UNIVERSITY OF ALBERTA

Intranet and its application ‘Community Networks’ to overcome Digital Divide

MINT 709 - Capstone Project
by
Ayush Taneja

Master of Science in Internetworking

Department of Electrical and Computer Engineering

University of Alberta

Supervisor

Dr. Mike MacGregor

Table of Contents

Table of Figures

Abstract

Remote communities often face challenges; two amongst them are connectivity and knowledge about digital space. Connectivity remains limited and unreliable at a place where population density is profoundly low. Remote communities consistently lack telecommunication development due to structural factors including geography, market failure, sparse infrastructure, and existing policy gaps [1]. As stated by the Canadian Radio-television and Telecommunication Commission (CRTC), 87.4% of Canadian homes have access to broadband services with advertised speeds that satisfy the CRTC's basic universal service standards (50 Mbps download and 10 Mbps upload) [2]. However, in remote communities, only 45.6% of households have access to services that fulfil the CRTC's standards. The telecommunication industry focuses on scaling businesses to target and draw exponential Return on Investment (ROI). Due to the above-iterated factors, remote communities fail to offer attractive ROI to telecom industries resulting in negligible investments. These gaps and the aforementioned sets of challenges together give rise to a problem commonly referred to as 'Digital Divide' or 'Digital Inequality'. The broadening of the Digital Divide in Canada poses a great reality check, it makes research, exploration, and strategy advancement a certified work-in-progress.

This capstone project will navigate around the problem of the Digital Divide and its associated solution in Canada's Northern communities and explore potential solutions to minimize the Digital Divide. The term Digital Divide refers to the lack of opportunities to access Information and Communication Technologies (ICT) and the Internet between individuals, households, and businesses for a wide variety of reasons. The problem exists at both global and local levels. In this context, this capstone project will focus on building a model to bridge the existing gap in remote communities and solve the connectivity issues. As part of this project, different networking devices will be assembled to form a hardware kit called 'Nimble'. The said kit will be configured during the project cycle to address connectivity challenges that exist in the geographically dispersed community i.e., Northwest Territories (NWT), Canada.

Note:

- This capstone project was performed in collaboration with DigitalNWT (DNWT) Project.
- Hardware components to build the 'Nimble' kit were sponsored by project mentor Dr. Mike MacGregor and DNWT project stakeholders Prof. Rob McMahon and Prof. Michael McNally from the University of Alberta.

1 Introduction and Literature Survey

1.1 Internet and its importance

In layman’s terms, the Internet is a vast network that connects billions of users. The Internet enables access to any sort of information. It allows communication anywhere in the world, which means users who are connected to the Internet irrespective of their geographic location can communicate with each other on a real-time basis and do much more. The needs of the Internet depend on a variety of factors as to what an individual is expecting from it. For example, an Information Technology (IT) professional may require the Internet for learning new technologies, organizing, and managing files on the cloud, and participating in online technical events, etc. While for some individuals, the Internet is limited to accessing a few applications e.g., WhatsApp, Signals, Telegram, etc. that help them to stay in touch with their families, friends, relatives, and colleagues. These applications with the help of the Internet allow the user to communicate irrespective of geographic location. An increasing number of people are now using the Internet for accessing media streaming applications, while others use it for promoting advertisements. There are also a bunch of people who use the Internet just for social networking that helps to strengthen their networking circle in a fast-paced life. Others may use the Internet just for browsing the content and performing the basic site navigation to read updated information available on the Internet, for example, online reading of white papers, articles, newspapers, etc. As iterated above, people use the Internet for a variety of reasons from listening to music, conducting research, managing finances, vacation planning, gaming, and virtual meetings. Another important utility of the Internet for remote communities is the emergence of the Internet of Things and cloud-based technologies that will potentially improve the resource management strategy and help to conduct the businesses efficiently.

Communication infrastructure becomes an important factor for both economic opportunities and social cohesion in the current information age. Hence, the scope of the Internet is gigantic, and growth of the online users has been increasing at an exponential rate. As shown in figure 1 and figure 2, a recent survey conducted by DataReportal during Oct 2021, demonstrates the variety of reasons that helps to understand the reason why people use the Internet. The survey also explains the top websites and applications used by people while working online. Hence the utility of the Internet is different for each user.

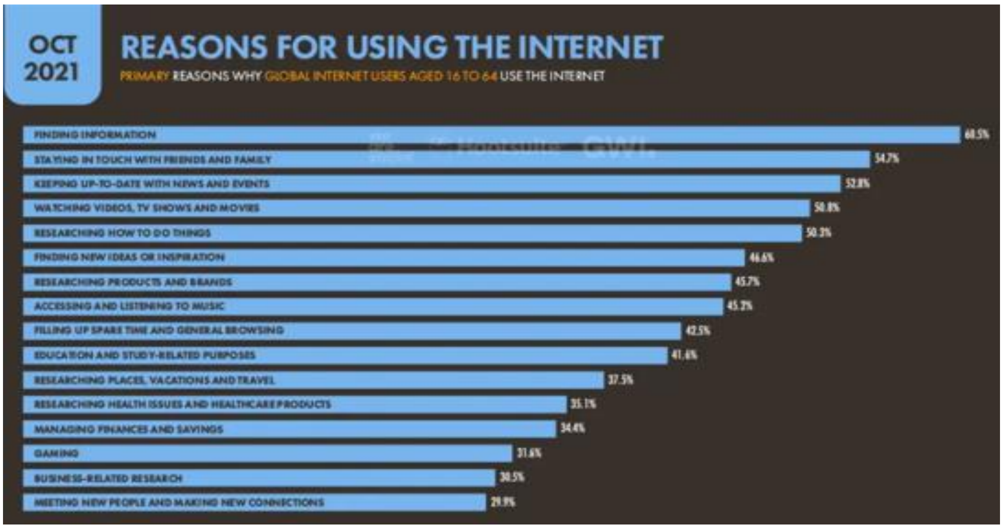


Figure 1: Internet Usage Motivations *[3]*

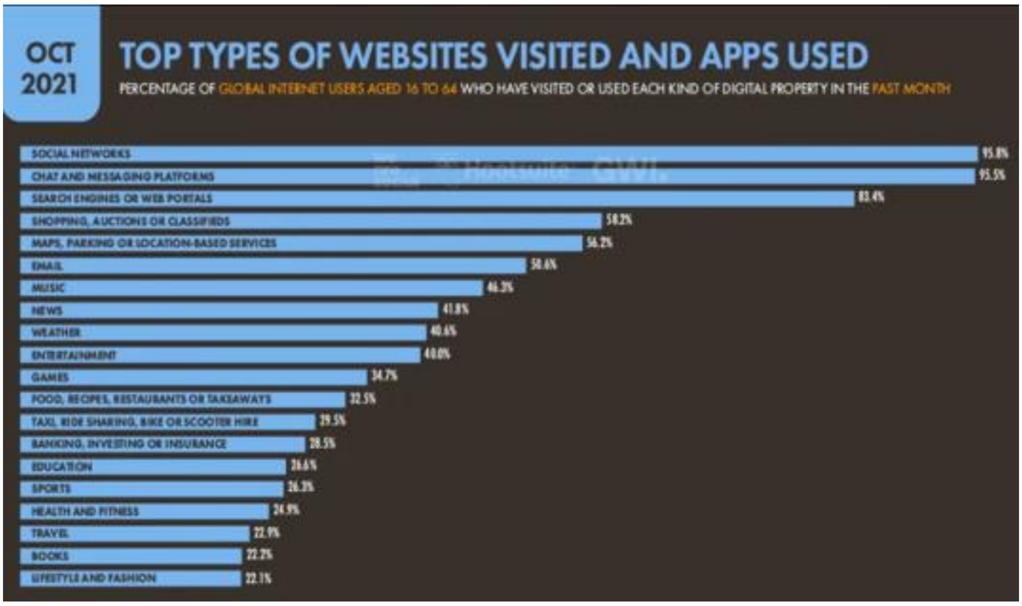


Figure 2: Top Websites and Apps Used *[3]*

For a considerable length of time, the Internet Society has been home to a global community of people who are driven by a common belief, "that when individuals acquire admittance to the Internet, incredible things may happen" [4]. Internet is evolving each day and it has opened a new world for many people around the globe. Internet is the epitome of constant innovation and endless creativity. The Internet can be used for sharing ideas and perspectives, forming communities, creating technologies that we never imagined, delivering effective healthcare systems, assisting youngsters in learning cutting-edge technologies, etc. Internet does not have any boundaries; it essentially creates opportunities and challenges for people in every country. Internet connectivity is underpinning for the new economy.

1.2 Overall World Population versus Digital Population

The world population is increasing multi-fold (see figure 3) and so is the number of connected users on the Internet. The current world population is estimated to be approximately 7.9 billion [5]. Further, surveys as shown below anticipate that the population will rise to 8.5 billion by the end of 2030. It is observed that the world population and number of online users are directly proportional to one another.

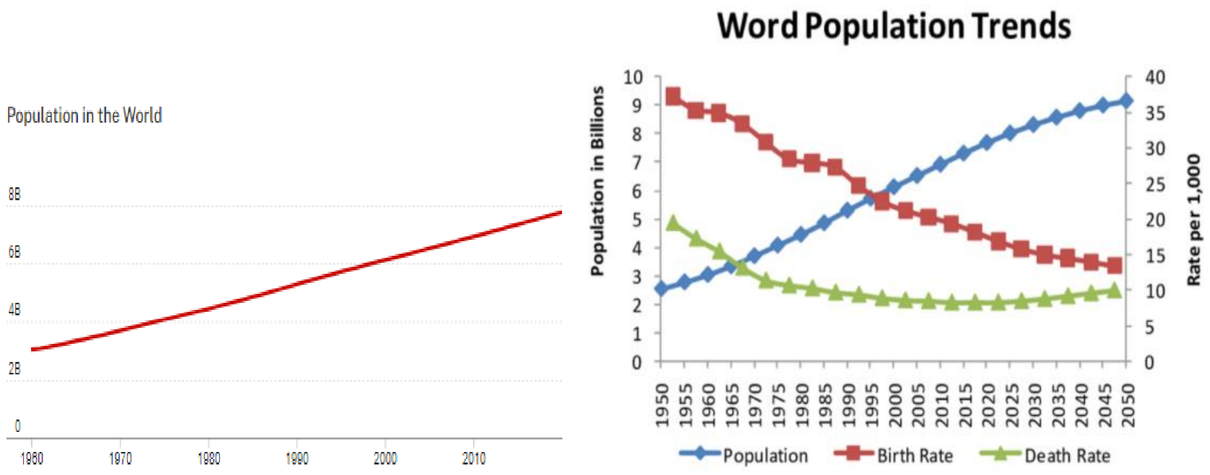


Figure 3: Total World Population Trend *[6] [7]*

According to a recent poll conducted by Statista, there were over 4.66 billion active Internet users globally in January 2021, accounting for 59.5% of the global population. The Internet, which connects billions of people throughout the world, is a key component of today's information society. During the past twelve months, 222 million new users came online. The same trend has been laid out in figure 4. The global Internet penetration rate (Internet users as a percentage of the total population) is 59.5%, with Northern Europe leading the way with 96% of the population having access to the Internet. During current times, the world without the Internet has become unimaginable. As of 2020, the Asia region contributed with the largest number of online users – over 2.5 billion at the latest count. Europe ranks second with about 728 million Internet users. China, India, and the United States rank ahead of all other countries in terms of Internet users. China has more than 854 million Internet users, while India has approximately 560 million online users. Both countries, along with others, still have some regions where parts of the population are still offline which means not connected to the Internet [3] [8].

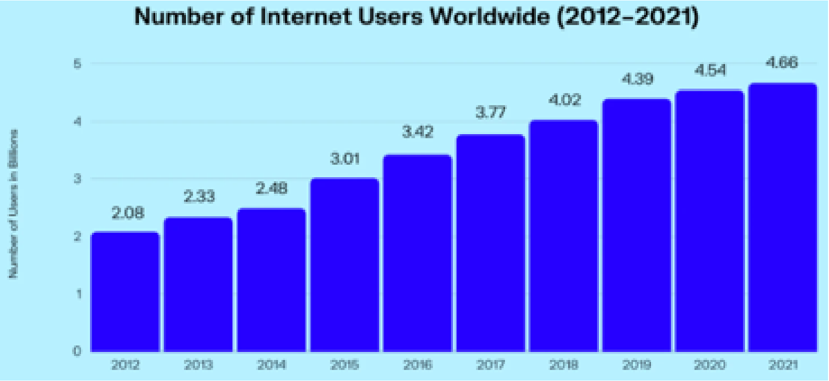


Figure 4: Digital Population Worldwide *[3]*

1.3 Digital Age in Canada, North America

Canada is a developed country, as it meets certain socioeconomic criteria. Canada's borders have changed several times throughout its history, and the country has grown from the original 4 provinces to the current 10 provinces and 3 territories. The main difference between the Canadian province and the Canadian territory is that the province is the creation of a constitution (April 17, 1982), while the territory is the creation of federal law. The majority of provinces are in urban centers while territories are in remote regions. Together, these Canadian provinces and territories form the second-largest country in the world in terms of total area. Canada is the world's largest economy and influences much of global trade. Almost all parts of Canadian provinces are developed, these provinces have sufficient necessary supplies and adequate resources to meet individuals' needs and desires. Canada's current population is approximately 38.19 million as of October 22, 2021, based on the latest United Nations (UN) data Worldometer draft. Below figure 5 shows the projection of the total Canadian population from 2016 to 2026 and the anticipated population of Canada will be 40.22 million at the end of 2026. On similar lines, figure 5 also demonstrates the Internet penetration rate in Canada from the period 2016 and 2026. The Internet penetration rate of Canada in 2021 was 36.39 million. This figure is projected to grow to 39.26 million Internet users in 2026 [9]. Hence, with this piece of available information, it can be concluded that there are a group of people who are still not connected to the Internet and these individuals are left behind in this ever-growing digital age. There can be a variety of reasons like geographic, political, demographic, service cost, accessibility that are restricting these individuals to participate in the fast-moving digital economy.

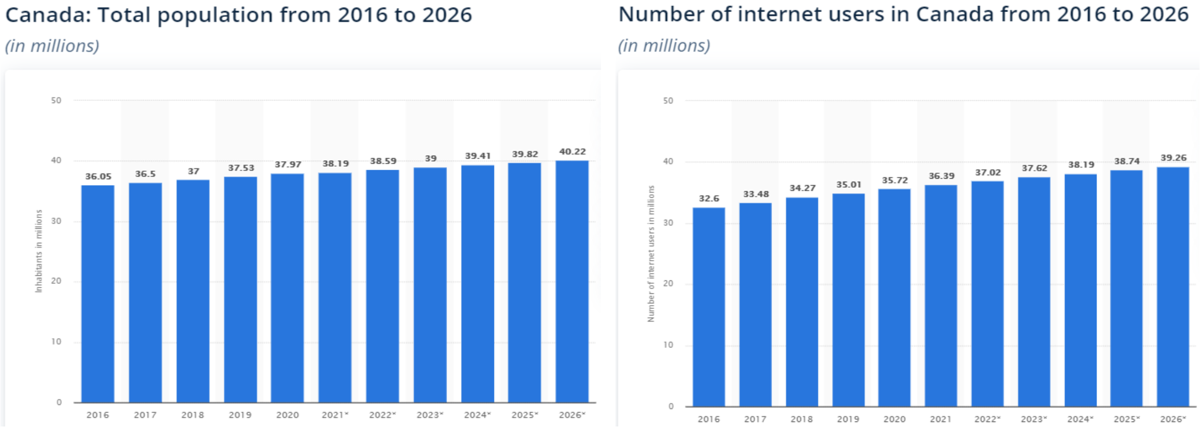


Figure 5: Canada's Total Population vs Digital Population *[9]*

As shown in figure 6, the total population of Canada can be looked in terms of urban centers and rural areas. While 81.4% of Canada's population lives in urban centers, 18.6% lives in rural areas. The overall Internet penetration rate in Canada is approximately 94%, as per the survey conducted by Datareportal in January 2021, which includes individuals living in both urban and remote sectors. Similarly, the percentage of people living in urban centers have easy access to high-speed, affordable, and reliable Internet and its associated services, whereas people living in remote communities face a tough time accessing the Internet services. Northerners usually fall into the category of remaining 6% out of the total Internet penetration rate because these remote regions do not have a strong infrastructure to support reliable Internet connectivity. This gap is often looked in terms of Northerners being disadvantaged in terms of their participation and contribution in growing digital space and economy, and the situations give rise to a problem called 'Digital Divide'. Despite major public and private sector efforts to assist broadband expansion, this problem remains the same.

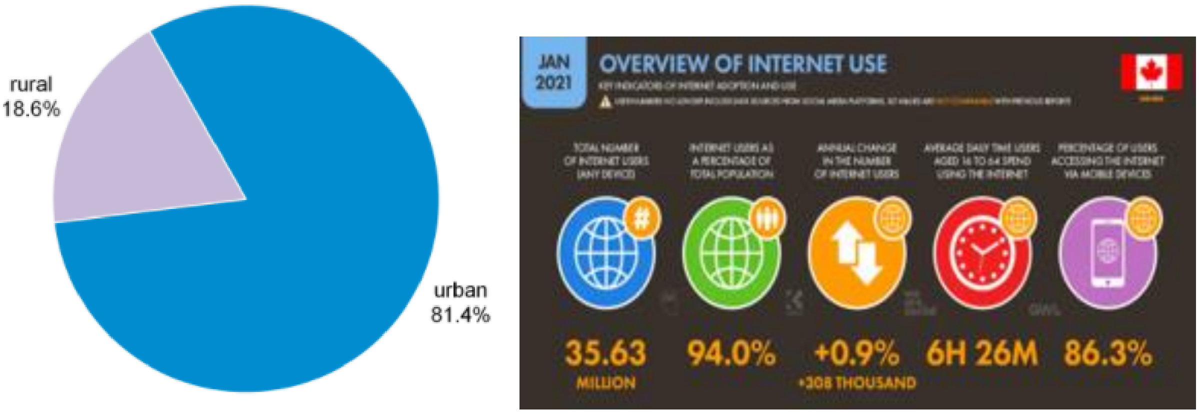


Figure 6: Rural vs Urban Centers and Internet Usage Overview *[10] [11]*

1.4 Digital Divide

The problem i.e., Digital Divide is used in the context of people getting obvious disadvantage, in terms of not being able to access reliable and affordable Internet service. In other words, the Digital Divide is defined as a gap between individuals who have the advantage to get benefits from the fast-paced digital age and the individuals who do not have that advantage of participating in digital space. People without access to the Internet and other IT related technologies are at a disadvantage because these individuals have limited or negligible capacity to obtain digital information, shop online, participate socially or learn and offer a variety of skills [12]. In 1995, the term ‘Digital Divide’ was first used in several newspapers in the United States. The content in the newspaper was used in the reference of ‘haves and have nots’, the similar context was published in the report ‘Falling Through the Net’ by the National Telecommunication and Information Administration (NTIA 1995). The actual state of the Digital Divide is much more complex, and it is linked to existing social, economic, and cultural divisions in the society. The biggest metaphor suggests that the Digital Divide is a technical issue and requires technical addressal, however in fact it is more of a social problem [13]. Moreover, many forums, discussions, and researchers have argued that Digital Divide is going to stay forever, even when the majority of these barriers are addressed. With all previous and ongoing efforts, the gap is going to be shorter, and the Digital Divide cannot be addressed all at once.

There can be a plenty of ways to define the Digital Divide, all with a slight differing emphasis, as evidenced by related concepts such as digital inclusion, digital participation, digital accessibility, and media literacy [12]. Digital Divide is multifaceted, for instance: there are communities in parts of America that do not have the access to the Internet, while on the other hand, there are regions that have the access to the Internet, but it is either expensive, unreliable, or less affordable. The problem can exist globally between nations and locally between regions or communities. The gap between the different nations is called the ‘Global Digital Divide’. Now to understand the extent of the problem on an international scale, consider the digital gap between developed and developing nations. Domestic disparities can usually refer to inequality between individuals, businesses, households, or geographic areas at various socio-economic levels or other demographic categories [12]. Hence, in the real-world scenario, one can imagine that there can be many factors that drive the Digital Divide. There are multiple aspects of this problem i.e., Infrastructure (the type of hardware required to establish the network), Location (where exactly connectivity will be utilized), Skills, and digital literacy (target audience and inequalities of capabilities or skills), and participation (individual’s involvement in the society/ community). Hence, the problem has many facets and can be further divided into 3 levels, which would essentially help researchers to work effectively on the problem using the ‘divide and conquer’ approach. This approach ensures strategically fixing the problem while taking all the factors into account at a time. The first level (also termed as Economic Divide) primarily focuses on physical access and affordability. The second level (also termed as Usability Divide) includes skills and usage. Finally, the third level (also termed as Empowerment Divide) focuses on aftermaths once infrastructure development is complete, and it is the time for potential users to take advantage of the established system [14].

There are powerful worldwide efforts underway to solve the Digital Divide, including a series of international summit gatherings. These different initiatives and movements led by government, researchers, and private organizations are explained in below sections. The goal of ‘eliminating the Digital Divide’ translates into meaningful access to Internet infrastructure, applications, and services. These practices are aimed to close or narrow down the existing digital gap, such that everyone irrespective of their geographic locations have access to Internet services which will allow them to contribute and participate in the digital economy. The key question is not how to connect remote communities or groups of individuals but how to leverage the future gains from the newly built solution. In short, ‘the desired impact and the end justifies the definition’ of the Digital Divide’ [15].

1.5 About Northern Canada and Northwest Territories (NWT)

The northern part of Canada is divided into 3 territories i.e., NWT, Yukon, and Nunavut. Out of the total land area of Canada i.e., 9,984,670 km^2 [16], the overall northern region covers approximately 48% and yet contains less than 1% of Canada’s total population, leading to distortion of national population density value.

The northern part of Canada has traditionally been home to the Indigenous people, that is the First Nations, who were hunters of moose, freshwater fishers, and trappers. The term ‘Indigenous communities in Canada’ refers to First Nations, Inuit, and Métis communities. Canada has more than 50 communities or cultural groups and 50 indigenous languages. First Nations people typically live in communities in the NWT and Yukon as well as in isolated communities in the northern regions of British Columbia, Alberta, Saskatchewan, Manitoba, Ontario, Quebec, Newfoundland, and Labrador. Inuit people live in 53 communities across Inuit Nunangat (‘the place where Inuit live’) in four regions: Inuvialuit (NWT and YT), Nunavut, Nunavik (Quebec), and Nunatsiavut (Labrador) [17].

NWT entered the confederation on July 15, 1870. It covers a total land area of 1,346,106 km^2, which includes both land and water. NWT was called as North-Western Territory, as its predecessor. It is the first largest and most populous of the three territories in Northern Canada, constituting approximately 45,504 as its total population, as per the recent 2021 census report. The capital of NWT is Yellowknife, which is the only city with the largest community in NWT, Canada. At present, the NWT’s official language act recognizes 11 official languages.

Since North-Western Territories (presently known as NWT) joined the Canadian confederation, the area of NWT has divided four times to expand the existing provinces and territories. Long-ago, the area of NWT has been used to create new provinces and territories as well. NWT hosts a few lakes featuring from largest to deepest body of water. The largest lake that exists in Canada i.e. Great Bear Lake is located in NWT. Also, it has Slave Lake, 614m (2014 ft), which has the deepest waters in North America. NWT is home to many rivers and canyons. Another fascinating geographic feature includes Mackenzie River and the canyons of the Nahanni National Park Reserve, a national park, and UNESCO World Heritage Site [18]. NWT is one of Canada's two jurisdictions, and Nunavut Territories is the other, with indigenous peoples accounting for a majority of 50.4% of the population. In 1905, Alberta and Saskatchewan provinces were created from NWT. The Nunavut territories were separated from NWT in 1999.

NWT has a total of 33 communities that are designated authorities, hamlets, villages, or cities positioned in 5 different regions. These range in size from Yellowknife with a total population of 19,569 to Kakisa with a population of 36 [1]. The community reported majority of First Nations status. These population numbers are based on the 2016 census report. Each community has a different management system, some are under the control of different types of indigenous peoples, others are called towns, villages, or settlements. The majority of the communities are managed and governed by municipal corporations. NWT is adjacent to 2 territories and more than 3 provinces. Explanation and figure 7 demonstrate the actual spread of NWT in Canada. NWT is bordered by 2 territories namely Nunavut in the east, Yukon in the west, and by the provinces of British Columbia, Alberta, and Saskatchewan to the south. It also touches Manitoba province at a quadripoint to the southeast. The land area of NWT is vast, and it is equal to the land area of 3 countries combined namely France, Portugal, and Spain [18].

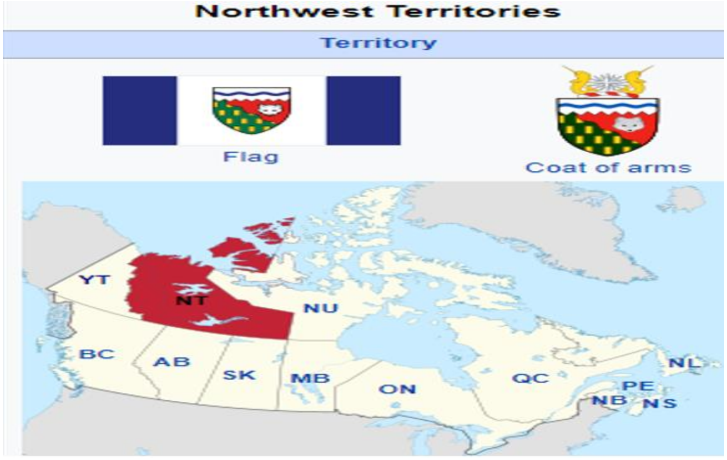


Figure 7: Flag and Positioning of Northwest Territories (NWT) *[18]*

NWT experiences a great climate change from south to north. The southern part has a subarctic climate, while the islands and northern parts have a polar climate. During summers, the temperature varies from 1 to 17 °C. Summers in the north are usually short and cool, on the other hand, winters are long and harsh. The temperature during winters varies from -20 to -45 °C. Thunderstorms and tornadoes are rare but do occur in a few parts of southern and northern NWT. On occasions, natural disasters severely disrupt the supply chain in NWT thereby making it difficult for northerners to even meet their basic needs efficiently.

