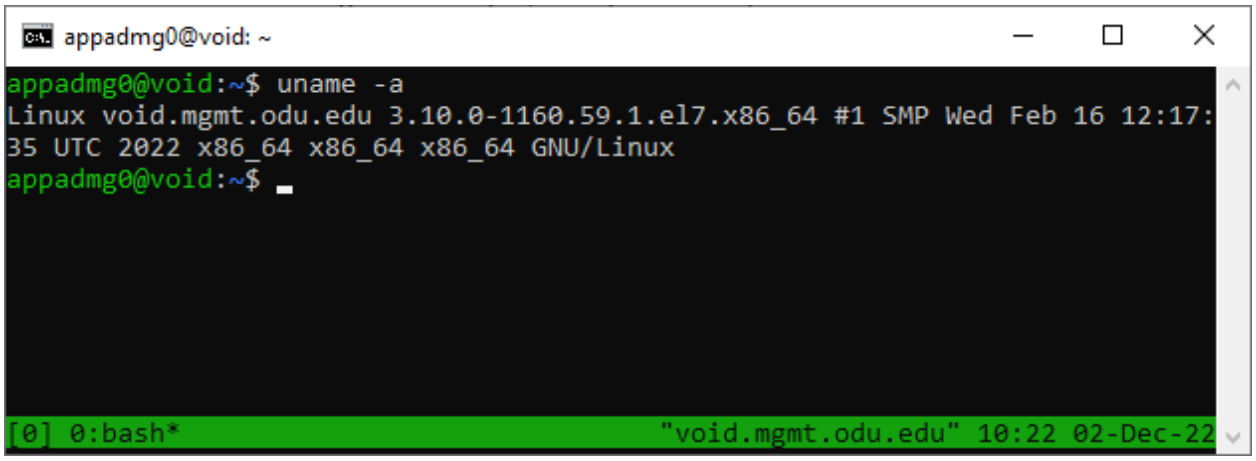


Fig. 5 - CentOS machine `void`

Scripting was also a useful skill I employed in this internship. The Networks department maintains a private `git` server, where almost all of the automation scripts ever developed are archived. Student Networking Technicians are also granted access to this server. A sample of a script I wrote for a specific purpose can be found in Appendix C.

Knowledge of port forwarding proved useful during my time at this internship. Student Networking Technicians are granted access to the ITS VPN, and so I eventually reached a point where I was able to bring my personal laptop to ticket service calls so that I could interface with a given switch while I was physically in front of it. My knowledge of port forwarding enabled me to reach services through a SOCKS proxy that were otherwise inaccessible unless I was at my workstation in the Networks department. I brought this to the attention of my supervisor, who said it was an important security vulnerability and “a pretty good find” which he would forward to the Security team. This specific brand of port forwarding has since been closed.

Something I learned more about in this job is the application of subnetting to a network. As a result, I am designing a network plan for my own home that will partition the address space into a section for IoT devices, and another section for personal devices, making my overall home network more secure by reducing the potential attack surface of my home network.

[8] While the output of `uname` doesn’t explicitly specify CentOS, a quick search of the kernel version will confirm the OS version

6. Preparation by ODU curriculum

Overall, I would say that the curriculum at ODU did not prepare me for the internship, but that is simply because much of the coursework I've had to date is more software-oriented than networking hardware-oriented. I know I've had modules on the use of Wireshark during my ODU coursework, so that came in useful when I had to use Wireshark a couple of times during the internship.

During this semester, I was also taking a networking course (ECE 355 - Introduction to Networks and Data Communications), so it was helpful to have access to a large, enterprise-level network in order to explore some of the concepts covered in that class and to see them used in practice. I was able to gain a deeper understanding of topics like subnetting and Dijkstra's Algorithm by seeing them employed in ODU's network.

7. Fulfillment of Learning Objectives

1. Engagement in PMO-directed projects

This goal was fulfilled by the internship. I was assigned to work with Senior Engineer Seth Mcfarland to execute the SDA migration project outlined in previous sections. This had a successful outcome.

2. Conducting and interview with a member of Security team

This goal was fulfilled by the internship. I coordinated with my supervisor, asking to be put in touch with a member of the Security team to see about conducting an interview for this internship. On October 8, 2022, I interviewed Matthew Thomas, Security Architect, ODU ITS. This interview was conducted over Zoom, and the entire interview is available in Reflection Paper 2 as well as in Appendix D.

3. Implementing Access Control Lists without a firewall

This goal was not fulfilled by the internship. I limited myself to fifteen hours per week at this internship, which enabled a good balance between the internship and the rest of my coursework, but unfortunately did not permit me enough time to properly complete this goal.

4. Implementing Rapid PVST in Packet Tracer

This goal was partially fulfilled by the internship. I managed to get access to Packet Tracer, and I found some documentation on Rapid PVST. I even got as far as following the steps of a

walkthrough describing a simplistic setup in Packet Tracer for RPVST, but I was unable to confirm whether I had achieved the intended implementation. Details are in Appendix E.

