UNIVERSITY OF ALBERTA

Analyzing Open-source Resources as an Alternative for Community Wireless Networks

Master of Science in Internetworking (MINT)

The Department of Computing Science

Capstone Project

MINT 709

By

Jose Alfredo Fragoso Monroy

Under the Supervision of

Dr. Mike MacGregor

Table of Contents

Table of Figures

Abstract

Community Wireless Networks (CWNs) were created to fight the broad digital divide that existed and still exists throughout many places worldwide. CWNs focus on the rural areas where communities have minimum means of communication and internet access is hard to access or where it is still inaccessible at all. Mostly volunteers from communities have been responsible for creating, maintaining, and developing new ways to make these CWNs function and provide a better service or communication source for communities to incorporate into the digital world, which would bring so many positive changes. It is a complex challenge as there can usually be many obstacles that interrupt the successful rise of this kind of network. One of the main issues encountered when working with CWNs is that the software and hardware available in the market is vendor locked. This not only causes an economic drawback when upgrading software or hardware, but it mainly makes it challenging to help improve CWNs as data is not easy to manipulate on proprietary products. This data would be very helpful when improving CWNs as it would be easier to analyze and understand what the communities require. Data analysis can indicate many statistics that can be used in favor of improvements. Another major obstacle faced within the communities that build these networks is insufficient funds to maintain and perform upgrades [2]. Nevertheless, CWNs have played an essential role in providing communication resources to many populations that have long struggled to acquire contact with the digital world and internet connectivity to their communities. Figure 1 shows a clear example of the overall process and how important it is for communities to organize and get everything ready to develop a community network. It involves organization, Internet, Network mapping, Node installations, maintenance, used devices, and planification [9].

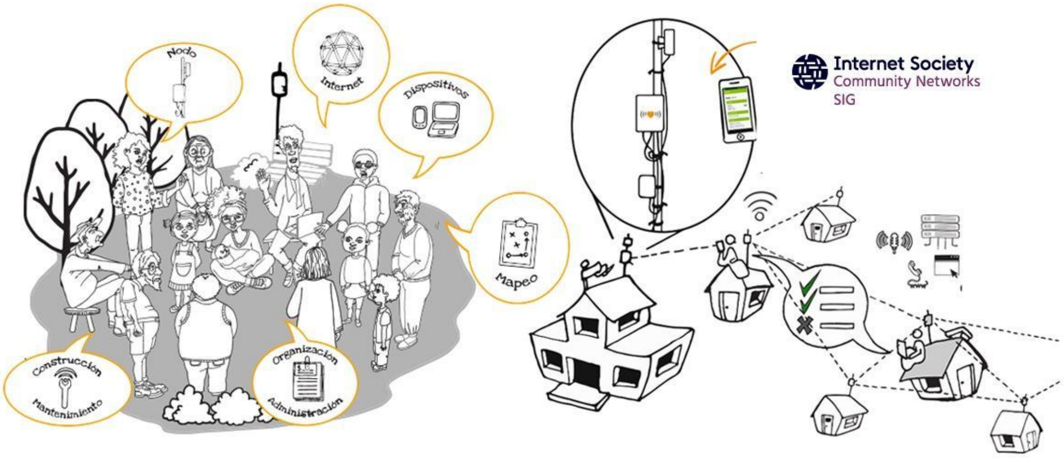


Figure 1: An overall example of how community networks work in rural areas [9]

In this capstone project, open-source software and hardware will analyze how to contribute to developing and improving current and past CWNs. An alternative option of a hybrid (open-source with vendor-locked) use of software and hardware will also be considered.

Existing open-source software and hardware will be analyzed, already used in other places as part of CWNs and different types of networks, but we will mainly focus on CWNs. For CWNs, using open-source hardware and software, when possible, will lower the costs and enable the option of modifications that cannot be done on proprietary locked products. Proprietary locked products have many unused features and can cause security issues. By opting to use open-source products, the availability of modifications is much broader and can bring many benefits when using them for CWNs.

1. Introduction and Literature

1.1 What are Community Wireless Networks (CWNs)?

The need to create and develop CWNs came from the lack of connectivity that the market and government have yet to reach and are mainly built in rural or remote areas where usually the population is low [3]. CWNs are essential to addressing this issue to reduce the digital divide. CWNs are defined as been sustainable approach that integrates the participation of different areas to build this kind of network. Mainly the same members from the communities are the ones who combine their abilities and resources to incorporate and develop this kind of network [4]. Another simple explanation of Community Networks (CNs) is as follows; Community Networks (CNs) are built by coalitions – community anchor institutions, community-based organizations, municipal representatives, and individuals work together to plan, design, and deploy these networks. Ownership and management duties are distributed among the community – often to individuals and organizations volunteering their time and expertise" [5].

Some interesting facts and statistics about CWNs in Canada are population coverage. According to the Canadian Radio-television and Telecommunications Commission (CRTC), approximately 17% of Canadians do not have access to the internet at home, with the highest rates of non-adoption occurring in rural and remote areas [18]. In recent years the Canadian government has made millions of dollars available for funding to support the development of community wireless networks in rural and remote areas. Internet usage, according to the CRTC, in 2019, approximately 86% of Canadians aged 16 and overused the internet, up from 82% in 2016 [18]. Rural access in rural areas approximately 64% of households have access to broadband internet, compared to nearly 95% of households in urban areas. Wireless adoption, according to the CRTC, in 2019, approximately 74% of Canadians aged 16 and overused a wireless device to access the internet, up from 68% in 2016 [18]. Community involvement in many communities across Canada, local volunteers, and organizations have come together to build and operate community wireless networks to provide internet access to those in need.

1.2 How do Community Wireless Networks (CWNs) operate?

When it comes to seeing how CWNs operate or work, the following description is one powerful way of describing them. Wireless community networks utilize two-way radios that operate on an unregulated portion of the telecommunications spectrum to provide internet access over the airwaves instead of landlines. They organize geographically to serve a specific neighborhood or community to improve their quality of life. These networks comprise many individuals linked in a complex web, offering flexibility to accommodate changing demands for bandwidth and adaptability to address any issues that may arise [6].

Nowadays, there are more existing CWNs that operate similarly and that have adopted new technologies. Some have slight differences, but the root idea is the same. One thing that all have in common is that the main impact must be in rural areas where there is still no internet access to the individuals within the communities or the lack of high speed in the existing CWNs. Community wireless networks in remote rural areas leverage various technologies and infrastructure to provide internet access to local residents. These networks are often community-led, with volunteers and community organizations working together to build, operate, and maintain the infrastructure. CWNs typically use a combination of fixed wireless access, satellite, and other technologies to connect residents to the internet. Fixed wireless access involves transmitting internet signals wirelessly from a fixed point, such as a tower or building, to a receiver at the user's location. Satellite technology sends and receives data via a satellite orbiting the earth.

Community wireless networks often use a mesh network architecture, enabling devices to communicate to extend the network's reach. Mesh networks can be particularly useful in remote areas with limited infrastructure, as they cover a large area with relatively few physical nodes. Mesh networks are a type of wireless network that is self-organizing and self-healing, making them well-suited to large geographic areas and environments where traditional wired networks may not be feasible or cost-effective. As per a report published by Research and Markets, the global mesh network market was valued at $6.9 billion in 2021, and it projects to reach $12.7 billion by 2026, growing at a compound annual growth rate (CAGR) of 13% [19].

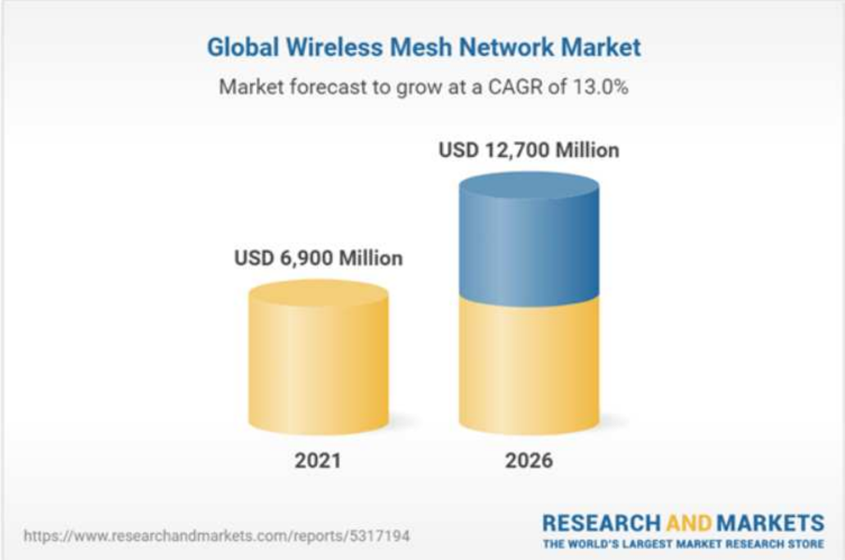


Figure 2: Global Wireless Mesh Network Market Values and CAGR [19]

The Wireless Internet Service Providers Association (WISPA) estimates that over 40% of fixed wireless networks in the United States use mesh technology to provide internet access to customers [20]. Ubiquiti, a networking company, estimates that its mesh network products have been used to deploy over 80,000 wireless networks worldwide [21]. Mesh networks have been used for various applications, including community wireless networks, disaster response, and public safety communications. In one study, researchers found that a mesh network deployed in a rural community in Nigeria could provide reliable connectivity to residents and local businesses, with an average throughput of 1.5 Mbps and a range of up to 8 km [22]. A mesh network was also used to provide emergency communications to residents and aid organizations in Puerto Rico following Hurricane Maria in 2017. The network comprised over 50 nodes and provided internet access to over 8,000 people [23]. To support the operation of these networks, community organizations often work with local businesses and individuals to secure funding and donations of equipment and other resources. They may also partner with local Internet Service Providers (ISPs) to obtain internet connectivity and leverage their technical expertise. In addition to providing internet access, community wireless networks may offer additional services and benefits to residents, such as digital literacy training, online services and resources, and support for local businesses and community organizations. Overall, community wireless networks in remote rural areas rely on the collaboration and support of residents and organizations to build and maintain the infrastructure necessary to provide internet access to those who may otherwise be underserved or unserved by traditional ISPs. As mentioned before, CWNs are mainly operated by community volunteers, which have a significant role in the operation process. Volunteers place nodes at their homes (roofs) and are configured by them [6]. Figure 3 displays a simple example of the nodes used by the "Libre Router" project, mainly placed on the house rooftops [1].

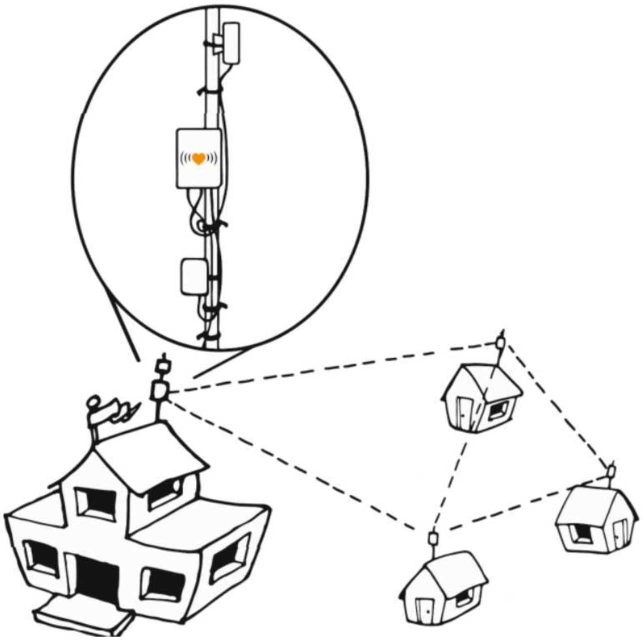


Figure 3: Nodes placed on house rooftops (Libre Router) [1]

Another example to display the high-level operation of a community network is deployed by Wakoma with their nimble project device. This is an example of a wireless mesh network whose primary focus is to connect offline first to be able to video and voice chat, stream videos, share files, build and run eLearning courses and websites, create collaborative spreadsheets and documents, read e-books, play games and many other valuable resources activities for the communities to take advantage of [24].

