

# CONSULTATION FOR THE UNIVERSITY OF LOUISIANA AT LAFAYETTE'S COMPUTING AND INFORMATICS DEPARTMENT

Nana Firdausi Hassan

## CONTENTS

Executive Summary.....	2
Describing the Existing Network .....	3
Network Maps/Diagrams.....	5
S.W.O.T Analysis.....	8
Problems with Existing Network .....	10
Network Limitations: .....	10
Gaps .....	11
Opportunities .....	12
Recommendations .....	13
Gantt Chart .....	14

## EXECUTIVE SUMMARY

The University of Louisiana at Lafayette's Computing and Informatics Department (CMIX) maintains a growing and dynamic network infrastructure, primarily servicing Oliver Hall. The CMIX network is supported by two main routers and an extensive switch stack which service different components of the department's resources. The CMIX network relies upstream on the greater University of Louisiana Lafayette network, including for internet connectivity, wireless access point management, and many aspects of network security. CMIX nonetheless maintains a full stack of network hardware, including their own managed and unmanaged switches.

The department uses a virtual local area network (VLAN) segmentation extensively, with older legacy networks still in use alongside newer ones. However, the network faces several challenges, including unmanaged switches that can cause network outages, limited redundancy in key components, and reliance on the campus-wide firewall for security, which might not currently provide sufficient protection for certain resources in the department's internal network, such as public-facing resources in the Demilitarized Zone (DMZ).

The CMIX network maintains both physical and virtualized servers which run on hypervisors. The server infrastructure supports a huge variety of application requirements, including web hosting, databases, cloud computing, student services, and research environments. Server and workstation management is primarily handled using Ansible scripts, with a mixture of Linux distributions and Windows-based systems in operation. Windows and Linus management are slightly compartmentalized, with different system administrators overseeing the respective network components.

Despite an overall impressive ability to service a diverse array of internal and external customers, the CMIX network shows several opportunities for improvement in both its optimization and security posture. We recommend finding a technical solution to unmanaged switch implementation, as well as the provisioning of key, managed switches in high-availability pairs. I also recommend improved security auditing, and implementation of firewall rules to supplement services from University Network Services. I also recommend setting time for hardware upgrades for older technology, disaster training and testing of disaster recovery protocols.

Most importantly, I recommend that CMIX work more closely with University Network Services and develop lines of communication between the departments to improve the ability of its systems and network administrators to have full visibility into the management plan governing some of their resources, as well as to provide documentation and redundancy for management of key systems areas.

Under the current organizational strategy, there is little ability for secondary personnel to manage systems they do not primarily oversee. Improving documentation and cross training of

technical personnel will mitigate scenarios where the primary manager of a system is unexpectedly unavailable.

## DESCRIBING THE EXISTING NETWORK

University of Louisiana at Lafayette's Computing and Informatics Department (CMIX) has an ever expanding and ever evolving network. There are two main routers that service Oliver Hall: 10.131.0.0/16 (131) and 10.132.0.0/16 (132). Both are Class C. The first router, 131, covers the CMIX and Center for Advanced Computer Studies (CACS) portion. The second router, 132, covers the rest of Oliver and is entirely managed by University Computing Support Services (UCSS). As router 132 is managed and operated by UCSS, this document will primarily focus on router 131. Currently, the CMIX network connects to Parker Hall and Madison Hall and then to the core router as seen in Figure 1. The 132 routers will eventually encompass the extension to Madison Hall, creating a quadrangle network.

The CMIX department is currently serviced by three different internet service providers (ISP); LUS Fiber, Louisiana Optical Network Infrastructure (LONI), and Cox. The department utilizes Cat5e RJ45 T-568B cables along with two different fiber optic cables, an LC & SC SFP+ and an XFP cable. 802.11ac 5GHz is the internet protocol this department uses.

CMIX has several physical switches throughout the building that it manages, but the Aruba AP-305 wireless access point network switches are serviced by UCSS only. There are 10 Arubas per floor for a total of 30 in Oliver. The following are physical switches maintained by CMIX: Dell Force 10 S50, Dell Force 10 S2410, Extreme Networks Summit X440, Netgear Business GS105, and Netgear Business GS108.

