T.C.

ALTINBAS UNIVERSITY
Institute of Graduate Studies
Electrical and Computer Engineering

DESIGN APPLICATION OF NETWORK MANAGEMENT BY USING API (APPLICATION PROGRAMMING INTERFACE)

Homam Eisam Almaz AL-JAAFAR

Master Thesis

Supervisor
Asst Prof. Dr. Abdullahi Abdu IBRAHIM

Istanbul, 2020

DESIGN APPLICATION OF NETWORK MANAGEMENT BY USING API (APPLICATION PROGRAMMING INTERFACE)

by

Homam Eisam Almaz AL-JAAFAR

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAS UNIVERSITY

2020

The thesis titled "DESIGN APPLICATION OF NETWORK MANAGEMENT BY USING API (APPLICATION PROGRAMMING INTERFACE)" prepared and presented by "Homam Eisam Almaz AL-JAAFAR"was accepted as a Master of Science Thesis in Electrical and Computer Engineering

Asst. Prof. Dr.Abdullahi Abdu IBRAHIM

Supervisor

Examining Committee Members (first name belongs to the chairperson of the jury and the second name belongs to supervisor)

Asst. Prof. Dr.Abdullahi Abdu IBRAHIM	School of Engireeng and Sciences, Altinbas University	
Asst. Prof. Muhammad Ilyas	School of Engireeng and Sciences, Altinbas University	
Asst. Prof. Izzet Paruğ Duru	Vocational School, Istanbul Gedik University	

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science

Approval Date of Institute of Graduate Studies:

30/10/2020

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.

Homam Eisam Almaz AL-JAAFAR

DEDICATION

This research study is dedicated to my father, Eisam Almaz, for my mother Iktifaa hameed, and in the memory of my brother, Harith Eisam.

ACKNOWLEDGEMENTS

First of all, I am thankful to God for the good health and well-being that has enabled me to complete this work. Secondly, I really would like to thank my family for their moral and material support. Finally, I would like to express my deep gratitude to my supervisor, Prof Dr. Abdullahi Abdu Ibrahim, colleagues, friends and others whom directly or indirectly support me in many ways for successful accomplishment of this thesis.

ABSTRACT

Design Application Of Network Management by using API (Application programming interface)

AL-JAAFAR, Homam Eisam

M. Sc., Electrical and Computer Engineering, Altinbas University

Supervisor: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Date : 30/10/2020

Pages: 44

Our daily lives depend heavily on devices, services and applications connected to the Internet. This reliance makes it more important than ever that the primary networks on which they depend are reliable, efficient and secure. At the same time, the increasing sophistication and diversity of devices, existing services and applications have made network management tasks more complex than ever before. Modern network management assumes that agents, general distributors of Internet networks can develop networks management by billing system in terms of many aspects and benefits on a regular basis, and use this information to take preventive or corrective actions in real time (control of network). Traditional approaches to network management In creating, configuring internet packages and distributing them its sometimes manual, slow need time, effort and negativity that are not appropriate for the desired performance measurements or applications. The contribution of this research is to design an application we have been call MaxBox, where it creates and configures internet networks and packets with the lowest possible time and less complicated, over three protocols Hotspot, broadband and User manager Through the application programming interface API, which in turn is a point of contact between a specific development environment and developers without the need to build everything from scratch. The purpose of the API is to hide the programming and method of write codes, such as command line interface CLI, then by the API is control the mikrotik.

Keywords: Network Management, Billing System, API, Broadband, Hotspot, User Manager

TABLE OF CONTENTS

Pages

DEDICATION ..... **v**

ACKNOWLEDGEMENTS ..... **vi**

ABSTRACT ..... **vii**

TABLE OF CONTENTS ..... **viii**

LIST OF FIGURES ..... **x**

1. INTRODUCTION **1**

1.1 OVERVIEW 1

1.2 BACKGROUND 2

1.2.1 Billing Systems 2

1.2.2 RouterOS 2

1.2.3 User Manger 2

1.3 PROBLEM STATEMENT 3

1.4 OBJECTIVES 3

1.5 PROJECT SCOPE 4

1.6 THESIS OUTLINE 4

2. LITERATURE REVIEW **6**

2.1 BILLING SYSTEM 6

2.2 DISTRIBUTED NETWORK SECURITY FIELD AGENTS 7

2.2.1 System of Management 8

2.3 FUNCTIONS INCLUDE SNMP SET, SNMP GET NEXT,SNMP TABLE AND SNMP SET 11

2.4 THE SYSTEM OF NETWORK MANAGEMENT 12

2.4.1 Three Growing Models Of Network Management 13

2.4.1.1 The centralized system 13

2.4.1.2 The hierarchical model 13

2.4.1.3 The distributed model 13

2.5 IMPLEMENTATION OF NETWORK SECURITY SYSTEMS IN BUSINESSES 13

2.5.1 Fault Management and Issues Management 15
2.5.2 Management Configuration 15
2.5.3 Control of Management 15
2.5.4 Control of Defense (SECURITY) 16
2.5.5 Manage of the Account 16
2.6 INFORMATION OF VULNERABILITY OF COMPUTER SYSTEMS TO ENHANCING THE NETWORK SECURITY 16
2.7 SUGGESTIONS ON THIS PROJECT 19
2.7.1 Enhancing Security 19
2.7.2 Decreasing Error Rate 19
2.7.3 Package Transmission Rate 19
2.8 WIRELESS COMMUNICATION 20
3. METHODOLOGY 22
3.1 INTRODUCTION 22
3.2 SIMULATION SETUP 22
3.3 JUSTIFICATIONS 23
3.3.1 The Reason of Choosing API 23
3.3.2 The Reason of Choosing Mikrotik the API 24
3.3.3 Access Mikrotik via API 24
3.3.4 Requirement of Project 24
4. SIMULATIONS RESULTS 25
4.1 OVERVIEW 25
4.2 SIMULATION 25
4.2.1 Create and Distribute Via a User Manager 28
4.2.2 Create and Distribute Via a Broadband Protocol 31
4.2.3 Create and Distribute Users Via a Hotspot Protocol 34
5. CONCLUSIONS AND FUTURE WORK 36
5.1 CONCLUSIONS 36
5.2 FUTURE WORK 36
REFERENCES 37

LIST OF FIGURES

Pages

Figure 1.1: A simple scheme (chart) for internet service in several countries 1
Figure 1.2: Flawchart of thesis outline 5
Figure 2.1: Mobile agent-based virtual network system [12] 8
Figure 2.2: Architecture of the demonstration network [13] 11
Figure 2.3: The output of HP Open View for the MIB ipRouteTable group [13] 12
Figure 2.4: The number of found vulnerabilities (b) the number of reported events [24] 20
Figure 3.1: The work of API [25] 22
Figure 3.2: API deal with a lot of applications [25] 23
Figure 4.1: Router board RB433 25
Figure 4.2: Winbox program The information of router: Mac address, IP address, Identity,Version, Broad and Uptime 26
Figure 4.3: Then Activating User Manager it combines hotspot and broadband simultaneously. 26
Figure 4.4: Then Activating User Manager it combines hotspot and broadband simultaneously 27
Figure 4.5: Then Activating User Manager it combines hotspot and broadband simultaneously 27
Figure 4.6: Create and Distribute Via a User Manager (Application of maxbox). 28
Figure 4.7: Create and Distribute Via a User Manager (The options of application) 29
Figure 4.8: Create and Distribute Via a User Manager (Created username and password) 29
Figure 4.9: Create and Distribute Via a User Manager (Program entry browser) 29
Figure 4.10: Create and Distribute Via a User Manager (Enable and disable) 30
Figure 4.11: Create and Distribute Via a User Manager The Connection 31
Figure 4.12: Create and Distribute Via a Broadband Protocol (Options of program) 31
Figure 4.13: Create and Distribute Via a Broadband Protocol (Created username and password) 32
Figure 4.14: Create and Distribute Via a Broadband Protocol (Login by username) 32
Figure 4.15: Create and Distribute Via a Broadband Protocol (This connection) 33
Figure 4.16: Create and Distribute Via a Broadband Protocol 33
Figure 4.17: Create and Distribute Via a Broadband Protocol (Successful connection) 33
Figure 4.18: Create and Distribute Users Via a Hotspot Protocol (Options of program) 34
Figure 4.19: Create and Distribute Users Via a Hotspot Protocol (Created username and password) 34
Figure 4.20: Create and Distribute Users Via a Hotspot Protocol (Done creation) 35
Figure 4.21: Create and Distribute Users Via a Hotspot Protocol 35

LIST OF ABBREVIATIONS

API	: Application Programming Interface
IP	: Internet Protocol
MAC	: Media Access Control
CLI	: Command Line Interface
PPPOE	: Point-to-Point Protocol over Ethernet
ISP	: Internet Service Provider
RouterOS	: Operating System Of Router Board
MIB	: Management Information Base
NAS	: Network Attached Storage
SNMP	: Simple Network Management Protocol
RFC	: Request For Comment
LAN	: Local Area Network
WAN	: Wide Area Network
VSAT	: Very Small Aperture Terminal
SSH	: Secure Shell
FTP	: File Transfer Protocol

1. INTRODUCTION

1.1 OVERVIEW

A brief summary of the internet world and how to develop and access it to users in my country, Iraq, where the environment in which these studies were carried out, Uruklink, which was the only provider of Internet services [1], competition from Internet service providers (ISPs) including broadband satellite Internet access services From the very-small-aperture terminal (VSAT) hubs in the Middle East and Europe, after a period of time and through an agreement with the Ministry of Communications, international terrestrial fiber-optic connections have been established with the Kingdom of Saudi Arabia, Kuwait, Turkey and Jordan 2011 [2]. The Ministry of Communications, through the General Company for Communications and Informatics [3]sells Internet packets to the provider, which it is the main root, after which it sells them to Internet service companies (ISPs), including EarthLink, where EarthLink became the largest provider of Internet services in Iraq for obtaining a license from the marine cable Falcon. EarthLink distributes packages to authorized agents with a specific download and upload, the agents divide it's into categories of 20$,30$ and 40$ etc. then sell its to users. The process of creating and designing Internet packages and what we have mentioned above are steps that require a lot of time, staff, and effort to work in a Billing system, regardless of the users whose internet service expired and the trial internet service users.

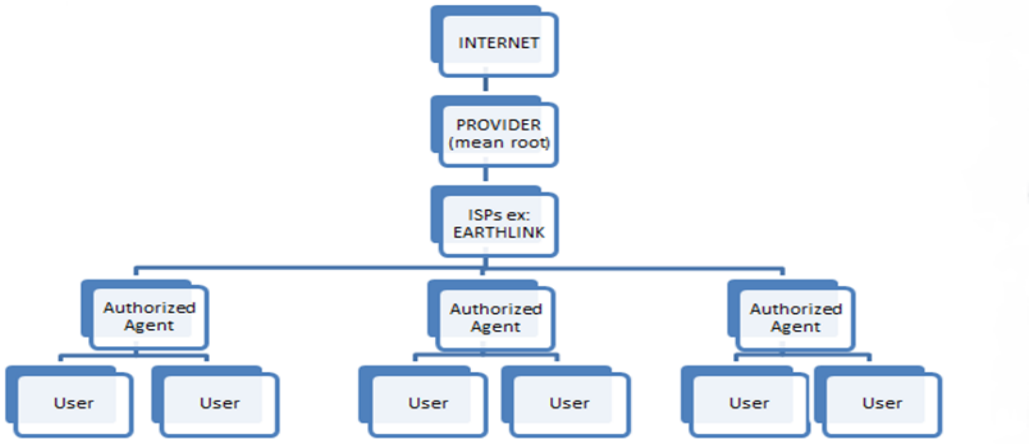

Figure 1.1: A simple scheme (chart) for internet service in several countries

1.2 BACKGROUND

1.2.1 Billing Systems

Managing internet networks are inaccurate, expensive, wire and slow so its need a lot of time, employees and effort. This is why some attempts to convert traditional systems to modern systems were made by billing system. in this project we suggested a complete solution So has been created a group of programs and tools that are interlinked with each other in order to reach the best performance in managing wireless system, where we removed the obstacles and difficulties that the network manager was facing in dealing with the Mikrotik system by creating new tools and programs that are not present in the Mikrotik and linking them wireless to the system and making interactive and easy interfaces dealing with it. so has been created an application programming interface API that we called Maxbox, where in a very short time, it can create a number of Internet (users) by IP or Mac address then designing and distributing them by three systems (protocols), Hotspot, Broadband and User manager.

1.2.2 RouterOS

We may not need to use the Mikrotik device as the Mikrotik company provides its own programming on the official website www.mikrotik.com [4], RouterOS is an operating network program optimized for deployment on MikroTik RouterBOARD routers. It can also be installed on a Computer, turning it into a firewall, VPN server and client router and a wireless access point. The program will act as a captive portal that is focused on wireless connectivity. a computer preferably with very high specifications (RAM, processor and hard) so the reason may need to create (3000~6000) cards (Users), so the direct proportion between the quality of the server (mikrotik) and the number of users, that is, whenever the router has a high quality and great features, produced a greater number of users.