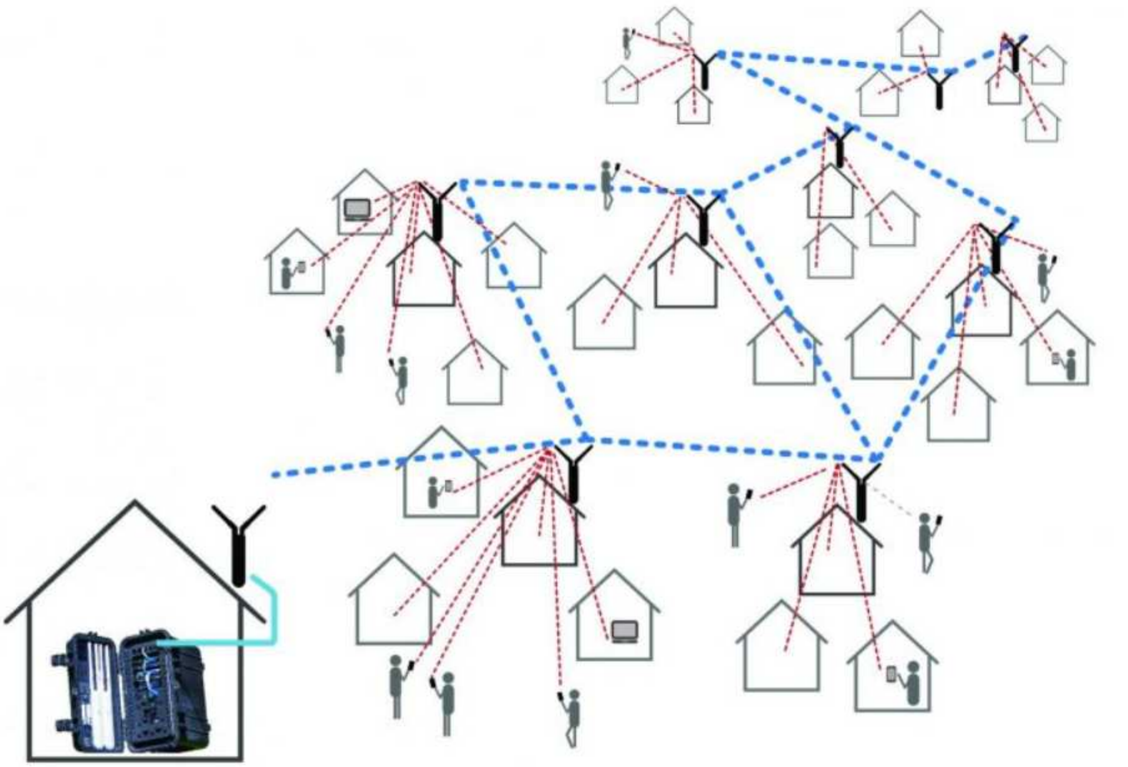


Figure 4: Nimble project operated in a wireless mesh network [24]

1.3 Places where Community Wireless Networks (CNWs) Are Used

CWNs nowadays exist everywhere in the world, but this project focuses on rural areas such as small villages, indigenous lands, and any other place where internet connectivity or intranet is hard to establish or needs improvement. In Canada, many rural areas are yet to overcome the digital divide. Still, with many projects from volunteers from within the communities and help from the government, this issue is becoming addressed, and the connectivity of CWNs is now very common. CWNs in Canada refer to decentralized networks of wireless access points owned, operated, and maintained by local communities. These networks are designed to provide internet access or an intranet to communities in rural and remote areas where commercial broadband services may not be available or in urban areas where the cost of commercial broadband is prohibitively high.

CWNs have gained popularity in Canada over the past few years as many communities strive to bridge the digital gap and enhance internet accessibility. The Canadian

government has supported these efforts and provided funding and other resources to help communities establish and operate CWNs. One of the key benefits of CWNs in Canada is their ability to provide fast and reliable internet access at an affordable cost. These networks can offer speeds comparable to commercial broadband services and often provide faster speeds than those from commercial providers in rural and remote areas. Community wireless networks have been implemented in various locations worldwide, particularly in areas where traditional internet infrastructure is unavailable or insufficient. For example, the Zenzeleni Networks project in South Africa has connected over 1,600 people to the internet since its inception in 2012 using a combination of mesh networks and solar-powered base stations [25].

In India, the Digital Empowerment Foundation has helped to establish community wireless networks in several rural villages, with the network in Sothi providing internet access to over 1,000 people [26]. In the United States, community wireless networks have been established in cities such as Detroit, New York City, and San Francisco. The Equitable Internet Initiative in Detroit provides high-speed internet access to underserved communities.

Projects around the world for building CWNs have been very successful. In South Africa, Mamaila is the story of a young student that became the CEO of a foundation that helped create a community network for her village by using her money resources and going from never even touching a computer to self-teaching about web development and other skills that helped her gain the knowledge to help her village [2].

Figure 5: “Kgopotso Magoro, founder of the Mamaila Community Network, with grade 11 students at Mathibadifate Secondary School in Mamaila in the Limpopo province of South Africa” [2].

As we can see, community networks are primarily needed in remote rural areas where it’s hard for big telecommunications companies to invest in expanding their infrastructure to these areas. In the northern parts of Canada, especially in the indigenous communities, the Internet Society and the National Research Council of Canada have teamed up to help create community networks for the indigenous habitants of those regions [7]. “Starting in November 2022, 10 Indigenous communities in Ontario and Northwest Territories attended training sessions, which will run until February 2023. Once complete, training materials and recordings will be publicly available to support other communities interested in building Internet infrastructure” [7].

1.4 Drawbacks faced in Community Wireless Networks (CWNs)

Once CWNs are set and established, drawbacks and challenges still need to be addressed. Establishing CWNs cannot be done from one day to another; it takes many different variables and efforts to accomplish them. Since CWNs are mainly built by community volunteers, insufficient funds will eventually catch up to the projects at specific development points or even when maintaining and upgrading them when they are already established. According to a survey conducted by the Electronic Frontier Foundation (EFF) in 2018, which included responses from 15 community wireless networks in the United States, lack of funding was one of the top challenges faced by these networks. 40% of the networks reported that funding was a significant challenge, with one respondent stating that "keeping the network alive and growing" was their biggest challenge [27]. Another factor of CWNs is that they seem like a risk for being in places unknown to many organizations. CWNs cannot guarantee a loan and need land [8]. There is also the part of choosing which hardware and software to use or making upgrades, as funds also influence here; usually, the most common hardware and software used is vendor locked with intellectual property. When using proprietary locked products, it usually means that their hardware and software are locked or limited to any modifications. Using proprietary vendor-locked hardware and software is a significant drawback for community wireless networks. This approach can limit the affordability and accessibility of community wireless networks, particularly in economically disadvantaged areas, as proprietary solutions can be expensive and less customizable. Furthermore, proprietary hardware and software can be challenging to troubleshoot and repair, leading to increased downtime, maintenance costs, and reduced network performance and reliability. Additionally, proprietary solutions can limit the ability of community wireless networks to interoperate with other networks and services, potentially creating information silos and reducing the reach and impact of the networks. In contrast, open-source hardware and software, and open standards and protocols, can provide more affordable, flexible, and interoperable alternatives that better support the needs and goals of community wireless networks. Therefore, community wireless networks must consider the drawbacks of proprietary solutions and explore alternative options that align with their goals and values. Another significant drawback of using proprietary vendor-locked hardware and software in community wireless networks is the lack of access to data. Proprietary hardware and software can make accessing and controlling data challenging, particularly since access to the underlying code and technical documentation is often restricted. This can create data silos and limit the ability of community wireless network operators to analyze and optimize their networks. In contrast, open-source hardware and software provide more transparent and accessible data management and analysis options, enabling community network operators to identify and address issues more quickly and effectively. Therefore, community wireless networks should prioritize using open-source hardware and software and open standards and protocols to maximize their potential and ensure that data is accessible and actionable.

A great example of the drawback in extracting data from networking devices is the UniFi systems. The UniFi hardware, manufactured by Ubiquiti Networks, is a range of wireless networking equipment, including access points, switches, routers, and other devices used in various networking environments. However, the hardware is proprietary and locked down, making it difficult for users to extract data from the devices. This could be a problem for community networks, often built and maintained by volunteers and community members who may need more technical skills or resources to work with proprietary hardware. Extracting data from the UniFi hardware would help improve community networks, including monitoring network performance and optimizing network configurations. Extracting data from UniFi networking devices can be challenging for various reasons. Firstly, by default, UniFi devices provide limited access to data through their user interface, which means that accessing all the required data may require additional steps. Secondly, UniFi devices are designed to be used in complex network environments, making extracting the correct data difficult. For example, if multiple UniFi devices exist in a network, data must be collected from each device and aggregated to get a complete picture of the network. Thirdly, UniFi devices do not have standard APIs, making it challenging to extract data. Even with third-party tools, data extraction may not be possible or require significant configuration and technical expertise. To extract detailed network statistics from an UniFi access point, one may need to enable advanced features, configure it to log required data, and use third-party tools to extract the data and combine it with data from other devices in the network. This process can be time-consuming and require significant technical expertise, making it challenging for non-experts to extract data from UniFi networking devices. According to several reports, vendor lock-in is a considerable challenge for many organizations when managing their IT infrastructure.

A Spiceworks survey found that 45% of organizations cited vendor lock-in as a critical challenge [28]. An EMA Research survey found that 69% of IT professionals viewed vendor lock-in as a barrier to adopting new network technologies [29]. Proprietary network devices can also be challenging to integrate with other systems, with 61% of EMA Research survey respondents reporting difficulties [29]. Additionally, a report by the Open Networking User Group (ONUG) found that vendor lock-in can lead to up to 80% higher costs for network infrastructure over a 5-year period compared to open, interoperable solutions [30]. A study by Forrester Research also found that vendor lock-in can limit the ability to negotiate better pricing and terms with vendors, making it more difficult to secure favorable contract terms [31]. These statistics underscore the importance of selecting network devices that promote interoperability, cost-effectiveness, and innovation and highlight the need for organizations to carefully consider the potential drawbacks of vendor lock-in when making purchasing decisions.

1.5 Common Hardware and Software Used

In Community Wireless Networks (CWNs), there can be many ways of building the networks, and configurations will also vary depending on the requirements. The hardware and software used also vary on the type of network and where it is deployed. The focus will be on hardware and software used in remote, rural areas. Mainly when it comes to

hardware, it is composed of but not limited to the following devices: servers, routers, switches, firewalls, access points, antennas (send and receive signal), RF cables, power banks, etc. Figure 4 shows the hardware components " LibreRouter " uses when deploying CWNs. The main components are one LibreRouter node, two 5GHz sector antennas, and four RF cables (two per 5GHz antenna) [10].

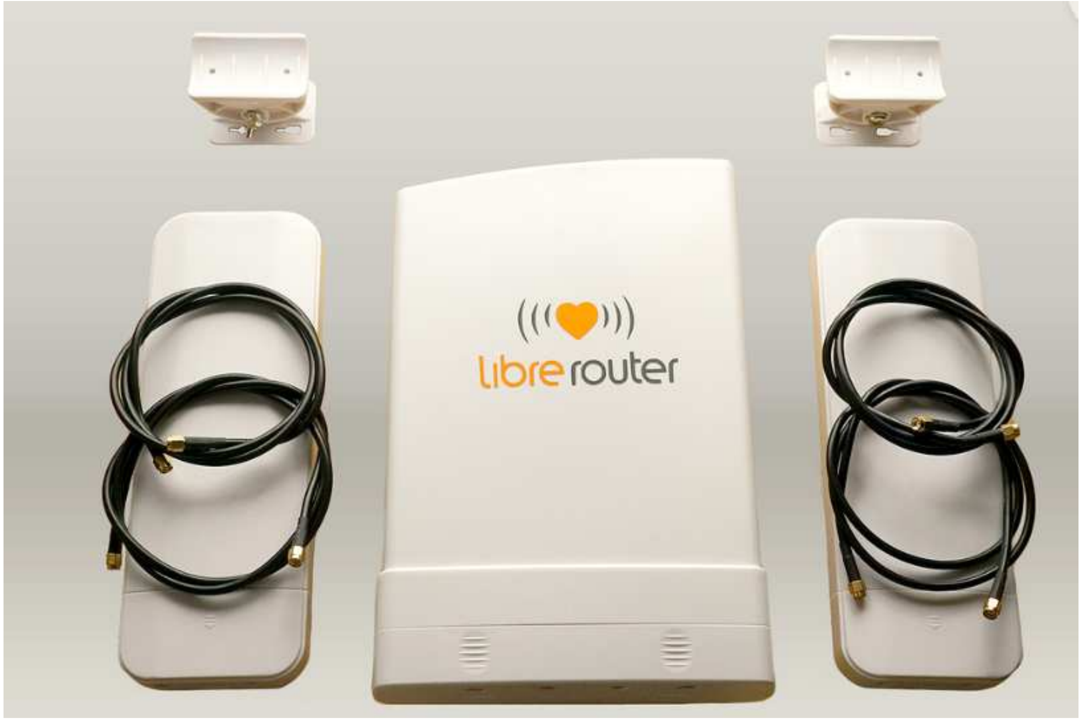


Figure 6: Main components used by LibreRouter for Community Wireless Networks [10].