8. Motivating aspects of internship

The most motivating aspects of this internship were the ease of the job and the apparent job security involved. I am an older student, approaching 40 years of age, and I have had a lot of experience in very high-stress work environments. I am very encouraged to have found a field of like-minded people who are similarly enchanted by anything to do with computers.

I'm also encouraged by the implications of job security I saw in this job. Again, we are currently living at the dawn of the Information Age, in which we've seen society totally and rapidly transformed by information technology.

This is something I don't foresee going away (short of total collapse of civilization), and so there will be a continued need for qualified people who possess the knowledge of how to build and maintain these systems, for as long as humans and computers coexist. Furthermore, some reflection led me to the conclusion that there must be thousands, possibly millions, of organizations at least as large as ODU all over the planet, which means there is demand all over the planet for people with this skill set. And, as we've seen during the Pandemic, most IT work can be performed remotely without loss of productivity. This is all very encouraging.

9. Discouraging aspects of internship

I did ask some of the full-time employees about their qualifications, and most of them could list off a litany of certifications they'd attained. I'm doing a mid-life career transition from a field that had no such certification system in place, and so I find the certification requirements for positions like this to be a little anxiety-inducing. While I do recognize their utility as a tool to maintain a minimum standard of competence within the field, at this point in my academic career I just see them as another demand on my time (and my wallet). For example, the Perry Library has copies of some preparatory materials for the latest version of the Cisco Certified Network Associate (CCNA) certification, and while they're very interesting, it's also just a lot of material to get through. Perhaps when I'm finished with this degree the commitment won't seem as daunting.

10. Most challenging aspects

One of the most challenging parts of this internship was getting a handle on all the jargon and shop talk. Networking contains a large body of knowledge, and a single semester is too short a time to even scratch the surface.

Another challenge was building the mental map of the systems and how they relate to each other. One of the onboarding steps contained some pre-saved browser bookmarks to a whole suite of software used by the Networks team to run and maintain the network. Keeping track of which service did what, and how they interacted with each other, was a difficult process that took some time. I'm certain that the tiny amount of knowledge I've gained to be able to do this job is just a mere fraction of the total body of knowledge.

Another challenge that surprised me was keeping straight the names for different things. There were tools that were called different names by different people. Buildings on campus have changed names, and some people who submit help tickets refer to them by the old name. The most recent changes to a procedure document might have been two years out of date. Unfamiliarity with the physical locations of buildings on campus presented a challenge, as well.

11. Recommendations to future interns

My recommendation to future students wishing to undertake this internship is to approach this with an open mind. My hiring interview was in two stages. The first stage was the traditional going over of the resume, answering questions. The second stage involved me coming to the Networks office and doing a "hiring project" that involved resetting and configuring a network switch with some specific instructions. I had no *a priori* knowledge of how to do any of this, but through research[9] I managed to get something workable. Some time after this interview, Bob explained to me that the goal of this part of the interview is not necessarily to evaluate whether the candidate can set up the switch perfectly, but whether they are resourceful enough to look up how to do things like reset the switch, and get around in the CLI.

So, to me, a successful intern will be one who is willing to seek information for themselves.

[9] Lots and lots of desperate googling

12. Conclusion

In conclusion, I found this internship to be challenging and rewarding. I greatly enjoyed the problem-solving aspect inherent in the help-desk oriented nature of the job, which meant that no two shifts were likely to be identical. During the remainder of my college time, I will endeavor to find time to chip away at the CCNA certification, provided my course load permits it.

The exposure to a large-scale enterprise operation like that found at ODU was helpful for me to broaden my post-degree job search. I have made invaluable professional connections, whom I hope I can rely on in the future for good references to potential employers.

Appendix A - Student Network Technician Job Description

What follows is the Position Summary of the job description from the ODU (Student Technology Employment Program) document describing the Student Network Technician position.

Position Summary

The Student Network Technician will help provide and maintain a safe and secure computing and communications environment. This position will install and configure network equipment as well as troubleshoot, diagnose, and resolve software or hardware technical issues related to networking systems. They will provide positive and responsive customer service to internal and external users on daily basis while assisting with handling of incidents, problems, or new requests

Appendix B - Sample of Work Pertaining to SDA Migration

Cisco SDA Migration Procedure

Pre Migration

These instructions need to be completed days in advance of the migration prodchange to allow for any VLANs or subnets that are not accommodated for in the new SDA fabric.

