CIS 403 SITE VISIT REPORT

Example image of data center - taken at Washington & Lee University (located in Lexington, VA)

source: https://www.five9dg.com/projects/richard-a-peterson/#gallery-4

Keith Reis

In-Depth Report of Clarion University’s Data Center/Networking Structure

Field Trip Led by Jason Werwie (CU Computing Services Staff Member)

INTRODUCTION

On October 25th of 2021, me and three others from our Data Communications class visited Jason Werwie's office, located in room G-0 of Still Hall on Clarion University Campus. To give a bit more background details on Mr.Werwie, who's apart of CU's Computing Services staff; the following information was given to us about his job:

- **Worked 10+ years as a Network/Systems Administrator for Clarion University IT Department.**
- **Works mainly in the back-end side of Clarion's network. (Tech-Infrastructure & Network Services)**
- **Maintains network-services/server-racks within the Still Hall Data Center.**
- **Learned a vast majority of his IT skills & expertise through on-the-job experience over the years.**
- **Emphasizes the importance of communication between fellow members of the IT Department; efficiency & organization is key in the proper maintenance of large networks.**

The Clarion IT Department or ‘Computing Services’ can be separated into 3 distinct teams, each with their own unique responsibilities to help maintain the overall well-being of the university network.

- **Tech-Infrastructure:** Manages and operates large IT environments in a back-end domain. Main purpose is to care for the data center, and ensure proper network traffic across all campus buildings & services. Looks for abnormalities in bandwidth usage across campus; and attempts to neutralize any threats found within said irregularities**(for instance, could be a ‘black-hat’ hacker who penetrated through the CU network’s firewall and gained access to information that allows them to execute a DDOS(distributed denial of service) attack against the network.)** Members of this team will also notify students & faculty via EagleMail in the event of suspicious email activity in order to prevent phishing scams from occurring.
- **Application Services:** This department deals with the maintenance and routine updates carried out across the various applications Clarion University offers to the public & it’s students. Notable applications include: MyClarion, StudentInfo System, the Alumni Donation System (located at https://alumniandfriends.cuf-inc.org/donatenow), and most importantly the clarion.edu main website. Staff will process & closely monitor daily traffic & bandwidth usage across these applications for any abnormalities.
- **Network Services:** Similar to the Tech-Infrastructure team; by helping to maintain the overall health and safety of CU-operated networks across campus. May have to repair systems provided via the CU network in the event of a malfunction such as security cameras, WAP**(wireless access points hanging from ceilings in classrooms across campus)**, eagle dollar vending machines, etc. all being accessed by system administrators through different virtual networks in order to avoid

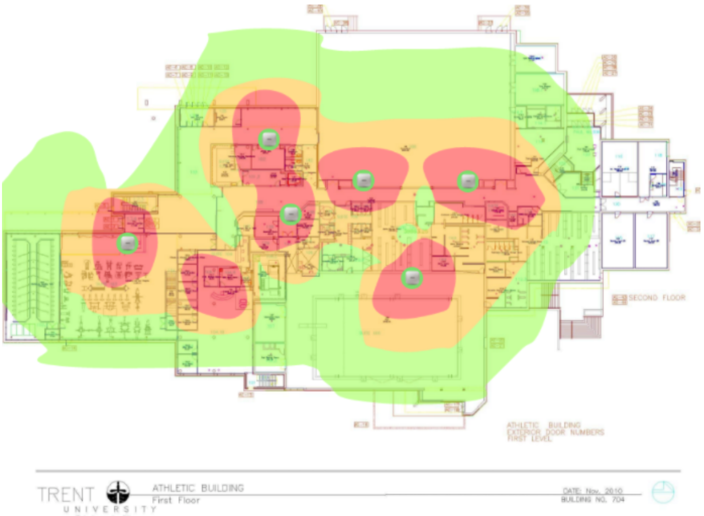
cross-communication over the network.

A team that’s separate but similar to those in the IT Department would be User Services located in Becht Hall. They handle most front-end services provided to the university, mainly tech & hardware used daily in the classroom such as: **(projectors, *SMART*® brand tech, video-conferencing equipment for Zoom(multi-modul classes: microphones, webcameras, etc.))**

CLARION UNIVERSITY NETWORK TOPOLOGY LAYOUT & MAINTENANCE

The physical layout and logical flow of the Clarion University network topology was a topic discussed with Mr.Werwie during our field trip. It was explained that each building on campus has a unique 3 digit identifier #, as well as each classroom or area with a WAP having its own unique identifier # as well. An example would be room G(0) in Still Hall, as it has 2 faceplates in the room named G(0) and G(1). Each building has a ‘server closet’ as well, which houses a server rack that holds switches and routers.Therefor providing network capabilities to the surrounding local environment via its connection to the main data center housed in Still Hall.