1.6 Current Situation in Northwest Territories (NWT)

In the 20th century, telephone, radio, and television communications functions revolutionized the way northern people meet, share, and interact. These institutions have gradually developed in the remote northern communities. In the first decade, northern occupants experienced a sample of what the Internet can offer but with limited bandwidth. In 2013, Internet-based voice, video, and smart mobile devices raised consumer expectations. Northerners in NWT are increasingly interested to use online technologies. However, only a small part of northern Canada enjoys access to a high-speed Internet connection. Regional hubs like Yellowknife have access to high-speed internet but constraints on affordable bandwidth translate into higher prices, particularly for satellite-based services [19].

As depicted in figure 5 above, it is obvious that the Internet penetration rate increases with an increase in the overall population. Individuals take interest in browsing information and using different applications and services online. These interests in services are real and it is not limited, technologies can interest anyone in different ways. In recent years, the penetration rate has increased significantly, yet tangible differences in Internet access prolongs, not only in developing countries but also in developed nations such as Canada. This gap demonstrates digital inequalities that majorly exist in remote communities of Canada i.e., NWT, which is home to the indigenous community. Certain population groups in Canada, particularly those in rural and remote areas, continue to be underserved when it comes to broadband high-speed Internet access.

Most of Canada's indigenous communities are small, remote, and rural. For indigenous people, these communities are the center of their world, wherein they conduct small businesses to meet their needs and desires. These small and remote places are the regions where indigenous people grow and nurture their well-being. On the same side, rural settlements and communities exist on the periphery of Canadian society from the perspective of southern Canada. People belonging from Indigenous communities are scarce in numbers as compared to the overall population of Canada, therefore these communities have minuscule geographic footprints to support local needs and fulfill their necessary desires. Even fulfilling an individual's basic needs like water, electricity, transportation medium, telecommunication-related services, etc. are difficult to conduct and manage, because of the scarcity of infrastructure and resources available in the region. For northerners, it is not only difficult to purchase a product online, but also it is an expensive affair. For instance: online shopping platforms i.e., via Amazon, Bestbuy, etc. usually take about a month to deliver products in remote northern regions. Often, the overhead cost of the delivery is more than the actual price of the product. Further, public services are not strong either in a few parts of northern Canada. Transportation, healthcare, medical, school, and governance facilities are usually encompassed by living/ residential units in comparatively small buildings.

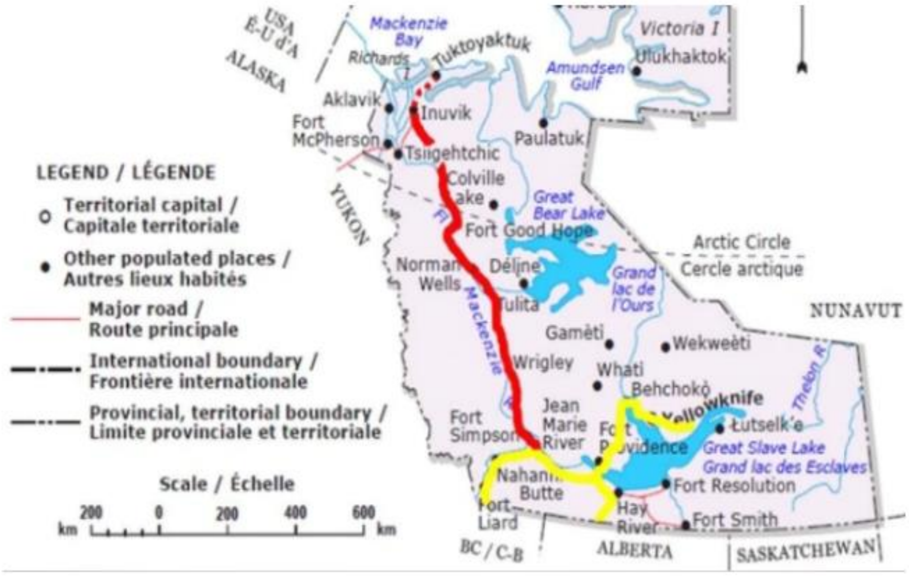
Payment of Internet/broadband bills can be pricey and cumbersome for individuals residing in remote communities. Even the best available internet plan does not ensure a steady internet connection. As per the literature survey, many northerners face bandwidth constraints. Almost every service provider in these remote communities restricts the data usage of the Internet and requires additional charges for data renewal in addition to monthly rental plans. This makes the overall experience of the end-user unreliable and high-priced. As per the journal published by the 'Edmonton Journal', owing to unsteady service in remote communities, many households in rural communities across the NWT could not participate in the National Day of Action for Affordable Internet, held on March 16, 2021. Moreover, 3 smaller communities in NWT namely: Tsiigehtchic, Tulita, and Ulukhaktok recently experienced Internet blackout for more than a week [20], resulting in the inability of individuals from these smaller communities to participate in the ever-growing digital space. Their capacity to access online services and actively partake in dialogues and forums aimed at addressing Digital Divide concerns, is hampered by the excruciatingly sluggish and expensive Internet connection. Few urban centers in NWT namely: Yellowknife and Inuvik have decent Internet service which works smoothly and allows individuals living there to enjoy reliable service and fast connection in the territory, but other rural communities report higher rental prices and slower average download speeds. As a recourse to effectively use the data, few individuals tend to disable video while attending zoom meetings, watching movies with lower picture quality, etc [20].

The need for the Internet is not restricted to learning new technologies, but it also allows an individual to manage finances, healthcare, school, etc. related infrastructure remotely. The dire need for steady and reliable Internet has surfaced during the recent pandemic. During the outbreak of COVID-19, when nationwide lockdowns were imposed, almost every business and corporation shifted to operate in online mode. Pandemic has forced everyone to operate, learn, manage, and socialize virtually.

Availability of the Internet will allow northerners to participate and contribute to the 21st-century economy. People in rural areas will also be able to access services that would otherwise only be available in urban centers like Toronto, Vancouver, British Columbia, etc [21]. This demonstrates the importance of the Internet in everyday life.

Service providers primarily focus on establishing the services in densely populated urban centers. This helps private companies to leverage future gains in order to maintain a healthy market portfolio. The population of remote communities is very small as compared to any city located in urban centers. As per the recent census report of 2021, the total population of NWT is 45,504. This population figure is significantly low from the perspective of the corporation to conduct a wealthy business. This is exactly when remote communities do not get adequate attraction from telecom market players. Moreover, infrastructure development is one of the biggest challenges in remote communities, where arrangement and management of goods and services are difficult to conduct because remote communities are located far from urban centers. Online orders take a lot of delivery turnaround time. The delivery cost of the product is sometimes more than the actual product. As elaborated above, winters are very harsh in NWT, these remote communities are covered in snow almost during all seasons. NWT hosts large rivers and lakes which freeze out during the winter season. Hence, people rely on ice roads to carry out chores. Other modes include travelling by plane or seasonally by boat, which makes it difficult to perform infrastructure development in remote communities [1]. Therefore, the telecommunication industry and other market players are not interested in settling business in remote communities because of high costs, limited opportunities, and a low population density which is not ideal for a wealthy business portfolio [22]. In this regard, telecommunications infrastructure in northern Canada is prone to bottlenecks and service interruptions.

However, as a respite, during recent years, public and private sector organizations, and groups, have started to increasingly take interest and pay attention to the connectivity concerns in Northern Canada. The governor in council appointed an independent public authority called Canadian Radio-television and Telecommunication Commission (CRTC). This organization was created in 1976 and undertakes the responsibility of regulating and supervising the telecommunication carriers. These organizations and government have planned together to reach the ‘last mile’, which is often defined as providing the optical fiber link to each household such that fast and reliable Internet can be established in remote communities to ensure smooth connectivity. Figure 8 demonstrates the same efforts, where the 1,154 Kms fiber link is established from Fort Simpson to Inuvik that covers almost 5 communities namely: Fort Simpson, Wrigley, Tulita, Fort Good Hope, and Norman Wells, that comes along the way of Mackenzie Valley. However, as per the experts, the link is not currently being used to its full potential and the project is not serving the original purpose of providing competitive and reliable Internet service. According to the assessments and media, there is no clear plan that exists for linking areas that are not directly on the fiber link path [23]. Furthermore, existing Internet performance monitoring activities lack data collection. Ideally testing samples should be gathered from different locations by conducting the test in different conditions, each time sample is collected. For instance, CRTC contracted Samknows, a ‘global Internet measurement, and analysis platform’, to conduct Internet performance tests throughout Canada to evaluate if consumers are getting the promised broadband Internet service. According to the recent test results published in 2020, all major Canadian ISPs are delivering subscribers with speeds that reach or surpass the claimed speed. However, the submitted report was criticized as it presents a counterfeit measurement of chosen systems, in chosen areas, for chosen clients at chosen speeds. Sources said that the report was flawed, biased, and results were purported to prove the data, these samples exclude many rural/ remote areas [24]. Significant public and corporate investments have helped to expand ‘high-speed’/broadband Internet connection to rural and isolated regions over the last two decades. Despite this, access to high-speed, low-cost internet remains a national nightmare.



A map of the Mackenzie Valley Fibre Link in the Northwest Territories. The red line represents the Mackenzie Valley fibre optic link. The yellow line represents line already in place before the MVFL was built. (CBC)

Figure 8: Establishment of 1,154 Kms long fiber link from Fort Simpson to Inuvik *[23]*

Communities with lower education and income levels are typically identified as primary factors that adversely affect Internet usage and its associated utilization. CRTC has already declared that broadband is universal, and therefore it should be available to all Canadians, including those living in remote North [25]. Since remote communities are located far away from urban centers hence the availability of the Internet becomes vital, where maybe there are limited/ no government offices, telehealth, physicians, banks, colleges, etc. Canada is the second-largest country in the world, with its varying climate and geography contributing approximately 9.1 million square kilometers. Hence, few remote regions face unique challenges in providing similar broadband Internet services for all Canadians. Average household income in NWT is typically lower than the Canadian average. Also, the household income for these kinds of communities is often seasonal because individuals living in these communities are involved in small businesses. These individuals are engaged in activities like fishing, hunting, and trapping. While on the other hand, the cost of living is considerably higher in remote communities. To illustrate, the cost of the Internet in NWT is nearly double as that of any region located in urban centers like Calgary, British Columbia, and Toronto. Incomes also vary within the North, with residents of small, remote communities generally earning less than those in larger centers or resource sites (mining, commercial fishing, etc.) For example, family incomes in Dene communities in the NWT are less than 45% of the average family income in Yellowknife [25].

The monthly rental price of Internet service across Canada varies from $25 to $63 CAD for a 5 Mbps connection. The monthly rental price increases as bandwidth increases. As per 2017 statistics published by CRTC, the average Canadian’s monthly cable bill was $52 CAD. Northerners pay substantially more for Internet service, and yet are offered services with limited constraints. There are 3 major service providers in NWT namely: NorthwesTel, SSi Micro, and Ice Wireless. These service providers offer unlimited data plans in communities like Norman Wells, Inuvik, and Yellowknife. These plans are unlimited and do not have any constraints on data usage. Unlimited plans are usually very expensive to afford, considering the household income is comparatively less as compared to the overall household income of Canada. There are lots of communities namely Whati, Paulatuk, etc. where service providers do not offer unlimited data plans because of inadequate infrastructure enablement. Communities like these have only DSL plans which have limited data usage and the rental becomes expensive as the data limit gets over and the surcharge gets activated for additional data usage. For example, tariff plan in regions of Inuvik and fly-in communities like Sachs Harbour, Paulatuk, and Ulukhaktok is $79.95 per month for 5 Mbps (the fastest available plan), 60 GB cap with every additional gigabyte of data costing the user an additional $3 [26] [27]. Individuals living in such communities must adhere and keep frequent observation on monthly data downloading quota limit; surpassing these caps results in overage additional charges. The cost of the Internet may be considered as a major challenge experienced by many households living in NWT [1]. This shows that affordability is a huge barrier in remote communities.

Modern telecommunication services are the basis of Canada's future economic prosperity, global competitiveness, social development, and democratic discourse [2]. Hence, these communities require a helping hand for fulling their essential needs to support infrastructure development. Unique programs led by community stakeholders, government, and interested researchers may come together to serve the cause, so that northerners can participate in the digital economy and society. These settlements are practical, rational, and vital for infrastructure development purposes. Formal settlements in the form of unique programs and collaborations between different stakeholders could help in streamlining the process that will essentially help in mitigating the existing challenges. DigitalNWT (DNWT) is one of such programs led by the University of Alberta, Aurora College, the Government of Canada, and private organization firms.

The Commission approved NorthwesTel's $16.8 million application for financing to improve local access and transportation infrastructure in 18 communities in the NWT. At the completion of the project, NorthwesTel has promised to provide fiber-to-home service in Dettah and 17 other communities. The plan is to offer a fixed broadband Internet access service of 50/10 Mbps with an unlimited capacity [28]. As per CRTC reports, high-speed Internet is an essential service for the nation, and it is vital to one’s quality of life. Many northern organizations continue to call for more affordable and reliable Internet service. About a year ago, Dene Nahjo, founder Melaw Nakehk’o started a petition called ‘Accessible/Affordable Internet across the North’. The petition was aimed to enable the access of reliable and high-speed internet during the difficult time of COVID-19. Residents living in NWT invited NorthwesTel to waive the overage fees and requested to establish unlimited data plans [29]. In 2018, the Internet Society hosted the annual Indigenous Peoples Connection Summit in Inuvik and published a community report focusing on policy recommendations made in collaboration with the people of the north. DigitalNWT encourages NWT residents to test their Internet speeds (if possible) and share the results with #NWTDigitalDivide [20]. These initiatives can also help to properly operate, maintain, and upgrade the infrastructure required to support the local needs of the communities. Fixed and mobile wireless broadband Internet access services are catalysts for innovation, supporting a vibrant, creative, and interactive world that connects Canadians to long distances and other parts of the world. Enabling the service will improve the quality of life for Canadians and empower them as citizens, creators, and consumers [2].

These initiatives and efforts by departments, individuals, and government are very much required to bridge the gap of the Digital Divide. The goal of this capstone project is to deliver a bundled solution that is aimed to shrink the existing connectivity gap that lies in remote communities. A different sets of hardware units are used as a building block to cater the connectivity challenges. Primarily, hardware units include Router, Switch, Server, and Access-Point to provide wireless connectivity in remote communities such as NWT. The final assembled kit is known as the 'Nimble' unit. Other important aspects of the Nimble unit are discussed in the ensuing sections.

2 Design & Implementation

2.1 Solution

Digital divide and its effects of being separated from digital space can introduce many negative impacts on society. Access is generally restricted in rural areas, resulting in poor connectivity. Most remote communities have Internet connectivity, however poor quality of service is one of the most reported problems. Technology advancements are happening in urban cities, these small rural communities do not get attraction because of their low population density and higher cost of infrastructure developments. Northern remote communities in Canada are a novel site to explore the advancing challenges of digital connectivity. As per the literature surveys and discussions, it may be clearly seen that the infrastructure development and availability of readily available resources are the key challenges that are being faced in northern communities. As part of this capstone project, we deliver a solution that works offline, thereby eliminating the need for the Internet. The solution is based upon the application of Intranet i.e., 'Community Networks' and leverages the advantages of wireless meshing techniques to increase the network coverage area.

Note: Internet is only required during the installation process and running the strategic synchronizations. This process can be used to synchronize multiple Nimble units at a time. Once the data available on the Internet is downloaded, synced, and stocked on Nimble instance, then offline access to the services would be possible. For instance: Updating the 'firmware package' of devices and uploading new media streaming libraries on 'Jellyfin' service would require the Internet.

2.2 Design

The Internet is a collection of interconnected networks that connects billions of users. Internet connects schools, jobs, opportunities, and each other. However, as learned from above sections, not everyone is online, especially individuals living in remote communities. Internet service is expensive, yet unreliable in remote regions like NWT, Yukon, and Nunavut. These places require an alternative strategy when it comes to connectivity. This project follows similar principles as guided by the First Nations principles of Ownership, Control, Access, Possession (OCAP) and delivers a solution based on 'Intranet' technology that is built to be 'offline first'.

This capstone project leverages the application of Intranet technology i.e., Community Networks (CNs). Intranet technology plays a vital role in building community wireless mesh networks. The term 'Community Networks' can be defined as the local community-led initiatives to govern, operate and manage the network infrastructure to empower digital communication. This approach follows the same OCAP principle, where the local community members take the overall control of the network. Community networks are less expensive and hence budget friendly. These types of networks (CNs) are easy to understand and hence are flexible to deploy. Community networks can cater multiple smaller networks to make one bigger Local Area Network (LAN). Hence, these CNs serve as a scalable solution, can be self-managed by remote communities and therefore are a source of employment as well.

Now, to enable CN and further eliminating the connectivity challenge in Digital Divide, there is a need for proper hardware and software, the selection between them being critical. Once required hardware and its associated components (shelves and wires) are arranged, then the software is required to be selected that can work with local services. This ideology is deployed for the final model to work in both online and offline modes. This way of coupling between hardware, software, and service contents can be termed as a bundled solution.

This bundled solution eliminates the hard need for the Internet and at the same time allows individuals living in remote communities to access the services locally without the need for expensive Internet plans. This mode of operation can be termed as offline mode. Hence, with this approach 'offline first' ideology can be promoted. Figure 9 demonstrates the traditional architecture of community networks (Intranet).

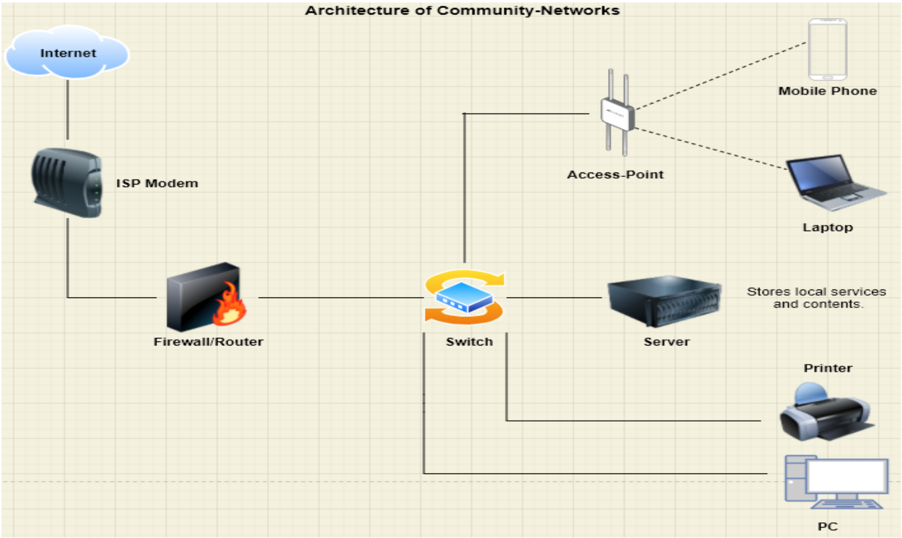
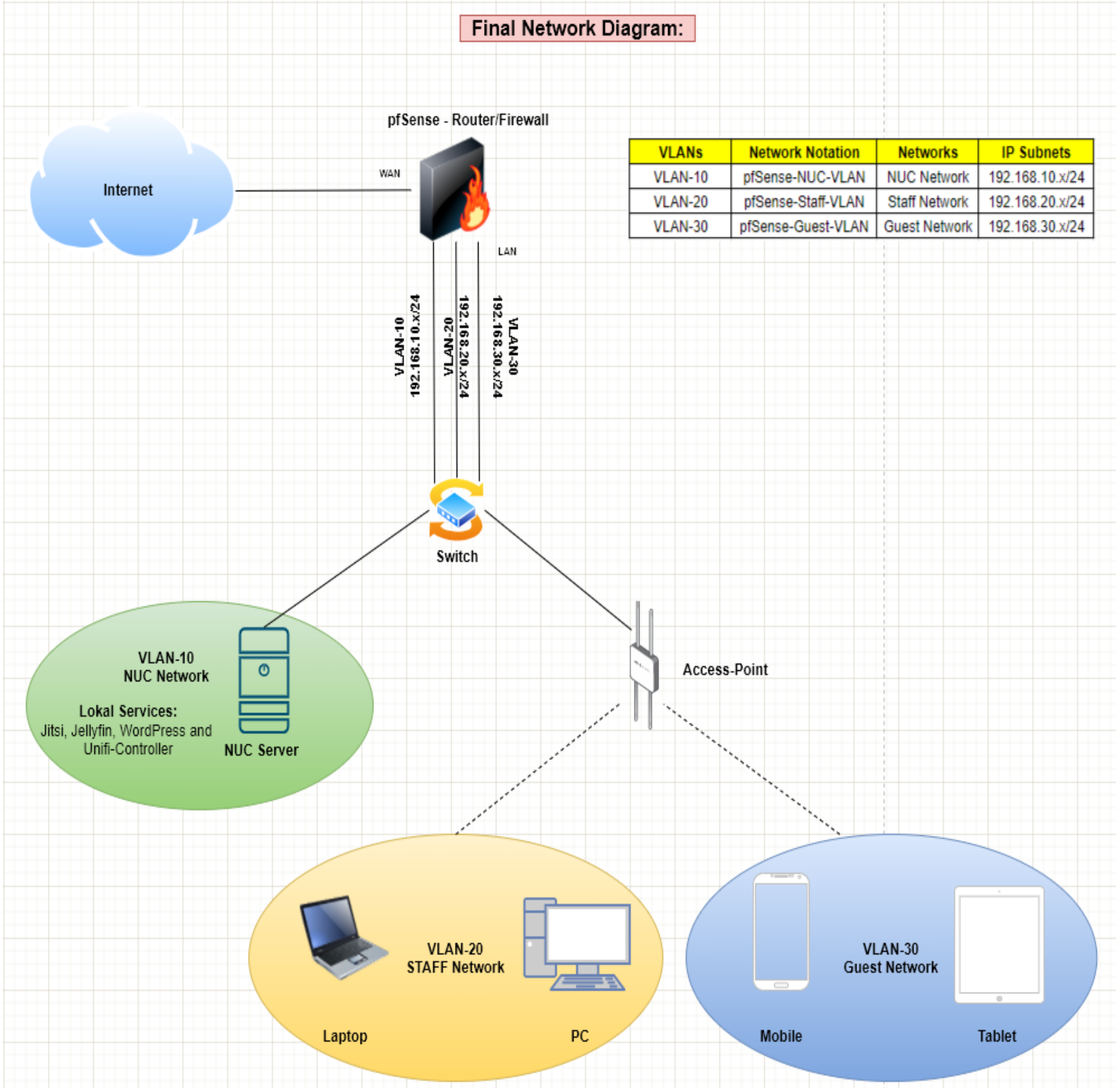


Figure 9: Traditional Architecture of Community Network (CN)

At this juncture, the final deployment of the 'Nimble' unit with all running services on the server and configuration is shown in figure 10. The network has been segregated using multiple Virtual Local Area Network (VLAN) approach. There are 3 VLANs that are designed for the final deployment use-case namely: VLAN-10, 20, and 30. VLAN-10 is specially designed for communication with the server only. Similarly, VLAN-20 and 30 are configured for provisioning of 2 SSIDs i.e., DNWT-Staff-Network and DNWT-Guest-Network. DHCP servers run individually on each network segment. The communication between different networks that are segregated via VLANs is only permitted based on firewall policies defined per VLAN network. Each device will be able to communicate with each other using inter VLAN routing approach. This use-case is commonly termed as 'Router-On-Stick'. Users connected on VLAN-20 (Staff Network) have read-write access to alter any configuration settings at any time. Tight firewall policies are designed to restrict admin access for the user connected to VLAN-30 (Guest Network). Users connected to the Guest network will not be able to alter any device level parameters. Note, further granularity can be achieved in designing a firewall rule engine based on network requirement at later stages.



VLANs	Network Notation	Networks	IP Subnets
VLAN-10	pfSense-NUC-VLAN	NUC Network	192.168.10.x/24
VLAN-20	pfSense-Staff-VLAN	Staff Network	192.168.20.x/24
VLAN-30	pfSense-Guest-VLAN	Guest Network	192.168.30.x/24

Figure 10: Final Nimble Deployed Use-Case

Also, the request and response diagram may be viewed from figure 11. This figure explains the working of a client-server model in a typical computer network. All clients will join the Nimble network using a Wi-Fi network. A user will be connected to Access-Point (AP) first. Then, the switch will perform the Media Access Control (MAC) learning action of the connected user's device. It will record the physical address of the device in the MAC table. Further, based on the destination MAC entry in the request frame, the switch will perform the forwarding action and send the request frame to the Router/Firewall device. The router will perform the routing action based on entries present in the routing table often termed as Routing Information Base (RIB) and route the traffic based on the received destination IP address in the request packet. This way each request packet will be received by the server, and it will be served with an appropriate response message following the same principles.