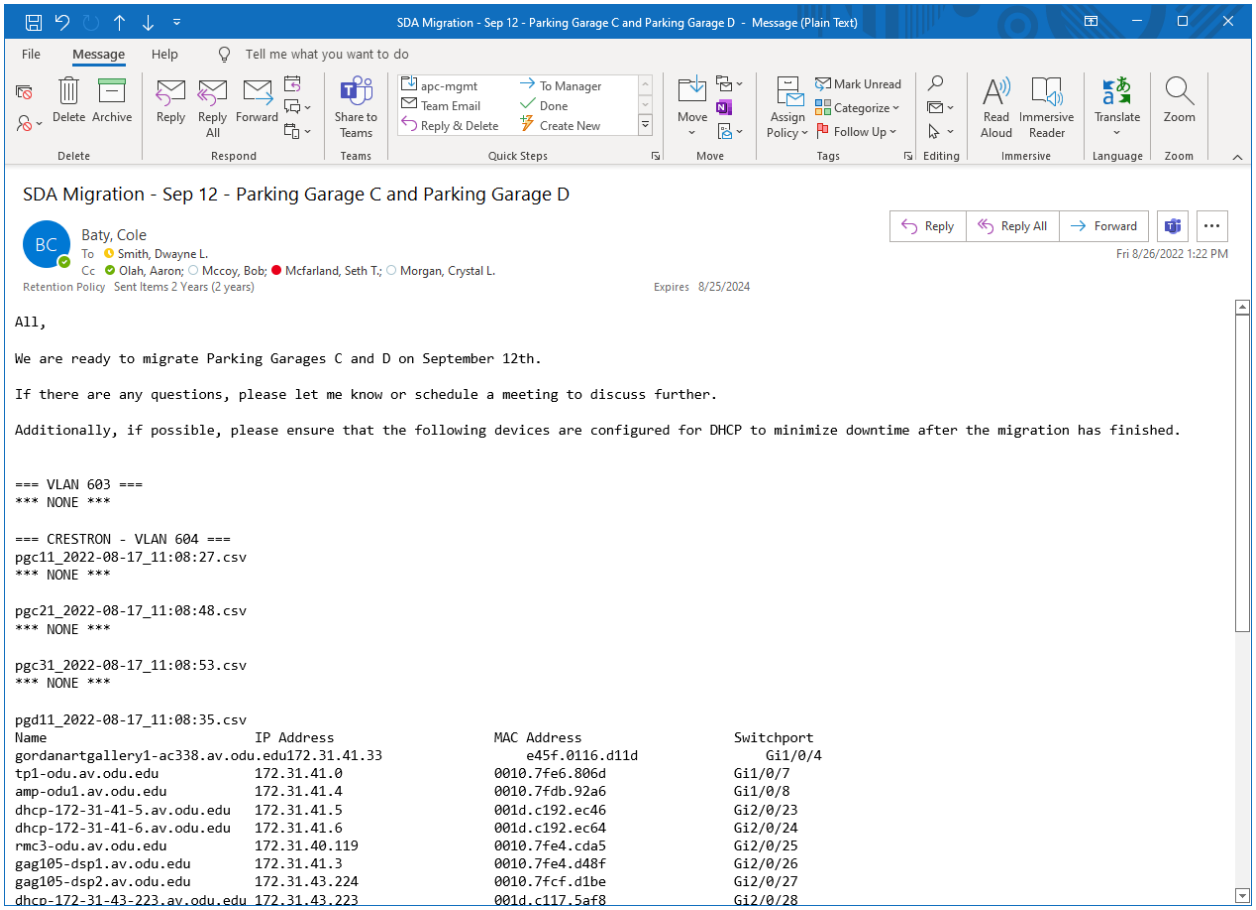
Void Scripts

Initial Checks

- **Run LCR script**
  - cd /usr0/networks/scripts/lcr_collection
  - ./LCR_get <switch1>
  - ./LCR_get <switch2> …
  - Email stake holders their device list
  - Collect MAC's, IP's of MFP, door controllers
- Run pre-migration checks
  - This will:
    - Verify license and install mode configuration
    - Verify necessary DNAC objects exist
    - Copy Infoblox network objects for lift-and-shift networks
    - Determine how to migrate networks (lift-and-shift vs re-IP, etc)
    - Print and clear interface counters on distribution uplinks (live only)
    - Create a config backup on each switch (flash:/backup) (live only)
    - Check for static routes on both firewalls
    - Create a hostname-to-serial number mapping file for LAN automation
    - Create configuration files needed for the vlans_to_pools and port_assignment scripts
    - Print warnings and useful information for the migration
  - cd /usr0/networks/scripts/dnac_provisioning
  - ./provision.py initial_checks <switch1-9300> <switch2-9400> <etc> -d –live

Id	Name	Network	Migration State	VN	SGT	Pool
73	ipvs-cameras-73	172.31.73.0/24	migrate_part	ipvs	ODU_ipvs	ODU_ipvs
80	campus-ups	172.31.149.0/24	migrate_part	control	ODU_ups	ODU_ups
200	ttnet	128.82.200.0/23	shift	ats	ODU_ats_servers	ODU_ttnet
371	clrc1-priv	192.168.171.0/24	shift	acdesk	ODU_acdesk	ODU_clrc1-priv
400	tt-lab	192.168.200.0/23	shift	admdesk	ODU_admdesk	ODU_tt-lab
516	wireless16-mgmt	172.16.16.0/24	skipped	None	None	None
523	wireless23-mgmt	172.16.23.0/24	migrate_part	None	ODU_nonfabric_devices	ODU_nonfabric_devices
524	gornto_aruba_ap	172.16.108.0/24	migrate	aruba	ODU_aruba	ODU_aruba

Fig. B.1
excerpt from procedure document



SDA Migration - Sep 12 - Parking Garage C and Parking Garage D - Message (Plain Text)

