Configuration for Wireless Network Based on Hotspot and CAPsMAN

Sanksi Pelanggaran Pasal 113
Undang-Undang No. 28 Tahun 2014 Tentang Hak Cipta

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

Configuration for Wireless Network Based on Hotspot and CAPsMAN

Maya Sari, S.Kom., M.Kom.
(Computer Network Lecturer, Department of Information Technology, Shanti Bhuana Institute)

Azriel Christian Nurcahyo
(PhD Student in Computing, University of Technology Sarawak)

AMERTA
MEDIA

Configuration for Wireless Network Based on Hotspot and CAPsMAN

Anggota IKAPI
No 192JTE/2020
Cetakan Pertama: Juli 2024
17,5 cm x 25 cm
ISBN: 978-623-419-665-8

Penulis:
Maya Sari, S.Kom., M.Kom.
Azriel Christian Nurcahyo

Desain Cover:
Dwi Prasetyo

Tata Letak:
Ladifa Nanda

Diterbitkan Oleh:
Penerbit Amerta Media

Jl. Raya Sidakangen, RT 001 RW 003, Kel, Kebanggan, Kec. Sumbang, Purwokerto, Banyumas 53183, Jawa Tengah. Telp. 081-356-3333-24
Email: mediaamerta@gmail.com
Website: amertamedia.co.id
Whatsapp : 081-356-3333-24

FOREWORD

We would like to offer our deepest appreciation and sincerest gratitude unto divine providence for His favors upon us, which granted the authors of this publication, "Wireless Network Configuration Based on Hotspot and CAPsMAN MikroTik," successful completion. This book has been developed as an operational handbook targeting IT experts, network engineers, and whoever is interested in understanding and implementing wireless networks through MikroTik technology. Wireless networks are in demand today for reliability and efficiency. As one of the prestige network solution providers, MikroTik offers several advanced features that can be utilized in creating centralized management protocols indispensable to these systems. The current study focuses on two of the most crucial utilities, Hotspot and CAPsMAN configuration, which are vital in establishing more robust and streamlined network management protocols. We sincerely wish that this book be used as a useful source of information that will provide the reader an opportunity to get a very clear understanding of how to set up wireless networks through Hotspot and CAPsMAN MikroTik. Our book uses an easy writing style with illustrative graphics and configuration examples, offering enhanced understanding and facilitating smooth implementation steps. We would like to extend our heartfelt appreciation to all those individuals who have supported us in bringing out this book. Our team does appreciate some of constructive criticisms /suggestions, as these actually help the authors make valuable improvements in the text towards future editions.

Sibu, Sarawak, 3 July 2024

Azriel Christian Nurcahyo

PREFACE

In the present scenario, a growing need is stressed on having wireless networks both indoors and outdoors of diverse large environments like public areas, corporate offices, and government sectors, schools, and colleges. Traditional network deployments, on the other hand, generally rely on either bridging or rather on the full CSS deployment method while often making use of NAT on every access point. This causes interference with access points operating beyond the DHCP server lease limits, with frequent loop issues arising within the wireless infrastructures. Thus, network administrators face the challenge of adding many simultaneous access points that do not have the ability to be integrated, thus giving rise to numerous challenges in meeting demand with reliable networking solutions that provide quick distribution of vouchers or enable user registrations per ID, especially during peak usage periods involving large numbers of users who are connected concurrently.

Previous studies have pointed out that a network system constructed with multiple hotspot servers is highly reliable but still further developed for wireless needs. Especially when multiple access points are needed and different collaborative techniques are required of them, the purpose of this study is to extend the previous study to build up a network structure in which an access point control mechanism can be combined with a hotspot server. The overall objective being to provide standards on deploying extensive networks made up of tens to hundreds of access points while making configuration changes easy, including but not limited to SSID, frequency modulation of the password and channel updating, without the need to individually reconfigure.

The stochastic fairness queuing technique is applied while executing this work basically. It is a system designed for fairly dividing traffic or flow of packets. These packets that arrive will be further subdivided among multiple sub-queues using a hash-based function. The SFQ implementation will try to achieve optimal parameters in wireless distribution with vouchers using two unique router bridges between a gateway server connected to a hotspot server. In this project, there are four routerboards. One of them is configured as a CAPsMAN gateway controller access point, another only as a voucher-based hotspot server gateway, and three routers connected with CAPs, all working in a switch configuration. We will measure resulting

outputs by testing them against TIPHON standards for only wireless links and excluding any other connections of any kind using test parameters that include throughput, jitter, roaming capabilities and both wired coverage coupled with lossless data transfer when vouchers are used respectively in the course of this testing process. We borrow the deepest appreciation and gratitude towards all people who have so generously offered their support and made invaluable contributions towards the creation of this book. We are far from being proud to acknowledge your dedication to this project and it is because of such commitment that has greatly helped to elevate this project from an idea into a book. We humbly request that in the future any constructive criticisms or recommendations that you may have as they are very vital for us in improving subsequent versions of this book. Your inputs will help us improve upon its quality even further while better serving the needs and preferences of our readership community.

Bengkayang, 3 July 2024

Maya Sari, S.Kom., M.Kom.

TABLE OF CONTENTS

Chapter 1
Why CAPsMAN and Hotspot, Problems and Existing Theories

A. Background

At the moment, the demand for networks has diversified from being a sub-requirement to a major requirement. Therefore, demands for indoor and outdoor wireless networks have invariably increased along big spaces such as public open areas, corporate institutions, government offices, schools, and universities. Nevertheless, the networks being designed are still traditional, with most of them either using the bridging or the extended service set methodology. Moreover, network address translation is often placed on every access point, leading to a numerousotechnical problems. The access points are often subject to interference when used out of range of the DHCP server lease restrictions, and looping problems commonly occur within the wireless networks. The problems are especially complex when network administrators try to integrate scores or even hundreds of access points simultaneously, as non-integrated systems present a lot of problems in network administration. Moreover, the reliability of the networks is increasingly supposed to be raised, especially during simultaneously vast accesses to the network either due to the number of voucher distributions or user registrations per ID.

This paper follows up on the effort started by the networking groups of Immanuel Christian University Yogyakarta and Shanti Bhuana Institute. These groups also started the process of implementing these concepts on Cisco systems at the University of Technology Sarawak. Previous studies have proven that network systems with multiple hotspot servers are highly reliable. Further development is necessary to accommodate wireless demands, especially in conditions that require a high number of access points and the ability to combine various techniques.

The objective is to develop a framework that would support Access Point Control through a Hotspot server. It is also envisioned that this work would be useful to industrial workers who have to implement huge and extensive

networks for which the number of access points is naturally high. This should reduce the configuration burden and facilitate changes in SSID, passwords, frequency, and channels without changing the same in individual access points.

The Controlled Access Point System Manager, or in brief, CAPsMAN, is one of the main features present in MikroTik's RouterOS. It allows managing multiple Access Points and gives the network administrator a possibility to configure, monitor and manage all the Access Points centrally. This is particularly useful in high-access point environments, such as campuses or large office buildings, where each of the access points used to be managed manually. It would have been overly time-consuming and error-prone.

The major features of CAPsMAN include SSID management, setting up security parameters, channel controls, and firmware management for access points. At the essence of CAPsMAN is that once it is used, any configuration changes can be applied concurrently to all managed access points, this provides uniformity and hence ease of administration. administrators can easily add or replace access points without the need to change the entire network configuration.

SFQ or Stochastic Fairness Queueing, definitely is one of the queuing strategies mostly used in policing network traffic. SFQ classifies arriving packet flows into multiple sub-queues by using a hashing method. The prime purpose of SFQ is avoiding dominating all network bandwidth by one data flow.

One such solution with MikroTik in regard to load balancing of the incoming traffic or packet flow that could avert congestion on the network is SFQ. This technique is very useful, especially in scenarios where many users are logging into the network simultaneously for example, public hotspots or campus networks. By implementing SFQ, the network administrator is assured of relatively equal bandwidth distribution among the users, hence reducing the chance of high latency or heavy packet loss.

Implementation of this book

This book deploys the SFQ technology that can be used for balancing traffic over a wireless network using the CAPsMAN system for access point management. The methodology to be implemented in this book is to use four routerboards: among them, one as the gateway controller access point, that is, CAPsMAN, another as the voucher based hotspot server gateway, that is, userman, and the rest as the three different CAPs, all running

connected to a switch. The output process is measured against the requirements of TIPHON for wireless links. Some test parameters covered in this book include throughput, packet loss, roaming, jitter, and wireless coverage using vouchers.

This book aims to offer proof of the practical functioning of a wireless network system, namely CAPsMAN and Hotspot Server using the SFQ methodology. It tries to evaluate the performance of the network system through throughput, delay, jitter, packet loss, and roaming, and also finds out the most suitable SFQ values. Such an in-depth analysis of the benefits and limitations of a network system is expected to provide some important and useful inputs into the development of wireless networks that are reliable and efficient.

