Network Architecture Review of Saini Medical Associates

By:

Ceren Engin

Ipek Kaya

Karan Saini

Niloofar Heidarikohol

Yalda Gheisi

TABLE OF CONTENTS

Executive Summary:

Saini Medical Associates is a privately owned healthcare clinic that provides medical assistance to walk in patients or appointment-based patients. The clinic focuses on delivering health care in a meaningful way as well as participating in clinical trial studies. The team decided it was appropriate to interview the IT manager as well as the Dr. Saini, the doctor that owns and runs the private business, in order to better understand the process of how the clinic functions and how the network compliments this process. During our interview with Dr. Saini, the team came to find out that Saini Medical Associates was running on a charting system that was all done by hand and patient files were filed into filing cabinets. However, recently in the last two years Saini Medical Associates have made the jump to fully online, meaning they had to adopt a new electronic health record system. Many new challenges arose from adopting the new system according to Dr. Saini. According to Mr. Mike Istre, the IT manager, some challenges included employee training, network infrastructure as well as network security. According to Mr. Mike, maintaining a secure network is something that has to be taught to employees. Furthermore, patient data is handled through portals meaning the security is fully outsourced to the companies providing the portal for patient data. The team came to find out the limitations of the network as well as the strengths. Additionally, the team uncovered some critical points of the network that need improvement. These critical points involved the upkeep of network connections between the fax machines and printers spread across the clinic. Moreover, older equipment can be swapped out for newer equipment in order to streamline employee workflow. Overall, the small network at Saini Medical Associates is successful at fulfilling the needs of the clinic however, an improvement is recommended by the team in order to help, Saini Medical Associates, provide a better service to their patients.

Describing the Existing Network:

The existing network at Saini Medical Associates has been implemented and improved over time. Currently the needs of the company revolve around providing network connection between workstations and other devices such as printers and faxes. Years ago, Saini Medical Associates handled all patient records through a charting file system, where they by hand wrote notes and filed patient charts in filing cabinets. The network back then only involved one router connecting the multitude of workstations, printers, and fax machines. However, the one router was not sufficient enough for the company. The one router was not supplying the other half of the building with proper Wi-Fi. Mr. Mike Istre, the IT manager of the office decided that in order to increase the range of the network the office should have two routers. The second router that was installed is being used as an access point for workstations and devices that are closer to the other side of the building. Furthermore, there are two other networks that are within the building. The reason the office has three different networks is due to the different teams working within the same building. Avant Research Associates, who deal with clinical trials, are working hand in hand with Saini Medical Associates. However, Avant has their own network within the building, ensuring they do not interfere with the Saini Medical Associates network. Figure, 1A is a video that shows the internet access point for the many workstations Avant Research Associates have as well as the many devices that run off their network. The third network that is within the building belongs to the CPL lab team. Furthermore, Figure 2A shows all the workstations and devices, such as printers and faxes, that are connected to the

Saini Medical Associates Network. Additionally, Figure 3A shows the small network of the CPL lab team that is within Saini Medical Associates. Lastly, all the phones displayed in the videos and picture below are connected through ethernet by ATT for access to VOIP.

Figure 1A:

Figure 2A:

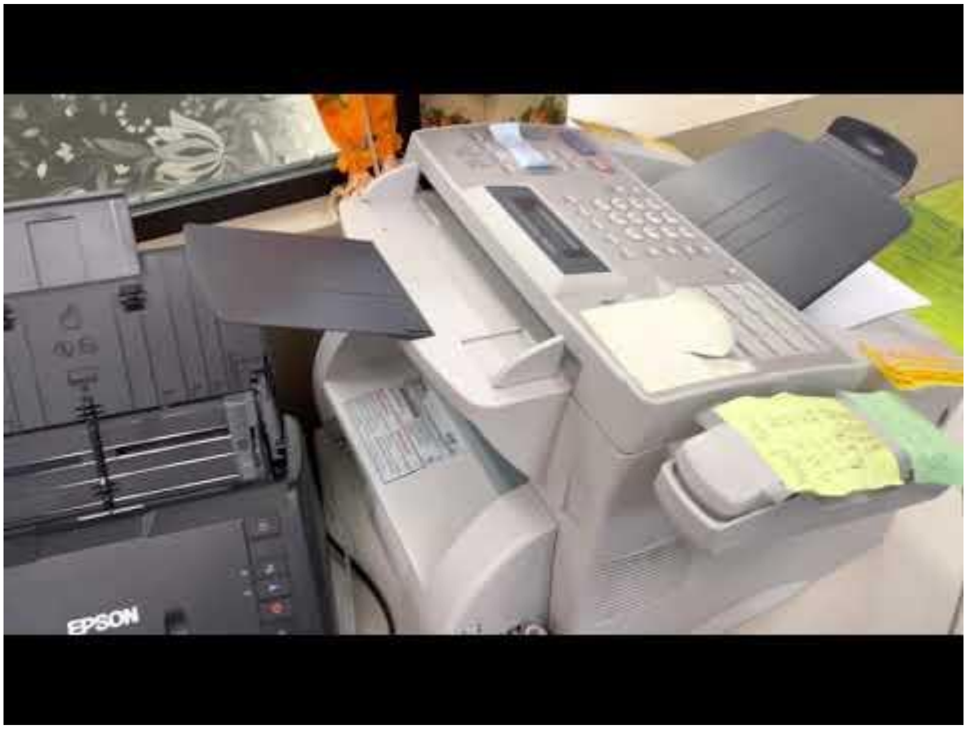
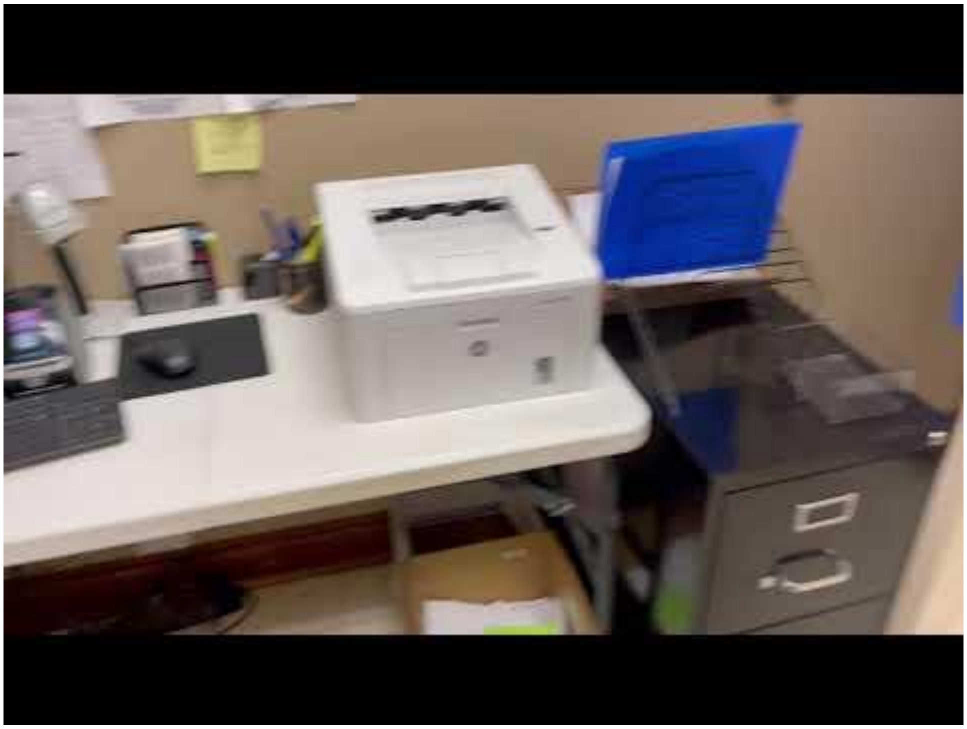