1.2.3 User Manger

The last updates where the user manger provides internal radius, also it can combines hotspot and broadband simultaneously it makes them authentication. User manager supports the validity service for users (hours,days) and at the end of the period, It will disable the internet service

automatically, in addition to that it is possible to configure unlimited cards. Suppose that the general agent (the main company) in Istanbul city and the sub-agent in Ankara city where he needs Internet service where the general agent can through the Maxbox application login to the sub-agent device by public IP through a username and a password to access it and control it, he can access through Mac address if the network is internally (private IP). As for if the network is external and from different places around the world (Public IP), it can only be accessed through IP address. Maxbox can deal with sub-agents and with users, the higher the specifications of the device, the more cards it has created (4000~5000 users). Apart from the Maxbox or programming for the Mikrotik site, we can create profiles (categories 20$, 35$, 40$ etc.), but the basic idea of Maxbox as well as CLI or other software is that they all need to write a lot of codes, time and effort to create only one card while Max Box specifies profiles, download, upload and choose one of the three protocols (Broadband, Hotspot or user manager) and creates the required number of cards for internet service at a very short time.

1.3 PROBLEM STATEMENT

There are many issues in the field of internet and telecommunications in my country and other countries, the most important of these problems is the wireless problems, which causes many to be resolved in order to solve these problems requires a long maintenance time of what will affect the performance of communication services or the internet services, often due to the configuration of internet and telecommunications networks close to some, the long time spent creating cards, Little storage space, Difficulty dealing with devices, Disconnect the internet service of user for a specified period and determine the amount of Internet packages, that mean the most problems in network management are time so it is better to solve these problems.

1.4 OBJECTIVES

The objectives of this project are:

1. Eliminate the obstacles and difficulties that the network manager was facing in dealing with the Mikrotik system.
2. creating new tools and programs that are not present in the Mikrotik.
3. linking them to the system and creating interactive and easy interface.

1.5 PROJECT SCOPE

The scope of the project will be concentrating as follows:

1. The primary aim of a biling system is to make a customer's life easier. This is a simple tool for customer support that also guarantees that payments are made on time. Once a billing account is set up, customers ' personal information is evaluated.
2. NAS (Network attached storage) Support, MaxBox supports Mikrotik & CISCO, unlimited NASs can be added to the system.
3. Automatically facilitating the billing system, whether distribution of service categories or quantities.
4. Data Limit, Set downloads/uploads for every profile or a total traffic limit.
5. Secure, with MaxBox, all actions are logged into system log database where admins can review and audit transactions and updates carefully.
6. Dynamic Rate Control, Setup time based policies for RX/TX rate control.
7. Managers & Commissions.
8. Supports unlimited levels of sub resellers. Each reseller can generate commissions automatically to his/her parent reseller.
9. Pricing MaxBox annual license priced according to the number of subscribers. Upgrade is possible at any time.

1.6 THESIS OUTLINE

The research encompasses five (5) main chapters, namely; Introduction, Literature Review, Methodology, Simulations Results, then Conclusion and Future Work . Details and explanation to every chapter will be discussed below::

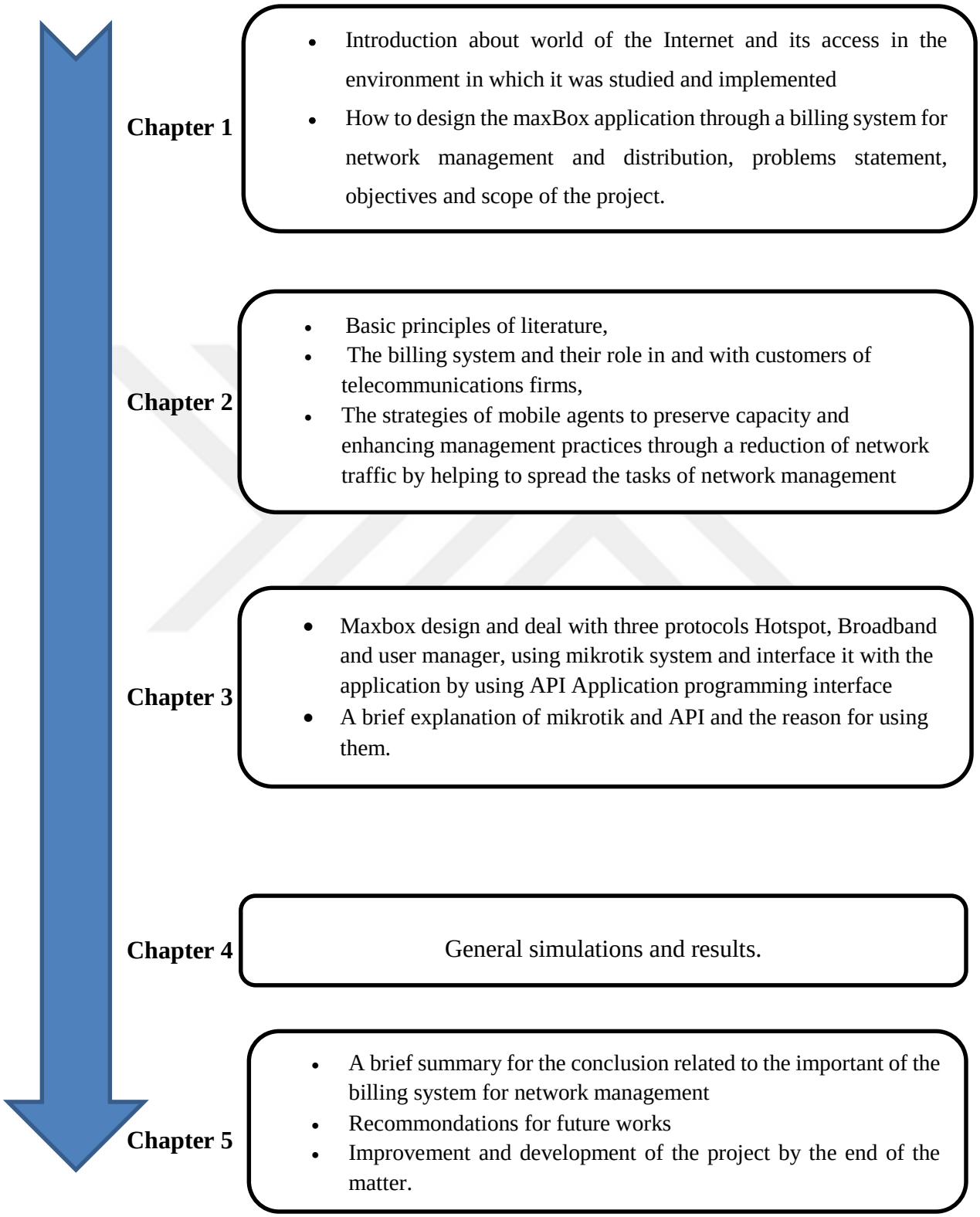

Figure 1.2 : Flawchart of thesis outline

2. LITERATURE REVIEW

2.1 BILLING SYSTEM

According to Matem Mustafa telecommunications companies need an effective and secure billing system for revenue collection[5]. During service operations, billing systems monitor the usage of network equipment in one call information record (CDR). The billing process consists, inter alia, in receiving billing records from different networks, determining the billing record charge levels, estimating costs for each billing record, attaching these records to the customer's daily invoice generating method, issuing invoices and collecting payments from the customer, etc. Billing systems are very complex, beginning with network components that use the billing system to pick, mediate, identify and invoicing uses. The program user navigates the web of the client and displays company services and decides to order one of the available services. If you don't have an account, register for a new one, and sign in. The customer then demands that the chosen service be ordered. The service may be repayable when it is necessary to pay for credits to use the service or after paying for a facility or lease to pay for the usage of each billing period. The service can be billed in advance. The billing system will give the user a service, collect utilization data and create invoices for each expired credit, each billing period depends on the kind of billing, payments are received and changes to customer balance.

The company is distributed and presented to the customer. that service is defined as a service catalog containing the engineering officer type of service, name, billing policy and default rating profile. the customer shall, following the customer's service order, take a specific account, given at a certain time by the customer's supply network. the customer account includes customer contact details, account type, authentication information and payment methods. that client account is linked to the different services provided to that client within the network and the client will be charged based on his use of these services. the customer account belongs to a certain form of account that is connected to certain pricing plans formed through reductions and promotions[6].

2.2 DISTRIBUTED NETWORK SECURITY FIELD AGENTS

Mobile technology helps preserve network flexibility and improve management efficiency by reducing network traffic and helping dissipate central tasks in the host subnet. Just a few years ago, the majority of networks were LANs with limited interface links. During this time, a centralized architecture dominated the networks. Owing to the simple and effective architecture, network maintenance operations have been carried out on a computer or workstation. Nevertheless, the exponential growth of Internet applications has led to a global network explosion, putting a huge burden on networks and administrators. However, it is not shocking that these changes cannot be governed by the traditional centralized structure. The central network server frequently asks for the status of the local units in this architecture. Contact data can also be lost during transmission. The network manager monitors network flow patterns in a distributed network to identify irregular circumstances and to assess network performance For network equipment management, descriptive data can be accessed from the management Information Base (MIB). MIB provides numerous data artifacts for network management, including system data, device status, connection status [7]. The MIB data is clustered and stored in a tree-like structure[8]. It allows the managing of complex network operations in the distributed network management system mobile agents that use a distributed network infrastructure[9][10] are part of the modern network model. The The mobile agent can be used to combine MIB data in the business area to track network traffic. Tasks for management are allocated to an agent and can be redirected to remote hosts to perform the work. After the mission has been completed, the handler returns the reports to the sender. The workload may be shared with the central network server between the local subordinate network (subnet) hosts. This approach has many advantages, as defined in[11]. Furthermore, mobile organization transforms the design of the traditional central network into a management delivery system. In the absence of a relation. Mobile and data agents may be temporarily put in the local hosts agent box and removed prior to reinstatement of the link between the server for the network management and the subnet. It is intended to create an unstable network environment. Latest Analysis [12].

The following are indicated the policy for administrators is not to own proprietary information systems but to outsource IT to Internet providers and in the near future we will definitely expect a significant spike in network traffic. This approach calls for effective distributed network

management, and offers the ability to prove its value in mobile network management (see sidebar). We identify a test system's mechanisms and features to demonstrate the benefits of mobile network delivery.

2.2.1 System of Management

A Distributed Network Management Mobile Agent Architecture We suggest an implementation prototype shown in Figure 2.1 demonstrates the distributed network control structure of the mobile agent. The Software is IBM Aglet and is a Java Virtual Machine & Aglets Development Software Kit, accessible from sourceforge.net. To access the MIB network, the server uses the Advent Net SNMPv1 API (www.adventnet.com). Note that SNMP communications protocol commands are simple and low-level. The network management system supplies only basic commands such as receipt of requests and next requests and the acquisition of subnet MIB objects. The type of network data is defined in the RFC-1213 MIB-II.

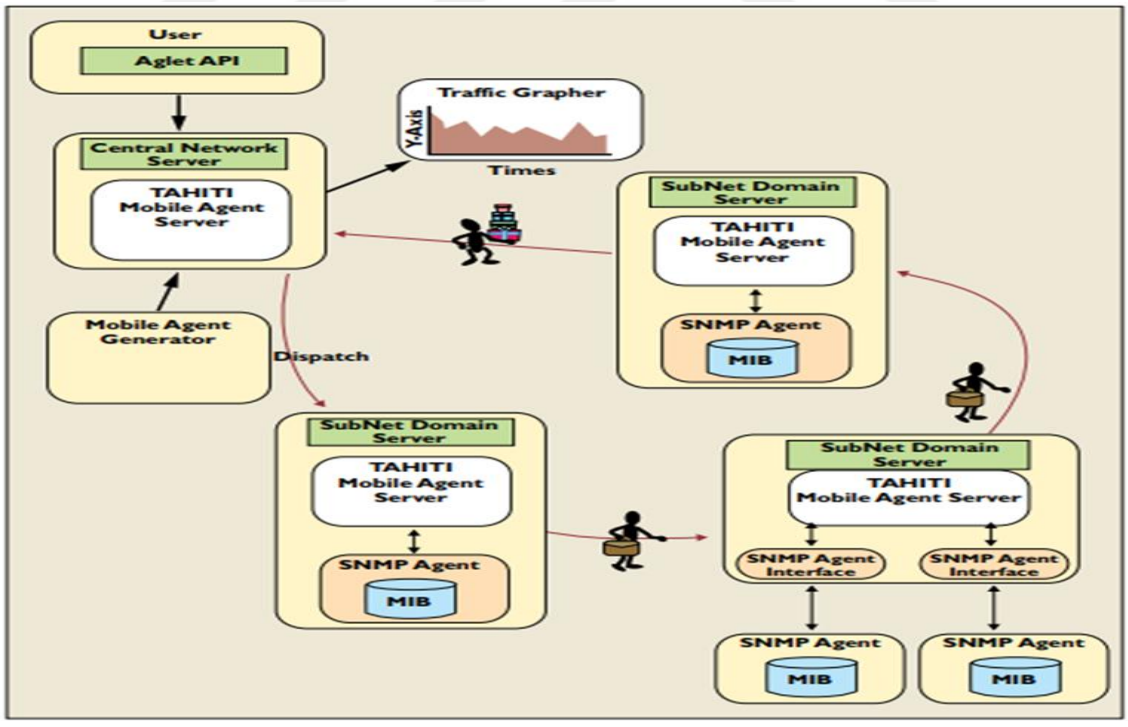

Figure 2.1: Mobile agent-based virtual network system [12]

The mobile agent gathers MIB data and sends the data to the network servers in the local hosts. The MIB has application types, interfaces and tree-like structures, ip, icmp, tcp , udp, egp and snmp. Such groups will mark objects and control agents which they are sending (RFC1213.txt at www.ietf.org). Such classes can also assign object identifiers. The object identification (OID) feature in the MIB tree node. An object is retrieved by SNMP through the OID. In the communications network control system , for example, OID 1.3.6.1.1.0 is issued to the SNMP network device. The overview of the device data can be obtained from the MIB network equipment. The network contains three types of data classes: unstable, list, time and integer, for example system set. There is a table group of data such as several network mapping index object interfaces, for example a data recovery system identification. In the first two classes, basic MIB things are available, whereas those indexes are more specific than MIB objects. The MIB object value can only be obtained from a request order in the SNMP communication protocol. The efficiency index of the network is typically obtained by combining several simple MIB objects.. It is difficult to accumulate network variables. The total bandwidth of the MIB object is around 606 MB (351 bytes x 100 hosts x 17.280), for example when accessing a single MIB object using the MIB-II sysUpTime Framework Team[13]. however, the mobile agent filters in the subnet host network variables and returns the calculated results only to the central server, network traffic will decrease considerably. was created a mobile agent system prototype to demonstrate the proposed structure for distributing network management, Enable users to pick network equipment, set the group list of SNMPs and delegate tasks for mobile agents. The mobile agent performs tasks and detects MIB objects or installs them on subnets hosts. After completing tasks on The mobile agent goes to the next host on a predefined local host path.

