REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

Information Technologies

NETWORK SECURITY WITH IPSEC HARDWARE ACCELERATION WITH AES AS A REPLACEMENT OF PPPOE USING MIKROTIK ROUTER OS

Abdullah Mahmood Abdulrazzaq AL-RAWE

Master's Thesis

Supervisor

Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Istanbul, 2022

NETWORK SECURITY WITH IPSEC HARDWARE ACCELERATION WITH AES AS A REPLACEMENT OF PPPOE USING MIKROTIK ROUTER OS

Abdullah Mahmood Abdulrazzaq AL-RAWE

Information Technologies

Master's Thesis

ALTINBAŞ University

2022

The thesis titled NETWORK SECURITY WITH IPSEC HARDWARE ACCELERATION WITHAES AS A REPLACEMENT OF PPPOE USING MIKROTIK ROUTER OS prepared by ABDULLAH MAHMOOD ABDULRAZZAQ AL-RAWE and submitted on 16/12/2022 has been **accepted** for the degree of Master of Science in Information Technologies.

Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

the Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN	Department of Software Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering, Arel University	_____

I hereby declare that this thesis meets all format and submission requirements of a Master's thesis.

Submission data of the thesis to Institute of Graduate Studies: ____/____/____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Abdullah Mahmood Abdulrazzaq AL-RAWE

Signature

DEDICATION

I would like to thank Allah Almighty for the power of the mind, health, strength, guidance, knowledge, and skills to complete this study. This thesis is wholeheartedly dedicated to my mother, my wife, my family and my friend Taha Al Rawe. There are no words to describe what you mean to me; there is nothing that I can repay for what you have done to me. I will continue to do my best to achieve your expectations.

I write my dissertation as a tribute to my numerous friends and family. I am especially appreciative of my devoted parents. I also dedicate this dissertation to all of my close friends for their help and encouragement during the writing process.

ACKNOWLEDGEMENTS

I would like to thank Asst. Prof. Dr. Ayca Kurnaz, without her I would not have been able to complete this research, and without whom I would not have made it through my master's degree. My colleagues have supported me and have had to endure my stresses for the past two years of study.

And my biggest thanks to my mother, my wife, my family and dear friend Taha Al Rawe for all the support you have shown me through this research, the culmination of two years of distance learning. Thanks for all your support, without you all I would have stopped these studies a long time ago, you have been amazing.

ABSTRACT

NETWORK SECURITY WITH IPSEC HARDWARE ACCELERATION WITH AES AS A REPLACEMENT OF PPPOE USING MIKROTIK ROUTER OS

AL-rawe, Abdullah Mahmood Abdulrazzaq

M.Sc., Information Technologies, Altınbaş University

Supervisor: Asst. Prof. Dr. Ayça Kurnaz TÜRKBEN

Date:12/2022

Pages: 64

Networking world is growing rapidly as new techniques appear due to the advanced technology implemented. For the Internet access service, obsolete methods and techniques are still used by the end-users or entities to get access the Internet service; are still used even in nowadays. One of the most commonly used service is the Point-to-Point over Ethernet (PPPoE). However, the Password Authentication Protocol (PAP) contains a security flaw that authentication sensitive data can easily be exploited or intercepted by using any rogue software tool capable of data sniffing and eavesdropping in the network. These sensitive data can be viewed and re-used to allow an unauthorized access to get behind the one. Accordingly, (PAP) is still be used in many ISPs as their main authentication protocol with PPPoE service. However, with the growing of the IPsec hardware acceleration technique implemented in newer chips; there is a need to replace obsolete services. It offers better stability, end-to-end data encryption and protection for the entire network. This paper is an attempt to utilize the hardware acceleration technique to accelerate and prioritize the IPsec encryption and decryption processes inside the main router that offers the Internet access service. Hardware acceleration technique has an enormous role in dealing with encryption and decryption processes, offers fast-processing operations without consuming more chips' power and energy. Thus, keeping the connection-sessions' active without being delayed nor interrupted. There is an extremely need to be used as a replacement for the obsolete PPPoE dial-up service.

Keywords: PPPoE, PAP, L2TP, IPsec, Hardware Acceleration, MikroTik, Router OS.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

1. INTRODUCTION

Since a long time, the Point-to-Point over Ethernet (PPPoE) broadband connection is still as one of the leading dial-up connections to offer the Internet service for home and business. One of its major advantages is that a PPPoE connection can easily be set without higher costs and resources. The (PPPoE) works as the PPP frames are encapsulated inside the Ethernet frames. The PPPoE discovery stage and the PPP session stage are the two independent phases of Point-to-Point Protocol over Ethernet. A peer uses the first stage of the PPP connection to learn more about the authentication server before the server authenticates the peer or even during mutual authentication. The peer freely browses the Internet when the PPP session has been verified, and the server will handle the bill-counting. In other words, when the time a peer gets authenticated by the server itself, Internet access is ready to go.

However, in today's modern world, networks become larger and larger due to new technology available. Despite, when the networked-world becomes larger, security remains as one of the most sensitive domains. No one and even ISPs cannot offer new services without neglecting security. The PPPoE dial-up connection security seems to be obsolete; it uses an old technique for authentication that the security mechanism which is used to securely authenticate the credentials have not been enhanced nor updated. Accordingly, it is simple to gather data on both the peers and PPPoE authentication servers silently by impersonating the server, which is invisible on the network nor can be detected. We can use this information to extract the authentication password. An unauthorized entity using a password sniffer software tool can get the real credentials and acts like-real identity [1]. For every ISP, of course, it is not ideal because the real identity has been tampered. Hence, network security, newer security policies are a must to be implemented in order the network performs as usual. However, the Layer 2 Tunneling Protocol (L2TP) dial-up connection offers newer, better, and enhanced security created by the network administrator or the ISP, as in addition, there is data encryption utilized by the Advanced Encryption Standard (AES) protocol. Accordingly, An L2TP connection uses the IP security policy (IPsec) protocol before a connection established. So, security policy is a must to be upgraded. As a more advanced kind of Internet security technology, a VPN can lower information management costs and offers good scalability. Consequently, VPN quickly gained popularity in businesses, research, and other industries.

However, an older issue within L2TP/IPsec VPN connections is that they consume more of devices' energy and power; resulting in a degraded performance of the entire network stability.

Moreover, clients might face connectivity issues or data processing timeouts. This because the encryption and decryption process implied. The new hardware acceleration technique overcomes such issue. It simply does speed, fast-processing operations and prioritizes IPsec among all other operation as long as the connection is still active [21].

1.1 GENERAL INFORMATION

Edward, M. and Forrest J., concluded that they can "can significantly accelerate the overall performance of a software-only system by moving time critical sections of code to hardware. In common with our previous hardware architecture, parameter passing overheads serve to diminish the achievable software acceleration factor" [14]. Ernst, M., Henhapl, B., Klupsch, S., & Huss, S. on their "FPGA based hardware acceleration for elliptic curve public key cryptosystems" concluded that "public key cryptosystems are highly sophisticated software products mainly due to the complexity of the underlying arithmetic." Only hardware acceleration, or moving the corresponding procedures from software to hardware, will greatly improve performance in terms of signature verification rate. However, the resulting hybrid systems must allow for efficiency and security level trade-offs. Therefore, we suggest incorporating programmable coprocessors into such cryptosystems" [16]. "Exploiting the heterogeneous resources on modern FPGAs enables the acceleration of complex algorithms such as the Trace transform. By analyzing the algorithm in detail and making some computational simplifications it is possible to tailor the implementation to hardware. At the same time, the on-chip BlockRAMs are exploited to provide a degree of flexibility, allowing an arbitrary set of trace transform functionals to be computed using generalized functional blocks" [17].

1.2 CONTRIBUTIONS OF THE THESIS

In this study we tested the IPsec hardware acceleration feature implemented in newly invented network devices and utilized in our local area where PPPoE is the main service for Internet access.

i. High resources usage when using L2TP/IPsec VPN connections inside main network device or modems used to access the Internet service eliminated by the IPsec hardware acceleration.
ii. Upgraded the connection type from PPPoE service to the newer one that offers better security and data encryption in addition to use a modern authentication algorithm.

iii. Utilizing of the hardware acceleration feature opened the doors for ISPs in local areas where this study is conducted to validate and replace the PPPoE by L2TP/IPsec connections.

1.3 RESEARCH QUESTIONS

Any academic research paper starts with a number of questions to be investigated, developed or at least an attempt to be solved by the researcher himself. The research questions represent the core component of the study whereas the entire study attempts to find the solutions at the end of the study. Several questions are presented during this study:

i. Is PPPoE dial-up connection service secure enough, in today?
ii. Why L2TP/IPsec VPN is mainly limited to business and industries?
iii. Does the hardware acceleration feature have an impact on the IPsec L2TP policies?

1.4 LIMITATIONS OF THE STUDY

The study limitations are:

The ISP (Gnet for Internet services) max throughput is limited to (60 Mbps) of download speed. The (60 Mbps) is changeable based on the ISP priority and time. The routers utilized are manufactured by MikroTik. The PPPoE configuration made as usual in any ISP. There is no in-depth consideration of PPPoE but only in testing its security with the PAP authentication enabled. The sample of clients not exceeded the number of (60) in the state in hardware acceleration tests. In PPPoE, the number of connected clients not exceeded (30). As regularly MikroTik releases software updates to its devices at regular periods, more than one time the devices' software versions were upgraded. Accordingly, only the "stable" update channel is considered for the tests.

This study might show different results when utilizing the same testing by using different ISP, max throughput speed, using other manufacturers' devices to conduct the same tests. Law and local country regulations must always be followed as allowed. A consideration that should be taken in this paper is that There are resources that are not citied in this paper because the researcher not quoted from them. But instead, these resources were read by the researcher and expended his ideas and thoughts. So, they were referenced at the end of this paper. Furthermore, there were less citations in chapter two because it is all related to the testing procedures. In other words, it is the practical part of this paper.

1.5 THESIS STRUCTURE

The thesis' structure is: Chapter one overviews the general overview of our study presented as; introduction, contributions, research questions, thesis structure, PPPoE and PAP, L2TP/IPsec, and hardware acceleration.

Chapter two utilizes our attempts' procedures to examine the PPPoE security, replacing PPPoE by L2TP/IPsec, utilizing hardware acceleration, and finally the conclusions and future recommendations.

1.6 PPPOE AND PAP

A host must first determine the Ethernet MAC address of the distant peer in order to start a PPPoE session, and then they must create a special PPPoE session ID. PPPoE discovery is the process of discovering the remote Ethernet MAC address. The discovery stage enables the client to communicate with each access concentrator on the network [5].

The Ethernet address of the peer and the session ID are used to uniquely identify each PPPoE session. As with any other PPP encapsulation, data is sent when the PPPoE session has been formed. An Ethernet frame containing the PPPoE information is then delivered to a unicast address. The behavior of magic numbers, echo requests, and every other type of PPP traffic is the same as in typical PPP sessions. At this point, the PPPoE logical interface requires resource allocation from both the client and the server. Any configurations change in the authentication protocols results in session-termination in which the remote device sends a PPPoE Active Discovery Termination (PADT) packet to terminate the session. This is generally the basic idea of PPPoE work inside any network – (if the service enabled by ISP) [40].

Point-to-Point Mechanism (PPP) uses the password-based authentication protocol known as Password Authentication Protocol (PAP) to verify users. PAP is exposed to any attacker who can view the PPP session since it transfers data in unencrypted "in clear text." The user's identity, password, and other data connected related to session is all visible to an attacker. This could easily be done by simply using a simple configuration: rogue PPPoE server and PAP enabled authentication [2]. All data will be transported in un insecure path which will expose information in a clear text format. They are visible to everyone. PAP today is enabled by default in PPP authentication and for this reason; it is considered insecure authentication method. Regardless, it is widely used in today's communications and authentications because in most systems it is still a choice. Any ISP who ignored the configuration and security, later would

face security issues due to sensitive data exposure. Later the data might be sold for third-parties or be used illegally.

1.7 L2TP/IPSEC

The Layer-2 Tunneling Protocol is also another type of connection that entirely depend on the PPP. A connection is established by creating a tunnel path which regarded as Virtual Private Network (VPN). By establishing virtual tunnels between a pair of hosts, VPN aims to ensure safe and secure communication. Data transfer is possible after the tunnel has been established. Two VPN options that are popular in WLANs are IPsec VPN and SSL VPN. Remote users can access Web applications, client/server programs, and internal network connections via SSL VPN. The integrity and confidentiality of the data are protected by encryption utilizing IPsec, which also uses Internet Key Exchange (IKE), Authentication Header (AH), and Encapsulating Security Payload (ESP). IPsec is used in the tunnel mode by VPN technology to offer authentication, integrity, and anonymity [48].

When the L2TP and IPSec VPN connections are established, each local network will communicate as if it were in the same network through a tunnel. Tunneling is a technology used to form a private network connection by safely applying two or more networks because there is an encapsulation process [39].

Since it is under the PPP, L2TP inside a network can be configured using the similar configurations as of PPPoE. Regardless of configuration, L2TP connections use a mechanism differs from PPPoE authentication. Its security enforced by cryptographic keys and algorithms to supply better security. Sessions cannot be established without neglecting the Internet Protocol Security (IPsec). The connection is mainly between “two parties” which it is a site-to-site connection. IPsec is a set of secure protocols used in computing that authenticates and encrypts data packets for communication between two computers over an IP network. These protocols include those for negotiating the cryptographic keys to be used throughout a session and for establishing mutual authentication between agents during initial “parties” contact. IPsec can secure data transfers from one host to another, from one security gateway to another, or from one security gateway to a host (network-to-host) [26]. To secure communications across Internet Protocol (IP) networks, IPsec uses cryptographic security services. It supports replay protection, data origin authentication, network-level peer authentication, data integrity, and data confidentiality (encryption) (protection from replay attacks).

IPsec can be used to defend against internal network threats such as IP spoofing, password-based attacks, man-in-the-middle attacks, eavesdropping, and manipulation. Because encryption, integrity, and authentication services are handled at the transport level [13], IPsec is totally transparent to applications. Some of the measure service can provide are: extended connections across multiple geographic locations without using a leased line, flexibility for remote offices and employees to use the business intranet over an existing, Internet connection as if they're directly connected to the network, saves time and expense for employees who commute from virtual workplaces, VPN is preferred over leased line since leases are expensive, and as the distance between offices increase, the cost of leased line increase.

Utilizing TCP and UDP ports, applications continue to connect with one another as usual. Before sending packets across a network, an IPsec sender can encrypt them. Data Reliability To confirm that the data was not changed during transmission, the IPsec receiver can authenticate packets transmitted by the IPsec sender. Data Origin Authentication: The recipient of an IPsec packet can verify the origin of the data being delivered. The data integrity service is necessary for this service to function. Anti-Replay: The IPsec receiver has the ability to recognize and dismiss replayed packets [24]. These security services are provided by IPsec at the IP layer; IKE is used to manage protocol and algorithm negotiation based on regional policy. Generally, cryptographic security is more secure than any basic or regular authentication. In other words, basic and regular authentication mechanisms usually do not involve encryption of data. IPsec uses the Advanced Encryption Standard (AES) security protocol in order to provide the encryption.

The National Institute of Standards and Technology of the US Government officially adopted the encryption method known as the Advanced Encryption Standard (AES), which is widely used today. It was well acknowledged that DES was “insecure” due to high computer processing capacity and resources [42]. AES is a block cipher that encrypts data using multiple rounds of encryption and an encryption key; meaning that data being transferred are involved in multiple “data changes” to avoid altering. Data change is not the real data changes in form, but in its place, then it back to the first state at the final destination. Sensitive data must be protected in order to promote customer loyalty, lower legal risk, and comply with data security regulations. Databases like Oracle Database, IBM DB2, Microsoft SQL Server, MySQL, and Microsoft Access are examples of those that may hold sensitive data. The real data should be encrypted to prevent loss, regardless of the disk or folder encryption mechanism that may be utilized.

Despite of the mentioned IPsec and AES advantages, L2TP/IPsec connections are mainly limited or at least used only in business and large companies. This is to be examined and tested in the next chapter.

1.8 HARDWARE ACCELERATION

Hardware acceleration combines the flexibility of general-purpose processors, like CPUs, with the efficiency of fully customized hardware, like GPUs and ASICs, increasing efficiency by orders of magnitude. For instance, visualization operations could be delegated to a graphics card to speed up and improve the overall performance while freeing up the CPU for other work. Systems for dedicated hardware acceleration come in a huge range. Tethering hardware acceleration is one common type that, when used as a Wi-Fi hotspot, offloads tethering activities onto a Wi-Fi chip, lowering system effort and improving energy efficiency. In order to produce interactive visualizations of high-cardinality data, hardware graphics acceleration, also known as GPU rendering, operates server-side leveraging buffer caching and contemporary graphics APIs. AI hardware acceleration is made for applications like machine learning, machine vision, and artificial neural networks, which are frequently used in the realms of robotics and the Internet of Things (IoT).

“Hardware acceleration can revolutionize robotics, enabling new applications by speeding up robot response times while remaining power-efficient. However, the diversity of acceleration options makes it difficult for roboticists to easily deploy accelerated systems without expertise in each specific hardware platform.” Neuman, S. (2022).

The ability to enable or disable hardware acceleration is frequently offered by systems and software. For instance, in software, the user has the right to turn on or off the hardware acceleration service by adjusting the software settings. For example, in video production and conversion software. The most hardware used for the acceleration feature or technique are: Graphics Processor Units (GPUs), Field Programmable Gate Arrays (FPGAs), and Application-Specific Integrated Circuits (ASICs). In networking, the hardware acceleration differs than in software. For example, sometimes it cannot be customized in network devices as it is locked by the manufacturer defaults or its control dynamically turned on or off according to the device’ needs and criteria. Accordingly, in order to increase device performance and cut down on battery consumption, tethering hardware acceleration refers to the transfer of tethering traffic onto hardware using a direct link between the modem and peripherals. Implementing

tethering calls for hardware that can send network packets from Wi-Fi/USB to the modem without going via the main processor.

high production volume, the high manufacturing cost of the IC is easily amortized. Among existing hardware platforms, custom ICs are easily the fastest accelerators. By being application specific, they can deliver very high performance for the target application. There exists a vast literature of advanced circuit design techniques which help in reducing the power consumption of such ICs while maintaining high performance [16].

Hardware acceleration typically offers benefits such as quicker development, reduced non-recurring engineering expenses, increased portability, and simplicity of updating features or fixing bugs, but at the expense of additional overhead to compute general operations. Focusing on hardware can have benefits like speedup, lower power consumption, lower latency, increased parallelism [36] [37], bandwidth, and better use of the functional components and available area on an integrated circuit, but at the expense of less ability to update designs once they have been etched onto silicon and more expensive functional verifications. Hardware acceleration is a very large domain. It depends on how the it is implied, where to be used, its destination benefits and so on. It uses very complicated operations and formulas when being used and acting. This paper is to test its advantages inside the MikroTik Router OS devices that supports this feature but not in-depth deal with it.

the number of parameters in the network can be greatly reduced by substituting the tensor with a low-rank matrix or tensor approximations. Tensor decomposition decomposes a high-rank tensor into a series of low-rank tensors, reducing both memory use and operations. It can be used in both convolutional and fully connected layers and performs well in compressing parameterized networks. [39].

This means that the total number of operations can be easily decreased by applying a specific operation using a calculation-parameters to allow priority higher than a normal operation. In other words, a mechanism that has the ability to quickly understands and prioritizes the more important operation. Accordingly, this process facilitates and accelerates any IPSec-related operation.

Hardware acceleration is like-sensor set of algorithms defined and set according to its aim. It differs from purpose to another according to its implementation. For example, hardware acceleration in a PC processor can boost the processor’s speed to do multiple operations at

once, in GPUs; its boosts the memory and video-related graphics properties, making the overall real-time operation on going without system or out of memory faults. In MikroTik routers, the hardware acceleration is implemented to allow fast-processing operations related to VPN, IPsec, and overall system stability. In difference, and unfortunately, not all network devices use this feature despite it is very effective especially in large-networks. The newer ones do. They have this feature enabled and implied by default.

Key cipher functions used in SSL-driven connections, which include AES-256 symmetric encryption, SHA-2 hashing, RSA-2048 public key cryptography, are accelerated in hardware. The embedded cryptosystem is prototyped completely on an Altera Stratix II FPGA development board. Experimental results show significant improvements in performance of the SSL transactions when the proposed embedded cryptosystem is deployed in the networking system [51].

According to the quote above, the security and encryption can be accelerated if a capable hardware can utilize it, meaning that devices can be faster, more effective and operate more than regular operation in real-time. The result will be to the side for home, small business and even projects.

Table 1.1. Comparison between new vs. old devices specifications

Routers' resources (Green: New) Vs. (Yellow: Old)		
Model / Product code	RBD53iG-5HacD2HnD	RB2011UiAS-2HnD-IN
Chip (CPU) architecture	ARM 32-bit	MIPSBE
Chip name / code	IPQ-4019	AR9433
Chip (CPU) cores	4	1
Chip base frequency	716 MHz	600 MHz
Dynmaic frequency scaling	✓	✗
IPsec hardware acceleration	✓	✗
Total memory (RAM)	256 Megabytes	128 Megabytes

Table 1.2. Ipsec hardware acceleration tests and evaluation

IPsec hardware acceleration feature evaluation		
Router model	RBD53iG-5HacD2HnD	RB2011UiAS-2HnD-IN
30 L2TP/IPsec sessions		
CPU load (heavy)	14%	80%
CPU load (normal)	9%	55%
CPU load (idle)	3%	44%
Dynamic frequency scaling	✓	✗
IPsec hardware acceleration	✓	✗
Sessions forced to disconnect	✗	✗
Tx/Rx drops	✗	✗
Tx/Rx errors	✗	✗
60 L2TP/IPsec sessions		
CPU load (heavy)	32%	85 – 95%
CPU load (normal)	12%	65%
CPU load (idle)	9%	52%
Dynamic frequency scaling	✓	✗
IPsec hardware acceleration	✓	✗
Sessions forced to disconnect	✗	✓
Tx/Rx drops ocurred	✗	✓
Tx/Rx errors occurred	✗	✓

2. MIKROTIK AND ROUTER OS OVERVIEW

MikroTik headquartered in Riga, Latvia. Established in 1996 to offer hardware and software solutions for ISPs and consumers to help extending connectivity for everyone around the globe. This is simply its main goal. MikroTik devices are widely used nowadays by individuals, ISPs, small-business to build data infrastructure networking. For the Internet to be available to a wide range of consumers, MikroTik helps to make the existing Internet technologies faster and more powerful as well as to be cost-efficient with less resources. Most MikroTik devices use power consumption equals to a simple LED light or LCD TV and it is one of the main factors widely used.

For example, MikroTik cloud core router 'CCR1016-12S-1S+' priced (815.00 $) – at the time of writing, is a heavy-duty business grade router with 16 cores CPU, clocked with 1.2 GHz speed uses 47.5 watts of max power consumption. Accordingly, the 'CCR1072-1G-8S+' priced (3350.00 $) – at the time of writing, is a flagship router, offers (120) million packet per second and (80 Gbps) of throughput; built with 72 cores CPU and each core clocked with 1 GHz speed. 125 watts is the max power consumption. Imagine a device with 72 cores of 1GHz just 125 watts of power! All MikroTik hardware devices can be accessed and purchased through the official products website https://www.mikrotik.com/products.

However, this chapter will concentrate on testing procedures by utilizing a MikroTik Router OS hardware device. The testing hardware device is the MikroTik 'hAP ac^3.' There are some main circumstances why this device has been selected among other manufacturers' routers. Firstly, its architecture is ARM 32-bit which is a modern architecture in routers. Secondly, the CPU (Central Processing Unit) chip of this device is powered by Qualcomm 'IPQ-4019' with 4 cores running at 716 MHz of speed for each with new features and capabilities. Thirdly, it supports IPsec hardware acceleration which is the targeted aim of this paper. In addition, the 'hAP ac3' uses two Wi-Fi chips; one for the 2.4 GHz band and the other is for the 5 GHz band rather than in one single chip. In other words, you can turn on the 2.4 GHz and 5 GHz in the same device rather than just choosing one single band. Accordingly, 256 MB (Megabytes) of RAM is more than enough for this router. Most manufacturers' devices offer just 8 MB of RAM. Other factors include 30 watts max power consumption, 5 ethernet ports that support throughput up to 1 Gbps, it also uses IP20 (Ingress Protection) which makes it resistant to debris, dust and other objects that are over 12mm. Additionally, MikroTik devices have long support of software updates. Usually more than four years while others only for one or two.