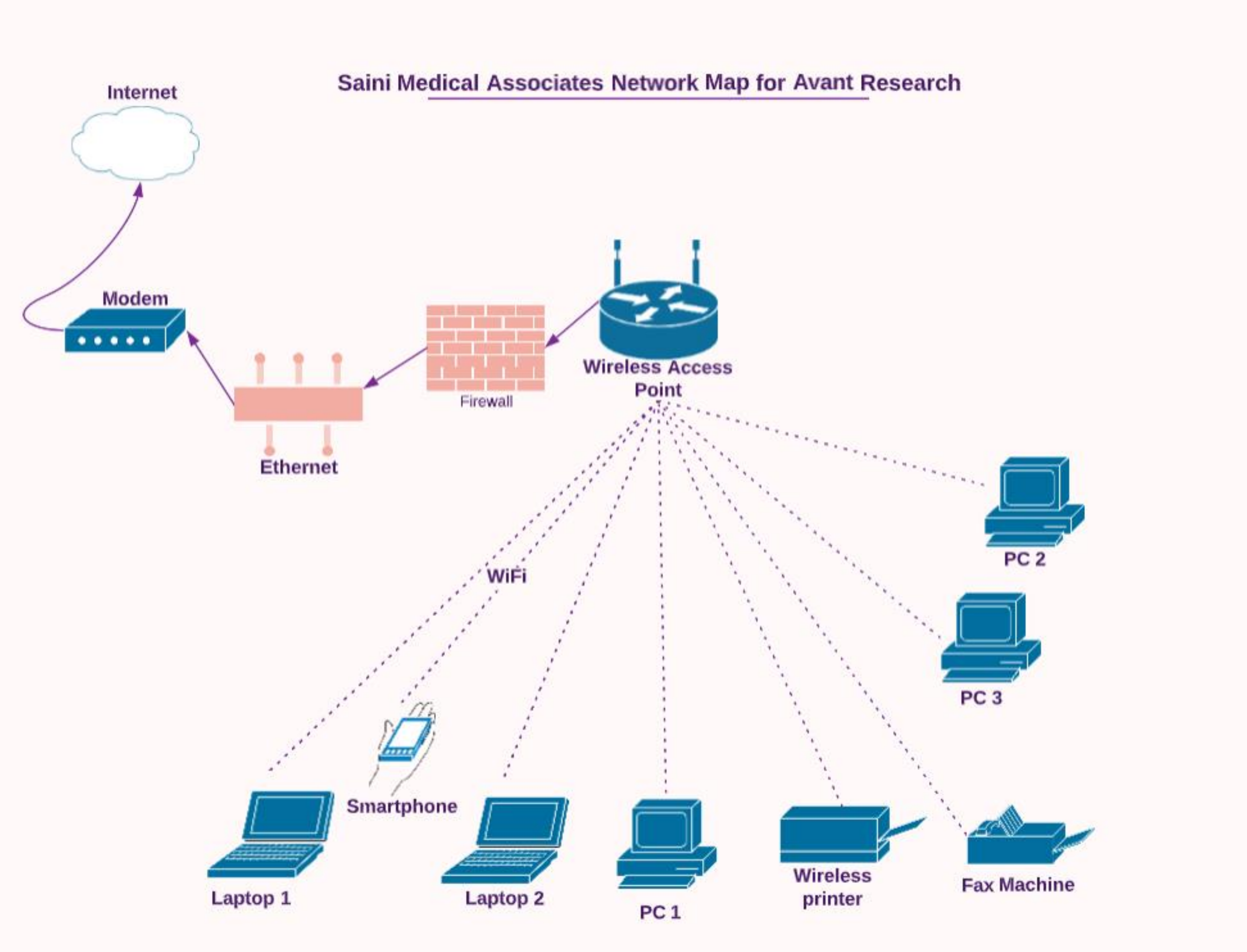
Figure 3A:



Network Maps/Diagrams:

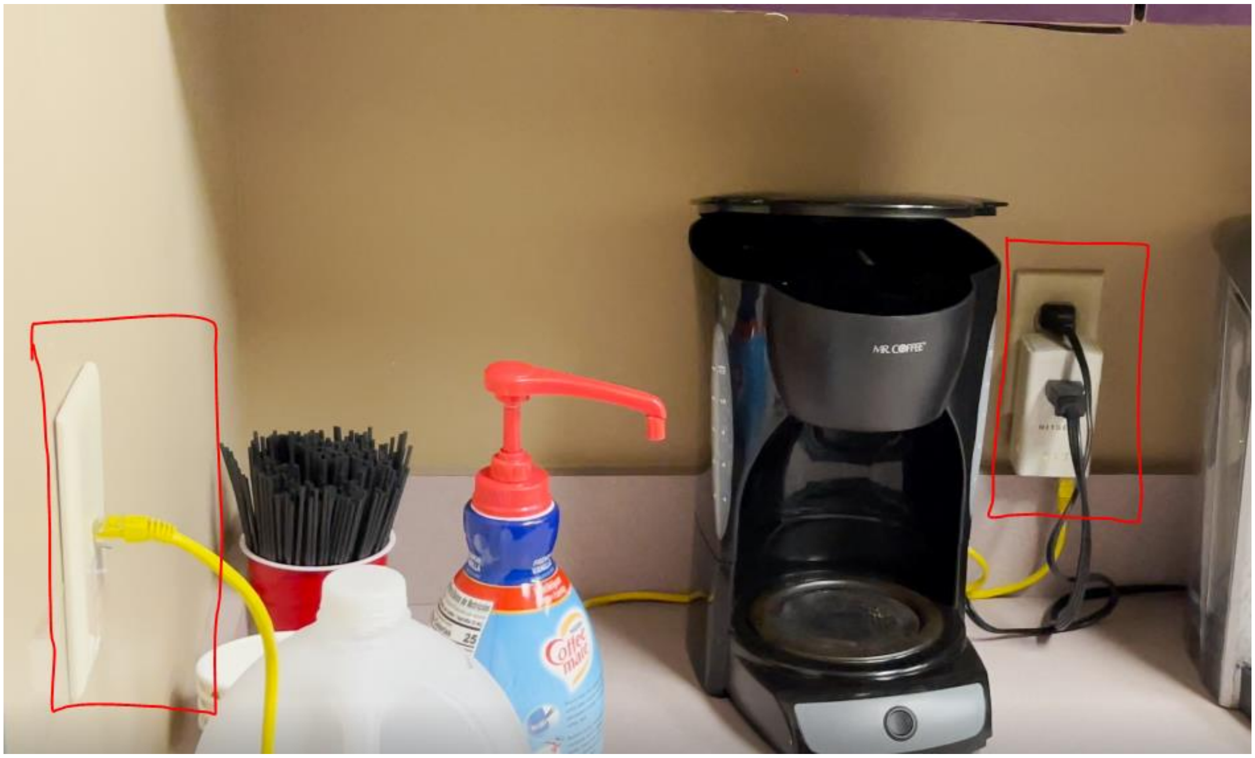
In order to further understand the network, the team decided to map out each of the networks within in the building. Figure 1B below shows the network mapping of the Avant Research network within the building.