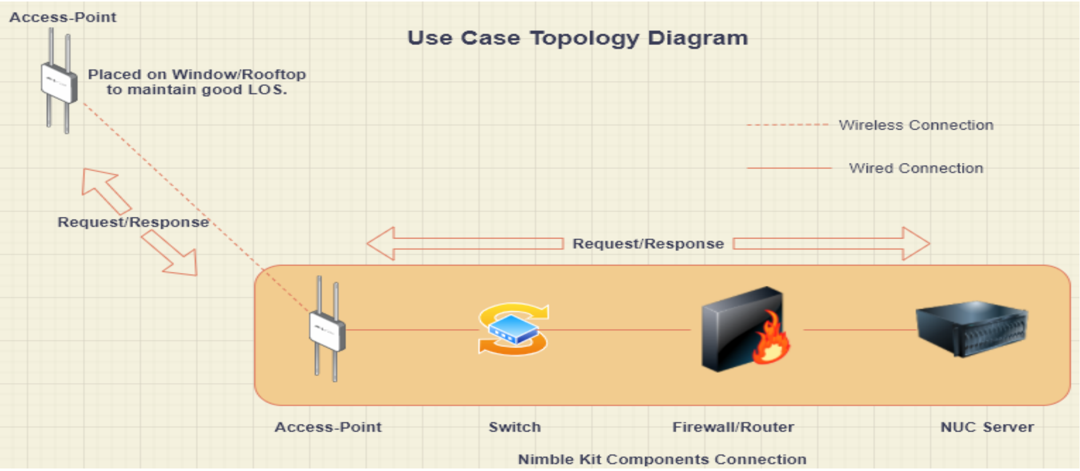


Figure 11: Request and Response Message Flow Diagram

2.2.1 Resources Requirement

The design aspect of the proposed solution is discussed in detail. It is the time to list all hardware components that are required to establish community networks. Intranet majorly deals with the enablement of networking devices and servers. Once networking devices start to work together in conjunction, then coupling the environment with a powerful server (capable of storing data, services, contents, and libraries) enables the accessibility of local services and contents while operating in offline (without Internet) mode.

S. No.	Hardware Components	Purpose
1.	Firewall/Router	Filters and routes the legitimate traffic between network boundaries
2.	Server	Stores local services e.g., Chat & Video messaging, Media Streaming, etc. that will be accessible in online & offline modes
3.	Switch	Switches traffic within network boundaries w or w/o VLAN tags
4.	Access Points	Creates WLAN & SSID, where users will connect to access local services
5.	Cables	Connects individual devices together to form a single unit
6.	Patch Panel	Bundles multiple ports together to organize group of cables
7.	3D Printed Shelves	Legs and shelves to form a rack. Capable of holding the Nimble kit together
8.	Screws	Screws different bolts to a form a robust rack
9.	Pelican Case	Holds the Nimble kit tightly. Later, kit can be used to travel distances to promote 'offline first'
10.	Power Bank	Useful in instances of power outage

2.3 Hardware & Software Selection

Individuals from remote communities drive the establishment of the network. They are the stakeholders who take care of assembling the hardware kit, spinning up the software and local services followed by configuring the individual hardware unit. This can be done under the supervision of a few specialists, who have the expertise of setting up the servers and networking devices. Selection of hardware and software should be performed carefully to achieve higher efficiency, throughput, performance, and maximum uptime of the network.

Hardware Component	Vendor Name	Model/Description
Server	Intel	NUC10i5FNH1
RAM	Crucial	CT16G4SFD824A
SSD	Samsung	970 EVO Plus NVMe M.2 SSD 500GB
HD	Western Digital	WD Blue 2TB HDD
Firewall/Router	Netgate	pfSense SG-1100
Switch	UniFi	USW-Flex
Access Point	UniFi	Access Point AC Mesh
Patch Panel	VCE	Dual Female RJ45 Keystone
Loader Case	Pelican	1430 Protector Case
Shelves and Legs	Prusa	Prusa I3 MK3S+
AC Power Supply	Trond	Trond Prime II
Power Bank	Omni	Omni 20+
Screws & Driver	NA	NA

2.3.1 Hardware Configuration

2.3.1.1 NUC Server

In this work, Intel NUC has been used as a server. Intel NUCs are often termed as mini-personnel computer (PC). This server is fully complete and ready to work out of the box. For instance: consider the hardware units bundled with a PC namely: keyboard, mouse, monitor, speakers, and Central Processing Unit (CPU). NUC works the same as CPUs. Intel NUC kit is used with a 10th generation processor. Other specification includes: 64-bit machine, capable of running any operating system (Windows, Linux, etc), supports solid-state drive (SSD) and internal hard drive (HD). This device has 4 cores and supports 8 threads execution to achieve fast operations. The device consists of 7 USB ports (including both Type-A and Type-C), 1 HDMI port, 1 Thunderbolt port, wireless, Bluetooth card, and 1 LAN port built into the system board. Intel NUC server can be controlled and managed via shell terminal using SSH service.

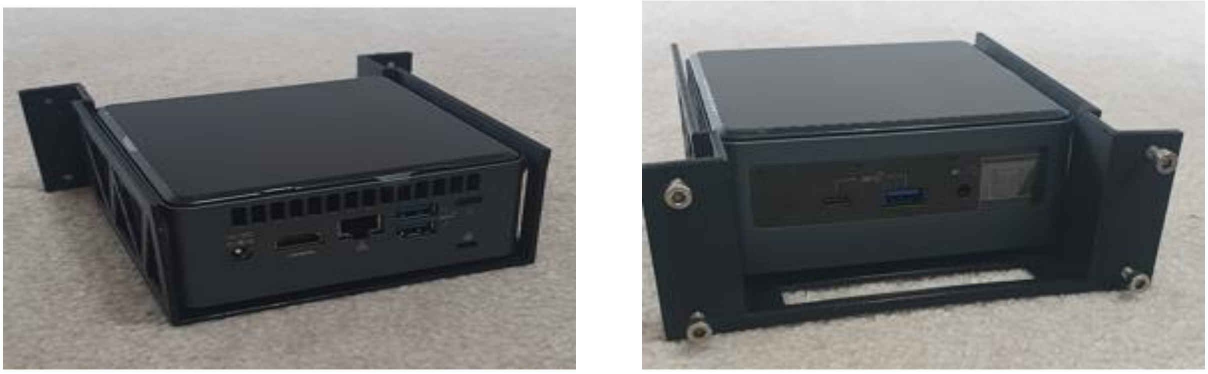


Figure 12: Intel NUC Server (NUC10i5FNH1) Assembly

2.3.1.2 RAM, SSD, and HDD

These below hardware units are required to run the NUC server. These devices must be placed inside NUC carefully. Specification of RAM and SSD helps in boosting the performance and overall efficiency of the system during the operational time. The RAM configuration was 16 GB Single DDR4 2400 MHz. The SSD was NVMe M2 with 500 GB capacity. This model helps to level up the performance and offer multitasking with ease. The HDD used has a capacity of storing 2 TB of data, which can be used to store media streaming libraries and educational contents. It further can be used to perform system backups and upgrades.

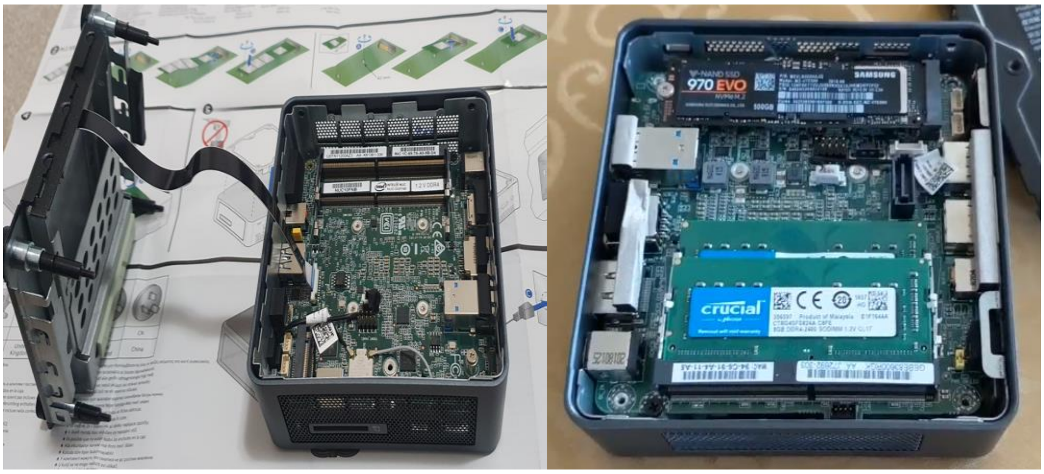


Figure 13: RAM, SSD, and HD Assembly within NUC Server

2.3.1.3 Firewall/Router

Router works at Network Layer (Layer-3) of the OSI layer model. It is a networking device, capable of routing traffic between network boundaries. Routers are widely used in Wide Area Network (WAN) and LAN. Any form of data at Layer-3 is termed as ‘Packets’. The router maintains the routing table and forwards the packets based on routing entries present in the routing table. The router supports static and dynamic routing that helps in forwarding the data packets to its appropriate destination. A router can learn routing entries dynamically with the help of dynamic routing protocols such as RIP, OSPF, ISIS, and BGP.

Netgate SG-1100 pfSense was used as a firewall/router device. pfSense stands for packet filtering sense. A firewall device is used to perform traffic filtering actions. Netgate device runs pfSense software which is based on FreeBSD. This device can provide gigabit (1000 Mbps) throughput with basic routing process (without VPN) and serves as a good device for small businesses and residential users. The primary function of Netgate device is to act as a firewall and accordingly, allow or block the traffic between different networks. The software pfSense supports a wide variety of protocols that are required to design a network from scratch. pfSense software is versatile and has an inbuilt routing and switching platform. This device can be managed via a user-friendly web interface called WebGUI. Users can also control the device using a shell terminal using the SSH service. pfSense is a stateful firewall machine, which essentially means that it maintains the state table about the connections flowing through the firewall such that reply traffic can be permitted automatically. This approach dramatically reduces the look-ups and hence increases the overall system performance. pfSense supports block and reject action to disallow the traffic and it is very important to decide between both actions. A network admin is required to possess expertise of the network and traffic stream, which will essentially help to decide which traffic to allow and which traffic to disallow between network boundaries. Netgate device has 1 WAN, 1 LAN, 1 OPT port, 2 USB ports, 1 GB DDR4 RAM onboard, and a reset button to perform factory default actions. The SG-1100 security gateway appliance with pfSense Plus software is an excellent compact device for home and small office networks. SG-1100 is a system-on-chip (SOC) and has pfSense software that runs on a Marvel hardware chipset. It may operate completely unnoticed on a desktop or wall due to its small form factor, low power use, and silent operation. It supports L3 forwarding, firewalling, and VPN features, which is sufficient for configuring community networks. SG-1100 is a much smaller package with a small power unit that is compatible to fit in small racks as Nimble and can be utilized for research-related projects. In summary, this firewall device has an excellent form factor, and it provides the performance and flexibility that is expected from a secure networking device.

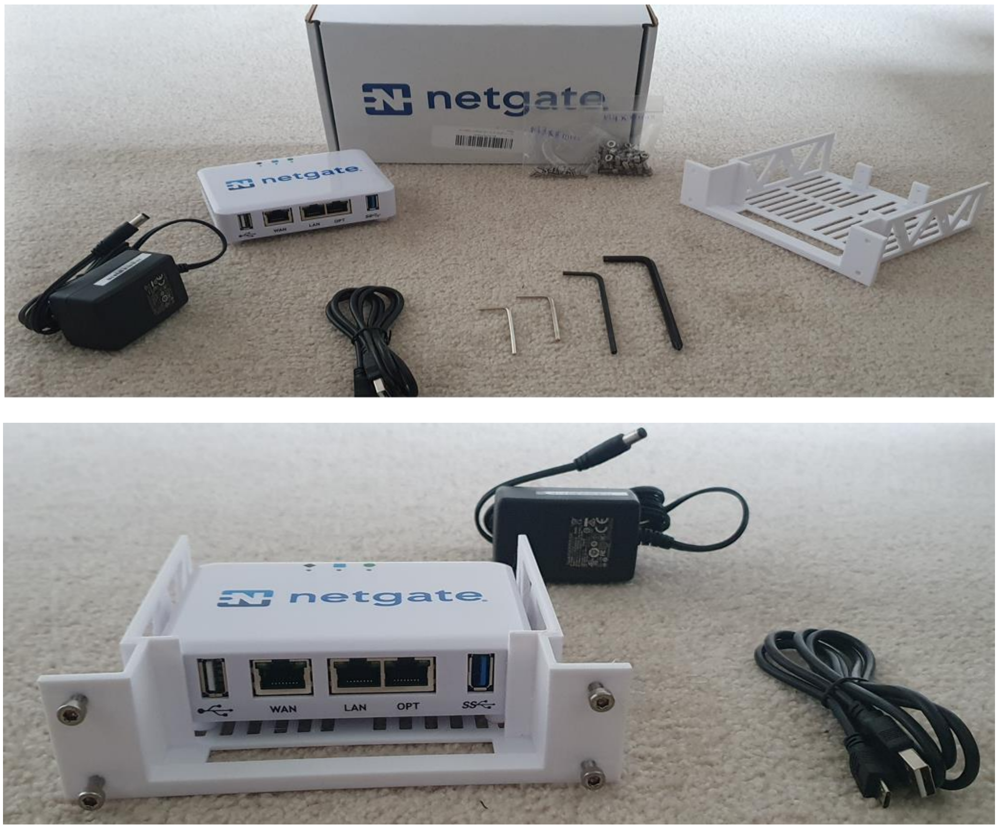


Figure 14: Netgate SG-1100 pfSense Firewall Assembly

2.3.1.4 Switch

Switch is a most common networking device. As per the OSI layer model, the switch operates at Layer-2 (Data Link Layer) and performs Layer-2 switching. Any form of data at Layer-2 is called 'Frames'. This device forwards the frames within network boundaries i.e., from one device to another. Switches are widely used in LAN and maintain the Media Access Control Address (MAC) table of all the devices participating in LAN. Switch forwards the frames based on based on the destination MAC address in the received frame. The basic action of switch includes flooding, learning, and forwarding. This switch has total of 5 GbE RJ45 ports, out of which 4 are 802.3at PoE+ ports and 1 is 802.3bt PoE++ input. Also, the switch comes with a reset button to perform factory default actions, if needed. The switch can be controlled using UniFi Network Application or shell terminal via SSH service. All UniFi equipment can be managed using a single interface, which offers intuitive configuration options, as well as robust device control and monitoring.

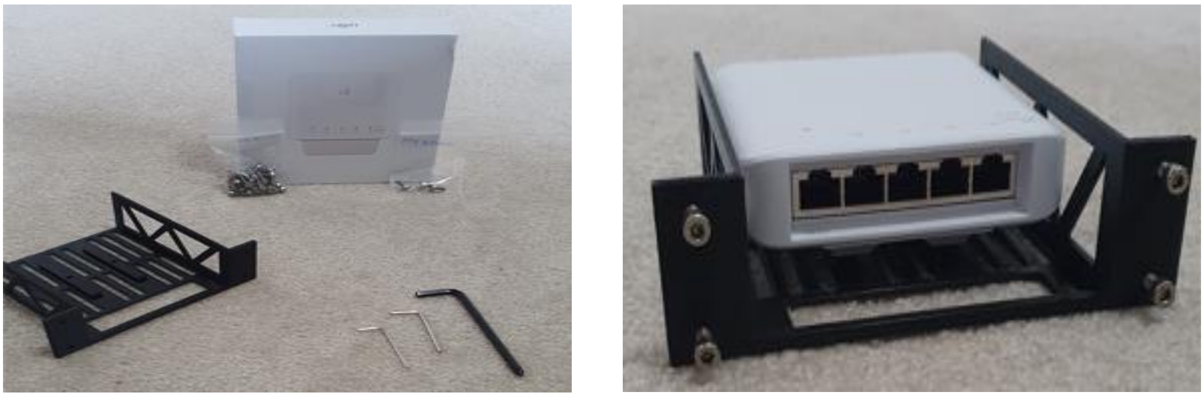


Figure 15: UniFi Switch (USW-Flex) Assembly

2.3.1.5 Patch-Panel

Keystones are arranged in a 3D printed shelves that have 5 jacks to hold these keystones to form a compact-looking patch-panel. A patch panel is a multi-port piece of hardware that helps to arrange and organize a set of cables. These keystones offer a double female CAT6 keystone that can be used with Cat.6, Cat5, CAT5e Ethernet cables. It can be used as an inline coupler for building small community networks, home networking, home office, and more.

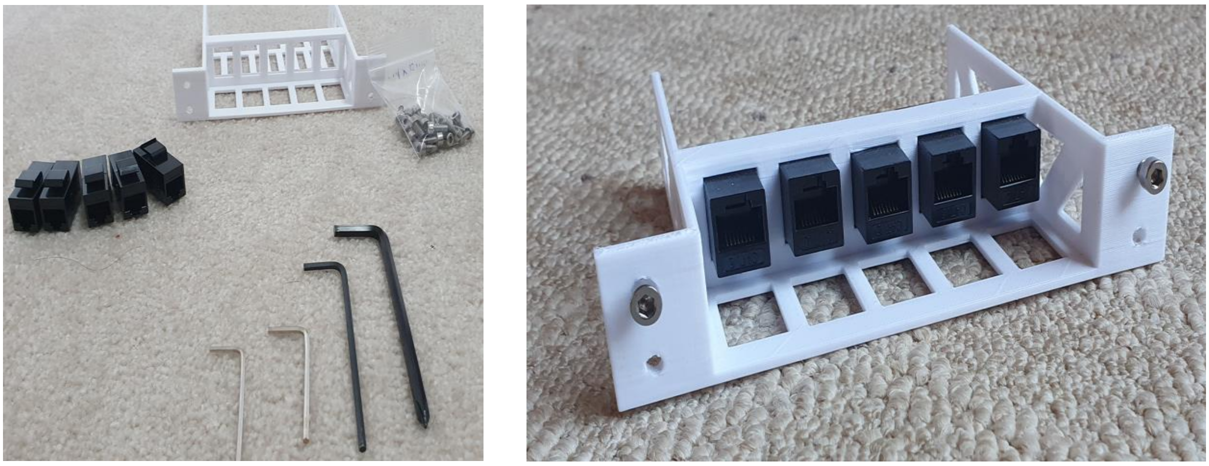


Figure 16: Patch-Panel (Keystones) Assembly

2.3.1.6 Access-Point

Access-point (AP) is a networking device that connects digital device with the LAN and facilitates communication with the end-user. It essentially creates a WLAN, typically used in an office or large buildings. AP usually broadcasts the Service Set Identifier (SSID), which is nothing but the network's name. Users connect their digital devices to access points to navigate the web and access the Internet. These SSIDs are available once users open the list of available Wi-Fi networks on their digital devices like Mobile Phones, Laptops, Tablets, etc. An AP connects to a router or switch with an Ethernet cable and distribute a good range of Wi-Fi signal to a designated area. AP can be controlled using UniFi Network Application or shell terminal via SSH service. UniFi Mesh AP offers dual-band (2.4 GHz and 5 GHz) support and offers 2 omnidirectional antennas to provide extensive 360-degree coverage. It is a high-performance, outdoor-ready 802.11ac Wi-Fi access point, capable of reaching 1.1+ Gbps throughput. It has a single POE port that must be powered with either 802.3af PoE or 24V passive PoE.

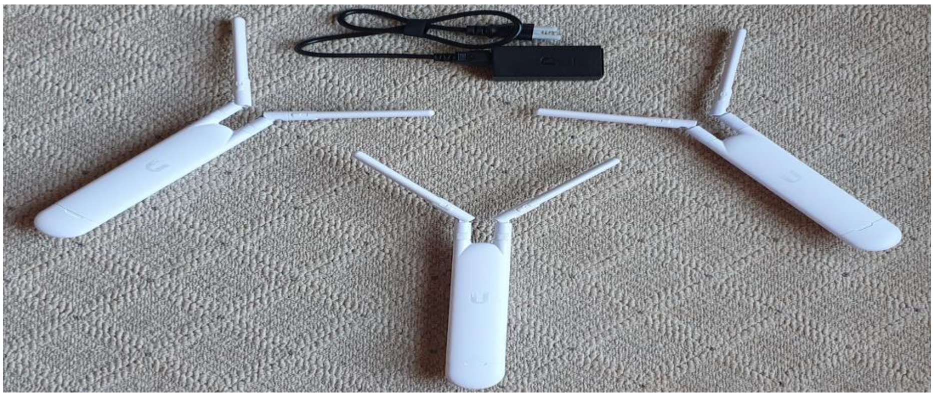


Figure 17: UniFi Access-Points (UAP-AC-M) Assembly

2.3.1.7 Loader Case

Pelican 1430 unit has been used as a top-loading case. It is a unique loading case with a dimension of 13.6"×5.8"×11.7". The case is strong and has a good form factor. It has comfortable rubber over handles, easy to operate double throw latches, and contains stainless steel hardware with a padlock protector. It automatically balances the interior pressure with an automatic pressure equalization valve. It comes with a shoulder strap and serves as a perfect fit to hold the Nimble unit and travel distances to promote 'offline first' ideology.

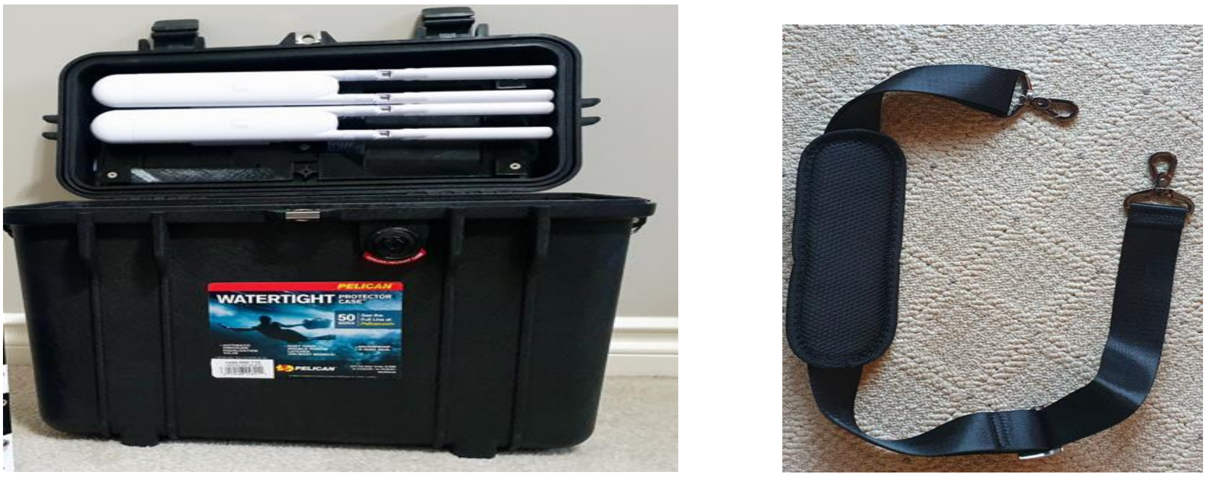


Figure 18: Pelican 1430 Protector Case

2.3.1.8 Shelves and Legs

A typical rack is formed using nearly 15 different shaped shelves and legs. With the help of various screws and bolts (different in sizes), a functional networking rack is built. These components are printed using a Prusa 3D printer. 3D object files (.stl) have been made with known dimensions and precision. All legs and shelves that are required to build a single nimble unit can be printed in about 2 or 3 days of printing job. There are a total of 8 shelves and 4 pillars to hold the unit tightly within the structure.

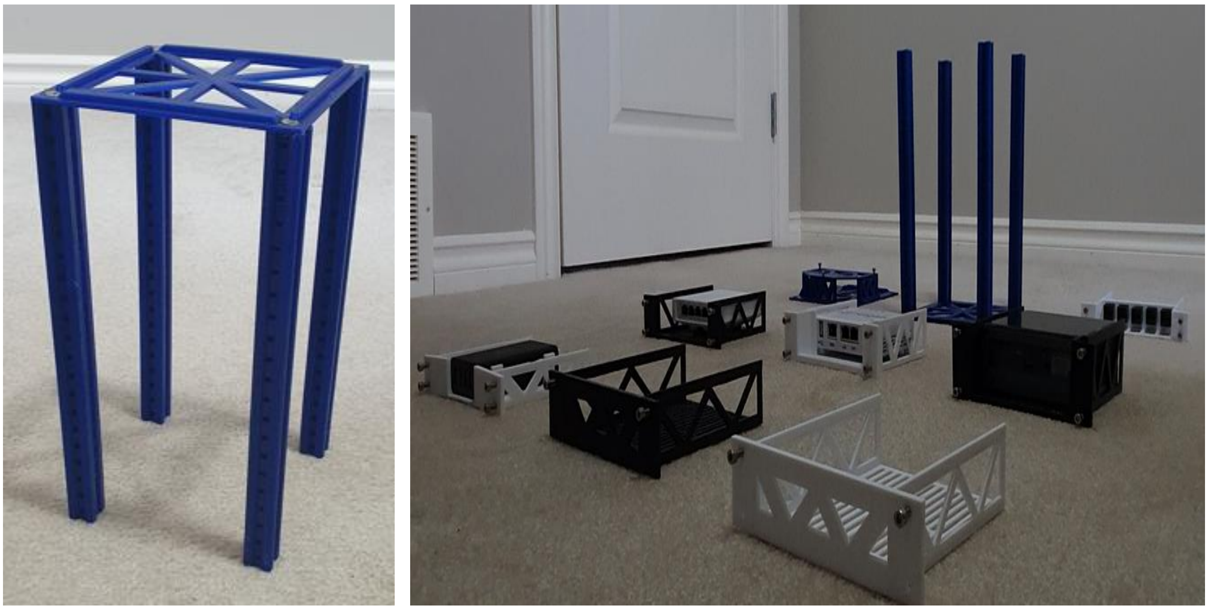


Figure 19: 3D Printed Shelves and Legs Assembly

2.3.1.9 AC Power Supply

Trond AC power supply is then mounted at the back of the Nimble unit. This component is a single power source for the Nimble kit. Power cords and adaptors from individual devices (server, switch, firewall, etc.) are plugged into the Trond power supply. This power bar has 4 typical 3-pin female adaptors slots and 4 USB ports that eliminate the need for multiple chargers. It comes with a 6-foot extension cord to help avoiding tangled cords.