Another example of the main components used by Wakoma to implement the Nimble device for community wireless networks are a router/firewall, switch, access points, server, and power bank. In Figure 7, all of the components that make up the nimble are integrated into a rack that was 3D printed.

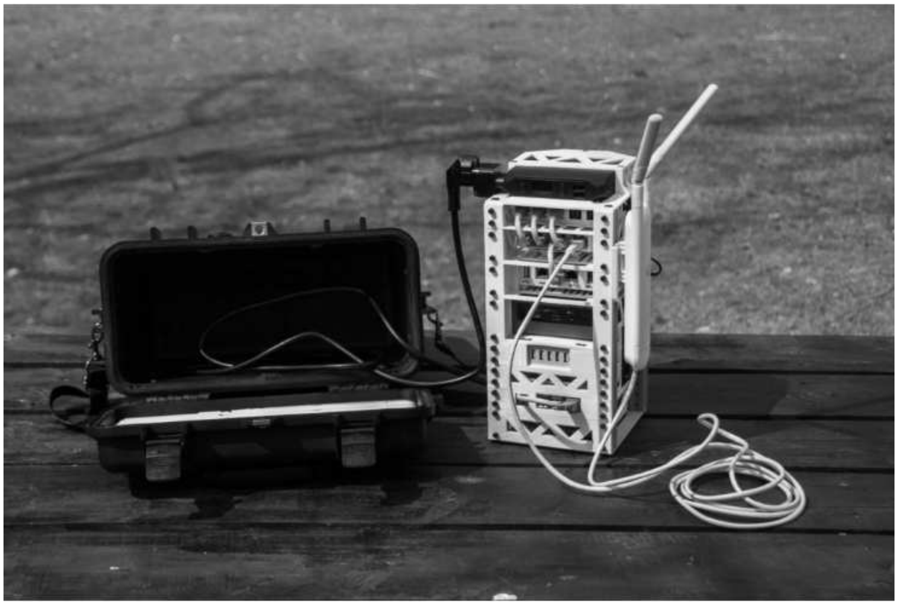


Figure 7: All of the components integrated that make up the Nimble [24]

1.6 Data Analysis

When Community Wireless Networks (CWNs) are finally up and running, it becomes a great accomplishment to all individuals who contributed to the project and the whole community who will take advantage of all the positive attributions this will enable them. As community members use their CWNs, at some point, issues may interfere with their proper function, or even if there are non-noticeable issues, things can be done to improve CWNs. One of the most important parts of monitoring a network is network analytics. Network analytics refers to the process of gathering and evaluating network data with the aim of enhancing network performance, reliability, visibility, or security [11]. A network analysis operates by collecting data from various sources such as network devices (such as routers, switches, access points, and wireless devices), servers (including Syslog, DHCP, AAA, configuration databases, etc.), and traffic-flow details (such as wireless congestion, data speeds, and latency). Network analytics can scale up to accommodate many devices, clients, users, and applications, aiming to improve the overall user experience without significantly increasing operating costs [11]. Network analytics offer several benefits, including solid visibility into leads and insights that can help identify bottlenecks, assess device health, conduct root-cause analysis, remediate issues, identify connected endpoints, and detect potential security gaps. [11]. The data collected from networks that will be analyzed does not easily come into one's hands. Most of the time, some network traffic and data analysis tool is required to obtain accurate data and have positive results. Nowadays, monitoring a network is crucial to improving network performance, gathering data for valuable insights and feedback, improving the overall network infrastructure if required changes, and security, to mention a few of the essential tasks of monitoring a network.

A network management system is one of the best ways to monitor networks and collect data that will be useful to improve the performance of such networks. The process of setting up, overseeing, and enhancing the performance of a network is referred to as network management [12]. Network management systems have advanced to assist IT teams in functioning with greater agility, integrating sophisticated analytics, machine learning, and intelligent automation to continuously fine-tune network performance [12]. Network management systems gather information from network devices like access points, routers, switches, and client devices and also offer administrators precise management of device behavior and interactions. The data obtained from these devices are employed to detect performance problems in advance, oversee security and division, and hasten the process of fixing issues [12].

According to a study by SolarWinds, 61% of IT professionals said network monitoring tools were an essential part of their toolkit for troubleshooting performance issues [13]. Another study by Gartner found that using network management systems can reduce network downtime by up to 80% [14]. Network management systems can also help improve network security by providing real-time threat detection and response capabilities. A study by Cisco found that 95% of companies that experienced a data breach needed a comprehensive network visibility and control system in place [15]. The implementation of network management systems can also help reduce operational costs. A study by the Ponemon Institute it was discovered that the cost of a data center outage, on average, was $740,000, while the average cost of network downtime was $5,600 per minute [16]. Network management systems can help optimize network performance by identifying and resolving bottlenecks, reducing network congestion, and optimizing network traffic. A study by IDC found that companies implementing network optimization technologies saw a 30-40% improvement in network performance [17]. Network management systems are essential to improve network performance, reduce downtime, enhance security, and optimize operational costs.

1.7 A Fortuitous Connection

This Capstone project has unleashed or unblocked a very particular memory of a self-build project I worked on around the year 2012. A bit of the backstory is when I was pursuing my bachelor's degree in my home country of Mexico. I lived in a small city called Pachuca in Hidalgo (about 90 minutes northeast of Mexico City). I was in the computer science program, which also focused on computer networks. Even when I lived in a city, some parts were still under development, and they would decay telecommunications infrastructure. Internet service providers (ISPs) were still working on trying to extend their infrastructure to those areas. Of course, they would prioritize areas with higher populations that would guarantee positive gains for their investment. For those areas, there were internet services, but it would be mainly serviced with point-to-point wireless connections. As Pachuca is a small city surrounded by big mountains, small wireless internet service providers would install their access points on the best-located mountains with point-to-point views, covering a great amount of area, especially in the more rural-urban areas mentioned earlier. The download speeds were incredibly low, and the price was too high for what was offered.

A visit to a classmate that lived a few kilometers away from my house was the step of a great idea that, without knowing at the moment, was my first interaction with creating a Community wireless network or a similar type of network. My classmate lived in a more developed area where infrastructures of ISPs were already there and provided high-speed internet connections. As we had taken a few courses related to computer networks, we decided to investigate if he could share his connection. Research of available networking devices needed to establish the planned connection led to acquiring some devices we needed and using some we already possessed. We used a Linksys router WRT54G, a USB Alfa network adapter AWUS036H, an Alfa R36 router/extender, a 10-meter coax cable for antennas with n female connectors and WLAN USB Adapter, and a TP-link unidirectional grid antenna for long distances. Those were the main hardware components to deploy the connection between our houses. Figure 8 displays the overall first attempt at accessing my classmate's Wi-Fi connection over a 4km distance approximately. The TP-Link Unidirectional antenna was mounted on top of my house. It was a high-gain antenna; we could establish the connection over a long distance as long as no major obstruction objects were in the way. The TP-Link antenna was connected to the Alfa network adapter with a coax cable, and the Alfa R36 router extender would connect to the Alfa network adapter via USB. The Alfa R36 provided a Wi-Fi connection for wireless devices and a LAN ethernet port. We manage to establish a successful connection with a low gain-loss.

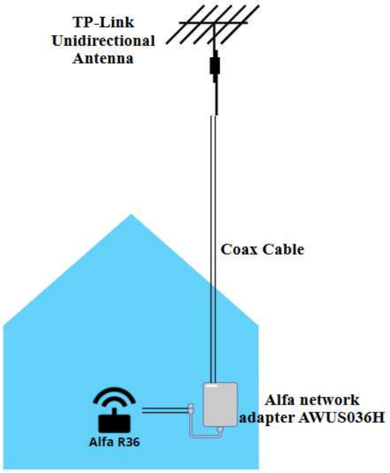


Figure 8: Our Network Diagram

This was the beginning of many ideas that started coming to my mind as many neighbors were going through the same issues as I was, some did not have an internet connection, and others had very poor services.

1.8 Expansion of Ideas

As I was getting my feet wet into the computer networking technologies, and with the current needs that the digital divide exposed. I started to work on the way to help as many neighbors as I could. A very good idea, but simultaneously very limited, was sharing the Alfas' router extender internet connection to another router via a direct ethernet cable connection. A 15-meter ethernet cable was used to install another router in the neighbor's house by configuring the router to be part of the original router’s network. Although it was a great idea, and the connection worked great, it had some limitations. The 15-meter ethernet cable caused a loss of signal. Only users within the neighbors’ house would benefit from this, and as the number of users increased, the bandwidth was reduced and caused performance issues. I knew that the idea of connecting more users was going to take more than just a simple sharing wired connection method. I did some further research for devices that would help expand the network. After a chat with my classmate, he was willing to share his high-speed internet connection so that we could experiment further. My hometown university lent us four TP-link access points which we installed on four houses. After watching a few tutorials online, we created a mesh network without realizing we did. It was only an experiment, and it worked well, sadly, to get more resources such as routers, access points, antennas, network adapters, and accessories was way out of our hands as help was not offered for us to continue this experiment and help out the community as we wanted. We tried a similar experiment on a small remote rural village where my grandparents live, about 1 hour from my home. A successful connection was established with several community members. However, unfortunately, due to insufficient funds, more devices such as routers, access points, high-gain antennas, and more could not be acquired. Networking technology knowledge also played a big factor as it was not enough at that time, we were in our early years of college, and many things were new.

Although our experiments had many great ideas, sometimes things might not go as planned. Many great things were learned, and without knowing it, we were trying to build a community network and got our feet wet with some networking technologies. This capstone project focuses on a problem related to an experience in the past, as we encountered the hardships of using proprietary vendor-locked hardware, which was expensive and not so flexible. I can fully understand how exhausting it is to improve the performance and set up this kind of network, as many variables can be great factors in accomplishing tasks such as data extraction for analysis.

2. Open-Source Hardware and Software as a Solution

2.1 Proprietary Hardware and Software

Proprietary vendor-locked software and hardware can be a drawback for community wireless networks because it limits the ability of the community to modify, customize, and maintain the network. This can make it difficult for the community to fully own and control its infrastructure. Vendor-locked software and hardware often have restrictive licenses that prevent users from modifying or distributing the software. This can make it difficult for the community to fix bugs, add new features, or adapt the network to their changing needs. The community may also be limited to using only the vendor's proprietary tools to manage and monitor the network rather than being able to use open-source alternatives. Vendor-locked hardware can also pose a problem because it can be difficult and expensive to obtain replacement parts or repair the hardware if it fails. This can lead to extended downtime and increased costs for the community, making it difficult for the community to fully own and control its network infrastructure.

2.1.1 High Costs

As per my experience, one of the most significant disadvantages of using proprietary vendor-locked software and hardware is the higher costs involved. Proprietary products are often priced at a premium because of insufficient competition in the market. Users are usually required to pay licensing fees, upgrades, and maintenance, which can add to significant expenses over time. This can be incredibly challenging for community wireless networks or individuals who may need more money to support these ongoing costs. Additionally, proprietary software and hardware often come with strict usage limitations, which can require additional licenses or fees for each additional user or device. These high costs can limit access to critical tools and technologies. In some cases, users may choose between limiting their access to critical technologies or paying high fees to maintain access. High costs can also limit competition and innovation in the market, as new players may need help to compete with established vendors who have locked in customers with high switching costs. In the long run, this can result in a lack of diversity and innovation in the industry, limiting users' ability to access and benefit from emerging technologies. This limits the communities that are trying to expand or set up new networks in remote rural areas.

2.1.2 Lack of Flexibility

Although proprietary vendor-locked software and hardware provide reliable performance, advanced features, and customer support, they come with significant disadvantages, including a lack of flexibility. Since proprietary solutions are exclusively designed to work with a vendor's products, integrating them with other systems or switching to another vendor is difficult. This inflexibility restricts a company's ability to adapt to changing business needs and emerging technologies, leading to vendor lock-in and higher costs. IT teams' ability to customize or optimize their systems for specific use cases or requirements is limited to proprietary vendor-locked solutions. Users are confined to the vendor's features and functionality with minimal ability to modify or extend the system beyond the vendor's capabilities. This restriction can cause problems in rapidly changing industries or environments with frequent emerging technologies or business requirements. The use of the Alfa network products previously mentioned in this capstone project forced us to struggle in some aspects. For example, many alfa network adapters’ chipsets are incompatible with the Alfa R36 router extender. As we tried to use different network adapters from different vendors, the chipset required was not very common and made it very difficult to be compatible with the Alfa R36. At last, the Alfa network adapter AWUS036H was compatible, and we could proceed with our tests.