Each of these are located on a designated floor for a total of 13 logical switches as shown in Figure 2. There is at least one switch per floor that bridges both the 131 and 132 networks. These switches can be found in three locations. Networking Closet 104, Networking Closet 218, and Networking Closet 319. At present, there are no high availability pairs, however, Information and Media Networks (IMN) are interested in changing this in the future.

As mentioned, there are two main routers that service Oliver Hall. 131 and 132. The IP Ranges that can be found are 10.131.0.0 to 10.131.255.255 and 10.132.0.0 to 10.132.255.255. There is no firewall that CMIX maintains but rather uses the domain firewall that the rest of the campus uses. Alex Mayer, the Senior System Administrator, said that it would be more complicated to have multiple firewalls.

Virtual local area networks (VLAN) are heavily used in this department. Any VLAN that is of the 700 series is a legacy network. VLANs will be created for research initiatives with their own rules. Figures 3, 4, and 5 have specific labeling for a sample of VLANs assigned. Within the VLANs,

there are several unused or underused VLANS and subnets with at least one subnet that has only one host in it. Whether or not that host is still active is uncertain.

Where only Oliver Hall is concerned with its static IP, there are easily over 400 machines operating as endpoints with over 700 end users. This is under the assumption that the users comprise of current faculty, undergraduates, and graduate students and does not include computers loaned out to other departments. CMIX additionally has assets located in other buildings and locations such as Abdalla Hall, Moody Hall, and Agnes Edwards Hall.

CMIX maintains 43 servers in its Data Center with some additional desktop servers in the department. The desktop servers will have Windows 10 or 11 installed on them as well as Linux Mint 18-21. Mint was chosen for its usability. Ubuntu 16-24 is used for the rack servers. AlmaLinux 8/9, Debian and Devuan are other Linux distributions that CMIX will use. CentOS 7 was used but due to its discontinuation, AlmaLinux 8/9 was chosen to be its successor.

Alex performs all server and most workstations updates through Ansible scripts. He and Troy Leger, another system administrator, maintain the Windows 10 machines. UCSS maintains the Windows 11 computers as they are domain joined to louisiana.edu and therefore need no interference.

CMIX also employs four hypervisors on bare metal servers for the public virtual machines. They are used by individual research groups to virtualize research environments. The hypervisors will typically have Ubuntu or another kind of Linux distro. The hypervisors are accessible with Linux's integrated Kernel-Based Virtual Machines (KVM) and a Virt-Manager thus eliminating any need for another operating system. These have a RAID 1 setup consisting of two drives: one original, and one mirror with a dual power supply for redundancy. The bare metal servers are older machines converted to handle lower computational power tasks. Dell PowerEdge 1950s is one example product used which holds monitoring information such as temperature.

Lastly, the CMIX network has several additional key applications outside of the hypervisors that assist with monitoring, accessibility, and functionality. These applications are named with specific purposes as shown in Figure 6 and 7, many of which are virtual machines or for storage.