B. Existing Theories

There are several fundamental theories in computer networking and telecommunications that support the integration of CAPsMAN and Hotspot solutions into network management. These theoretical frameworks work to increase the efficiency and reliability of these technologies, making them functional to their expected purposes. This brings to mind the theory on centralized network management. Centralized management, as defined with the CAP's MAN implementation principle, enhances efficiency and consistency by managing the whole network from a single central point of control. It can thus enforce uniform policies and configurations on access points, reducing configuration errors and ensuring optimal user experience end to end. Also, this approach makes the networking process easier because new access points are accepted into the network with fast automatic configurational settings without manual interference at each device, therefore saving time and increasing the productivity level in general for networking systems (Paillissé et al., 2020). The network administrators' management is centralized in an effective manner for monitoring, configuring, and maintaining the entire network infrastructure from a single joint interface to carry better visibility, control, and optimization of the wireless environment (Jha & Karandikar, 2018).

One of the key concepts in network management is the implementation of queuing mechanisms, and one of them is Stochastic Fairness Queueing. SFQ is an algorithm premised on the notion that users should equally share bandwidth. SFQ breaks new traffic into many subqueues by hashing techniques so that one data stream cannot use more than another data stream of the available bandwidth in the system, this in turn, overcomes

congestion in the system and ensures every end user enjoys his or her fair share of the shareable resources. This is done through hashing techniques to ensure that no one data stream uses a higher proportion of available bandwidth in a network. Doing this ensures avoidance of congestion, and it makes sure every user gets fair access to shareable resources. This comes in handy with high-density settings like public hotspots or campuses where there are many users connected at the same time with assured service levels. SFQ divides available bandwidth into equal shares through which different flows have flowed in with fairness, not allowing one user or application to choke the links and consequently degrade the overall experience for the other linked users (Zeng et al, 2009).

Access control and security principles are very crucial in hotspot solutions. For instance, the success of user authentication mechanisms and principles is seen through the measures governing issues like voucher-based access or mechanisms for individual user registrations. Such undertakings are very critical in ensuring a great level of precaution against unauthorized use and possible threats to the integrity of the network. Additionally, users' activity monitoring also provides important information applied in the identification of any abnormal activities suggestive of suspicion of activity in order to further reinforce the network security configurations. The same information is also applied in analyzing several potential vulnerabilities and proactively mitigate emerging threats to network infrastructure and its connected users by Zhao et al., 2019.

Quality of service theoretical framework also supports the application of the two technologies: CAPsMAN and Hotspot. The fundamental objective of QoS principles is to offer network performance that ensures the adequate provisioning of bandwidth, no latency-related problems, and an absolute reduction in packet loss incidents (Quality Of Service, 1995). The strict implementation of relevant policies that would preferentially select only mission-critical services and applications is an inextricable aspect of this paradigm to ensure reach to the best operational efficiency levels. This is very crucial for all types of traffic, heterogeneous in nature, such as video, VoIP, and data transfers, to be successfully carried out at the same time without degrading quality of experience. On the other hand, admins ensure that bandwidth is effectively shared and prioritized through QoS, which keeps the performance resilient and does not allow any one application or user to dominate the given resources and hence deteriorate the experience for the rest of the network.

The overall functionality, stability, and security focus in wireless networks are enhanced with basic theories and principles integrated into practical realization concerning CAPsMAN and Hotspot solutions (Sen & Sivalingam, 2015). Network administrators can, therefore, use this unique advantage of centralized administration of networks to set equitable traffic allocation policies that will cater to quality-of-service, and include in the process of implementing network systems which are efficiently managed, scalable and operationally resilient that entail strong security. These technologies, both conceptually and strategically interwoven, avail network administrators with the capability to address dynamic needs and diverse requirements of modern user communities befittingly with their infrastructure wireless (Costa & Yang, 2020).

The configuration and management of the Wireless devices that are connected to this network, the feature of MikroTik networks, is CAPsMAN. CAPsMAN allows administrators one system to control and manage all wireless devices, hence harmonizing configurations of the SSID, security, and all other wireless settings. This reduces configurations in environments with many access points since central control ensures uniform configurations.

Moreover, another great strength of MikroTik is in the management of network hotspots. A hotspot refers to a wireless internet network through which a user is able to connect to the internet in some specific locations such as cafes, hotels, airports, and other public places. It can further be configured to offer full-service hotspots, such as user management, bandwidth control, login with portal features, and integration with authentication systems among others (Hidayat et al., 2022). Centralized management and configuration of wireless devices within the domacile are all crucial to the performance of an indoor wireless network, that is achievable with the CAPsMAN. Another feature of the MikroTik that can be useful for deploying hotspot services is the built-in Hotspot feature. This makes MikroTik an ideal solution for building controlled and efficient hotspot networks.

CAPsMAN makes it easier to control and manage all wireless devices centrally, works effectively with other MikroTik features, and allows flexibility when setting parameters for the network. It will not be comfortable to manage an indoor wireless network without using CAPsMAN, since every device has to be configured separately. Dewi & Islami, 2021. In the case that where CAPsMAN does not support hotspot services, it would be a complicated process with difficulties in managing the login portals, user authentication, and allocation of the desired bandwidth.

For instance, setting up the 100 access point configuration independently would be a huge task without integration, and it includes marking out its differences in the wireless frequency, which adds another layer of complication to the management of networks in public locations that require this precise, constant, constant, and timely maintenance of information (Hidayat et al., 2022).

Such, use of CAPsMAN and the hotspot feature by MikroTik, is set to have effectively managed indoor wireless networks and hotspot services. The combined CAPsMAN allows a rather simplified process of full management of networks to ensure all devices operated under a uniform kind of configuration, hence its network efficiency and reliability. The centralized management is not only easy but also leaves configurations without lots of human touch errors. As such, the wireless environment is more stable and user friendly.

C. TCP / IP

The abbreviation Transmission Control Protocol/Internet Protocol, TCP/IP, is widely recognized in the Internet community. As a result, it is a popular data communication standard. The major role that it plays is in enabling computers connected to the Internet network to exchange information smoothly and efficiently. According to Bernaschi et al. 2009, TCP/IP operates as a composite of interconnected protocols commonly known as protocol suite, but it does not act independently. In general practice, TCP/IP implementation is carried out through software integration within operating systems, which are usually known as "whether the TCP/IP stack" (The TCP /IP Protocol Suite 1997). This enables the smooth running of administrative operations in respect to providing the required functionalities and the regulations incumbent on ensuring Interoperability while engaging multi-variate computer systems wired into totality on glocal scale networks. Langenbach et al. (2013), there also confirm its importance to making the motive of allowing effective transmission with ease across these cumbersome structures at any one period of demand. The TCP/IP architecture depends on the OSI (Open Systems Interconnection) model, which consists of seven different layers physical, data link, network, transport, session, presentation, and application.

Such a layered structure is intended to give a broad framework for hardware and network designers regarding interoperable systems, focusing explicitly on the development of effective and efficient machine-to-machine

functionality. An explicit boundary between each layer allows the designers to focus on the properties of the system at each layer while at the same time it assures compatibility with the overall philosophy in the design. In addition, this modular approach also promotes diversity in the development of networking components that are able to interoperate with one another smoothly and, therefore, resilient communication networks that scale at an exponential rate through time, this is according to Doherty and others in 2008. By strictly following the clear responsibilities and interactions presented by each OSI layer, the designers are in a position to come up with flexile, supportable, and reliable solutions designed specifically to tackle problems of a contemporary computing nature according to Solvie in 2005. TCP/IP has a significant function in the networking of Mikrotik, as it is the foundation around which central communication and data management protocols are checked.

Most beneficial attributes of Mikrotik are the CAPsMAN attribute, which helps in configure and monitor wireless devices connecting to the network according to Zhang, & Liu (2013). In capsman, administrators can have a centralized control of the wireless clients under one integrated system, in other words, the whole process of setting up a wireless network is made more accessible and the job of centrally changing the configuration relating to the SSID parameters, the security measures among other attributes that apply to the wireless interfaces, easier and more straightforward (Cheng, Yang, 2006). This is not to mention that Mikrotik delivers hotspot features: extremely useful for enabling one to build well-managed and secured wireless access points.

This, therefore, allows the network to easily bring users on board, providing services to them accordingly without failure or security compromise on the network (Arta & Nugraha, 2020). When these powerful capabilities, including but not limited to features found in TCP/IP à mated with the in-use functionality in CAPsMAN and Hotspot, administrators can be able to design for themselves a relatively broad but highly efficient structure for their wireless networks in the provision of services to all manners of users across devices. Being managed centrally, this approach not only increases efficiency but also ensures consistency and improves deployability while considering several access points and their clients wirelessly connected. The Mikrotik RouterOS provides a feature where CAPsMAN stands for Controlled Access Point system Manager. This allows for centralized configuration and control for all the multiple wireless access points. This gives network administrators the widest solution to supervise and control the Wireless Info-structure with efficacy (Naman et al., 2020).