2.1.3 **Dependence on Vendor**

Dependence on vendors for proprietary vendor-locked software and hardware is a significant challenge for many organizations. Such solutions offer many advantages, including reliable performance, advanced features, and customer support. However, this reliance on a single vendor creates significant vendor lock-in, limiting the organization's ability to adapt to changing business needs and emerging technologies. The lack of flexibility in proprietary solutions can make it challenging to integrate with other systems, and switching to a different vendor can be costly and time-consuming. Additionally, the dependence on the vendor for customization, updates, and support can create significant challenges for IT teams, including reduced control over systems and limited access to underlying data. This can also make troubleshooting and resolving issues challenging, as the organization relies on the vendor for support [57]. While proprietary vendor-locked software and hardware may offer some benefits, dependence on a single vendor can create significant challenges. Depending on a single vendor did not work well for us, and we had to integrate the use of different networking technology brands such as Cisco, TP-Link, and Alfa Networks. Some vendors provide more technical support than others, and some require special skills and knowledge to understand technical configurations.

2.1.4 Security Risks

Proprietary vendor-locked software and hardware can pose significant security risks. Because the vendor has complete control over the software and hardware, it is difficult for users to assess the system's security or make changes to improve it. Moreover, the closed nature of proprietary systems can make it challenging for security researchers to identify and report vulnerabilities that attackers could exploit.

In addition, because vendor-locked systems are designed to work exclusively with the vendor's products, it can be challenging to integrate them with third-party security tools or to implement industry-standard security protocols [57]. This can leave organizations vulnerable to cyber-attacks, data breaches, and other security incidents. Furthermore, vendor lock-in can make it difficult for organizations to switch to more secure solutions, even if security issues are identified, as they are tied to the vendor's products and support. Therefore, one should carefully consider the security risks of vendor-locked solutions and weigh the benefits against potential security threats.

2.1.5 Data Inaccessibility

Proprietary vendor-locked software and hardware can pose significant challenges to accessing and managing critical data. Since proprietary solutions are designed to work exclusively with the vendor's products, it may be challenging to integrate them with other systems or tools that an organization relies on for data management. Additionally, proprietary solutions may use proprietary file formats or databases that can limit access to the data by other software tools or applications. This can result in data silos and make it difficult to share information across the organization. Furthermore, vendor lock-in can result in high costs for accessing and exporting data from proprietary systems, which can be problematic when the organization wants to migrate to a different solution or vendor. These challenges can be tough in environments where data is critical, such as healthcare, finance, or government, where regulations may require access to data for compliance or audit purposes.

2.2 Solution

Open-source hardware and software can offer a solution for community wireless networks by providing transparent and accessible technology that is flexible and customizable to meet community-specific needs. Open-source hardware, such as routers and access points, allows communities to build and maintain their wireless networks without incurring large upfront costs or ongoing expenses associated with proprietary networking hardware. One of the main benefits of using open-source hardware is the flexibility it offers. Open-source hardware can be customized and modified to meet the specific needs of a community. In addition, it can be configured to work with a wide range of software and applications, making it easier for communities to manage and monitor their networks. The hardware used in successful projects, such as the “LibreRouter” and the “Nimble,” can easily be implemented in many existing or new community wireless networks. Depending on the situation or requirements that best fit these technologies and ideas, some modifications might be possible. I honestly believe that a hybrid implementation of both technologies used in both projects, with the addition of Artificial Intelligence (AI), can have a very positive and incredible outcome.

Moreover, open-source software like Prometheus, Grafana, Unifi Poller, OpenWisp, and Zeek can extract data, help with network monitoring and management, and make it more straightforward to configure and manage community wireless networks. By using open-source hardware and software, community wireless networks can benefit from the great features of data extraction and network monitoring for better data analysis, improving CWNs. Additionally, it will provide a more cost-effective and accessible solution, especially for communities that lack access to reliable, high-speed internet connections or cannot afford expensive proprietary networking hardware and software.

2.3 Open-Source Hardware

Deploying community wireless networks using open-source hardware is a growing trend in the world of wireless networking. Open-source hardware, such as routers and access points, allows communities to build and maintain their wireless networks using transparent and accessible technology. This is especially beneficial for communities that need access to reliable, high-speed internet connections or need help to afford expensive proprietary networking hardware. One of the main benefits of using open-source hardware for community wireless networks is its flexibility. Open-source hardware can be customized and modified to meet the specific needs of a community. For example, hardware can be designed to work in extreme weather conditions or to be energy-efficient in areas with limited power supplies. In addition, open-source hardware can be configured to work with a wide range of software and applications, making it easier for communities to manage and monitor their networks. Another advantage of using open-source hardware for community wireless networks is the lower cost. Proprietary networking hardware can be expensive and require ongoing licensing or maintenance fees. Open-source hardware is often more affordable, and may need only basic technical skills to assemble and configure. This means communities can build and maintain their wireless networks without incurring high upfront costs or ongoing expenses. The lack of knowledge in networking and open-source tools played a big role when I first encountered the challenge of providing an internet connection to a community. I have a great interest in contributing to my hometown community or any community worldwide with the knowledge I've been acquiring over the years with my Internetworking master's degree and many valuable learnings and lessons from this capstone project.

2.3.1 LibreRouter

A great project that was developed with open-source hardware is the LibreRouter project. An open-source hardware and software initiative aims to provide a flexible and customizable solution for community wireless networks [32]. The hardware used in the project is based on the Atheros AR9331 chipset, which is widely used in networking hardware and is well-supported by open-source software. The LibreRouter hardware includes two radios, which can operate on different frequency bands, Ethernet ports, and a USB port for additional connectivity options. Users can customize the router's functionality by adding or removing modules as required, thanks to its modular design [33]. For example, users can add additional radios to support more frequency bands or increase the range of the network. The LibreRouter hardware is designed to be easily configurable and manageable by users with basic technical skills. The software is based on OpenWRT, a popular open-source router operating system, and includes a range of tools for configuring and monitoring the network. The software is also designed to be flexible and can be customized for community requirements [34]. Figure 9 shows some of the main components of the LibreRouter that are put together and configured before it’s deployed.

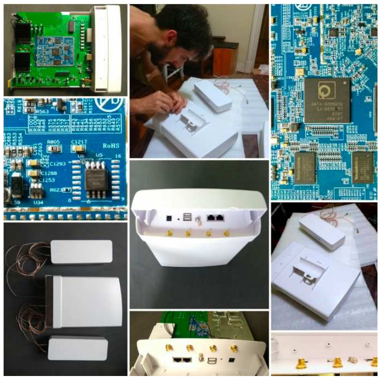
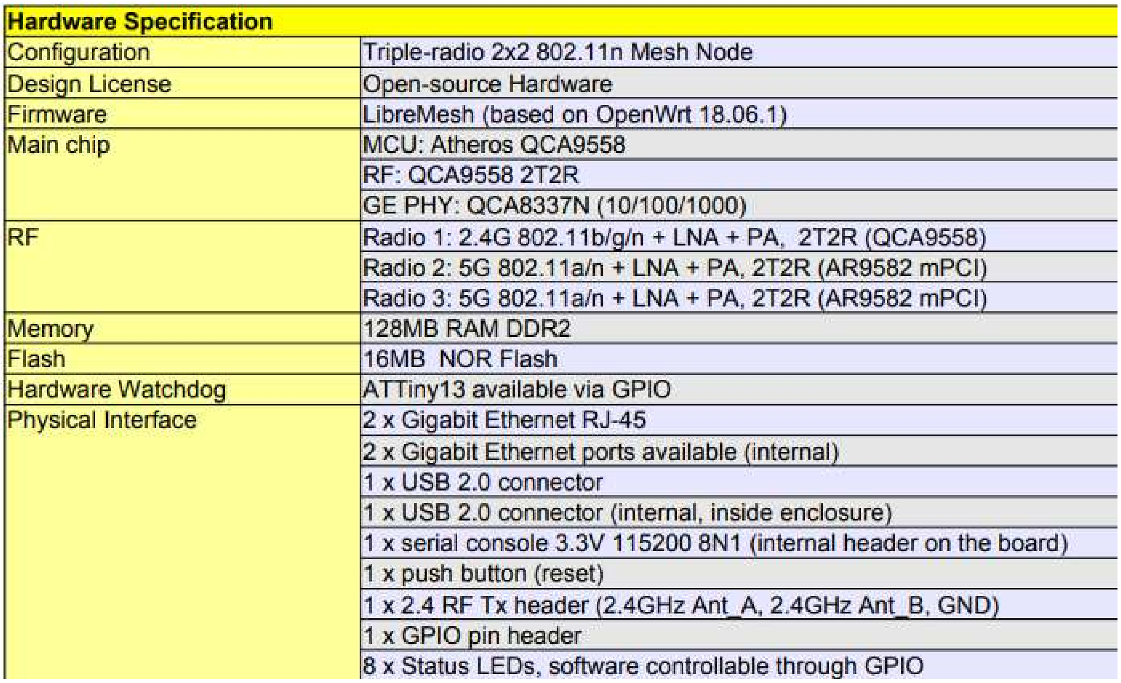


Figure 9: The LibreRouter board components [35]

In Figure 10, the hardware specifications of the LibreRouter are outlined. Some of the specifications to remark on are that’s open-source hardware, the Main chip MCU is Atheros QCA9558 RF: QCA9558 2T2R GE PHY: QCA8337N (10/100/1000). The physical interface is composed as follows: 2 - Gigabit Ethernet RJ-45, 2 - Gigabit Ethernet ports available (internal), USB 2.0 connector, USB 2.0 connector (internal, inside enclosure), serial console 3.3V 115200 8N1 (internal header on the board), push button (reset), 2.4 RF Tx header (2.4GHz Ant_A, 2.4GHz Ant_B, GND), GPIO pin header 8 x Status LEDs, software controllable through GPIO [36].



Hardware Specification	
Configuration	Triple-radio 2x2 802.11n Mesh Node
Design License	Open-source Hardware
Firmware	LibreMesh (based on OpenWrt 18.06.1)
Main chip	MCU: Atheros QCA9558
	RF: QCA9558 2T2R
	GE PHY: QCA8337N (10/100/1000)
RF	Radio 1: 2.4G 802.11b/g/n + LNA + PA, 2T2R (QCA9558)
	Radio 2: 5G 802.11a/n + LNA + PA, 2T2R (AR9582 mPCI)
	Radio 3: 5G 802.11a/n + LNA + PA, 2T2R (AR9582 mPCI)
Memory	128MB RAM DDR2
Flash	16MB NOR Flash
Hardware Watchdog	ATTiny13 available via GPIO
Physical Interface	2 x Gigabit Ethernet RJ-45
	2 x Gigabit Ethernet ports available (internal)
	1 x USB 2.0 connector
	1 x USB 2.0 connector (internal, inside enclosure)
	1 x serial console 3.3V 115200 8N1 (internal header on the board)
	1 x push button (reset)
	1 x 2.4 RF Tx header (2.4GHz Ant_A, 2.4GHz Ant_B, GND)
	1 x GPIO pin header
	8 x Status LEDs, software controllable through GPIO