Each of these separate networks unique to the building they’re located in can be remotely monitored via the CISCO Prime Infrastructure application**(total of 490 CISCO & 178 Alcatel access points across campus)**. The application has site maps that will load Google Maps into the tool, displaying the entire campus and buildings outlined by their unique network ID. A Green outline stood for UP & OK, meaning bandwidth usage and traffic was normal & healthy. A Yellow outline stood for WARNING, meaning the bandwidth & traffic flow on the network was suspiciously abnormal and should be further inspected by a network administrator. A Red outline stood for DOWN/OFFLINE, meaning the outlined area within the building was experiencing an outage; and should be attended to by the IT Department. You can click a building and zoom in to see the floorplan (which was created by Mr.Werwie himself, as he would visit each classroom and draw the outline ‘concrete walls’ which is done to account for data not being able to properly flow through any sort of concrete barriers). The tool also allows you to search for specific networks by name, transmit level, channel, etc.; and can also generate a heat map of the entire campus based on signal strength.



Example image of network heat map taken from the first floor of Trent University’s Athletics Building. As you can see, red areas would be those that have heavy network traffic/bandwidth usage; while yellow and green areas have less stress and better signal strength.

source: https://www.trentu.ca/it/wifi-heat-maps-non-residence-areas

We were taken to a typical IDF**(Intermediate Distribution Frame)** closet that you would find within each building on campus; the one we visited being directly across the hall from room G(0) in Still Hall. These racks use 6350 and 6450 level switches, the 6350 versions having a 1 Gig uplink speed; while the 6450 version switches have a 10 Gig uplink speed. Port-Based Authentication is therefore used, meaning a user can only pass traffic through a switch port if authentication to the server is granted. A system administrator would have to remotely login to access said ports, with ports 1-10 being in VLAN1, ports 11-15 in VLAN2, etc. As stated, the switch will contact the authentication server, and separates the VLAN of devices based on device type. I inquired as to what the massive black box located on top of the IDF was, and Mr.Werwie explained to me that it stores a large amount of orange multimode fiber cables.

We were also told that in the event of a bad weather storm or ‘power blip’, all network equipment (IDFs) across campus have a built in UPS**(Uninterruptible Power Supply)**, which will provide 10-15 minutes of extra runtime while power is attempted to be restored in the area. This is executed by UPSs to avoid extended periods of unplanned downtime; and possible damage to the network structure.

STILL HALL DATA CENTER

After exiting the IDF, our second half of the field trip was spent in the data center located within Still Hall. There exists one more CU data center as well, located in Becht that was installed around the early 70s with much older & outdated networking equipment. Before even entering the room, a key was needed in order to gain access. Mr.Werwie emphasized this by stating how important following proper security protocols & procedures are in an IT position. You wouldn’t want someone randomly walking into the data center, unplugging switch cables or taking pictures of how everything is set up. You should always ensure to lock the door behind you upon exiting a secure network environment.

Once we entered the data center, me and my groupmates immediately noted how the flooring felt very odd, almost as if the floor tiles were loose and hollow underneath. Mr.Werwie explained that the reason the floor in a data center is so unnatural is because of the massive amount of cables and equipment running underneath the surface-area networking equipment. Certain tiles had a mesh grate over the top, which allowed for temperature control via these cooling ducts built into the floor. In a data center, both temperature and humidity have to be accounted for and maintained in order to keep all network equipment & hardware healthy and fully operational. Mr.Werwie opened a large gray cabinet, showing us the data center’s UPS system; which housed a plethora of battery packs strapped together. In the event of a severe power outage **(one that would last longer than 1 hour max)**, the emergency generator of 275kw diesel-power will kick in; and has the capability to run the entire data center room for 7 days on ‘full juice'. A transfer switch flips over in order to begin using said generator power, and it is tested weekly by maintenance in order to ensure proper functionality.

Upon further inspection of the server cabinets located in the data center, it was seen that DELL Servers were used for Clarion's network; while the nimbleStorage brand is used for virtual environments. Two 6900 switch series are also used in one black server rack, as they are beefier and overall better than other switch series available. I asked Mr.Werwie what the orange plastic tube located throughout the back of the rack was; and he explained it's an 'inter-duct', or more specifically: orange corrugated loom tubing. Any type of fiber cabling must be run through either a plastic conduit such as the one I saw on the field trip in the IDF closet's rack & data center's racks, or use armored fiber optic cables. Depending on the distance needed to be travelled by said cabling. STC has the most fiber cables coming in & out of the building, as well as the highest # of total network connections. The 2 fiber types used throughout the data center are multi-mode(**aqua cables**) for close distance connections, and single-mode**(orange cables)** for long distances.