## NETWORK MAPS/DIAGRAMS

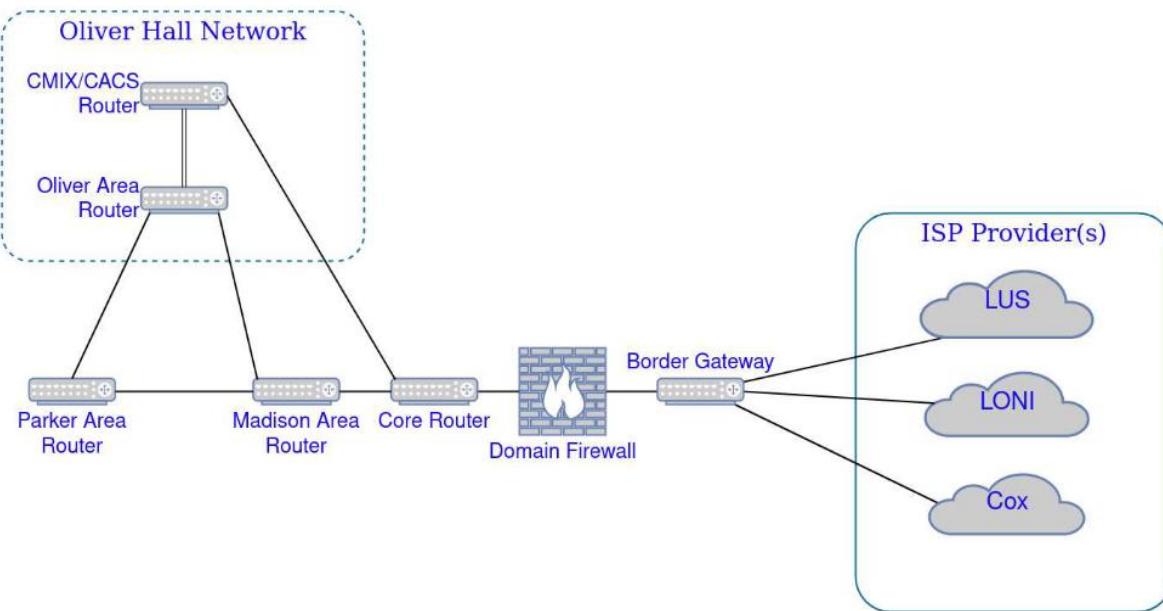


Figure 1

## Layer 2 – Switch Diagram

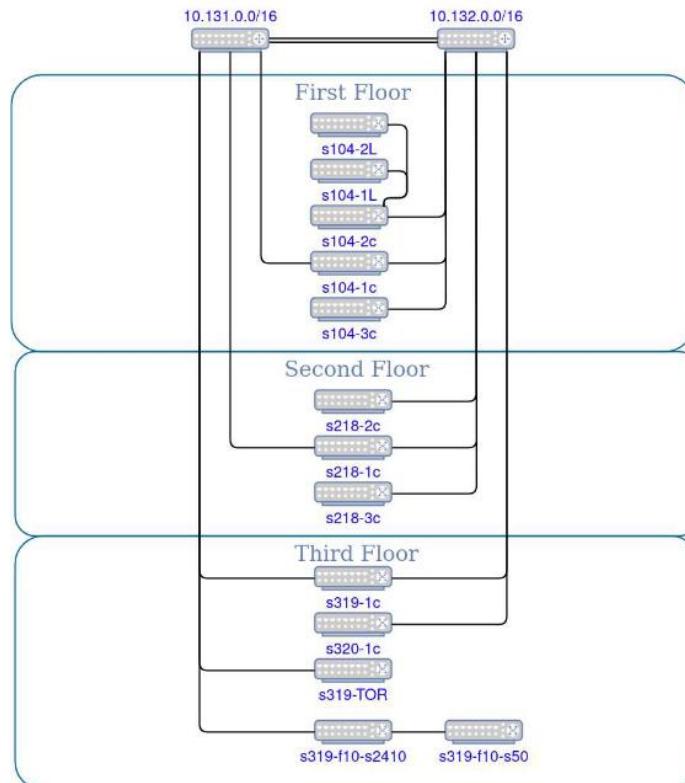


Figure 2

### Subnets/VLANs under 10.131.0.0/8

- 10.131.0.0/24 VLAN 200 (IMN service VLAN)
- 10.131.29.0/24 VLAN 729 (previously used for research initiative)
- 10.131.30.0/24 VLAN730 (public/outbound access for people.cmix.louisiana.edu and others)
- 10.131.31.0/24 VLAN731 (internal access only, primarily servers in datacenter)
- 10.131.36.0/24 VLAN736 (previously used for research initiative)
- 10.131.37.0/24 VLAN737 (10GB Connects to Stephen's Hall for disaster recovery backups)
- 10.131.38.0/24 VLAN738 (Network Cameras/TVs/Audio)
- 10.131.39.0/24 VLAN739 (management, iDRAC and other hardware monitoring services)
- 10.31.40.0/24 VLAN740 (single outbound IP for ongoing research initiative)