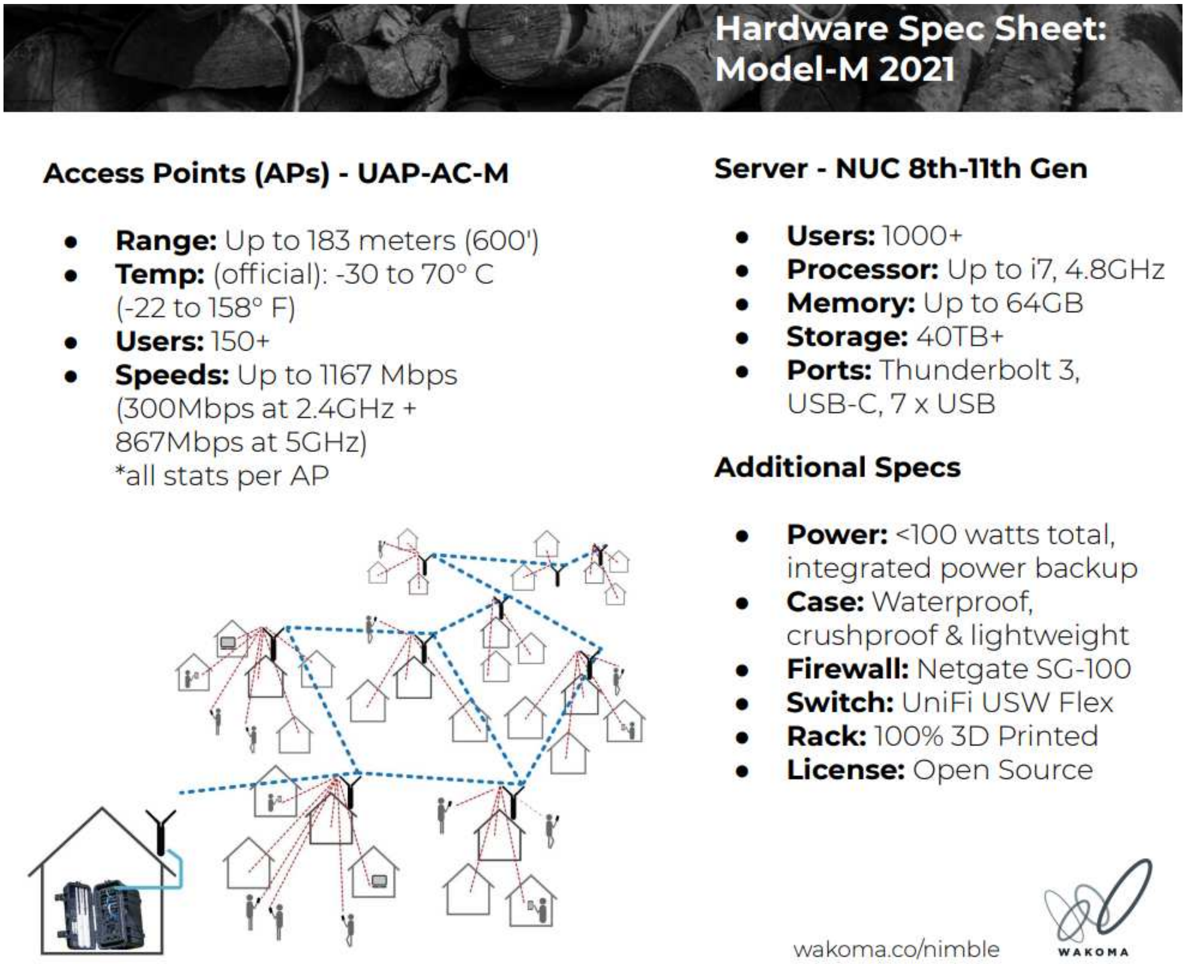
Figure 10: LibreRouter Hardware Specifications [36]

The hardware used in the LibreRouter project is well-suited for community wireless networks, which is a great alternate solution when contrasted with proprietary vendor-locked hardware. The Atheros AR9331 chipset is widely used and well-supported by open-source software, which makes it easier for community members to work with and customize the hardware. The modular design of the LibreRouter hardware allows for flexibility and customization, while the software is easy to configure and manage with basic technical skills. These features make the LibreRouter project a promising solution for communities looking to build and maintain their own wireless networks. I admire the work and effort being made for this project, as it needs support from as many individuals as possible.

2.3.2 Nimble

Another example of a project where open-source hardware was used is the Nimble. It is a powerful wireless mesh network that offers a range of offline capabilities, including video and voice chat, file sharing, eLearning course creation and website building, spreadsheet collaboration, document sharing, e-book reading, and gaming. Its ability to function offline sets the nimble apart, which means users can enjoy all these features without an internet connection. If a single internet connection is available, the

nimble can be used to provide free or paid internet access to anyone on the network. It is worth noting that the nimble uses open-source hardware, making it accessible to anyone with the right components and expertise. Furthermore, the nimble's modular design allows users to add or remove components as necessary to customize the router's functionality to their specific needs. The nimble's potential applications are vast and varied. For example, it is currently being used to expand the reach and functionality of existing community networks in places like South Africa and to enable digital literacy training in remote Indigenous communities in Canada. Due to its open-source nature and ability to function offline, the nimble is an accessible and scalable solution that can bring offline capabilities to communities worldwide. Its portability and flexibility make it an ideal solution for disaster relief efforts or any situation where internet connectivity is limited or unreliable. The nimble is a powerful and versatile tool that can connect communities, foster collaboration, and enable new forms of learning and communication [24]. Figure 11 outlines the hardware specifications of the nimble.



Hardware Spec Sheet: Model-M 2021

Access Points (APs) - UAP-AC-M

- **Range:** Up to 183 meters (600')
- **Temp:** (official): -30 to 70° C (-22 to 158° F)
- **Users:** 150+
- **Speeds:** Up to 1167 Mbps (300Mbps at 2.4GHz + 867Mbps at 5GHz)
*all stats per AP

Server - NUC 8th-11th Gen

- **Users:** 1000+
- **Processor:** Up to i7, 4.8GHz
- **Memory:** Up to 64GB
- **Storage:** 40TB+
- **Ports:** Thunderbolt 3, USB-C, 7 x USB

Additional Specs

- **Power:** <100 watts total, integrated power backup
- **Case:** Waterproof, crushproof & lightweight
- **Firewall:** Netgate SG-100
- **Switch:** UniFi USW Flex
- **Rack:** 100% 3D Printed
- **License:** Open Source

wakoma.co/nimble

WAKOMA

Figure 11: Hardware specification of the nimble [37]

The nimble router is a versatile and modular open-source hardware solution specifically designed for community wireless networks. It has two radios that can operate on different frequency bands, Ethernet ports, and a USB port for additional connectivity options. With its offline capabilities and ability to provide free or paid internet access to anyone on the network, the nimble is a powerful tool that can expand the reach and functionality of existing community networks. Additionally, it is being used to enable digital literacy training in remote Indigenous communities in Canada. The Nimble's portable and scalable nature and its open-source design make it an ideal solution for community wireless networks, disaster relief efforts, and other situations where internet connectivity is limited or unreliable.

2.4Open-Source Software

2.4.1 Lokal

Lokal is a platform that provides open-source software and services that allow communities and organizations to communicate, create and consume content either online or offline, depending on the availability of connectivity. The platform is designed to be customized and can operate on most servers, including single-board computers, nimble servers, or virtual private servers in the cloud. Unlike similar platforms, Lokal is designed to be offline-first and is developed specifically for communities and partners operating in areas with limited or expensive internet access and excessive censorship. With Lokal, users can run services and synchronize content between local and global servers that work online or offline. The platform offers a range of features, including social e-learning, video and audio calling, messaging, high-speed file-sharing, wireless network management, media streaming, and collaborative document and spreadsheet creation, among others. It is like a box of modular Lego services that can be combined in different ways to meet the needs of diverse communities worldwide. Lokal is a comprehensive solution that provides communities with the tools they need to connect, communicate, and learn in a way that is flexible and accessible, regardless of their level of internet connectivity [38]. One of the reasons the Nimble project by Wakoma was very successful and has made it this far is because of the implantation of the Lokal platform, which makes it easy to integrate so many open-source applications and services that make a significant impact in benefiting community wireless networks. Some of the services that are relevant to analysis are Prometheus, Grafana, and UniFi Poller.

2.4.1.1 Prometheus

Prometheus is a powerful open-source systems monitoring and alerting toolkit that was originally created at SoundCloud. Over the years, the project has become increasingly popular, with many companies and organizations adopting it. As a result, it has attracted a large and active developer and user community, making it a standalone open-source project that is now maintained independently of any company. As a result of its growing popularity, Prometheus has become a highly respected tool in the IT world, trusted by developers and system administrators alike. Prometheus is designed to collect and store metrics as time series data, with metrics information stored alongside optional key-value pairs called labels. Figure 12 shows an overview of the whole architecture of Prometheus.

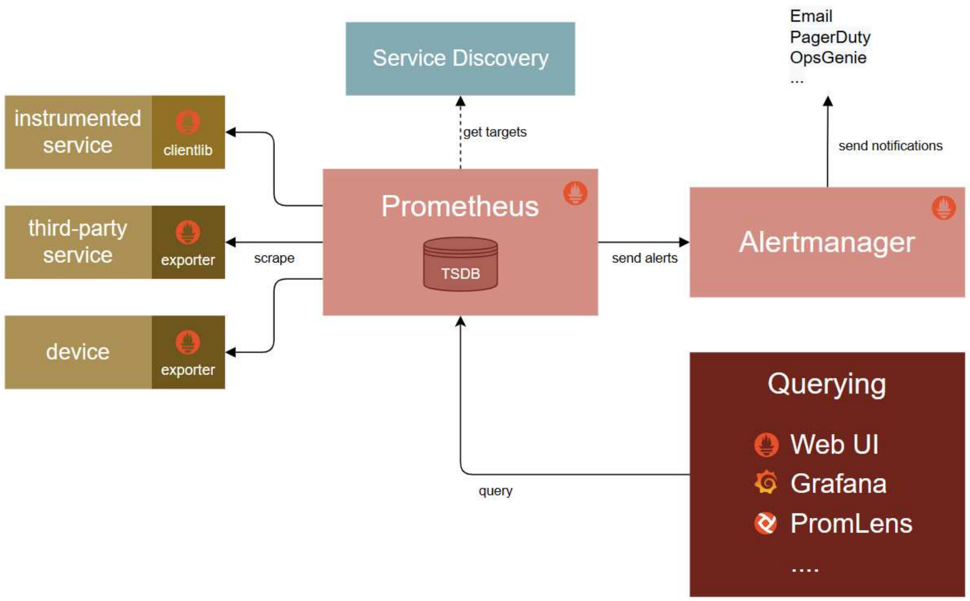


Figure 12: Prometheus overview of the system architecture [41]

The primary characteristics of this tool comprise a multi-dimensional data model that identifies time series data via metric name and key/value pairs, a versatile query language referred to as PromQL that allows users to harness this dimensionality, and no dependence on distributed storage. As mentioned earlier, Prometheus employs its own query language, named PromQL, to utilize the gathered data. PromQL is a functional language that assesses adaptable and efficient computations on time series data. Unlike SQL-based languages, PromQL is exclusively employed for data retrieval and not for performing actions such as inserting, updating, or deleting data. These operations occur outside of the query engine.

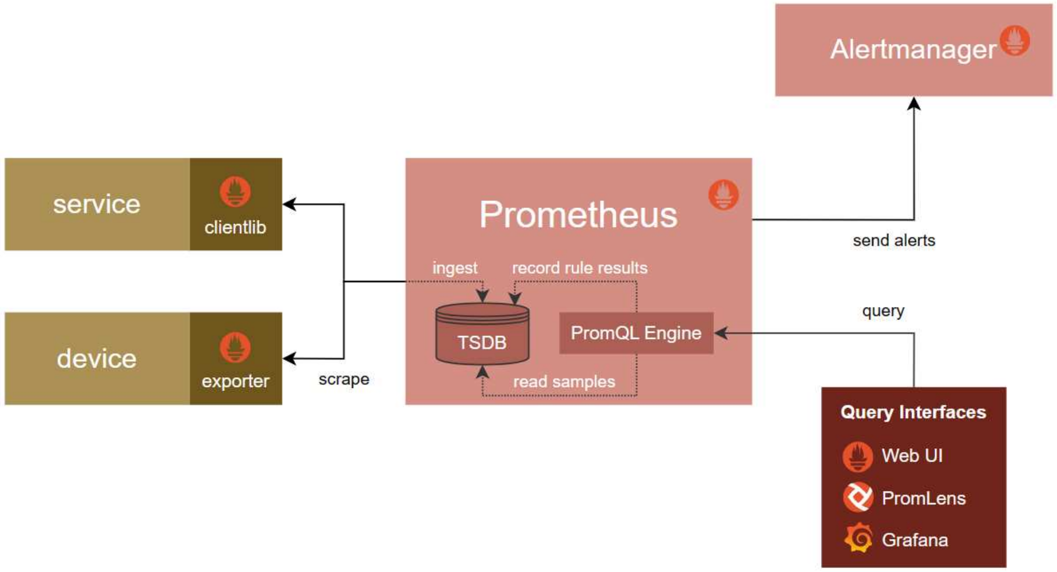


Figure 13: Prometheus query language “PromQL” [41]

Autonomous single server nodes collect time series data through a pull model over HTTP, and pushing time series is facilitated via an intermediary gateway. Service discovery or static configuration is used to identify targets. Metrics are numerical measurements logged over time, with time series data providing the ability to track changes over time. The metrics that users wish to track vary depending on the application. For instance, request times might be significant for a web server, while active connections or queries may be crucial for a database. Metrics play a crucial role in understanding why an application works in a certain way. For example, if a web application is slow, the request count metric can help identify the cause, such as high request volume. Knowing this, developers can increase the number of servers to handle the load. The Prometheus ecosystem encompasses several components, many of which are voluntary, such as the primary Prometheus server responsible for collecting and preserving time series data, client libraries that allow for application code instrumentation, a push gateway that facilitates short-lived jobs, and specialized exporters for services such as HAProxy, StatsD, Graphite, and others. An alert manager is also included to handle alerts, along with various support tools. With its many features and components, Prometheus is a versatile and powerful monitoring tool [39]. Figure 14 shows how Prometheus pulls data and where it stores it.