File Message Help Tell me what you want to do

Delete Archive Reply Reply All Forward Share to Teams apc-mgmt Team Email Reply & Delete To Manager Done Create New Move Assign Policy Mark Unread Categorize Follow Up Read Aloud Immersive Reader Translate Zoom

Delete Respond Teams Quick Steps Move Tags Editing Immersive Language Zoom

SDA Migration - Sep 12 - Parking Garage C and Parking Garage D

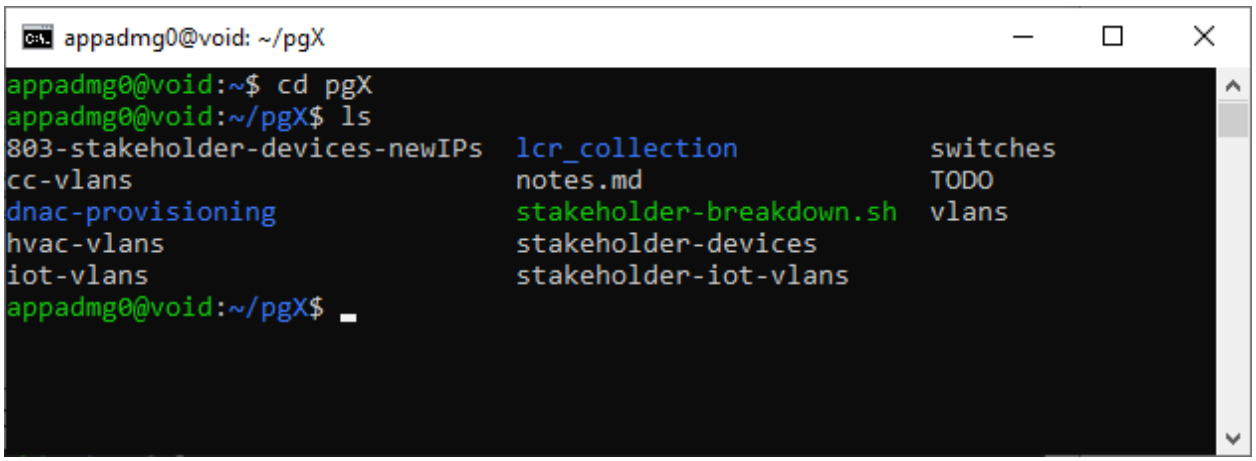
Baty, Cole
To Smith, Dwayne L.
Cc Olah, Aaron; Mccoy, Bob; Mcfarland, Seth T.; Morgan, Crystal L.
Retention Policy Sent Items 2 Years (2 years) Expires 8/25/2024

Reply Reply All Forward

Fri 8/26/2022 1:22 PM

```
All,

We are ready to migrate Parking Garages C and D on September 12th.

If there are any questions, please let me know or schedule a meeting to discuss further.

Additionally, if possible, please ensure that the following devices are configured for DHCP to minimize downtime after the migration has finished.


=== VLAN 603 ===
*** NONE ***

=== CRESTRON - VLAN 604 ===
pgc11_2022-08-17_11:08:27.csv
*** NONE ***

pgc21_2022-08-17_11:08:48.csv
*** NONE ***

pgc31_2022-08-17_11:08:53.csv
*** NONE ***

pgd11_2022-08-17_11:08:35.csv
Name                          IP Address                MAC Address               Switchport
gordanartgallery1-ac338.av.odu.edu172.31.41.33              e45f.0116.d11d              Gi1/0/4
tp1-odu.av.odu.edu            172.31.41.0               0010.7fe6.806d            Gi1/0/7
amp-odu1.av.odu.edu           172.31.41.4               0010.7fdb.92a6            Gi1/0/8
dhcp-172-31-41-5.av.odu.edu   172.31.41.5               001d.c192.ec46            Gi2/0/23
dhcp-172-31-41-6.av.odu.edu   172.31.41.6               001d.c192.ec64            Gi2/0/24
rmc3-odu.av.odu.edu           172.31.40.119             0010.7fe4.cda5            Gi2/0/25
gag105-dsp1.av.odu.edu        172.31.41.3               0010.7fe4.d48f            Gi2/0/26
gag105-dsp2.av.odu.edu        172.31.43.224             0010.7fcf.d1be            Gi2/0/27
dhcp-172-31-43-223.av.odu.edu 172.31.43.223             001d.c117.5af8            Gi2/0/28
```

Fig B.2
sample email message sent to stakeholders
affected by the SDA migration



```
appadmg0@void: ~/pgX
appadmg0@void:~$ cd pgX
appadmg0@void:~/pgX$ ls
803-stakeholder-devices-newIPs  lcr_collection           switches
cc-vlans                        notes.md                 TODO
dnac-provisioning               stakeholder-breakdown.sh vlans
hvac-vlans                      stakeholder-devices
iot-vlans                       stakeholder-iot-vlans
appadmg0@void:~/pgX$
```

Fig B.3
state of working directory on `void`
during preparation phase of migration

Appendix C - Networking script written in Python

This is a script I wrote to help out with a very repetitive task. Occasionally, network equipment needs to be replaced ("life cycle replacements" or LCRs). One of the steps in preparing for an LCR is to manually confirm that the port description stored on the switch matches the label of the port reached on the patch panel. This can be a long, tedious process, and I found myself mixing up numbers and labels all the time.