With the help of CAPsMAN, numerous access points can be easily added, controlled, and supervised on a single interface. This approach is very beneficial and indeed comes in handy for settings with huge numbers of such access points college campuses or vast office complexes since doing this manually would be cumbersome and prone to errors (Lin & Tsai 2015).

The critical features of CAPsMAN include management of service set identifiers (SSIDs), security profile settings, channel configuration, and access point software updating. With such a feature in place, system administrators centrally synchronize configuration changes to all access points under control, thus avoiding inconsistency and making the management of wireless networks much easier and more realistic. This finally leads to better overall systems performance, with lower chances for configuration errors, as the changes are automatically propagated. (Ducret et al., 2017).

Besides, CAPsMAN readily allows the addition or replacement of access points in the network. It, therefore, becomes quite easy for network administrators to introduce new access points or replace existing access points without any hindrances to the general configuration of the whole wireless infrastructure (Lin & Tsai, 2015). Such flexibility makes it possible for networks to adapt to changing requirements and expand as it is needed by users and the devices themselves.

CAPsMAN is a powerful integrated feature found at the Mikrotik RouterOS that makes centralised management and configuration of multiple wireless Access Points. The use of CapMAN allows all access points to be configured, monitored, and controlled through one central access point easily. This centralized management interface gains far more importance in the case of large scale deployments, like a large office or campus with numerous access points, that would otherwise need to be done manually for each device, leading to drudgery and a lot of errors bound to be made in the process (Lin & Tsai, 2015). The primary functions of CAPsMAN encompass the management of SSID, security settings, channel selection, and access point firmware updates.

With such potent capabilities, network administrators can easily apply configuration changes in a consistent way across all managed access points, thereby accelerating wireless network management while reducing potential misconfigurations (Dezfouli et al., 2019). The general networking performance is improved, and the general likelihood of potential misconfigurations is easily reduced by these mentioned functionalities, since every update is immediately reflected across the breadth of the

system. Similarly, CAPsMAN makes it easier to add or change access points throughout a network. This task is no longer something that needs to have the entire system reconfigured, as new access points or changes in access points can be introduced without significantly causing disruption to the network ecosystem. This real-time adjustment is what makes networks able to adapt and grow with the changing demands from people and their devices as well.

Mikrotik installs an integrated hotspot application that allows the configuration of secured and controllable wireless access points.

A hotspot always paves a way for users to connect to certain places, including cafes, hotels, and airports. One can also configure Mikrotik to provide full hotspot services and features of a login portal, which includes user management, bandwidth control, and integration of the authentication system. In the indoor WiFi networks, it is the key point to have centralized setup/management functionalities for the CAPsMAN, while utilizing the hotspot feature, allows effective implementation of a wireless access solution in an effective way. Combining the two functionalities on offer at CAPsMan and MiKroTiks in terms of their respective "Hotspot" functionality can help get put in place a well-managed Wi-Fi infrastructure that serves your organizational needs in an efficient way. The supplied Mikrotik CAPsMAN feature provides many advantages.

Firstly, it can be used to control and manage wireless devices centrally, resulting in easier administration of the network. Furthermore, CAPsMAN can be combined best with other major features, such as hotspot support provided by Mikrotik, and it provides a better performance system. In addition, its flexible deployment options allow network parameters of critical nature, such as routing protocols and security policies, to be quickly tailored with ease, ensuring effective use of resources while overseeing all aspects of ad hoc network establishment. It is worth noting that, without these powers in place, utilizing such applications as CAPsMAN capability, Access Points would quickly become complex entities that would require individual configurations per device, overburdening the admin efforts that are otherwise avoidable if one adheres completely to the centralized control mandates in place at deployment onset stages, respectively prepared beforehand or during assessment phases conducted preinstallation and proactively vetting the likely contingencies that will be inevitably encountered throughout lifecycle operations under various circumstances, warranting changes / maintenance concerns met associatively over time (Wireless High Client Density Design Best PracticesCompendium). The Mikrotik network infrastructure is, in turn, based on the TCP/IP protocol

suite, which is a protocol suite running the basics of communication and data management.

There are many different protocols running at the application layer, namely: FTP, SMTP, and TELNET, they provide all the necessary services that user applications need. In a study carried out by Vasseur & Dunkels 2010, it has been identified that TCP, through its dependability on error control plus its delivery mechanisms, using Transport Layer Protocol (TCP) ensures that there is seamless transmission to the end points of interest while ensuring flawless provision free of faults. This is applied at the network layer by the use of the Internet Protocol. IP in a routing data between the source and the points of interest.

Inside the Network Layer of the TCP/IP model lies a collection of functions that pertain to the manipulation of IP addresses and the associated routing algorithms intended to direct information properly. Peripheral protocols, commonly referred to as Address Resolution Protocol, with its "companion", Reverse ARP, adding basic functionality to locate physical hardware on a network with their corresponding IP addresses, which is a fundamental capability used on local area networks. The Address Resolution Protocol (ARP) maps the physical addresses to IP addresses.

Within Local Area Network (LAN), a host and even a router are also identified by their respective private physical addresses assigned by the NIC. In the network, it is possible to solicit information about the physical address of another host or router on the same local network by sending out an ARP query packet in a broadcast manner. This process allows all remote routers and hosts from within another network to be listening out for signals for an incoming request. However, only one will be responsive, which is the one that has the matching IP address that corresponds to the one within that ARP query message. The receiver then receiving such reply will in turn forward relevant information about both the Internet protocol and relevant physical locations back to the original sender by unicast means. Address Resolution Protocol optimizes network performance and security.

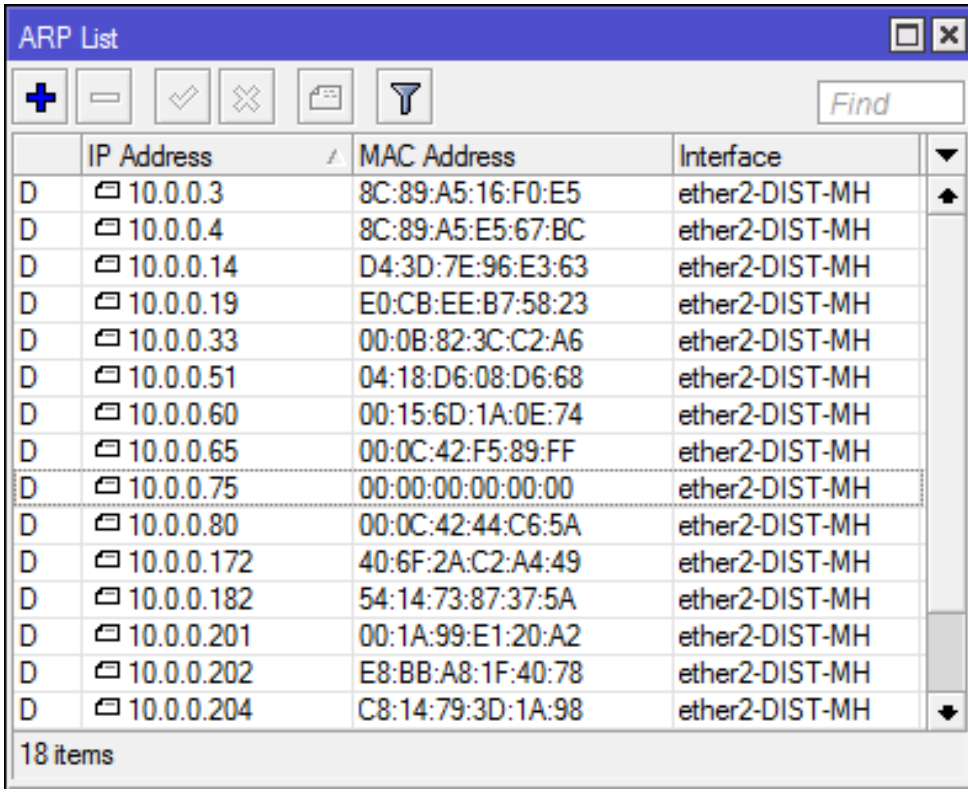

Figure 1. ARP Model

With regard to the network layer, it is IP that serves as a means by which data paths originating from a particular source may be directed towards their intended destination. The Network Layer incorporated in TCP/IP protocol suite assumes responsibility for managing Internet Protocol (IP) addresses along with routing processes designed to ensure unencumbered delivery of data packets and subsequent receipt at accurate destination locations (Overview of TCP/IP, 2010). Given ARP or Address Resolution Protocol and RARP or Reverse Address Resolution Protocols play an instrumental role in mapping physical address designations - such as MAC Addresses - onto assigned IP Addresses while conversely accommodating reverse protocols crucial within existing Local Area Networks (LANs)- wherein this functional framework proves indispensable.