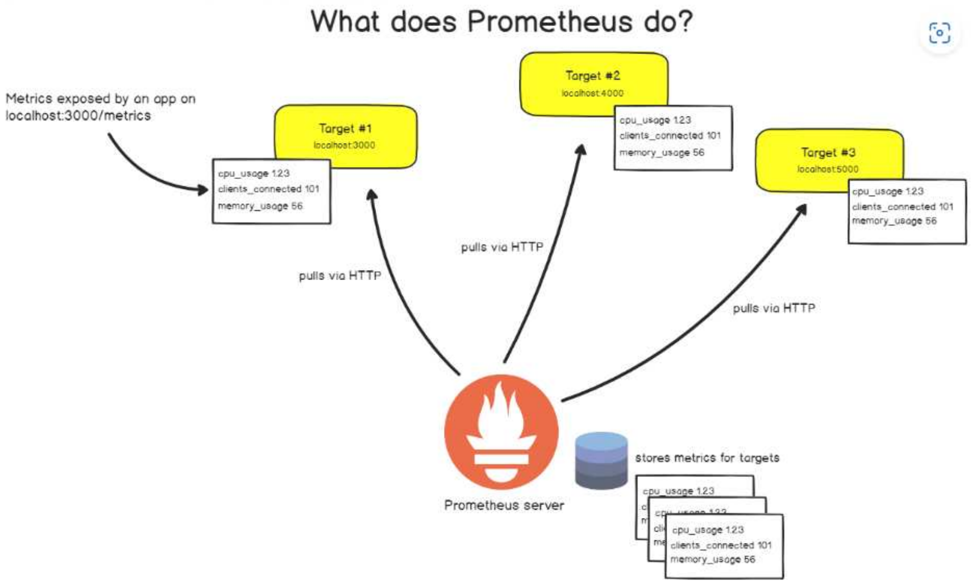


Figure 14: Prometheus pulling and storing data from targets [40]

2.4.1.2 Grafana

As Prometheus does an excellent and efficient job of collecting and storing data, an additional tool called Grafana complements using the collected data. I can say that it's a great service the Nimble by Wakoma project has that can be implemented in other community network projects. Grafana's customizable dashboards, integration with multiple data sources, and powerful alerting and notification features allow us to monitor and visualize data in a flexible and efficient manner. Furthermore, Grafana's scalability would be especially useful in similar projects like the Nimble, which involves processing and analyzing large volumes of data. I believe that Grafana is a valuable service that the Nimble by Wakoma project contains, helping to streamline data monitoring and visualization and enabling the project to make more informed decisions based on data insights [42]. Further down this project, I will mention how this tool can play an important role when set up with Artificial Intelligence.

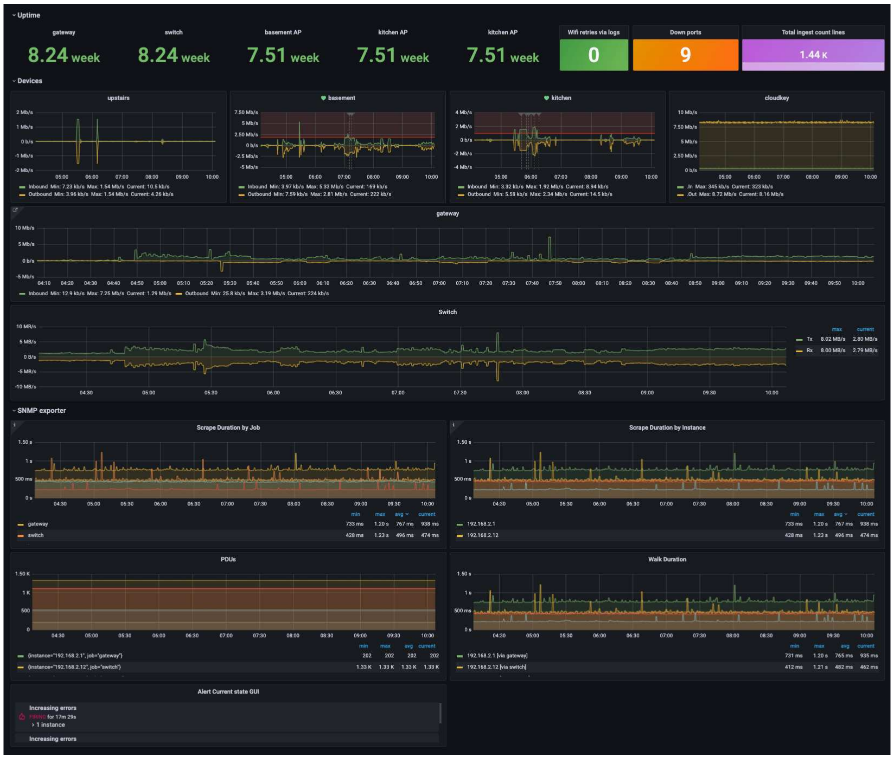

Uptime
gateway 8.24 week
switch 8.24 week
basement AP 7.51 week
kitchen AP 7.51 week
kitchen AP 7.51 week
Wifi retries via logs 0
Down ports 9
Total ingest count lines 1.44 K
Devices
upstairs
Inbound Min: 7.23 kb/s Max: 1.54 Mb/s Current: 10.5 kb/s
Outbound Min: 3.96 kb/s Max: 1.54 Mb/s Current: 4.26 kb/s
basement
Inbound Min: 3.97 kb/s Max: 5.33 Mb/s Current: 169 kb/s
Outbound Min: 7.59 kb/s Max: 2.81 Mb/s Current: 222 kb/s
kitchen
Inbound Min: 3.32 kb/s Max: 1.92 Mb/s Current: 8.94 kb/s
Outbound Min: 5.58 kb/s Max: 2.34 Mb/s Current: 14.5 kb/s
cloudkey
.In Max: 345 kb/s Current: 323 kb/s
.Out Max: 8.72 Mb/s Current: 8.16 Mb/s
gateway
Inbound Min: 12.9 kb/s Max: 7.25 Mb/s Current: 1.29 Mb/s
Outbound Min: 25.8 kb/s Max: 3.19 Mb/s Current: 224 kb/s
Switch
max current
Tx 8.02 MB/s 2.80 MB/s
Rx 8.00 MB/s 2.79 MB/s
SNMP exporter
Scrape Duration by Job
min max avg current
gateway 733 ms 1.20 s 767 ms 938 ms
switch 428 ms 1.23 s 496 ms 474 ms
Scrape Duration by Instance
min max avg current
192.168.2.1 733 ms 1.20 s 767 ms 938 ms
192.168.2.12 428 ms 1.23 s 496 ms 474 ms
PDUs
min max avg current
{instance="192.168.2.1", job="gateway"} 202 202 202 202
{instance="192.168.2.12", job="switch"} 1.33 K 1.33 K 1.33 K 1.33 K
Walk Duration
min max avg current
192.168.2.1 [via gateway] 731 ms 1.20 s 765 ms 935 ms
192.168.2.12 [via switch] 412 ms 1.21 s 482 ms 462 ms
Alert Current state GUI
Increasing errors
FIRING for 17m 29s
› 1 instance
Increasing errors

Figure 15: Dashboard of the visualization of network performance with Grafana [43]

In addition to its many features and capabilities, Grafana can be highly beneficial for community wireless networks. With the ability to support a variety of data sources and visualizations, users can easily monitor and analyze network performance, identify areas of improvement, and make data-driven decisions to optimize network performance. The alerting feature allows for timely notifications of network issues, helping to minimize downtime and improve user experience.

2.4.1.3 UniFi Poller

Even when efforts get maximized in trying to use open-source hardware and software, when possible, there will be instances where the use of proprietary vendor-locked devices might be used along with open-source ones. For example, some UniFi Access points were used in the nimble project, which could make it hard to extract and analyze data. UniFi Poller is a convenient tool that will help with monitoring and collecting data from Ubiquiti UniFi network devices [44]. My main focus is for community networks to use open-source hardware and software, but sometimes it may not be possible. Hybrid use of both open-source and proprietary can work very well. In my opinion, Ubiquiti UniFi network devices can greatly complement a project due to their great quality. If the case comes of using UniFI devices, then UniFi Poller would be a great tool.

2.4.2 OpenWisp

OpenWISP is an open-source network management and monitoring tool that is designed to simplify the task of managing complex networks. It is a modular system that is highly scalable, easy to use, and can be customized as required. One of the most important features of OpenWISP is its ability to manage a wide range of network devices, including access points, routers, and switches [46]. The tool allows network administrators to easily configure, monitor, and troubleshoot these devices from a central location. It also supports various networking protocols, making it suitable for use in various network environments. Another essential feature of OpenWISP is its scalability [46]. The tool can be used to manage networks of any size, from small local networks to large enterprise networks. This is achieved using modular components that can be easily scaled up or down as needed. In addition to device management, OpenWISP provides various tools for network monitoring and analysis [47]. Network administrators can use the tool to monitor network traffic, analyze network performance, and identify and troubleshoot network problems. The tool also provides real-time alerts and notifications, allowing administrators to respond quickly to any issues that arise. OpenWISP also offers advanced features for network visualization and topology mapping [46]. The tool can be used to create graphical representations of network topology, making it easier for network administrators to understand the layout of the network and identify any areas that may be causing performance issues. This feature is particularly useful for large and complex networks. One of the key advantages of OpenWISP is its open-source nature [46][47]. This means that the tool is freely available to anyone and can be customized to meet the specific needs of different users. The tool has an extensive community of developers that help by providing support to users. OpenWISP has many usages, from small local networks to large enterprise networks [46]. It is suitable for use in various industries, including healthcare, education, and finance. The tool can be used to manage both wired and wireless networks, making it a versatile and flexible tool for network management [47]. In summary, OpenWISP is a powerful and versatile tool for managing and monitoring networks that can be used to manage networks of any size and complexity. Its key features include device management, scalability, network monitoring and analysis, visualization and topology mapping, and open-source nature. Its usages are diverse and can be applied in various industries. As such, OpenWISP is a valuable tool for any organization or individual that needs to manage any network. OpenWISP is an ideal tool for managing community wireless networks because it is a low-cost, scalable, and flexible network management tool that can be tailored to fulfill the distinct requirements of diverse communities. OpenWISP provides a user-friendly interface that makes it easy for community members with limited technical expertise to manage their wireless networks. The tool allows community members to manage network devices, monitor network performance, and troubleshoot any issues that may arise. It also provides real-time alerts and notifications, enabling community members to respond quickly to any network problems. OpenWISP's scalability is particularly useful for community wireless networks, as these networks often start small and grow over time as more community members join. The modular nature of OpenWISP allows community members to easily add new devices and services to their network as needed without having to invest in expensive proprietary solutions. Furthermore, OpenWISP's open-source nature allows community members to customize the tool to meet their specific needs. This means that the tool can be adapted to the unique requirements of different communities, enabling them to create a network that meets their specific needs and goals. Overall, OpenWISP is an ideal tool for community wireless networks as it provides the scalability, flexibility, and ease of use that these networks require. With OpenWISP, community members can build and manage their own wireless networks, providing internet access to underserved areas and promoting digital inclusion.