All mentioned features usually not offer by other routers' manufacturers except the dual band options (2.4 GHz and 5 GHz). The 'hap ac^3' priced (109.00$) – at the time of writing.

2.1 PREPARING MIKROTIK ROUTER OS DEVICE 'HAP AC^3'

Before powering the device on, it is a must to attach the two antennas that came up in the device box because MikroTik made a yellow sticker warning hint. When the two antennas are completely attached, we need to attach the power adapter in the AC plug then the other side in router. Turning the power on will start the device and the LEDs on the front side of the device will flash meaning the device has successfully powered on. However, to access the device, an ethernet cable is needed. One side in the device and the other side in the computer through any ethernet port. For the first-time configuration, the 'Winbox' tool must be downloaded through MikroTik official downloads website. When downloading, it is recommended to select the latest version of the tool and choosing either 32-bit or 64-bit depending on the Microsoft Windows operating system's architecture. Version 3.37 is the latest version available (at the time of writing). Opening 'Winbox' will shows up a window like in the figure bellow. It shows information like the MAC address of the ethernet port we link the device with, default preconfigured IP address of MikroTik devices which is (192.168.88.1), identity, router version, board name, login (username), password as well as the uptime.

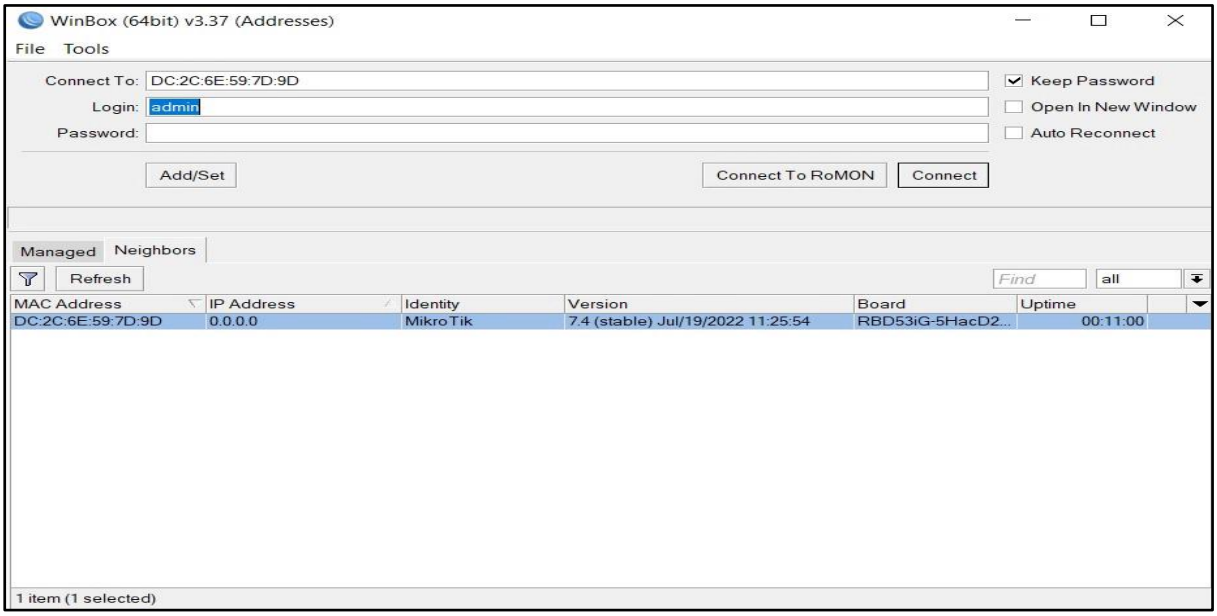

Figure 2.1: MikroTik Winbox Tool

To connect and access the device for the first time, we just need to select and click on the device' MAC address. It will becomes with a blue line and the device' MAC address will automatically be inserted in the Winbox connect field. The default login (username) and password for the device are the login is "admin" without quote and no password (blank) which are provided in the device' manual (as in the figure above). Accordingly, these are usually the same for every MikroTik device unless they are changed by an administartor or owner. Simply pressing connect will let an owner or an administartor access the device.

By accessing the router, the device' administartor can observe the friendly-user menu and layout. On the left, there are the main menus of managing and configuring the router. But before configuring, it is highly recommended to check the device software version and update it to the latest one. MikroTik regularly makes new software versions available which improve, enhance, add new features and bug fix device-related issues. Keeping the device' software up to date ensures the router works correctly without bugs. Figure (2) shows the MikroTik device main menus.

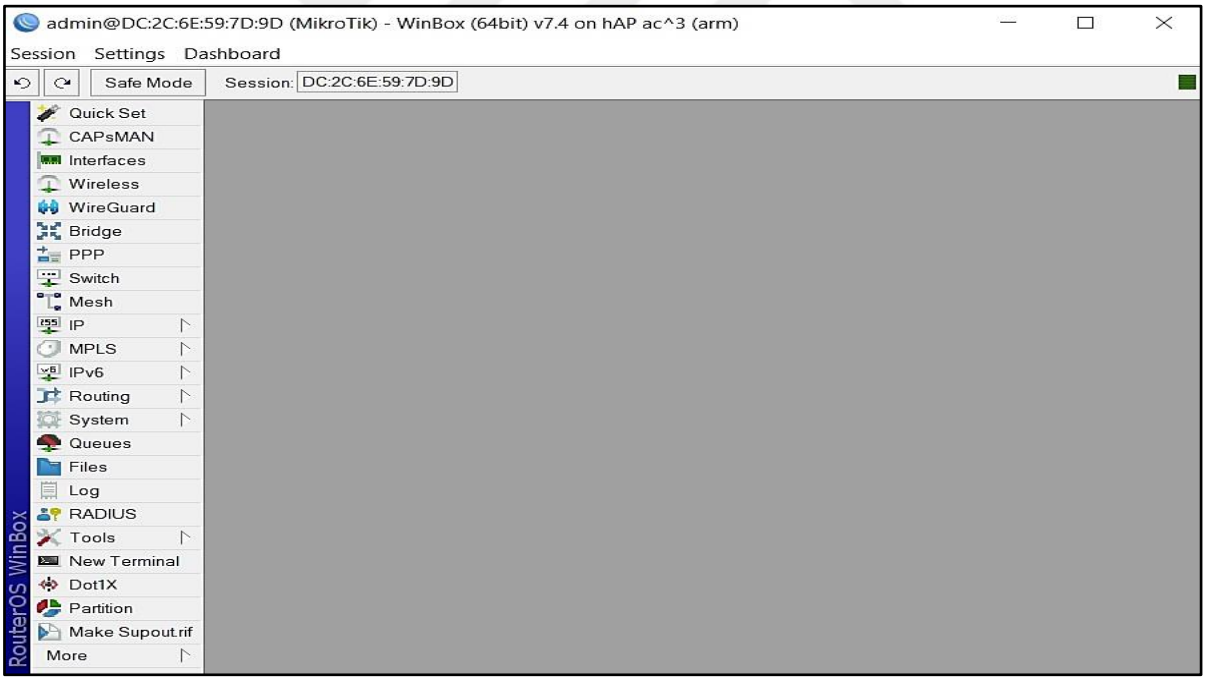

Figure 2.2: MikroTik device' main menu by using Winbox tool

There are different ways an administrator can use in order to update or upgrade the device' software version. The most commnly used method by clicking the Quick Set menu from WinBox then Check for Updates. In this step, an Internet connection is required. There are four different channels of software update. The most widely used is either the "stable" and "long-term" channels. The stable channel is the MikroTik recommended software version to be used with new, improved and compatible version. Usually realsed monthly. The long-term channel ensures long period of device stability and bugs-free. The other two versions are the "testing" and "development" channels. Testing channel is the software version which like beta software, comes with new features but it might contain some or compatibility isuues when installed on devices. It is not recommended for owners and ISPs because of this. So, it is important to make a backup for the configurations before installing or updating to these two channels. For this paper, the testing procedures will be based on the stable software version. Currently the latest stable version is (v7.4) which is already installed in the MikroTik device (at the time of writing). Another way to update the router is by surfing to MikroTik's official download website, then download the latest versions and uploading to the device. When downloading latest software versions, it is a must to download the version for the correct device' architecture type. MikroTik devices are of many architectures like ARM, ARM64, MIPSBE, MMIPS, SMIPS, TILE, PPC and x86 in which a software can be installed on any PC device to be turned into a MikroTik device with its main features. However, the testing device in our state is built upon ARM 32-bit achitecture. For new owners and administartors to know which their devices' architectures are, simply going to "system" menu then "resources". Figure (3) shows the way to identify the device' architecture.

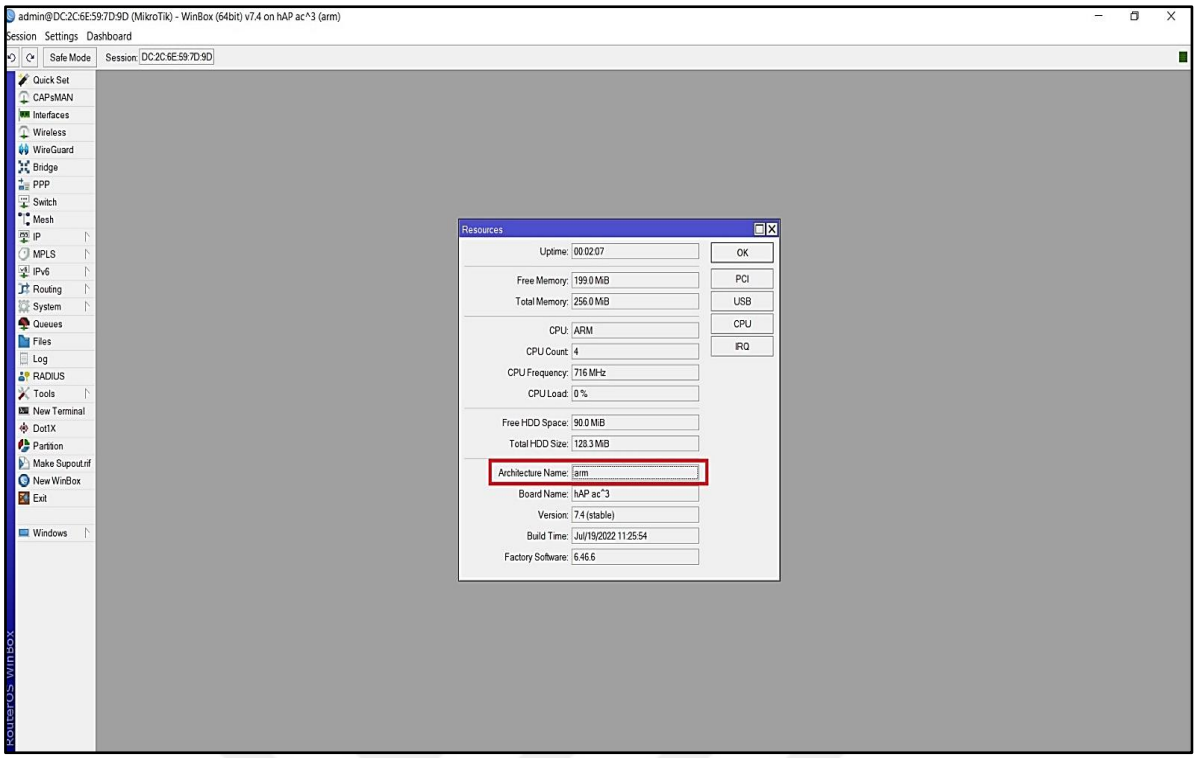

Figure 2.3: Winbox system and resources menu to identify the device' architecture

The architecture name filed shows what architecture the device is built on. Moreover, the resources window as shown above contains some useful information. Uptime shows how much time of the device since the last reboot or power on. Free and total memory clarify information about device' RAM. The more RAM available, the more stability the device offer. Board name is the name of the device, version for the installed software version. The factory version shows the software version which firstly installed on the device by the manufacturer before the device to be available in stores and ready for purchasing. When buying MikroTik device with new purchasing date, the owner of the device will notice a newer version is installed on the device.

After an important software update applied. It is highly to move to the main steps for configuring the router to be used by clients. The first step is to prepare something called "Bridge." In MikroTik devices, a bridge is a linking path that connects two or more "access ports" or Wi-Fi chips by setting them up in the same configuration environment. For example, a bridge for ethernet port 1 and Wi-Fi 2.4 GHz chip in the same configuration. To make this bridge, from the winbox bridge menu then the first "Bridge" tab.

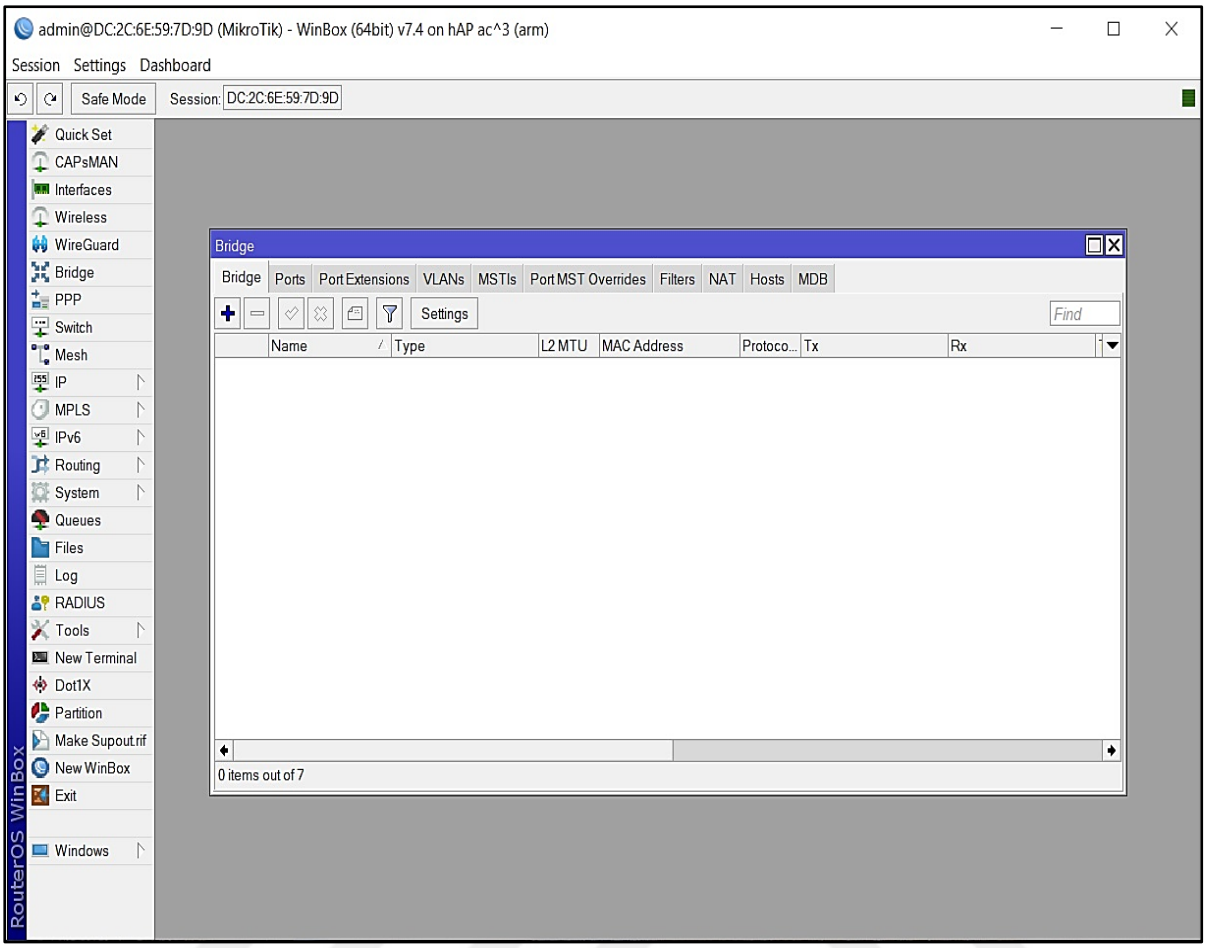

Figure 2.4: MikroTik router Bridge tab

There are different reasons prefered to use a bridge rather than configuring each interface (port) in a different configuration. Firstly, the bridge can be used to isolate ports. For example, ethernet port 1 for smart TV, ethernet port 2 is for gaming console and wireless interface is for mobile devices and so on. All configuration on the bridge will be the same and applied for each interface. Secondly, bridge provides better security. Thirdly, the bridge can be used to enable the Spanning Tree Protocol (STP) which eliminates invalid data (leftovers) moving between two connected switches or devices in the same domain (same environment and subnet). Moreover, It offers the features of (IGMP Snooping) and (DHCP Snooping).

2.2 IGMP SNOOPING

IGMP stands for Internet Group Management Protocol which is responsible for the data-routing process amoung routers and connected devices. Without this protocol, Internet cannot be accessed nor reached. The snooping process related to this protocol makes the device or any router that supports this feature to only forward IGMP data to the destination device which requested the IGMP data rather than forwarding all IGMP data coming from every connected

device, router or a switch. This way, devices which support this feature will of course be able to reduce load on the CPU and making more bandwidth available for the clients. Other manufacturers' devices either do not support it or support it at basic critieria. (Haddad, 2021).

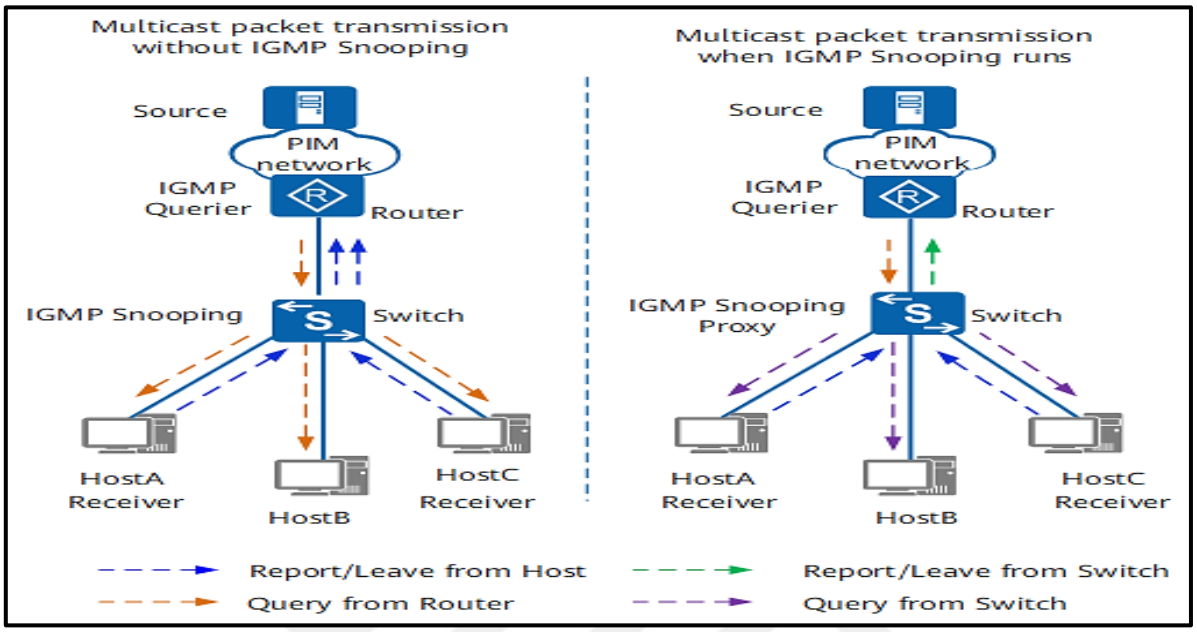

Figure 2.5: IGMP Snooping on and off state diagram (Huawei)

On the other hand, DHCP stands for Dynamic Host Configuration Protocol which is responsible for dynamically allocating and offering connected device an IP Address (Internet Protocol) rather than to statically assign each new device an IP address on the subnet. When a DHCP server configured, it will automatically allocates an IP address for the client associated with the device' MAC address. Any two or more connected devices cannot offered to use the same IP address; because each device has a different MAC address.

DHCP server has some type of relation with the Address Resolution Protocol (ARP). ARP is a protocol used for the link-layer address and discovery. It is basically shows which MAC address associated with which IP address. ARP cannot be totally disabled from a network because it will result with no Internet access. However, an unauthorized client (has no authorization to access the network) might use discovery software based on idea of the ARP; the software might of course explicit the connected devices, their MAC address, devices' names, vendors and other discovery related information. This process is called Man-In-The-Middle attack (MITM). Hence, at this point the security of the entire network degraded or either likely does not exisit at all. The attacker sometimes is able to be the source of the routing information rather than the original Internet source. For example, the attacker can make a fake payment website or a login website to steal clients' sensetive information.

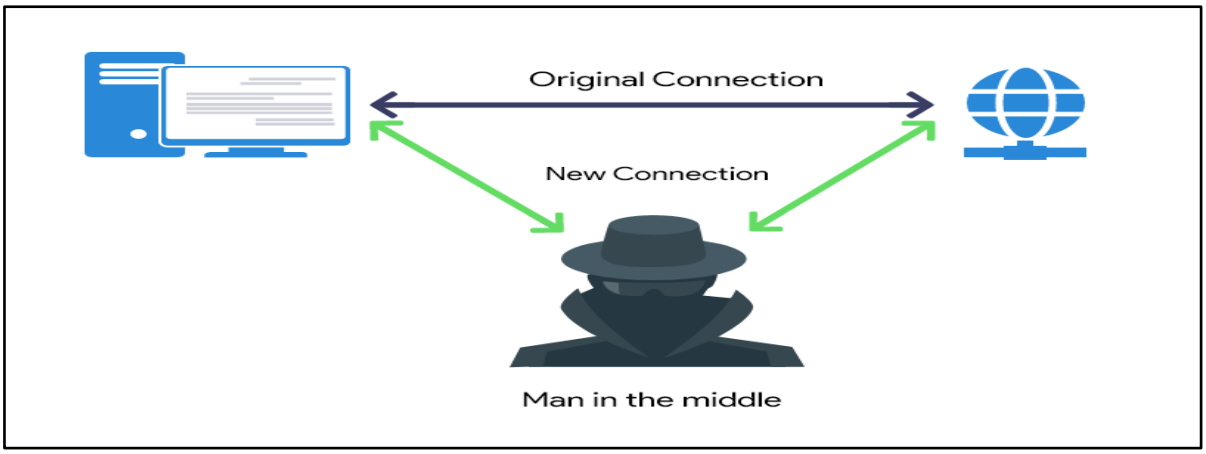

Figure 2.6: Man-In-The-Middle (MITM) Process

2.3 DHCP SNOOPING AND WI-FI SETUP

The DHCP snooping feature embeeded in MikroTik bridge interface will eliminate such type of attacks as in figure (6). The DHCP snooping will only forward from and to the real destination by checking the ARP table of which IPs linked to the exisited MAC addresses. Here, the ARP of the bridge needed to be set on “replay-only” than deafult “enabled” state. In addition, fake or any an unauthorized client (attacker) will be unable to offer information for the connected client. That’s it. The security of a network becomes enhanced with DHCP-Snooping enabled. As mentioned, if each interface (port) is configured alone without the bridge, both IGMP and DHCP snooping will be unavaliable.

From the “Bridge” tab to add a bridge interface, the (+) sign is used to add a new one. To apply and use the previously mentioned features, we simply tick the “IGMP Snooping” and “DHCP Snooping” options to enable it, then changing the ARP to “replay-only” state. We can also name the bridge interface but we will keep the default name which is “bridge1.” The bridge also offers options for the Spanning Tree Protocol (STP). The default configuration is set to Rapid Spanning Tree Protocol (RSTP). RSTP is an improved version of Spanning Tree Protocol (STP) and both of them nearly do the same job. The only difference is that RSTP has four roles for the configured one while STP has three roles. Keeping the mode set on RSTP is doing fine and we do not change it usually unless it is necessary in some circumstances.