Figure 3

### Subnets/VLANs under 10.131.0.0/8 Contd.

- 10.131.60.0/24 VLAN760 (faculty offices)
- 10.131.61.0/24 VLAN761 (TA offices)
- 10.131.62.0/24 10.131.64.0/24 VLAN762-764 (unused)
- 10.131.65.0/24 VLAN765 (classroom dynamic addresses)
- 10.131.66.0/24 VLAN766 (unused)
- 10.131.80.0/24 VLAN780 (uncategorized labs)
- 10.131.81.0/24 VLAN781 (CMPS lab 106)
- 10.131.82.0/24 VLAN782 (CMPS game lab 105)
- 10.131.83.0/24 VLAN783 (2nd floor labs)
- 10.131.84.0/24 VLAN784 (3rd floor labs)
- 10.131.85.0/24 VLAN785 (Unique 3rd floor lab)
- 10.131.86.0/24 VLAN 786 (Unique 2nd floor lab)

Figure 4

## Subnets/VLANs under 10.132.0.0/8

- 10.132.0.0/24 (IMN service VLAN)
- 10.132.3.0/24 (Area Access Management)
- 10.132.60.0/24 (Dean's office)
- 10.132.80.0/24 (STEP Lab(s))
- 10.132.81.0/24 (Unique third floor VR lab)
- 10.132.90.0/24 (Energy Management)