My next question had to do with the surrounding lights flashing around us constantly since we had entered the data center. Each panel & rack had a line of either green or amber flashing LED bulbs, and it was explained that these are known as 'link indicators' or 'status lights'. A green light indicates a 10 gig connection, while an amber light indicates a 1gig connection.

Josh, who was a part of my group, proceeded to point out another notable facet of the data center, which was a large chain-link cage in the back corner surrounding an isolated server rack. This acts as a safety divider between the CU Data Center, and the PennREN service node we share our space with. Whenever someone from the ISP company (PennREN) needs to come in to check the node, they can do so by entering a locked door located at the back of the caged area; and will have no way of gaining access to the data center due to said divider. As previously mentioned, good security is key in preventing unwanted damage to the networking environment. We proceeded to ask Mr.Werwie if any other security or safety measures are in place within the data center, and were told the following 2 bits of information:

- There are 2 cameras in the Data Center that the Public Safety building monitors consistently.
- In the event of a fire, a flame-extinguishing chemical will be released out of sprayers onto the equipment. Water or other more common flame-extinguishing methods cannot be used due to the heavy damage it can cause to surrounding equipment.

COMMONLY USED APPLICATIONS/NETWORK TOOLS

After our visit to the data center, we returned back to Mr.Werwie's office and sat down for the last 20 minutes to go over some of the commonly used applications and tools he uses throughout his average workday as a systems administrator. As stated by Mr.Werwie at this time, *"Documentation is key to maintaining a network."* which can be done through the use of organizational networking tools. I've compiled the following list, which states each application we went over, as well as documentation of Mr.Werwie demonstrating how to use said tools.

- **OmniVista:** Used for remote management of Alcatel wireless access points throughout campus. Looks roughly the same as the CISCO Prime Infrastructure tool. Shows a generated map of Clarion campus with a heat-map of each WAP's signal strength: closer to 0 means it is a strong signal, while something like -40 means it is a much weaker signal.
- **Cacti:** Used to monitor network bandwidth usage across campus. Also graphs important Juniper router traffic information for system administrator analysis. As Mr.Werwie went into detail about

his analysis of bandwidth usage over recent time across campus, he stated bandwidth usage hasn't really recovered since COVID. With everyone in the area using considerably less bandwidth in recent months. If a link reaches maximum bandwidth usage, the system administrator will get an email notification telling them the abnormality in traffic requires further inspection.

- **EATON:** Tool for management & monitoring of UPSs. Can look at a UPS cabinet's power consumption, see when batteries need replaced, and other important energy-related information.
- **WhatsUpGold:** Application used for availability monitoring across our network. Uses pings on switches to see if they're ok and operating normally. Has a built-in system that will send text to system administrators when switches and/or network devices go offline.