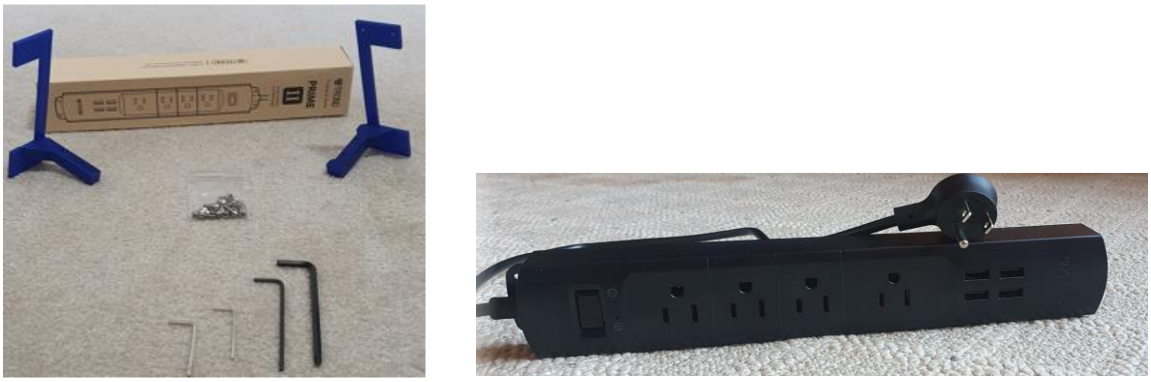


Figure 20: Trond Prime II Power Strip Assembly

2.3.1.10 Power Bank

Omni 20+ power bank has been used as a secondary source of power supply in case the primary source is not able to serve the power to the Nimble unit. This device is smart and highly portable. It has the capability of powering multiple devices at the same time. Omni power bank is equipped with a 100W AC outlet, high powered 60W USB-C port, 150W DC port, 2 USB-A ports, and wireless charging point. It also has a compact screen where it displays the parameters like leftover battery, total power consumption and number of devices connected, etc.

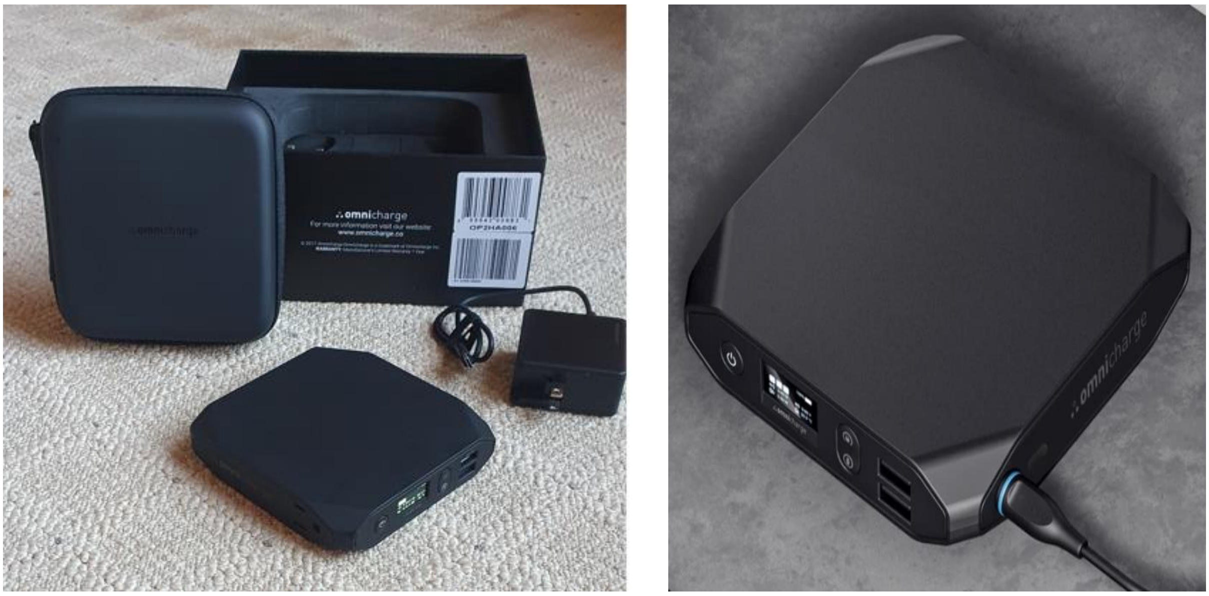


Figure 21: Omni Power Bank

2.3.1.11 Screws & Driver

There are multiple screws of different sizes that have been utilized to hold the shelves and legs to form a Nimble unit. The kit overall looks robust and represents a tight fit, hence the Nimble kit is highly portable. 4 screwdrivers have been used that helped to tighten the screws at appropriate places. Total 6 screw sizes have been used namely: M3x8mm (Flathead), M4x8mm, M4x8mm (flat-head), M4x10mm, M4x12mm, and M5x8mm (flat-head). The blue-colored screw measuring metric device can be used to find out the exact size of the screws.

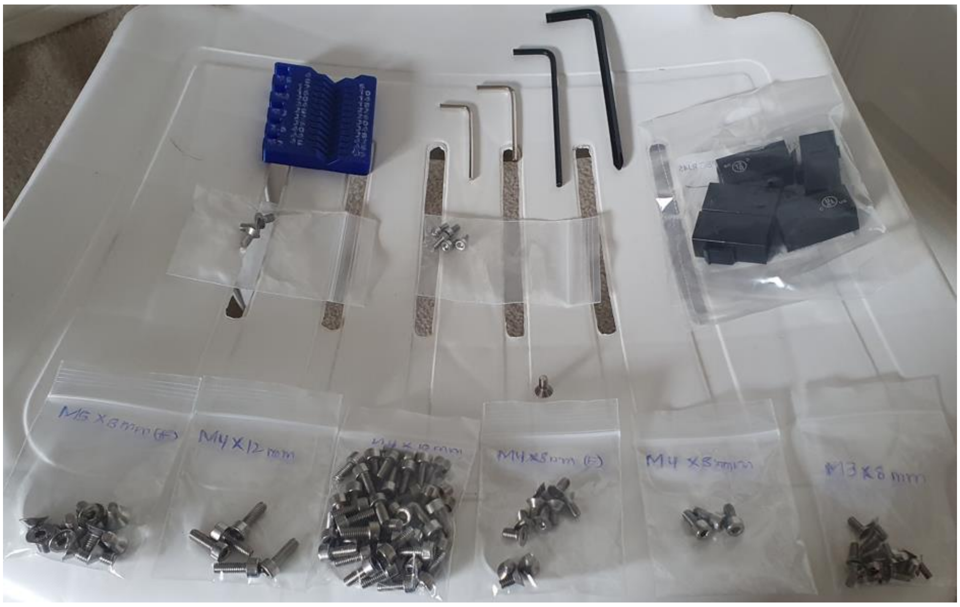


Figure 22: Screw Manifest

2.3.2 Operating System and Software Platform Configuration

As mentioned above, the proposed method is a bundled solution that requires hardware assembly and operation system (OS) installation. These individual components are assembled to form a 'Nimble' kit. Now, to maximize the efficiency of the system, OS and software selection is critical. Below facts provides detailed insights into these selections:

2.3.2.1 Operating System (OS)

There is a plethora of OS available in the market. An OS is one of the most important software that runs on a computer. An operating system acts as an interface between the user and computer hardware. It is a platform that takes human-level instructions and converts them into machine language, such that computer hardware can decipher it. The function of OS includes memory management, process management, security, file management, device management, and much more. It also coordinates between multiple software applications which run on a single machine. The operation of an OS is not limited since it also provides a variety of services like resource allocation, handles program execution, handles I/O operations, performs error detection and accounting. The operating system provides all these functions and services for the users' comfort and to make difficult tasks easier by running them in the background. All different kinds of operating systems are available online and provide similar kind of services, however internal logic, sequences, and programming may be different between multiple OS. Hence, the selection between the OS becomes crucial.

For this capstone project, multiple OS candidates have been critiqued based on their usage, efficiency, and end-user experience. There are many variants of OS that are readily available namely: Debian, Fedora, Kali, Ubuntu, Solus, OpenBSD, etc. There are more than 100 Linux distributions available online [30]. All these distributions are free and fall into the category of the open-source projects. This capstone project selects Ubuntu Server 20.04 LTS as the most appropriate based on the requirement of this project. Ubuntu server image (.iso) has been downloaded from its official website [31]. Ubuntu servers ensure security and stability. The Ubuntu OS has been around for many years now, which guarantees its reputation and market presence. It also comes with long-term support. Furthermore, it will be supported until 2025, and its Extended Security Maintenance (EMS) is deemed to be covered until 2030. From development to production, Ubuntu Server 20.04 LTS is an excellent choice for enterprise-class installations spanning public clouds, data centers, and the edge [32]. It offers security patches regularly and is consistent in providing the new LTS releases with critical bugs fixes and new feature development. Ubuntu server is an appropriate solution for the project fit, which would be required in the longer run to meet the scaling requirements in the Nimble deployment use case.

2.3.2.2 Software Platform

Software is a series of instructions or programs that tells the computer to execute a specific task. Software in generic terms is called as computer programs. Hardware is something that can be touched physically, however, the software is intangible because it is just a series of instructions to achieve a specific task. Hardware is virtually useless without software running on it.

For this capstone project, we have selected the open-source project that is being developed by Wakoma Incorporated Company. It is freely available on the GitHub website GitHub-Wakoma.

The name of the open-source project is ‘Lokal’, which is aimed to be platform agnostic. It is an open-source glue to stitch open-source services and applications together. ‘Lokal’ is a powerful platform put together to distribute services/content w/o the need of the Internet. The ‘Lokal’ platform/software can be used for content creation, curation, and sharing. It works on the ideology of making global footprints and is branded as ‘Lokal Services Global Impact’. With the help of hardware and OS, this platform can work in both offline and online modes of operation. ‘Lokal’ is a customizable open-source software and service platform that allows communities and organizations to produce, consume, and interact offline or online. ‘Lokal’ platform is built to be offline first. This platform offers a wide variety of services that enables Video & Audio Calling, Messaging, Music, E-learning, E-books, Network monitoring, Wikipedia, File-sharing, social networking, wireless network management, media streaming, collaborative document, and spreadsheet creation, etc. The platform is extremely easy to install and can be installed with the execution of a one-liner script. Currently ‘Lokal’ platform runs on modern Linux OS i.e., Ubuntu. This platform is an appropriate choice to cater the needs of remote communities like NWT where Internet connection is not reliable.

2.4 Implementation

There are a lot of individual pieces involved in building the Nimble kit i.e., hardware assembly and configuring each device (Server, Firewall/Router, Switch, and Access-Point) to form a big LAN that enables community networking. The end system should ensure access to services locally and connectivity should be accomplished while operating in offline (w/0 Internet) mode. The architecture diagram of the NUC server that is running Ubuntu (OS) and the ‘Lokal’ platform to deliver access to local services can be viewed from figure 23. The overall implementation is briefly discussed in the below 2 sections, which explains hardware assembly, configuration settings, and provisioning execution flow:

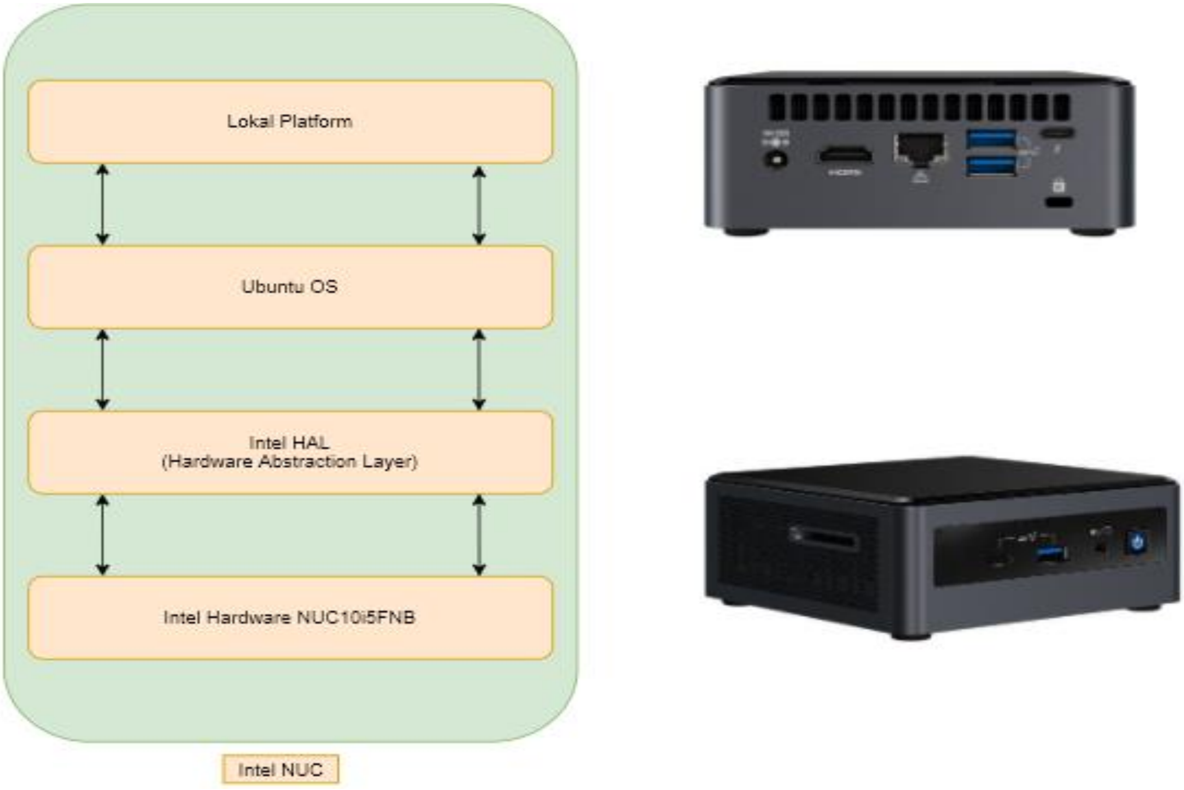


Figure 23: Top-Level Server Architecture

2.4.1 Hardware Assembly

2.4.1.1 Pre-requisites

- Arrange screws of different sizes and screwdriver with hex bits on the table
- Use a screw metric measurement device to measure the size of each screw
- Screwdriver and hex bits are useful for performing screw tightening
- 2 screws from the front of the shelf, 4 screws from the bottom and top of the Nimble unit, are sufficient to hold the shelves and kit tightly within the vertical structure
- Put 2 screws in all shelves from front side of the shelf. It comes in handy at a later stage
- Start building the kit from bottom to top. Prepare each shelf/rack individually

2.4.1.2 Building the Nimble Structure

For reference, a video link is added below that demonstrates the hardware assembly. It is clear and any novice can build a Nimble unit effortlessly.

As mentioned in the pre-requisites section, after arranging all the pieces of stuff on ground-zero, Nimble kit can be built in below easy steps:

Note: After each step, tightening 2 screws from the front of the shelves is a must.

- Start with base and hook it with 4 pillars, such that it forms a shape of an empty rack
- Insert 2 empty stuff shelves
- Insert the shelf with a USB hub
- Insert the shelf with Intel NUC server
- Insert the shelf with Netgate SG-1100 pfSense firewall/router
- Insert the shelf with UniFi switch
- Insert the shelf with patch-panel
- Close the kit from the top using shelf Closner and screw it up with 4 flat-headed screws
- Prepare the topmost rack (half-open) to hold the Omni power bank
- Screw the legs vertically at the back of the Nimble unit to hold the Trond power strip

Ayush-Nimble-Assembly.mp4

2.4.2 Provisioning and Testing Execution Flow

For the sake of understanding and briefly emphasizing each stage, this section is further divided into 10 stages:

2.4.2.1 Stage 1: Installing Ubuntu on NUC server

- Download the latest Ubuntu LTS server .iso image from the Ubuntu-Server link
- Create the bootable media using Rufus or Etcher
- Plug bootable USB stick, wired keyboard, and mouse into the NUC
- Connect the Internet cable within the NUC and turn it on
- The installation process will start automatically. To adjust any settings, press F10 to enter in the boot menu
- Select the USB memory stick (UEFI)

- Select ‘Install Ubuntu Server’
- Select Language and Layout. Note: There is a possibility that installation directly starts from this step onwards
- Select the network cable (eno1). Click on edit IPv4 and select the auto DHCP option
- Click done for further instructions
- Select the right disk:
    - 10th Gen NUC model has a space for SSD cards. Select 500 GB Samsung SSD
    - 8th Gen NUC model doesn’t have a space for SSD cards. Select WD 2TB HDD
- Click done and continue for further instructions
- Choose appropriate credentials: your name, server name, username, and password
- Install OpenSSH server. Press the spacebar key to select the same
- Nothing else requires installation, click Done to continue
- Select reboot and hit enter. Remove the USB stick
- NUC will boot and take 2 or 3 minutes to come up
- Use the username and password to login to the NUC server

2.4.2.2 Stage 2: Provisioning WireGuard (WG) on NUC server

- Create a user (client) on nextcloud with a username and password
- Generate WG keypairs on the server
- Make proper WG client configuration file with keys and all necessary parameters. Upload ‘wg0-client.conf’ file to the ‘client-bundle’ folder
- Share the same file (wg0-client.conf) to the newly created user
- Add the client at server-side under /etc/wireguard/wg0.conf file
- Execute the WG install script at client side: bash <(curl -Ls get.lokal.network/wg)
- Sync the WG configs: ‘wg syncconf wg0 <(wg-quick strip wg0)’
- Verify WG tunnel status using ‘wg show’ command. Try pinging client from the server
- If the WG status is not UP. Restart the WG service: ‘systemctl restart wg-quick@wg0’
- Note:
    - This process is quite easy for clients. The client is merely required to execute a one-liner WG install script. Upon execution, the client will get the client config file and WG neighborship will be established automatically.
    - WG service is required to remotely manage the NUC server for extra services add-ons and performing troubleshooting in the future.

2.4.2.3 Stage 3: Installing ‘Lokal’ platform remotely

- Become a root user using the ‘sudo -i’ command
- Execute the one-liner script: bash <(curl -Ls kutt.it/lokal) to install ‘Lokal’ platform
- Enter nextcloud username and password
- The script will automatically install necessary packages, utilities, services, and content in the background without manual human intervention
- The requirement of DNWT project is to install only 4 services namely: Jitsi, Jellyfin, WordPress, and UniFi-Controller. Hence, most of the ‘Lokal’ installation are handled remotely using WG service, as these are custom installs.

2.4.2.4 Stage 4: Wiring

- Power UBQ POE: Connect the power cord from Ubiquiti POE to the main power brick
- Power Switch: Connect Switch port-1 to Ubiquiti POE
- NUC Connection: Connect Switch port-2 to patch panel-2. Then, patch panel-2 to NUC
- pfSense Connection: Connect Switch port-3 to pfSense LAN port
- Access Point Connection: Connect Switch port-4 to AP
- Device Connection: Connect pfSense OPT port or Switch port-5 to a device (laptop/PC) and monitor DHCP leasing process
- Make sure that NUC server, pfSense, Ubiquiti POE, Switch, and Access-Point is powered on

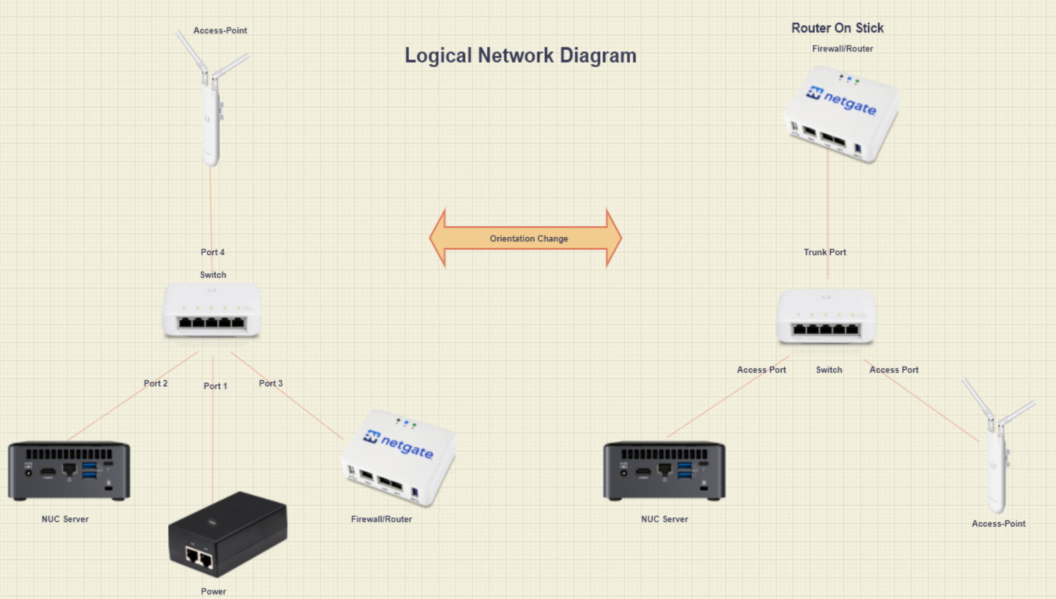


Figure 24: Logical Network Diagram

2.4.2.5 Stage 5: Configuring Firewall/Router (Netgate SG-1100 pfSense)

- Open 192.168.1.1 (default IP address of pfSense) on the browser
- Enter credentials: admin/pfSense on the pfSense dashboard
- Skip the set-up wizard by clicking next
- Navigate to Diagnostics > Backup & Restore
- Upload the DNWT-pfSense.conf XML file
- Click on ‘Restore Configuration’
- Click yes on ‘Are you sure you want to restore the configuration?’
- The device will automatically reboot and boot up with DNWT specific configs
- Wait 1-2 minutes, then open 192.168.5.1 (new IP address of pfSense) on the browser
- Enter new credentials: admin/dnwt@123 on the pfSense dashboard
- Note: DNS resolver requires config changes to access ‘lokal’ services. Depends on the nature of set-up execution/workflow. Check DHCP lease of the server

2.4.2.6 Stage 6: Configuring UniFi Switch and Access-Point

- Switch and access points can be configured using ‘UniFi Network Application’ called the controller

- Access the UniFi controller by opening ‘unifi.lokal.network’ in the browser
- Click on ‘Restore from Backup’ on the set-up wizard page
- Upload the DNWT-controller.unf file
- Controller will reboot automatically. Wait for 1 minute and the controller login page will be loaded automatically
- Enter credentials: dnwtadmin/digitalNWT@123 on the controller login page
- Check the list of available options on left side and navigate to the ‘UniFi Device’ page
- Start the adoption process for switch and access-point separately
- Execute ‘set-inform http://192.168.x.x:8080/inform’ command with an appropriate IP address of the NUC server
- Once the adoption process is successfully done, confirm the ‘Green’ light and ‘Online’ status on the controller screen for each device

2.4.2.7 Stage 7: How to join Hotspot/Wi-Fi:

- After the successful deployment of the Nimble network, AP will broadcast below 2 SSIDs. Hence, 2 networks will be seen in the list of available networks:
  - DNWT-Staff-Network (Staff Network)
  - DNWT-Guest-Network (Guest Network)
- Open the list of available Wi-Fi on your system (Laptop/PC/Phone/Tablets)
- Click on the available network from the list of available/reachable Wi-Fi hotspots
- It will prompt to enter a Wi-Fi password to join the network
  - Password for DNWT-Staff-Network is 24faa699
  - Password for DNWT-Guest-Network is guest@123

2.4.2.8 Stage 8: pfSense Captive Portal Login

- After joining the Wi-Fi network, the system will redirect to the captive portal page
- There are 2 different captive portal pages i.e., defined one captive portal per network:
  - For Guest network, users can just accept the terms & conditions and start navigating to 'Lokal' services
  - For Staff network, users must enter the captive portal credentials (admin/dnwt@123) before navigating to 'Lokal' services
- Note: Bandwidth capping is done on available networks. The 'Staff' network does not have any bandwidth limitation whereas the 'Guest' network will have only 5 Mbps upload and download speed. Data capping is not done on any of the networks.

2.4.2.9 Stage 9: Testing Services

Any user connected to the Nimble will be able to access the 4 services mentioned in the below table. Users are required to enter the Uniform Resource Locator (URL) in the browser, this will allow access to the services.

Service Name	Usage	Domain-Name (URL)
WordPress	• Create a website, blog, or app, as per choice. • It is the landing page from where all the services can be accessed.	lokal.network
Jitsi	• Secure, flexible & completely free video-conferencing application.	meet.lokal.network

Jellyfin	• Volunteer-built media solution that puts you in control of your media. Stream media to any device.	video.lokal.network
UniFi Controller	• Network Management Software that binds gateways, switches, and wireless access points together with one graphical front end. • Not open source.	unifi.lokal.network

2.4.2.10 Stage 10: How to test 'Lokal' services in offline mode?

- Turn on the power of your Nimble unit
- Open the list of available Wi-Fi on your device
- Join any of the available DNWT networks using the credentials mentioned above
- Enjoy out-of-the-box services i.e., Jitsi, Jellyfin, WordPress, and UniFi-Controller in both online and offline mode of operation. There are 2 methods to access services:
  - The first method is as follows. After connecting to any one of the 2 available DNWT networks, the system will automatically redirect the user to WordPress (WP) landing page. Users will be able to access services using soft links mentioned on the WordPress (WP) landing page.