Figure 5

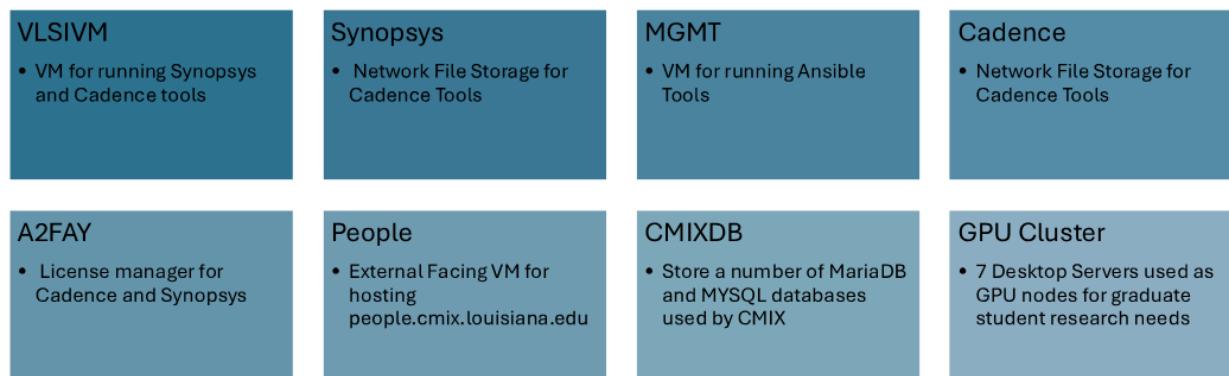


Figure 6

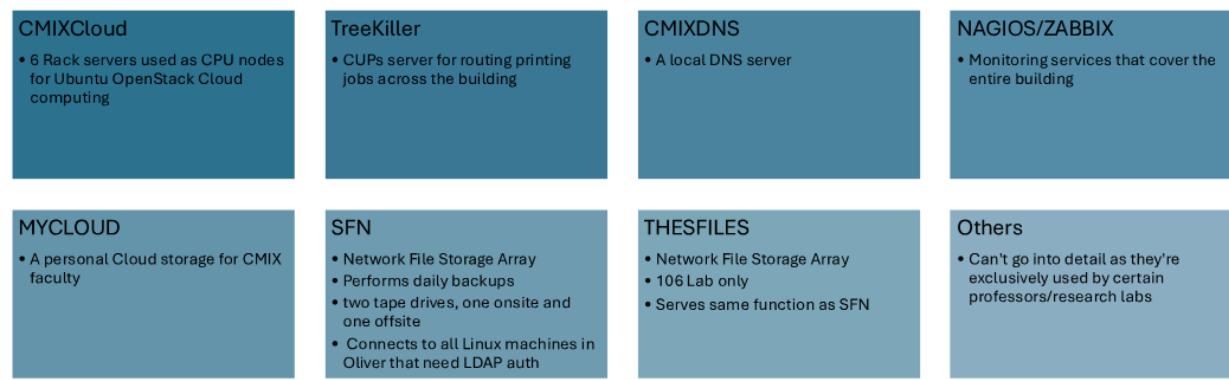


Figure 7

## S.W.O.T ANALYSIS

### Strengths

- Robust Network Infrastructure
- Automated Updates and Management
- Comprehensive Server Support
- Disaster Recovery

### Weaknesses

- Dependency on UCSS
- Limited Redundancy and High Availability Issues
- Outdated physical connections

### Opportunities

- Automation
- Infrastructure Learning
- Backup and Data Management

### Threats

- Reliance on UCSS
- Aging hardware and legacy systems
- Insufficient backup

## **STRENGTHS**

- Robust Network Infrastructure: The department uses multiple internet service providers (ISPs) and has extensive physical and wireless networks within Oliver Hall, with designated switches across floors and high-speed internet protocols.
- Automated Updates and Management: Server and workstation updates are efficiently managed through Ansible scripts, ensuring consistency in security and performance.
- Comprehensive Server Support: The department has 43 servers that support multiple operating systems, including Windows and several Linux distributions, which enhances its flexibility and resourcefulness.
- Disaster Recovery: Documented disaster recovery protocols indicate a level of preparedness for network resilience and data recovery.

## **WEAKNESS**

- Dependency on UCSS for Network Management: UCSS controls significant network resources, limiting the department's ability to manage or troubleshoot outages independently.
- Limited Redundancy and High Availability Issues: Some network closets house critical switches without high-availability configurations, meaning that a single point of failure can isolate up to 20 servers. Additionally, in the event of switch failures, network closets may be inaccessible.
- Aging or outdated physical connections or switches could hamper network speed and reliability.

## **OPPORTUNITIES**

- Automating routine network tasks and security monitoring could enhance efficiency and free up resources for strategic initiatives
- Infrastructure Learning: Improving team knowledge about the infrastructure could optimize operations and improve response times to incidents.
- Backup and Data Management Improvements: With recent improvements in data backup, further advancements could streamline data recovery processes and storage management.

## **THREATS**

- Reliance on External Management (UCSS): Dependency on UCSS for network support can result in delayed response times during outages or other network issues, which could impact departmental productivity.
- Aging Hardware and Legacy Systems: Some network hardware and legacy VLAN configurations may become outdated, leading to maintenance challenges, higher replacement costs, and compatibility issues with newer systems.
- Insufficient backup or recovery could lead to prolonged downtimes in the event of hardware failure, natural disasters, or other catastrophic events.

## PROBLEMS WITH EXISTING NETWORK

As of now, the current network is running fine, but there are a few gaps that are keeping it from running as efficiently as possible. The gaps identified are:

- Lack of managed switches
- Absence of application layer security scan
- Inadequate user training on cybersecurity
- Single firewall dependency
- Backup storage scalability
- Switch failure and limited redundancy

## NETWORK LIMITATIONS:

One of the problems with the network includes unmanaged switches. These unmanaged switches cause loops and network outages. The switches create a loop because 2 wall ethernet cables are plugged into it. Students have mistakenly caused network outages because of this. Speaking of students, another network concern is when they unknowingly fall for phishing scams and other things related to that nature. Falling for these scams exposes the network vulnerability.

When that happens, it is up to UCSS to fix the issue. Anytime an issue arises with the network, it is either UCSS or IMN that handles it. This becomes an issue because UL isn't authorized to fix it, and they must wait for them to handle it.