The Virtual LAN (VLAN) is not configured and it is left without configuration. This feature is usually for ISPs and large enterprised networks which have many clients and sub-ISPs. VLANs help to reduce the costs of the network and offer better security than Local Area Connection ports (LANs). We do not need it in the testing process and in writing this paper.

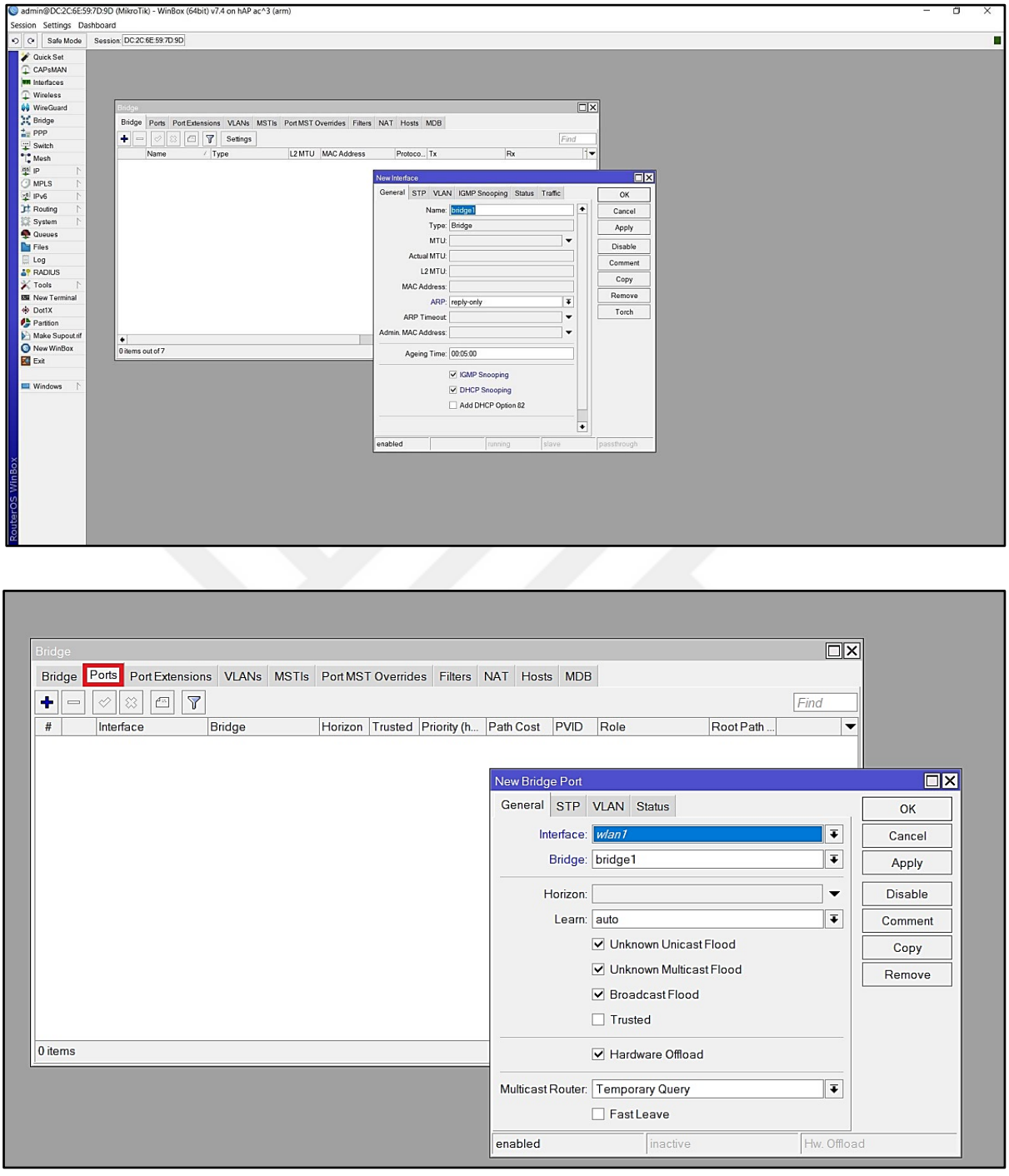

Figure 2.7: Creating a new bridge interface

In order to assign an interface to the bridge interface, we use bridge menu, then click ports tab. A new popup window will appear as shown in figure above. A significant step is to let the newly created “bridge1” identify which are the interfaces (an ethernet port or a wireless interface) are the members (interfaces) belong to the bridge. The settings of the bridge ports can be customized according to the purpose of the ISP or the owner. In this state, we will keep to use the defaults.

Since we make “wlan1” which is the wireless interface of (2.4 GHz) band a member of the “bridge1” interface, we need to configure “wlan1” and enable it. To do so, from the main menu on the left, choose “wireless” and it will open like in the figure (8) bellow.

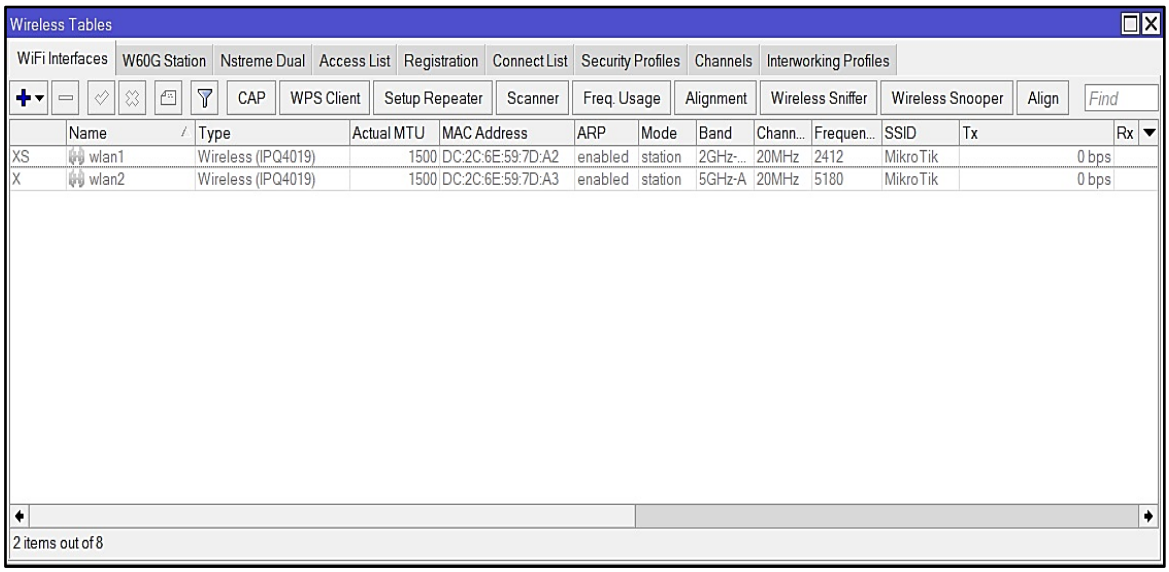

Figure 2.8: Wireless Tables menu

It is recommended firstly to setup a security profile for the “wlan1”, to enable password-protected access Wi-Fi before enabling Wi-Fi for the clients.

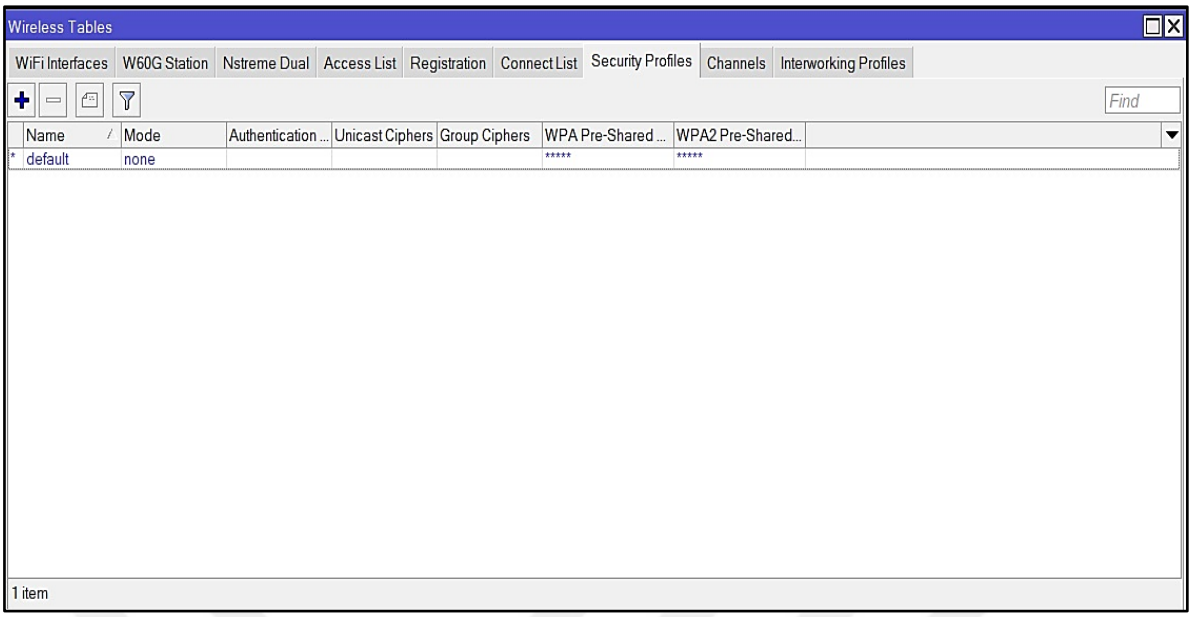

Figure 2.9: Wireless Security Profiles

The default profile exist but not a password-protected. In this state the Wi-Fi is an open-access and it is not likely to be used anymore. So, either we configure it as password-protected acces or creating a new profile. Either using the default or creating a new profile does not provide any difference. The default security profile will be used after configuration. Doubling the click on default profile let an administator sets-up the security that suit the needs and criterias. We have successfully setup the password-protected access as in the bellow figure. Enforcing Advanced Encryption Standard (AES) for both Unicast Ciphers and Group Ciphers will enhance the security of the Wi-Fi network. More options are also can be used such as the RADIUS authentication method, EAP which uses an SSL/TLS authenication securely and the static keys option.

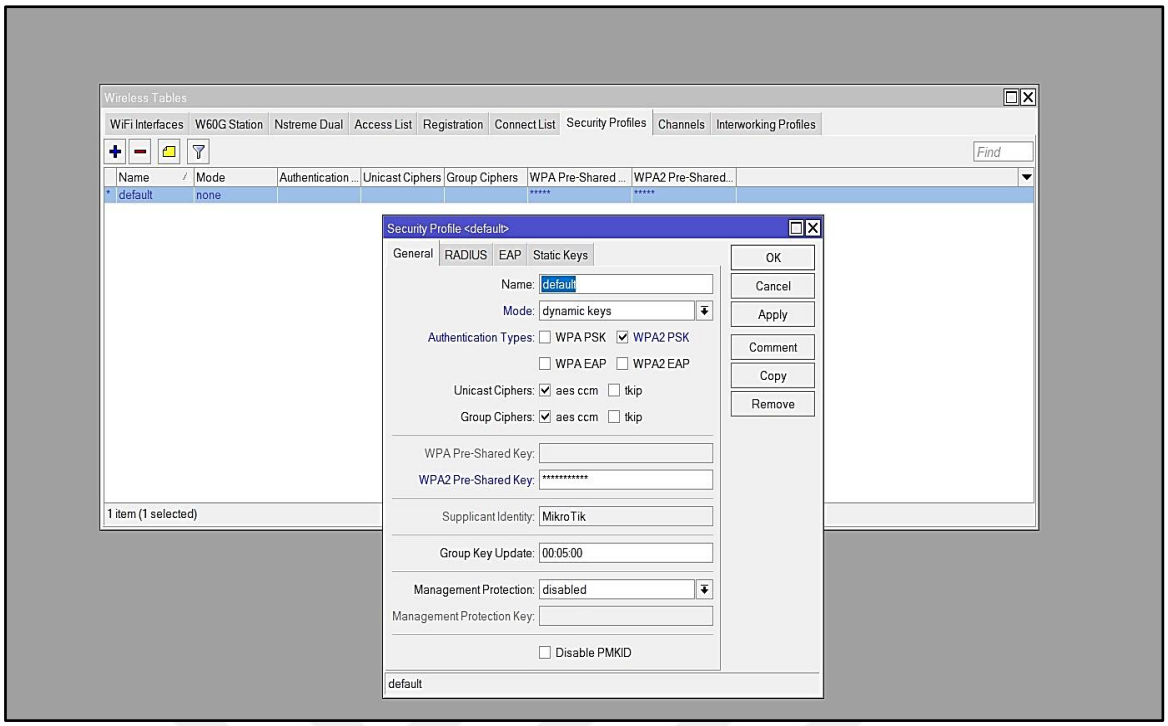

Figure 2.10: Setting the default security profile up

There are two Wi-Fi interfaces as described earlier in this chapter because this MikroTik device of two Wi-Fi chips: “wlan1” for the (2.4 GHz) band and the other one “wlan2” for the (5 GHz) band. “wlan2” will not e used in this testing procedures because only new devices supports the (5 GHz) band while the (2.4 GHz) is mostly used. This process we made is to let more devices able to connect in this testing procedure. Most MikroTik devices has one Wi-Fi chip interface usually “wlan1” for the (2.4 GHz) band and do not support the (5 GHz). So, only one interface exists. Double click on “wlan1” will pops-up the configuration menu and options.

Back to the wireless interfaces tab as in the figure bellow, there are two modes for configuration: advanced and simple. Simple mode is a basic mode to setup the Wi-Fi interface. The advanced mode offers more options to be configured. The advanced mode will be selected. By just clicking on the “Advanced mode” button, more options appear. From the general tab of the “wlan1” interface ARP should be set to “replay-only” mode for the same purpose as in the ARP mode of the “bridge1” interface. The most important tab in configuration is the wireless tab of the “wlan1” interface.

Throughout the “wlan1” interface wireless tab, changes usually needed for the correct setup based on the purpose of the Wi-Fi mode. Our purpose in this testing procedure is make the Wi-Fi available for clients. Generally speaking, we will prepare the Wi-Fi so users can access the Internet. Accordingly, the mode of the wireless must be set to “ap bridge.” This mode will

make the Wi-Fi as an access point (AP) for clients. Band is set to “2GHz-B/G/N”, channel width “20MHz”, frequency “auto”, SSID – the wireless broadcasting name “hAp ac3”, radio name – the associated information with broadcasting wireless name; usually the information of an owner or administrator and it is not the name of the broadcasting signal; is set to “Testing Procedures.” Wireless protocol “802.11” standarad, WPS mode “disabled” because we do not need this old-fashioned feature, and the country – it is a must for an administrator to be careful and submitted to local law regulation when choosing channel width, country and frequency mode options, but since this is for testing, we set the country to “no_country_set”, unchecking “default forward” is useful which does not allow clients’ devices to access each other. It is preferable for security purposes then leaving all other settings to manufacturer-defaults. One important notice to be taken into consideration is the “distance” option through the advanced tab. If the router is to be used in homes or small-offices, it is suggested to make it “indoors” rather than to dynamically allocated distance in Kilometers. Finally, clicking on apply button, enable then Ok and the signal is on air.

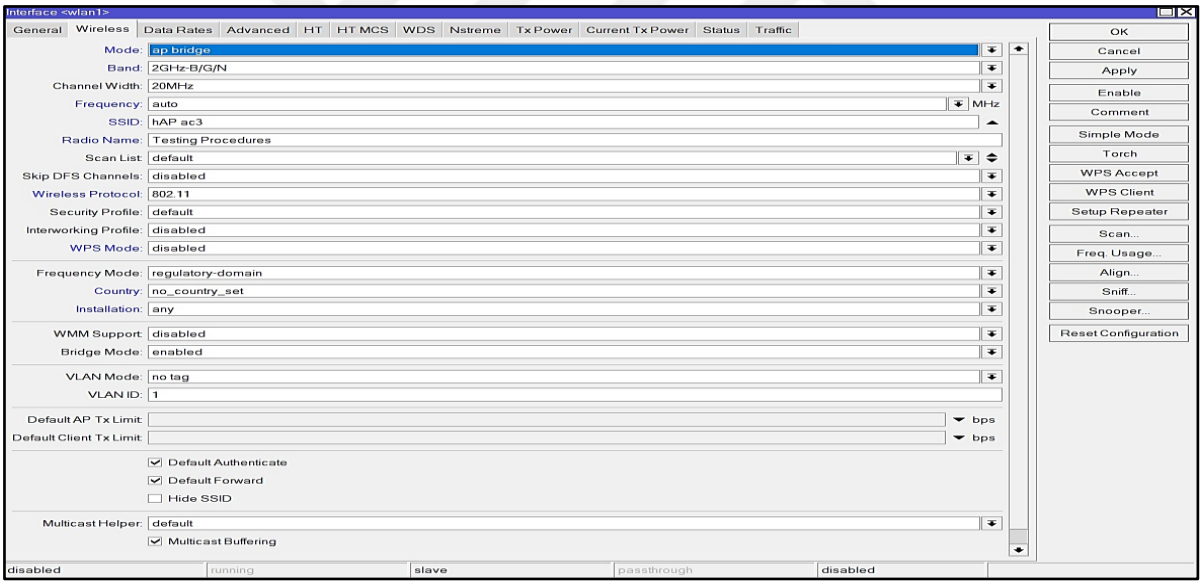

Figure 2.11: Wireless “wlan1” interface configured settings

At this level, any Wi-Fi capable device near to the network signal would be able to connect and access it using the password we made earlier. Thus, the Wi-Fi interface is ready for clients.

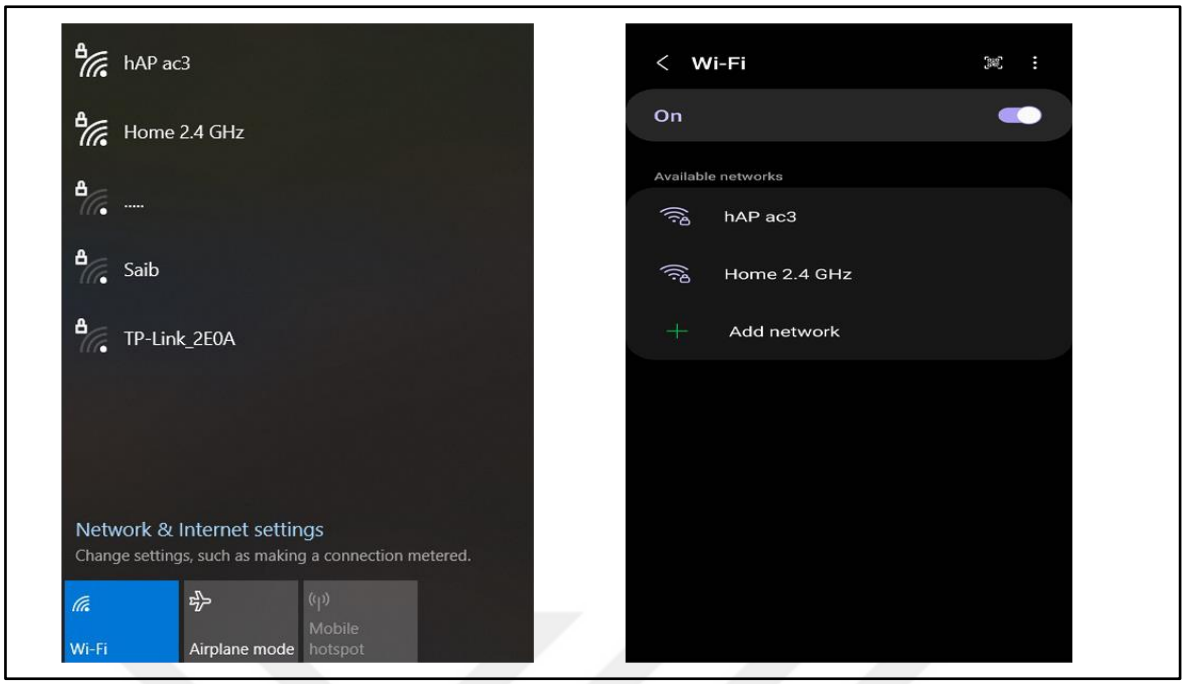

Figure 2.12: Clients' nearby devices able to receive the Wi-Fi signal

When a laptop or PC connects to the Wi-Fi we created, the connection will be successful and the network status will be unidentified. The same thing will happen for a smart phone or tablet when connects but in phones and tablets, the connection will fail and a message might appear telling failed to get IP address. This is truly would happen because until now we have not configured the IP address and the DHCP server to be used later in offering IPs dynamically to clients' devices. The next procedure is to set the MikroTik router IP or IPs based on usage. We are going to setup one IP address on the "bridge1" interface then assigning the DHCP server for the created IP address. This is so important because without an IP addresses, device unable to connect and contacted from a network to network, gateways or subnets.

To procceed for creating an IP address, we click on the IP menu from the left sidebar of WinBox then choosing "Addresses." Clicking the (+) sign will allow an administrator to specify an owner-prefered choice of entering the IP address. It is not something obligatory to choose a specific IP – unless it is required by the ISP or the management-side enterprise. As intended for testing purpose, we are going to set it as the device factory default IP which is (192.168.88.1) with subnet mask (255.255.255.224) – CIDR notation of (/27). It is an important note that in this testing process we are only to use IPv4 version and all tests will depend on IPv4 rather of IPv6. Because IPv6 Internet access is limited only to private suituations or companies like research facilities or studying purposes. In other words, currently not available for public.

The subnet mask (255.255.255.224) – CIDR notation of (/27) will allow clients connections of up to 30 hosts. In this process, we are going to take a sample of 30 connected hosts (clients) in the same time (session) to get better testing results and discover the router capablilities.

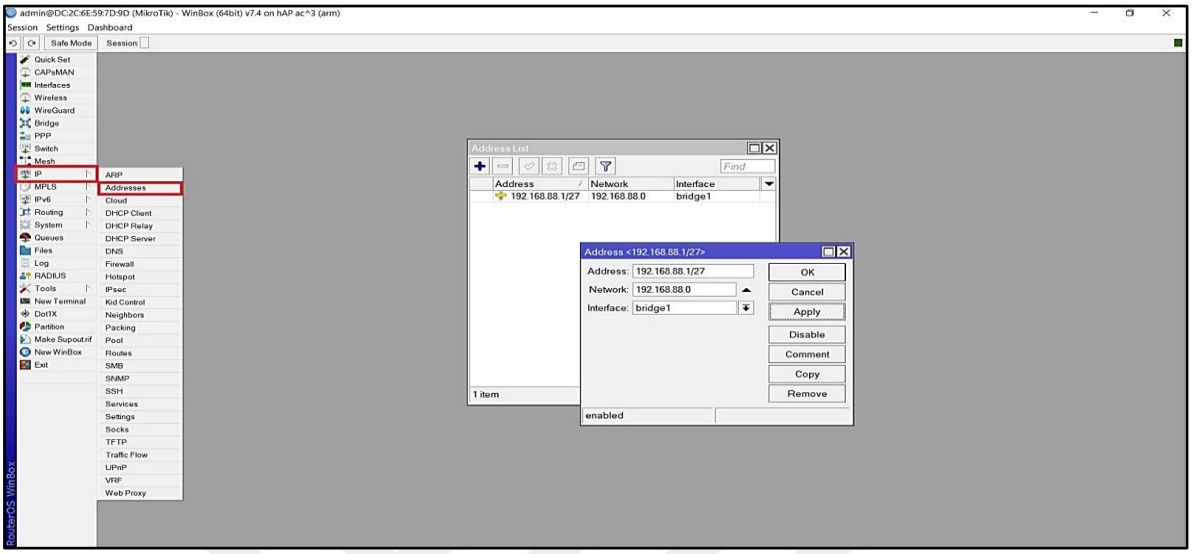

Figure 2.13: Setting up the IP address and subnet mask on bridge1 interface

Setting up the IP address and subnet mask do not successfully let clients connect and get dynamic IPs. Hence, the DHCP server is required for this criteria. From the IP menu we just select the “DHCP Server” option and the DHCP server options window opens. Choosing “DHCP Setup” will allow us to install and configure the DHCP server for an interface. Since we assigned the IP address for the “bridge1” interface, DHCP server will be also associated for this IP address; meaning that DHCP server would also be on the “bridge1” interface. From the setup window, we select the “bridge1” interface then clicking next button, the DHCP address space will be automatically entered because we have already configured the IP address and subnet mask on the choosen interface which it is (192.168.88.0/27). The next step is to specify the “Gateway for DHCP network” which is usually the same IP address – unless it is necessary to be manually entered and required by an ISP.