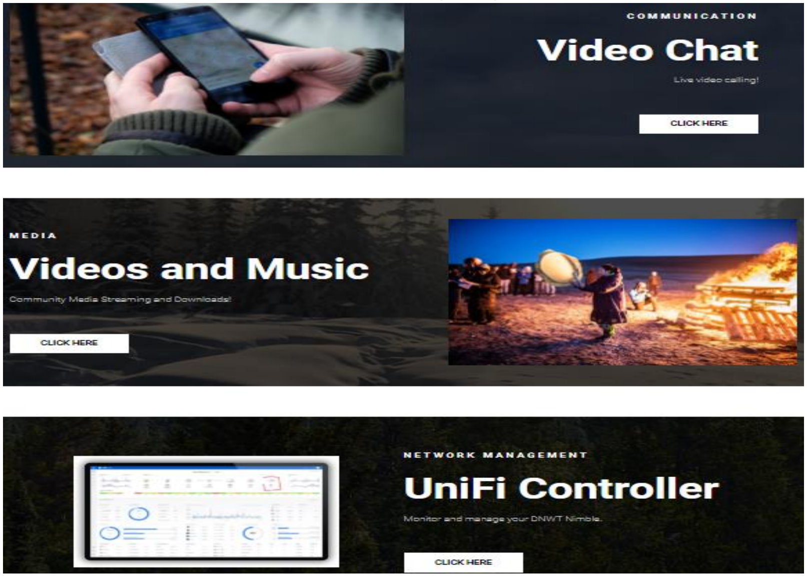


Figure 25: Service Access via WP Landing Page (Automatic Method)

  - The second method is as follows. Simultaneously any connected user can manually type the domain name (URL) in the URL section of the browser to access the services.

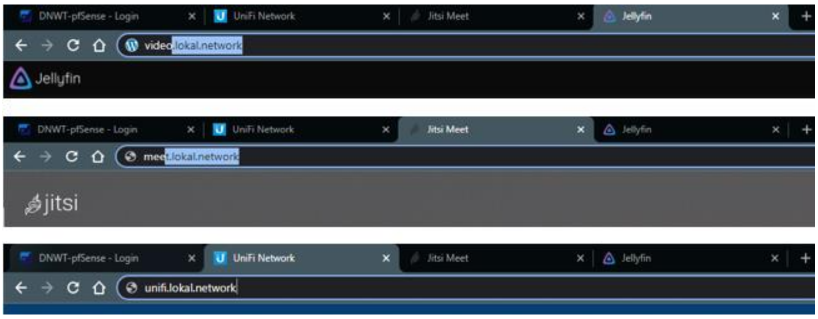


Figure 26: Service Access via Domain-Name (Manual Method)

- Note that pfSense does not have a WAN (Internet) connection, hence Nimble is operating in totally offline mode.

3 Configuration, Testing Logs, and Performance Evaluation

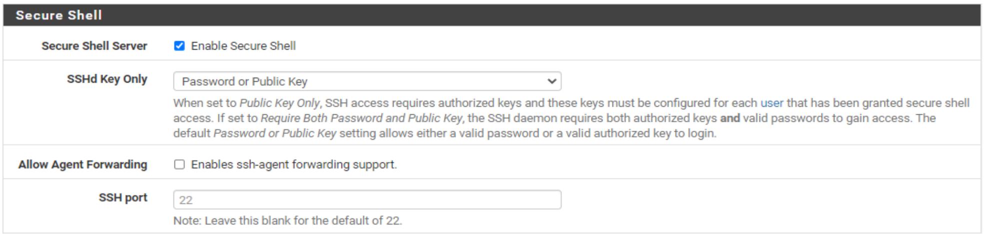
Following each principle and fundamental details are a must while designing an efficient networking system. A few thumb rules in this context have been elaborated in the below sections. The significance of protocols and running configurations on pfSense, and controller are also briefly discussed. These are the bare minimum configurations required to set-up the Nimble environment. Once the set-up is configured as explained below, the user will be able to access services while being totally disconnected from the Internet.

3.1 Must-to-have pfSense Configurations:

There is always a set of necessary configurations required on routers while setting up a LAN network. Basic configurations required for pfSense in Nimble environment are outlined below:

- 3 VLANs have been created i.e., VLAN-10, 20, and 30 to introduce an extra layer of security. VLAN creations significantly reduce the size of broadcast domains. It makes network management easier, improves performance, and reduces latency

- SSH service is enabled to control pfSense via secure shell access



Secure Shell

Secure Shell Server: ☑ Enable Secure Shell

SSHd Key Only: Password or Public Key

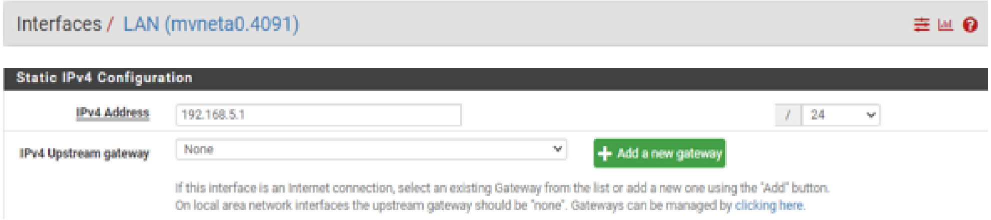
When set to *Public Key Only*, SSH access requires authorized keys and these keys must be configured for each user that has been granted secure shell access. If set to *Require Both Password and Public Key*, the SSH daemon requires both authorized keys **and** valid passwords to gain access. The default *Password or Public Key* setting allows either a valid password or a valid authorized key to login.

Allow Agent Forwarding: □ Enables ssh-agent forwarding support.

SSH port: 22

Note: Leave this blank for the default of 22.

- Static IP address (192.168.5.1) has been configured on the LAN interface. The DHCP server pool values have been automatically adjusted to a new range



Interfaces / LAN (mvneta0.4091)

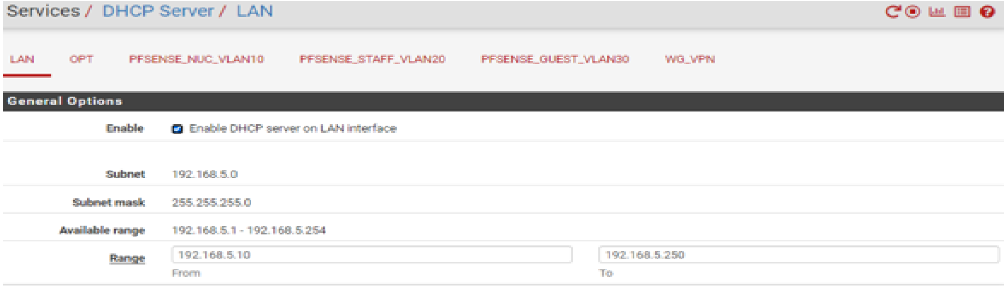
Static IPv4 Configuration

IPv4 Address: 192.168.5.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

- DHCP server is running on each interface LAN, OPT, and manually created VLANs



Services / DHCP Server / LAN

General Options

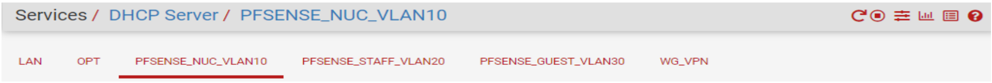
Enable: ☑ Enable DHCP server on LAN interface

Subnet: 192.168.5.0

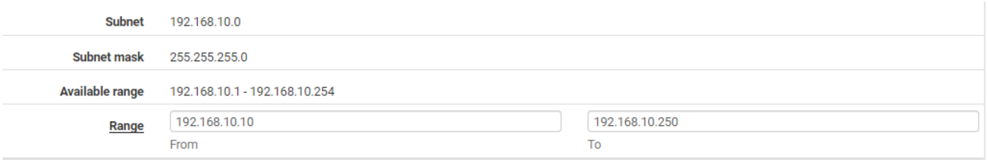
Subnet mask: 255.255.255.0

Available range: 192.168.5.1 - 192.168.5.254

Range: From 192.168.5.10 To 192.168.5.250

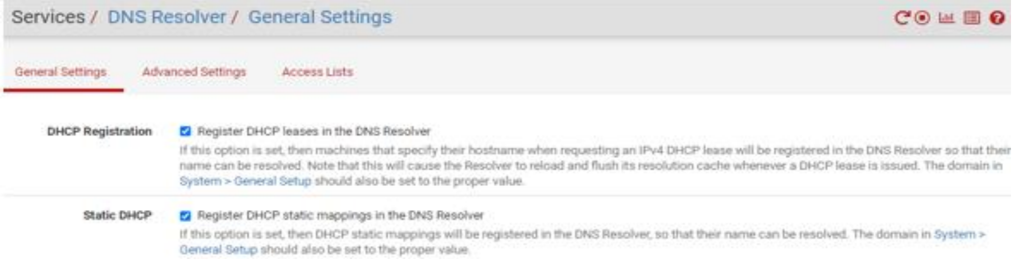


Services / DHCP Server / PFSENSE_NUC_VLAN10



Subnet	192.168.10.0	
Subnet mask	255.255.255.0	
Available range	192.168.10.1 - 192.168.10.254	
Range	192.168.10.10 From	192.168.10.250 To

- DHCP server is running in conjunction with DNS. This means, allocated leases are getting registered in /etc/hosts file automatically to ensure fast operations



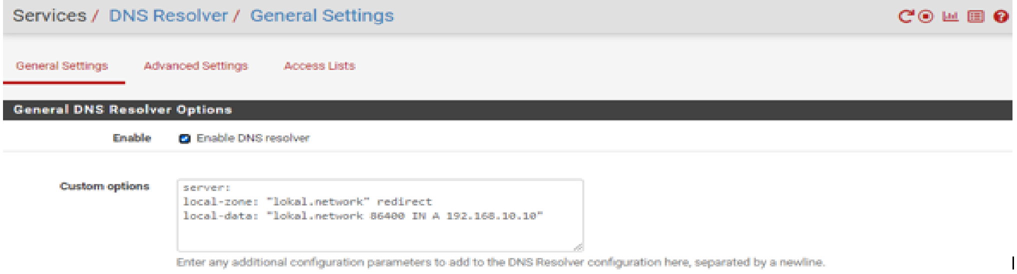
DHCP Registration: ☑ Register DHCP leases in the DNS Resolver

If this option is set, then machines that specify their hostname when requesting an IPv4 DHCP lease will be registered in the DNS Resolver so that their name can be resolved. Note that this will cause the Resolver to reload and flush its resolution cache whenever a DHCP lease is issued. The domain in System > General Setup should also be set to the proper value.

Static DHCP: ☑ Register DHCP static mappings in the DNS Resolver

If this option is set, then DHCP static mappings will be registered in the DNS Resolver, so that their name can be resolved. The domain in System > General Setup should also be set to the proper value.

- DNS resolver has been configured with a custom advanced option to cater wildcard DNS entry i.e., ‘*.lokal.network’



General DNS Resolver Options

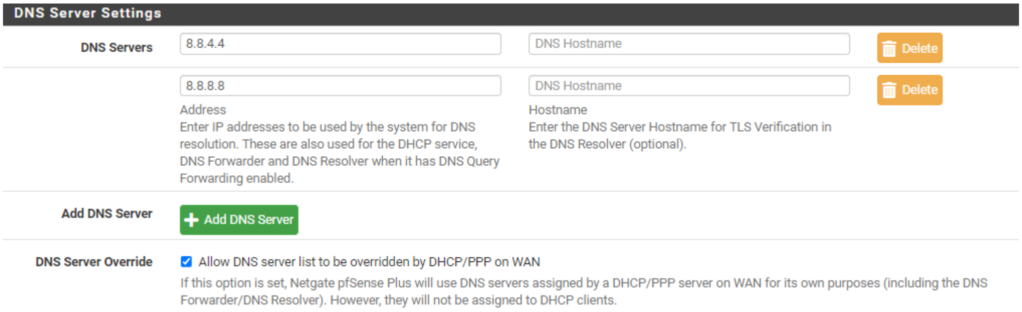
Enable: ☑ Enable DNS resolver

Custom options:

```
server:
local-zone: "lokal.network" redirect
local-data: "lokal.network 86400 IN A 192.168.10.10"
```

Enter any additional configuration parameters to add to the DNS Resolver configuration here, separated by a newline.

- DNS server has been configured with manual entries 8.8.8.8 and 8.8.4.4 (google DNS records). Also, ‘Allow DNS server list to be overridden by DHCP/PPP on WAN’ setting has been enabled that overrides entries with entries served to DHCP clients running on the WAN interface



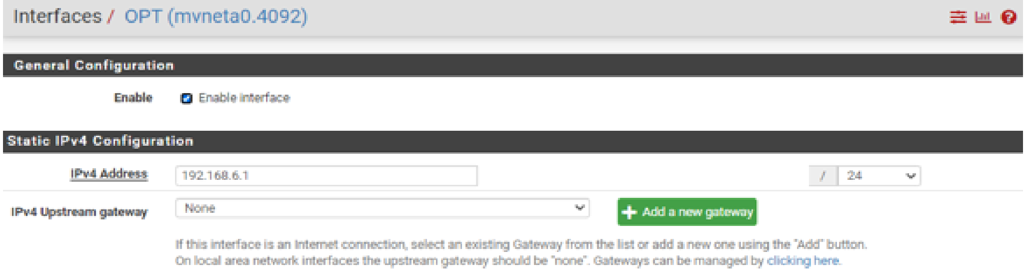
DNS Server Settings

DNS Servers	8.8.4.4	DNS Hostname	Delete
	8.8.8.8 Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.	DNS Hostname Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).	Delete
Add DNS Server	+ Add DNS Server		

DNS Server Override: ☑ Allow DNS server list to be overridden by DHCP/PPP on WAN

If this option is set, Netgate pfSense Plus will use DNS servers assigned by a DHCP/PPP server on WAN for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

- OPT interface has been enabled for troubleshooting purposes. Firewall rules on this interface are loosely bound for debugging



General Configuration

Enable: ☑ Enable interface

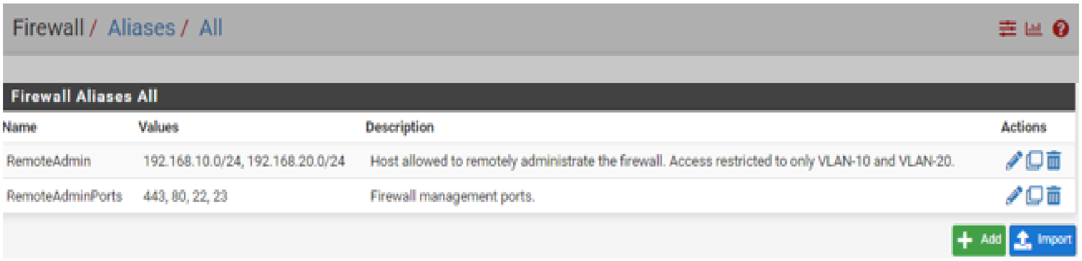
Static IPv4 Configuration

IPv4 Address: 192.168.6.1 / 24

IPv4 Upstream gateway: None

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Gateways can be managed by clicking here.

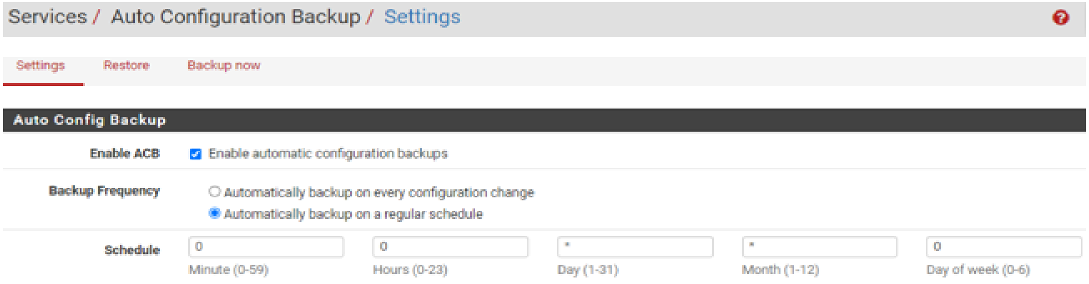
- Firewall Aliasing feature has been used to define group ports and networks. This results in significantly shorter, self-documenting, and more manageable rulesets



Firewall Aliases All

Name	Values	Description	Actions
RemoteAdmin	192.168.10.0/24, 192.168.20.0/24	Host allowed to remotely administrate the firewall. Access restricted to only VLAN-10 and VLAN-20.	
RemoteAdminPorts	443, 80, 22, 23	Firewall management ports.	

- Auto-Configuration Backup (ACB) is configured to ensure frequent device backups. ACB is designed to take weekly backup and the same is stored in the system's memory



Auto Config Backup

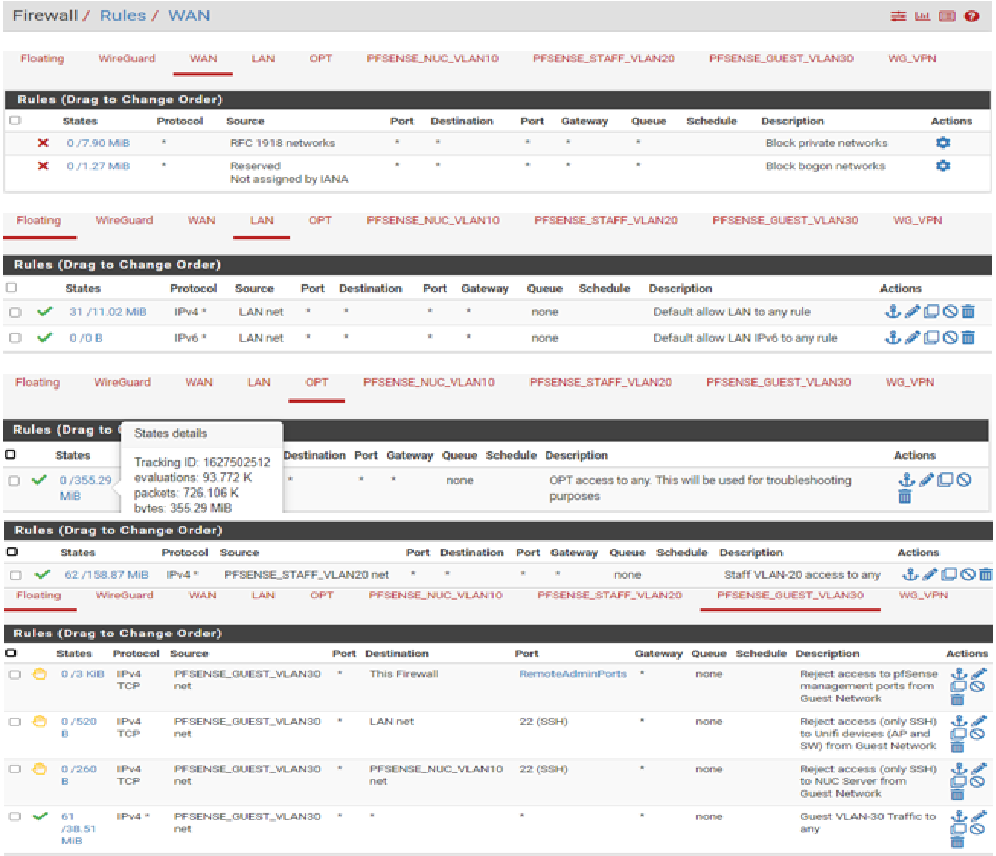
Enable ACB ☑ Enable automatic configuration backups

Backup Frequency ○ Automatically backup on every configuration change
● Automatically backup on a regular schedule

Schedule

0	0	*	*	0
Minute (0-59)	Hours (0-23)	Day (1-31)	Month (1-12)	Day of week (0-6)

- The thumb rules behind firewall rule creation are discussed below [33]:
  - pfSense is a stateful firewall. This means that outbound rules are never required, because filtering is applied on the inbound direction of every interface
  - The default ingress policy on the WAN interface is to block all traffic. Hence, traffic from outside of the LAN network which is generated on the Internet will be blocked
  - This potentially means, everything inbound from the Internet is denied, and everything out to the Internet from the LAN is permitted
  - Permit only what a network requires and avoid leaving the default allow all rules on the LAN interface
  - Firewall rules on interface tabs are applied on a per-interface basis and works always in the inbound direction on that interface
  - Most importantly, pfSense firewall works on the default deny rule. This means, rules that do not have a match to any user-defined rules nor to any other automatically generated rules will be silently blocked by the default deny rule
- In Nimble network, Firewall rules are designed to achieve a fine grade of granularity:
  - WAN interface: All rules are 'default' on this interface. Traffic originating from the Internet will be blocked by default
  - LAN interface: All rules are 'default'. It allows all devices participating in LAN to access the Internet, 'Lokal' services and communicate with each other
  - OPT interface: Same rules as on LAN interface
  - PFSENSE_NUC_VLAN10: Same rules as on LAN interface
  - PFSENSE_STAFF_VLAN20: Same rules as on LAN interface
  - PFSENSE_GUEST_VLAN30: Strict firewall policies are designed for this network. Services like SSH, Telnet, HTTP, HTTPS, etc. are blocked. Internet access and DNS related traffic are permitted to access 'Lokal' services



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0 /7.90 MiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0 /1.27 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	31 /11.02 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ❐ ⊘ 🗑
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ❐ ⊘ 🗑

Rules (Drag to

States details

Tracking ID: 1627502512
evaluations: 93.772 K
packets: 726.106 K
bytes: 355.29 MiB

□		States	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /355.29 MiB	*	*	*	none		OPT access to any. This will be used for troubleshooting purposes	⚓ ✎ ❐ ⊘ 🗑

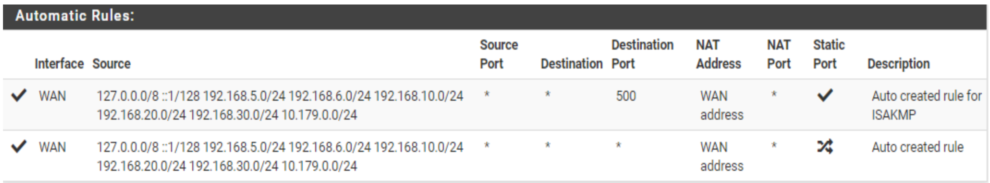
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	62 /158.87 MiB	IPv4 *	PFSENSE_STAFF_VLAN20 net	*	*	*	*	none		Staff VLAN-20 access to any	⚓ ✎ ❐ ⊘ 🗑

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✋	0 /3 KiB	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	This Firewall	RemoteAdminPorts	*	none		Reject access to pfSense management ports from Guest Network	⚓ ✎ ❐ ⊘ 🗑
□	✋	0 /520 B	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	LAN net	22 (SSH)	*	none		Reject access (only SSH) to Unifi devices (AP and SW) from Guest Network	⚓ ✎ ❐ ⊘ 🗑
□	✋	0 /260 B	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	PFSENSE_NUC_VLAN10 net	22 (SSH)	*	none		Reject access (only SSH) to NUC Server from Guest Network	⚓ ✎ ❐ ⊘ 🗑
□	✓	61 /38.51 MiB	IPv4 *	PFSENSE_GUEST_VLAN30 net	*	*	*	*	none		Guest VLAN-30 Traffic to any	⚓ ✎ ❐ ⊘ 🗑

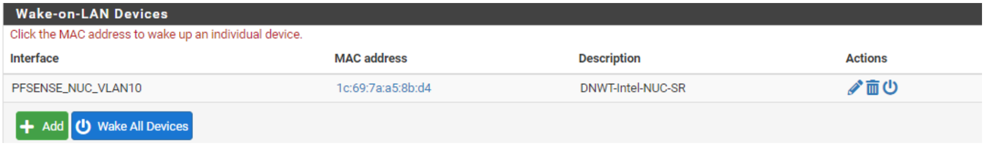
- NAT rules are working across network boundaries to ensure successful mapping of private to public IP addresses. These rules are generated automatically via the 'Automatic Outbound NAT' feature



Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.5.0/24 192.168.6.0/24 192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 10.179.0.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.5.0/24 192.168.6.0/24 192.168.10.0/24 192.168.20.0/24 192.168.30.0/24 10.179.0.0/24	*	*	*	WAN address	*	⤮	Auto created rule

- Wake-On-LAN (WOL) feature is enabled that helps in waking up the devices from a powered-off state by sending special 'Magic Packets'. This feature must be enabled locally per device



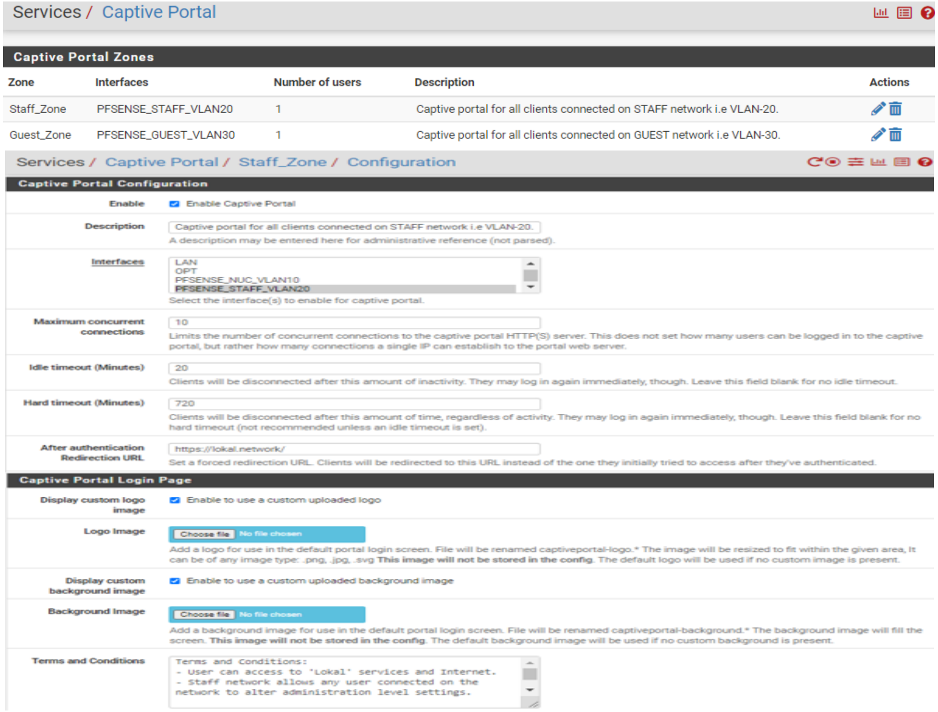
Wake-on-LAN Devices

Click the MAC address to wake up an individual device.