The Address Resolution Protocol (ARP) is a fundamental element that facilitates efficient communication within a Local Area Network (LAN). It operates by associating logical IP addresses with their corresponding physical Media Access Control (MAC) addresses. Whenever there is a need

for one host or router to communicate with another device in the local network, it first requires knowledge of the target device's physical address. To obtain this information, an ARP query packet requesting matching hardware details will be sent as broadcast and received by all hosts and routers connected directly to the same LAN segment (Carthern et al., 2015). The process continues whereby only those devices having compatible IPs respond accordingly, such responses facilitate storage of necessary mappings needed for future direct data transmission using known diverse MAC identities. Notably, this protocol remains indispensable when translating logical IP into Physical Addresses required for confined data transmissions across different applications used on various LANs (Bradley & Brown, 1992).

The Address Resolution Protocol (ARP) is an integral constituent in Local Area Networks (LANs), serving the purpose of establishing correspondence between physical addresses, namely Media Access Control (MAC) addresses and their associated Internet Protocol (IP) counterparts. In a LAN setting, each piece of equipment such as routers or hosts can be recognized by its unique physical address which has been retrieved from the Network Interface Card (NIC). This information was sourced from "Address Resolution Protocol" published in 2017.

In order for a host or router to establish communication with another device within the same local network, it is imperative that it ascertain the physical address of said target device. This information may be obtained through transmission of an ARP query packet using broadcast methodology, thereby enabling all hosts and routers in the localized network to receive it. Nevertheless, only those devices whose IP addresses match the transmitted ARP query are expected to respond by disclosing their respective physical addresses. The initiator of such a request will then proceed to save this mapping between IP-to-physical address data points which serves as evidence for direct communication with aforementioned targeted equipment (Song et al., 2014).

The Address Resolution Protocol (ARP) holds great significance in facilitating streamlined data communication within a Local Area Network (LAN). Its primary function involves enabling devices to convert logical IP addresses into physical ones, thus allowing direct and efficient transmission of data. A thorough comprehension and diligent application of ARP alongside other pertinent TCP/IP principles as well as Mikrotik functionalities such as CAPsMAN and hotspot services can aid network administrators in establishing dependable indoor wireless networks that cater to the constantly evolving demands of both users and devices. This

notion is supported by scholarly sources including Zhang & Liu's 2013 study along with Wang et al.'s research from 2023.

TCP/IP Calculation in Networks Calculating TCP/IP in networks is an essential skill for network administrators. TCP/IP is the protocol used for communication between devices on a network. It is important to understand how to calculate TCP/IP to ensure that the network is functioning correctly. One common calculation used in TCP/IP is subnetting. Subnetting is the process of dividing a network into smaller subnetworks. This is done to improve network performance and security. To calculate subnetting, you need to know the network address, subnet mask, and the number of subnets required. Another important calculation is determining the IP address range. This is done by using the subnet mask and the network address. The IP address range is the range of IP addresses that can be assigned to devices on the network. In conclusion, understanding TCP/IP calculations is crucial for network administrators. It allows them to properly manage and maintain the network, ensuring that it is functioning at its best.

Performing TCP/IP calculations in networks is crucial to ensure efficient and reliable network operations. This process involves various aspects, such as IP addressing, subnetting, and routing management. Here is a detailed explanation of how to perform TCP/IP calculations in a network.

IP addressing IP addressing is a fundamental concept in computer networking. It is a method of assigning unique numerical identifiers to devices connected to a network. An IP address is a 32-bit number that is divided into four 8-bit segments, each separated by a period. The four segments are called octets. An example of an IP address is 192.168.1.1. There are two types of IP addresses: IPv4 and IPv6. IPv4 is the older version and uses a 32-bit address space, which limits the number of unique addresses that can be assigned. IPv6 is the newer version and uses a 128-bit address space, which allows for a much larger number of unique addresses. IP addresses are used to identify devices on a network and to route data between them. They are also used for security purposes, such as to restrict access to certain resources or to track the source of network traffic.

An IP address is a numerical label used to identify devices on a network. There are two commonly used versions of IP addresses: IPv4 and IPv6. IPv4 uses a 32-bit address divided into four octets, while IPv6 uses a 128-bit address consisting of eight groups of hexadecimal digits.

An example of an IPv4 address is 192.168.1.1.

Here is a corrected version of the text: Example of an IPv6 address: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

Subnetting is the process of dividing a network into smaller subnetworks, called subnets. This is done to improve network performance and security. Subnetting allows for better management of IP addresses and reduces network congestion. It also helps to isolate network problems and contain security breaches. To subnet a network, you must first determine the network address and the subnet mask. The subnet mask is used to identify the network and the subnet. Once you have determined the network address and the subnet mask, you can then divide the network into subnets. Each subnet will have its own network address and subnet mask.

Subnetting is the process of dividing a large IP network into smaller networks or subnets. This helps to reduce network congestion and increase security. Subnetting involves calculating the number of subnets and the number of hosts required for each subnet.

IP addressing in IPv4 subnetting involves several steps. Firstly, we need to determine the subnet mask. The subnet mask defines which part of the IP address is the network identifier and which part is the host identifier. For instance, a subnet mask of 255.255.255.0 means that the first three octets are the network identifier, and the last octet is the host identifier.

The formula for calculating the number of subnets is 2^n, where n represents the number of bits borrowed from the host portion for subnetting. For example, if we have an IP address of 192.168.1.0/24 and we want to create four subnets, we need to borrow two bits (since 2^2 = 4). Therefore, the new subnet mask becomes /26 (24 + 2).

The formula for calculating the number of hosts per subnet is 2^h - 2, where h represents the number of host bits that remain after subnetting. The subtraction of two is necessary to account for the network address and the broadcast address. For instance, with a /26 subnet mask, there are 6 bits left for hosts (32 - 26 = 6). Therefore, the number of hosts per subnet is 2^6 - 2, which equals 62 hosts.

Therefore, we have 4 subnets, each with 62 hosts.

Subnet 1: 192.168.1.0/26 (192.168.1.1 - 192.168.1.62)

Subnet 2: 192.168.1.64/26 (192.168.1.65 - 192.168.1.126)

Subnet 3 is 192.168.1.128/26,

which includes IP addresses ranging from 192.168.1.129 to 192.168.1.190.

Subnet 4: 192.168.1.192/26 (192.168.1.193 - 192.168.1.254)

Routing is the process of selecting a path for traffic in a network. It involves determining the most efficient way to send data packets from one network to another. Routing is essential for the proper functioning of the internet and other computer networks. There are two main types of routing: static and dynamic. Static routing involves manually configuring the routes that data packets will take. Dynamic routing, on the other hand, uses algorithms to automatically determine the best path for data packets based on network conditions. Routing protocols are used to facilitate the exchange of routing information between routers. Some common routing protocols include OSPF, BGP, and RIP. Overall, routing plays a crucial role in ensuring that data is transmitted efficiently and reliably across networks.

Routing is the process of determining the best path for data on a network. Routers use routing tables that contain information about known networks and how to reach them. The calculation of the routing table involves two main steps.

First, the router builds the routing table by gathering information from directly connected networks and dynamic routing protocols such as OSPF or BGP. Second, the router uses algorithms like Dijkstra or Bellman-Ford to calculate the best path based on metrics such as hop count, bandwidth, and latency.

For example, let's consider three networks: 192.168.1.0/24, 192.168.2.0/24, and 192.168.3.0/24. Router A is connected to the 192.168.1.0/24 and 192.168.2.0/24 networks, while Router B is connected to the 192.168.2.0/24 and 192.168.3.0/24 networks. Router A and Router B are connected via the 192.168.2.0/24 network.

The routing table on Router A may appear as follows:

The correct sentence is: "Network 192.168.1.0/24 is accessible via the interface eth0."

"Network 192.168.2.0/24 is accessible via the eth1 interface."

"Network 192.168.3.0/24 is accessible via Router B."

Router A will have an entry in its routing table indicating that the 192.168.3.0/24 network can be reached through Router B, which is connected via the 192.168.2.0/24 network. This ensures that any data packets destined for the 192.168.3.0/24 network are directed to Router B.

D. Quality of Service (QoS) in Wireless Networks

The concept of QoS, or Quality of Service, is a critical element within the field of networking. It refers to the measurement and evaluation of network performance while defining service properties and characteristics. As outlined by Paul Ferguson in his work entitled "Quality of Service," it involves assessing multiple dimensions related to specific services in order to optimize their efficacy within Internet Protocol (IP)-based networks with packets traveling through one or several interconnected systems. QoS plays an important role in enhancing end-users' productivity as they rely on network-based applications that require dependable functionality regardless of bandwidth constraints caused by other forms traffic transmissions from various sources sharing those same communication pathways between endpoints. Consequently, this technology encompasses different solutions designed for delivering better user experiences via advanced technologies aimed at optimizing device operating efficiencies capacity handling functions consistently. However, adequately implementing QoS protocols across IP-networks poses significant challenges relevant even beyond intuitive frameworks because satisfying varying needs while using shared infrastructure demands fulfilling diverse requirements supported properly based on qualitative evaluations when offering defined quantitative levels for differing attributes-network services' configuration achieves optimal results thus ensuring congruous network data flows along its transit points according. In summary: The essential characterisation-Quality-of-Service(QOS)is vital foundational basis integral towards sustaining Networking competence whose measurements evaluate-internet performances whilst encapsulating core-service-properties-functions.by supporting expedient functionally capabilities reliant upon these concepts, efficiency optimisations usable cross-depiction-transmissions,it provides consistent high-end-output-quality productions valued-launched-data-flows inclusive-designing-equations more amenability observational quantification's effectively improving-user-experience per such metric agreeance delivery requisite parameters accomplishing operational conversation guidelines-productively fulfilled underparticipating-consumption subdivisions-underlining technical-requital measures exceed speed efficaciousness strategies efficiently

enabled throughout multicast archives-standardization-consistent appreciable-client synergy accomplishment advancements held DevOps culture-dependant harmony thriving concurrently AF reconfigurable management etrix attainment for oft-shared systems/subsystems.