The mobile agent operating via SNMP agent interfaces is unable to communicate with the network computer in a new version of IBM Aglet. When all operations are over, the agents return the data obtained to the network managements system. The mobile agents are periodically transferred and the data obtained can be used for analysis in order to collect long-standing data in the management network. The device requires three module: a mobile agent module, an application network flow data collection module and an application network module. The mobile agent module is built on the main servers and subnet node hosts. Both sides will be provided with JDK 1.1 (Java Development Kit) and ASDK 1.1 (IBM Aglet Development Java Language). The core component

is the network security program Database Contains Aglet's Tahiti database and Master and Distribute Aglet programmers. This Circulate Aglet is a mobile agent program that sends the agent to the local host and returns data to the central server.

Master Aglet, on the other hand, is the central stationary server agent that sends and receives a mobile agent to local hosts. Also, the local host is provided by the Tahiti server for the execution of mobile agents and the networks of SNMP agents for the collection of MIB subnet data. The agent program contains data generated by the data collection module of the network. The network data collection module is designed to implement the SNMP agent program in the AdventNet SNMPv1 API for local hosts (see www.adventnet.com).

The API includes commands such as request receipt, request receipt, device receipt, monitor, etc. This module generates data on mobile devices, for example, network IP apps, SNMP and SNMP MIB requests for object ID. The Network Data Collection module transfers SNMP packets to network equipment that request MIB data after receiving requests from a mobile agent. The network flux analysis module adds Tobias Oeticer / Dave Rand to the multi-router traffic graphics (MRTG) system. You will find this in people.ee.ethz.ch/~oetiker / mrtg/). This module can be installed for the analytical network flow on the main server or other device. The module analyzes the MIB data of the cell handler. It is expected to install an ActiveState module for Win32 with Perl5 (www.activestate.com) on the server and the mrtg.cfg parameters shall be the same as the mobile agent. The network flow can be measured by day, week, month or year. The machine was based on the campus' Ethernet, Fast Ethernet, FDDI and laser networks. IP address for Group B (140.135.xxx.xxx). The mask was set to 255,255,248.0, to differentiate between departmental flow volumes and to sustain network expansion. A total of 32 subnet domains can be linked to the campus network. In order to maintain a viable testing environment, only three subnet servers monitor three subnet domains. Architecture as shown in Figure 3. This includes a Cisco 4700-speed router, a 3Com BLN 3300 Super Ethernet 3300 exchanger and a 3Com Super 1100 Super Ethernet 3Com 3rd level Super StackII 1100, and several 3Com Super Ethernet 1100 second level and 4 NT servers Java (Sun Microsystems' JDK1.1.8) is a language of experimental network operating system development, IBM Aglet is a mobile agent language and the SNMP internet protocol is TCP / IP. For the study of flow an MRTG flow map is used while for MIB objects the mobile agent interfaces of the SNMPv1 API Release 3.1 are used. The MIB is designed to follow the RFC-1213

(MIB-II) standard. SNMPv1 API Communication functions for the MIB Release 3.1 are compliant to both RFC-1155 and RFC-1157.

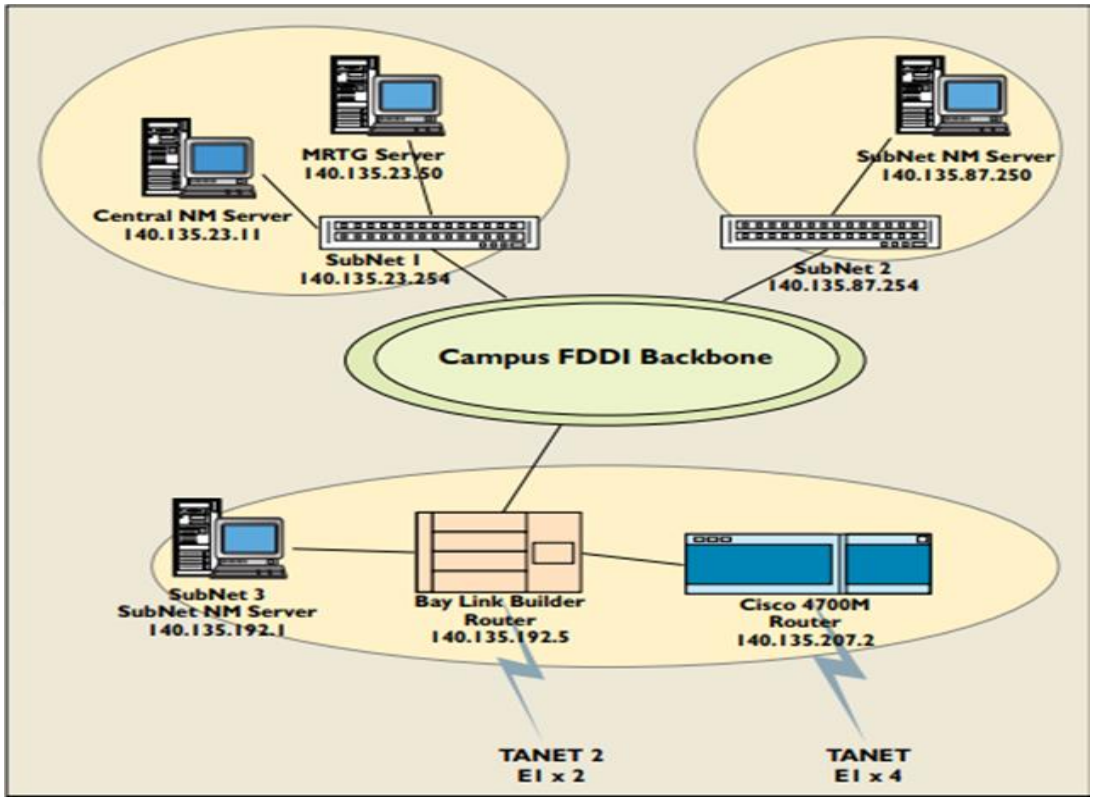

Figure 2.2: Architecture of the demonstration network [13]

2.3 FUNCTIONS INCLUDE SNMP SET, SNMP GET NEXT, SNMP TABLE AND SNMP SET

Functions SNMP, which retrieves the following data, finds the table information and sets the MIB network connection system information on the basis of the MIB object tree ID. The presentation tests the precision and efficiency of the system. To ensure accuracy, network operations are compared to conventional network management systems and bandwidth and network utilization efficiency are measured. For network packet inspection, the Network Associates sniffer is used and the Protocol Inspect is used for the study of network packets. The domain server receives the MIB values from the subnet devices and sends them to the central network server through a mobile agent. In the subnet table community, the host domain retrieves MIB values from routers, such as the IP

Route Table MIB-II. The network management program HP Open View shows the efficiency of data collection and guarantees operational accuracy. The IP route table in MIB-II form is shown in Figure 4. Finally, the domain host subnet receives a subnet equipment's network flow volume via D-Link Network Management Software. The data is transmitted via the mobile agent to the central network server and used for network performance assessment.

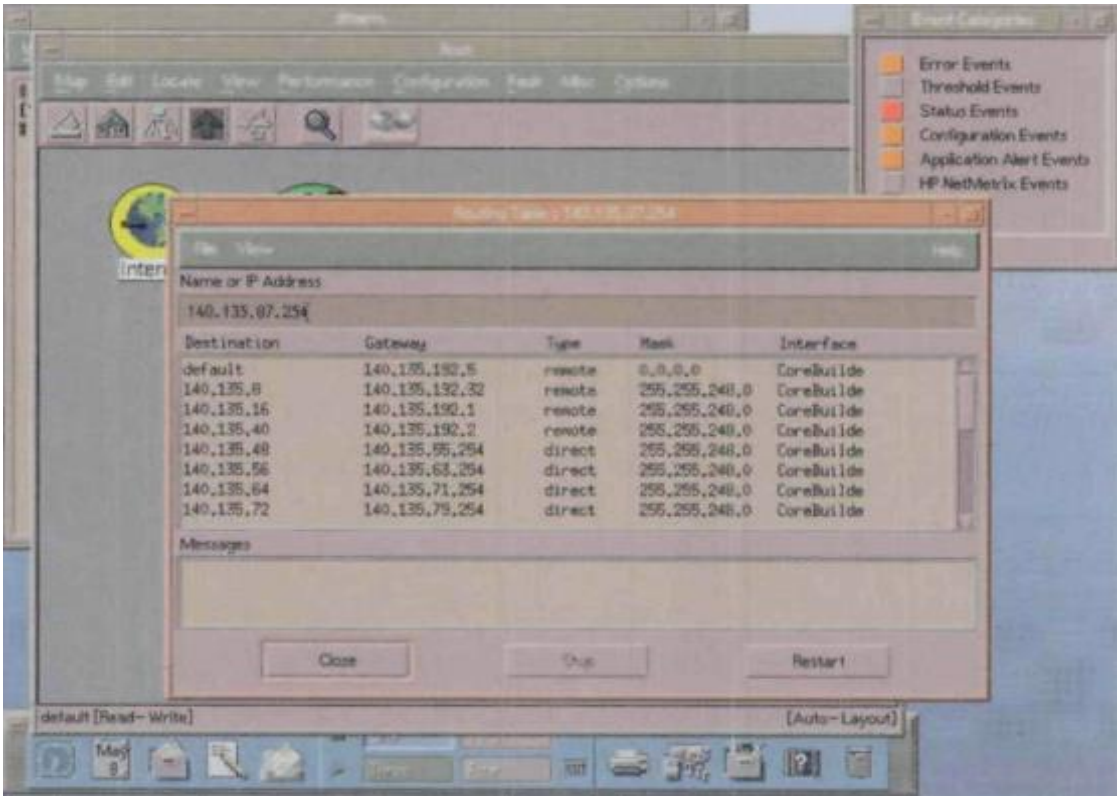

Figure 2.3: The output of HP Open View for the MIB ipRouteTable group [13]

2.4 THE SYSTEM OF NETWORK MANAGEMENT

The network Control framework is a method of network management data collection. The network manager tracks, registers and controls the network performance of the program. This system includes a specification for network management that is consistent with network hardware and software. In order to share information between equipment types a communication standard is also required. The well-known Internet protocol TCP / IP is the most common one and follows the Simple Networking Management Protocol (SNMP).In 1990 RFC1157 * published the first version

of the SNMP and is now being revised in version 2 of the SNMP. For communications with subnet device types, SNMP offers a basic network management system protocol.

2.4.1 Three Growing Models Of Network Management

2.4.1.1 The centralized system

The unified model, relies on the mainframe of the central network. As stated, it is not efficient if the network nodes increase dramatically. SNMPv1 is a management protocol example.

2.4.1.2 The hierarchical model

Currently is the most common hierarchical model. TMN, CMIP and SNMPv2 demonstrate this trend. While the hierarchical model shares responsibility for management, management activities tend to rely on the Nodes of Administration. This prevents networks from adapting to the environment dynamically.

2.4.1.3 The distributed model

Provides local networks' administrative tasks. that model is available via distributed artifacts or mobile devices. For example, RMON, the IETF task force provides traffic monitoring statistics on subnet hosts. Researchers have suggested four functions for an agent-based mobile network management framework: manager apps, mobile servers, mobile agent generators and mobile agents[14] [15]. It allows mobile agents to add multiple MIB values, to obtain SNMP tables and to filter tables in snapshots. Carleton University's Perpetuum Mobile Procura initiative[16] has developed an architecture to include mobile agents in SNMP, since SNMP gathers crucial information on the node and With minimal complexity, the mobile agent can provide code agility, security and reliability.

2.5 IMPLEMENTATION OF NETWORK SECURITY SYSTEMS IN BUSINESSES

Today, network managers face huge obstacles in the management of the numerous client networks. While a network manager provides many network management tools to support the mission, these devices have their own limits on usability and the requisite skills to use them, as well as to be

introduced at corporate network level. This paper analyzes the operational understanding and the harmonization of the network management method with organizational objectives. It addresses the challenges that Network Managers face by using this tool to fulfill their needs and encourages their operators to use this tool to deal with their everyday activities and establish a solution framework. In a case study, this concept was checked. The results of this case study are positive and can be applied for other similar corporate network management applications.