Interface	MAC address	Description	Actions
PFSENSE_NUC_VLAN10	1c:69:7a:a5:8b:d4	DNWT-Intel-NUC-SR	✎ 🗑 ⏻

- Captive Portal feature has been enabled to ensure authentication before granting access to the Internet and 'Lokal' services. pfSense device will automatically redirect to a login web page in which the user must enter credentials such as username/password, a voucher code, or a simple click-through agreement. This feature takes all connected users to <u>WordPress Landing Page</u> upon successful login. There 2 captive portal zones defined in Nimble per network:
  - Staff Zone for Staff network
  - Guest Zone for Guest network

- Bandwidth capping is done on available networks. However, there is no data capping done on any of the networks. The 'Staff' network does not have any bandwidth limitation whereas the 'Guest' network can access only 5 Mbps upload and download speed



Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
Staff_Zone	PFSENSE_STAFF_VLAN20	1	Captive portal for all clients connected on STAFF network i.e VLAN-20.	
Guest_Zone	PFSENSE_GUEST_VLAN30	1	Captive portal for all clients connected on GUEST network i.e VLAN-30.	

Services / Captive Portal / Staff_Zone / Configuration

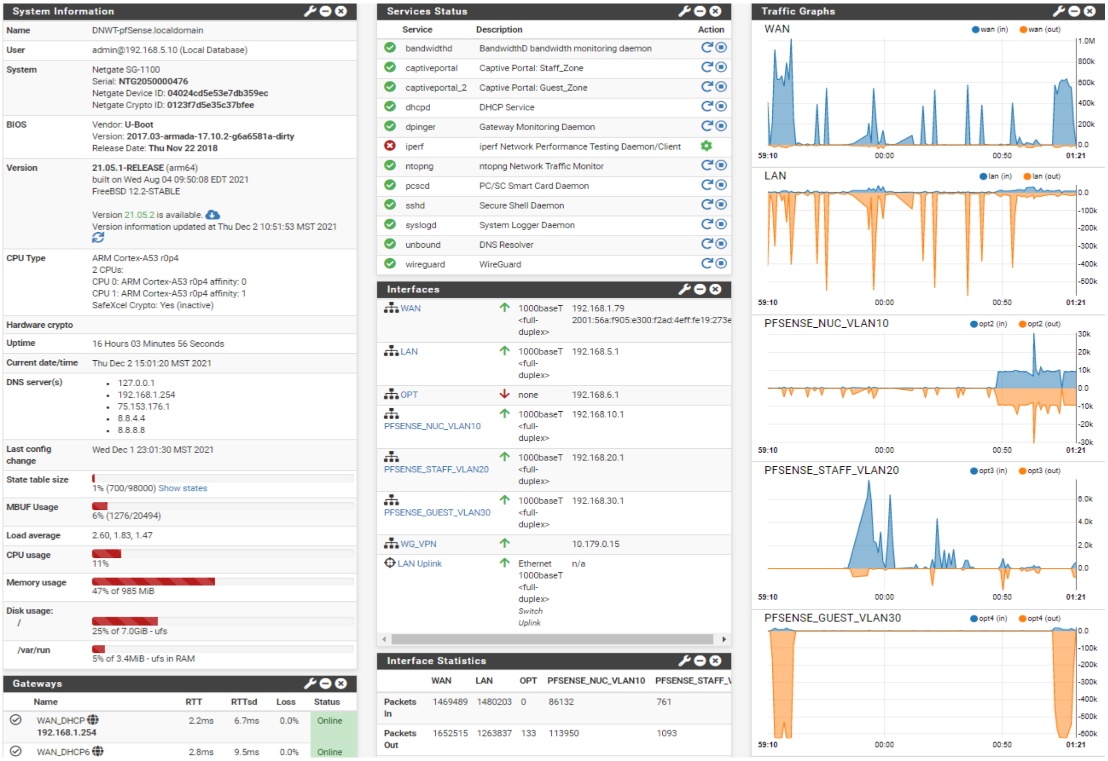
Captive Portal Configuration

Enable	☑ Enable Captive Portal
Description	Captive portal for all clients connected on STAFF network i.e VLAN-20. A description may be entered here for administrative reference (not parsed).
Interfaces	LAN OPT PFSENSE_NUC_VLAN10 PFSENSE_STAFF_VLAN20 Select the interface(s) to enable for captive portal.
Maximum concurrent connections	10 Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.
Idle timeout (Minutes)	20 Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.
Hard timeout (Minutes)	720 Clients will be disconnected after this amount of time, regardless of activity. They may log in again immediately, though. Leave this field blank for no hard timeout (not recommended unless an idle timeout is set).
After authentication Redirection URL	https://lokal.network/ Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

Captive Portal Login Page

Display custom logo image	☑ Enable to use a custom uploaded logo
Logo Image	Choose file No file chosen Add a logo for use in the default portal login screen. File will be renamed captiveportal-logo.* The image will be resized to fit within the given area, It can be of any image type: .png, .jpg, .svg **This image will not be stored in the config**. The default logo will be used if no custom image is present.
Display custom background image	☑ Enable to use a custom uploaded background image
Background Image	Choose file No file chosen Add a background image for use in the default portal login screen. File will be renamed captiveportal-background.* The background image will fill the screen. **This image will not be stored in the config**. The default background image will be used if no custom background is present.
Terms and Conditions	Terms and Conditions: - User can access to 'Lokal' services and Internet. - Staff network allows any user connected on the network to alter administration level settings.

- Dashboard customization feature has been utilized to display the important and useful information on the dashboard. System Information, Service Status, Traffic Graphs, Captive Portal Status, and Interface Statistics can be viewed on the front dashboard for quick references. This feature is convenient and comes in handy to perform troubleshooting during network outages



System Information

Name	DNWT-pfSense.localdomain
User	admin@192.168.5.10 (Local Database)
System	Netgate SG-1100 Serial: **NTG2050000476** Netgate Device ID: **04024cd5e53e7db359ec** Netgate Crypto ID: **0123f7d5e35c37bfee**
BIOS	Vendor: **U-Boot** Version: **2017.03-armada-17.10.2-g6a6581a-dirty** Release Date: **Thu Nov 22 2018**
Version	**21.05.1-RELEASE** (arm64) built on Wed Aug 04 09:50:08 EDT 2021 FreeBSD 12.2-STABLE Version 21.05.2 is available. Version information updated at Thu Dec 2 10:51:53 MST 2021
CPU Type	ARM Cortex-A53 r0p4 2 CPUs: CPU 0: ARM Cortex-A53 r0p4 affinity: 0 CPU 1: ARM Cortex-A53 r0p4 affinity: 1 SafeXcel Crypto: Yes (inactive)
Hardware crypto	
Uptime	16 Hours 03 Minutes 56 Seconds
Current date/time	Thu Dec 2 15:01:20 MST 2021
DNS server(s)	• 127.0.0.1 • 192.168.1.254 • 75.153.176.1 • 8.8.4.4 • 8.8.8.8
Last config change	Wed Dec 1 23:01:30 MST 2021
State table size	1% (700/98000) Show states
MBUF Usage	6% (1276/20494)
Load average	2.60, 1.83, 1.47
CPU usage	11%
Memory usage	47% of 985 MiB
Disk usage: /	25% of 7.0GiB - ufs
/var/run	5% of 3.4MiB - ufs in RAM

Gateways

	Name	RTT	RTTsd	Loss	Status
✓	WAN_DHCP **192.168.1.254**	2.2ms	6.7ms	0.0%	Online
✓	WAN_DHCP6	2.8ms	9.5ms	0.0%	Online

Services Status

	Service	Description	Action
✓	bandwidthd	BandwidthD bandwidth monitoring daemon	
✓	captiveportal	Captive Portal: Staff_Zone	
✓	captiveportal_2	Captive Portal: Guest_Zone	
✓	dhcpd	DHCP Service	
✓	dpinger	Gateway Monitoring Daemon	
✗	iperf	iperf Network Performance Testing Daemon/Client	
✓	ntopng	ntopng Network Traffic Monitor	
✓	pcscd	PC/SC Smart Card Daemon	
✓	sshd	Secure Shell Daemon	
✓	syslogd	System Logger Daemon	
✓	unbound	DNS Resolver	
✓	wireguard	WireGuard	

Interfaces

WAN	↑	1000baseT <full-duplex>	192.168.1.79 2001:56a:f905:e300:f2ad:4eff:fe19:273e
LAN	↑	1000baseT <full-duplex>	192.168.5.1
OPT	↓	none	192.168.6.1
PFSENSE_NUC_VLAN10	↑	1000baseT <full-duplex>	192.168.10.1
PFSENSE_STAFF_VLAN20	↑	1000baseT <full-duplex>	192.168.20.1
PFSENSE_GUEST_VLAN30	↑	1000baseT <full-duplex>	192.168.30.1
WG_VPN	↑		10.179.0.15
LAN Uplink	↑	Ethernet 1000baseT <full-duplex> *Switch Uplink*	n/a

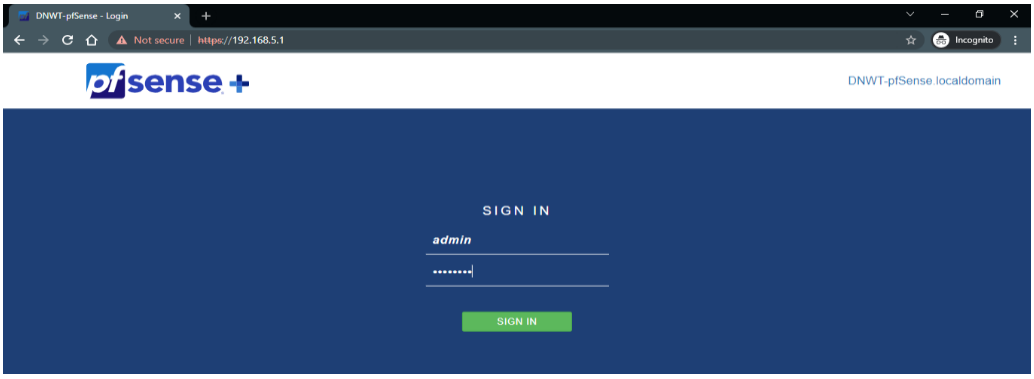
Interface Statistics

	WAN	LAN	OPT	PFSENSE_NUC_VLAN10	PFSENSE_STAFF_V
Packets In	1469489	1480203	0	86132	761
Packets Out	1652515	1263837	133	113950	1093

Traffic Graphs

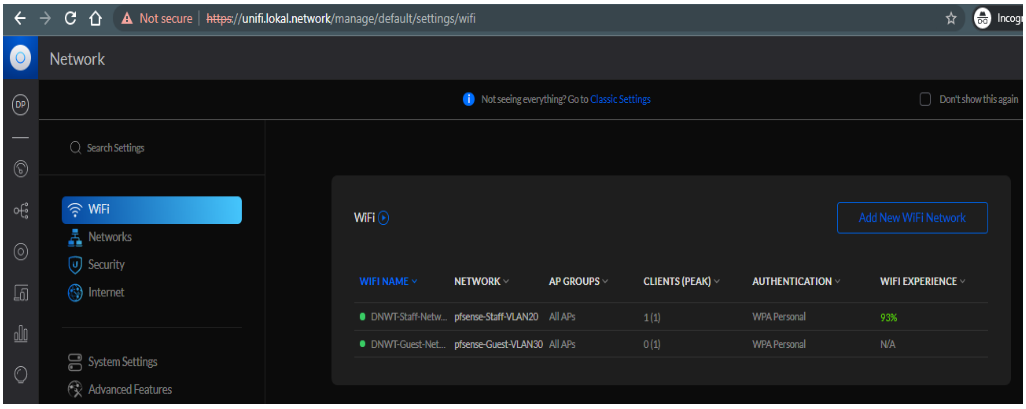
3.1.1 How to login into pfSense dashboard

- Open the browser and enter ‘192.168.5.1’ in the URL section
- Click on the ‘Advanced’ button and tap on ‘Proceed to 192.168.5.1 (unsafe)’
- Enter the credentials ‘admin/dnwt@123’



3.2 Must-to-Have Controller Configurations:

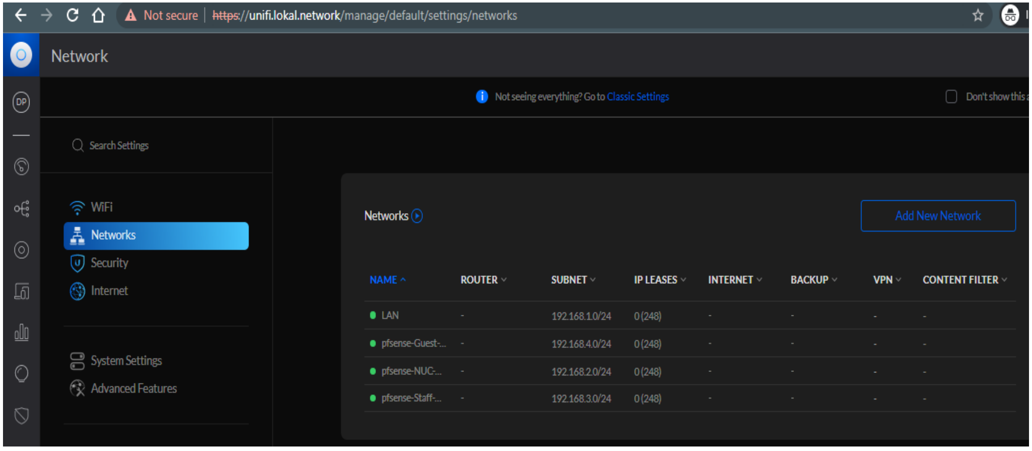
- Switch and Access Points are UniFi make devices
- All UniFi devices are controlled via UniFi Network Application called as ‘Controller’
- UniFi controller is installed directly on Intel NUC server as docker/container image
- 2 Wi-Fi are configured namely: DNWT-Staff-Network and DNWT-Guest-Network. That means AP will broadcast 2 SSIDs:



WiFi

WIFI NAME	NETWORK	AP GROUPS	CLIENTS (PEAK)	AUTHENTICATION	WIFI EXPERIENCE
DNWT-Staff-Netw...	pfsense-Staff-VLAN20	All APs	1 (1)	WPA Personal	93%
DNWT-Guest-Net...	pfsense-Guest-VLAN30	All APs	0 (1)	WPA Personal	N/A

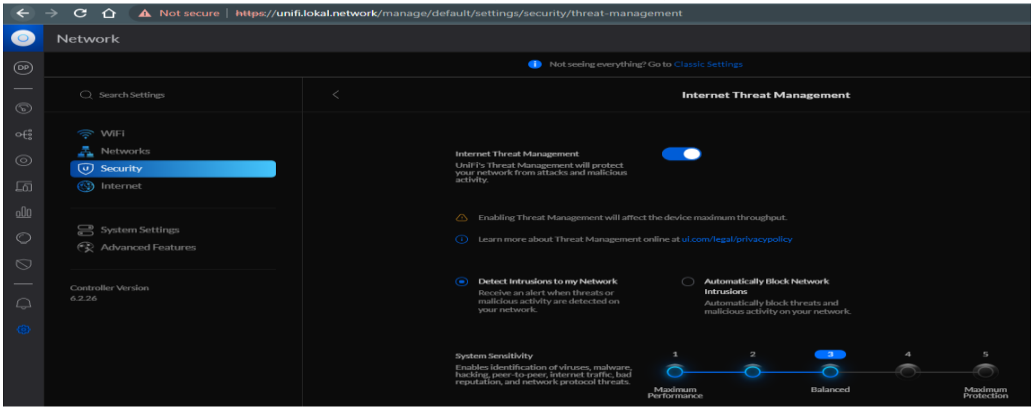
- 4 VLANS networks are configured namely: LAN, pfSense-NUC-VLAN10, pfSense-Staff-VLAN20, and pfSense-Guest-VLAN30, such that the switch works with pfSense:



Networks

NAME	ROUTER	SUBNET	IP LEASES	INTERNET	BACKUP	VPN	CONTENT FILTER
LAN	-	192.168.1.0/24	0 (248)	-	-	-	-
pfsense-Guest-...	-	192.168.4.0/24	0 (248)	-	-	-	-
pfsense-NUC-...	-	192.168.2.0/24	0 (248)	-	-	-	-
pfsense-Staff-...	-	192.168.3.0/24	0 (248)	-	-	-	-

- Security parameters like ‘Internet Threat Management’ and ‘Deep Packet Inspection’ are also enabled to introduce an extra layer of security:



https://unifi.lokal.network/manage/default/settings/security/threat-management

Not seeing everything? Go to Classic Settings

Internet Threat Management

Internet Threat Management — UniFi's Threat Management will protect your network from attacks and malicious activity. (on)

Enabling Threat Management will affect the device maximum throughput.

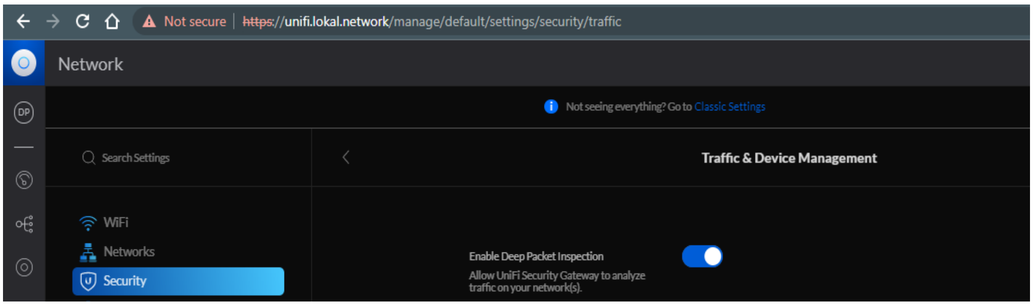
Learn more about Threat Management online at ui.com/legal/privacypolicy

● Detect Intrusions to my Network — Receive an alert when threats or malicious activity are detected on your network.

○ Automatically Block Network Intrusions — Automatically block threats and malicious activity on your network.

System Sensitivity — Enables identification of viruses, malware, hacking, peer-to-peer, internet traffic, bad reputation, and network protocol threats.

1 Maximum Performance · 2 · 3 Balanced · 4 · 5 Maximum Protection



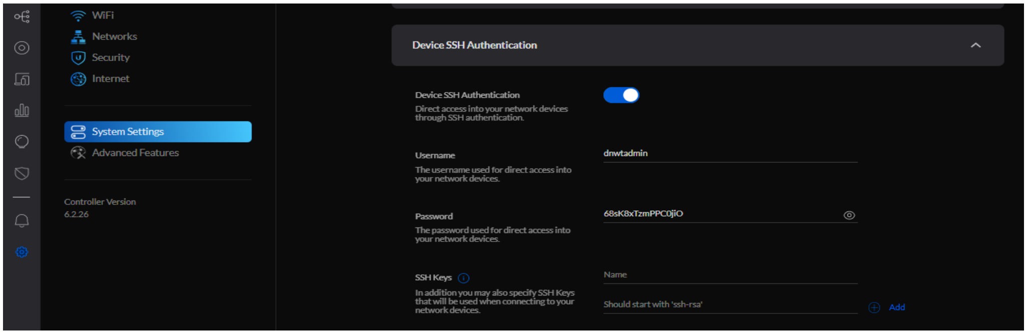
https://unifi.lokal.network/manage/default/settings/security/traffic

Not seeing everything? Go to Classic Settings

Traffic & Device Management

Enable Deep Packet Inspection — Allow UniFi Security Gateway to analyze traffic on your network(s). (on)

- System-related settings like Alerts are set to auto. Automatic device config backups are enabled to take weekly backups and SSH service is also enabled to perform troubleshooting via SSH terminal:



Device SSH Authentication

Device SSH Authentication — Direct access into your network devices through SSH authentication. (on)

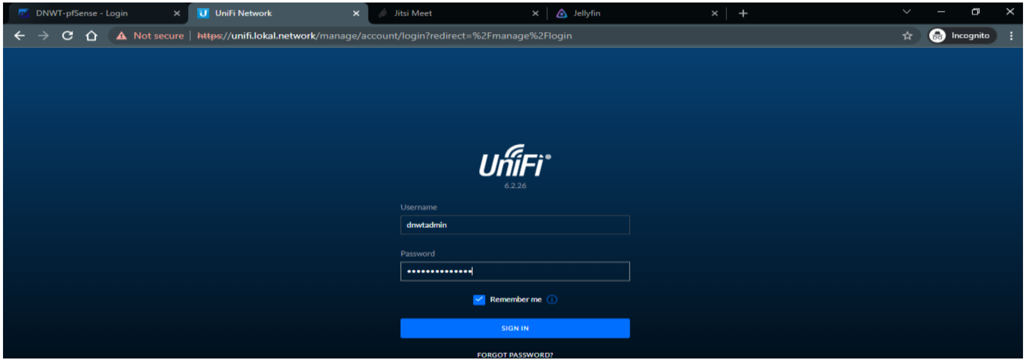
Username — The username used for direct access into your network devices. dnwtadmin

Password — The password used for direct access into your network devices. 68sK8xTzmPPC0jiO

SSH Keys — In addition you may also specify SSH Keys that will be used when connecting to your network devices. Name | Should start with 'ssh-rsa' | Add

3.2.1 How to login into UniFi Controller Dashboard:

- Connect any 1 of the 2 available DNWT networks
- Open the browser and enter ‘unifi.lokal.network’
- Enter the credentials ‘dnwtadmin/digitalNWT@123’



https://unifi.lokal.network/manage/account/login?redirect=%2Fmanage%2Flogin

Username: dnwtadmin

Password: ••••••••••••••

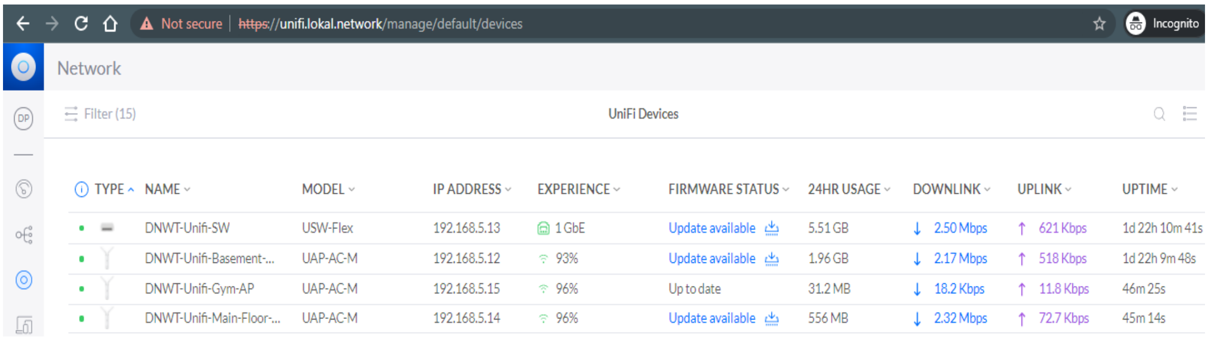
☑ Remember me

3.3 Service Testing Logs

3.3.1 UniFi Controller Logs

UniFi Controller is a wireless network management software, which allows users to manage multiple devices like Switch, Gateways, Access-Points using a WebGUI. As shown below, the controller collects various statistics at run-time. It updates the client table, topology, and statistics from the connected devices at a real-time basis. Figure 27 demonstrates the list of UniFi devices. There are 3 Access-Points (UAP-AC-M) and 1 Switch (USW-Flex), that are used in building Nimble environment. In figure 28, all clients connected to different APs placed at 3 locations namely: Main-Floor, Gym, and Basement will be shown on the 'Clients' page of the UniFi controller. The controller will record various parameters like client name, hardware type used by the client, IP address allocated by pfSense, SSID connection, and uptime of the device. The controller also records the Wi-Fi experience for each connected user within the LAN. 3 APs will mesh automatically and provide network coverage of nearly 400 meters. The meshing approach is very useful in building community networks. Multiple UniFi devices can be meshed and deployed in the NWT region to improve reliability and network coverage area.