Figure 1B



The wireless access point in Figure 1B is shown below in Figure 1.1B. As you can see in Figure 1.1B the wireless access point is connected VIA ethernet to a modem that is within in the wall. Saini Medical Associates have paid Cox to run their network through the walls in order to help keep cables to a minimum. The network map for Figure 1B is constantly changing due to the fact most of the users are connecting through Wi-Fi. Some employees might only connect through their phones for the day, or some employees might connect through multiple laptops. The network seems like a revolving door for anyone that knows the password to access the network.

Figure 1.1 B



Furthermore, looking at Figure 1.2B below we can see that there is multitude of scanners and fax machines that are connected to the network. The whole office utilizes fax machines and scanners to their maximum potential. Having backups incase one fax machine or scanner is down is a must for Saini Medical Associates. The easiest way to connect these machines is wirelessly to the network, thus forgoing the need for multiple ethernet connections. However, later on we will discuss the problems of connecting these devices through Wi-Fi. Lastly, we can also see the multitude of laptops in Figure 1.2 B that are also used to connect to the network.

Many day-to-day operations require employees to be in different rooms of the office thus having laptops to make it easier for employees to transfer from one room to another.

Figure 1.2 B

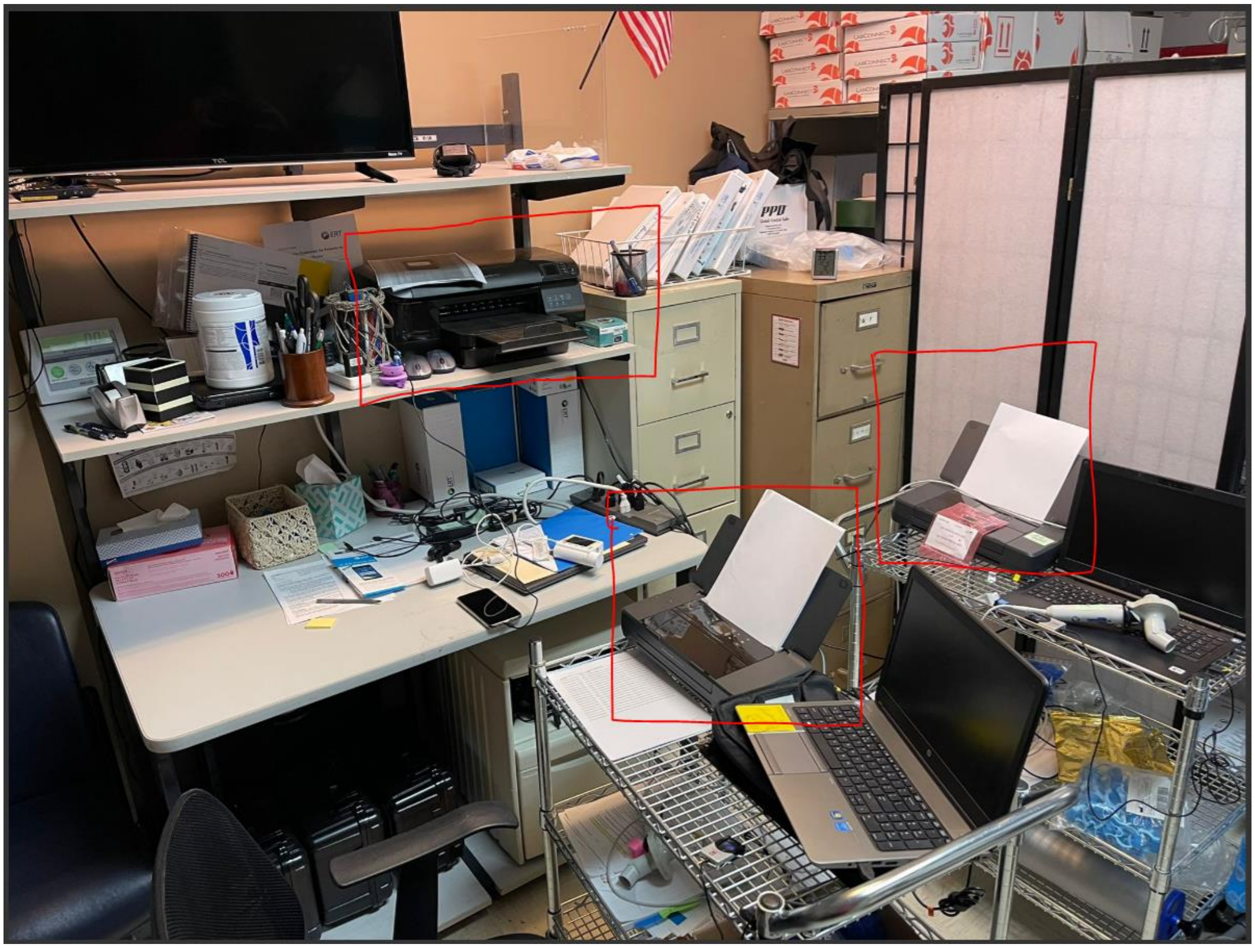


Figure 2B below shows the network map of just the Saini Medical Associates network. As you can see in the network map, Saini Medical Associates uses a two-router setup in order to cover the whole office with Wi-fi. Wireless router 1 is protected through a firewall which is then connected to a Cox modem which gives the office internet access. The reason for the two-router setup is because one part of the office was not getting a proper connection. Wireless router 2 is setup as an access point for employees that are closer to wireless router 2. The two routers can be seen in Figure 2.1 B and Figure 2.2 B. Figure 2.1 B is wireless router 1 and Figure 2.2 B is wireless router 2 or better known as another access point for the office.