Within the realm of networking, Quality of Service (QoS) pertains to the capacity to furnish distinct tiers of service catering towards various classifications for network traffic. The primary objective behind QoS is enhancing and heightening predictability in network services by procuring dedicated bandwidths, regulating latency levels as well as refining loss characteristics. Fundamentally, QoS ensures uninterrupted provision of vital data streams through a compilation performance criteria that gauge customer satisfaction with regard to a particular servicedomain.

QoS analysis entails the computation of various crucial parameters, which are referred to as 'protocols'. These protocols hold significant importance in accurately measuring and assessing QoS. Bandwidth pertains to the width or range of frequencies employed by a signal in a transmission medium. The frequency of signals is quantified in Hertz (Hz). Within computer networks, bandwidth frequently denotes data transfer rate - that being the volume of information transmitted between two points within an allocated time interval measured typically in seconds. This type of bandwidth is usually expressed as bits per second (bps).

Throughput refers to the measurable bandwidth utilized over a designated interval for transmitting an allocated quantity of data. Optimal download time is achieved by dividing file size by bandwidth, whereas actual time involves division of file size by throughput. Packet loss is a phenomenon that refers to the failure of data packets to successfully traverse the network. Causes may include excessive network traffic, congestion, errors in physical media and receiver-side issues such as router buffer overflow.

The term "delay" denotes the duration of time that is necessary for data to travel from one point (origin) to its destination. There are several contributing factors that exert a considerable impact on delay, namely distance, physical media involved in transmission, traffic congestion levels and processing times. Wireless networks, particularly those under the management of MikroTik devices, attribute considerable importance to QoS in ensuring optimal and dependable service delivery. The RouterOS software from MikroTik provides a comprehensive QoS framework enabling system administrators to regulate bandwidth allocation, prioritize traffic flow and minimize latency accompanied by packet loss. This implementation ensures that crucial applications are allocated adequate

resources resulting in an overall enhancement of network performance for heightened user satisfaction. In a wireless network setting, it is crucial to maintain sufficient bandwidth for prioritized applications such as Voice over IP (VoIP) or streaming services. Bandwidth management entails the allocation of distinct portions of available bandwidth based on users' and applications' priority levels. Utilizing Quality of Service (QoS) protocols enables administrators to reserve ample bandwidth for critical applications while preventing lower-priority traffic from monopolizing all accessible resources.

It is imperative that the measurement of effective data transfer capacity, commonly referred to as throughput, be continuously evaluated and enhanced. In a wireless environment, several factors including signal interference , proximity to access points and quantity of connected devices have an impact on throughput rate. By adjusting Quality-of-Service (QoS) settings in MikroTik technology solutions these variables can be effectively managed thus ensuring steady network performance standards are maintained.

The maintenance of high service quality is contingent upon the minimalization of packet loss, particularly concerning applications that are susceptible to data loss - for instance, video conferencing or online gaming. MikroTik bears QoS mechanisms which have proven effective in identifying and reducing potent sources of packet absence: namely network congestions as well as physical layer anomalies.

Latency, or delay, constitutes a crucial element in ensuring Quality of Service (QoS). Applications that heavily rely on real-time interaction - such as online gaming and Voice over Internet Protocol (VoIP) communication - are particularly vulnerable to adverse effects from high latency. QoS policies can strategically prioritize these applications by regulating traffic flow and limiting congestion so they may operate with minimal delays.

As a final consideration, it is worth noting that Quality of Service (QoS) constitutes an essential element of network management aimed at guaranteeing the delivery of reliable and efficient services. Through knowledge acquisition and implementation efforts pertaining to QoS principles and configurations, network administrators can considerably augment wireless networks' performance while simultaneously fulfilling varying end-user requirements across applications.

Firstly, we need to determine the total available bandwidth on the network. Suppose we have an internet connection with a total bandwidth of 100 Mbps from our Internet Service Provider (ISP). To ensure that high-

performance applications such as Voice over Internet Protocol (VoIP) and video streaming receive optimal service, we decide to allocate 50 Mbps specifically for these applications. The remaining 50 Mbps is then allocated for other types of apps like web browsing and email.

Throughput measures the actual speed of data transferred through a network over a specific period. Suppose during a one-minute observation, we note that VoIP and video streaming applications transfer 2700 Megabits of total data. To calculate throughput, we use the formula:

Throughput equals the total amount of data transferred divided by the time it took to transfer that data. The formula is expressed as: Throughput = Total Data Transferred / Time.

With a total data transfer of 2700 megabits and an observation time of 60 seconds, the throughput can be calculated as follows:

Throughput equals 2700 Megabits per second divided by 60 seconds which results in a throughput of 45 Mbps.

This result shows that the actual throughput for VoIP and video streaming applications is 45 Mbps out of the allocated 50 Mbps. This indicates that the bandwidth allocation for these applications is sufficient, since the throughput is close to the maximum allocated bandwidth.

Packet loss measures the percentage of data packets that were lost during transmission through a network. For instance, in an experiment where we sent 1000 data packets and received only 980 back, we can calculate packet loss using this formula:

Packet loss is calculated by subtracting the number of packets received from the total number of packets sent, dividing that result by the total number of packets sent, and multiplying it by 100%. The formula should be written as: PacketLoss = (Packets Sent – Packets Received) / PacketsSent * 100%

With 1000 packets sent and 980 packets received, packet loss can be calculated as follows:

Packet loss is calculated by taking the difference between 1000 and 980, dividing it by 1000, then multiplying that result by 100%. The correct calculation shows a packet loss of only 2%. So the corrected version would read: Packet Loss = (1000 -980)/1000 x % = 2%

This result indicates that 2% of the data packets are lost during transmission. A packet loss rate of 2% is acceptable for most applications, including VoIP and video streaming, which require high reliability.

Delay or latency measures the time taken by data to travel from its source to destination. If we consider measuring round-trip time (RTT), i.e., the duration that a packet takes traveling between sender and receiver, it amounts on average 40 milliseconds (ms). In order to compute one-way delay, we simply have divided RTT by two:

The corrected text is: Delay = Round-Trip Time / 2.

The delay can be calculated as follows with a round-trip time of 40 ms:

The corrected text is: Delay = 40 ms / 2 = 20 ms.

This result indicates that the duration required for data transmission from sender to receiver is 20 ms. A delay of this magnitude proves advantageous for real-time applications such as VoIP, which necessitates minimal latency in order to sustain optimal voice quality.

In summary, let's consolidate all of these calculations into one scenario. We have a total bandwidth of 100 Mbps with 50 Mbps allocated for high-priority applications such as VoIP and video streaming. During observation, the measured throughput for these applications is 45 Mbps. The measured packet loss rate was found to be at 2%, while the delay amounted to just over twenty milliseconds (20 ms).

With these parameters, it can be seen that the QoS configuration works well. The allocated bandwidth matches the needs of critical applications and the measured throughput is close to the given bandwidth allocation, indicating efficient network usage. The low packet loss rate of 2% shows that the network is reliable while a delay as low as 20 milliseconds ensures good performance for real-time applications.

In a wireless MikroTik network, proper QoS configuration ensures that high-priority applications receive sufficient resources while other applications continue to function effectively. This not only enhances the quality of service but also helps maintain user satisfaction and operational efficiency. By continuously monitoring and optimizing QoS parameters such as bandwidth, throughput, packet loss, and delay, we can ensure that the wireless MikroTik network operates optimally and meets the needs of all users.

E. PCQ

Per Connection Queue (PCQ) is a smart way to manage internet speed on MikroTik devices. It creates smaller streams based on different characteristics of each user's connection, like IP address or port number. This helps make sure everyone gets a fair amount of bandwidth when lots of people are using the network at once.

Let's say there are two computers downloading files on a network. PCQ will divide the bandwidth into two parts, one for each computer. If 50 devices download at once, it creates 50 equal parts to share the bandwidth fairly. The cool thing about PCQ is that it can change how many parts based on how many connections there are so everyone gets an even amount of speed. PCQ works by splitting up the total available internet speed so that everyone gets a fair amount. For example, if there are 50 people downloading at once and the total speed is 100 Mbps, each person will get an equal share of it.