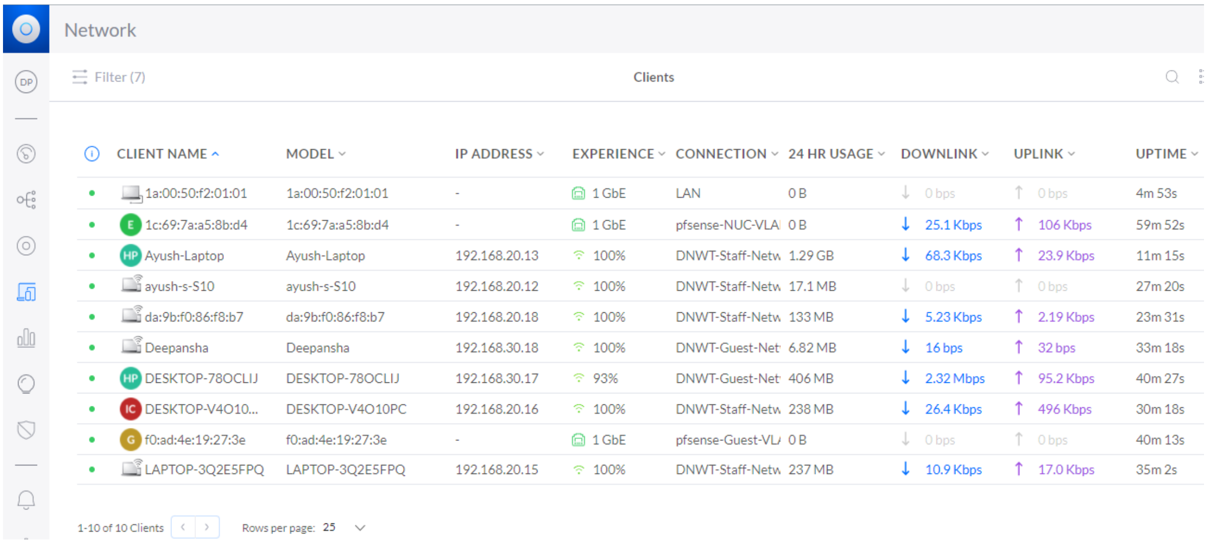
Besides collecting important parameters, the controller will also make the topology map and floorplan on a real-time basis, as demonstrated in figure 29. It connects the new device as it joins the network. Signal handover to other meshed APs can be clearly explained from the topology map.



UniFi Devices

TYPE	NAME	MODEL	IP ADDRESS	EXPERIENCE	FIRMWARE STATUS	24HR USAGE	DOWNLINK	UPLINK	UPTIME
●	DNWT-Unifi-SW	USW-Flex	192.168.5.13	1 GbE	Update available	5.51 GB	↓ 2.50 Mbps	↑ 621 Kbps	1d 22h 10m 41s
●	DNWT-Unifi-Basement-...	UAP-AC-M	192.168.5.12	93%	Update available	1.96 GB	↓ 2.17 Mbps	↑ 518 Kbps	1d 22h 9m 48s
●	DNWT-Unifi-Gym-AP	UAP-AC-M	192.168.5.15	96%	Up to date	31.2 MB	↓ 18.2 Kbps	↑ 11.8 Kbps	46m 25s
●	DNWT-Unifi-Main-Floor-...	UAP-AC-M	192.168.5.14	96%	Update available	556 MB	↓ 2.32 Mbps	↑ 72.7 Kbps	45m 14s

Figure 27: List of UniFi Devices



Clients

CLIENT NAME	MODEL	IP ADDRESS	EXPERIENCE	CONNECTION	24 HR USAGE	DOWNLINK	UPLINK	UPTIME
1a:00:50:f2:01:01	1a:00:50:f2:01:01	-	1 GbE	LAN	0 B	↓ 0 bps	↑ 0 bps	4m 53s
1c:69:7a:a5:8b:d4	1c:69:7a:a5:8b:d4	-	1 GbE	pfsense-NUC-VLA	0 B	↓ 25.1 Kbps	↑ 106 Kbps	59m 52s
Ayush-Laptop	Ayush-Laptop	192.168.20.13	100%	DNWT-Staff-Netw	1.29 GB	↓ 68.3 Kbps	↑ 23.9 Kbps	11m 15s
ayush-s-S10	ayush-s-S10	192.168.20.12	100%	DNWT-Staff-Netw	17.1 MB	↓ 0 bps	↑ 0 bps	27m 20s
da:9b:f0:86:f8:b7	da:9b:f0:86:f8:b7	192.168.20.18	100%	DNWT-Staff-Netw	133 MB	↓ 5.23 Kbps	↑ 2.19 Kbps	23m 31s
Deepansha	Deepansha	192.168.30.18	100%	DNWT-Guest-Net	6.82 MB	↓ 16 bps	↑ 32 bps	33m 18s
DESKTOP-78OCLIJ	DESKTOP-78OCLIJ	192.168.30.17	93%	DNWT-Guest-Net	406 MB	↓ 2.32 Mbps	↑ 95.2 Kbps	40m 27s
DESKTOP-V4O10...	DESKTOP-V4O10PC	192.168.20.16	100%	DNWT-Staff-Netw	238 MB	↓ 26.4 Kbps	↑ 496 Kbps	30m 18s
f0:ad:4e:19:27:3e	f0:ad:4e:19:27:3e	-	1 GbE	pfsense-Guest-VL/	0 B	↓ 0 bps	↑ 0 bps	40m 13s
LAPTOP-3Q2E5FPQ	LAPTOP-3Q2E5FPQ	192.168.20.15	100%	DNWT-Staff-Netw	237 MB	↓ 10.9 Kbps	↑ 17.0 Kbps	35m 2s

1-10 of 10 Clients ‹ › Rows per page: 25

Figure 28: List of connected clients with different APs

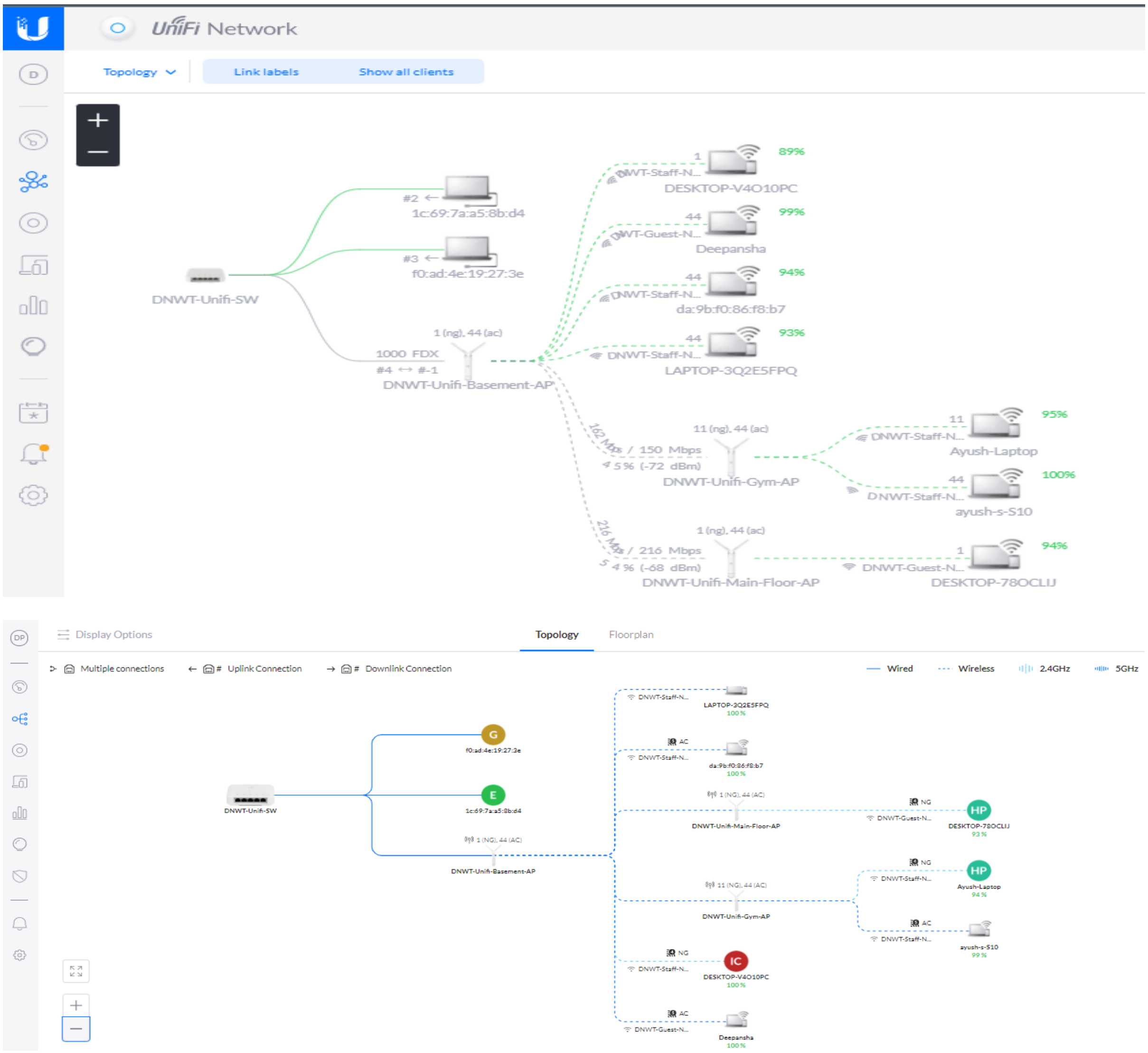
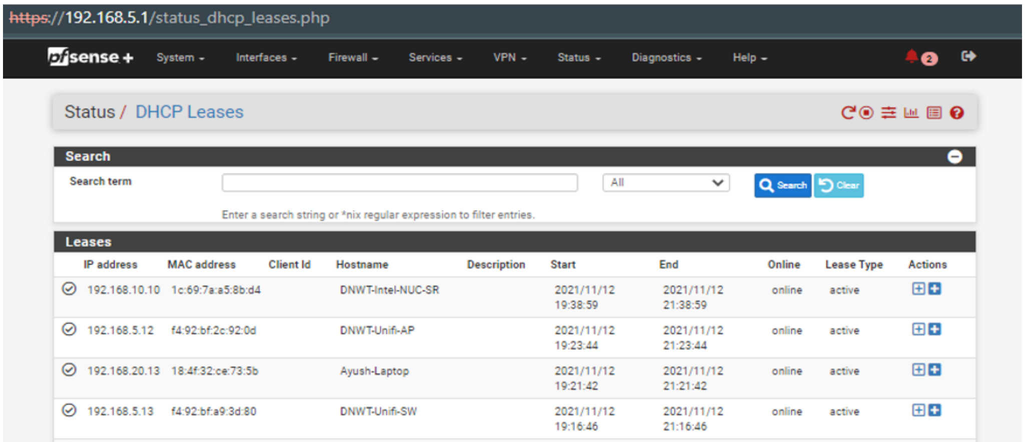


Figure 29: Topology Map

3.3.2 pfSense Logs

Netgate SG-1100 pfSense firewall device is configured with mandatory services like DHCP, DNS, SSH, Firewall Rules, NAT, Captive Portal, etc. to ensure smooth operation and access to services w/o Internet. Figure 30 shows the DHCP leases corresponding to each client. IP address allocation is required, as devices are uniquely identified using IP address on a network.



Status / DHCP Leases

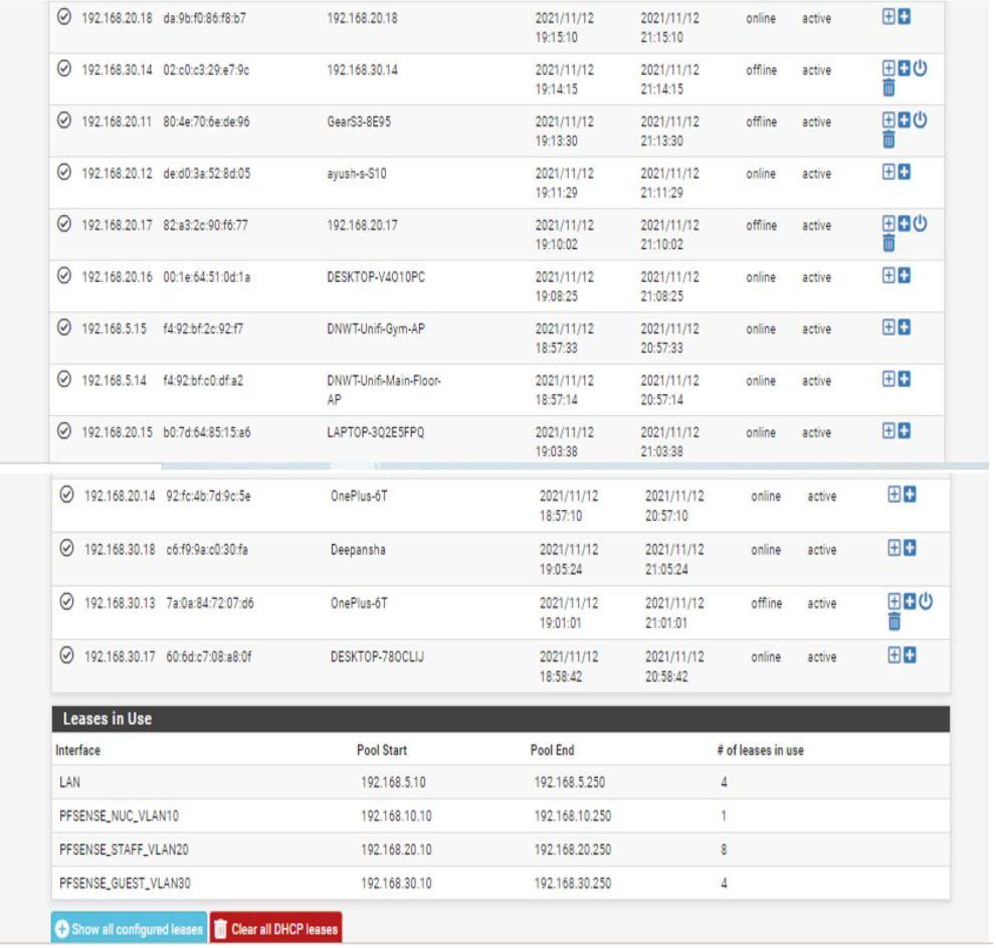
Search

Search term

Enter a search string or *nix regular expression to filter entries.

Leases

	IP address	MAC address	Client Id	Hostname	Description	Start	End	Online	Lease Type	Actions
✓	192.168.10.10	1c:69:7a:a5:8b:d4		DNWT-Intel-NUC-SR		2021/11/12 19:38:59	2021/11/12 21:38:59	online	active	⊞ ⊞
✓	192.168.5.12	f4:92:bf:2c:92:0d		DNWT-Unifi-AP		2021/11/12 19:23:44	2021/11/12 21:23:44	online	active	⊞ ⊞
✓	192.168.20.13	18:4f:32:ce:73:5b		Ayush-Laptop		2021/11/12 19:21:42	2021/11/12 21:21:42	online	active	⊞ ⊞
✓	192.168.5.13	f4:92:bf:a9:3d:80		DNWT-Unifi-SW		2021/11/12 19:16:46	2021/11/12 21:16:46	online	active	⊞ ⊞



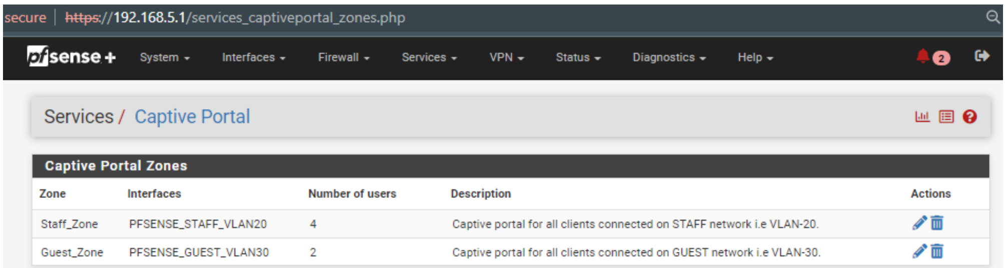
✓	192.168.20.18	da:9b:f0:86:f8:b7	192.168.20.18	2021/11/12 19:15:10	2021/11/12 21:15:10	online	active
✓	192.168.30.14	02:c0:c3:29:e7:9c	192.168.30.14	2021/11/12 19:14:15	2021/11/12 21:14:15	offline	active
✓	192.168.20.11	80:4e:70:6e:de:96	GearS3-8E95	2021/11/12 19:13:30	2021/11/12 21:13:30	offline	active
✓	192.168.20.12	de:d0:3a:52:8d:05	ayush-s-S10	2021/11/12 19:11:29	2021/11/12 21:11:29	online	active
✓	192.168.20.17	82:a3:2c:90:f6:77	192.168.20.17	2021/11/12 19:10:02	2021/11/12 21:10:02	offline	active
✓	192.168.20.16	00:1e:64:51:0d:1a	DESKTOP-V4O10PC	2021/11/12 19:08:25	2021/11/12 21:08:25	online	active
✓	192.168.5.15	f4:92:bf:2c:92:f7	DNWT-Unifi-Gym-AP	2021/11/12 18:57:33	2021/11/12 20:57:33	online	active
✓	192.168.5.14	f4:92:bf:c0:df:a2	DNWT-Unifi-Main-Floor-AP	2021/11/12 18:57:14	2021/11/12 20:57:14	online	active
✓	192.168.20.15	b0:7d:64:85:15:a6	LAPTOP-3Q2E5FPQ	2021/11/12 19:03:38	2021/11/12 21:03:38	online	active
✓	192.168.20.14	92:fc:4b:7d:9c:5e	OnePlus-6T	2021/11/12 18:57:10	2021/11/12 20:57:10	online	active
✓	192.168.30.18	c6:f9:9a:c0:30:fa	Deepansha	2021/11/12 19:05:24	2021/11/12 21:05:24	online	active
✓	192.168.30.13	7a:0a:84:72:07:d6	OnePlus-6T	2021/11/12 19:01:01	2021/11/12 21:01:01	offline	active
✓	192.168.30.17	60:6d:c7:08:a8:0f	DESKTOP-78OCLIJ	2021/11/12 18:58:42	2021/11/12 20:58:42	online	active

Leases in Use

Interface	Pool Start	Pool End	# of leases in use
LAN	192.168.5.10	192.168.5.250	4
PFSENSE_NUC_VLAN10	192.168.10.10	192.168.10.250	1
PFSENSE_STAFF_VLAN20	192.168.20.10	192.168.20.250	8
PFSENSE_GUEST_VLAN30	192.168.30.10	192.168.30.250	4

Figure 30: DHCP leases per interface

Captive portal automatically redirects clients to the authentication page before granting access to services. Figure 31 demonstrates that there are 4 clients connected on Staff network and 2 clients connected to the Guest network. Building a system with multiple networks driven by different captive portals is a powerful approach in building community networks. For example, a 'Nimble' unit deployed in schools located in remote communities can be designed to broadcast 2 SSIDs namely 'staff' and 'student' with different privilege settings. This enables the teaching staff to edit the course material, while simultaneously allowing students to participate in classes with only 'read-only' access.



secure | ~~https~~://192.168.5.1/services_captiveportal_zones.php
pfsense+
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
2
Services / Captive Portal

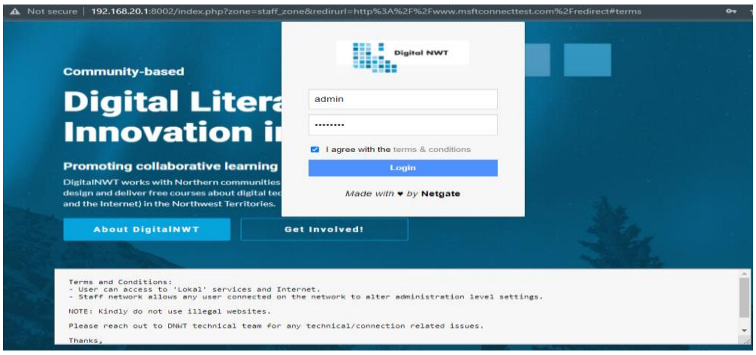
Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
Staff_Zone	PFSENSE_STAFF_VLAN20	4	Captive portal for all clients connected on STAFF network i.e VLAN-20.	
Guest_Zone	PFSENSE_GUEST_VLAN30	2	Captive portal for all clients connected on GUEST network i.e VLAN-30.	

Figure 31: Number of clients per Captive Portals

Once a user connects to the 'Nimble' network, the system will authenticate the new user using the captive portal feature. The system will automatically redirect the user for authentication.

Figures 32 and 33 demonstrates that while users require authentication to join the 'Staff' network, no authentication is required to join the 'Guest' network. Needless, acceptance of terms and condition is common.



Not secure | 192.168.20.1:8002/index.php?zone=staff_zone&redirurl=http%3A%2F%2Fwww.msftconnecttest.com%2Fredirect#terms

Community-based

Digital Litera

Innovation i

Promoting collaborative learning

DigitalNWT works with Northern communities design and deliver free courses about digital tec and the Internet) in the Northwest Territories.

admin

•••••••••

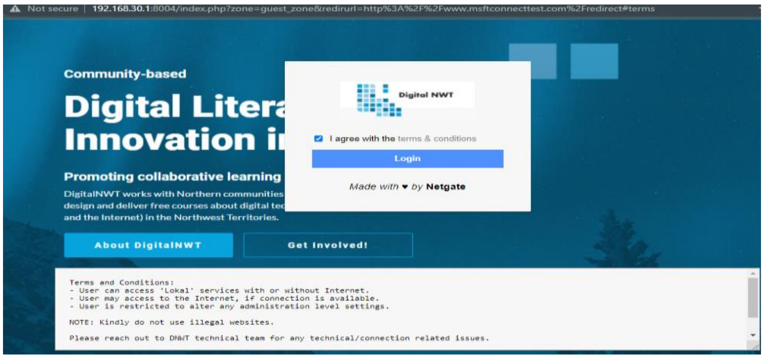
☑ I agree with the terms & conditions

Login

Made with ♥ by Netgate

```
Terms and Conditions:
- User can access to 'Lokal' services and Internet.
- Staff network allows any user connected on the network to alter administration level settings.

NOTE: Kindly do not use illegal websites.

Please reach out to DNWT technical team for any technical/connection related issues.

Thanks,
```

Figure 32: Captive portal for Staff Network (DNWT-Staff-Network)



Not secure | 192.168.30.1:8004/index.php?zone=guest_zone&redirurl=http%3A%2F%2Fwww.msftconnecttest.com%2Fredirect#terms

Community-based

Digital Litera

Innovation i

Promoting collaborative learning

DigitalNWT works with Northern communities design and deliver free courses about digital tec and the Internet) in the Northwest Territories.

☑ I agree with the terms & conditions

Login

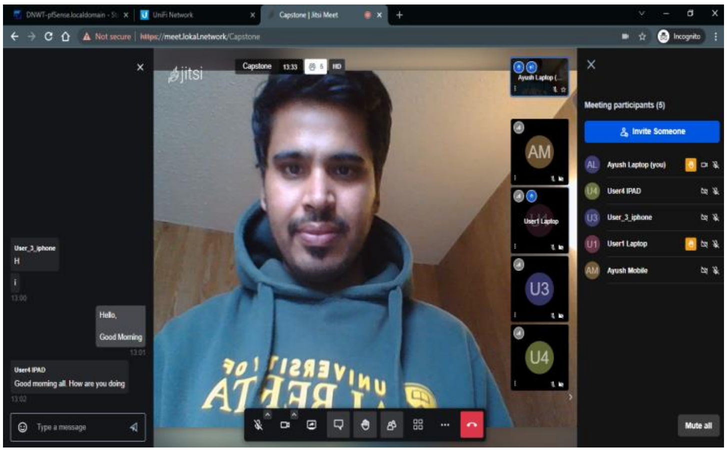
Made with ♥ by Netgate

```
Terms and Conditions:
- User can access 'Lokal' services with or without Internet.
- User may access to the Internet, if connection is available.
- User is restricted to alter any administration level settings.

NOTE: Kindly do not use illegal websites.

Please reach out to DNWT technical team for any technical/connection related issues.
```

Figure 33: Captive portal for Guest Network (DNWT-Guest-Network)

3.3.3 Jitsi Logs

Jitsi service is a set of open-source projects that allow users to deploy video conferencing solutions. Further, the Jitsi service supports audio, dial-in, recording, and live streaming features. It has a feature to control video and audio quality for low bandwidth connections. Figure 34 depicts the demonstration of the Jitsi video conferencing call with 5 different participants. The name of the meeting is 'Capstone'. This feature will allow individuals in remote communities to participate in social and school events remotely. It thereby enables individuals to stay in touch with their families, friends, relatives, etc.



Not secure | https://meet.lokal.network/Capstone

User_3_iphone
H
i
13:00

Hello,
Good Morning
13:01

User4 IPAD
Good morning all. How are you doing
13:02

Meeting participants (5)

- AL Ayush Laptop (you)
- U4 User4 IPAD
- U3 User_3_iphone
- U1 User1 Laptop
- AM Ayush Mobile

Figure 34: Jitsi Video Conferencing Call

3.3.4 Jellyfin Logs

Jellyfin is an open-source media streaming solution. Users can control their media and curate a personalized playlist. Streaming is possible to any device with its community servers. Watching movies, TV shows, music, and live TV are possible with the Jellyfin service. Figures 35 and 36 demonstrate the Jellyfin dashboard and playable media of building Nimble Kit. It is important to mention here that the work for media content development (courses) is currently under progress, which shall be shortly loaded to the Jellyfin application shortly. Few short clips and videos are successfully stocked on the Jellyfin instance, as displayed in below figures. The content will help adult educators in remote regions of NWT to teach courses to students and other interested participants.