Figure 2B

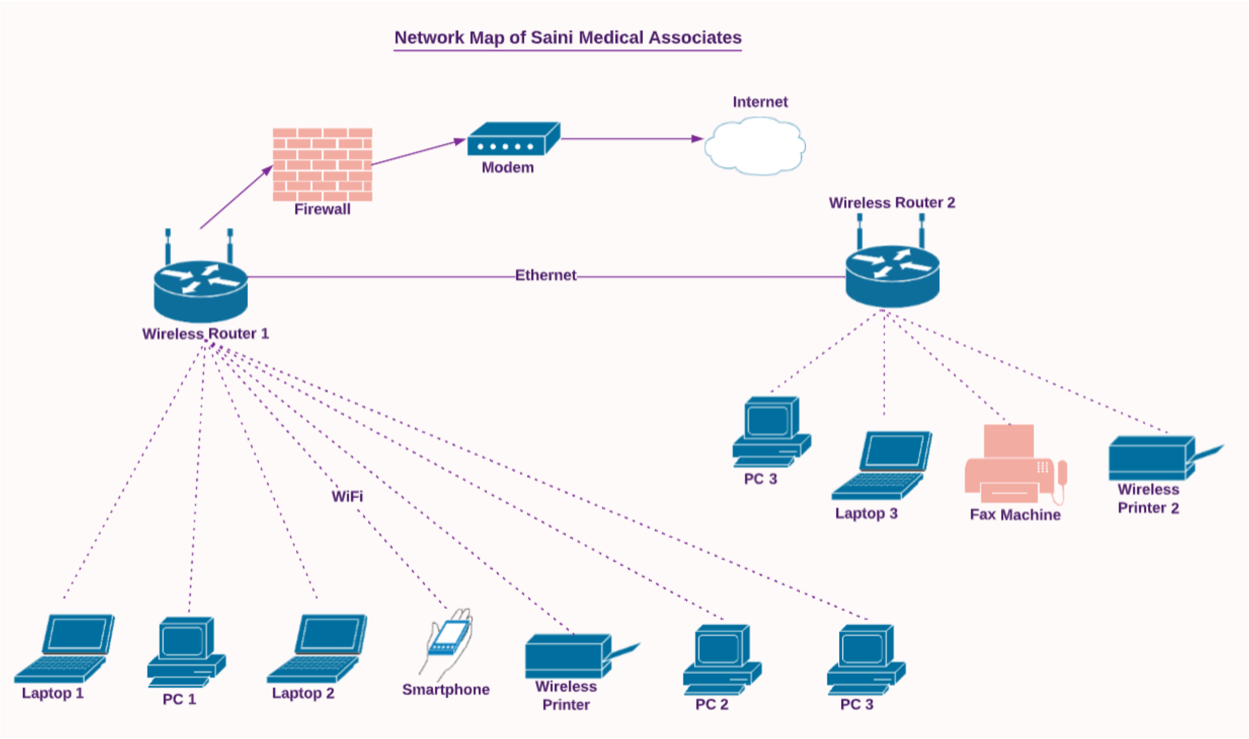


Figure 2.1 B

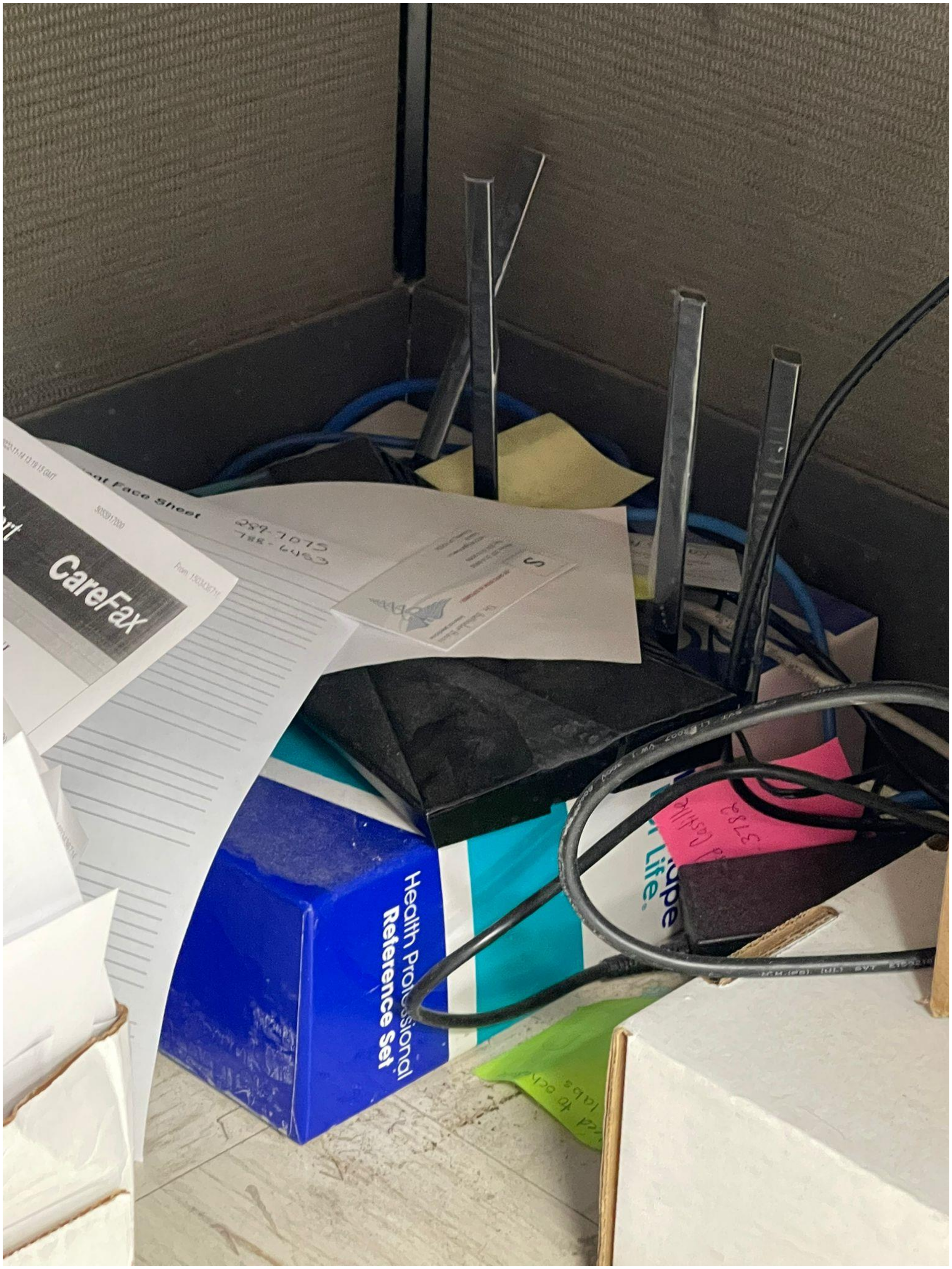
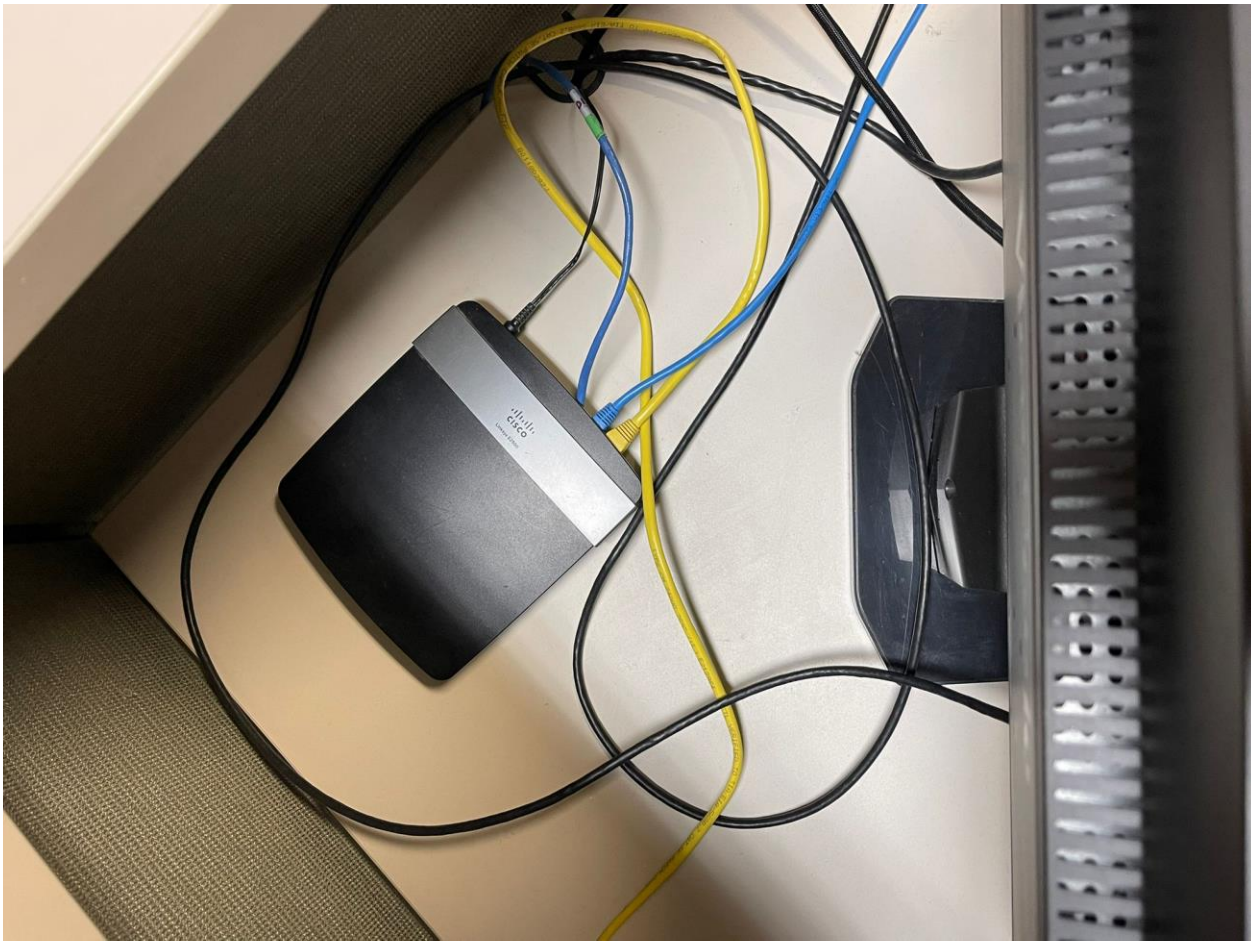