Networks form the foundation of enterprise in the globalized world of today. The backbone network consists of essential tools, including routers, gateways, switches , firewalls and servers from different providers. Business continuity relies directly on the quality of the network. Just a few minutes of network failure can have a direct effect on sales as major business services are impacted. The complexity of the network is also growing as business needs grow [17]. Network executives are under constant pressure to ensure that the network meets the business requirements of the company. Systems are becoming more complex and evolving. They are therefore exposed to problems of failure, inefficient performance and security. The network administrator must control the complex network efficiently to ensure access, protection, reliability , efficiency and usage of the network bandwidth.

According to Goers and others [18], business criteria include network planning, architecture, performance tuning and power modeling. Network reliability is based on base fittings, historical use studies, SLA reports and performance monitoring from a service management point of view. Network operators may execute these operations manually or continuously using network control software. Due to the administrative repetitive, time consuming and error-prone management of the enterprise network , Network Managers rely heavily on software to help their daily work. Just one network management framework may be used to integrate all of the above activities or resources to provide such services. Network administration is typically a program that facilitates the control, troubleshooting and maintenance of network administrators. the networks will usually be categorized as telephone networks and internet (IP) networks as Mo Li et al. Two different principles were adopted by network management systems , i.e. the ITU-T Telecommunication Management Network (TMN) and the IETF Basic Network Management Protocol (Mon Li et al). Both of these have advantages and disadvantages, but this paper only discusses issues and concerns related to data processing instruments (IP).

Network management systems typically have three basic approaches: centralized, hierarchical and distributed. Actually most network Centralized and frequently managed control systems use the Basic Network Management Protocol (SNMP). The central management station gathers and handles the entire network. The network management mechanism fails if the central manager fails. Network management tools automatically track network equipment, build topology diagrams of network in real time, adjust the topology and trends, helping network managers take proactive action to control network services.

Network management can be divided broadly into five categories of function, They are the following:

2.5.1 Fault Management and Issues Management

Network failures can cause downtime, weaken the network, and ultimately affect network users' performance. The aim of fault management is to detect, log, alert users about the problem and remotely fix problems to maintain the network efficiently. Fault management includes the detection and removal of network faults. The solution must be fixed and tested and used on all or even defective devices until the problem has been found.

2.5.2 Management Configuration

The network equipment remote control is responsible for the configuration management task. Configuration management seeks to control device configurations in order to track and manage the effect of different hardware and software component models on network activity. Management settings include operating system, Ethernet port and version type, TCP / IP stack variant, SNMP model, etc. Often this management information is stored in a user-friendly database. An knowledge base can be searched to help solve a problem. Parameters such as system status service, routing table transmission information, etc. can be set up remotely.

2.5.3 Control of Management

It’s important to calculate the role Performance management network elements such as hardware, software and media. Quality management is structured to measure various aspects of the network

output parameters and preserve the efficiency of the network at an acceptable level. The results include network performance, consumption rate, error rates, response times and line utilization. Quality control consists in defining outputs to indicate an investigable or exploratory network problem such as interface traffic, TCP connection, number of transmitted and received packets. Management of quality can be reactive and positive. In the event of failure, the computer responds with a response. Network models could be used to prepare and establish trends in network traffic by proactive management, and the necessary steps could be taken accordingly.

2.5.4 Control of Defense (SECURITY)

Safety management seeks to monitor network access in accordance with organizational standards , ensuring that the network is not compromised deliberately or accidentally. the purpose is also to prevent individuals without proper authorization from accessing Sensitive information. Confidential information. the network resource logging users can track a security management system to prevent people's access without correct access codes. By partitioning the network resources, the security management system will function as allowed and forbidden areas. For example, access to human resource data for other departments is inadequate and should therefore be restricted to this department alone.

2.5.5 Manage of The Account

The aim of inventory management is to consider the behavior of the network by inventorying and reviewing users, network devices and bandwidth utilization to provide insights into existing use trends. Using quotas can be assigned on the basis of this analysis to individual users or classes. Optimum access points can be achieved after multiple iterations and a correction. when efficient, calculation will include details on the equal and efficient usage of resources and assessment.

2.6 INFORMATION OF VULNERABILITY OF COMPUTER SYSTEMS TO ENHANCING THE NETWORK SECURITY

The security problem becomes more critical for anyone who uses computers in these years. Nevertheless, code bugs are so often discovered that device administrators won't be able to fix any of these bugs on network hosts in no time. They will carry out a risk assessment to decide the

priority of vulnerabilities to fix up. In addition, they do not have the administrator right on all network hosts but just have the right on certain network computers. The system administrators should set the ACL scripts on network devices to prevent these vulnerabilities from exploitation on hosts. The solution immediately improves network security, as some threatened service ports on hosts are blocked from being accessed. This paper introduces a method for improving network security consisting of network management, vulnerability scanning, risk assessment, access control, and incident reporting. The risk evaluation, which is followed by the network topology, Shows the threatened service ports which should be blocked within ACL scripts. Such techniques do not cost any additional pieces of hardware. Network security increases nearly 40% with just 8% of threatened ports being blocked in the examined Class B network with the proposed process. Those two indices, the overview of CVSS values and the number of vulnerabilities in the network, measure the 40% increase in network security.

The network technologies have recently been extended to other fields, such as tax payments, online trading, e-commerce, electronic voting. Such application systems are composed of network equipment and host computers. Protecting certain application servers and network devices from data tapped or falsified by malicious attackers is very critical. Many commercial hardware and software, such as firewall systems, intrusion detection tools, malware security software, Vulnerability scanning software and so on, are designed to protect against such malicious attackers. Using such hardware and software, However, Cannot guarantee computer systems against all attacks. According to the February 2005 report of the President's Information Technology Advisory Committee (PITAC), the computer network protocols were conceived in the concept of interacting between trusted partners[19]. In other words, at that time the security properties were not known, so that some kinds of attacks could quickly spread over the Internet, such as Distributed Denial of Service (DDOS), the computer virus – Code Red[20], or the computer worms Slammer[21]. The wider the damage spreads, the higher the cost. As a matter of facts, a single device on which the program has exploited a vulnerability will result in the damages. Therefore it is very important to eradicate the abuse of vulnerability. According to data from Computer Emergency Response Team/Coordination Center (CERT/CC) reports, the number of vulnerabilities exploited is rising dramatically. In the decade of 1996–2005, the number of vulnerabilities reported was between 345 and 5990[22]. The number of incidents registered to CERT / CC in 1996 was 2573. It was at an

amazed 137529[23]. During the cyber-war, the "victor" between network administrators and malicious attackers is the one who can get and use vulnerability information during computer systems. Therefore the "Vulnerability Management Program" is implemented in the security control of the computer system. The knowledge from evaluating computer system vulnerabilities lets system administrators know how to protect the network from suspected attacks of intrusion or infection. The vulnerability management conducts security tests of the device as declared new vulnerabilities or as installed new hosts after a period of time. After patching these vulnerable systems, the systems would be safe from attacks. This patching process is definitely time consuming. In fact, certain flaws cannot cause the damage to costs. Such severe bugs can only be patched by device administrators, rather than others. Network administrators will periodically search intra network.

Program administrators may have the following problems following testing of the system:

1- What weakness will I fix for fist?
2- Which host can cause a lot of trouble?
3- Where are those insecure hosts?
4- Do I have the right to patch those hosts and control them?
5- Is the patched host still sufficient for all requests software?

In reality, most system managers for a small business or association do not consider the above questions. They 're still in passive behavior, waiting for feedback from users and only seeking solutions. They are looking up these vulnerability databases published in some popular web pages to solve the problems of users. They should seek to locate the patch-up system or install the threatened hardware or software properly after the vulnerability information is identified. The databases have only given the characteristics to certain vulnerabilities but no solution technique has yet been established. System managers then don't have a solution to these problems This paper provides a way of determining the risk rates of intruding and infecting hosts. The system manager orders a list of hosts on which patching processes are needed, firstly, according to the risk level on-host. Second, administrators use the technique of access control on network devices to distinguish these hosts from those with vulnerabilities. Managers then report the vulnerabilities to those hosts'

owners. Before that, managers start patching those hosts they have the right to administrate on. Thus network security is enhanced.

2.7 SUGGESTIONS ON THIS PROJECT

2.7.1 Enhancing Security

Each company has its own firewall security system, such as Mikrotik and Cisco, where Cisco is one of the strongest companies in domain security, also every ISP Internet service provider company has a firewall product such as Fortinet and Palo Alto, to protect network security from the danger of any exposure For expected attacks. The Maxbox application, when used to login the Mikrotik router, needs a user name and a password, in addition to deals with devices of Mikrotik company thus it has a security system**.** The warning of any security bugs that may lead to danger, there are commands that must be taken:

1- Disable Ports of SSH and Talent to not allow access to any untrusted person.
2- General blocking to not allow access to the router for any user only allowed.
3- Switch of services ports.
4- Disable Port 80 (www) because it is not secure and hack able (penetrable), unlike Port 443 (https) as it is very safe.
5- Continuous monitoring of updates to address previous bugs.

2.7.2 Decreasing Error Rate

The MaxBox program has errors that may occur in the most remote possibility when it is given an order to create cards (users) in a large number greater than that programmed, for example the requested number 5000 users and the creation order 7000 user or more, as mentioned previously MikroTik RouterBOARD (RouterOS), and this negatively effects of the database and thus affects CPU then the program will stop and restart, but these errors are unusual to happen because the program was designed primarily based on the speed and that errors occur depends on the features of the device.

2.7.3 Package Transmission Rate

First this application has been designed based on the speed, meaning that its purpose is speed in creating cards (users), there is a small difference in the rate of speed of creating the required numbers of users depending on the way the of linked the program with router, whether it is wireless or wired where access is And creating the required numbers with a (wired) cable is tens of times faster in its work than connecting it wirelessly. The reason is that the wireless connection leads to data loss through being affected by noise, interference, etc.

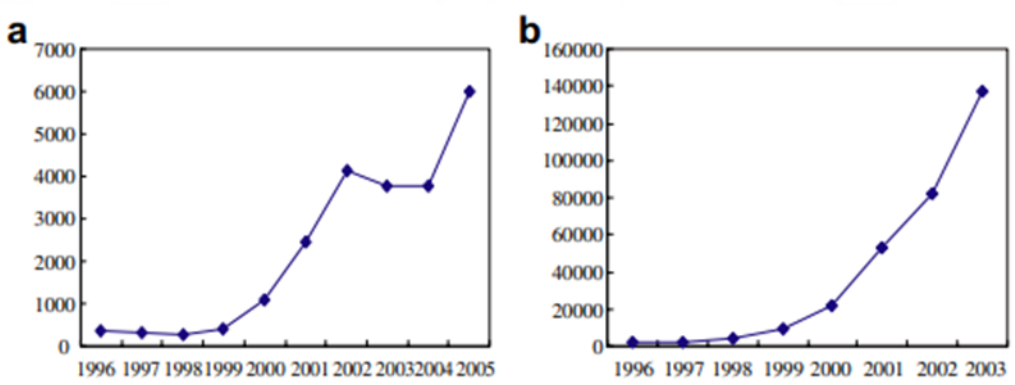

Figure 2.4: The number of found vulnerabilities , the number of reported events [24]

2.8 WIRELESS COMMUNICATION

Wireless connection can be defined as a method of transferring information or power between two or more points that are not connected by physical wires.

The process of transferring the Internet through it:

1. Provider is the main root.
2. ISP is the customer of the service provider.

The process of transferring the Internet from the provider to the ISP:

1- Via optical fiber cable.

2- Via Link Wireless with high specifications that handle the amount of transmitted bandwidth.

The process to transfer the internet from ISP to sub-agents:

1- Main tower equipped with Tx antennas, each antenna is directed at the location of the branch tower, which is Rx.
2- When providing the agent with Internet service, he can access all the services provided by the company, whether it is a media service, share or any other application of the company.

The process of access the maxmox program:

1- Through connection with the company's servers through the point to point / Tx-Rx wireless link, it is possible to access the application and create the cards.
2- The Maxbox program can be accessed from outside the network through VPN technology and through the public IP.

Suppose that the general agent (the main company) in Istanbul city and the sub-agent in Ankara city where he needs Internet service where the general agent can through the Maxbox application login to the sub-agent device by public IP through a username and a password to access it and control it, he can access through Mac address if the network is internally (private IP). As for if the network is external and from different places around the world (Public IP), it can only be accessed through IP address. Maxbox can deal with sub-agents and with users, the higher the specifications of the device, the more cards it has created (4000~5000 users). Apart from the Maxbox or programming for the Mikrotik site, we can create profiles (categories 20$, 35$, 40$ etc.), but the basic idea of Maxbox as well as CLI or other software is that they all need to write a lot of codes, time and effort to create only one card while Maxbox specifies profiles, download, upload and choose one of the three protocols (Broadband, Hotspot or user manager) and creates the required number of cards for internet service at a very short time.