So I wrote this script that will iterate over the stored port descriptions for a given switch. It will display the currently stored description, and prompt the user to select whether this is the correct description. If it is not, the user is prompted to enter a new port description. Otherwise, it moves on to the next switch port.

I only wrote the `update_descr` function. The rest of the script comes from another tool built by one of the automation engineers to automate logging into the management port of a given switch.

```
#!/usr/bin/python4
import pexpect
import getpass
import termios
import shutil
import base64
import signal
import struct
import fcntl
import stat
import sys
import os


child = None


def stderr(*strings):
    for s in strings:
        sys.stderr.write(str(s) + ' ')
    sys.stderr.write('\b\n')


def processError(before):
```

```
    before = before.decode('ascii')
    if 'Name or service not known' in before:
        sys.exit(1)
    elif 'REMOTE HOST IDENTIFICATION HAS CHANGED' in before:
        sys.exit(2)
    else:
        sys.exit(3)


def handleSigInt(signal, frame):
    stderr("Caught SIGINT. Exiting...")
    sys.exit(4)


def handle_sigwinch(sig, data):
    global child
    # from
https://pexpect.readthedocs.io/en/stable/api/pexpect.html#pexpect.spawn.int
eract
    s = struct.pack("HHHH", 0, 0, 0, 0)
    a = struct.unpack('hhhh', fcntl.ioctl(sys.stdout.fileno(),
        termios.TIOCGWINSZ , s))
    if not child.closed:
        child.setwinsize(a[0],a[1])

def load_password(password_path):
    try:
        pfile = open(password_path, 'r')
    except:
        stderr("Could not open password file.")
        sys.exit(-1)
    p = pfile.readline().strip()
    #p = 'BASE64_PASSWORD'
    p2 = base64.b64decode(p).decode('ascii')
    pfile.close()
    return p2


def show_help():
    print("Usage:")
    print("\t", sys.argv[0], "<switch>", "[start-at]")
    description = """
    This tool is designed to be used while manually tracing cables before
```

```
an LCR.
    Proceeds switchport by switchport, displaying current
description/cross-connect.
    Prompts user to confirm current description is correct.
    If correct, moves to next switchport.
    If not correct, prompts new cross-connect description, which is then
applied to current
    switchport config.

    Args
    \t<switch> - the switch name
    \t[start-at] - optional: the port to begin with; default is first
interface on switch

    """.format(sys.argv[0])
    print(description)
    sys.exit(5)


'''
    sys.argv is accessible globally, apparently
'''
def update_descr(child):
    if len(sys.argv) == 3:
        startat = sys.argv[-1]

    # get all ports
    child.sendline('term len 0')
    r = child.expect(['[\r\n][0-9a-zA-Z\._-]+#']) #Cisco (already enabled)
    child.sendline('show int status')
    r = child.expect(['[\r\n][0-9a-zA-Z\._-]+#']) #Cisco (already enabled)
    x = child.before

    if 'startat' in locals(): # start at specified port
        lines = x.decode("utf-8").splitlines()
        start = [i for i, line in enumerate(lines) if startat.lower() in
line.lower()]
        ports = x.decode("utf-8").splitlines()[start[0]:]
    else: # start at first port
        ports = x.decode("utf-8").splitlines()[3:]

    # for each port
    for port in ports:
```

```
        # display current config
        print('\n-----------------------------------')
        print(port)
        print('-----------------------------------')
        portname = port.split()[0]

        # if correct -> accept and move to next port
        ans = input("Is this configuration correct? (y/n) ")
        while not ans in ['y', 'n']:
            ans = input("Try again; please type y or n.\nIs this
configuration correct? (y/n)")
        if ans == 'y':
            continue
        # else
        elif ans == 'n':
            # prompt for new description
            desc = input("new description: ")
            print(desc)

            # update switchport
            #child.sendline()
            child.sendline('conf t')
            child.expect(['[\r\n][0-9a-zA-Z\._-]+\(config\)#']) #Cisco
(already enabled)
            print('entered configuration terminal')
            child.sendline('int {0}'.format(portname))
            child.expect(['[\r\n][0-9a-zA-Z\._-]+\(config-if\)#']) #Cisco
(already enabled)
            child.sendline('description {0}'.format(desc))
            print('set new description')
            child.expect(['[\r\n][0-9a-zA-Z\._-]+\(config-if\)#']) #Cisco
(already enabled)
            child.sendcontrol('z')
            print('exited conf t')
            child.expect(['[\r\n][0-9a-zA-Z\._-]+#']) #Cisco (already
enabled)
            # wr mem
            child.sendline('wr mem')
            print('wrote to memory')


def main():
    global child
```

```
    signal.signal(signal.SIGINT, handleSigInt)
    ppath = os.path.expanduser('~/.sshp.password')

    if len(sys.argv) < 2 or '-h' in sys.argv or '--help' in sys.argv:
        show_help()

    password = load_password(ppath)
    child = pexpect.spawn('ssh', sys.argv[1:2])
    shutil_size = shutil.get_terminal_size()
    child.setwinsize(shutil_size.lines, shutil_size.columns)
    signal.signal(signal.SIGWINCH, handle_sigwinch)
    child.logfile_read = sys.stdout.buffer
    ret = child.expect(['assword:', pexpect.EOF, '\(yes/no\)\?'])
    if ret == 1:
        processError(child.before)
    if ret == 2:
        while ret != 0:
            input = sys.stdin.readline()
            child.send(input)
            ret =  child.expect(['assword:', pexpect.EOF, '\(yes/no\)\?',
"'yes' or 'no'"])
            if ret == 1: sys.exit(6)
    child.sendline(password)
    r = child.expect(['[\r\n][0-9a-zA-Z_-]+@[0-9a-zA-Z\._-]+>', # Juniper
                      '[\r\n]apc>', #APC UPS
                      '[\r\n]\([0-9a-z-]+\) .*#', #Aruba MM, MD
                      '[\r\n][0-9a-zA-Z\._-]+>', #Cisco IOS
                      '[\r\n][0-9a-zA-Z\._-]+#', #Cisco (already enabled)
                      '[\r\n][0-9a-zA-Z_-]+@(.*)#', #F5 TMOS
                      '[\r\n]\x1b\[.*[0-9a-zA-Z_-]+#']) # Cisco ACI (ANSI
xterm sequence???)
    ''' regex notes:
        - serv1 (NX-OS) prints \r\n\r before the prompt line. so you can't
just expect a \n
        - juniper has username@hostname> format.
        - Cisco (IOS) has hostname> format with no trailing space.
        - NX-OS has a trailing space after the prompt.
        - F5 has a long prompt with lots of info. Starts with
'username@(hostname) and ends with #'
        - we are allowing hostnames (and usernames) to contain
alphanumerals, hyphen underscore and period.
    '''
    if r==0:
```

```
        # Juniper (don't try to enable at '>' prompt)
        pass
    elif r==1:
        #APC prompt always 'apc>'
        pass
    elif r==2:
        #already enabled (aruba mm, md)
        pass
    elif r==3:
        # need to enable
        child.sendline('enable')
        child.expect('assword:')
        child.sendline(password)
    elif r==4:
        # already enabled (or NX-OS)
        pass
    elif r == 5:
        # already enabled (F5 TMOS)
        pass
    elif r == 6:
        # Cisco ACI - no enable needed
        pass
    child.logfile_read=None
    update_descr(child)


if __name__ == '__main__':
    main()
```