Figure 2.2 B



Lastly, Figure 3B below shows the small network of the clinical pathology lab (CPL) lab. This small network deals with any pathology that needed to be done per patient. Furthermore, the CPL lab is worked by the on-site phlebotomist dealing with anything that requires drawing of blood. Furthermore, Figure 3.1 B shows the CPL room as well has the router/modem combo provided to the lab by Cox. Furthermore, you can also see the wireless printer circled in red this is because this printer can be connected to by anyone in the office. This is important because many times patient's pathology reports need to be sent to the CPL lab and employees can print pathology records straight to the printer in the CPL lab.

Figure 3B

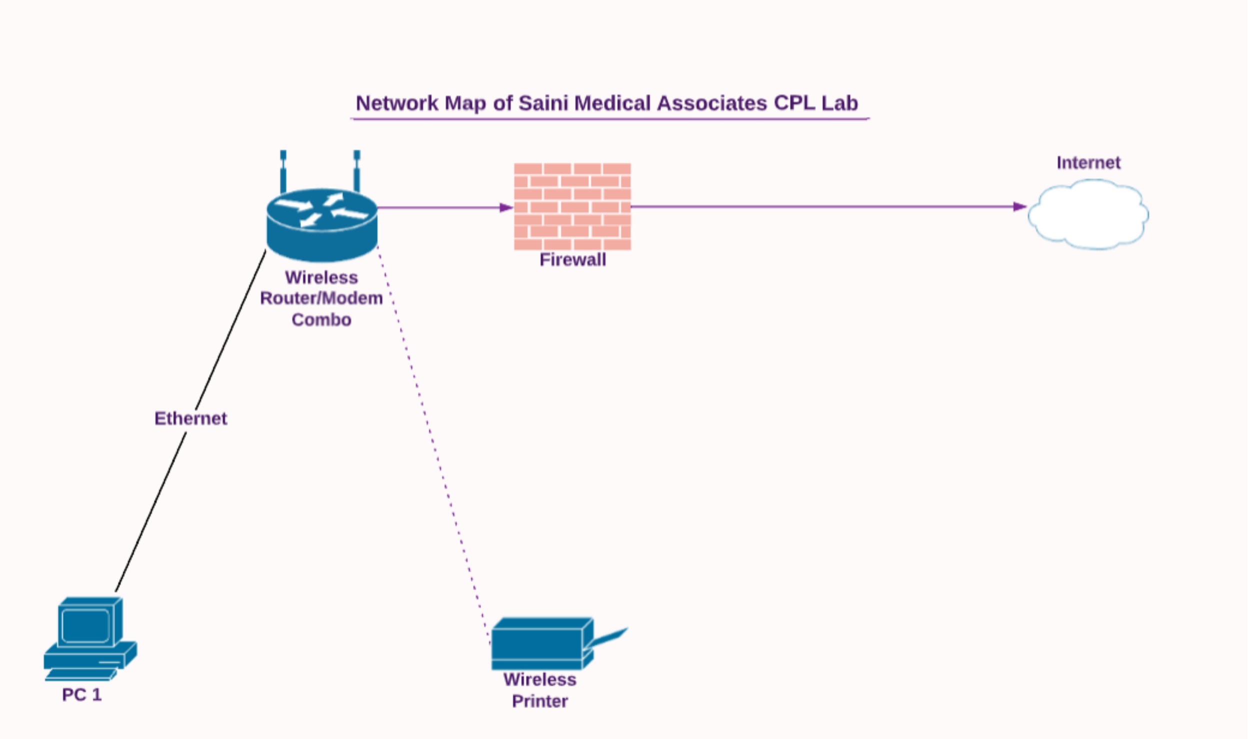
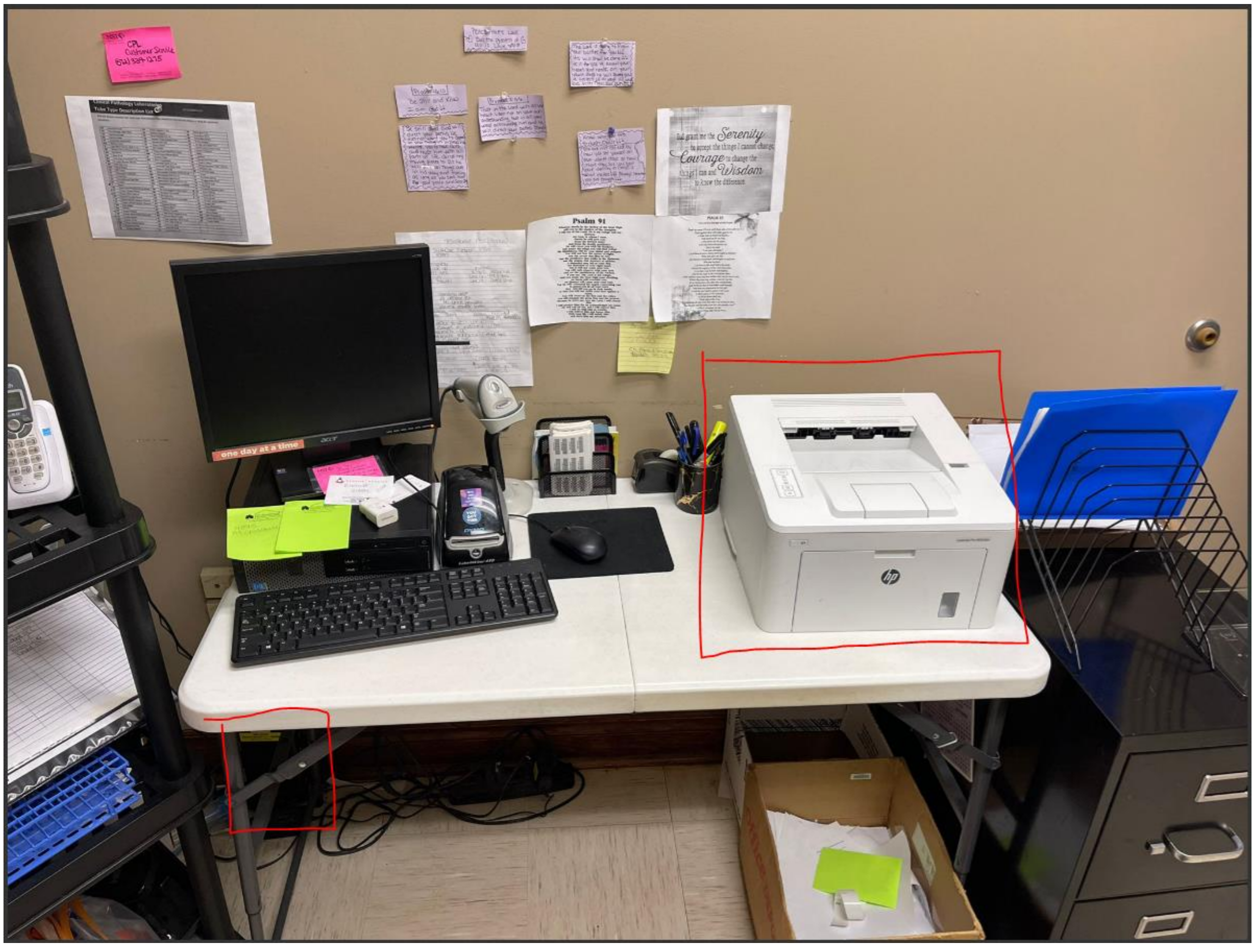

Network Map of Saini Medical Associates CPL Lab
Internet
Firewall
Wireless Router/Modem Combo
Ethernet
PC 1
Wireless Printer

Figure 3.1 B