3. METHODOLOGY

3.1 INTRODUCTION

This chapter of the research includes an explanation about API and its goal, as well as how to design the program with the reasons for choosing it and different it with other programs, Also the application programming language and the reason for choosing it, the reason For choosing Mikrotik and how to access it via API, also requirement of project.

3.2 SIMULATION SETUP

The API is a collection of subset definitions, Protocols, and software building tools, specified methods of communication between different software components, the object of the application programming interface of the API is to hide the programming and method of writing codes, for example, Facebook allows the application programming interface API for sites to log in via it without the need to build a log-in system from scratch, so when you want to add this addition to your site, you will not know how to build it, but what matters to you is how to use it to add it to your site or application. As we know every application needs setup, this program has been setup by Microsoft Access by creating a database on it previously, we have been chose Microsoft Access Because it is safe, fast access, simple and has the ability to make interfaces.

Figure 3.1: The work of API [25]

3.3 JUSTIFICATIONS

The router that we chose is Mikrotik, the idea of choosing Mikrotik company instead of Cisco, Huawei and Juniper because Mikrotik supports the feature of the billing system as well as other companies in addition to that Mikrotik supports the wireless feature. We may be wondering whether can we access the program or a group of devices and link them in ways other than API, it is possible to access via FTP, SSH, Telnet and the browser (WWW), but it's all work and deal with Command Line interface (CLI), that its need to write a lot of codes, the API is easily accessible to any Program directly by Its programming has been setup previously.

3.3.1 The Reason of Choosing API

1. For machine to machine communication (e.g. exchange rate, provisioning, single sign on, etc.).
2. For automation (e.g. Facebook login, twitter login, etc.).
3. To develop advanced services (Uber, gojek, Google map API, etc.).
4. For security limitation of access rights.
5. Many other reasons.

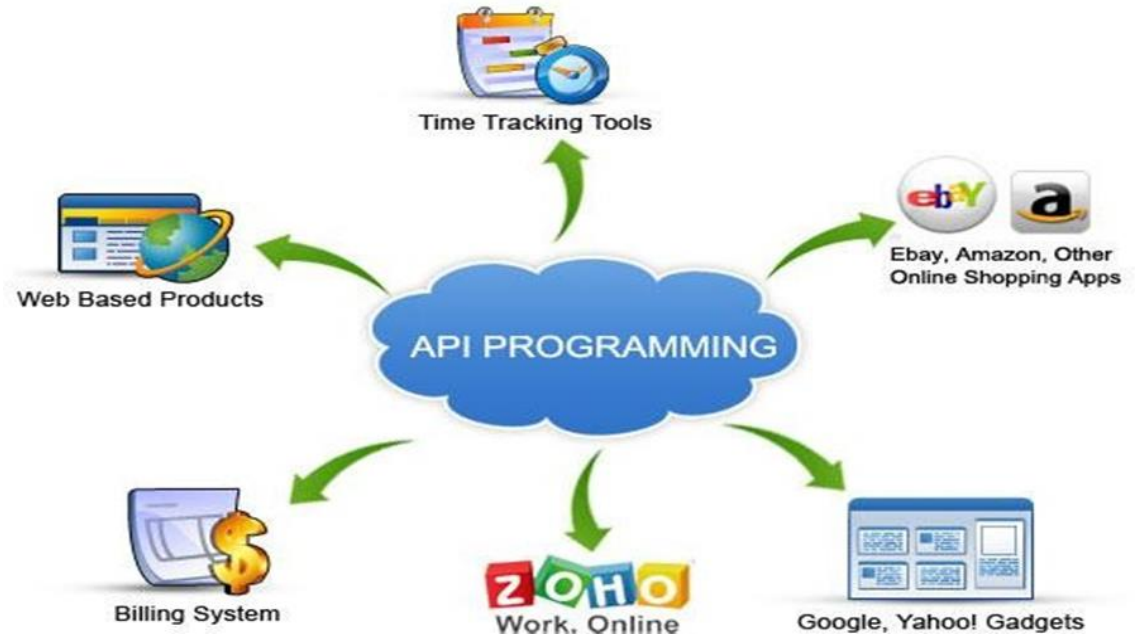

Figure 3.2: API deal with a lot of applications [25]

3.3.2 The Reason of Choosing Mikrotik the API

1- Security: define more fine-grained security, indirect access to the devices.
2- Provisioning: add, delete and update user.
3- Monitoring.
4- Develop a new service (Facebook login, single-sign-on, etc.).
5- Communicate with external application (e.g. billing system, monitoring, self-service application).
6- API is more rigid and consistent (suitable for machines). Unlike SSH (SSH is for human interface).

3.3.3 Access Mikrotik via API

1- You need to understand programming language. E.g. PHP.
2- You need to provide a middle server that connects to mikrotik devices.
3- Make sure no firewall is blocking the mikrotik API.
4- API service need to be activated.
5- Make sure the user has API privileges.
6- Tips: only allow specific IP address that can access mikrotik API.

3.3.4 Requirement of Project

1- create database by using Access Microsoft.
2- Using visual studio program to deal with the database.
3- Using Mikrotik system and interface it with the application by using API application programming interface.

4. SIMULATIONS RESULTS

4.1 OVERVIEW

In this chapter we will introduces and discuss that results which obtained through the proposed method which explained it in the project, Simulation the results of the create and distribute users via three protocols, user manager, broadband and hotspot.

4.2 SIMULATION

First we login router by connecting it to the WAN cable where the internet service is entering by it, we buy internet packages from the public company ISP by optical fiber, link wireless or others.

Figure 4.1: Router board RB433

Then we login the router to do the routing through either winbox or private programming through a copy of the operating system OS which provided by Mikrotik company to configure of setting hotspot and broadband as well as activating User Manager as we mentioned previously that it combines hotspot and broadband simultaneously (that's mean you can have a ppp or hotspot through the distribution system).

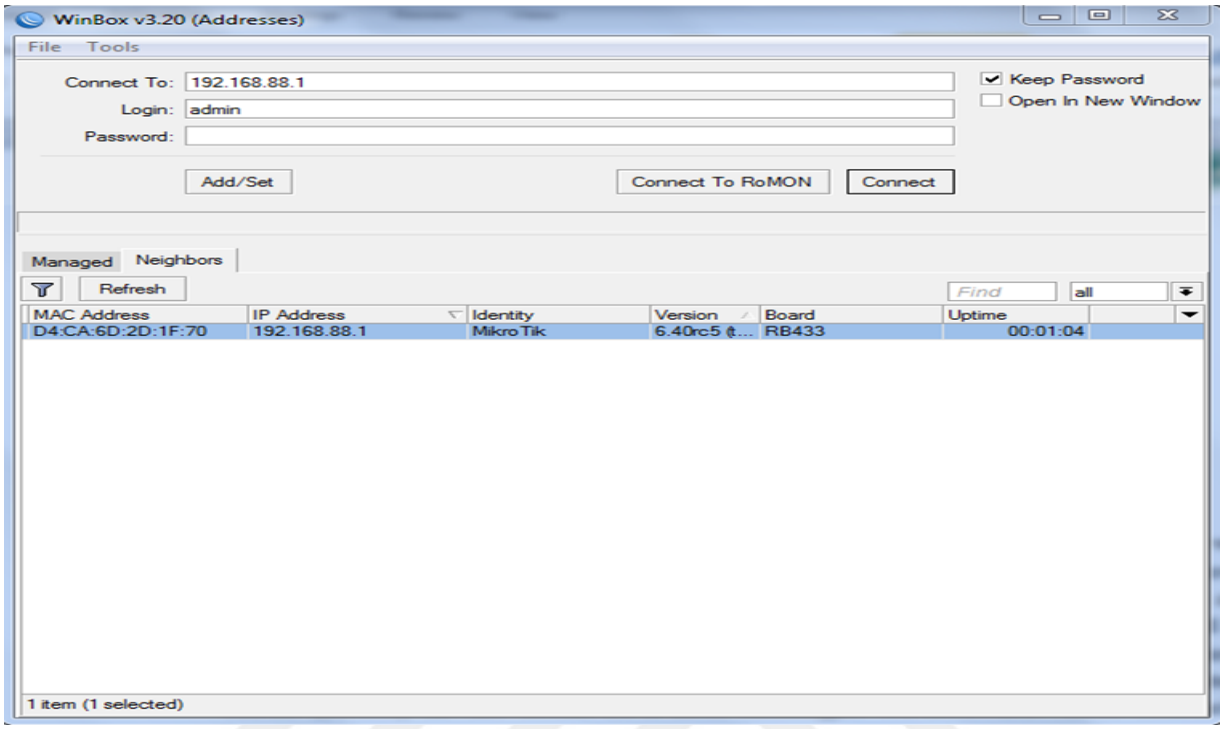

Figure 4.2: Winbox program the information of router: Mac address, IP address, Identity, Version, Broad and Uptime

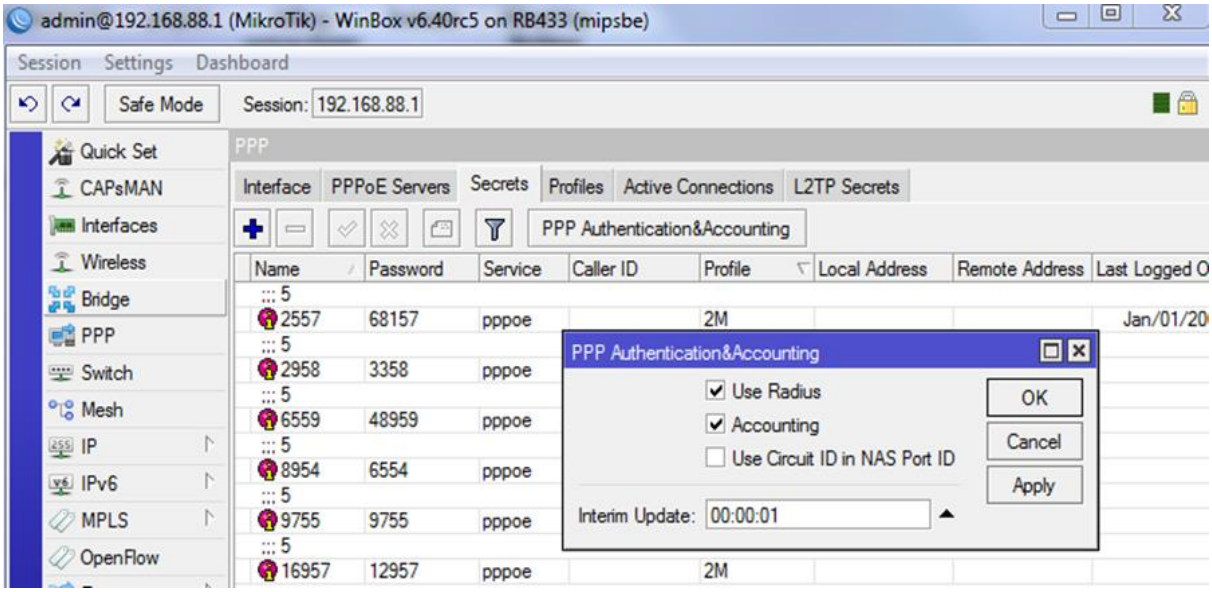

Figure 4.3: Then Activating User Manager it combines hotspot and broadband simultaneously.

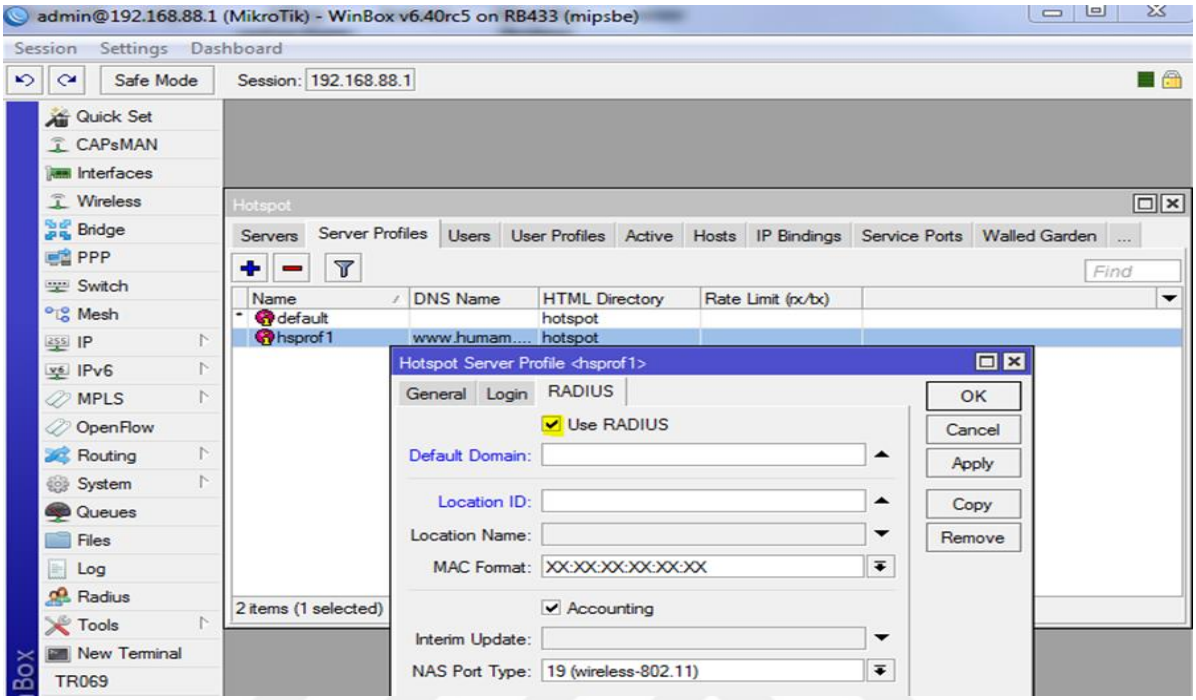

Figure 4.4: Then Activating User Manager it combines hotspot and broadband simultaneously