Appendix D - Interview with Security Team

Interview Date: October 8, 2022

Matt Thomas is the Information Security Architect for Old Dominion University's (ODU) Internet Technology Services (ITS) department. A graduate of Radford University, Thomas joined ODU in June of 2021.

His background in IT extends as far back as high school, where he operated his school's computer repair shop. During this time, he acquired his Linux+ and A+ certifications, and took two years of programming classes. Encouraged by some of his teachers, he matriculated to Radford University as a Computer Science major, concentrating in Software Engineering and Database Management, as well as attaining an undergraduate Information Security certificate.

While attending Radford University, he interned in the web department as an associate web developer. Shortly before graduation, he was offered a full-time position in this department - "an interesting job, a very small shop," as he describes it. "The whole web department for the public website, the mobile app, all of it was just three people, and I was one of those three."

Additionally, Thomas assisted the Security department. "We had one Security engineer, and a [Chief Information Security Officer (CISO)] position, which was always unfilled. So I was always supporting and helping in Security matters. I got very interested in Systems, and started branching out a lot into System Administration, and then Networking on top of that."

Thomas felt he had gained all the experience he could from the position he was in, and so began looking for a new position as either a DevOps engineer or a Security Engineer, with a preference for Security. When the Security Engineer position at Radford became available, he took that position.

Eventually, he was made backup CISO, and after the CISO left that position, he was made acting CISO for Radford University. Through this position, he became involved in the Virginia Alliance for Secure Computing and Networking (VASCAN), where he was able to meet and collaborate with other CISO-level peers throughout the Commonwealth to gain insight on best practices and lessons learned. Through connections made at VASCAN, he learned of the ISA position at ODU.

I met with him over Zoom on November 4th, 2022, to get some of his insight as a working professional in the field of CyberSecurity.

Baty: What are the most important knowledge, skills, and abilities needed by someone in this field?

Thomas: Information Security is one of the few fields that has an incredibly wide background of people coming in. In a way, you getting a Cybersecurity degree makes you a minority in the field.

I would say that program should teach you a ton of theory of the why and how. Things like “principles of least privilege” and all these principles of Security. And those are great and good things to know.

But without a background in the actual core of IT, they can be hard to apply. So I have felt incredibly well-served from my background as a developer, for one. That's a skillset not a lot of people have in Security, so that’s been invaluable in a lot of ways.