Swot Analysis:

Strengths:

- The company is collaborating with two other research teams under Saini Medical Associates, working with two other networks, so there is no traffic using the network
- Data is maintained and stored by a third-party company, illustrating the importance of storing data.
- Using some access points in the right places to have a better network connection.

Weaknesses:

- There is no access by the medical center for data; data is stored on the portal by a third-party company named Next Gen.
- The center has old equipment, so there should be slow connections or devices with slow speed while working, causing employees to be exhausted.
- Documents in filing blocks must be scanned and added to the Next Gen portal.
- The computer in the CPL lab has a connection to the Internet by Ethernet, which means when the network is disconnected, there is no other way to connect with other networks.

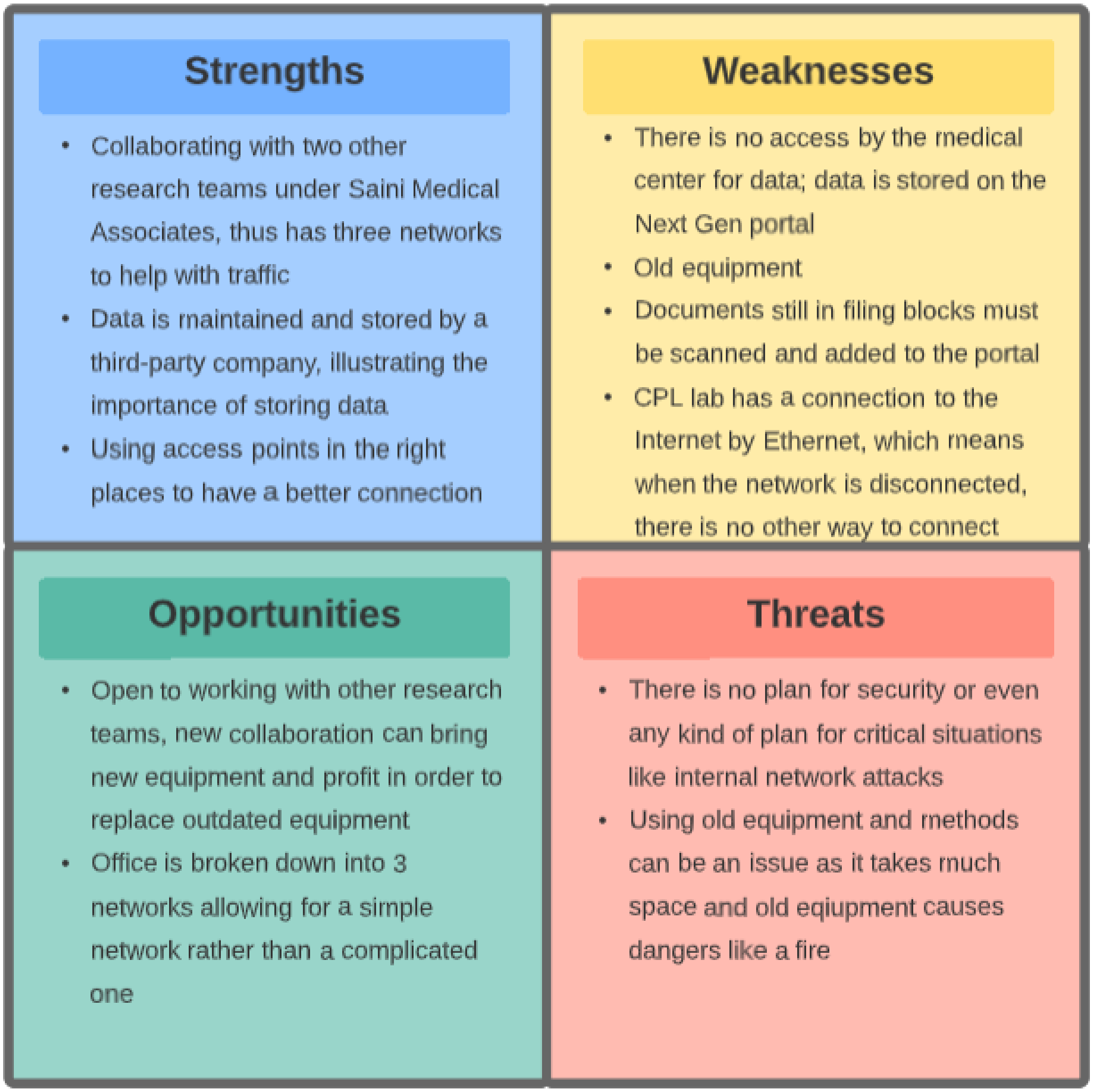
Opportunity:

- The center is open to working with other research centers; that is to say, new collaboration can bring new equipment and profit in order to replace demanded equipment.
- The office uses three different networks, assisting each section in taking advantage of a small network instead of having a big or complicated one.

Threats:

- There is no plan for security or even any kind of plan for critical situations like internal network attacks
- All used old methods and equipment can be an issue as it takes much space and causes some dangers like a fire.

Saini Medical Associates SWOT Analysis



Strengths

- Collaborating with two other research teams under Saini Medical Associates, thus has three networks to help with traffic
- Data is maintained and stored by a third-party company, illustrating the importance of storing data
- Using access points in the right places to have a better connection

Weaknesses

- There is no access by the medical center for data; data is stored on the Next Gen portal
- Old equipment
- Documents still in filing blocks must be scanned and added to the portal
- CPL lab has a connection to the Internet by Ethernet, which means when the network is disconnected, there is no other way to connect

Opportunities

- Open to working with other research teams, new collaboration can bring new equipment and profit in order to replace outdated equipment
- Office is broken down into 3 networks allowing for a simple network rather than a complicated one

Threats

- There is no plan for security or even any kind of plan for critical situations like internal network attacks
- Using old equipment and methods can be an issue as it takes much space and old eqiupment causes dangers like a fire

Problems with the Existing Network:

The existing network is working properly at the time of preparing this report as the staff agreed. However, by passing the time, patients will increase. Increase of the patients, requires more workstations and more employees. In this condition, network need update. Not only the network, but also most of the equipment that now are using by staff. The facilities are using now are outdated technology, therefore slow connections or gadgets should be used while working, and exhausting staff members. To be more specific on the equipment and the problem they might create, the next following paragraphs, precisely describe this:

The ability to connect two or more devices in a local area network (LAN) without a physical connection is made possible by a wireless local area network (WLAN). A wireless LAN with a wireless router or access point can be used to connect the printer. To do so, we must be sure the wireless router is set up with an SSID, a passcode, and security protocols before connecting the printer to a wireless network.

Fax machines are still a crucial and often used component of office technology, despite their waning popularity. Business owners and staff rely on their fax machines to send documents, whether they are working from home offices or large enterprises. Most faxed documents have several pages and transmitting multiple page documents with a fax machine only needs a few steps thanks to the standard technology included in the large majority of fax machine types.

However, the wireless helps the mobility, in compare with wired Ethernet, its speed is slower in wireless. Therefore, slow connection with the high demand on fax and printer is a big problem of this network.

Another problem with the network, is the security. Lack of backup plan is one. The other one is that there is no lock on the doors of files and documents. We will expand these problems in the following parts.

Network Limitations:

The first limitation that comes to mind is the budget of the company. As the company is small and customers are mostly local, so there is no requirement to have an expansive network. Also, purchasing cables, servers, tools, and software for maintaining data can be expensive and surpass the company's budget. In addition, the medical center possesses old equipment that cannot meet the demand of these days' technologies. To address the problem we mentioned, there are some procedures. First, it can be prioritizing the budget; if there is a high need for changing, expanding, and repairing the network, the company should consider it. Next, can be managing the budget for any expenses that can improve the network, including the detail of the project, how and who can collaborate, and so on.

Second can be the provided network service for the medical center; as the center is in a small city, there are a few network companies for collaboration, so there is no competition to access the better network connection with a better bandwidth. That is to say, whenever the company plans to change the network, they might have problems finding a good service at a reasonable price or near the center. Also, there is a probability of network disconnection especially for telephone network of the center as the number of service companies is limited, and users take advantage of the whole bandwidth. One of the conspicuous methods to address this problem is to implement two or more different network service providers in one set. This will help have a better connection between devices, hosts, and workstations; it also assists users in accessing the internet when one of the internet networks is unstable or weak. However, this may cost more than the normal cost for the network. The other method they can use is to have an extra router as an access point in different parts of the center, although this method is not able to assist the center during weak connection. It is evident that the company implemented the last method.

The following limitation is the number of devices and small space for documenting, including printers and providing suitable spaces for them and archiving documents. There are a limited number of printers in the center based on workload as the center are printing a lot; when three research centers want to use devices such as a printer, fax, and so on, employees may have to wait for some time, causing a delay in their duties. Also, regarding the budget and space, providing more devices might not be possible. If there is enough room in the budget, the obvious solution can be purchasing new appliances or cables to connect to more workstations; otherwise, users might use another approach, such as archiving data in the medical center website or application. A good illustration of that can be utilizing the paperless method for some parts of their work regarding the importance of implementing some new technology. Also, another approach can be moving documentation to a warehouse or a room or collapsing those are in online data system in order to find a bigger and enough space for printer. Documentation room would be a great place to organize printer and fax machines.

Last but not least would be the significance of maintaining data. The company works with customers who are all patients, and all their data are confidential. This means the company cannot be negligible about the significance of its data. There is a possibility that employees reveal data unintentionally or by purpose while they are working with them. That type of data is not easy to work with and leads to penalties if details do not pay some policies attention. In addition, customers should be aware of keeping their data safe to prevent a data breach. Regarding the importance of data preservation, it can be mentioned that training employees on how to work with data. Employees cannot be novices when it comes to confidential data. Furthermore, patients should be trained as well to maintain data. The other method the company implemented for customers is to have a server to store the data, which helps customers securely store their data.