Going forward by clicking on next button will give us the suggested pool IP address range. The pool or the IP range determines how many clients will be offered an IP address available from the DHCP server. Each new client will get an IP address as long as there are address available from the DHCP server. When the DHCP server does not have addresses, clients cannot connect unless one of them ends the connection. However, the next step is to config the DNS server associated with the DHCP server – In our testing procedures we are likely to to use the same IP address of the default gateway – this has some advantages that to be discussed later. When

setting the IP of the DNS server, it must be taken into the consideration that some ISPs never to allow an owner to choose the DNS but only the ISPs DNS. It is highly recommended to contact with the ISP for DNS options. The final step would be the DHCP lease-time. It is simply means how much time an IP address will lasts for the connected client. Usually measured and configured in seconds up to couple years defined by the administrator. If a client disconnects from the DHCP server within one hour and the DHCP server lease time is set to two days for example, the IP address will expire in two days despite the client had already disconnected. For this reason, it is not recommended to set the lease-time more than one day. In our testing, we are going to set the DHCP lease-time up to six hours max. applying and OK.

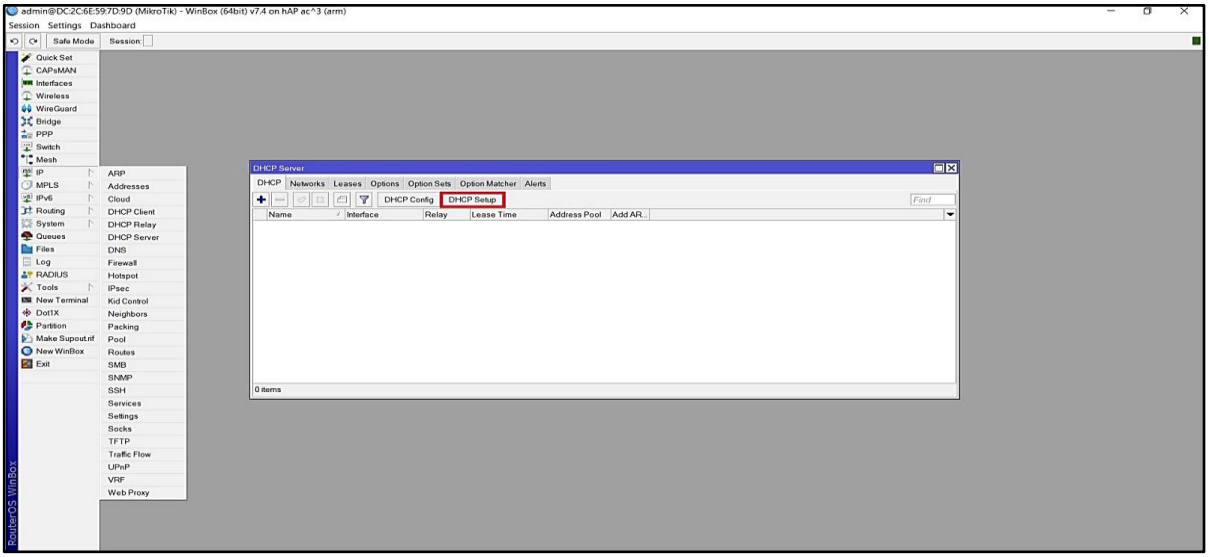

Figure 2.14: Setting up the DHCP server

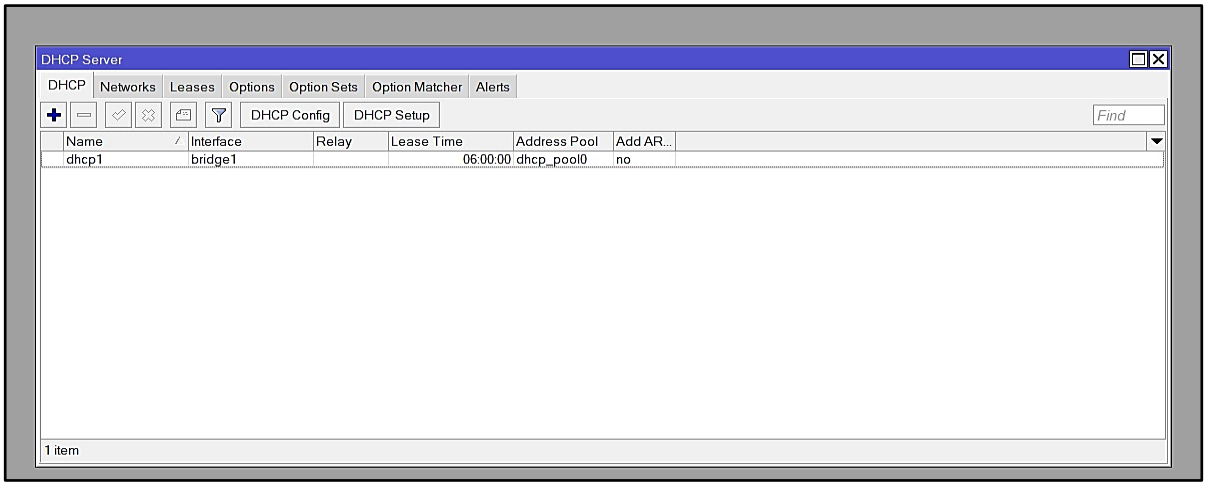

Figure 2.15: DHCP Server Configured

However, some DHCP server settings need to be modified. As shown in figure (15) above, to modify, we double-click on the “dhcp1” to open the DHCP server settings. It is a must that we check the “Add ARP For Leases” option because we set “bridge1” and “wlan1” interface on “replay-only” ARP mode. If this option is neglected nor ticked or checked, devices cannot access the Internet even if they have successfully got their IP addresses from the DHCP server. Other two settings are to set the “Bootp Support” to dynamic to let us furthur select the “Bootp Lease Time” to lease time – the lease time we set earlier up to 6 hours.

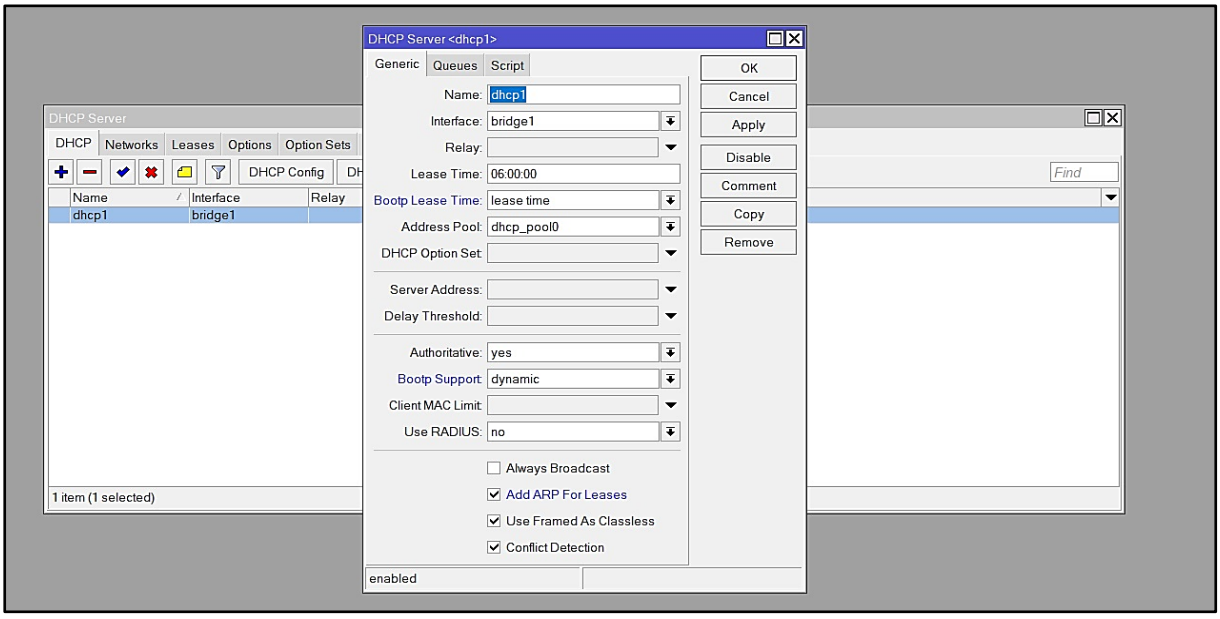

Figure 2.16: Changing some DHCP Server Settings

At this point, our device for the testing is ready for the clients connections. However, clients’ connections at this level is regular and basic. In other words, they connect to the Wi-Fi network, DHCP server assigns an IP address, the client accesses the Internet – Network Address Translation (NAT) must be configured on the DHCP server space in the device’ firewall nat section to allow clients access the Internet. Despite, we will setup another type of service to let clients connect rather than using one basic connections type – like the simple DHCP access point. It is the time to setup the Point-to-Point over Ethernet (PPPoE) server for clients to be later used in make comparisons for reliablity, performance, test results and in addition, comparing these with other models of routers.

2.4 POINT-TO-POINT OVER ETHERNET (PPPOE) SERVER

The PPPoE is a communication protocol used by many ISPs to connect many hosts across ethernet networks. A PPPoE makes the administration process for ISPs easier. Simply, it encapsulates PPP frames inside the ethernet frame. Thus, expanding connections among hosts. An ISP can enable encryption and compression for a PPPoE connection. However, to create a PPPoE server we usually add a new IP pool for the PPPoE server first. From the "IP" menu then "Pool." The (+) sign used to add an IP pool range. The range can be set according to the administrator or ISP-specific range. In ours, the range will be between (192.168.140.1-192.168.140.30). This range will only allow up to 30 maximum connected hosts for our testing procedures. It can be longer or shorter than this range according to an administrator preference.

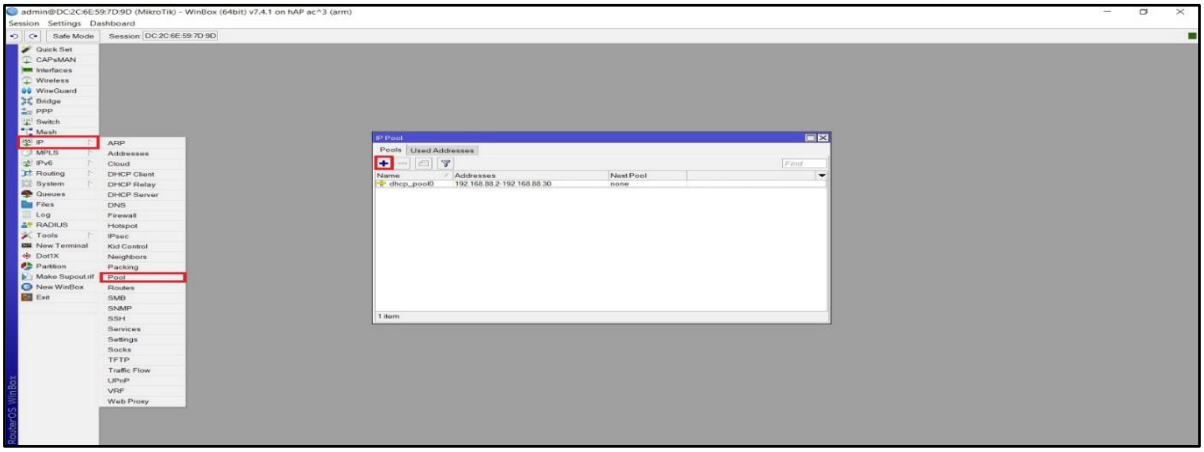

Figure 2.17: Create a new IP pool

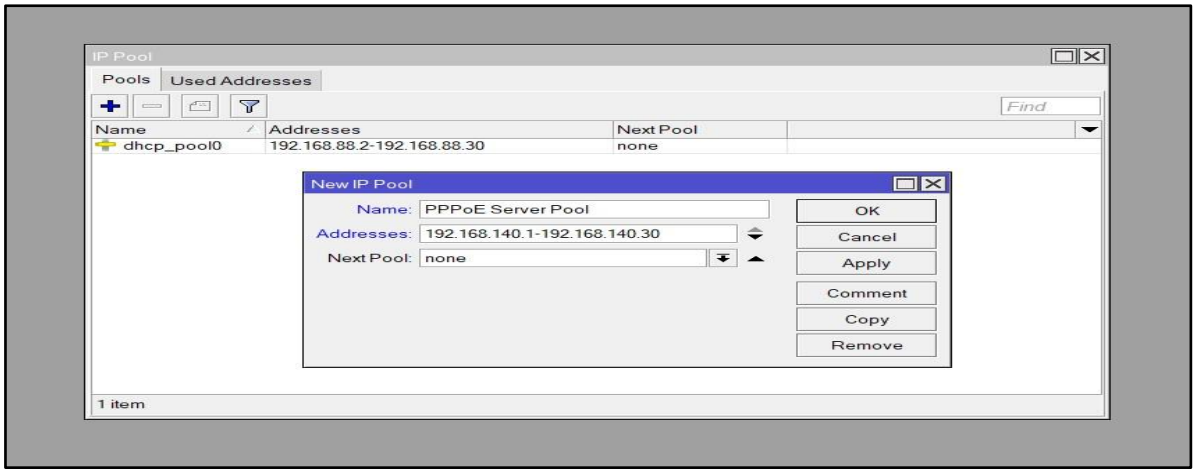

Figure 2.18: Pppoe server pool IP range

When the pool IP set, it leads us to the next step in order to set the PPPoE server up. At first we must setup a PPPoE profile. A PPPoE profile is a mode-like configuration that can be set to same configuration for all the connected clients or hosts. When creating a PPPoE profile there are some settings need to be taken in consideration.

To proceed creating the PPPoE profile, we need to click on the “PPP” menu, clicking on the plus sign, then we congigure the PPPoE profile. All the connected clients who belong to this PPPoE profile configuration will all have the same parameters except the remote address – which it is an IP address that a client gets from the PPPoE pool IP address range that we have created earlier.

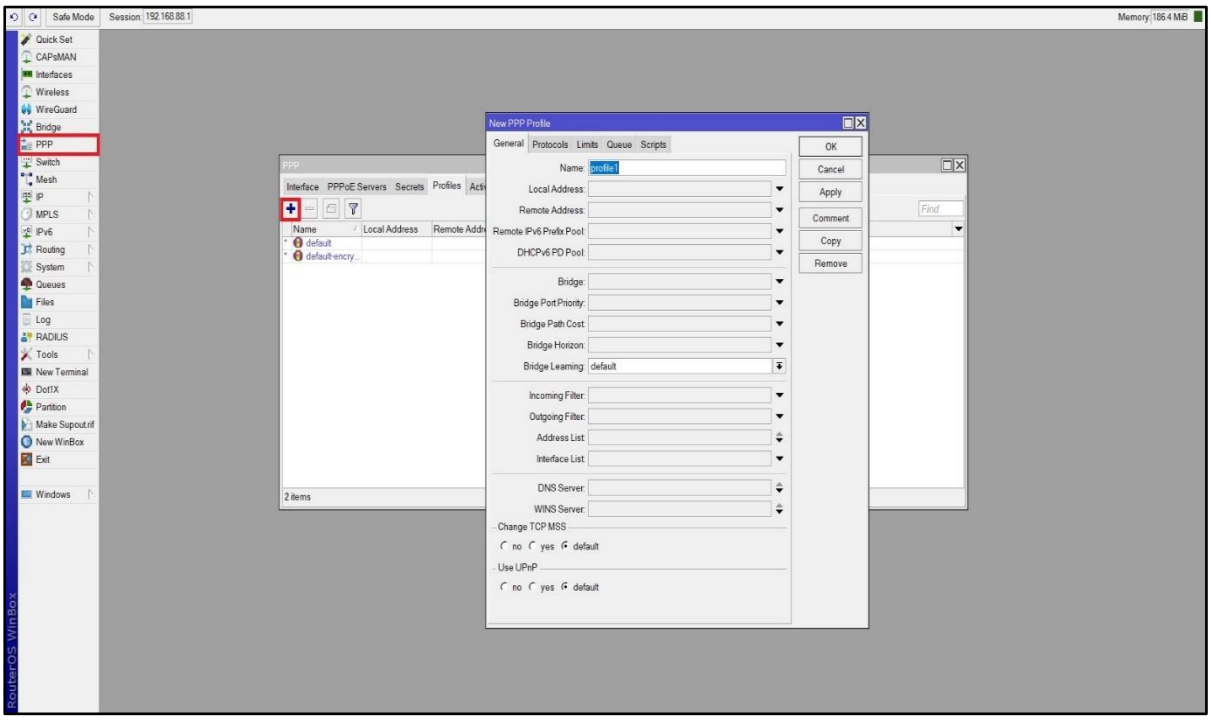

Figure 2.19: Creating the PPPoE Profile

After the configuration profile successfully created, it is a must that we assign some clients their PPPoE credentials, likely a username and password for each client. From the same “PPP” menu, then moving to the “secrets” tab which it is an essential menu that we can use not just to assign users credentails for PPPoE usernames and passwords, but also for other types of connections, such as PPTP and L2TP/IPsec VPN connections. In this step, we will add (30) clients for the testing procedures in order to test the MikroTik router ability, CPU power and throughput as in addition to the PPPoE security. A packet capturing tool which it is an open-source software will be used to check for PPPoE security issues and discovery matters. This tool is called ‘Wireshark’ which can be downloaded for free from http://www.wireshark.org.

Here, our clients usernames will be “client1” for the first client and “client30” for the last one and we will assign each client a password which is different from other clients’ password. No two clients have the same password and this setep is to avoid a clients access the Internet using another client’s credentials and for other security purposes. However, the “Wireshark” tool will be used for analyzing the packets through the PPPoE clients and the MikroTik router. It is important to notice that this step is to discover network weakness and security issues related to the entire network environment but not for unauthorized access, eavesdropping, corrupting the network and other similar issues related. One should be careful in using ‘Wireshark’ because it might be not allowed in some countries or it is only allowed for the network administartors. So, we should always follow the law and specific country regulations.

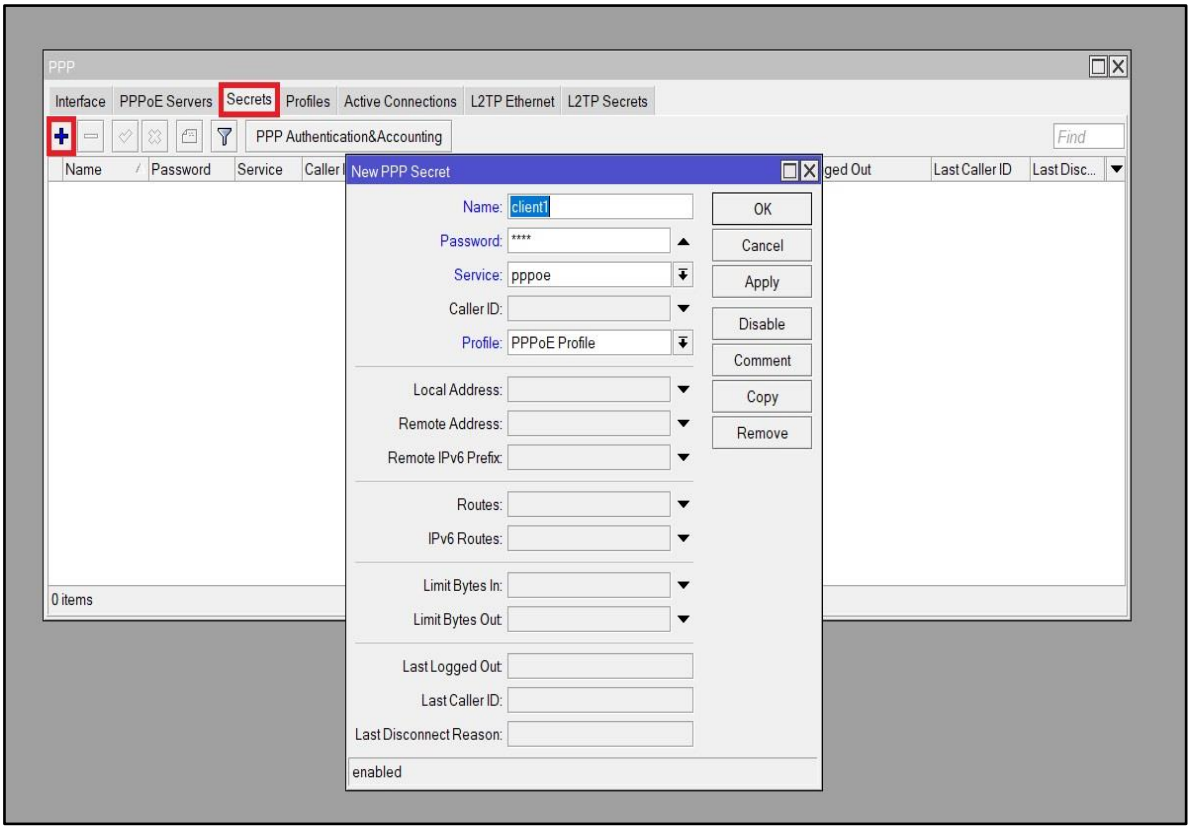

Figure 2.20: Assign PPPoE clients their credentials

For the clients to be able to connect to the MikroTik PPPoE server, we must specify which outgoing interface will be used as PPPoE server. To setup, from the “PPP” menu moving to the “PPPoE Servers” tab and add the PPPoE service through the plus sign as in the figure (20) below.

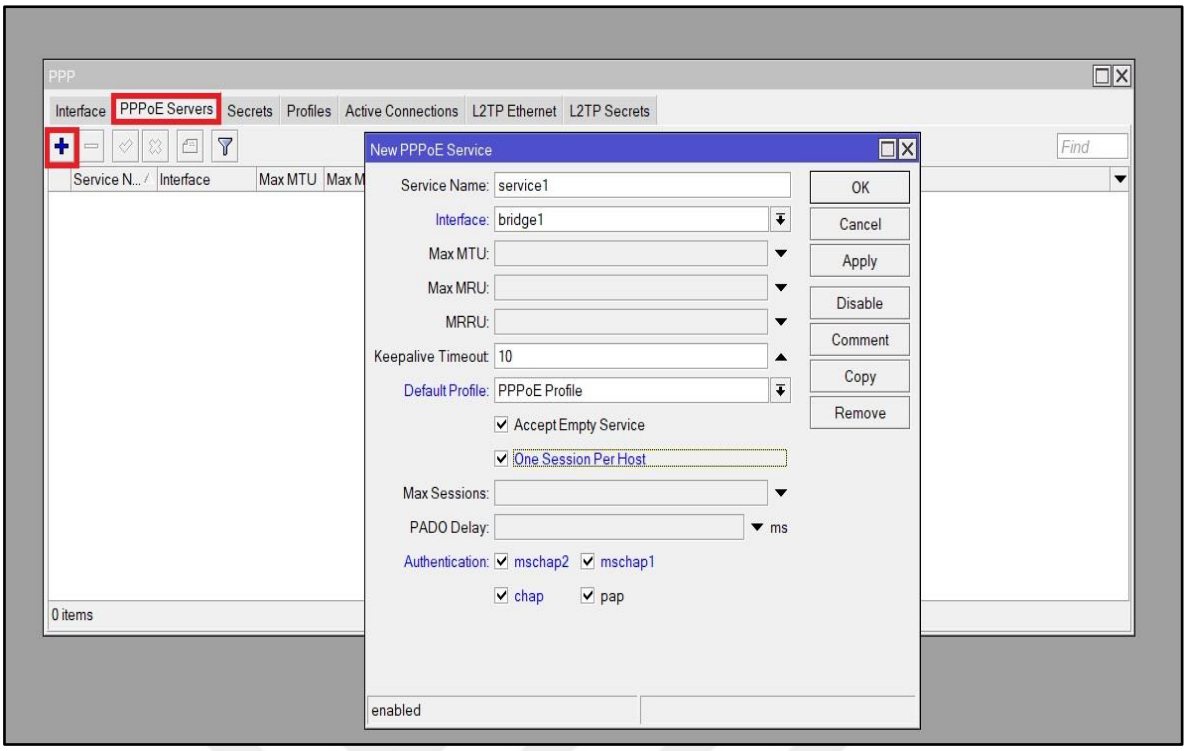

Figure 2.21: PPPoE server setup

The “Service Name” can be anything according to the administrator’s own, “Interface” is the outgoing port or the wlan port which is intended for clients to connect through, “Keepalive Timeout” is the seconds where the client will be disconnected from the PPPoE server if there is no active frames or packets, “One Session Per Host” ensures no more than one session per the same client. For example, client1 cannot have two session for himself using the same credentials unless it is allowed by an administrator and “Authentication” is the authentication protocol supported by the PPPoE server and the client-side to allow access. Authentication is very important and it must be compatible between the client’s device and enabled by the PPPoE server. If it is not, a client might face issues and will result in unsuccessful connection and connections might be terminated by the MikroTik PPPoE server. Anyway, at this level, clients are ready to get connected to the MikroTik PPPoE server we created earlier but they cannot access the Internet unless we created a firewall NAT (Network Address Translation) rule for the PPPoE IP Pool address. Simply from the “IP”, “Firewall”, “NAT”, then adding the rule by clicking the plus sign, add the source address and setting the action to “masquerade” through the action tab, apply and OK.