And the other: SysAdmin, and Help Desk, for that matter. You know, when you rise up out, especially out of Operations…. It’s incredibly common for people to start in the field as a [Security Operations Center (SOC)] Analyst. You’re sitting there, you’re responding to alerts, you’re following your procedures and your playbooks, you’re escalating, and you rise up the ranks there. But as you get into Security engineering, now you’re building all those tools and procedures, and helping inform the business on risk, and ‘what should we do’. There is a cost to implementing two-factor authentication for an entire university, and not just a monetary cost, right? The politics, the getting buy-in, the supporting from a help desk standpoint, when it doesn’t work, when they lose a phone.

It’s one thing to read in a book ‘hey, this is what you should do - you should block all outbound traffic’. Oh yeah, that sounds great! And now have fun writing forty thousand firewall rules to allow what’s needed, granularly. So you’ve gotta take tradeoffs. There is a huge benefit of having other backgrounds than just running IT, and business, to help inform the Security. So I wouldn’t trade my Systems background for the world. It’s been invaluable on top of the Security skills.

Baty: Do you find the skills learned at CTFs useful in your job?

Thomas*:* If you want to be a penetration tester, CTFs are wonderful. You know, they’re not always one hundred percent applicable, but they’re far more applicable to that career path. And that is my recommendation for people who want to do pentesting. You should go do Hack The Box and Try Hack Me and compete in CTFs, because it’s that sort of relentless ‘try this, fail, try again, do this again’ - that is what pentesting is at the end of the day. So it’s a pretty applicable skillset, even if in the real world no one’s using steganography and hiding flags like that.

But what CTFs really help show, especially to a potential employer, is some drive and curiosity, and that can be a very valuable thing to show, without a doubt.

Baty: What is your most favorite or most challenging event or project you’ve worked on?

***Thomas**:* Small things can have huge impacts. Our SSO page at Radford got, I think it was forty thousand authentications a day. Which is not actually that big, in the grand scheme of tech - it's not Twitter, right? But, when you pulled up our SSO page, it didn't have the auto-focus attribute on the username, so you'd actually have to go and click 'username' to put in your username. And I saw that one day and went and changed it, added autofocus. This is where your cursor should start, you know?

And I thought to myself, "over ten years, forty thousand logins a day, how many seconds of time did I save? Like, aggregate human time of not having to grab your mouse and click the username box". Admittedly, this was bad. Like, I didn't follow change management, I didn't get approval, I didn't go through any of the stuff we were supposed to. But the thing that just made me personally happy was just, "How much time did I save?"

Baty: The focus of the degree I'm doing is very technical: programming/CS type classes; electrical engineering type of classes; and then policy/cyber law type classes. I realize this is pretty broad, but I was interested to know what you might suggest as far as entry-level jobs, or what sort of jobs I should be looking at in the next eighteen months for when I graduate?

I don't know a ton about ODU's program, and it's a little heartening for me to hear that there is a bunch of technical stuff. I'm biased, I'm a computer science major, right? Like, I did software engineering. But I do think that it did help me a bunch. Did it teach me my day-to-day on the job skills? No, not at all. But it does inform that foundation of knowledge, without a doubt.

So, what do you like?

Baty: I really enjoy programming. I'm really attracted to the hands-on-keyboard, digging around in memory, researching, looking up man pages. That's what I'm interested in.

Thomas: Are you interested in consulting? Being billable? Working your own hours? Or would you rather be ingrained in an organization and be part of that team? Huge companies? Small companies?

Baty: What I'm looking for most is stability, ideally something fully remote. And maybe the flexibility to take some freelance work, but I don't love the idea of relying on freelance work. I would love a full-time position with benefits somewhere.

Thomas: Well, that's why I ask. Very few companies have an internal red team. They do, but they're the huge companies that can afford that, so you're gonna work at like Fortune 500 to do that sort of thing. I personally know that I don't like tracking hours, I don't like billing hours to clients. So even if you're not freelancing, most pentesting firms, that's what they're doing. If you work for the pentesting firm, you're a consultant for a client for a week or two, and you're billing and tracking your hours. I just happen to know that's something I'm not interested in, so I just rule all that stuff out.

I'm also a little risk averse, like you said 'stability'. I ain't taking contract jobs - nope! I don't want a six-month contract and try to figure out where my next job is after. So that's why I ask, because it can change things a little bit.

I would say, obviously, most blue team jobs aren't so much the contract/consultant. You're usually ingrained in an organization and part of their IT program. So if that's something you're interested in, or if those sorts of things are important, there's more doors there than if you wanted to go red team side. Not to say you can't - you can have it both ways there too, it's just a little harder. It changes how you're applying to companies, I'd say, to an extent. Landing jobs at Silicon Valley and Fortune 500 – they're just different and weirder.

SOC Analyst is the poster board entry-level job, and depending on how mature the organization, it can be fifteen dollars an hour, checking alerts, and following step one-two-three-four-five, and escalating higher up. Not super engaging work. Or it can be something more like what we do. Like our entry level SOC Analyst, sure, you're getting that operations experience, and doing that alert triage. But you're also probably doing incident response. You might get to do forensics on a compromised server or workstation, but we don't do a lot of that because time is scarce. If it came to the point where we need forensics done, we've probably engaged an external forensics firm at that point. We're gonna pay them to do it, just because those skills are so niche, you've got to do it to keep those skills sharp, and we don't have a business case to do it all the time.