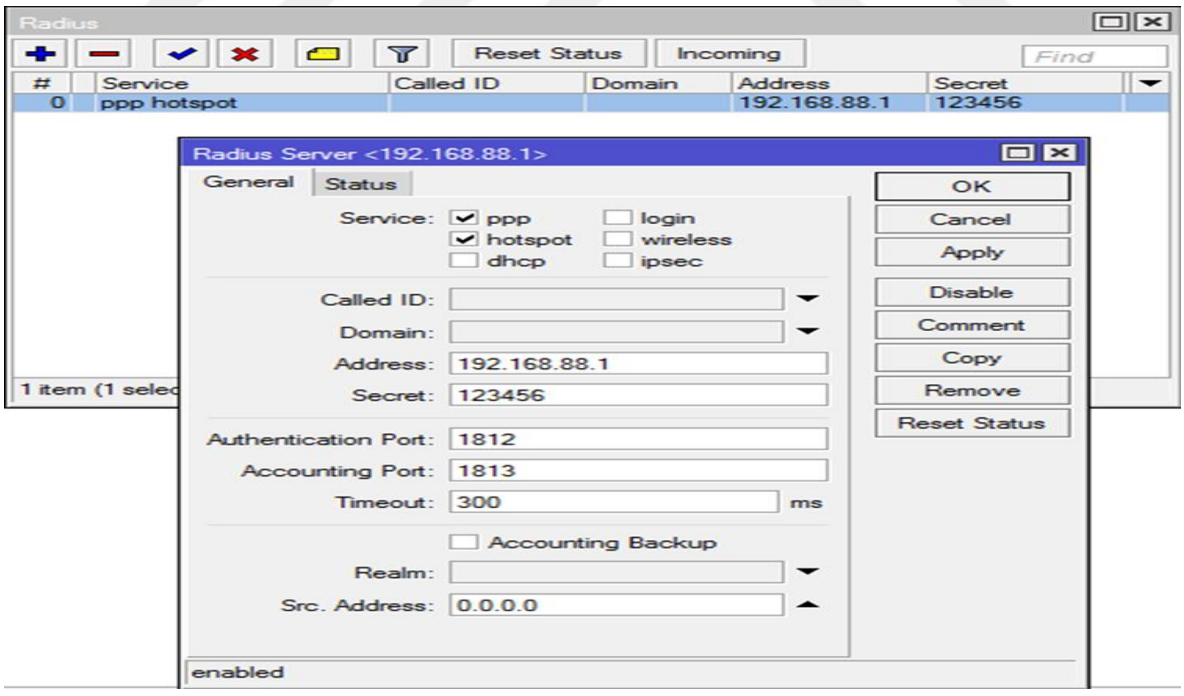

Figure 4.5: Then Activating User Manager it combines hotspot and broadband simultaneously

4.2.1 Create and Distribute Via a User Manager

To distribute the Internet service by LAN to sub-agents or users Whatever it is, to create cards (users) in the form of a user manager we activate "user radius".

First open the application (Maxbox). IP address here means the IP mikrotik router that we have been need to access.

Figure 4.6: Create and Distribute Via a User Manager (Application of maxbox).

Application options:

User number: means number of users who need internet service.

The number: means the beginning of the packet's number (e.g. 123……245).

Then choose: one of the three protocols (pppoe, hotspot and user manager).

Profile: means the categories previously configured (e.g. download, upload) by the winbox's program.

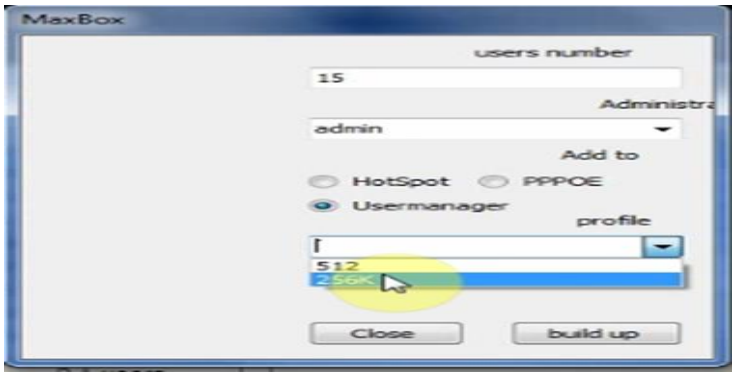

Figure 4.7: Create and Distribute Via a User Manager (The options of application)

Here 15 cards (users) were created in just seconds, these usernames and passwords e.g. (username 77541, password 42341).

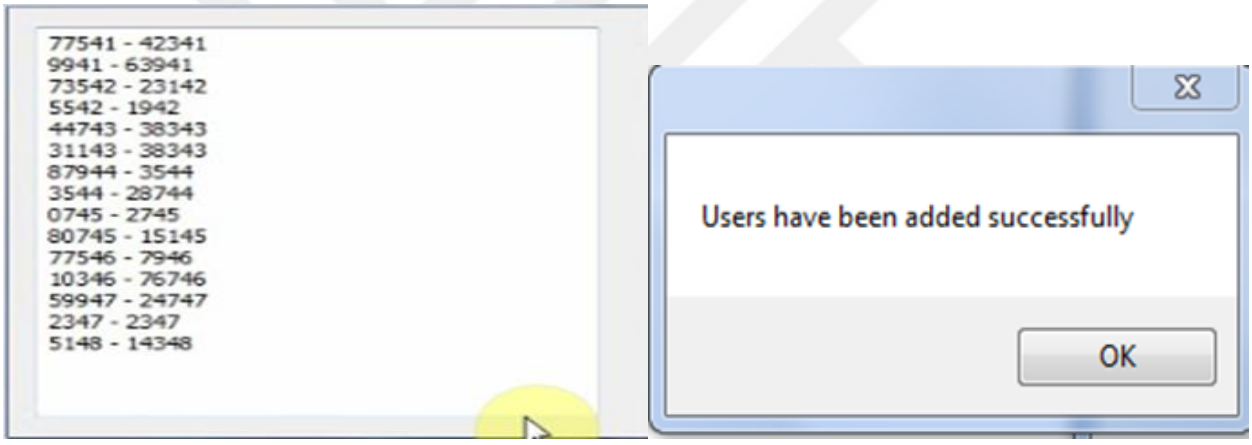

Figure 4.8: Create and Distribute Via a User Manager (Created username and password)

Figure 4.9: Create and Distribute Via a User Manager (Program entry browser)

Note: we could determine all of the users or that need activation

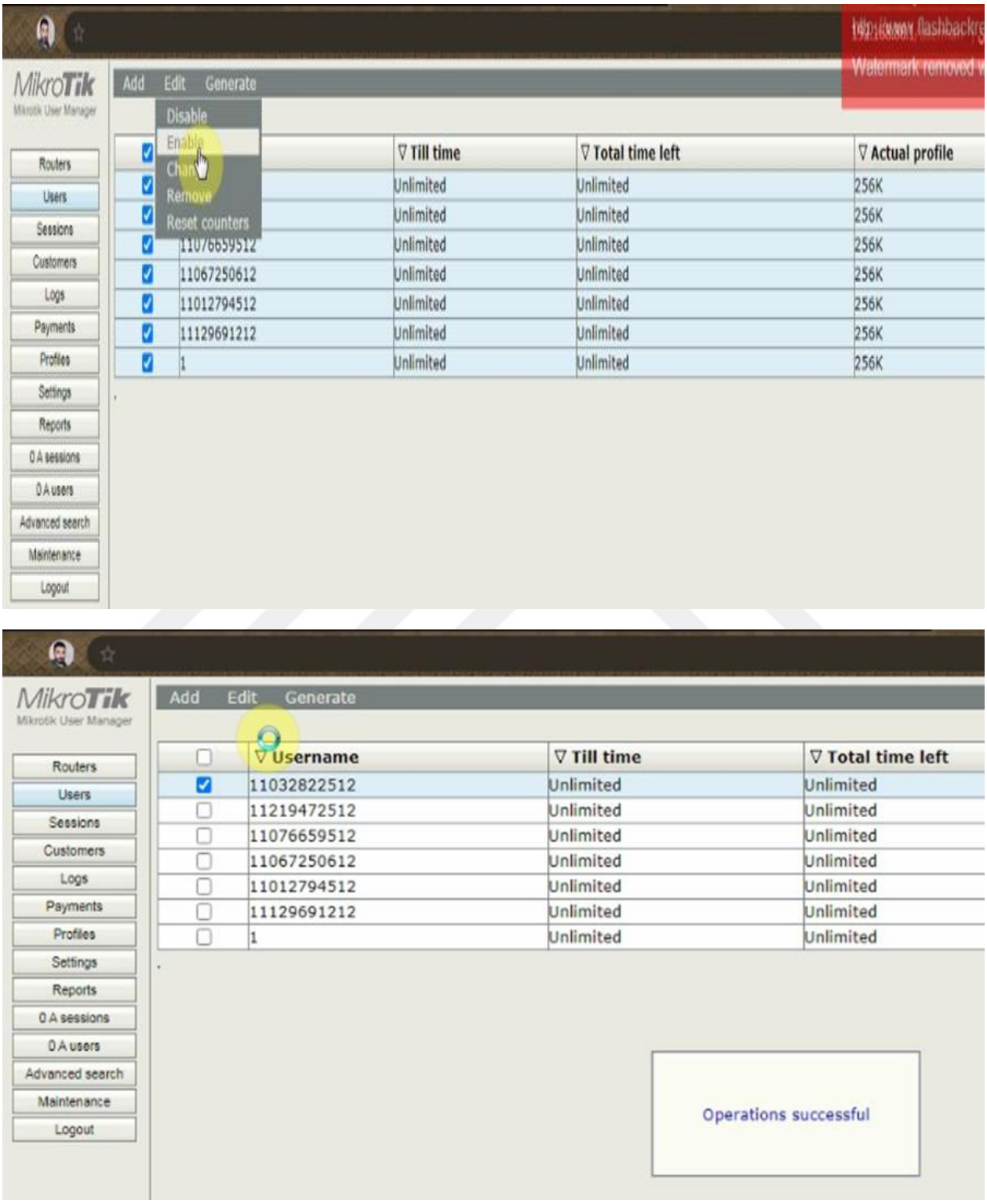

Figure 4.10: Create and Distribute Via a User Manager (Enable and disable)

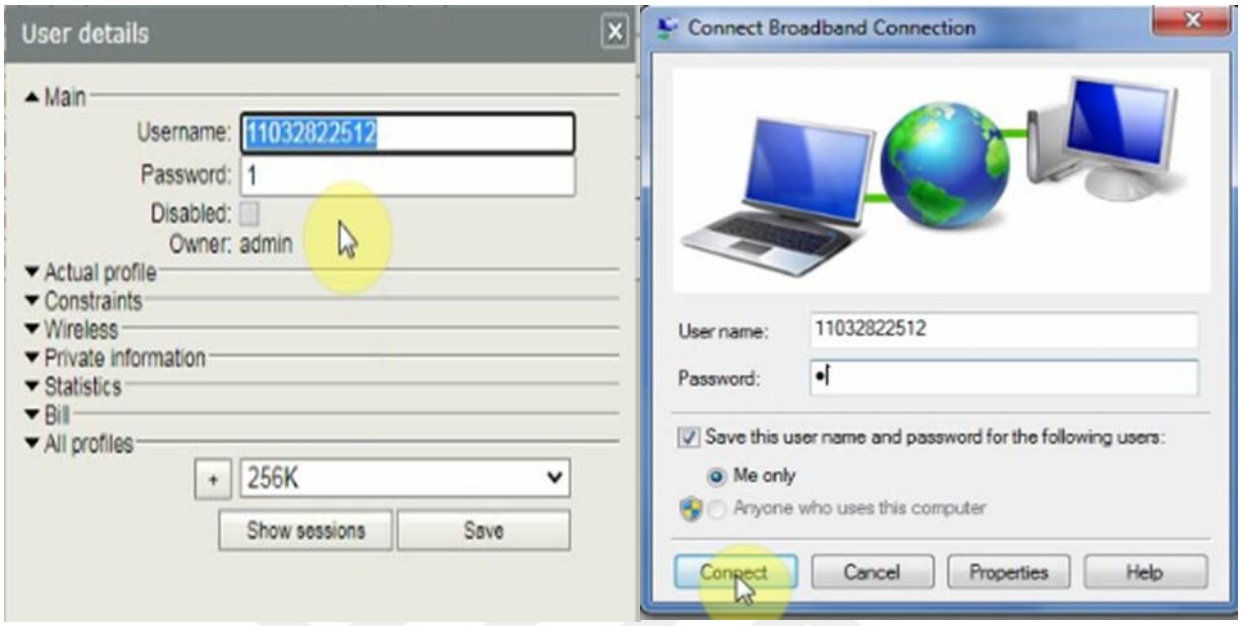

Figure 4.11: Create and Distribute Via a User Manager The Connection

4.2.2 Create and Distribute Via a Broadband Protocol

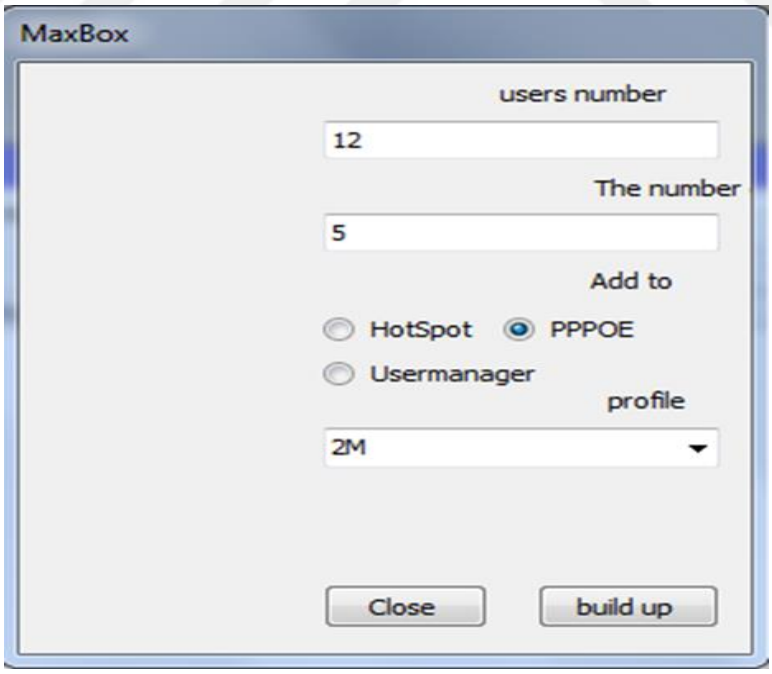

Figure 4.12: Create and Distribute Via a Broadband Protocol (Options of program)