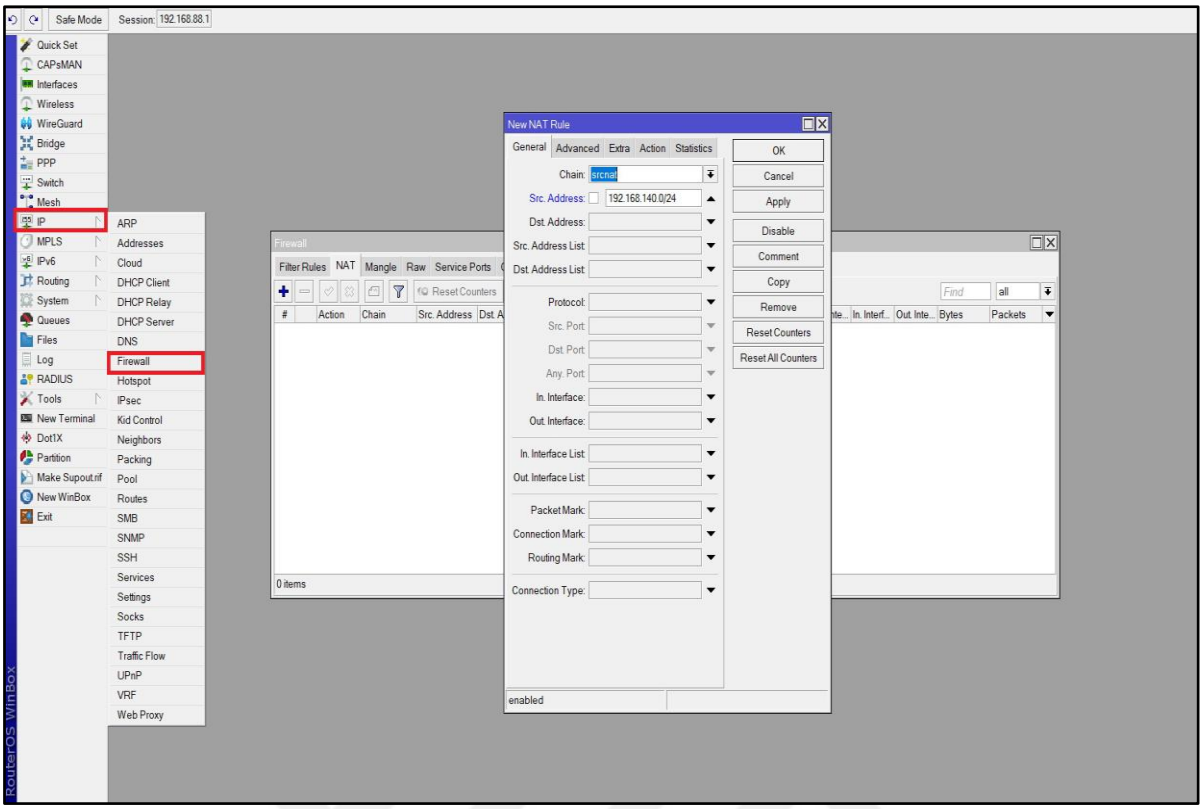

Figure 2.22: Firewall NAT rule to allow Internet Access for clients

Now let's run the "Wireshark" discovery tool first and then connecting the first client to the MikroTik PPPoE server. For the first client, we have already set its username as "client1" and the password we assigned. We will use a Windows PC to run the tool and connect the client. The tool will be running through a different PC and the client will use another PC to connected. In other words, the tool and "client1" are not using the same Windows PC for this test. It is also to mention that all the (30) PPPoE clients will be using their own PCs to connect for this testing. Each client will use his/her own PC. The 'Wireshark' tool will be running on a PC in which the network administrator's own. It is an important notice that connecting to a PPPoE server through PC differs from connecting through an Apple MacOS device. So, a device manual might be needed.

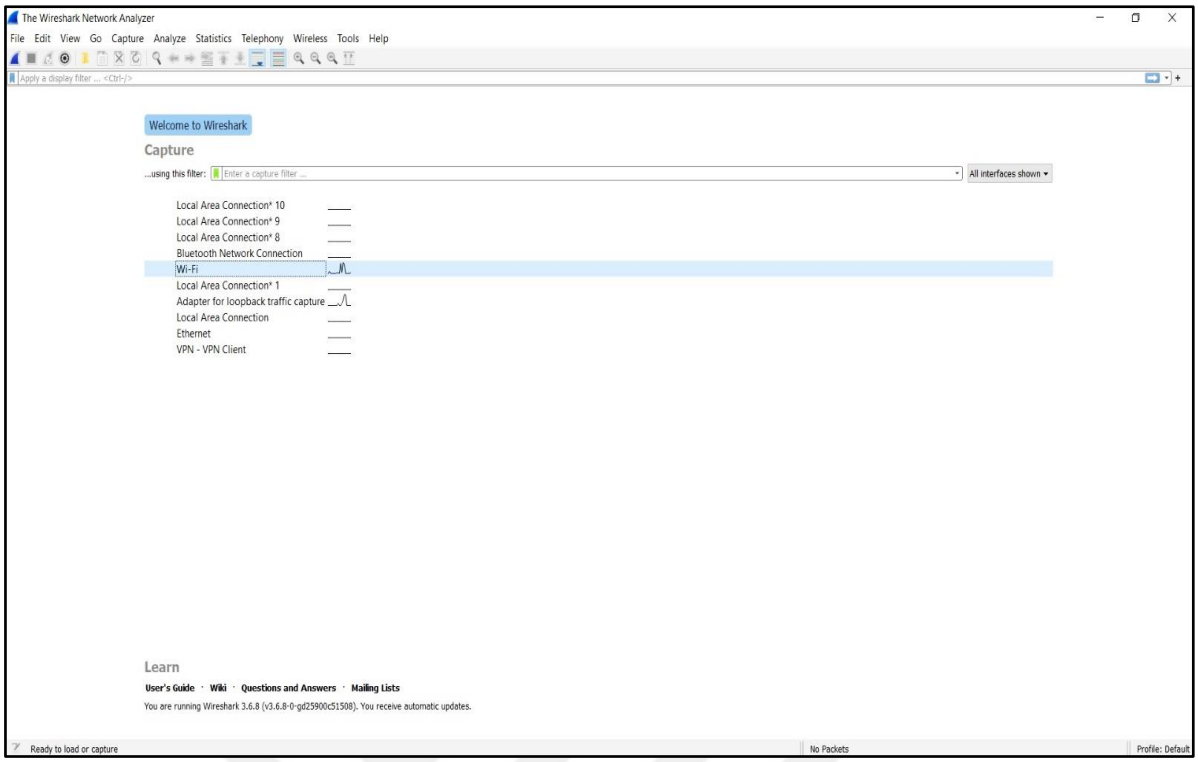

Figure 2.23: Wireshark tool layout at first run

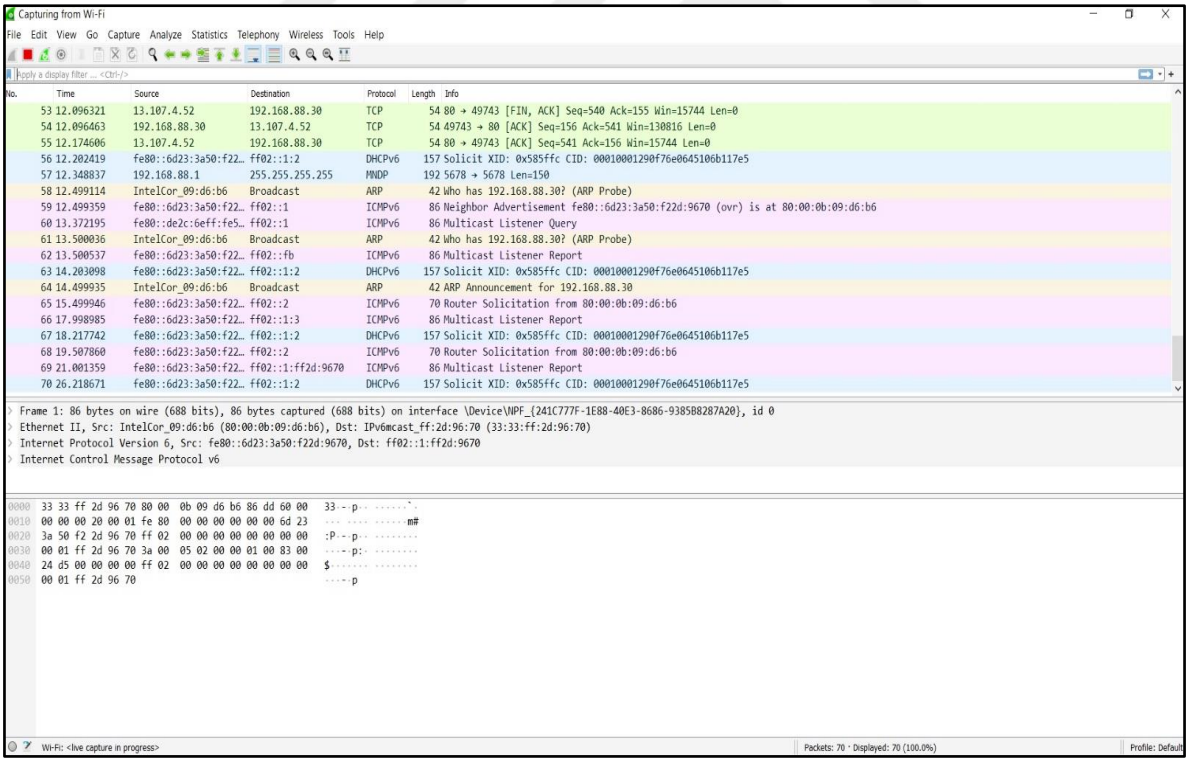

Figure 2.24: Wireshark tool is capturing packets throughout the Wi-Fi interface

From the above, we can see that by doubling the click on the Wi-Fi interface allow "Wireshark" to start capturing packets on the selected interface. In front of the WiFi in figure (22), shows an activity and other interfaces only a line which indicates there is no activity on the interface.

So, we have selected the Wi-Fi interface because there is an activity and it is the interface we conneced the “Wireshark” administrator PC to the router. Figure (24) shows that “Wireshark” tool is bringing some captured data and these will of course be more data and more as long as the capturing tool is running. Here, the first client will connect through another PC to the MikroTik PPPoE server.

After the “client1” successfully get connected, the “Wireshark” in the administrator’s PC tool captured a security flaw in the PPPoE authentication protocol that we have setup earlier. This flaw can be used by an unathorized client which leads him to explicit clients’ usernames and password as in addition it might be used for others to access the Internet even if they have not paid for the service or for the subscribtion. Figure (24) below shows the PPPoE server’s security flaw in the authentication protocol.

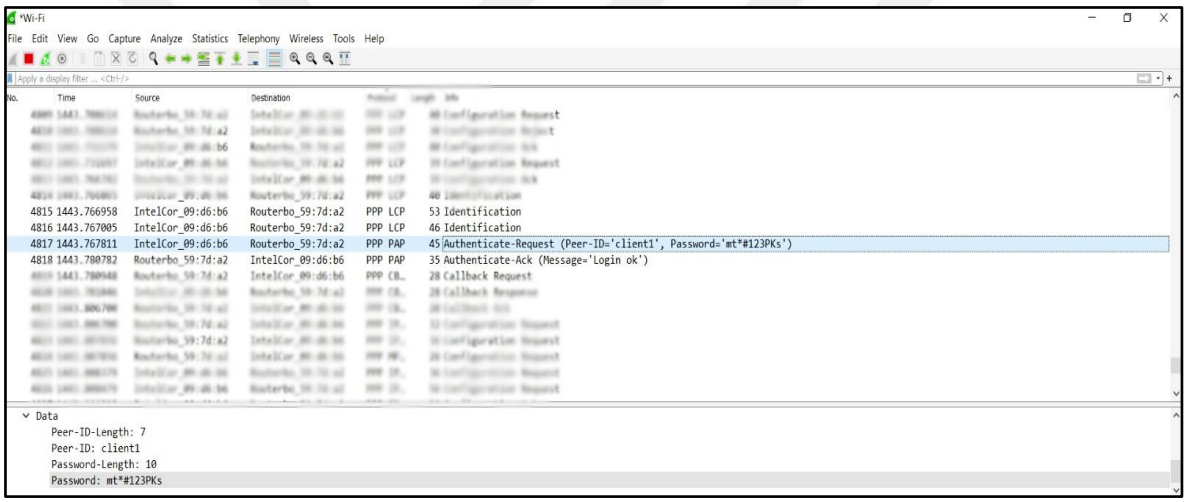

Figure 2.25: PPPoE server authentication security flaw captured by the Wireshark tool

From the figure (24), the “Peer-ID” is the client’s username – which it is “client1” we have created in the MikroTik and “password” is the “client1’s” password that we have assigned to. If you look at the password; it is “mt*#123PKs” which it is the real password we have assigned to “client1.” This will of course happen to all the clients. Their usernames and passwords can be easily captured in a plain text which it is something a network administartor must immediately avoid because it will lead to other risky issues such as clients subscribtions’ theft and money loss for the network administrator.

To avoid such securty flaw the network administrator must modify the PPPoE server configuration for the allowed authentication protocols. This will simply be done by clicking on “PPP” menu, “PPPoE Servers” tab, then doubling the click on the PPPoE server we have

already created – which it is “service1” in our state. If we look at the tool in figure (24) above, we can draw that the authentication protocol used to connect “client1” for the PPPoE server is PAP (Password Authentication Protocol). This protocol used a mechanism to allow authentication between two sides (usually a client and server) to tranform data in a plain text which it is the flaw that leads to password discovery in plain text. For the modification of the MikroTik PPPoE server, we will allow the PPPoE server to use all the authentication protocols except the PAP protocol. This will reduce the risk that passwords transferred in a plain text from the client to the server.

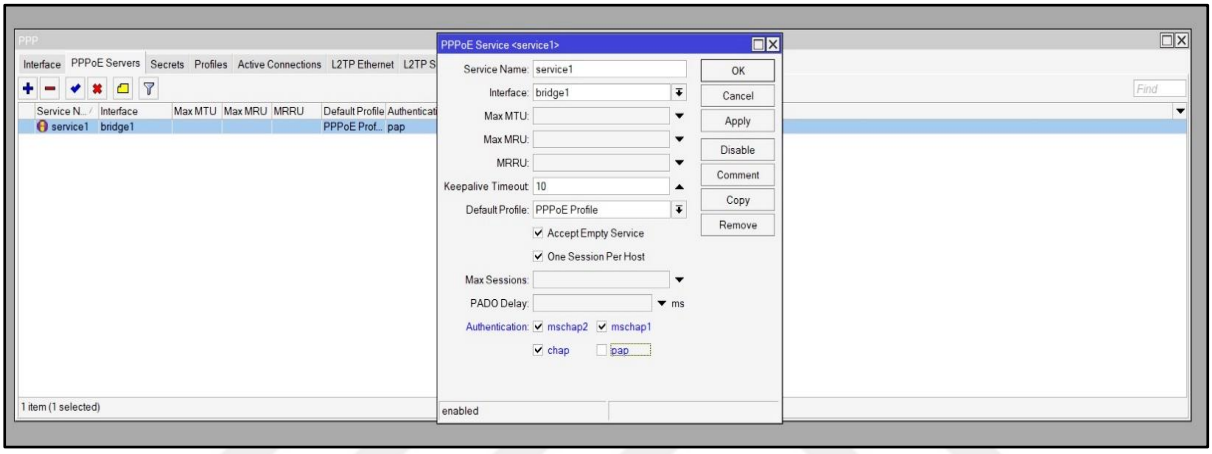

Figure 2.26: Modifying the PPPoE server authentication protocols

After the modification of the authentication protocols, let’s reconnect “client1” and see the data captured by the Wireshark tool.

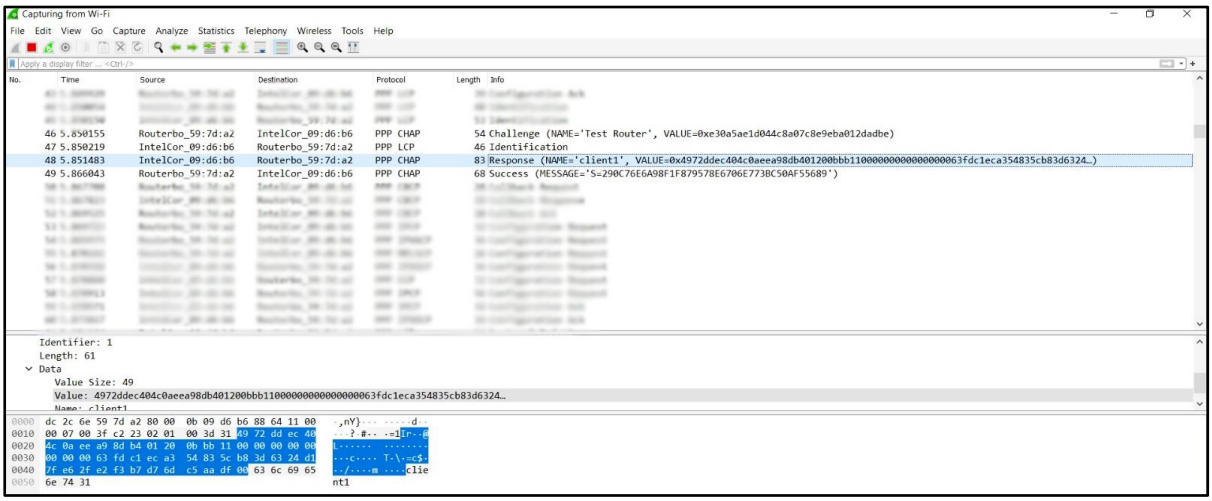

Figure 2.27: Data captured after the modification of authentication protocols

The data captured above shows that the PPP authentication protocol used is CHAP (Challenge Handshake Authentication Protocol) rather than PAP in the previous connection state. Accordingly, the "VALUE" field represents the clients' password which it is not in a plain text format but instead, it is an encrypted data. We can draw the conclusion that data (usernames and passwords) transferred in an encrypted mechanism. The risk of getting passwords leakage is reduced. Despite this mechanism is less risky than PAP, there are some password-cracking tools that can decrypt the data in the "VALUE" filed to a plain text (which it is not to be mentioned do not for security purposes). In addition, some devices cannot connect to the PPPoE server because they are only compatible with PAP. However, these two issues: the password and compatibility in a PPPoE; leads us to look for a better and enhanced-security connection type. So, we will use the L2TP/IPsec VPN method to allow clients connect to the MikroTik device and access the Internet without having the issues metioned earlier.

The L2TP/IPsec is another connection type widely used as VPN and also depends on the PPP (Point-to-Point Protocol) but with a higher security enforced by the IPsec (IP Security) protocol that data entirely encrypted by the policy in which the network administrator creates for clients rather than only the encryption of the athentication credentials because IPsec uses encryption and authentication algorithms.

2.5 SETTING-UP THE L2TP/IPSEC SERVER

In order to prepare the L2TP server for the clients, it is essentially to setup the IPsec (IP Security) policy first because without the IPsec policy clients will be unable to access the server. However, to proceed, from the "IP" menu, "IPsec", then the "Proposals" tab. Since this is for testing procedures, we will modify the preset "default" MikroTik proposal as in the figure (27) below.

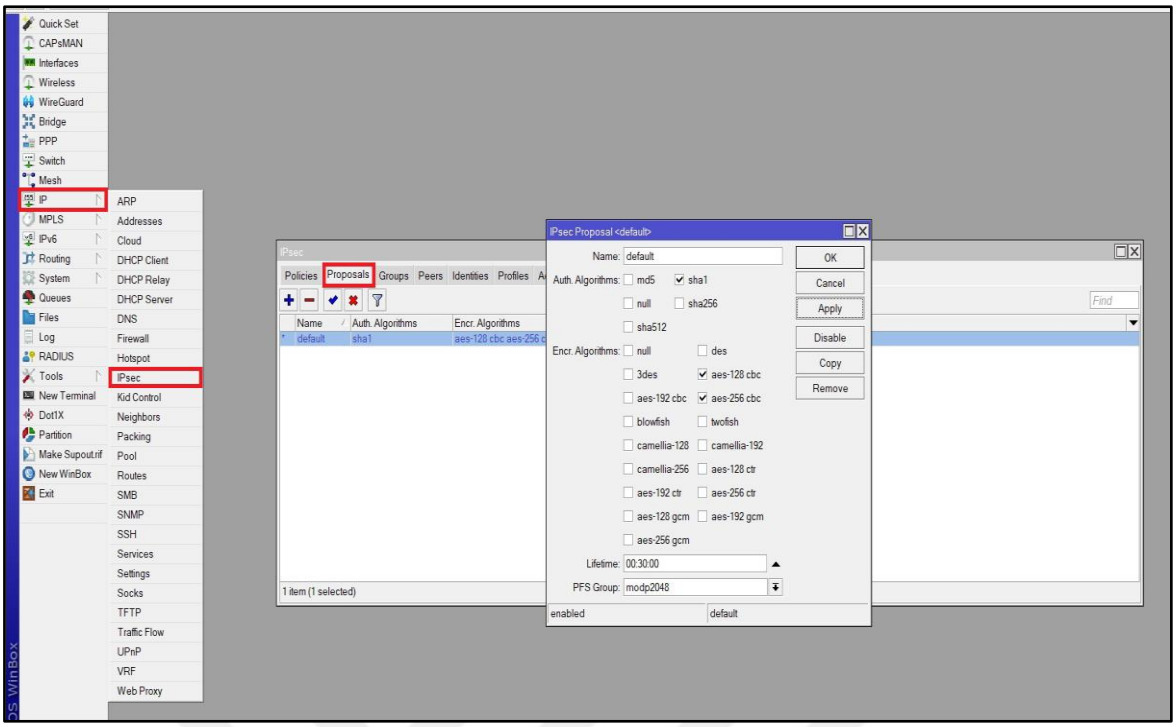

Figure 2.28: Modifying IPsec encryption and authentication algorithms

Our modification involves using the (sha1) as the authentication algorithm in which the authentication data exchanged, AES 128-bit and AES 256-bit with CBC as well as key length to be of "modp2048." The AES (Advanced Encryption Standard) will be used to securely exchange clients' data not just to the MikroTik server but also for outside the MikroTik device. This ensures better security than using PPPoE server. It is a matter that in this test we have not set an IPsec policy for a specific IP address, client or an IP address range because the default MikroTik policy allow all IPs. However, in real use the administrator might need to alter these settings.