So, you know, that's always the staple, if you can get a SOC Analyst job. The most important thing is getting some experience in the industry, to then go the direction you want to go. You almost can't go wrong there.

I wouldn't stray away from a SysAdmin job. I think that could be - you talk about hands-on-keyboard, wanting to program. SysAdmins who can program - people will love you. You wanna script and automate stuff? People love you. And it's great experience. Computing in an advanced, corporate enterprise is completely different than your home lab.

If you like programming, I wouldn't be afraid of a developer job. Especially, there might be some jobs around application security. That's its own entire field. That was one of the things they were excited about hiring me for, because we didn't have a lot of people versed in development and security. So DevSecOps, that's its own entire field, if you're more interested in being part of a development shop.

Appendix E - Rapid PVST in Packet Tracer

To learn more about Rapid PVST, I consulted the Cisco Systems documentation on their own website. Additionally, since I'm not terribly familiar with Cisco Packet Tracer, I found another guide demonstrating how to set up a Rapid PVST topology.

Following the guide, I was able to reproduce the results, but I'm not certain I fully achieved the desired implementation. Figure E.1 shows my results in Packet Tracer.

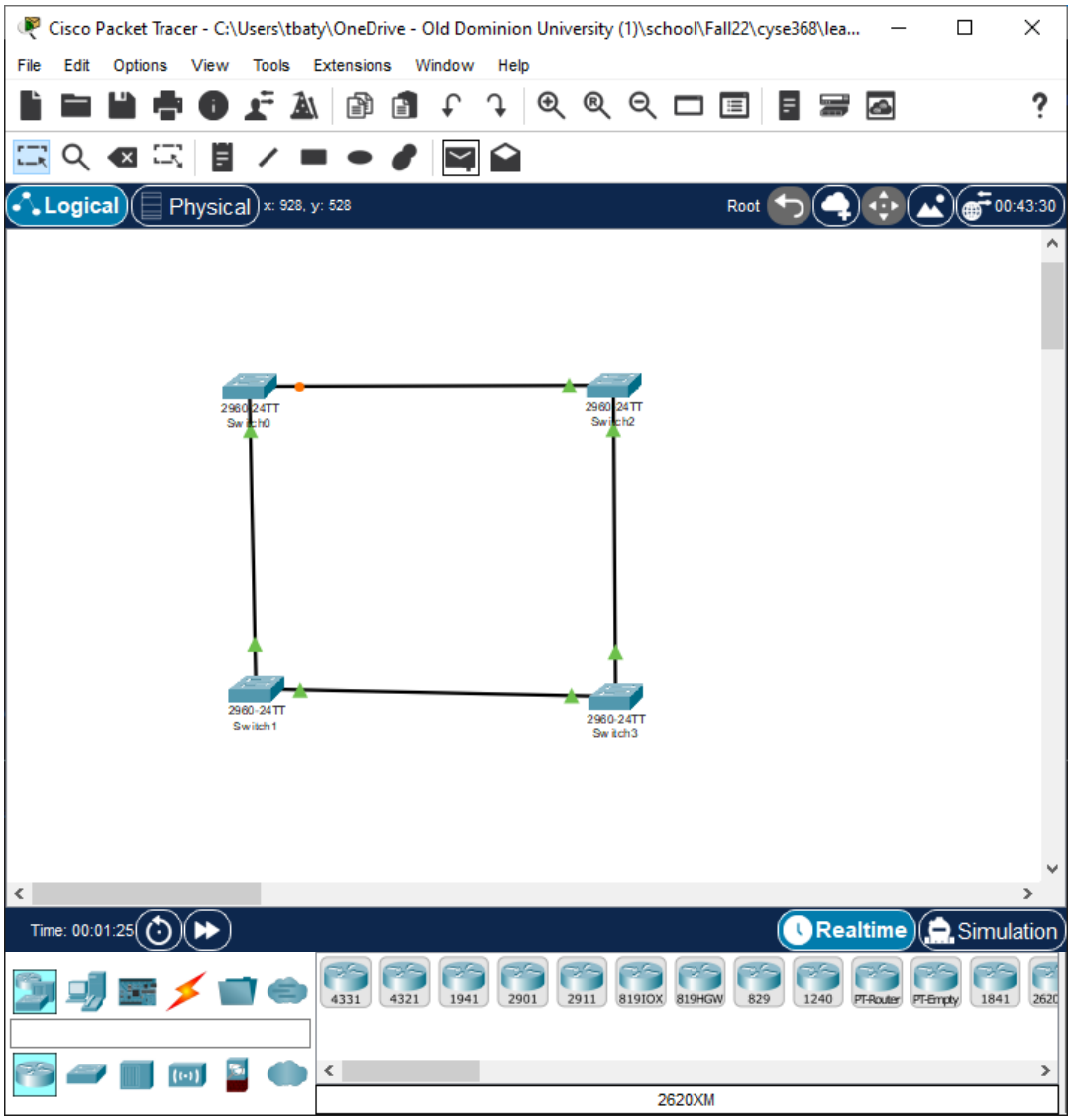


Fig. E.1 - Rapid PVST topology