Because they are not authorized, UCSS/IMN are responsible for handling any issues relating to the routers/switches and they are also responsible for when the network is scheduled goes through unexpected downtime. This is a unique case though because depending on why the downtime is happening, UL can possibly fix the issue. If it is network related, then it is still UCSS/IMN responsibility to fix it. However, if the issue is related to either heat, storage, or RAID then UL can fix the issue. When the issue is related to heat, powering off the devices will allow them to cool, if the issue is related to storage, then replacing the disk will add storage, and if the issue is related to RAID, then implementing the backup and getting rid of the old one will fix the issue. The reason why the solutions to the storage and RAID issue are similar is because they are both related to storage drives. The difference between the two is that the storage issue comes from a singular drive while RAID is an array of multiple drives combined.

Going back to switches, another problem that the network has is that when one switch stops working, it will isolate 20 servers. Not only does this happen, but when the switch is down, the network closets are unable to be accessed. As mentioned earlier, USCC/IMN is responsible for fixing that issue.

Despite receiving multiple monthly vulnerability reports, there isn't any checking for application layer vulnerabilities. This is bad because it increases the potential risk of a security breach for attackers to exploit.

The network originally had a problem with backing up its data. This was mainly because it couldn't back up the data consistently, and the backups also became too large to handle manageably. Eventually this was fixed, and they now run more backup testing to ensure that the data is saved.

The network also doesn't have its own firewall. It is unable to due to the fact that it would be complicated to run it through two layers. Therefore, they go through a domain firewall. While this is not necessarily bad this means that if any threat manages to bypass the domain firewall, information that is on the network would be accessible to the attackers whereas if the network had its own firewall, then then it would be more secure as opposed to the rest of campus because the attacker would have to target the network specifically to obtain information.

## GAPS

The identified gaps highlight several critical issues across the network's layers and components. Physical connections lack clarity regarding ISP bandwidth, redundancy, and service level agreements, while scalability and performance monitoring for evolving standards like Wi-Fi 6 are not addressed. Unmanaged switches present risks, with no redundancy plans for critical hardware. In data links and switches, there are no provisions for cooling, power redundancy, or physical security in network closets. The absence of high availability pairs adds further vulnerabilities, with no defined implementation timeline.

At the network level, reliance on campus-wide firewalls limits customization, and outdated VLANs create security concerns. There are no strategies for addressing wireless dead zones or interference. Endpoint management procedures for device lifecycle and decommissioning are inadequate, with a mismatch between endpoints and users creating potential resource strain. Datacenter operations rely heavily on manual updates, increasing the risk of errors, while outdated operating systems introduce security vulnerabilities. Disaster recovery protocols remain untested, and power redundancy is insufficient for extended outages.

In virtualization, minimal RAID redundancy and outdated hardware limit performance, with no load-balancing strategies for high-demand applications. Security vulnerabilities are compounded by delayed scans and insufficient measures to mitigate internal threats such as phishing. Future scalability plans lack emphasis on storage expansion and AI/ML advancements, while upgrade timelines are vague, with no strategies to minimize downtime.

Addressing these challenges requires enhanced documentation for planning and monitoring, stronger security measures to tackle outdated systems and internal threats, and disaster recovery testing to ensure resilience. Scalability efforts should include detailed timelines and specific resource

upgrades, while automation of updates and endpoint management is essential to reduce errors and improve efficiency. Additionally, regular user training is crucial to mitigate security risks from human behavior.

## OPPORTUNITIES

Based on the limitations above, there are several opportunities that CMIX can take advantage of that would help enhance the network's efficiency, security, and stability.

Taking stability into account, there are several measures that can be taken. By replacing the unmanaged switches with managed switches, this would help prevent accidental loops that are often accidentally created by students. As well as helping to prevent outages. Another option is to perform regular audits and testing of the backup storage and the processes. It is also important to create a better optimization of the backup storage and data compression. This would help reduce the risks that can be associated with unmanageably large files, it ensures data integrity in case there is any data loss.