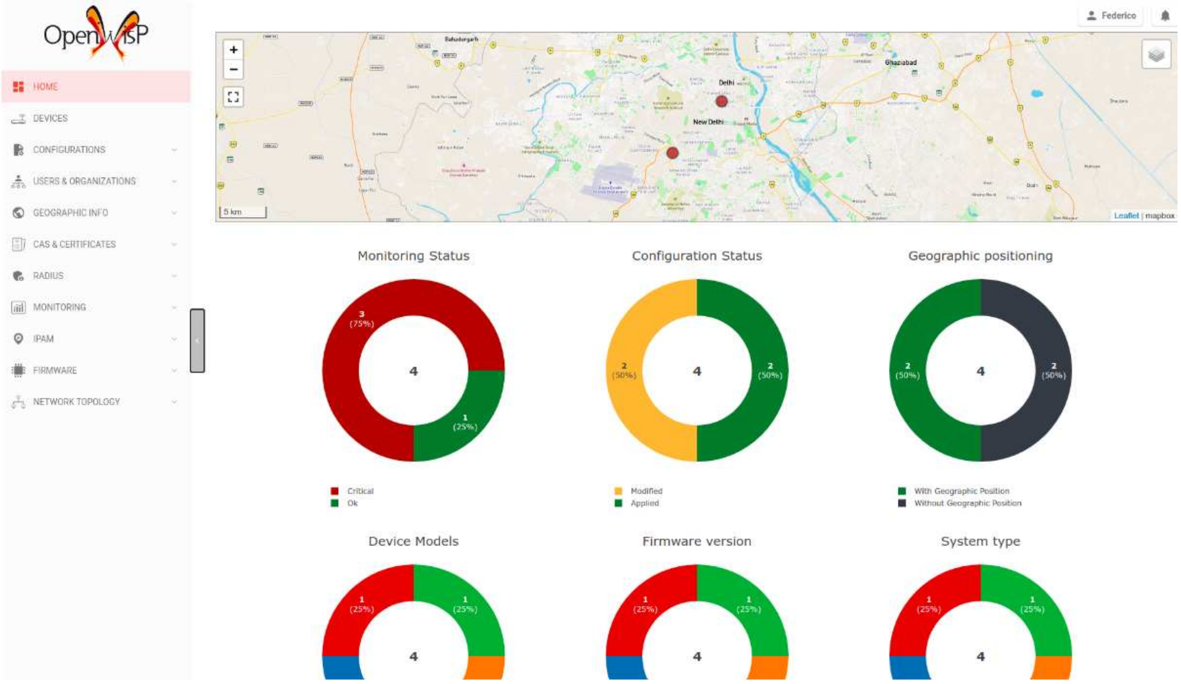


Figure 16: OpenWisp Demo site [50]

2.4.3 Zeek

Zeek, previously known as Bro, is a robust open-source network security monitoring tool that provides powerful real-time capabilities to monitor and analyze network traffic. It is a widely used tool in the network security field and has numerous features that make it valuable for monitoring and securing networks. One of the key features of Zeek is its flexibility, which enables network administrators to customize the tool according to their specific needs. Zeek supports many network protocols and can capture, parse, and process them in real-time [48]. Moreover, Zeek's signature feature, Bro Scripts, allows users to write custom scripts to extract the desired network metadata from network traffic [49]. Zeek also has an advanced set of built-in analytic tools to detect various network anomalies and security threats [48]. It generates alerts and logs for events such as port scans, brute-force attacks, and malware traffic, enabling administrators to investigate and respond to potential security breaches in real time. Furthermore, Zeek provides valuable insights into network traffic patterns and can be used to create reports and graphs to better visualize network activity [48]. This feature allows administrators to gain deeper insights into network performance, monitor bandwidth usage, and optimize network resources. Another notable feature of Zeek is its ability to integrate with other tools and services. As a result, network administrators find it more convenient to automate network security and streamline their security operations [49]. Zeek's integration with security information and event management (SIEM) systems allows network administrators to collect, store, and analyze security-related data in a central location, providing a holistic view of network security events. Zeek is open-source software and has an active community of developers who regularly help with its development [48]. This means the tool is constantly being improved, and new features and capabilities are regularly added. In terms of community wireless networks, Zeek can be an invaluable tool. Community wireless networks are typically built and maintained by community members with limited budgets and resources. Zeek's open-source nature makes it accessible to these communities, and its features can be customized to meet the specific needs of each community. Zeek can be used to monitor network traffic, detect network anomalies and security threats, and generate reports on network activity. These features enable community network administrators to optimize their networks' performance and maintain a secure and reliable connection for their users. In conclusion, Zeek is a highly flexible, customizable, and powerful open-source network security monitoring tool that can be used to monitor and secure networks. Its integration with other tools and services, advanced analytics, and real-time monitoring capabilities make it a valuable tool for network administrators. In addition, Zeek's open-source nature and customizability make it an ideal tool for community wireless networks that require reliable and secure connectivity for their users.

3 Real-Life Use Cases Point of Views

3.1 Altermundi (LibreRouter)

In my opinion, the LibreRouter project is an amazing initiative that uses some great technologies to bring internet connectivity to communities that are underserved by traditional internet infrastructure. The more I read about the LibreRouter and all its success stories, the more amazed I am at how technology can make a great impact when people make above-and-beyond efforts to help others make a significant difference in this world. The project's focus on open-source principles and community-driven development is also impressive, as it allows people from all over the world to collaborate and contribute to the project's success. One of the technologies used in the LibreRouter project that is particularly impressive is mesh networking. By leveraging mesh networking, the LibreRouter can create a decentralized network that is highly resilient and flexible [32]. However, I think that this network can bring problems or, at some point, will cause some issues like congestion and latency, which could potentially limit the performance of the network, especially in areas with high traffic volumes. I always say that no wireless scenario in the world is perfect and will eventually come across challenges that can be difficult to address depending on the many circumstances of a network.

Despite these potential challenges, the technologies used in the LibreRouter project are still highly impressive. The use of open-source software, such as OpenWRT and LibreMesh, allows for a high degree of flexibility and customization [34]. I was very impressed by how old commercial routers can be simply modified by installing a new operating system and taking advantage of the specific features the LibreRouter is designed to do. Although many routers can be modified with a new operating system, there are characteristics they still must include to be useful, having two radios being one of the main requirements. I think that this will lead to another potential issue, the acquisition of hardware such as the routers mentioned earlier might be or become quite difficult because of the current global shortage, which causes an increase in demand for electronics and their price [58].

The LibreRouter project is a great example of how technology can be used to create positive change in the world; its focus on open-source principles and community-driven development, combined with its use of innovative technologies such as mesh networking, make it a highly impressive initiative that has the potential to make a real difference in the lives of people worldwide. While there may be potential challenges, as stated earlier, I believe that the benefits of this technology and the overall vision of the LibreRouter project outweigh any potential drawbacks.

3.2 The Nimble by Wakoma

I was amazed when I first read about the Nimble project by Wakoma. Even when you have an IT background, sometimes you can never get enriched or know about these unique wonderful ideas and successful projects such as the nimble that exist or have been existing for years. The different case uses for the nimble are very impressive. I think that in today's world, the fact that we rely vastly on technology is something that's unavoidable. For example, this might be a very insignificant case, but when working from home for a company, IT administrators rely on employees to have a mobile phone to be able to install an authentication app that will provide an extra layer of security when trying to access the company's network. Many things now rely on registering online rather than filling out a physical paper. Why? Because it is much easier and more efficient for everyone. Where am I going with this? The digital and technological world may be limited to certain areas. Certain communities, especially the ones in remote rural areas, lack these technologies and the education about them. The nimble surprised me with the many features and ways of use that it can provide.

Whenever I think of video and voice chatting with someone, it has always come to my mind that an internet connection is required to accomplish such tasks. When I found out that all those things were accomplished with the nimble and that it was doing it mainly offline, it just blew my mind at first. There are many other services that, thanks to the open-source Lokal platform, are available [38].

On the other hand, just like in the LibreRouter project, this project also uses a mesh network topology, which, as mentioned before, wireless technologies will always come across issues. As many open-source resources are used in the nimble, and being something new, it will bring great challenges in regard the functionality. The services can be limited and may not work fully as some users may expect. The support for this project also plays a big role as anyone is welcome to bring ideas, but sometimes it may not be enough.

I truly believe that this project has a great future, and the more mature it gets, the better functions it will provide. It would be amazing to use some of the ideas from this project in a hybrid way with the ideas like the LibreRouter.

3.3 A Hybrid Idea

As an advocate for community networks, I believe that combining the ideas of the LibreRouter and Nimble by Wakoma can lead to a hybrid solution that greatly improves the performance of community networks, especially with data extraction. The LibreRouter is an open-source wireless router designed to provide reliable and affordable internet access to underserved communities. It is highly customizable and can be tailored to meet the specific needs of different communities. The Nimble by Wakoma, on the other hand, can be used as a powerful data extraction and analysis tool that can help collect, store, and analyze data from various sources (most likely with the use of the services already offered by the Lokal platform, like Prometheus, Grafana, and UniFi Poller). This tool is easy to use and can help make data-driven decisions to improve their operations.

By combining the LibreRouter and Nimble, we can create a community network that not only provides internet access but also allows for the collection and analysis of data to improve the network's performance. To implement this hybrid solution, we can install the LibreRouter in the community and configure it to provide internet access to users. We can then install Nimble on a server connected to the LibreRouter and configure it to collect data from various sources, such as network traffic, user behavior, and network performance metrics.

We can then use Nimble to analyze the collected data and identify areas where the network could be improved. For example, Nimble could detect areas with poor Wi-Fi coverage or high network congestion and suggest ways to optimize the network.

Using the insights gained from Nimble, we can make improvements to the network, such as adding more access points or adjusting network settings. These improvements can be made in a data-driven way based on the insights gained from the data collected by the Nimble. We can continuously monitor the network performance using the Nimble and make adjustments as needed to ensure that the network is performing optimally.

Combining the LibreRouter and Nimble by Wakoma can lead to a powerful community network that provides reliable and affordable internet access while allowing for data-driven improvements to the network's performance. This solution can help to ensure that the network continues to meet the needs of the community over time.

4 Final Discussion and Conclusion

This Capstone project analyzes using open-source hardware and software as an alternative solution to provide better data extraction and analysis for a better performance of community wireless networks. Community wireless networks are coming up on the rise as part of the digital divide problem. Various projects have been successful in the deployment of CWNs worldwide. In this capstone project, we have explored the deployment of community wireless networks and the use of open-source hardware and software in building these networks. We have found that while proprietary vendor-locked solutions are commonly used, they often have significant disadvantages, such as limited data extraction and analysis capabilities.

In contrast, implementing open-source hardware and software offers several advantages, including improved data extraction and analysis, greater flexibility, and increased collaboration and innovation within the community. Open-source solutions are designed to be transparent, customizable, and accessible, enabling communities to take control of their network infrastructure and tailor it to their specific needs. One of the primary benefits of open-source hardware and software is the ability to extract and analyze data more effectively. With proprietary solutions, the data is often locked behind closed doors, making it difficult to access and analyze. On the other hand, open-source solutions provide access to the underlying data and enable developers to create custom data analysis tools that can help communities better understand their network usage and performance.

Moreover, open-source solutions are generally more flexible than their proprietary counterparts, which are often limited in their functionality and locked into specific vendor ecosystems. With open-source solutions, communities can modify the code and hardware to suit better their specific needs and use cases, which can be especially important in areas where network infrastructure is lacking.

In this capstone project, we have analyzed the benefits of using open-source hardware and software in community wireless networks. Specifically, we have examined two open-source hardware projects - the LibreRouter and The Nimble by Wakoma - and found that they offer several advantages over proprietary hardware options. These advantages include greater data extraction and analysis capabilities, lower costs, greater flexibility, and increased transparency and accountability. The idea of a possible hybrid implementation of the LibreRouter and the Nimble can be very promising and can work with adequate planification and support from anyone that is interested in the idea.

Furthermore, we have also examined a range of open-source software tools that can be used in conjunction with open-source hardware to create effective and efficient community wireless networks. These tools include the Lokal platform, Prometheus, Grafana, UniFi Poller, OpenWisp, and Zeek. Each of these tools offers unique benefits, such as network monitoring and management, data extraction and visualization, and network security. Together, the use of open-source hardware and software can have a significant impact on community wireless networks. Additionally, using open-source tools can help foster greater collaboration and knowledge sharing among community members, which can lead to further innovation and growth.

In conclusion, open-source hardware and software offer a compelling alternative to proprietary vendor-locked solutions for deploying community wireless networks. By providing greater data extraction and analysis capabilities, flexibility, and opportunities for collaboration and innovation, open-source solutions can enable communities to take control of their network infrastructure and build solutions tailored to their specific needs. As more community wireless networks are deployed, we expect to see greater adoption of open-source solutions and continued innovations.

5 Recommendations

CWNs can be significantly improved in many aspects, as explained throughout this capstone project, especially in the data extraction, analysis, and monitoring performance parts. Below are some recommendations that can significantly benefit CWNs.

5.1 AI for Data Extraction and Performance Optimization

In my view, integrating an AI service into the hybrid solution of the LibreRouter and Nimble for data extraction and performance optimization could significantly improve the reliability and efficiency of community networks. By using machine learning algorithms to analyze the data collected by Nimble, we could automatically adjust the network settings to optimize performance based on current network conditions.

For example, we can train an AI model to identify patterns in network traffic and adjust the bandwidth allocation of different devices accordingly [59]. The model can also detect areas with poor Wi-Fi coverage and suggest the optimal placement of access points. AI can sound like a broad and expensive implementation due to the requirements that are involved in implementing it, but as more technology is being developed, the use of AI will be crucial, and it does not hurt to at least consider it for this type of community networks.

Some of the steps to take for this to be possible can be the following:

1. Data collection: Collecting a large dataset of network traffic data, including information on the devices connected to the network, the types of data being transferred, and the bandwidth usage of each device.
2. Feature extraction: Identifying relevant features of the network traffic data that can be used to train the AI model [59]. These features might include the type of device, the time of day, the protocol used, and the amount of data transferred.
3. Selecting a model: Choosing an appropriate machine learning algorithm that can effectively learn from the network traffic data and make accurate predictions about the bandwidth allocation of different devices [60].
4. Training: Using the collected dataset to train the AI model, which involves feeding the model with the network traffic data and modifying the model parameters to decrease the difference between the predicted and actual bandwidth allocations [61].
5. Evaluation: Evaluate the performance of the AI model on a separate dataset of network traffic data to ensure that the model can connect new data and make accurate predictions [61].