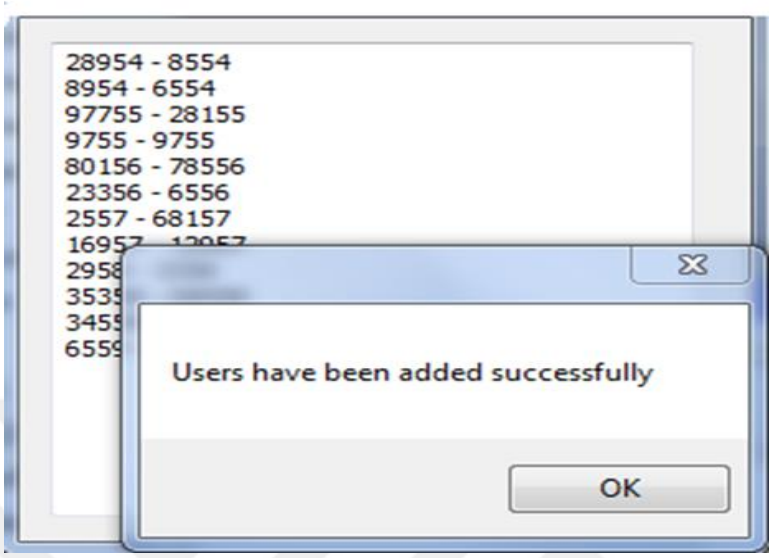

Figure 4.13: Create and Distribute Via a Broadband Protocol (Created username and password)

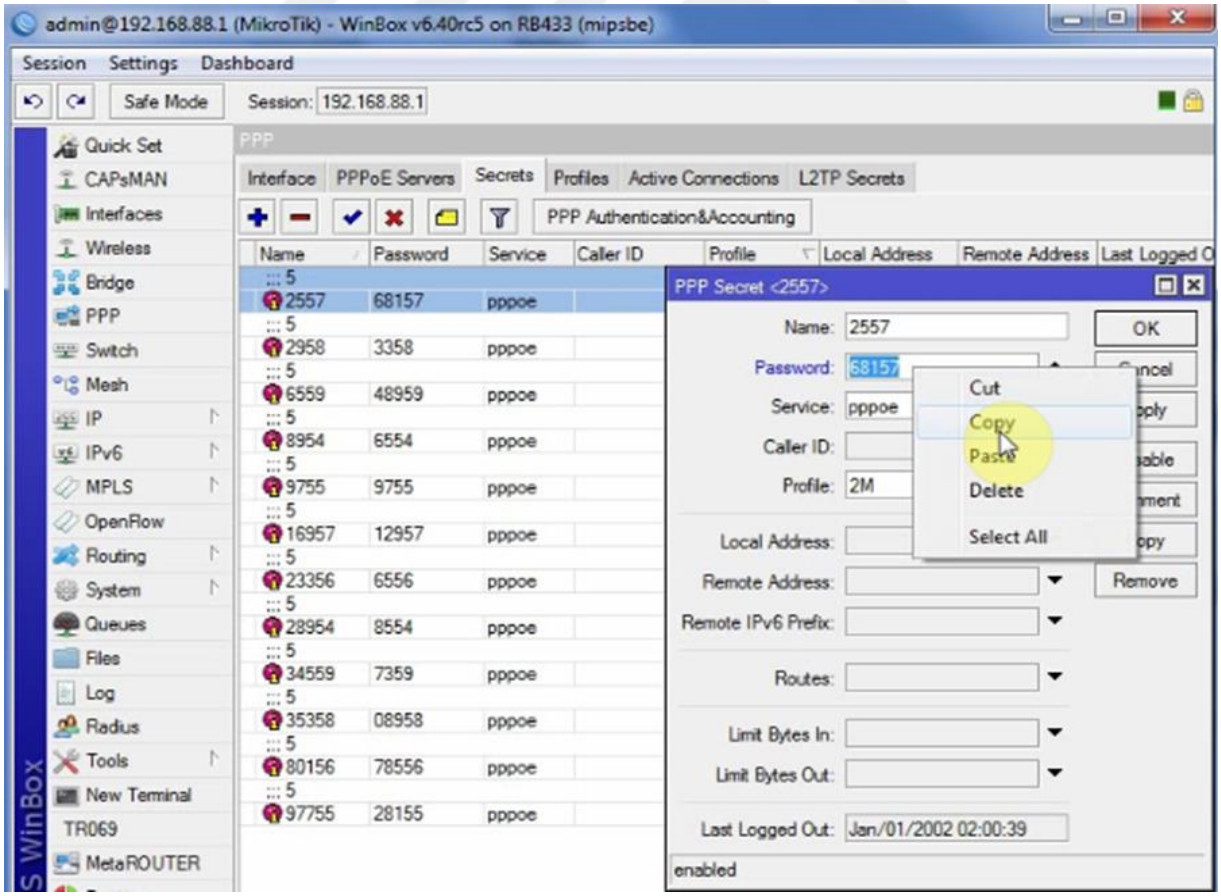

Figure 4.14: Create and Distribute Via a Broadband Protocol (Login by username)

Figure 4.15: Create and Distribute Via a Broadband Protocol (This connection)

Figure 4.16: Create and Distribute Via a Broadband Protocol

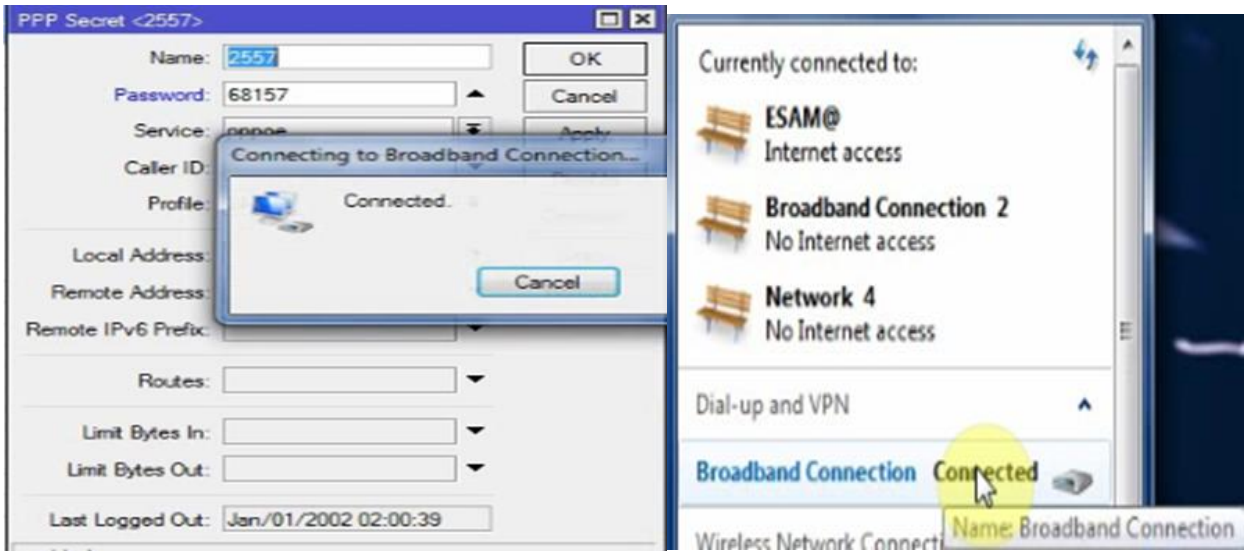

Figure 4.17: Create and Distribute Via a Broadband Protocol (Successful connection)

4.2.3 Create and Distribute Users Via a Hotspot Protocol

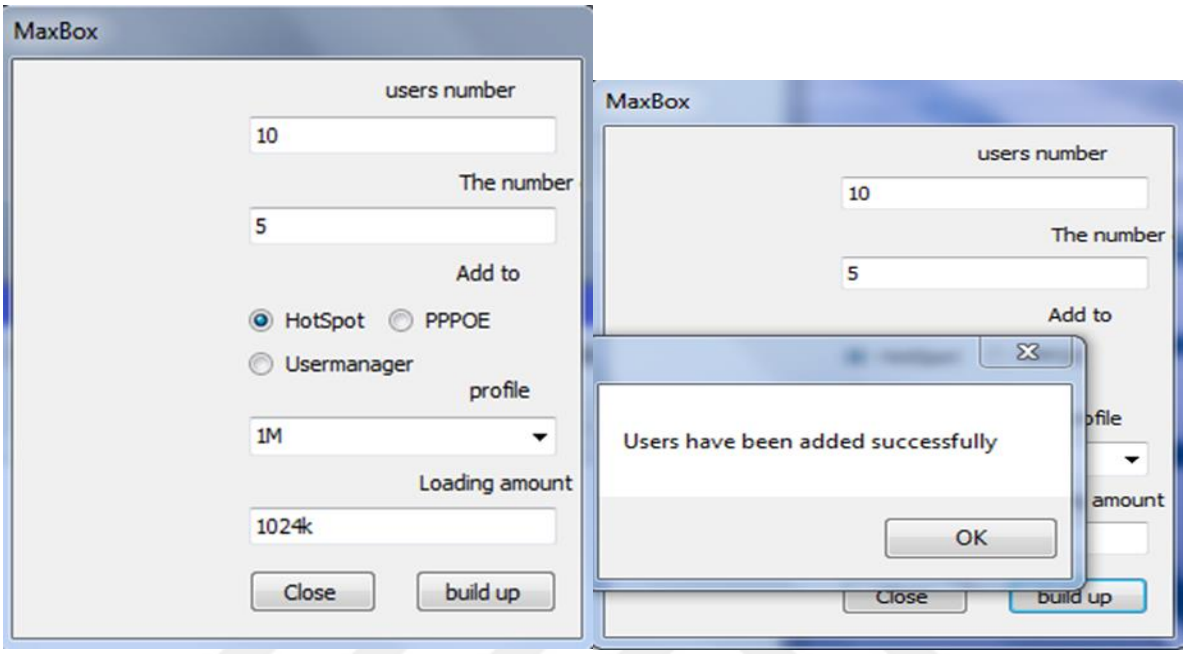

Figure 4.18: Create and Distribute Users Via a Hotspot Protocol (Options of program)

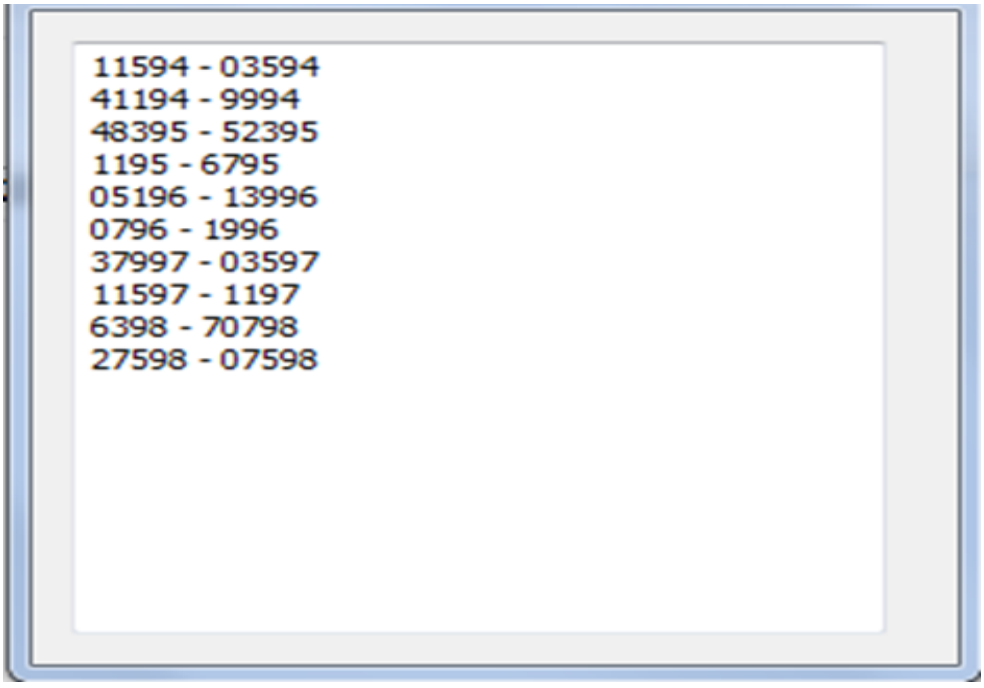

Figure 4.19: Create and Distribute Users Via a Hotspot Protocol (Created username and password)