Another important setting for IPsec is the profile settings. Like the PPPoE profile has some basic parameters, the IPsec has parameters also but is related for more security beyond the basics. These parameters allow the network administrator to select the encryption algorithms for clients that also should be supported on a wide range of devices. For example, smart phones and tablets can use the L2TP/IPsec connection type and for the PPPoE connection type; they are not. This allows better compatibility than PPPoE.

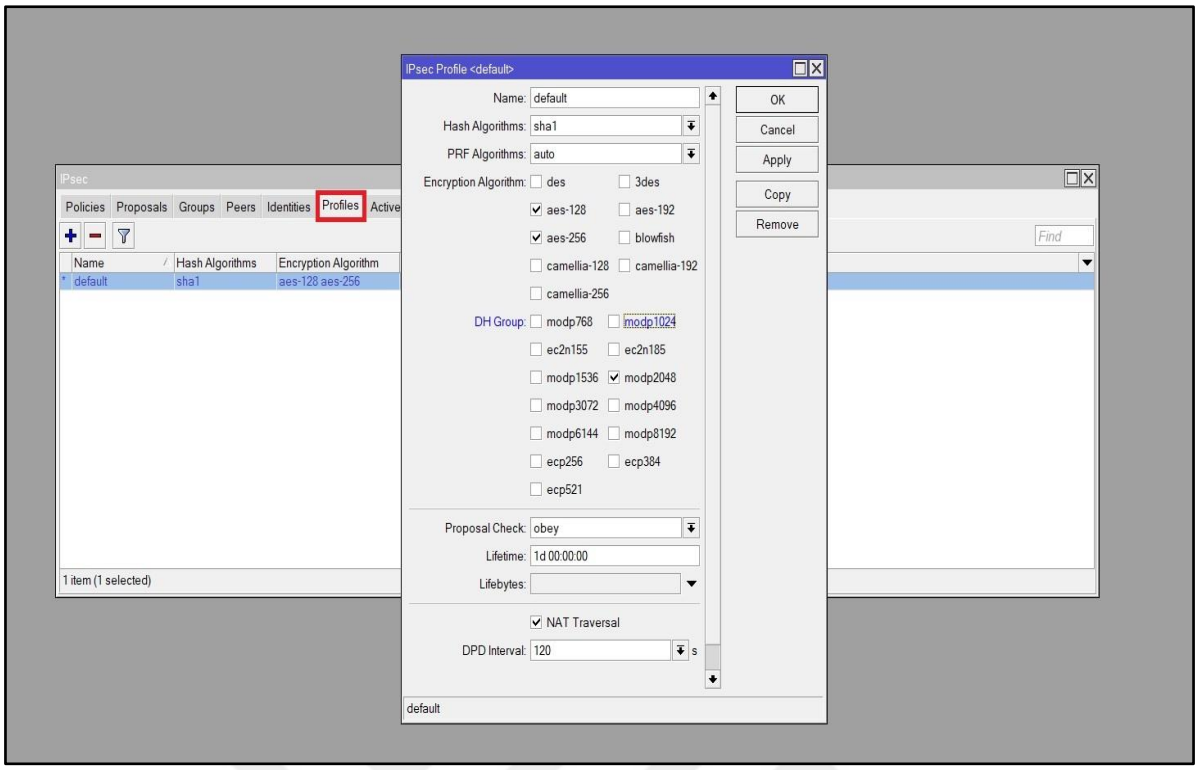

Figure 2.29: L2TP IP pool address range

At this step, the IPsec protocol has successfully been set. Next step should consider adding an IP address range for the L2TP/IPsec connection. As explained earlier using the same way we created an IP pool for the PPPoE server, we will create one but with a different IP address range. In other words, the PPPoE address range differs than the L2TP range. There is no problem to use the PPPoE pool address range for the L2TP or vice-versa, but in our state we prefer to add a different IP pool address range for the L2TP. The L2TP address range will start from (100.100.100.100) up to (100.100.100.30) which indicates (30) connected clients at max. We can make it longer range but our test will only include 30 clients in this paper. It is preferable to mention that the address or IPs we used in this paper do not belong to ISP. They are set by the administrator.

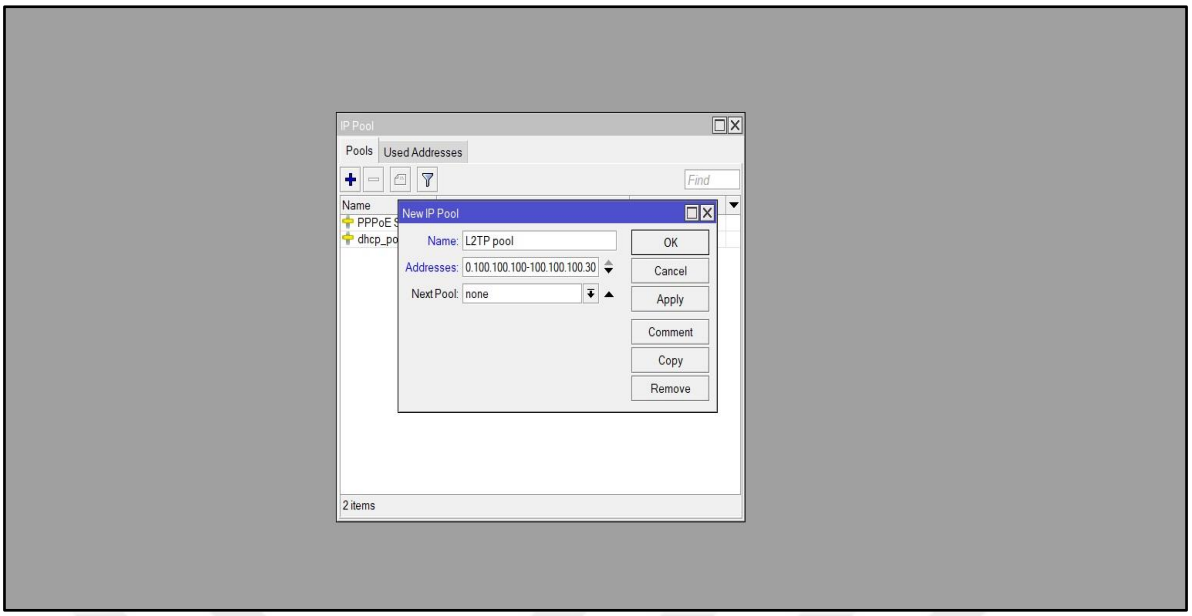

Figure 2.30: L2TP IP pool address range

After the pool address range, we need to create a PPP L2TP profile configuration for our clients. This will be done throughout "PPP" menu, "Profiles" and the sign plus. Our L2TP profile configurations look like the figure below:

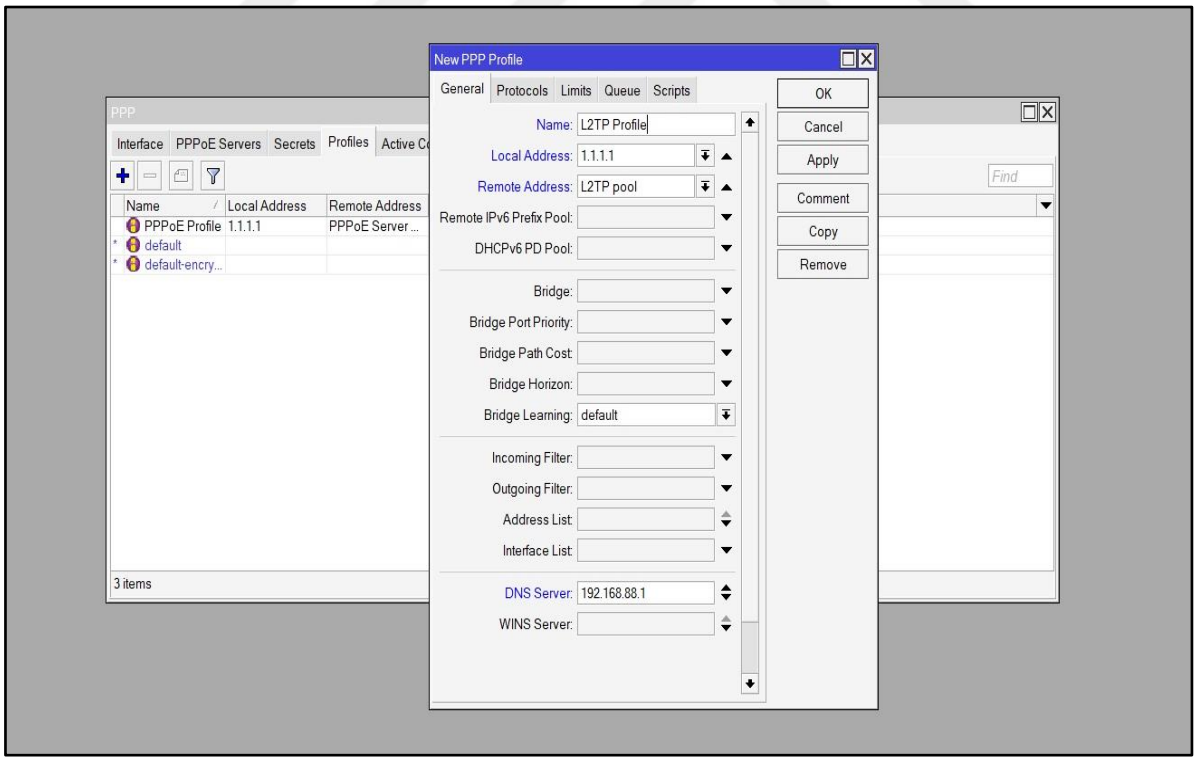

Figure 2.31: L2TP profile general configurations

The general profile tab allows the network administrator to set the profile name which we have set it as "L2TP Profile", local address will be the gateway for all the clients and we have set it

as “1.1.1.1” IP address. It must be taken into consideration that some ISPs requires the network administrator to use a specific IP address set the ISP. But in our test, the ISP we cooperated with in the test gave us the permission to choose any according to the network administrator’s choice.

In the same tab like the figure above, the “Remote Address” will be the L2TP pool address range that we created earlier. It also can be manually set to an IP address but since we have (30) clients, we prefer to use an IP address range. The “DNS Server” usually be the same as the router’s gateway. It can also be modified and an administrator should take into consideration that some ISPs prohibit altering the DNS IPs. As mentioned earlier, the ISP in our test gave us the full permission to use any settings we would like to. There are some settings we have left as default in the general profile tab like the bridge, port priority, path cost, bridge horizon, incoming and outgoing filter, address and interface list. In real-world the network administrator might configure these settings for different scenarios. For example, using the bridge horizon to split PPP ports, applying filters related to data processing before and after the connections.

These configurations can of course be used to enhance the network security and connectivity. But in large enterprise and complex ISPs can be set for different purpose. ISPs might also use more than one PPP profile. For example, three profiles for L2TP and two profiles for PPPoE and each profile has different settings.

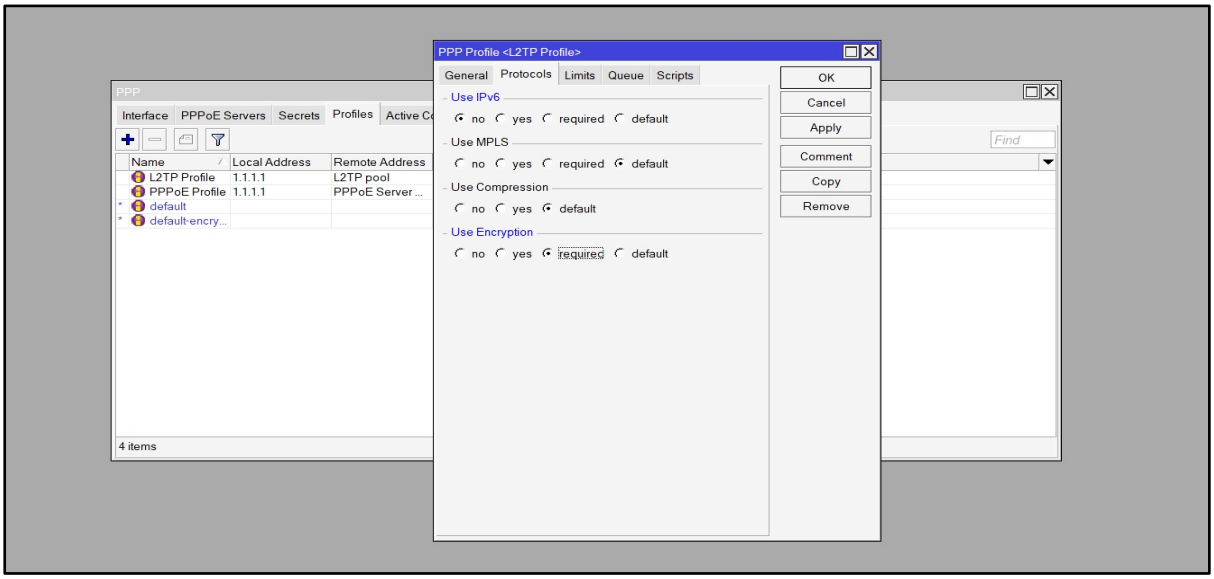

Figure 2.32: L2TP Profile protocols configurations

Another important PPP profile configuration that we must not neglect is the protocols from the PPP profile "Protocols" tab. The figure (31) above shows whether to clients to use IPv6 – which in our state do not have Internet access with, MPLS, compression whether to use data compression by the router device, and the most important option is the "Use Encryption." Here, the default encryption value is set to "yes." This looks like whether the client to use the encryption or not. But since we extremely need this option to encrypt data and authentication, we simply change the default value to "required." When the Encryption value set to required, this will force the router to accept only encrypted clients' connections and terminates all L2TP connection that configured not to use the encryption. This will upgrade the connections' security.

On the profile "Limits" tab, we can set the (tx/rx) client speed, and mostly used option is "Only One" set to "yes" rather than "default." This will allow each client to connection for one session. For example, the first client has only one session with his own credentials as in addition to the rest of clients. The network admnistrator must take into consideration this option because it might be left in configuration. If it is, this will result clients can connect into multiple sessions. For example, "client1" can connect to the L2TP server with two sessions using the same credentials; one session from the PC and the other session from the smart phone. It also might be more than two sessions as long as the client has devices able to connect and access the Internet. This will consume more of the router power and bandwidth for the network administrator.

If we suppose each of the 30 clients has at least two devices can use the L2TP connection, they will be as (60) connections. The router will deal with those (60) connections as (60) connected clients. The bandwidth cost will be higher and the router power of course will be degraded because the L2TP uses encryption. If they become three devices for each, 90 connections will be. This is something we need to avoid when configuring a PPP profile. It also can be happen even for the PPPoE since they are a part of the PPP protocol.

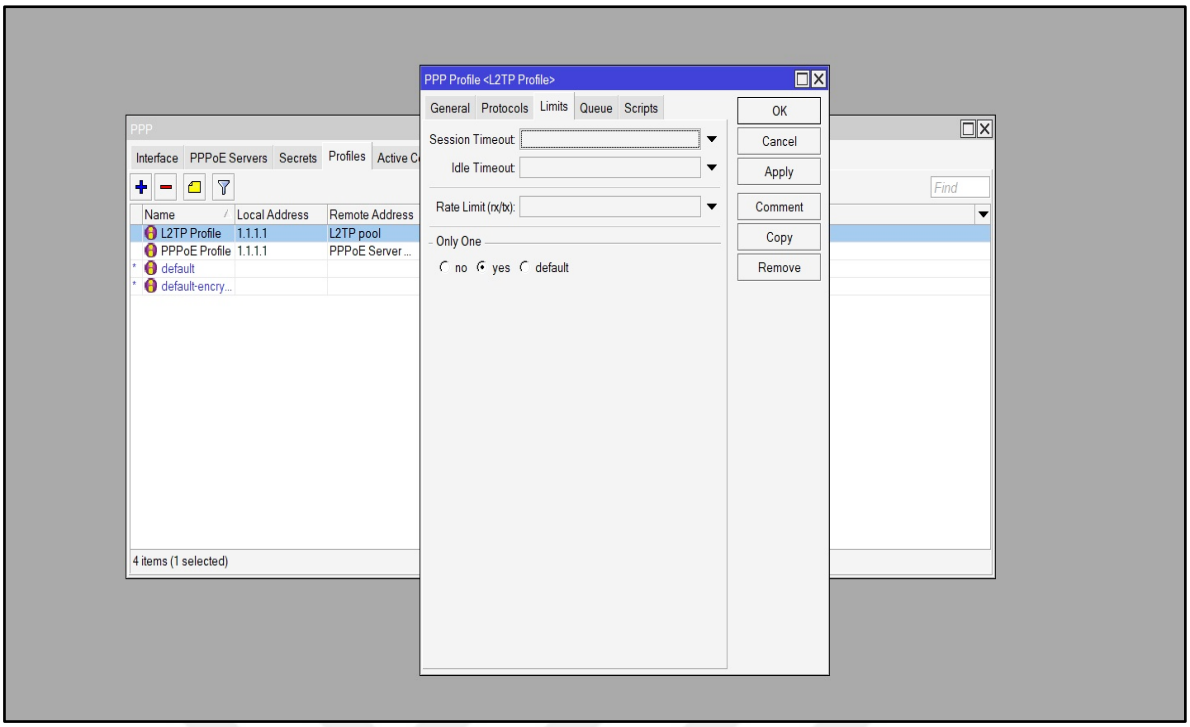

Figure 2.33: PPP profile Limits tab

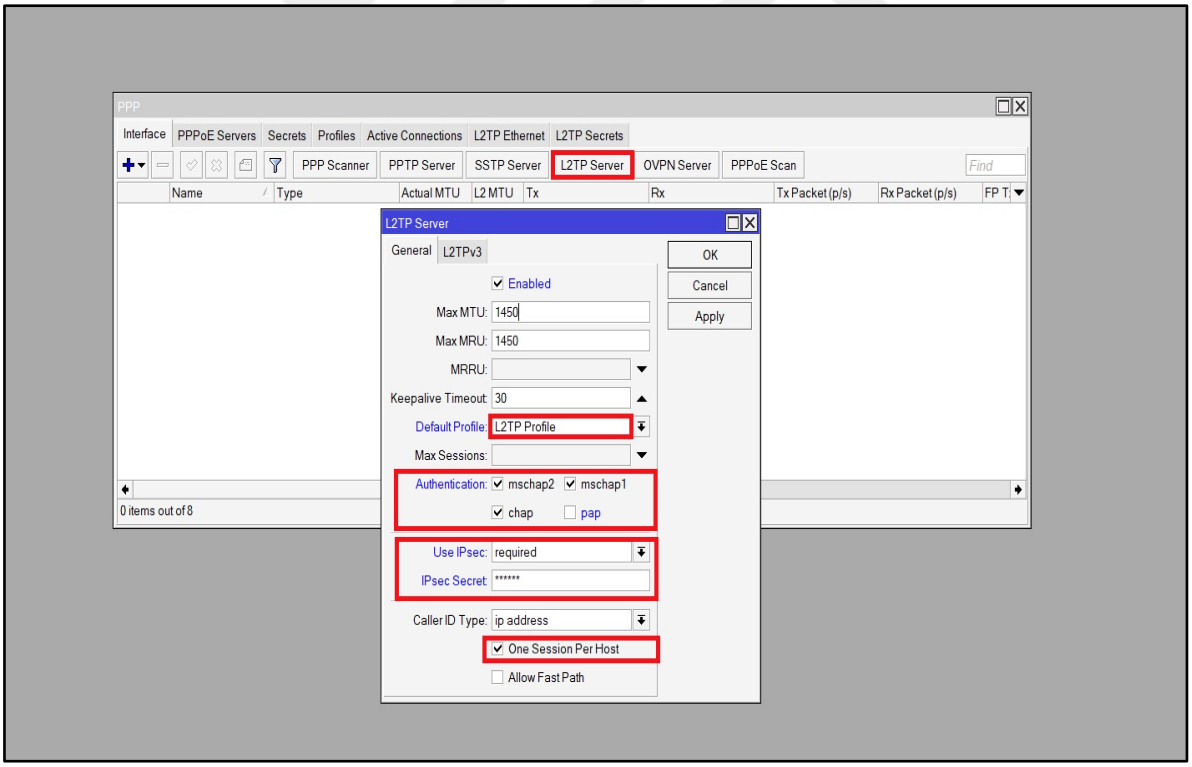

Figure 2.34: Enabling L2TP/IPsec server on MikroTik router

As shown in the figure above, the L2TP server must firstly be enabled by the network administrator inside the MikroTik device because it is not enabled by default. So, through "PPP" menu, "Interface" then "L2TP Server" and the window will pop-up like in the figure

above. In our state, we left the default “Max MTU”, “Max MRU” and “Caller ID Type” options. It is suggested not to alter the default MTU and MRU values unless they are necessary for an ISP. For example, an ISP might use different values according to the environment or other needs. If they are randomly increased or deceased, they might result in connections’ issues like data traffic or very slow connections. So, the administrator should really know about these two options. The important values we have changed are “Default Profile” and we specified the L2TP profile that we have created earlier to be the default profile for L2TP connections, “Authentication” protocols and we have disabled PAP protocol option because it will no longer be used since we forced the L2TP profile to require encryption. This step enhances the security alongside all devices can connect even without PAP enabled; unlike in the PPPoE state some devices unable to connect without PAP enabled. This is an additional security layer for the L2TP.

We have also set the “Use IPsec” option to “required” value. This will let the router only to accept encrypted clients’ connections. If a client connection settings set not to use encryption for the L2TP, the MikroTik device will immediately terminate this connection at its initial contact. The “IPsec Secret” is a type of secure password that corresponds to clients L2TP connections as in addition it has a relationship with IPsec policy and proposals we have setup earlier. This secret password must be the exact value in devices in order the connection being established. When we click apply and OK, the L2TP server is ready to accept clients’ connections. However, we just need to modify our PPP secret options (our 30 client) to use L2TP rather than the PPPoE connection. This will be done through “PPP”, “Secrets”, then double click to modify each client to use L2TP service and PPP profile as in the figure below.

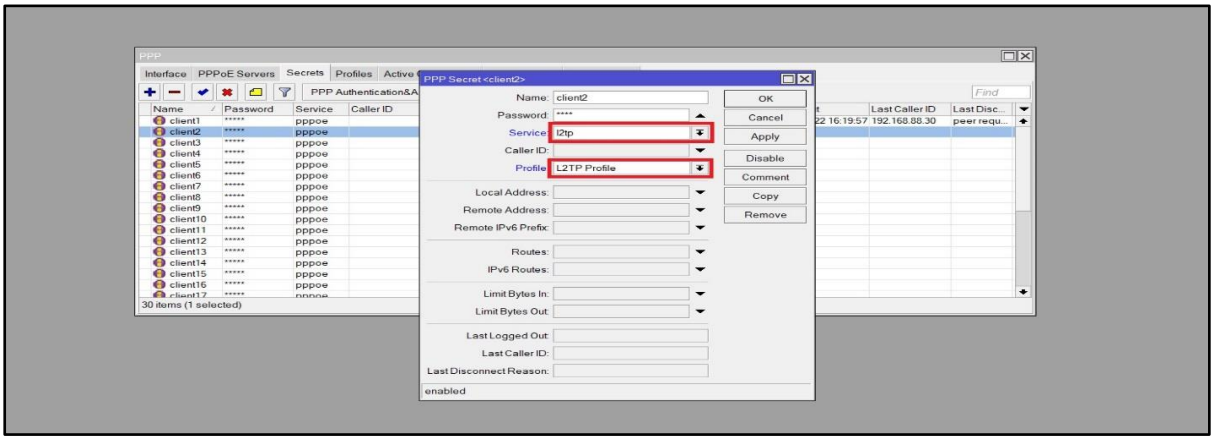

Figure 2.35: Changing secrets PPP profile and service type

This step will be the same for each of our (30) clients and we need to configure the masquerade NAT for the L2TP pool range in the MikroTik router firewall NAT option. They will use L2TP connection rather than PPPoE and their default PPP profile will be the “L2TP Profile” that we already have created before. This will result that all the (30) clienst can connect to the MikroTik L2TP enabled server. Now let’s connect one of our clients mobile device by using the L2TP/IPsec connection type. Depending on the mobile device vendor in our state; we firstly connect to the MikroTik router through Wi-Fi in order the client gets an IP address from the MikroTik DHCP Server (no Internet access) through the DHCP server because the DHCP server used only to assign clients dynamic IP address as discussed earlier. After the our clients gets connected through Wi-Fi, we go through phone’s settings, connections, more connection settings, VPN, then we add a VPN profile. Like in the collage figure below.