The amount of bandwidth each host gets equals the total amount of bandwidth divided by the number of hosts. Using the numbers from this sample:

Each host has a bandwidth of 2 megabits per second. This means that if there are 50 hosts, they will share 100 Mbps equally.

This makes sure that every device gets 2 Mbps, so the network stays steady.

Let's look at an example to understand how it works. Say there is a network that has 200 Mbps total speed and employees in the office can download or upload data at the same time from their own computers. The aim is to divide up bandwidth fairly, so no one computer uses too much of it. We make settings on the MikroTik router to distribute internet equally. It will sort data based on where it comes from (IP address), treating each one separately.

When the number of people using a website changes, the PCQ automatically adjusts how much internet speed each person gets. For example, if there are 10 people downloading things from the site:

Each user has a bandwidth of 20 Mbps.

If 40 people start using the app:

Each user has 5 Mbps of bandwidth, which is determined by dividing the total of 200 Mbps among a group of 40 users. With PCQ, everyone gets an equal amount of internet speed that changes if more people join or leave. This makes sure no one uses too much bandwidth and slows down the network for others.

Let's learn more about setting up MikroTik. We use a tool called Winbox to configure it, and create a type of configuration for bandwidth using PCQ. In the Queues section in Winbox, we specify rules like source address and set limits on how much data each person can use so that everyone gets their fair share without hogging all the bandwidth.

To set up the PCQ, we need to do a few things on our computer. First, go into Winbox and select Queues. Then choose Queue Types and add a new one called PCQ. Next, we set some rules for how it will work by selecting src-address classifiers and setting max limits so everyone gets an equal share of bandwidth. Lastly, apply this setup to your internet connection (like ether1) using something called Queue Tree that references the earlier created queue type "PCQ".

This settings makes sure that the PCQ rules control all traffic on the interface. It splits up bandwidth fairly based on how many people are using it, so everyone gets a fair amount of network resources.

Simply put, PCQ is a great tool for controlling the amount of data each user can use in MikroTik networks. It creates different sub-streams based on things like IP addresses and automatically changes how much bandwidth each one gets as more people connect or disconnect. This keeps everyone's internet speeds fair and prevents problems with slow connections caused by too many people using the network at once.

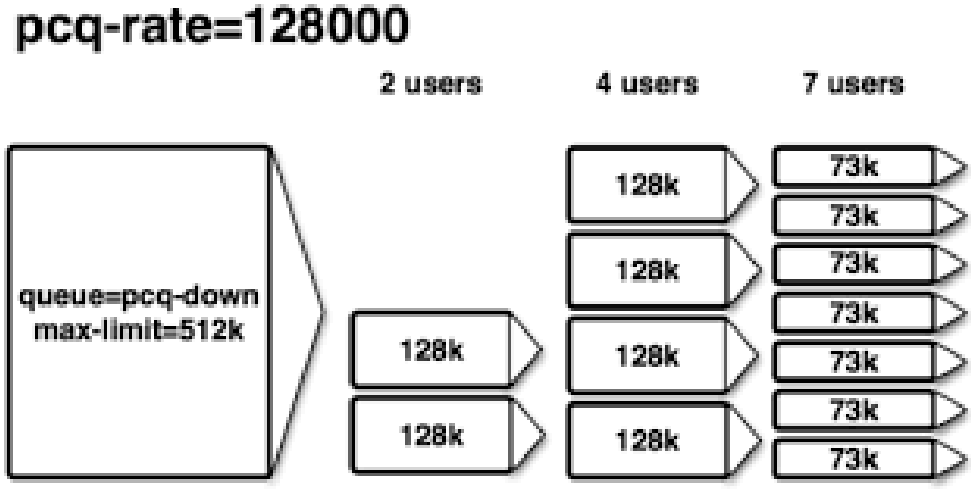

Figure 2. Concept of PCQ in Mikrotik

F. SFQ

Stochastic Fairness Queuing (SFQ) is an advanced queuing algorithm that has been specifically devised to achieve equitable allocation of network traffic in conditions where a signal link reaches its saturation point. This sophisticated mechanism can be deployed for both TCP and UDP transmissions, with the operational principle being based on segmenting incoming data into 1024 sub-queues by implementing give-and-take hash functions alongside round robin methods. Should the number of available queues surpass this boundary value, superfluous packets will be discarded as proactive measures to preserve fairness across connections -such approach proving particularly effective when implemented within heavily loaded networks.

The fundamental operation of SFQ entails the utilization of a hashing function to allocate incoming data packets onto one among 1024 sub-queues. This allocation is executed via an analysis of specific attributes within each packet, including source and destination IP addresses. The mathematical representation for this mapping procedure can be expressed as follows:

The proposed revision is as follows, Calculate the hash value by applying a Hash function to the source and destination IP addresses, followed by computing its modulo with respect to 1024. This can be represented mathematically as hash = (HashFunction(src_IP,dst_IP) mod 1024).

The aforementioned formula exemplifies the operational mechanism of the hash function, which entails processing both source and destination IP addresses to yield a remainder after division by 1024. The quotient determines the specific sub-queue where each packet will be assigned probabilistically among all available options.

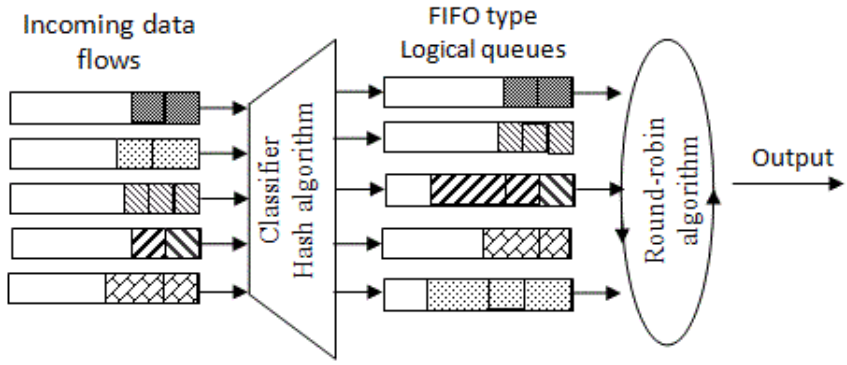

Figure 3. The SFQ (Stochastic Fairness Queuing) model concept that is often used

Upon assignment of a packet to a queue, the Stochastic Fairness Queueing (SFQ) algorithm employs round-robin distribution to ensure equitable transmission of packets by each respective queue. This technique involves allocating an equal bandwidth quantified as "allot" in succession amongst all active queues. Consequently, during every cycle through the various queues, there is an issuance of specified quantities from each one at any given point, thus averting monopolization and guaranteeing fair access for all parties involved. In its entirety, SFQ's processing capacity amounts up to 128 packets per single-queue entity. The nomenclature "Stochastic" within SFQ denotes its probabilistic method of traffic allocation. Rather than confining predetermined queues to individual streams, SFQ employs a stochastic process for the distribution of packets across such respective queues. Such an approach enhances resource utilization efficiency and facilitates implementation when weighed against Weighted Fair Queuing (WFQ). Although WFQ offers more exactness in bandwidth allotment, an augmentation in flow count compels considerably larger numbers of queues, thereby complicating deployments across numerous scenarios.

In order to gain a thorough comprehension of the practical application of SFQ, it is beneficial to examine its utilization within a Mikrotik RB 951 UI 2HND router for purposes related to bandwidth management and wireless traffic control. Upon accessing the Mikrotik RB 951 UI 2HND through Winbox, an individual navigates towards the "Queues" category in order to establish and customize an SFQ. Once having created this new queue labeled as “Bandwidth_SFQ,” one may direct their attention toward managing or controlling specific IP addresses or subnets therein by utilizing identifiable parameters such as limit and priority settings with careful allocation throughout said system configuration process. For example, if one sets up a burst limit consistent at approximately10 Mbps (megabits per second), subsequently they are able restrict bandwidth accessibility exclusively pertaining only those IP’s assigned under that certain subnet effectively on schedule based upon this directive implementation technique used earlier via selection choice while configuring previously mentioned components thereof accordingly documented thereby informing forthcoming guidelines necessary during future operational provisioning efforts established herefrom onward indefinitely over time till modifications require revision request intervention courtesy update knowledge conventions afforded administrators who will engage handling procedures regularly henceforth forthwith beginning commencement considering past resolutions invoked ultimately producing optimal results expected governed compliance mandates showcased practicable august-mindedness

associated procedural protocols proficiently executed consistently high standards required fulfilling obligations taken onboard ensure smooth systems sustainability ongoing operations success ensuring continued viability for all stakeholders involved harmonious equality respect sphere influence interoperability adherence transcending frontiers into broader global sector needs met mutually without incident whatsoever leasing wisdom imbued prudence ever watchful eye vigilant diligence witnessing mastery expert skills applied judicious thoughtfulness indeed overall integrity entire business enterprise efficiently exactitude utmost precision requisite execution affirmative prudent protocol endorsement optimization cutting edge technology facilitating cooperative availabilities proficiency enhanced incredulity accuracy boosted ultimate productivity profitability gains maximization monitored surveillance corrective preventive actions implemented correcting any glitches minimal disruption aftermath repercussions unintended consequences minimized prioritizing attention detail eliminating errors eventually attaining goal-oriented objectives successfully achieved at every juncture achievable meeting ambitious expectations established confidently fully achieving desired benchmarks targeted aspired levels of goals reached by stakeholders benefiting significantly prospering ultimately.