Opportunities:

Saini Medical Associates has 3 different networks in the building that are owned by Avant Research Associates, CPL lab team and Saini Medical. Avant Research Associates is not part of Saini Medical Associates, they only share the building. Therefore, there is no need to share the same network for these two companies. However, the CPL lab team is part of Saini Medical Associates, and they carry sensitive information about patients' health. For that reason, they have their own network to keep the information secure and prevent data from leaking. However, since they are part of Saini Medical Associates, it would make more sense to have same network but having a subnet that does not share any information with other subnetworks to make IT management and maintenance easier and more structured. On the other hand, their current system works fine and having a totally different network provides the security they need.

Saini Medical Associates has a network containing 2 routers, along with workstations, laptops, mobile devices, and printers. One of the routers used here as an access point to make the Wi-Fi signal wider and stronger to reach all devices across the building. For now, they think their network size is enough for their workload and end point devices they have in the infrastructure. Their centralized network infrastructure is good for their system. However, if they use only wireless connection, using multiple access points would make the connection wider and therefore Wi-Fi would reach all the devices without any performance reduction.

On the other hand, having wired ethernet connection along with wireless would be a better approach for the network. Ethernet is generally faster than the wireless connection and provides reliability and security. Wi-Fi is better for mobility for devices such as laptops, smart phones, and tablets. Saini Medical Associates does not need mobility for desktop workstations and printers. Therefore, they can use a hybrid approach which includes both ethernet and Wi-Fi. Thus, they will need access points only for the mobile devices that require wireless connection. Having less devices connected to the wireless network reduces the traffic and makes the connection faster for devices that require Wi-Fi.

In the future, if they need to expand their network to add more workstations and other end devices, they might need to have additional routers and create subnets to make the network more efficient. Larger networks can run slower due to high traffic going through the network. With subnetting networks, they will have improved network security, better network performance and speed, administrative advantages, easier control of network growth and less network congestion. The network can be split to subnets depending on their department.

Therefore, no devices from one department can access other department information. For example, front desk employees should not have access to payroll services.

Network Security/Recommendations:

The company uses a portal cloud system to collect clients' information online. This portal also provides security for the company's data. The portal and the security of the portal is provided by the company Next Gen. Mr. Mike shared that they have never had an issue with the security of their data since they started using the patient portal hosted by Next Gen.

Before collecting data online, they were keeping client information on paper as we have seen in the video there is a room that has all of the client information fields. The company uploads that past information to the portal if the client visits the company again. The recommendations for these situations.

1. The field room was open as we have received in the video and there was no lock to secure those fields. This is a vulnerability of the company. The door should keep locked.
2. The company should create a management plan to upload those fields instead of waiting for the past client to visit the office again. Because there is no backup for those fields. When all of the fields are uploaded, the company will have a lot of space to use, and they will not need to worry about the security of the field. So, the recommendation for this vulnerability is fields should be uploaded as soon as possible.
3. The company has logins on their computers; however, employees do not sign out of their computers. They just leave themselves logged in until the next day. It creates a security

problem for the company. The employees should train about their security responsibilities.

4. The employees have logins for the portal and the portal signed out by itself if it goes idle for long enough and the employees should sign in again. This increases security of critical data.

As we mentioned earlier, they use a Wireless network with two routers and one of these routers is used as an access point. Let's analyze what they can do to protect their wireless network.

Router Settings:

1. They should change the SSID name, this is the id name that comes from the manufacturer. That router may have known its vulnerabilities, so the company should change the SSID name to secure our router information.
2. They should set up a new router password which should be unique and strong.
3. They should disable remote access. By doing that the company will be able to manage its access control.
4. They should create a separate guest Wi-Fi network. The client might need Wi-Fi and the company should not share the Wi-Fi that they use. That can be done by using a separate router or advanced router that has an option for what they call a guest ID.

The company uses WPA2 protocol on their router. Nowadays, there are protocol versions.

1. WEP (Wired Equivalent Privacy) is most old wireless security protocol which has 40-bit encryption key that has found by attackers. So, WEB is easy to hack by attacker.

2. WPA (Wi-Fi Protected Access) has stronger encryption methods which is called TKIP (Temporal Key Integrity Protocol). Basically, it changes the key that has been used. However, TKIP has some vulnerabilities.
3. WPA2 uses AES (Advanced Encryption Standard) which has a symmetric encryption algorithm is more secure than TKIP. Since 2006, all Wi-Fi products certified WPA2.
4. WPA3 has new features for Wi-Fi security and provides cutting-edge security protocols for companies. It also enables robust authentication, so this will increase protection from password-guessing attempts.
5. WPS (Wi-Fi Protected Setup) is the network security standard. Most of the wi-fi devices has software or WPS button to activate. There is also WPS pin option for activating the protocol.

The company can set up these protocols by going Wi-Fi security function on the Wi-Fi configuration page. Based on my searched officially certified routers and devices has WPA2 over 15 years and vulnerabilities has been found in WPA2. 15 years is fairly old enough to update version of standard. The recommendation to the company for this vulnerability is to update their protocol version as a WPA3 which was ratified in January 2019.

The company uses the firewall that is built into the main router. The company does not have a server so we can think that this built-in firewall is enough for the security of the company. However, the firewall that is built into the router will not protect the company from something on another computer on their network, for this reason, the company needs local software firewalls for each computer. In addition, each computer has the ability to log into the portal, therefore, those computers should be protected with strong passwords and employees should be trained about phishing attacks.

On both routers, DHCP is turned off. The reasons for using DHCP turned off are that they use one of the routers as an access point and they want to protect their network. So, let's explain what DHCP is and why the company was turned off the DHCP.

DHCP is a protocol that allows your computer to dynamically receive an IP address without you having manually enter any information. It does this by broadcasting requests out to the DHCP server and the DHCP server will grab an IP address out of it and assign it to you. If you turn off DHCP, you will have to manually configure each connected device and assign it an IP address. So, the Saini medical use DHCP turned off on the main router.

DHCP is considered insecure because it can be abused by attackers. There are two well-known DHCP-related attacks that is explained below:

DHCP Starvation

An attacker can constantly ask for IP addresses until there are no more IP addresses left in the pool given out. And this is going to cause a problem because now real hosts who need addresses are not able to get IP addresses and this is going to cause a denial of service.

DHCP Spoofing

When your computer is broadcasting out and asking for IP address everybody on the network can see it which means anybody can respond to it. Attackers can sit there and say hey I am the DHCP server here is the IP address and you should send all of your traffics through me, I am the gateway. This is the type of man-in-the-middle attack.

That is why the company turned off DHCP on their router and assign IP addresses manually.

As a result, my first and foremost recommendation for the company is to use a wired network. It is more secure for the company and their office has the ability to build a wired network.

Contributions:

- Executive summary: Karan
- Network Maps/Diagrams/Videos: Karan
- SWOT Analysis/Diagram: Niloofar
- Problems with the Existing Network: Yalda
- Network Limitations: Niloofar
- Opportunities: Ceren
- Recommendations/Security Overview: Ipek