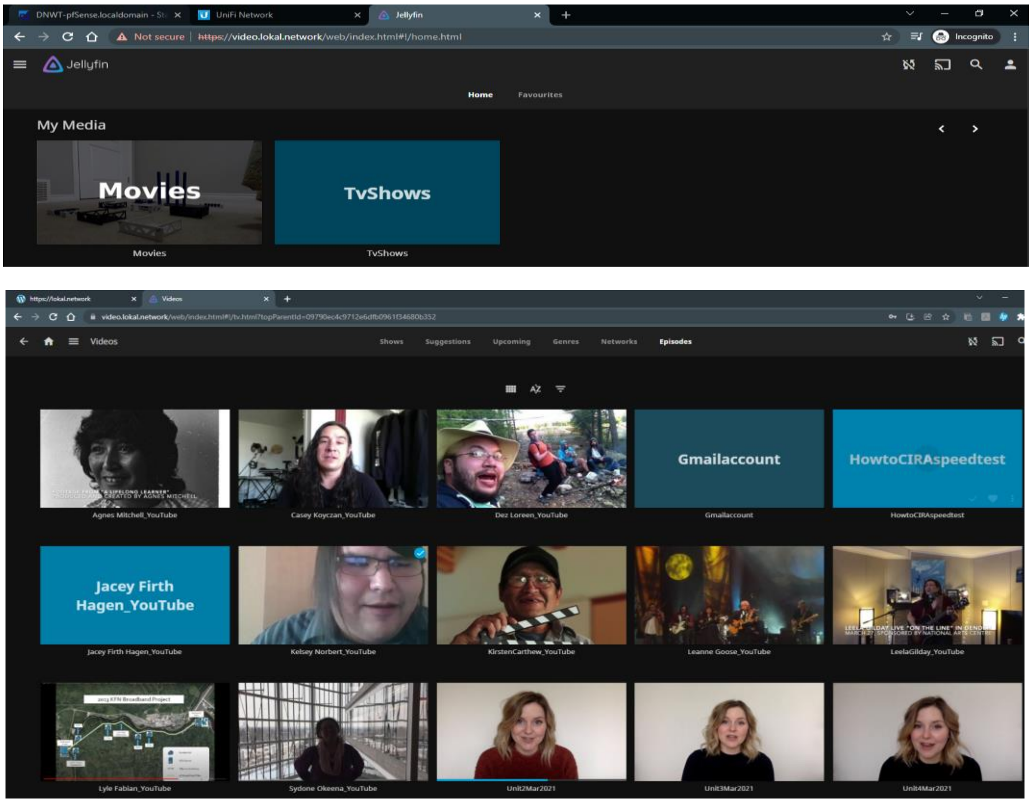


Figure 35: Jellyfin Media Library

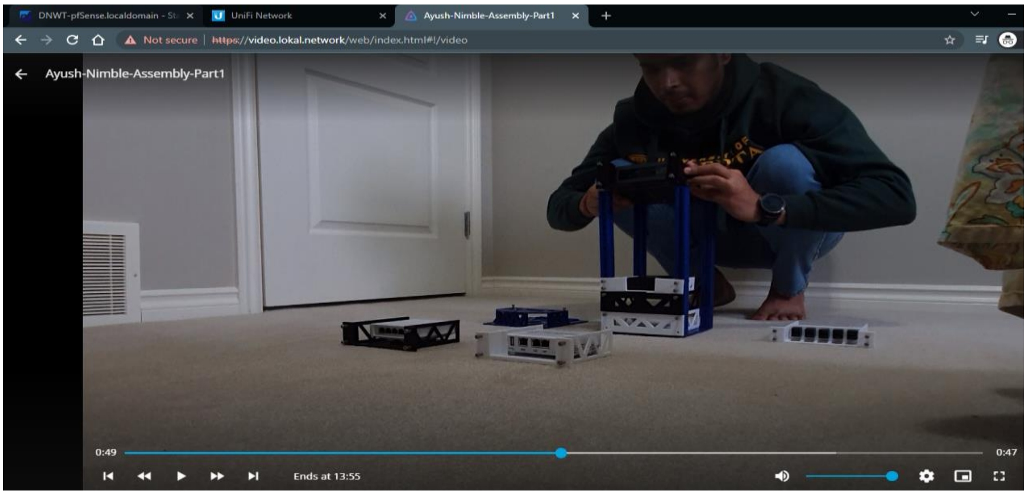
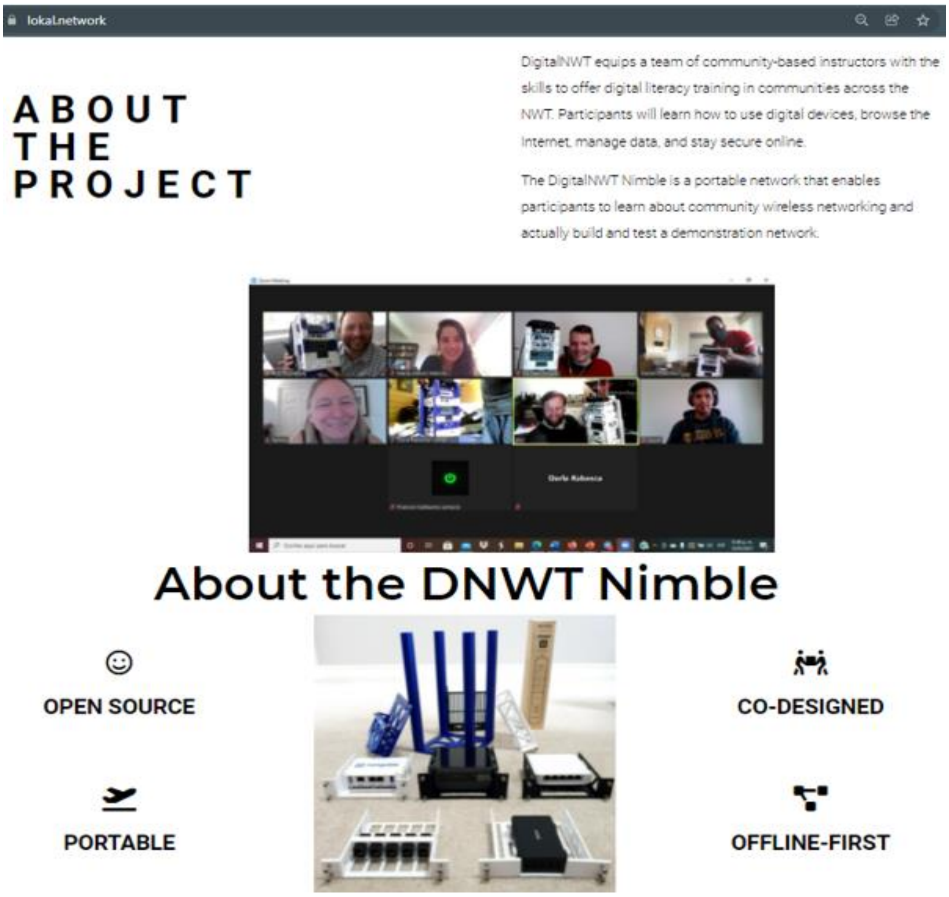

DNWT-pfSense.localdomain - St
UniFi Network
Ayush-Nimble-Assembly-Part1
Not secure | https://video.lokal.network/web/index.html#!/video
Ayush-Nimble-Assembly-Part1
0:49
0:47
Ends at 13:55

Figure 36: Playable Media of Building Nimble Kit in Jellyfin library

3.3.5 WordPress (WP) Logs

WordPress (WP) is an open-source project that allows users to build the simplest yet most efficient website or a blog. WP is a content management system (CMS) that makes it easy to manage important aspects of a website without needing to know about programming. Figure 37 shows the snippet from the WP landing page which displays a soft-link to services like Jitsi, Jellyfin, and UniFi-Controller. This approach will help any novice user to start the services easily. Information related to the project and upcoming services will be displayed on the WP landing page for quick reference.



ABOUT THE PROJECT

DigitalNWT equips a team of community-based instructors with the skills to offer digital literacy training in communities across the NWT. Participants will learn how to use digital devices, browse the Internet, manage data, and stay secure online.

The DigitalNWT Nimble is a portable network that enables participants to learn about community wireless networking and actually build and test a demonstration network.

About the DNWT Nimble

OPEN SOURCE

CO-DESIGNED

PORTABLE

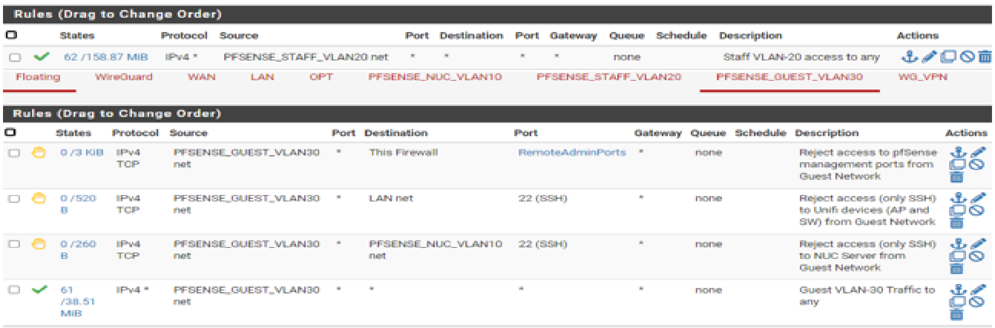
OFFLINE-FIRST

Figure 37: WordPress (WP) Landing Page Snippet

3.3.6 ‘Guest’ Network Restrictions Logs

We have discussed in the above section that any user connected to the ‘Guest’ network will be treated differently as compared to the ‘Staff’ network. Bandwidth capping is set to 5 Mbps per connection, hence users connected on the ‘Guest’ network will be able to access the Internet with only 5 Mbps download and upload speed. However, data capping is not done on any of the networks. In essence, the user will be able to download or upload any form of data with a 5 Mbps connection speed.

Furthermore, users on the ‘Guest’ network have a ‘read-only’ permission. Hence, a user will not be able to access pfSense, Intel NUC Server, UniFi Switch, and UniFi AP via SSH or WebGUI service. As shown in figure 38, remote administration ports (443-HTTPS, 80-HTTP, 22-SSH, and 23-Telnet) are blocked using the firewall aliasing feature in pfSense. Figure 39 demonstrates how firewall policies block ‘Guest’ users from accessing devices.



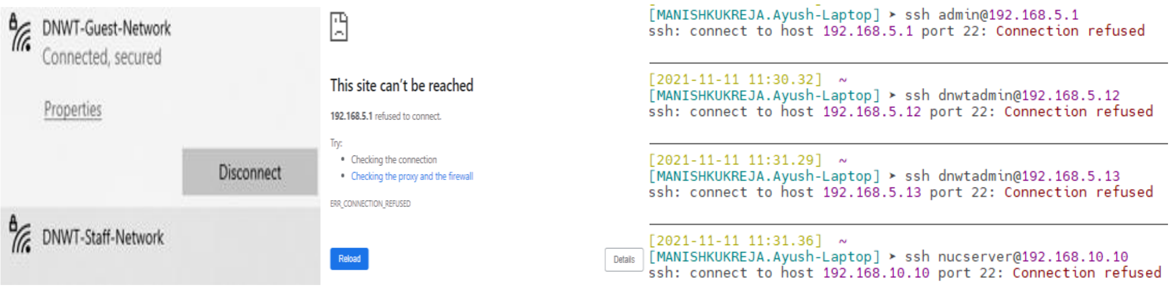
Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	62 /158.87 MiB	IPv4 *	PFSENSE_STAFF_VLAN20 net	*	*	*	*	none		Staff VLAN-20 access to any	

Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐		0 /3 KiB	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	This Firewall	RemoteAdminPorts	*	none		Reject access to pfSense management ports from Guest Network	
☐		0 /520 B	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	LAN net	22 (SSH)	*	none		Reject access (only SSH) to Unifi devices (AP and SW) from Guest Network	
☐		0 /260 B	IPv4 TCP	PFSENSE_GUEST_VLAN30 net	*	PFSENSE_NUC_VLAN10 net	22 (SSH)	*	none		Reject access (only SSH) to NUC Server from Guest Network	
☐	✓	61 /38.51 MiB	IPv4 *	PFSENSE_GUEST_VLAN30 net	*	*	*	*	none		Guest VLAN-30 Traffic to any	

Figure 38: Strict Firewall Policies on ‘Guest’ Network



This site can't be reached

192.168.5.1 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

```
[MANISHKUKREJA.Ayush-Laptop] ➤ ssh admin@192.168.5.1
ssh: connect to host 192.168.5.1 port 22: Connection refused

[2021-11-11 11:30.32]  ~
[MANISHKUKREJA.Ayush-Laptop] ➤ ssh dnwtadmin@192.168.5.12
ssh: connect to host 192.168.5.12 port 22: Connection refused

[2021-11-11 11:31.29]  ~
[MANISHKUKREJA.Ayush-Laptop] ➤ ssh dnwtadmin@192.168.5.13
ssh: connect to host 192.168.5.13 port 22: Connection refused

[2021-11-11 11:31.36]  ~
[MANISHKUKREJA.Ayush-Laptop] ➤ ssh nucserver@192.168.10.10
ssh: connect to host 192.168.10.10 port 22: Connection refused
```

Figure 39: 'Guest' Network Firewall Testing

4 Final Discussion and Conclusion

This capstone project provides a detailed analysis and assessment of various aspects of ‘Digital Divide’. The project also critiques different levels of the Digital Divide and suggests ways to overcome the same. The problem may be solved efficiently using the ‘divide and conquer’ principle, wherein required and adequate attention is given to each level of the problem separately. This project majorly focuses on challenges associated with the first-level Digital Divide that people living in remote communities’ face. It provides a smart solution in a creative way that addresses the connectivity issues existing in remote communities like the NWT. The data used in this project report is based on empirical evidence collected during the literature survey. The data has been sampled and verified during various peer discussions, workshops, and fruitful discussions with northerners during the Nimble kit installation phase which were conducted as part of the DNWT project. This project establishes meaningful footprints on the Information and Communication Technology (ICT) society, as it aims to solve connectivity challenges in geographically dispersed communities. The remote communities are otherwise often excluded from the research because of their low population density and small geographic footprints.

After completing the literature survey and conducting a survey with individuals living in NWT, it may be clearly seen that they hold a strong desire and interest in digital technology adoption. Individuals living in these communities are paying excruciatingly high prices for Internet service, which comes with limited yet expensive data caps. Few parts of remote communities are equipped with a fiber Internet connection; however, service is often not reliable. Interested and motivated people have altered and adjusted their digital ecosystem in response to the obstacles they face [1]. Hence, affordability, reliability, and slow Internet speed are the major challenges in Northern Canada. These kinds of digital inequalities hinder their presence in digital space and discourage them from participating and contributing to the digital technology ecosystem.

The government has also started to invest significantly in improving Internet service across Northern Canada. A recent example of such efforts is fiber optic link in the Mackenzie Valley that stretches 1,154 kms long. The Canadian Radio-television and Telecommunication Commission (CRTC) was appointed by the governing council to regulate the telecommunication service across Canada. The ultimate and promised goal is to reach the 'last mile' i.e., providing optical fiber links to each household to ensure fast and reliable Internet connection. However, these promises are long-due and are underway in their development process for a long time. During these times while settlements and planning are underway, northerners are getting disadvantaged with unreliable and slow-speed Internet connections. Since modern technology and telecommunication services have become the measure of Canada's every growing future economy, research, and small projects can help northerners to support their need of connectivity in the form of small infrastructural developments. Unique programs led by interested individuals, researchers, and government could help in streamlining the process to support the global cause of connectivity that helps in moderating against existing barriers to connectivity.

Considering different aspects of Digital Divide, this capstone project presents a 'Nimble' kit that is built to operate in offline mode and promotes the ideology of 'offline first'. The Nimble design works on the principle of the 'Intranet' application and enables 'Community Networking'. Community Networks (CN) are also be termed as Do It Yourself (DIY) networks, in which local community members can serve as the stakeholders of the networks. Ownership, resource sharing, and control lies within the community. This approach allows flexibility in choosing software applications and services. NUC server is the brain behind the nimble, which runs the 'Lokal' platform and is an open-source software platform that allows individuals to not only receive but also develop, curate, and distribute information in local languages relevant to local communities. It works on the methodology of 'connectivity for people & by people'. The Nimble kit consists of various hardware components such as Server (Intel NUC), Firewall/Router (Netgate SG-1100 pfSense), Switch (UniFi), Access-Points (UniFi), and Power Bank (Omni). These are the bare minimum devices that are required to enable connectivity. Four services that enable video & audio calling (Jitsi), wireless network management (UniFi-Controller), media streaming (Jellyfin), and website creation (WordPress) are installed on the server. Multiple digital devices viz: laptops, mobile phones, tablets, smart-watch, etc. from the house of Apple, Samsung, One-Plus, etc. have been utilized while performing the use-case testing. All individual hardware components are coupled together to form a shape of a networking rack that enables secure data routing across network boundaries. The resulting environment is further stitched with the 'Ubuntu' OS and the 'Lokal' platform to deliver a bundled solution that is powerful enough to solve connectivity issues in remote communities. Social networking, eLearning, and blog creation are possible with the help of the above 4 services. The scope is not limited, services and content can be expanded as per the community requirement. The Nimble kit is highly portable, and it enables individuals to carry the unit in a strong pelican case. Individuals can travel miles and carry connectivity as they go. The model introduced in this project demonstrates the power of the Nimble kit and the expansion of services is beyond imagination based on the hardware type used. This capstone project is capable to enable 3.8 billion unconnected people to connect themselves locally via community networking methodology.

5 Recommendations

The Nimble kit has been regressed and tested properly. The said kit proves to be a solution for connectivity. Remote communities will be able to deploy the kits on their own by following the steps mentioned in the above sections. In terms of hardware and software, below are some possible recommendations for future development of the Nimble unit:

5.1 Additional Services

The current Nimble unit offers 4 out-of-the-box services. Additional services that enable social networking, educational library, real-time document editing, learning management system (LMS), photos and videos editing, network report generator, etc. further can be accommodated in future services wish list. Potential service candidates are: WikiIndex, UniFi-Poller, Grafana, Signal, Kolibri, Calibre Web, Moodle, Matomo, Discourse, and Etherpad.

5.2 Additional Hardware

The nimble design may be slightly modified to accommodate new devices to enable wireless Internet connectivity. The current way is to plug the Internet cable into the WAN port of the pfSense. This way suggests accommodating additional devices that should have built-in support for 3G/4G/LTE/5G modules. These chipsets will allow future Nimble units to access the Internet wirelessly. Potential candidates are the SXT LTE kit, Router Alcatel Link Hub HH42NK-2BLDUS1, and Alcatel Link Hub 4G LTE, etc.

5.3 Hardware Customization

There are two customizations possible in the hardware:

1. Switch and router/firewall may be replaced with a single device that can perform switching, routing, and firewalling actions. There are a handful of devices for consideration, e.g.: MikroTik hEX S Router. This approach will introduce vacant space for the additional devices to be accommodated in the emptied shelf.
2. Within the existing model, the pfSense device may be replaced with UniFi Secure Gateway (USG), which offers similar capabilities as pfSense. USG is a router with firewall capabilities. Ultimately, this replacement will make the entire network and security to be managed and controlled via a single dashboard i.e., 'UniFi Network Application', as all devices (router/firewall, switch, and AP) will become UniFi make.

5.4 Traffic Shaping and Policing

Netgate SG-1100 pfSense further can be configured with Quality of Service (QoS). The traffic shaping approach will help in prioritizing network traffic. Traditionally without QOS, the device processes the packets on First Come First Serve (FCFS) basis. QoS allows different types of traffic to be prioritized, such that high-priority services get a higher bandwidth as compared to lower-priority services. QOS works on the principles of 'Shaping' and 'Policing/Limiting'. It provides special treatment for VIPs (Very Important Packets). The core concept of traffic shaping is to raise and lower packet priorities while keeping them within a specified speed. This idea protects the network from high latency (or lag) caused by excessive buffering of packets.

6 Bibliography

[1] Rob McMahon, Murat Akcayir, Michael B. McNally, Sydonie Okheena, “Making sense of digital access in remote contexts: Conceptions of and responses to digital connectivity challenges in the Northwest Territories, Canada,” *International Journal of Communication (IJOC),* vol. 15, 2021.

[2] Canadian Radio-television and Telecommunications Commission, “Telecom Regulatory Policy CRTC 2016-496,” 21 Dec 2016. [Online]. Available: https://crtc.gc.ca/eng/archive/2016/2016-496.htm.

[3] S. Kemp, “Digital Around the World,” https://kepios.com/, 2021. [Online]. Available: https://datareportal.com/global-digital-overview.

[4] L. Belli, “Community Networks: the Internet by the People for the People.,” United Nations Internet Governance Forum: Geneva., 2017.

[5] “Current World Population,” Worldometer, 2021. [Online]. Available: https://www.worldometers.info/world-population/.

[6] “Demographics,” Data Commons, [Online]. Available: https://datacommons.org/place/Earth?utm_medium=explore&mprop=count&popt=Person&hl=en.

[7] A. Trotman, “World Populaton Trend,” ReseachGate, [Online]. Available: https://www.researchgate.net/figure/World-population-trends-between-1950-and-2050-This-graph-is-based-on-the-United-Nations_fig1_245025696.

[8] Statista, “Global digital population as of January 2021,” Joseph Johnson, 2021.

[9] J. Johnson, “Canada: number of online users 2016-2026,” Statista, 24 Aug 2021. [Online]. Available: https://www.statista.com/statistics/325649/canada-number-of-internet-users/ and https://www.statista.com/statistics/263742/total-population-in-canada/.

[10] S. Kemp, “Digital 2021: Canada,” Data Reportal, 2021. [Online]. Available: https://datareportal.com/reports/digital-2021-canada.

[11] Britannica, “Settlement patterns,” Britannica, 2018. [Online]. Available: https://www.britannica.com/place/Canada/Demographic-trends.

[12] “Digital divide,” Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Digital_divide.

[13] J. V. Dijk, The Digital Divide, Polity, 2020.

[14] J. Nielsen, "Digital Divide: The 3 Stages," Nielsen Norman Group logoNielsen Norman Group, 19 Nov 2006. [Online]. Available: https://www.nngroup.com/articles/digital-divide-the-three-stages/.

[15] H. Galperin, "Goodbye Digital Divide, Hello Digital Confusion? A Critical Embrace of the Emerging ICT4D Consensus," 2010.

[16] S. Canada, "Geography," [Online]. Available: https://www150.statcan.gc.ca/n1/pub/11-402-x/2011000/chap/geo/geo-eng.htm.

[17] Beaton, B., McMahon, R., O'Donnell, S., Hudson, H., Whiteduck, T., & Williams, D, "Digital Technology Adoption in Northern and Remote Indigenous Communities.," 26 April 2016. [Online]. Available: http://firstmile.ca/report-digital-technology-adoption-in-northern-and-remote-indigenous-communities-in-canada/.

[18] "Northwest Territories," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Northwest_Territories.

[19] A. Fiser, "Telecommunications and Broadband Connectivity," in *The Conference Board of Canada*, 2013.

[20] Catarina Owen, Christopher Hunt, Rob McMahon, Kyle Napier, Giselle Marion, "Opinion: The North needs more equitable, accessible Internet," *Edmonton Journal,* Mar 16, 2021.

[21] OAG, "Connectivity in Rural and Remote Areas," 2018.

[22] L. Roth, "Digital self-development and Canadian First Peoples of the north," *Media Development*, 2014.

[23] A. Desmarais, "N.W.T.'s Mackenzie Valley fibre line not living up to expectations, experts say," CBC, 2020.

[24] "Buying Speed? What Canadians Pay for Broadband: Part 1 – The CRTC's "Measuring Broadband Canada" report does not measure up," PIAC, 2020. [Online]. Available: https://www.piac.ca/2020/10/29/buying-speed-what-canadians-pay-for-broadband-part-1-the-crtcs-measuring-broadband-canada-report-does-not-measure-up/.

[25] H. E. Hudson, "When Regulation fills a Policy Gap: Toward Universal Broadband in the Remote North," 2017.

[26] NorthwesTel, "Internet plans," NorthwesTel, 2021. [Online]. Available: https://www.nwtel.ca/internet-plans.

[27] "Internet Pricing in the NWT (Consumer)," Government of Northwest Territories, 2021. [Online]. Available: https://www.fin.gov.nt.ca/en/internet-pricing-nwt-consumer.

[28] "Telecom Decision CRTC 2020-258," CRTC, 12 Aug 2020. [Online]. Available: https://crtc.gc.ca/eng/archive/2020/2020-258.htm.

[29] M. Nakehk'o, “Accessible/Affordable Internet across the North. - #COVID19NWT,” change.org, 2020. [Online]. Available: https://www.change.org/p/northwestel-accessible-affordable-internet-across-the-north-covid19nwt?utm_content=cl_sharecopy_21044675_en-CA%3Av1&recruiter=1185152637&recruited_by_id=52830ac0-81dc-11eb-8039-596f365171bf&utm_source=share_petition&utm_medium=cop.

[30] DistroWatch, “Lasted Distributions,” [Online]. Available: https://distrowatch.com/.

[31] Canonical, “Get Ubuntu Server,” Ubuntu, 2021. [Online]. Available: https://ubuntu.com/download/server.

[32] Canonical, “What’s new in Ubuntu 20.04 LTS?,” Ubuntu, 2021. [Online]. Available: https://ubuntu.com/engage/20.04-webinars.

[33] Netgate, “pfSense Documentation,” 19 Jan 2021. [Online]. Available: https://docs.netgate.com/pfsense/en/latest/.