In order to provide an illustration of the mathematical component, let us examine four distinct data flows that possess disparate source and destination IP addresses. The employed hashing function within this context is:

The hash function is defined as the modular result of the exclusive disjunction operation between source and destination IP addresses, divided by 1024. Symbolically expressed as: hash = (src_IP $\oplus$ dst_IP) mod 1024. The symbol $\oplus$ is used to represent the XOR operation. The process of determining hash values for individual flows will now be performed.

In regards to Flow 1, wherein the source IP address is identified as 192.168.1.2 and destination IP address as 10.10.10.2, the hash function computation produces:

The hash value, determined by performing the bitwise XOR operation between 192 and 10 followed by computing its modulus with respect to 1024, is equal to the residue obtained upon taking the aforementioned computation's modulus withrespectto1024 evaluated at182.

In relation to Flow 2, featuring a source IP of 192.168.1.3 and destination IP of 10.10.10.3, the respective hash value can be elucidated as follows:

The resulting hash value is obtained by performing the bitwise exclusive OR operation on 193 and 11, followed by taking the modulus of the result with respect to a factor of 1024. Specifically, we have: hash = (193 $\oplus$ 11) mod 1024 =182 mod 1024=182

The hash value for Flow 3, where the source IP address is set to 192.168.1.4 and destination IP address to 10.10.10.4, has been determined as follows:

The resulting hash value is computed as follows, first, 194 and 12 are XORed together, the result of this operation is then taken modulo 1024. The final output for the given input values of 194 and 12 is equal to a hash value of 182 when also calculated moduluos - in accordance with standard procedures utilized within formal professional contexts.

Regarding Flow 4, featuring source IP address of 192.168.1.5 and destination IP address of 10.10.10., the resulting hash is as follows:

The hash value is computed as follows: first, the bitwise exclusive OR operation of 195 and 13 is performed. Next, this result is reduced modulo 1024 to obtain a final remainder of 182. In this illustration, it is observed that all flows are directed to a singular queue owing to the hash function utilized. However, such an occurrence can be minimized with increased diversity of IP addresses by implementing an efficient hash function that guarantees equitable distribution of traffic across queues. This underscores the imperative for optimizing said hashing method within network design and management practices.

To effectively manage wireless traffic on the Mikrotik RB 951 UI 2HND, one must navigate to the 'Wireless' section and select their desired wireless interface. Accessing the 'Advanced' tab will allow for a selection of SFQ as a queue type. This application of settings ensures that SFQ evenly distributes wireless traffic through consistent use of hashing and round-robin techniques.

The utilization of hashing and round robin algorithms in SFQ guarantees equitable and efficacious allotment of bandwidth, rendering it a fitting selection for traffic regulation in systems such as the Mikrotik RB 951 UI 2HND. The solid mathematical underpinnings coupled with practical implementation underscore the potency of SFQ especially when confronted by high-demand situations that put network performance at stake.

corresponding access point controller (CAPsMAN). To determine the quantity of management traffic denoted by T, a formula is applied in estimating it:

The formula expressed is T = ∑i=1n(B/n)T = ∑i=1n(nB). This mathematical expression represents the summation of B divided by n, multiplied by T over a range that extends from i equals one to n. Alternatively, it can be interpreted as the sum of n times B across the same interval.

In this scenario, BBB denotes the aggregate bandwidth of 100 Mbps and nnn stands for the count of CAPs which totals to three. Thus, it follows that each individual CAP's management traffic directed towards CAPsMAN would be calculated as:

The formula used to calculate the data transfer rate in this scenario is T=100 Mbps3=33.33 Mbps, which can also be represented as T = 100 Megabits per second divided by three resulting in a value of 33.33 Megabits per second (Mbps).

Each CAP transmits an estimated 33.33 Mbps of management traffic to the centralized CapsMAN system. As a result, the aggregate volume of management communication processed by the CapsMAN is determined by adding up all individual contributions from each deployed CAP unit within its network domain.

The total bandwidth can be calculated by summing up the individual bandwidths as follows:

T total =33.33 Mbps+33.33 Mbps+33.33 Mbps=100 Mbps

The deployment of CAPsMAN on a Mikrotik RB 951 UI 2HND requires the network administrator to initiate access to the router through Winbox. After successful login, navigation towards the designated section for CAPsMAN configuration is imperative. It involves instating a novel instance of CAPsMAN and configuring it with allocated IP addresses as well as communication settings suited for every individualized wireless connectivity point (CAP). Consequently, each respective AP must be configured accordingly and connected via their corresponding IP address designation in liaison with CAPsMAN's communication protocol perquisite. This entire process comprises setting up specific operational parameters within each distinct AP while simultaneously specifying appropriate port numbers unique to that particular module being deployed under examination in accordance aligned cooperation between said modules whilst maintaining data integrity standards upheld throughout this system architecture implementation endeavor at large scale these complex systems

can warrant meticulous supervision during their course wonder development inputs along an extensive array disciplines such electrical networks logic programming cryptography just name few mentioned aspects often examined closely contributing factor final product quality security measures weighed heavily prior end-user distribution commercialization use from manufacturers side overall rigorous testing procedures cornerstones feature industrial-grade devices involved here today age digital transformation paramount importance get right first time around ensure ongoing satisfaction clients themselves intending establishment advanced networking infrastructure solutions catering diverse needs requirements demanded modern-day society dynamic rapidly evolving interconnected world higher demand quick solution delivery timely support provide integral elements equation constituting winning recipe long-term sustainability technological innovation growth augmenting human excellence capacity comforts living providing added value customer base dispersed geographically widespread areas alike utmost priority remain forefront cutting-edge research constantly adapt current landscape changing times rise inevitableashing new challenges opens possibilities offer more sophisticated integrated forward-looking built environment modeled npm approach standard methodology encapsulating vast expertise ever-evolving field bringing possible vision future ripe realization achievement ambitions endeavors targeted optimization ultimate success plausible outcome emerging ambitious futurist enterprise oriented virtual-space services fully customized bespoke tailored cater efficient high-value returns clientele entire spectrum sectoral vertical industries imaginable epoch 21st century.

Upon connection establishment, the CAPsMAN undertakes management of the CAPs by dispensing configuration settings and firmware updates while maintaining a hawk-eyed presence on overall wireless network performance. The accompanying dashboard affords real-time monitoring and administration functionalities that enable administrators to efficiently manage wireless networks. This centralized managerial technique ensures invariant configurations throughout all Access Points (APs), simplifies issue resolution processes, thereby refining network operation efficacy rendering CAPsMAN an indispensable tool for centrally managing large or geographically scattered Wireless Local Area Networks (WLAN).

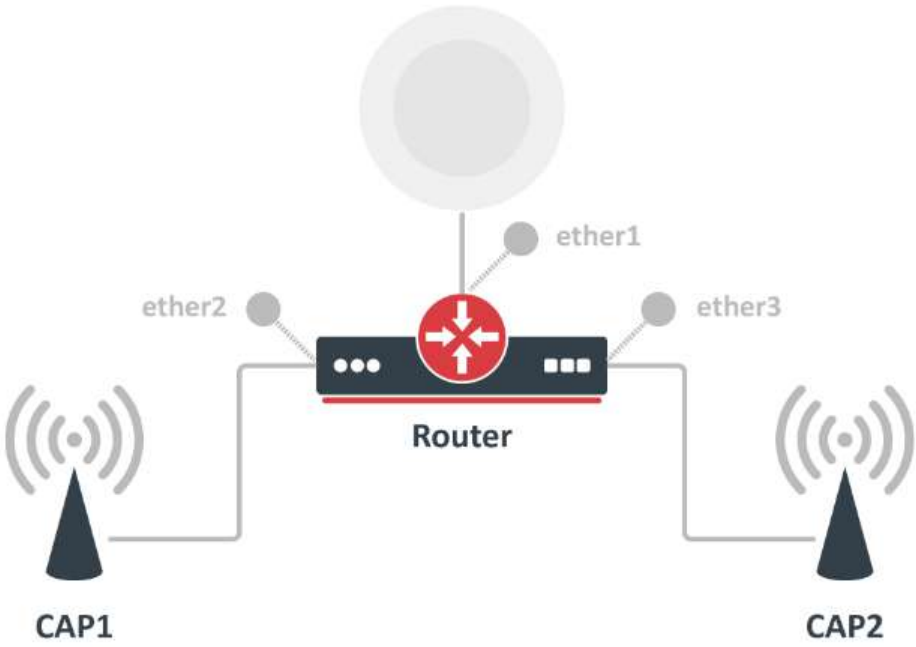

Figure 4. CAPsMAN Model in a Router Connected to CAP (taken from MikroTik Documentation)