When it comes to security, there are a couple of things that can be done. For starters, implementing mandatory training and awareness programs for both faculty and students about social engineering, phishing, and other cyber threats. By educating the students and faculty this should reduce the number of incidents that occur and help to protect sensitive information. Another consideration for upping security is to conduct regular security checks. This can be accomplished by creating an additional layer that would identify and mitigate the vulnerabilities that some attackers could exploit. The final opportunity for security would be to consider an additional network firewall installation as it would add an additional security layer that would help to ensure better protection.

In addition to the opportunities listed above, there is another opportunity to be explored. Introducing switch redundancy or even creating a failover plan could be used to minimize the risk of server isolation caused by single switch failures. This helps to reduce downtime for critical systems, as well as ensures continuous access to resources

## RECOMMENDATIONS

Several improvements are recommended to enhance the network at the University of Louisiana at Lafayette's Computing and Informatics Department (CMIX).

First, replacing the current unmanaged switches with managed ones is essential. This change will prevent accidental errors, such as incorrect cable connections, which often cause network outages. Managed switches also offer better control and security, improving overall reliability.

Adding backups for critical equipment, like switches, is another important step. Currently, if a key switch fails, it can disconnect many servers. Backup switches will ensure the network remains operational even if issues arise, reducing downtime and improving stability.

Mandatory training for students and staff is suggested to help them recognize and avoid phishing scams and other online threats. Installing a dedicated firewall specifically for CMIX is also recommended to add an extra layer of security and better protect sensitive data. Regular security scans should be conducted to identify and address potential vulnerabilities.

The backup system needs optimization to ensure efficiency. Backups should be smaller, easier to manage, and regularly tested to confirm they are working properly. Improved storage management will prevent issues with large files and ensure data can be restored quickly if needed.

Monitoring tools should be implemented to detect network issues early and track overall performance. Futureproofing the network by planning for upgrades, such as faster Wi-Fi and additional storage, is also crucial as the department continues to grow.

Outdated virtual servers should be replaced with faster and more efficient options. Load-balancing systems should also be introduced to distribute workloads and prevent servers from becoming overwhelmed during high usage.

Testing the disaster recovery plan regularly is essential to prepare for emergencies, such as power outages or hardware failures. Adding better power backup solutions, like extra batteries or generators, will help keep the network running even during outages.

These improvements will make the CMIX network more reliable, secure, and capable of handling future demands.

## GANTT CHART

TASK	PROGRESS	START	END
Define goals	100%	9/30/24	10/3/24
Request interview and meeting	100%	10/3/24	10/14/24
Collect Information about the Company	100%	10/14/24	10/21/24
Division of duties	100%	10/3/24	10/9/24
Set up team	100%	9/30/24	10/1/24
Create Gantt Chart	100%	10/3/24	10/9/24
Identify Questions	100%	10/9/24	10/23/24
Take pictures and notetaking during interview	100%	10/24/24	10/27/24
Gather feedback/ Find Gaps and issues	100%	10/27/24	10/30/24
Analysis the interview	100%	10/15/24	10/20/24
Provide updates	100%	10/21/24	10/25/24
First draft - Describing the existing network	100%	10/26/24	11/3/24
First draft - Problems with the existing network	100%	11/4/24	11/6/24
SWOT Analysis	100%	10/26/24	11/4/24
Prepare Table of Contents	100%	11/6/24	11/9/24
Prepare the Powerpoint	100%	11/9/24	11/16/24
Evaluate progress	100%	11/17/24	11/20/24
Prepare the final draft of the document	100%	11/11/24	11/23/24
Gather feedback - Recommendation / security overview	100%	11/13/24	11/18/24
Presentation and video script	100%	11/18/24	11/25/24
Edit videos	100%	11/21/24	11/29/24
Submit final report	100%	11/29/24	12/6/24

Sep 23, 2024	Sep 30, 2024	Oct 7, 2024	Oct 14, 2024	Oct 21, 2024	Oct 28, 2024	Nov 4, 2024	Nov 11, 2024	Nov 18, 2024	Nov 25, 2024	Dec 2, 2024
M	T	W	T	F	S	S	M	T	W	T
23	24	25	26	27	28	29	30	1	2	3