6. Deployment: Deploying the trained AI model in a real-world network environment and integrating it with the network infrastructure to dynamically adjust the bandwidth allocation of different devices based on the predicted traffic patterns.

6 Bibliography

[1] "LibreRouter," 08 April 2021. [Online]. Available: https://librerouter.org/the-librerouter-is-almost-out-who-wants-one. [Accessed 27 September 2022].

[2] "Lifting the Curse of Digital Isolation: How One Rural Community in South Africa Is Creating Opportunities for Its Youth," Internet Society, 21 September 2022. [Online]. Available: https://www.internetsociety.org/issues/community-networks/success-stories/mamaila/. [Accessed 26 September 2022].

[3] "International Federation of Library Associations and Institutions," [Online]. Available: https://www.ifla.org/publications/community-networks-a-briefing-for-libraries/. [Accessed 2 10 2022].

[4] G. Byrum, "The Journal of Community Informatics," 30 10 2015. [Online]. Available: https://openjournals.uwaterloo.ca/index.php/JoCI/article/view/2707/3451. [Accessed 19 10 2022].

[5] Fundação Getulio Vargas (FGV), The International Telecommunication Union (ITU), and the Internet Society (ISOC), The Community Network Manual: How to Build the Internet Yourself, Paris: FGV Direito Rio, 2018.

[6] "The Center for Neighborhood Technology (CNT)," November 2006. [Online]. Available: https://cnt.org/sites/default/files/publications/CNT_CommunityWirelessNetworks.pdf. [Accessed 25 September 2022].

[7] H. Badran, "Supporting Indigenous Connectivity in Canada," Internet Society, 17 November 2022. [Online]. Available: https://www.internetsociety.org/blog/2022/11/supporting-indigenous-connectivity-in-canada/. [Accessed 18 November 2022].

[8] L. B. a. S. Hadzic, Community Networks: Towards Sustainable Funding Models, Katowice: FGV Direito Rio, 2021.

[9] "Internet Society," LibreRouter: A Multi-Radio Wireless Router for Community Networks, 10 February 2022. [Online]. Available:

https://www.internetsociety.org/blog/2018/12/librerouter-a-multi-radio-wireless-router-for-community-networks/. [Accessed 02 October 2022].

[10] "LibreRouter," What comes in the LibreRouter set?, 21 April 2020. [Online]. Available: https://foro.librerouter.org/t/what-comes-in-the-librerouter-set/32. [Accessed 2 November 2022].

[11] "Cisco," What Is Network Analytics?, 7 February 2021. [Online]. Available: https://www.cisco.com/c/en/us/solutions/analytics/what-is-network-analytics.html. [Accessed 10 December 2022].

[12] "What Is Network Management?," Cisco, 2022 June 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-management.html. [Accessed 10 December 2022].

[13] SolarWinds, "2019 IT Trends Report: The Universal Language of IT," 01 February 2019. [Online]. Available: https://www.solarwinds.com/-/media/solarwinds-swip-2019-it-trends-report.pdf. [Accessed 22 November 2022].

[14] Gartner, "Improve Network Performance and Reduce Downtime with Network Performance Monitoring," 2 December 2016. [Online]. Available: https://www.gartner.com/document/3320118. [Accessed 11 November 2022].

[15] Cisco, "The Cisco 2018 Annual Cybersecurity Report," 2018. [Online]. Available: https://www.cisco.com/c/dam/en_us/products/security/cybersecurity-report-2018.pdf. [Accessed 15 November 2022].

[16] P. Institute, "Cost of Data Center Outages," 2016. [Online]. Available: https://www.vertiv.com/globalassets/documents/reports/ponemon-study/2016-cost-of-data-center-outages-11-11.pdf. [Accessed 19 November 2022].

[17] IDC, "Business Value of Riverbed SteelHead," 2014. [Online]. Available: https://www.riverbed.com/content/dam/riverbed-www/documents/analyst-reports/IDC-Business-Value-of-Riverbed-SteelHead.pdf. [Accessed 19 November 2022].

[18] C. R.-t. a. T. C. (CRTC), "Communications Monitoring Report: 2019," 2019. [Online]. Available: https://crtc.gc.ca/eng/publications/reports/policymonitoring/2019/cmr1.htm. [Accessed 2 December 2022].

[19] R. a. M. -. Market, "Global Wireless Mesh Network Market (2021-2026) by Component, Mesh Design, Service, Radio Frequency, Application, End-use, Geography, Competitive Analysis and the Impact of COVID-19 with Ansoff Analysis," 2021. [Online]. Available: https://www.researchandmarkets.com/reports/5317194/global-wireless-mesh-network-market-2021-2026. [Accessed 15 December 2022].

[20] W. I. S. P. Association, "WISP Industry Market Report," 2021. [Online]. Available: https://www.wispa.org/Industry-Research. [Accessed 2 December 2022].

[21] Ubiquiti, "About Ubiquiti Networks," 2020. [Online]. Available: https://www.ui.com/about/. [Accessed 22 November 2022].

[22] S. A. A. G. A. &. A. A. T. Adeyemo, "A review of mesh networks in rural communities. International Journal of Computer Networks and Communications Security," 2018. [Online]. Available: https://www.researchgate.net/publication/327096387-A-Review-of-Mesh-Networks-in-Rural-Communities. [Accessed 25 November 2022].

[23] T. N. Y. Times, "When Puerto Rico's power went out, these volunteers sprang into action," 9 October 2017. [Online]. Available: https://www.nytimes.com/2017/10/09/us/puerto-rico-hurricane-maria-volunteers.html. [Accessed 22 November 2022].

[24] W. Co, "nimble," 2021. [Online]. Available: https://wakoma.co/nimble/. [Accessed 27 October 2022].

[25] Zenzeleni, "Our Journey," 2020. [Online]. Available: https://zenzeleni.net/our-journey. [Accessed 8 December 2022].

[26] D. E. Foundation, "DEF reaches to the last village," 2018. [Online]. Available: https://www.defindia.org/def-reaches-to-the-last-village. [Accessed 23 November 2022].

[27] "Electronic Frontier Foundation," Whitepapers, 2018. [Online]. Available: https://www.eff.org/wp/community-wireless-networks-empirical-study-citizen-efforts-extend-and-improve-wireless. [Accessed 2 December 2022].

[28] "IT Budgets, Priorities, and Challenges in 2019," Spiceworks, 2 February 2019. [Online]. Available: https://www.spiceworks.com/marketing/resources/reports/it-budgets-priorities-and-challenges. [Accessed 13 December 2022].

[29] "Network Management Megatrends 2018: Exploring Network Management in the Era of IoT, AI, and Digital Transformation.," EMA Research, 19 October 2018. [Online]. Available: https://www.enterprisemanagement.com/research/asset.php/3589/Network-Management-Megatrends-2018:-Exploring-Network-Management-in-the-Era-of-IoT,-AI,-and-Digital-Transformation. [Accessed 2 November 2022].

[30] "Open Cloud Foundation Reference Architecture 2.0," Open Networking User Group (ONUG), 21 February 2021. [Online]. Available: https://onug.net/resources/references/architecture-2-0. [Accessed 19 December 2022].

[31] "Overcoming the Top Challenges of Network Procurement," Forrester Research, 12 August 2017. [Online]. Available: https://www.forrester.com/report/Overcoming-The-Top-Challenges-Of-Network-Procurement/-/E-RES138090. [Accessed 29 October 2022].

[32] "What," LibreRouter, 16 June 2020. [Online]. Available: https://librerouter.org/what. [Accessed 14 December 2022].

[33] A. D. D. D. G. G. a. F. R. S. Bartsch, "LibreRouter: Modular Open-Source Networking Hardware," *IEEE Consumer Electronics Magazine,* vol. 7, no. 10.1109/MCE.2018.2815885, pp. 21-26, 2018.

[34] "Libre design," LibreRouter, 20 July 2020. [Online]. Available: https://librerouter.org/libre-design. [Accessed 22 November 2022].

[35] Flor, "Tasting the magic. Testing the hardware." LibreRouter, 18 July 2020. [Online]. Available: https://librerouter.org/tasting-the-magic-testing-the-hardware. [Accessed 22 December 2022].

[36] GitHub, "Datasheets," 27 January 2020. [Online]. Available: https://github.com/LibreRouterOrg/board/wiki/Datasheets. [Accessed 14 December 2022].

[37] Wakoma, "Nimble," 2021. [Online]. Available: https://wakoma.co/wp-content/uploads/2021/04/nimble-model-m-specs.pdf. [Accessed 21 December 2020].

[38] "Lokal," Wakoma, 2021. [Online]. Available: https://wakoma.co/lokal/. [Accessed 2 December 2022].

[39] "Overview: Prometheus," Prometheus Blog, 2020. [Online]. Available: https://prometheus.io/docs/introduction/overview/. [Accessed 7 December 2022].

[40] "What is Prometheus and How it works?," DevOpsSchool.com, 26 September 2021. [Online]. Available: https://www.devopsschool.com/blog/what-is-prometheus-and-how-it-works/. [Accessed 21 December 2022].

[41] "Introduction to Prometheus," Learn Prometheus From the Creator, 2021. [Online]. Available: https://training.promlabs.com/training/introduction-to-prometheus/prometheus-an-overview/system-architecture. [Accessed 28 December 2022].

[42] "Grafana: Query, visualize, alerting observability platform," Grafana Labs, 2021. [Online]. Available: https://grafana.com/grafana/. [Accessed 2 January 2022].

[43] "Grafana & Prometheus SNMP: beginner's network monitoring guide," Grafana Labs, 30 September 2022. [Online]. Available: https://grafana.com/blog/2022/01/19/a-beginners-guide-to-network-monitoring-with-grafana-and-prometheus/. [Accessed 4 January 2023].

[44] "Introduction: Unpoller - UniFi Poller," Unpoller, 2022. [Online]. Available: https://unpoller.com/docs/poller/introduction/. [Accessed 3 January 2023].

[45] "UniFi-Poller: Network Sites - Prometheus," Grafana Labs, 2022. [Online]. Available: https://grafana.com/grafana/dashboards/11311-unifi-poller-network-sites-prometheus/. [Accessed 9 January 2023].

[46] "OpenWISP," OpenWISP, 2022. [Online]. Available: https://openwisp.org/. [Accessed 5 January 2023].

[47] M. Z. a. F. G. F. Capoano, "OpenWISP: A Management System for Community Wireless Networks," *IEEE Communications Magazine,* vol. 56, no. 11, pp. 98-104, 2018.

[48] "Zeek," What is Zeek?, 2022. [Online]. Available: https://zeek.org/about/. [Accessed 8 January 2023].

[49] H. S. a. M. Abadi, "Intrusion Detection Using Bro IDS," *International Journal of Computer Science and Information Security,* vol. 14, no. 7, pp. 68-74, 2016.

[50] "OpenWISP Demo," OpenWISP, 2022. [Online]. Available: https://openwisp.org/demo.html. [Accessed 10 January 2023].

[55] Flor, "LibreRouter Fase II," Altermundi, 1 November 2018. [Online]. Available: https://altermundi.net/2018/11/01/librerouter-fase-ii/. [Accessed 13 January 2023].

[56] K. PRETZ, "This Community-Run Internet Is Bridging the Digital Divide - The low-power open-source wireless mesh network is portable," IEEE Spectrum, 14 April 2022. [Online]. Available: https://spectrum.ieee.org/community-run-internet. [Accessed 12 January 2023].

[57] B. Sjoerdstra, "Sjoerdstra, Bianca. Dealing with vendor lock-in," the University of Twente, The Netherlands, 2016.

[58] "Why We're in a Global Electronic Components Shortage," IEEE Spectrum, 2021. [Online]. Available: https://spectrum.ieee.org/semiconductors/devices/why-were-in-a-global-electronic-components-shortage. [Accessed 22 February 2023].

[59] A. S. A. T. Mahmoud Abbasi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey," *Computer Communications,* vol. 170, no. 0140-3664, pp. 19-41, 2021.

[60] "How to Choose a Machine Learning Algorithm," Label Your Data, 4 May 2021. [Online]. Available: https://labelyourdata.com/articles/how-to-choose-a-machine-learning-algorithm. [Accessed 24 February 2023].

[61] "Evaluating Model Performance Using Validation Dataset and Cross-validation Techniques," Deepchecks, 23 November 2022. [Online]. Available: https://deepchecks.com/evaluating-model-performance-using-validation-dataset-splits-and-cross-validation-techniques/. [Accessed 25 February 2023].