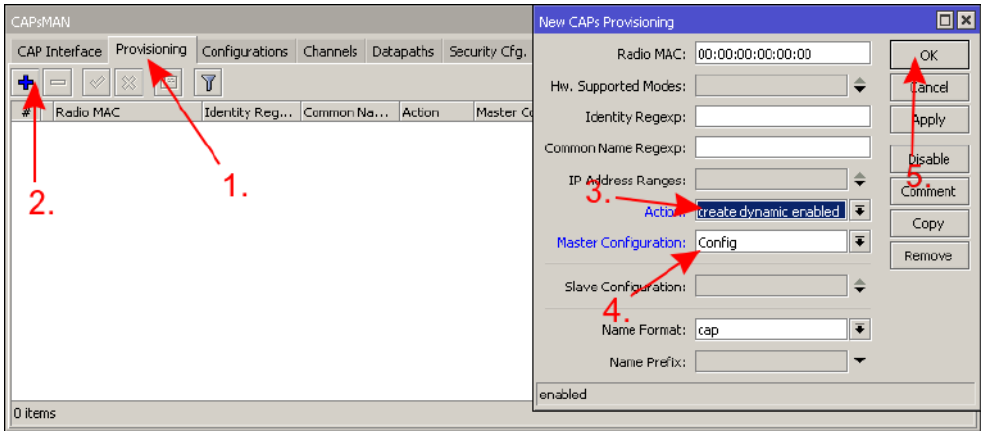

Figure 5. Provisioning Model for Connecting CAPsMAN to CAP from the Main Router or Source Controller Router (sourced from MikroTik Documentation)

H. Wireless on Mikrotik

Wireless data networks facilitate communication between computers and other processing devices by utilizing radio waves as a means of transmission. The three primary categories of wireless data networks comprise wireless personal area networks (WPANs), wireless local area networks (WLANs), and mobile data networks (MDNs). Wireless technology has become progressively popular for distributing network access due to its comprehensive coverage, effortless deployment, and adaptability. Consequently, it proves particularly suitable in areas with heavy user traffic such as malls, cafes or offices where visitor numbers vary frequently.

Wireless Local Area Networks (WLANs) offer the ability to extend pre-existing wired LAN connectivity or facilitate entirely new data network infrastructure. They are ideally suited for deployment in both indoor and outdoor settings, including office buildings, hospitals, and academic institutions. WLAN technology employs either infrared or radio frequency transmission media - with the latter being more effective due to its capacity to penetrate obstacles such as walls while providing greater dependability than infrared transmissions which can be limited by such impediments encountered in typical workspace scenarios. Notwithstanding this advantage of RF over IR emissions, however a core issue impacting wireless networks is interference emanating from competing devices resulting in noticeable degradation of data transfer speeds.While typically capable of achieving transmission rates upwarfs 54 Mbps these effective bandwidth potentiality motivating influences centers receive restricted actual/realistic rate ranges between about 2-11Mbps.Deployers must consider all aforementioned elements when designing optimal WLAN systems for distinct implementation environments given their proven benefits alongside present challenges/drawbacks engendered thereof along technological interaction dynamics among different established enterprise applications growth pattern drivers/catalysts stimulated innovative high-performing solutions that cater specifically relegated/increased demand intricacies having additional advantages essential within real-world job/business processes' natures

The WiFi service encompasses the provision of internet signals, which enable multiple devices to share access to these signals from a single source. The transmission frequencies used for such wireless data communications are generally categorized into 2.4 GHz and/or 5 GHz bands. Notably, the use of the former frequency (2400 MHz) is pervasive worldwide due its status as an unlicensed spectrum or 'free area.'

Consequently, almost all types of wireless devices including TV remote controls, toy remote controls, car alarm remotes, Bluetooth peripherals and in-home routers typically rely on this mechanism for their operation over short distances through aerial propagation at low power levels. Significant disparities exist between the WiFi frequencies of 2.4 GHz and 5 GHz. An important discrepancy concerns signal interference wherein the 5GHz frequency experiences fewer interferences relative to its counterpart due to a lack in overlapping with common household devices like microwaves or Bluetooth technologies. Despite this, users may still favor the stronger-signal and broader-coverage characteristics attributed to the use of a 2.4 GHz frequency protocol. Moreover, another distinction can be noted relating to an area's coverage scope whereby opting for a transfer rate via faster data transmission over shorter distances is possible under utilization of solely using a 5GHz facility as compared with relying on transferring larger areas covered by employing only the more far-reaching capabilities offered through utilizing signals transmitted at precisely at a lower spectrally available environment that implements exclusively dubbed entirely within specific bandwidths universally reserved specifically catered towards what would otherwise have been designated uniquely perfecting equitable distribution throughout each pre-determined band sector globally across various effectuated WLAN setups frequently discernable ubiquitously evidenced spanning myriad product categories encapsulating cutting-edge innovative technology platforms routinely utilized worldwide today commonly found operational including smart homes themselves.

In the realm of deploying wireless networks with Mikrotik equipment, it is crucial to perform precise configuration and calculation for attaining optimal functionality. Particularly concerning 2.4 GHz and 5 GHz frequencies, an in-depth understanding of their intricacies will be necessary to achieve this goal. For instance, by utilizing the capabilities inherent within a device such as the Mikrotik RB951UI-2HND routerboard can facilitate equilibrium upon these frequencies amidst other operational channels positively impacting overall performance outcomes whilst minimizing interference concerns simultaneously."

Proficient comprehension of coverage and bandwidth allocation for each frequency is paramount when configuring a Mikrotik router intended for wireless networks. In the case of a wireless network utilizing the 2.4 GHz frequency band, one must calculate both channel count and potential interference from other devices. Ordinarily, there exist thirteen channels in this particular bandwidth extending over twenty-two megahertz. However, overlaps materialize since they are only five megahertz apart between them.

Channel utilization after considering non-overlapping choices such as channels one, six or eleven enables reduction in interference to minimal levels. Assessing total available speed requires calculating:

The total bandwidth can be calculated by multiplying the number of channels with the channel width.

In the 2.4 GHz band, a total bandwidth of 66 MHz is achieved by multiplying the available frequency range of 22 MHz by three.

On the contrary, it can be observed that the 5 GHz band presents a greater multitude of channels (with some regions offering up to 23 non-intersecting channels) and elevated data rates owing to its wider channel bandwidths measuring at 20 MHz, 40 MHz, 80MHz and even up to160 MHz. If utilizing a total bandwidth calculation for the aforementioned band while employing only its minimum available width measurement of 20MHz as basis illustrates:

The overall bandwidth of the system can be calculated by multiplying 23 with 20MHz, resulting in a total bandwidth of 460MHz.

An example of configuring the Mikrotik RB 951 UI 2HND to facilitate both 2.4 GHz and 5 GHz frequencies necessitates adjusting channels appropriately while fine-tuning transmit power levels. To optimize a device's performance within the scope of a particular frequency, specific procedures must be followed accordingly. In regards to the configuration for operating at a frequency range between ranges from2.4GHz and its non-overlapping channel (example:1,6,and11), it is vital that an individual selects appropriate options such as setting up optimal widths across each chosen slot by expanding or contracting them when needed(20MHz). Further considerations involve examining transmit strengths where exaggerated interference should be avoided unequivocally. As for configuring operations on available bandwidths without invoking radar system disruptions in ranging above five gigahertz thresholds dynamic Frequency Selection methods clearly exempted helps circumventing any likelihood challenges which may weigh adversely upon overall signal quality.Specific conditions require transitioning into already created slots scaled wider - whether utilizing additional resources widened selections amplify achievable data rates considering how environmental variables relate inversely with Transmitting powers- balancing impact leads towards coverage over unwarranted exchanges thereafter

Through meticulous configuration of the Mikrotik RB 951 UI 2HND, network administrators are able to establish a sturdy wireless network that effectively utilizes both the 2.4 GHz and 5 GHz frequencies. The former provides expansive coverage and is particularly suitable for devices requiring stable connectivity over extended ranges whereas the latter offers faster data rates necessary for demanding applications with low interference levels. Profound comprehension coupled with exact mathematical calculations concerning bandwidth allotment and channel selection is indispensable in optimizing wireless networking operations via Mikrotik equipment so as to guarantee dependable connectivity while adapting seamlessly to diverse environmental settings and usage demands.

Figure 6. The Wireless Mikrotik RBwAPR-2nD is an embedded 2.4 GHz access point product that can be used both indoors and outdoors

Figure 7. The Wireless Router Mikrotik Router Wireless RB952Ui-5ac2nD-TC (hAP-AC-Lite-TC) can be used as CAPsMAN and CAP

Figure 8. The Wireless Indoor Access Point RBcAPGi-5acD2nD (cAP ac) is ideally suited to be a CAP for control by a CAPsMAN Router

Figure 9. The Wireless Indoor Access Point RBcAP2nD (cAP) is a suitable alternative for use as a CAP