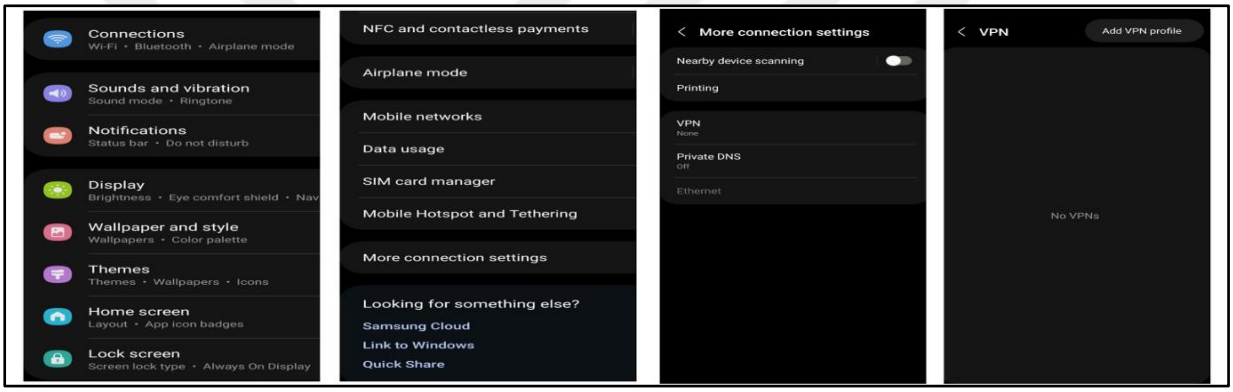

Figure 2.36: A client L2TP setup to connect to the router

Figure 2.37: Clients are able to connect to the MikroTik L2TP server

The L2TP/IPsec configuration might be different on other devices. For example an L2TP/IPsec connection throught a PC differs from a smart phone’s or tablet’s. Let’s connect a PC to the MikroTik L2TP server and see if the connection succeeds or gets terminated.

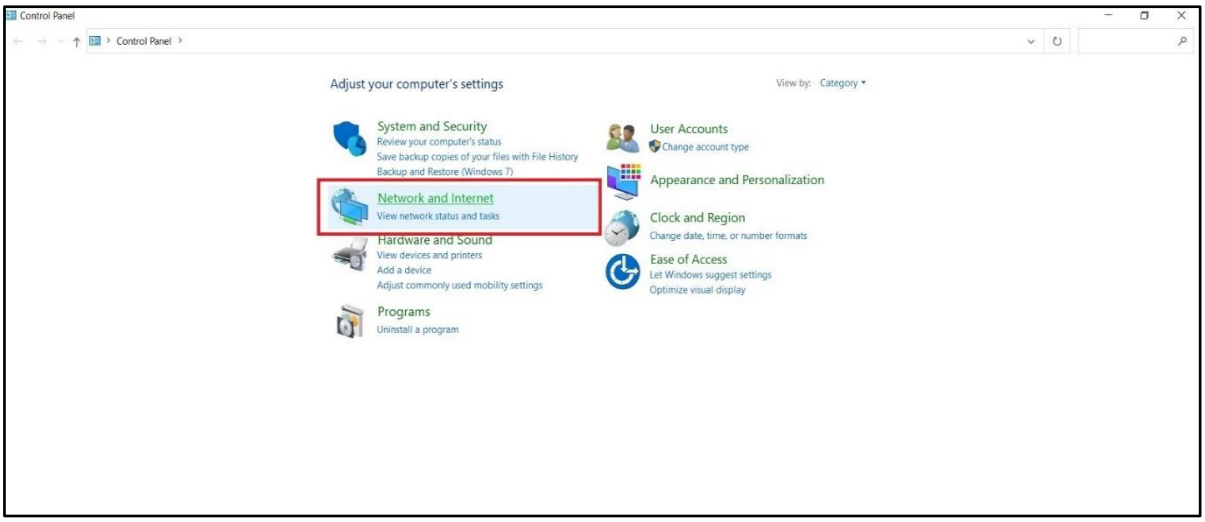

Figure 2.38: Access Network and Internet through Control Panel

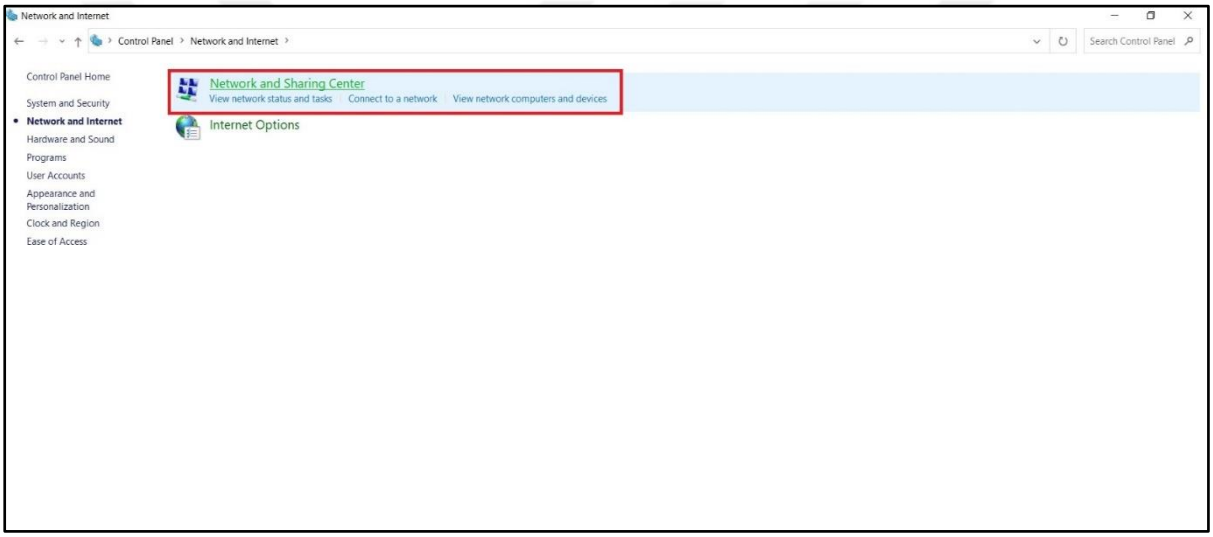

Figure 2.39: Access Network and Sharing Center

Figure 2.40: Setup a new connection or network

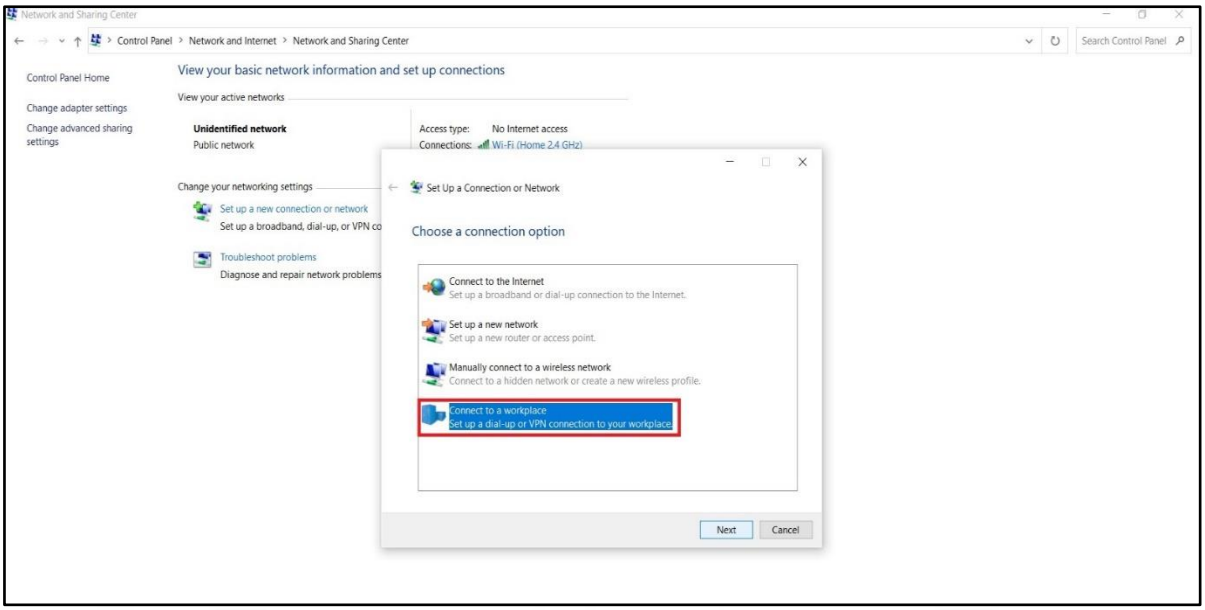

Figure 2.41: Follow the on-screen instructions to setup the L2TP connection

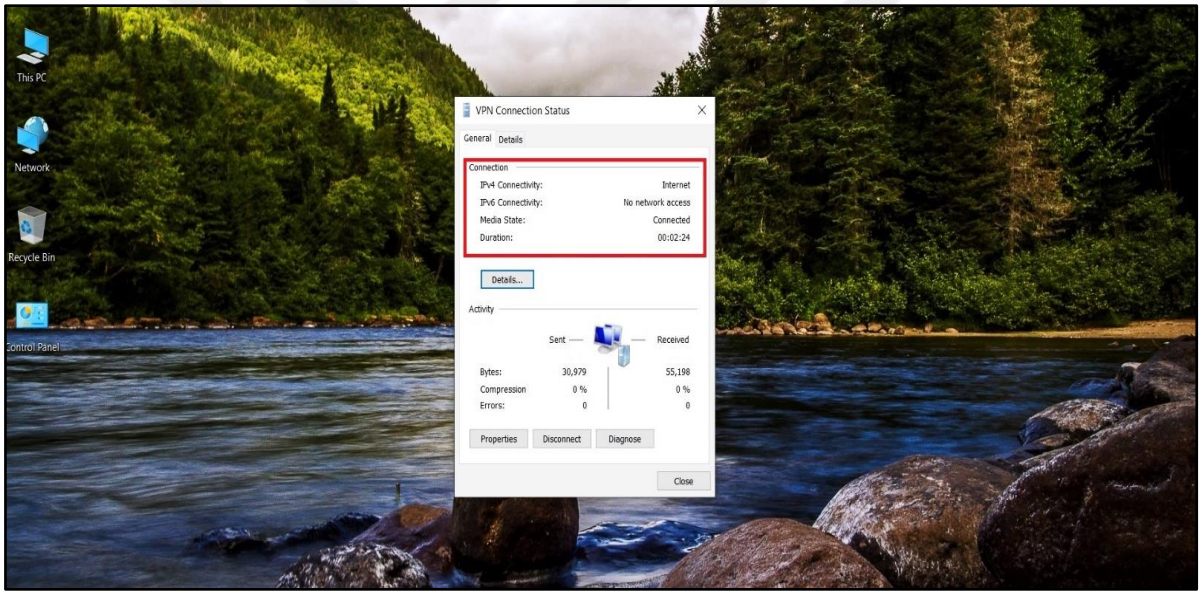

Figure 2.42: The PC has successfully connected to the MikroTik L2TP server

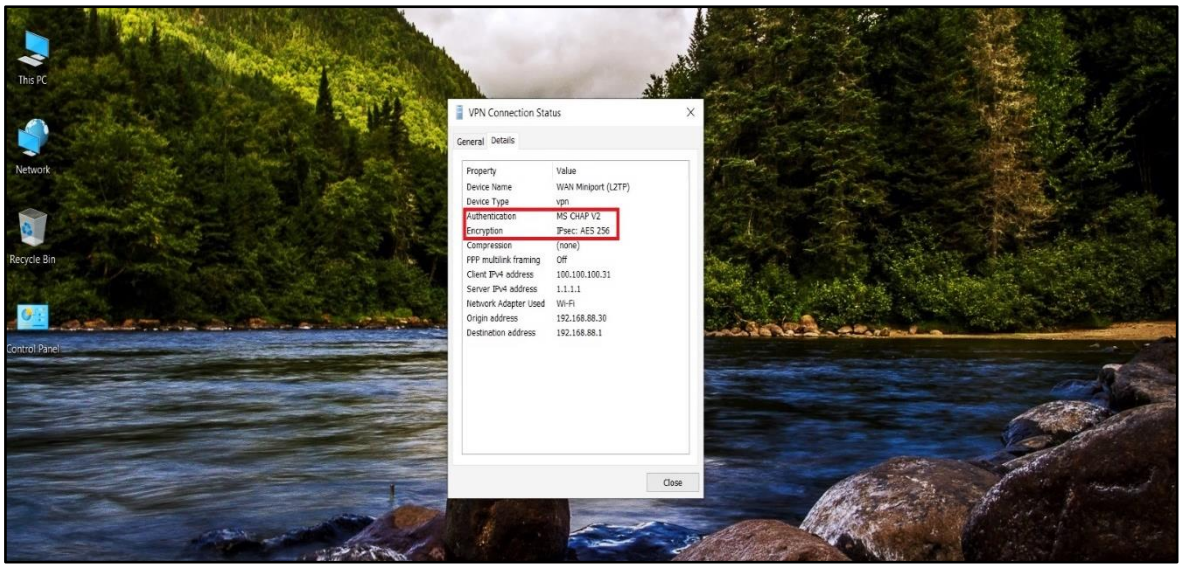

Figure 2.43: The client L2TP connection is encrypted with AES 256-bit key

As the client PC gets connected to the MikroTik L2TP server, the connection will be encrypted by AES 256-bit encryption key. This ensures that all data traffic is encrypted which improves the security. Let's verify the connection is encrypted throughout the MikroTik L2TP server and IPsec configurations. However, to the verify the encrypted connection we need to go to the "IP" menu, "IPsec", then "Installed SAs." These are the encyption keys that dynamically changed alongside the connection is still established. This will make the data encryption is impossible to be cracked or decrypted.

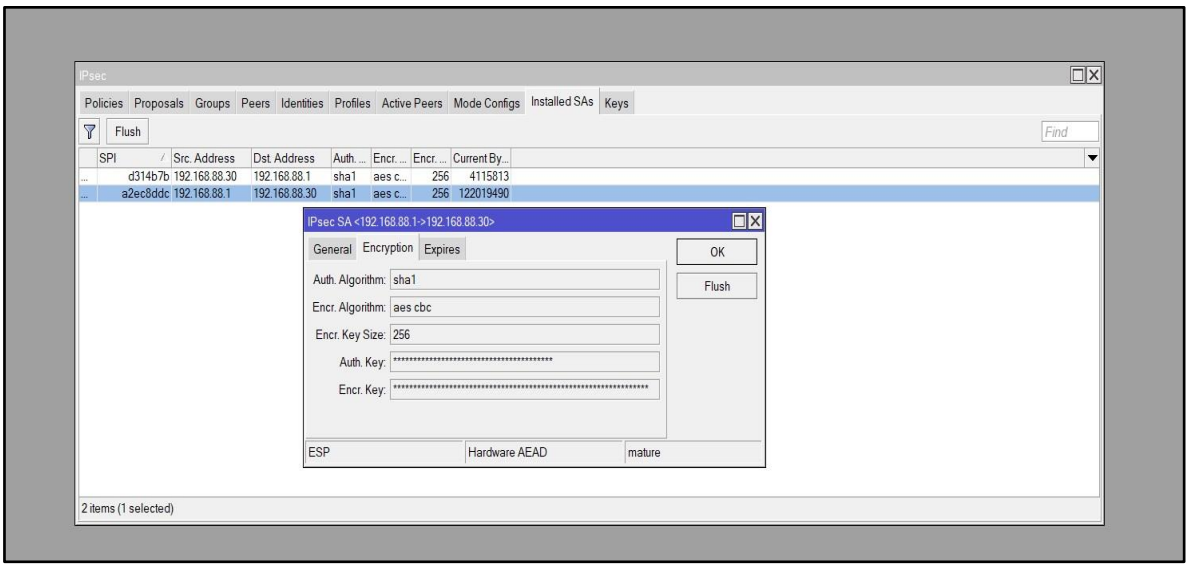

Figure 2.44: Client L2TP connection is encrypted

If we look at the figure (43) above, there is "Auth. Key" and "Encr. Key" and both of them are encrypted in the realtime of the connection. Now, let's back to the "Wireshark" capturing tool

from the network administrator's PC and see the data captured when a client connects through the L2TP/IPsec connection.

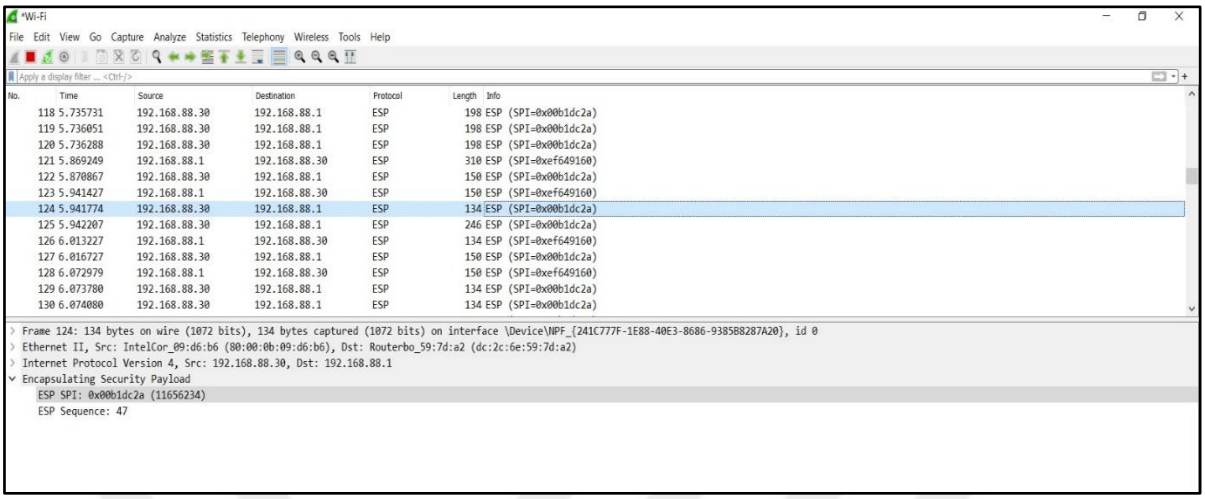

Figure 2.45: Data captured by Wireshark when clients connect through L2TP server

As shown above, all data uses the ESP (Encapsulating Security Payload) which is a protocol used in the IPsec to securely exchange users' data and information without being interupted or captured in a plain text format. This result in stronger security and even the network administartor can not intercept the data.

However, it is the time now to get all our (30) clients get connected to the MikroTik L2TP/IPsec server to test the router power and see things that will happen inside the router. Accordingly, in this step we will stress the router power and do some heavy-duty load on it. This procedure will be on two phases. In the first phase all the (30) clients will connect through their PCs and we will conclude some results. The second phase will involve doubling the clients up to (60) devices (PCs, smart phones and tablets) and make a comparison between the two phases.

2.6 CONNECTING A SAMPLE OF (30) DEVICES TO THE L2TP/IPSEC SERVER

In this phase, the 30 clients will use their own PCs to access the MikroTik L2TP server that we have just created. Each client will use one session at time. Each client has sets-up the L2TP/IPsec configuration on his/her device and the network administrator has given each client his/her credentials to connect.

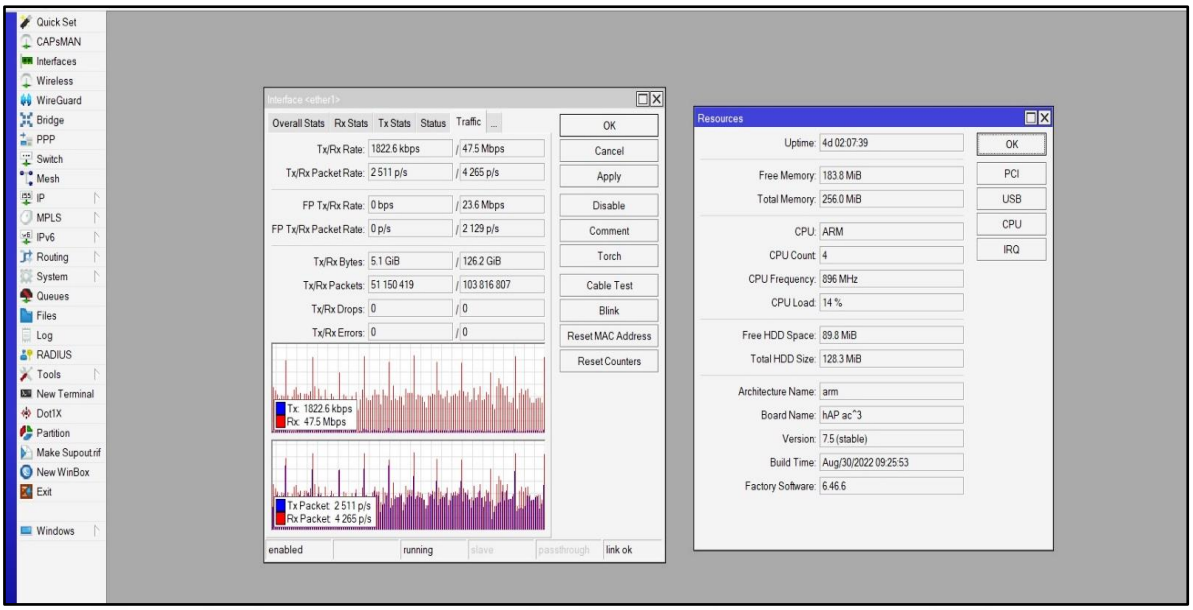

Figure 2.46: MikroTik router state with 30 connected L2TP clients at heavy-load

Figure (45) above shows that the MikroTik router up time is four days and two hours. The dialogue box on the right side shows the interface "ether1" traffic which it is the WAN interface for outer world. On the left side dialogue box, the router CPU frequency shows a clock speed of (896 MHz), (14%) load and (183.8 MB) of the router's available RAM. In comparison, the (14%) CPU load is at the state where all the 30 clients are connected and active. In addition, the figure above shows that the MikroTik router we are currently using is processing nearly up to (50 Mbps) – and it is the max speed allowed for us from the ISP. For this phase, in short; the (14%) CPU load is not something big for a router is processing 30 active L2TP connections. This CPU percentage is less than the average. As a result, the router is able to handle all the 30 L2TP encrypted connections without data-drop nor a single L2TP connection to be terminated by the server itself.

2.7 DOUBLING THE SAMPLE OF CONNECTED DEVICES UP TO (60)

In this stage, we have rebooted the MikroTik router device . New (30) clinets joined in addition to the previous (30) clients. So, the total clients number become (60). They will all connect in the same time. Furthermore, we have not increased the ISP max Internet speed that given for us to get better and accurate results as possible by limiting the Internet speed. This test is not based on speed increase and decrease, but instead, it depends on how the router will deal with bigger number of connected clients active and encrypted connections. L2TP is an encrypted connection that consumes a lot of CPU power for encryption and data-processing since all the

L2TP/IPsec data exchanged (transferred) in a secure tunnel or path. So, we need to test the router's ability not the throughput (upload and download) speed.

However, the figure (46) below shows the results during the 60 connected clients through the peak time and all the 60 clients connected to the MikroTik router.