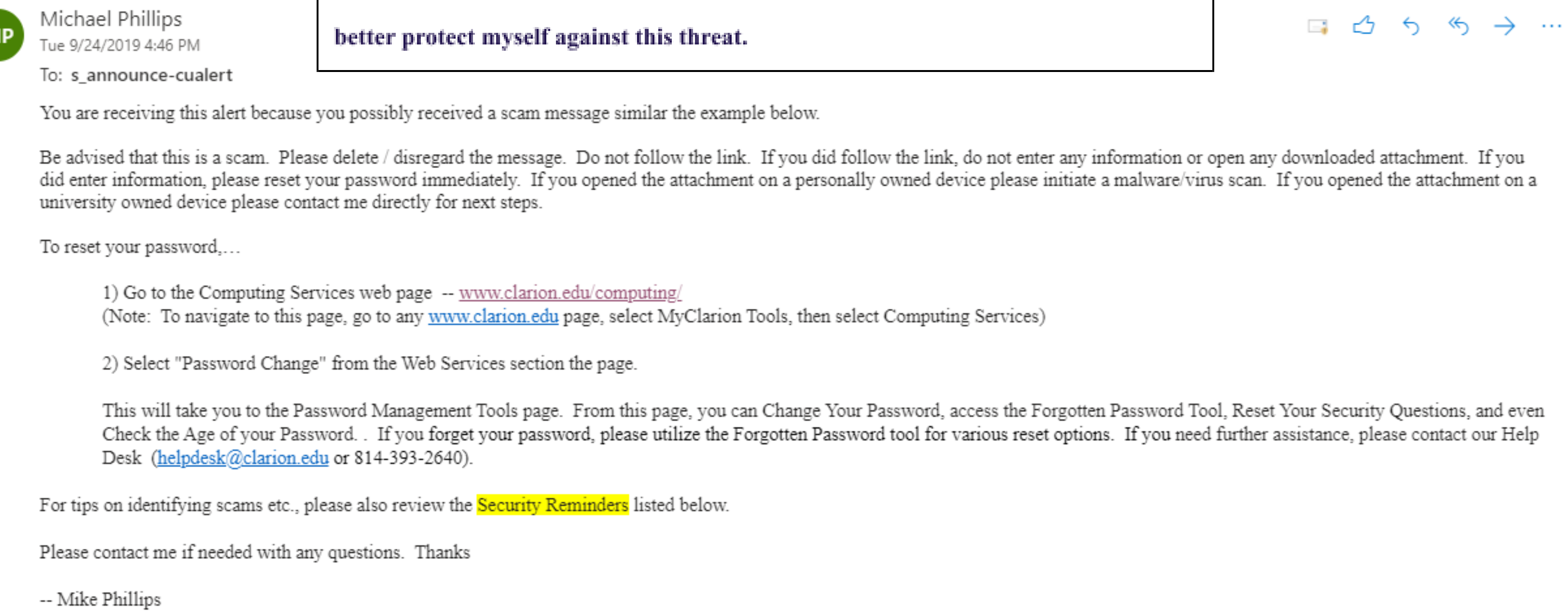
Q&A PORTION

As we closed in on the end of the field trip and were running short on time, Mr.Werwie allowed us to ask any final questions or clarifications to previous bits of information if needed. I queried Mr.Werwie about one of my Field Trip questions I had uploaded to D2L, which was:

> "Has there ever been a time where the Clarion University network came under attack from outside threats? (Through use of DDOS (Denial of Service), Ransomware, SQL Injection, etc.) If yes, how was the threat avoided/resolved; and what steps were taken to better protect against future threats to the network?"

Mr.Werwie informed me that the biggest threat thus far to Clarion University has been phishing scams. There is a heavy usage of email notifications to let system administrators know if someone with a school email has been receiving suspicious or abnormal emails from outside sources. Although the firewalls do have intrusion protection, he stated that our network has been breached in the past before despite our best efforts to protect against it. For example, if someone clicked a phishing link, and accidentally downloaded a powershell file, the hacker could possibly gain access to vulnerable areas of data such as the staff registry. Mr.Werwie then summarized this by saying *“Once an endpoint is compromised, they’ll most likely search for more areas to access.”*

This is an example of an email sent to me from system administrator M. Phillips in 2019. He alerts me that I received a possible scam message, and advises me how to better protect myself against this threat.



Michael Phillips
Tue 9/24/2019 4:46 PM
To: s_announce-cualert

You are receiving this alert because you possibly received a scam message similar the example below.

Be advised that this is a scam. Please delete / disregard the message. Do not follow the link. If you did follow the link, do not enter any information or open any downloaded attachment. If you did enter information, please reset your password immediately. If you opened the attachment on a personally owned device please initiate a malware/virus scan. If you opened the attachment on a university owned device please contact me directly for next steps.

To reset your password,…

1) Go to the Computing Services web page -- www.clarion.edu/computing/
(Note: To navigate to this page, go to any www.clarion.edu page, select MyClarion Tools, then select Computing Services)

2) Select "Password Change" from the Web Services section the page.

This will take you to the Password Management Tools page. From this page, you can Change Your Password, access the Forgotten Password Tool, Reset Your Security Questions, and even Check the Age of your Password. . If you forget your password, please utilize the Forgotten Password tool for various reset options. If you need further assistance, please contact our Help Desk (helpdesk@clarion.edu or 814-393-2640).

For tips on identifying scams etc., please also review the Security Reminders listed below.

Please contact me if needed with any questions. Thanks

-- Mike Phillips

CONCLUSION

To conclude my report with a more personal and informal perspective, the CIS 403 Site Visit was an absolutely enlightening and eye-opening experience for me as a CS student. I genuinely enjoyed learning what occurs behind-the-scenes in the Networking Services department while following a seasoned IT specialist. I most definitely felt a sense afterwards of a more solid foundation of knowledge regarding the main chapter topics we've discussed throughout class, as well as topics I was completely unaware of. I'm grateful for the opportunity given to us to spend time in a hands-on environment, seeing up-close and personal how the concepts we went over in class apply to a career in that field.