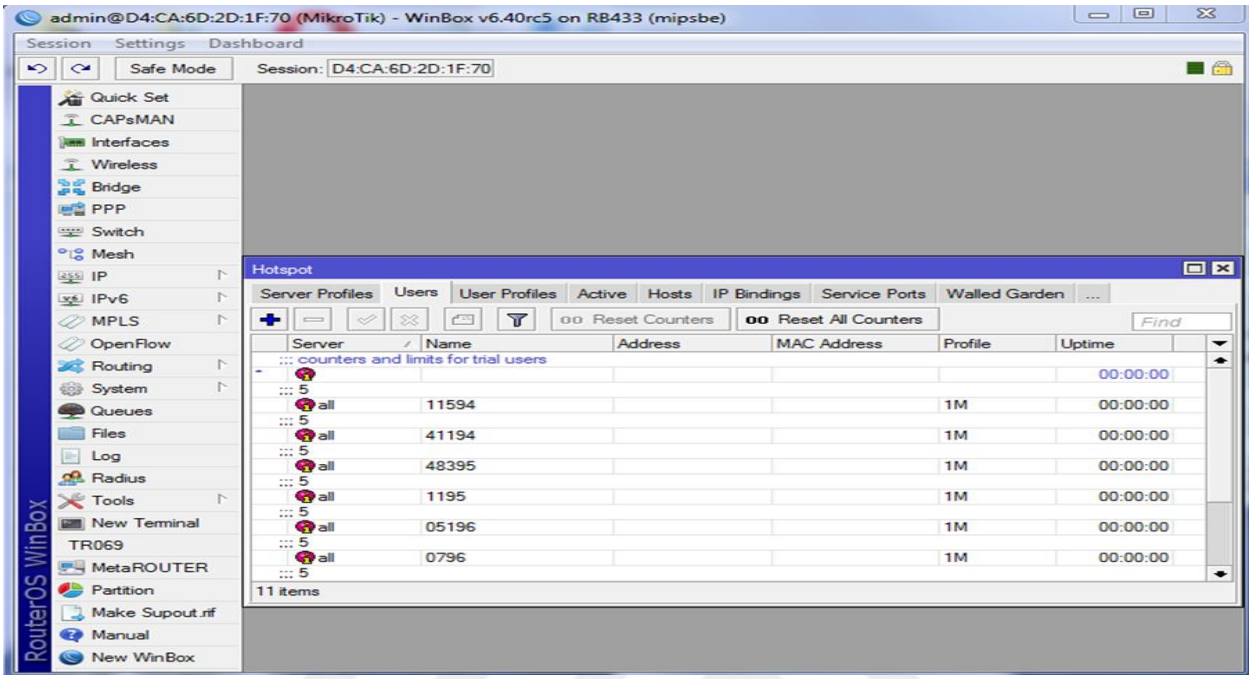

Figure 4.20: Create and Distribute Users Via a Hotspot Protocol (Done creation)

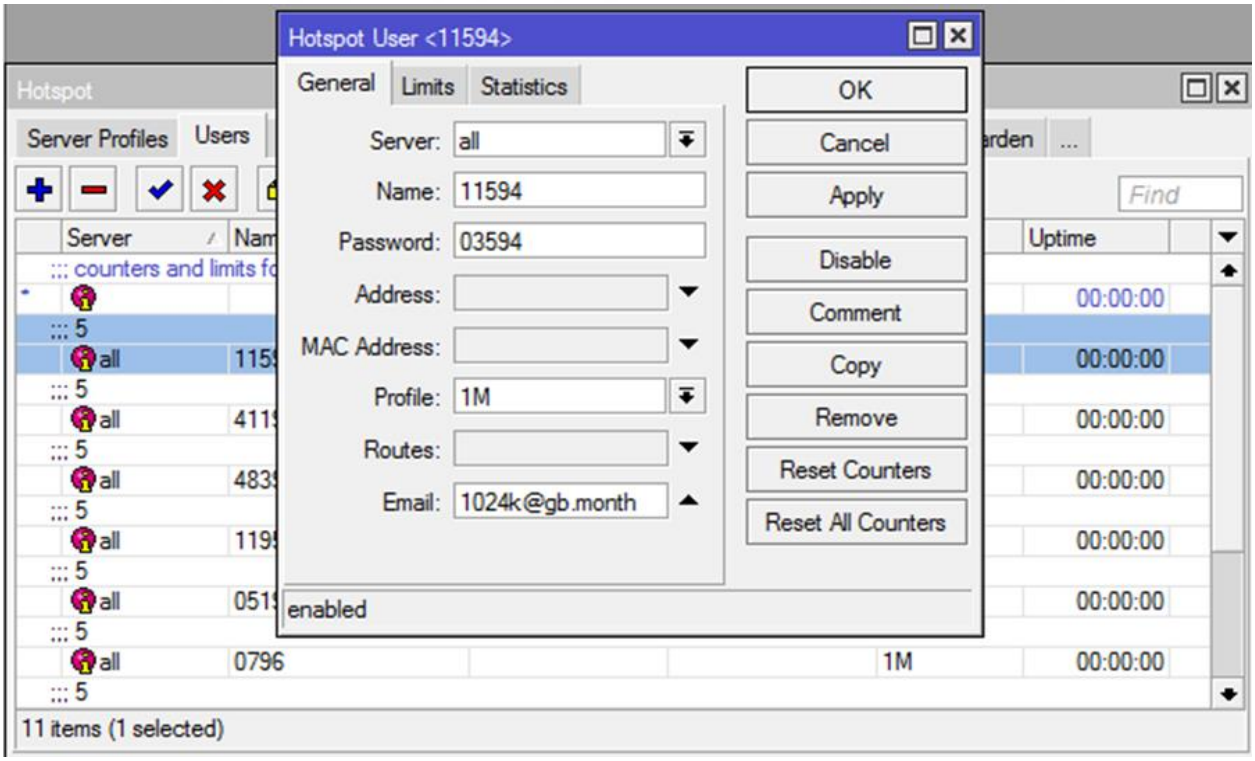

Figure 4.21: Create and Distribute Users Via a Hotspot Protocol

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

The ever-growing scale and complexity of networks makes managing more and more complicated. Here is our approach to investigate the network management framework maxbox function. We presented a case study after a first overview of the features and potential advantages of network management systems wherein we have explained the architecture and design of a system based on Billing System because it’s also a network management system for the specific case of configuration management. The implementation has been tested successfully. As mentioned in the practical section, certainly we had been extend the configuration management features already implemented to Eliminate the obstacles and difficulties that the network manager was facing in dealing with the mikrotik system by creating new tools and programs that are not present in the mikrotik, linking them to the system and creating interactive and easy interfaces.

5.2 FUTURE WORK

Our work is intended to be a case study to build complex network management systems API. The expertise gained in designing the network management program, We hope to be able to provide this to build this system compliant management station which will act as a proxy for the devices it manages, In addition we are able completely edit and print Internet cards, Add the secret feature to manage the device without admin, Automatic update feature of the router, Access to user's devices and Borrowing service. These are yet another area that we would like to work on and publish the results.

REFERENCES

[1] V. Poosala, P. L. Bohannon, M. Kamenetsky, D. V. Hester, and C. A. Daniels, "Internet service provider management platform." Google Patents, May 26, 2020.

[2] J. Stevenson and S. Baker, "References', Refugees in Higher Education (Great Debates in Higher Education)." Emerald Publishing Limited, 2018.

[3] S. O. Al-mamory, J. K. Alwan, and A. D. Hussein, *New Trends in Information and Communications Technology Applications: Third International Conference, NTICT 2018, Baghdad, Iraq, October 2–4, 2018, Proceedings*, vol. 938. Springer, 2018.

[4] P. Mollick, S. Biswas, A. Halder, and M. Salmani, "Mikrotik Router Configuration using IPv6," *Int. J. Innov. Res. Comput.*, vol. 4, no. 2, pp. 2001–2007, 2016.

[5] K. L. S. Clair, E. Pineda, and E. Garcia, "A Study to Evaluate the Success of Digicel's Mind Billing System on its Internal Users," *J. MIS@ UB*, vol. 4, no. 1, 2020.

[6] S. A. Rosano, B.-E. Kerola, P. Ow, and D. M. Lohman, "Integrated file structure useful in connection with apparatus and method for facilitating account restructuring in an electronic bill payment system." Google Patents, Sep. 26, 2017.

[7] R. Gupta and S. K. Muttoo, "Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA.," *Netw. Protoc. Algorithms*, vol. 8, no. 4, pp. 1–28, 2016.

[8] M. Rudolf, S. G. Dick, T. J. Hunkeler, S. A. Rahman, and J. A. Kwak, "Method and system for transferring information between network management entities of a wireless communication system." Google Patents, Aug. 08, 2017.

[9] P. Bagga and R. Hans, "Mobile agents system security: a systematic survey," *ACM Comput. Surv.*, vol. 50, no. 5, pp. 1–45, 2017.

[10] M. Zubair and U. Manzoor, "Mobile agent based network management applications and fault-tolerance mechanisms," in *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, 2016, pp. 441–446.

[11] Z. Ben Yahya, F. B. Ktata, and K. Ghedira, “MA-MOrBAC: A Distributed Access Control Model Based on Mobile Agent for Multi-organizational, Collaborative and Heterogeneous Systems,” in *International Conference on Risks and Security of Internet and Systems*, 2017, pp. 101–114.

[12] C. Devece, D. Palacios-Marqués, M.-Á. Galindo-Martín, and C. Llopis-Albert, “Information systems strategy and its relationship with innovation differentiation and organizational performance,” *Inf. Syst. Manag.*, vol. 34, no. 3, pp. 250–264, 2017.

[13] J. J. Lavín Montes, “Estudio para la implantación de infraestructura Wi-Fi en el parking público del Aeropuerto Seve Ballesteros–Santander,” 2019.

[14] M. A. Khan, “Autonomic network Management,” *5G Radio Access Networks Cent. RAN, Cloud-RAN, Virtualization Small Cells*, p. 185, 2017.

[15] C. Sauer, M. Sliskovic, and M. Schmidt, “Flooding-based network monitoring for mobile wireless networks,” *J. Commun.*, vol. 14, no. 10, 2019.

[16] L. A. Clemm, Y. Chandramouli, S. Krishnamurthy, and S. Srinivasa, “Network embedded framework for distributed network analytics.” Google Patents, Mar. 31, 2016.

[17] R. B. Agnihotri, N. Pandey, and S. Verma, “Analysis of behavior of MAC protocol and Simulation of different MAC protocol and proposal protocol for wireless sensor network,” in *2018 4th International Conference on Computational Intelligence & Communication Technology (CICT)*, 2018, pp. 1–6.

[18] G. C. Sankaran, “Method and system for detecting changes in a network using simple network management protocol polling.” Google Patents, Oct. 18, 2016.

[19] F. Smith and G. Ingram, “Organising cyber security in Australia and beyond,” *Aust. J. Int. Aff.*, vol. 71, no. 6, pp. 642–660, 2017.

[20] D. Chumachenko, K. Chumachenko, and S. Yakovlev, “Intelligent simulation of network worm propagation using the code red as an example,” *Telecommun. Radio Eng.*, vol. 78, no. 5, 2019.

[21] Y. Zhou, Y. Zhou, S. Chen, and O. P. Kreidl, “Limiting Self-Propagating Malware Based on Connection Failure Behavior through Hyper-Compact Estimators,” *arXiv Prepr. arXiv1602.03153*, 2016.

[22] N. Katin-Borland, “Cyberwar: A real and growing threat,” in *Cyberspaces and Global Affairs*, Routledge, 2016, pp. 29–48.

[23] M. Khari, G. Shrivastava, S. Gupta, and R. Gupta, “Role of Cyber Security in Today’s Scenario,” in *Detecting and Mitigating Robotic Cyber Security Risks*, IGI Global, 2017, pp. 177–191.

[24] J. Jacobs, S. Romanosky, I. Adjerid, and W. Baker, “Improving vulnerability remediation through better exploit prediction,” *J. Cybersecurity*, vol. 6, no. 1, p. tyaa015, 2020.

[25] M. I. Mazdadi, I. Riadi, and A. Luthfi, “Live Forensics on RouterOS using API Services to Investigate Network Attacks,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 2, 2017.