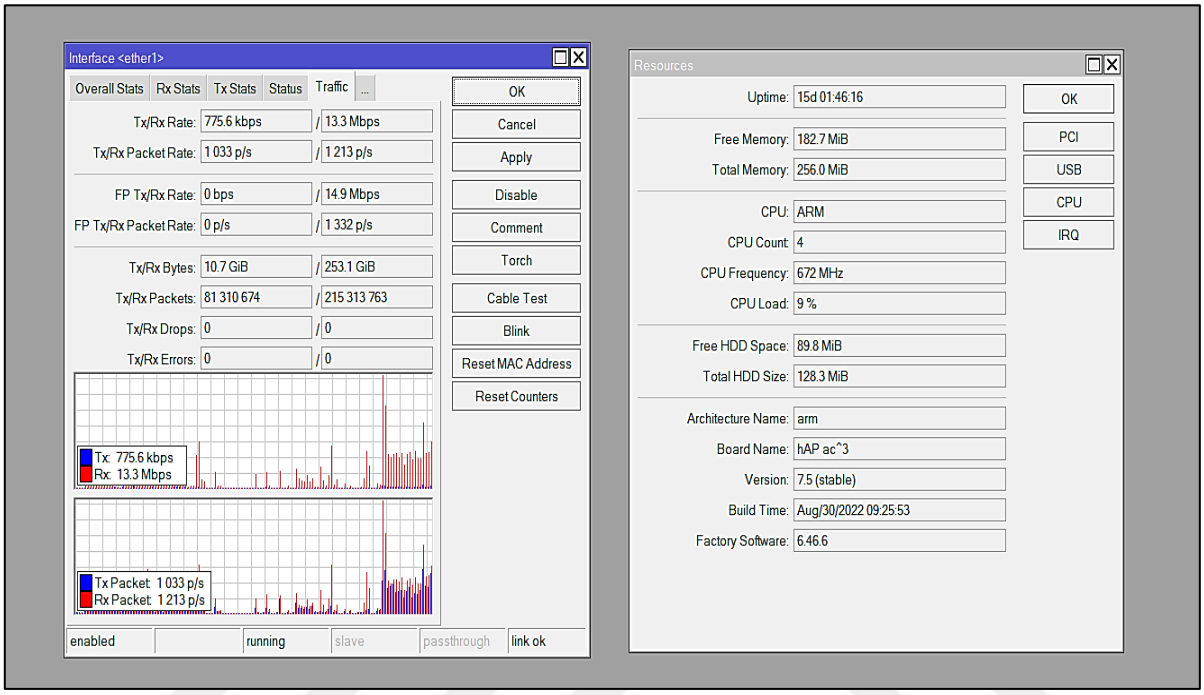

Figure 2.47: Router resources with in all 60 clients connected

If we take a look at the figure above, the router uptime is lasts for fifteen days, though all the (60) L2TP sessions connected, the CPU frequency (clock speed) runs at 672 MHz which can be "boosted up to 896 MHz" according to its manufacturer dynamic scaling frequency product brief (Qualcomm, 2015). The great surprise is in the CPU load. It is only (9%). The four cores has a great impact as in addition to the chip's archeticture ARM which it is a very modern architecture chip (Elahi, 2022). Free memory is another great deal. In the state of (30) connected L2TP/IPsec connection, the free memory was (183.8) Megabytes while in the state of (60), it is (182.7) Megabytes. It seems that the device memory is not impact in the two states; even there is data being processed at speed of (13.3) Mbps at the time of the figure (46) above captured.

Since the number of the (30) clients doubled to (60) to make a heavier load on the 'hap ac^3', the device resources likely have not been afected – (limited to this testing environment and conditions). Accordingly, no data drop (Tx/Rx) drops nor (Tx/Rx) errors have been occurred. The 'hap ac3' device successfully dealt with the obsolete issue of "encryption and decryption

process with IPsec policy when using the AES algorithn for authentication and encryption that consumes power and higher resources." (Doraswamy & Harkins, 2003). The hardware acceleration feature that is supported by the 'IPQ-4019' chip likely contributed in dealing with these such things: (60) connected L2TP/IPsec sessions, (9%) CPU load, no data processing errors due to the encryption/decryption occurred during the tests. To examine if the hardware acceleration feature solves the issues with IPsec and L2TP sessions, we will examine and re-test the same procedure but this time; with an older MikroTik device that has an older CPU chip which does not support the hardware acceleration feature or technique In addition, the older device CPU chip is with different archietecture.

2.8 UTILIZING AN OLDER DEVICE FOR COMPARISION

The older MikroTik router selected is the 'RB2011UiAS-2HnD' which it is powered by Atheros 'AR9344' CPU chip, MIPSBE acrheticture, one CPU core, and 128 Megabytes of (RAM). Also, it can be purchased from MikroTik local distributor or the MikroTik products website. However, in order to get accurate results as much as possible, we have upgraded the RouterOS version to the latest one (v7.6) – at the time of writing, made the same configuration of IPsec policy and encryption on the 'hap ac3', as in addition we used the same number of clients (30) and (60).

At the very beginning of connecting (30) L2TP/IPsec VPN sessions to the router, and more particularly, we have noticed that the CPU usage is at (44%) in the state only (20) clients connected. When the clients are all connected (30) to the router, higher CPU usage observed. It was (55%). The final stage involved doubling the (30) clients up to (60) to connect. When they all connected, the CPU usage was (80%). The (80%) CPU load was higher than expected. Beause the router was at the idel state where less data being processed. When heavy data being processed, the CPU usage nearly between (85% - 95%) of load! At this level; data being dropped, packet loss likely exisited, (Tx/Rx) errors occurred, and a number of the (60) clients were unexpectedly disconnected and forced to be deauthenticated by the router itself.

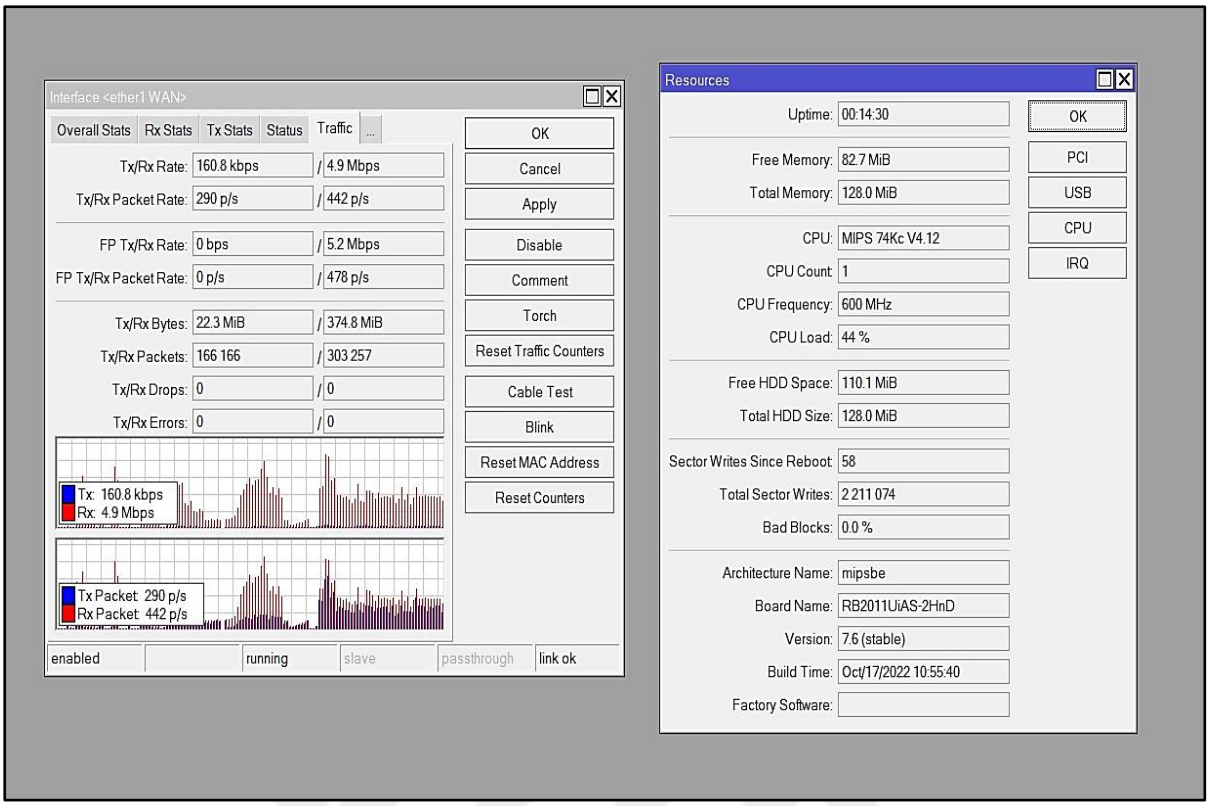

Figure 2.48: Resource usage without IPsec hardware acceleration

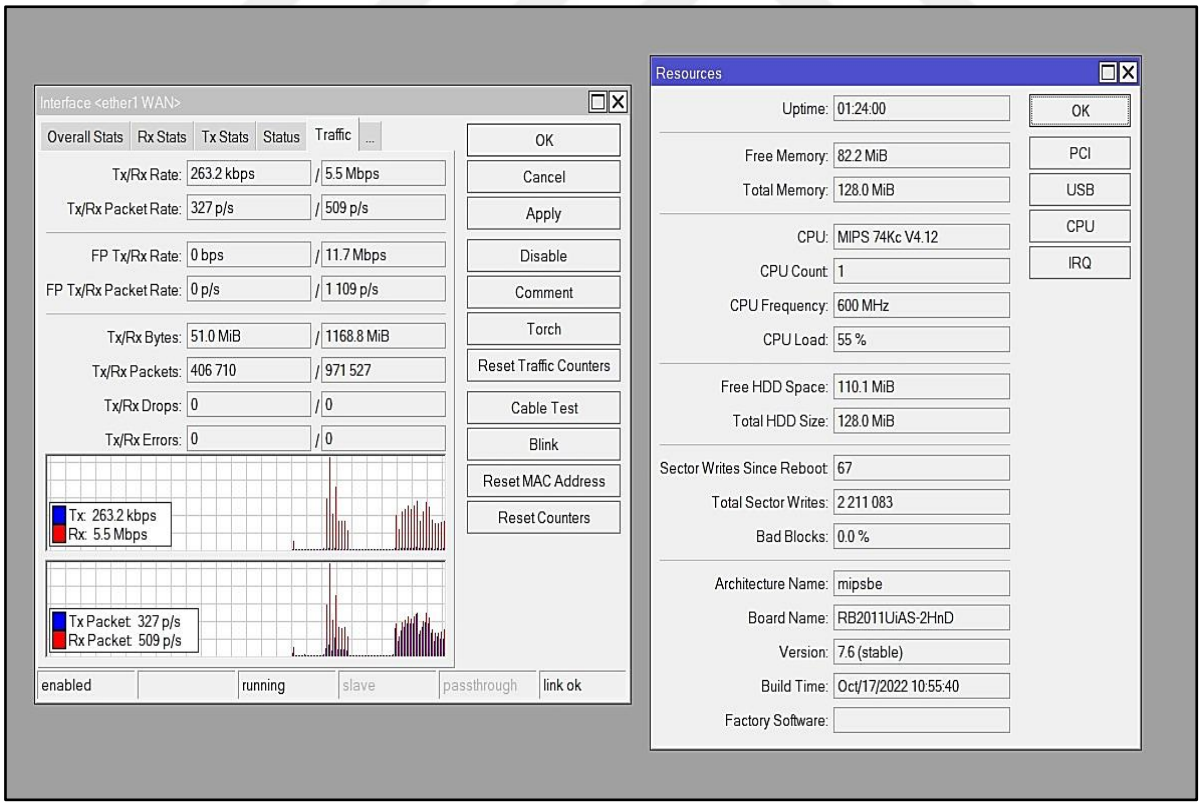

Figure 2.49: Normal load resources usage

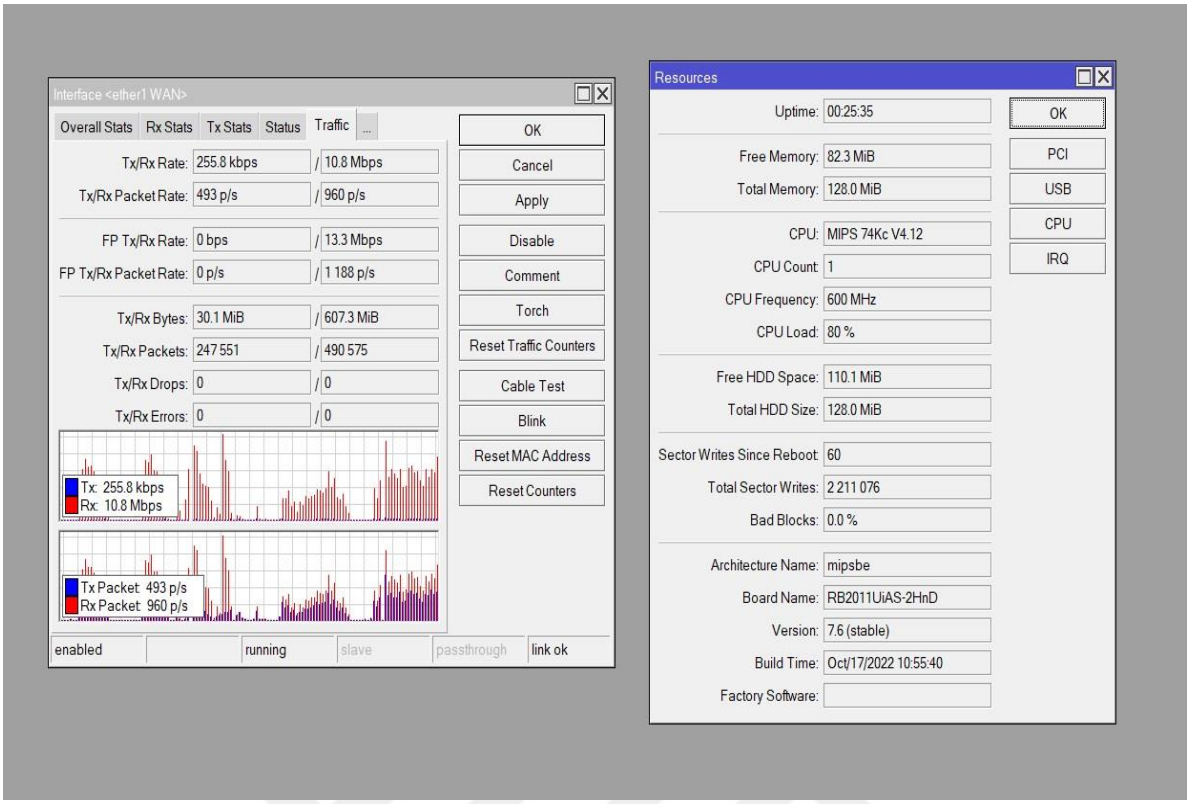

Figure 2.50: Heavy-duty data processing and load without IPsec hardware acceleration

However, there is a great difference between the two routers. Despite they are from the same manufacturer and use the same RouterOS operating system; the difference of the CPU usage is huge. The causes of these differences depend on: router's chip achitecture, the number of chip cores, and the hardware acceleration feature whether supported or not inside the chip itself. So, let's summarize our testing procedures:

3. CONCLUSION AND FUTURE RECOMMENDATIONS

3.1 CONCLUSION

The hardware acceleration technique or feature implemented in modern integrated chips resulted in faster processing operations for the IPsec encryption, decryption and authentication processes. Since the IPsec uses a security policy, this policy forces the Advanced Encryption Standard (AES) for data encryption and decryption. Any encryption or decryption process, is of course, consumes more of the chips' power and energy; depending on the type of data, encryption keys length (usually in bits) such as the (AES) 256-bit encryption key, and file size. Larger data estimate larger time and consume more power in order the process to be completed [50]. In networking, IPsec sessions, every time the number of increases; processes take longer time, then the entire network performance is likely degraded. Newer IPsec sessions might fail to authenticate or connected. The hardware acceleration facilitates the IPsec processing by giving the process a priority higher than normal operations. By comparing the devices; the older device consumes nearly (55%) of its CPU usage when only (30) L2TP/IPsec connection established. By doubling the number to (60), CPU usage is nearly at full (80 – 95%). As a result, newer or even connected sessions got terminated (by force) because the 'AR9344' Atheros chip performance has greatly decreased due to encryption and decryption. The older 'AR9344' is not optimized for IPsec, has single core clocked at 600 MHz whereas the newer one 'IPQ-4019', consists of four cores; clocked at 716 MHz for each. In addition, it supports the IPsec hardware acceleration. The newer device was able to process all the (60) clients' L2TP/IPsec sessions without consuming more than (32%) of its CPU usage. None of the newer connections nor the existed ones faced issues, delay or termination as long as connections are still active. There is a great difference between (80%) usage and no more than (32%) during the IPsec encryption and decryption. The technique has successfully eliminated the older issues related to data encryption and decryption. It is a promising feature that should be utilized by newly created network devices.

3.2 FUTURE RECOMMENDATIONS

This paper recommends IT-industries should develop its devices by offering the ability to use L2TP/IPsec connections instead of just through older means, such as by static, dynamic IPs, and PPPoE. Despite some devices are newer, the hardware acceleration feature is not supported especially in-home devices. Moreover, networking or IoT home devices usually made with less costs by companies to get more income without offering new features. As usual, most home devices (routers or access points) released and be available for purchase by only newer chip implied. Regardless, it might be the same older chip used but with a very rare customizations that have limited features, too.

Because of limited features for home network devices, these devices lack the ability to process encryption and decryption processes in real-time; resulting in timeouts and interruptions. This resulted that L2TP/IPsec connections only available and used in business because the business' devices are, of course, has advanced features and capable of dealing with multiple processes at time. IPsec policies also allow authentication, encryption and decryption by forcing the use of SSL/TLS certificates – which are still one of the most secure mechanisms of data protection.

REFERENCES

[1] Al, C. Ü. (2022). Embedded System Design with Arm Cortex-M Microcontrollers - Applications with C, C++. Springer.

[2] Ashutosh, M. J. (2023). Artificial Intelligence and Hardware Accelerators. Springer.

[3] Biryukov, A. (2007). Fast Software Encryption: 14th International Workshop. Springer.

[4] Black, U. (1999). PPP and L2TP: Remote Access Communications. Prentice Hall.

[5] Blokdyk, G. (2022). Advanced Encryption Standard Standard Requirements. 5 Star Cooks.

[6] Carlson, J. D. (2002). PPP Design, Implementation, and Debugging. Addison-Wesley Professional.

[7] Daemen, J. &. (2020). The Design of Rijndael: The Advanced Encryption Standard (AES). Berlin: Springer.

[8] Davis, C. (2001). IPSec: Securing VPNs. McGraw-Hill Osborne Media.

[9] DAYONG, L. (2021). Full Explanation of Central Processing Unit. WENYUE Publisher, Inc.

[10] Doraswamy, N. &. (2003). IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Upper Saddle River: Prentice Hall.

[11] Dudley, M. H. (2018). Death and Accident Investigation Protocols. CRC Press.

[12] Edwards, M. &. (1996). A practical hardware architecture to support software acceleration. Microprocessors and Microsystems, 20(3), pp. 167-174.

[13] Elahi, A. (2022). Computer Systems: Digital Design, Fundamentals of Computer Architecture and ARM Assembly Language (2nd Edition ed.). New Haven: Springer.

[14] Ernst, M. H. (2004). FPGA based hardware acceleration for elliptic curve public key. The Journal of Systems and Software, 70(3), 299-313.

[15] Fahmy, S. A.-S. (2007). Real-time hardware acceleration of the trace transform. J Real-Time Image Proc, 4(2), 235-248.

[16] Frankel, S. (2001). Demystifying the IPsec Puzzle. Artech-house.

[17] Graham, B. &. (2016). IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. Cisco Press.

[18] Guha, R. (2009). Embedded System Design: Algorithms Acceleration by a Reconfigurable Computing Platform of FPGAs. VDM Verlag.

[19] Gulati, K., & Khatri, S. P. (2010). Hardware Acceleration of EDA Algorithms: Custom ICs, FPGAs and GPUs. Coppell: Springer.

[20] Haddad, M. (2021). Multicast on MikroTik with LABS: Master Multicast on RouterOS using step-by-step LABS. Maher Haddad Publishing.

[21] Hao, L. S.-t.-q.-w. (2006). Design and implementation of an IPSec VPN education experiment system. Computer Applications and Software, 23(7), 3-4.

[22] Hart, T. (2017). MikroTik Security Guide. Independently published.

[23] Hart, T. (2017). Networking with MikroTik: MTCNA Study Guide. Manito Networks.

[24] Henry, J. C. (2010). IPsec virtual private network fundamentals: An introduction to VPNs (4th Edition ed.). Indianapolis: Cisco Press.

[25] Hoxha, D. (2017). Managing Internet Connections with PPPoE, Mikrotik and Radius. AP Lambert Academic Publishing.

[26] Huawei. (n.d.). S600-E V200R010C00 Configuration Guide-IP Multicast. Retrieved July 8, 2022, from https://support.huawei.com/enterprise/en/doc/EDOC1000141881/4e3b3b7e/igmp-snooping-proxy

[27] Hunter, L. E. (2005). Firewall Policies And VPN Configurations. Apress.

[28] Ihrig, C. J. (2008). Improving Performance and Reducing Power with Hardware Acceleration: Static Timing Analysis Based Transformations of Combinational Logic in a High Level ASIC Synthesis Flow. VDM Verlag Dr. Müller.

[29] Jay, B. &. (2007). Wireshark & Ethereal Network Protocol Analyzer Toolkit: Jay Beale's Open Source Security. Open Source Security.

[30] Jonathan, K. &. (2007). Introduction to Modern Cryptography: Principles and Protocols Chapman & Hall/CRC Cryptography and Network Security Series. Chapman and Hall/CRC.

[31] Liu, F. X. (2012). On the security of PPPoE network. Security and Communication Networks, 10(5), 1-10.

[32] Luciano, L. &. (2018). lectronic Design Automation for IC System Design, Verification, and Testing. CRC Press.

[33] Lukman, S. &. (2010). IPSec: A Practical Approach: Network Security. LAP Lambert Academic Publishing.

[34] M, F. V. (2020, December 3). Beagle Security. Retrieved July 12, 2022, from Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention: https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html

[35] Maxfield, C. (2006, August 9). Embeeded. Retrieved May 21, 2022, from FPGA Architectures from A to Z Part 2: https://web.archive.org/web/20071008163016/http://www.embedded.com/columns/showArticle.jhtml?articleID=192700615

[36] McMillan, T. (2015). Cisco Networking Essentials. Sybex.

[37] Michael H. Behringer, M. J. (2005). MPLS VPN Security. New York: Cisco Press.

[38] Networks, J. (2021, September 28). Juniper Networks. Retrieved May 7, 2022, from Configuring Point-to-Point Protocol over Ethernet: https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-config-pppoe.html

[39] Petzold, C. (2022). Code: The Hidden Language of Computer Hardware and Software. Microsoft Press.

[40] Pub, F. (2021). Announcing the ADVANCED ENCRYPTION STANDARD (AES): Federal Information Processing Standards Publication. USA: FIPS PUB. Retrieved from Announcing the ADVANCED ENCRYPTION STANDARD (AES).

[41] Robert, M. (2014, June 16). Microsoft Supercharges Bing Search With Programmable Chips. Retrieved April 13, 2022, from https://www.wired.com/2014/06/microsoft-fpga

[42] Shaheen, M. H. (2022). Hybrid Encryption Algorithms over Wireless Communication Channels. CRC Press.

[43] Sheila, F. K. (2005). Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology. Create Space Independent Publishing Platform.

[44] Shimobaba, T. &. (2019). Computer Holography: Acceleration Algorithms and Hardware Implementations. CRC Press.

[45] Shneyderman, Alex; Casati, Alessio Casati;. (2002). Mobile VPN: Delivering Advanced Services in Next Generation Wireless Systems. Wiley.

[46] Sisejkovic, D. &. (2022). Logic Locking: A Practical Approach to Secure Hardware. Springer.

[47] Snader, J. C. (2005). VPNs Illustrated: Tunnels, VPNs, and IPsec. Addison-Wesley Professional.

[48] Sun, A. (1999). Using and Managing PPP. O'Reilly.

[49] V., R. (2004). PC Hardware Tuning and Acceleration. Independently Published.

[50] Xiao, S. (2011). The Software in Hardware: FPGA Hardware Acceleration for High Performance Neutron Transport Simulation. LAP Lambert Academic Publishing.

[51] Zen, V. (2019). Theory, laboratories and exercises for Mikrotik RouterOS - Routing. Independently published.