**Authentication, Authorization and Accounting (AAA) in Wi-Fi Hotspot's Environments**

**Student Name:** Haroon Shah

**ID**: 21005330

**ABSTRACT**

Internet is the backbone for every organization and personal use. Internet network has been designed differently to establish connection and access to the world via a particular device such as a Laptop and Mobile phone etc. Wireless LAN (WLAN) is now a days popular and rapidly growing technology for day to day and official use. WLAN is more needed technology than the wired network as it gives a user many facilities and secure connections to a user devices and daily data usage. WLAN could be more restrictive than other networks as a person can have more feathers and technology regarding device configuration and end-user devices. There are different brands with different feathers designed according to the users. The team is going to discuss the technology that could be used as a wired and wireless network, depending on the network size and frequency confliction measures. Hotspot is the only solution that makes a person connection more secure and authentic using AAA (Authentication, Authorization and Accounting) server. According to this dissertation, the team will be doing and setting up all the hotspot environments with the AAA Billing system. The hotspot system plays an important role while the team talk about secure internet access and gives a person a great range of communication securely. My practical work uses VMware (VMware Workstation) and EVE-ENG (Software that the team can run real-time router and switches) to run the switches, router and PC in real-time. Moreover, the MIKROTIK USER-MANAGER acts as AAA while the same MIKROTIK the team will use as a Hotspot NAS (Network Access System) The team have designed the scenario that can provide a real-time test and demonstrate that how the real AAA system with hotspot works and the scratch card batch (could be thousands of cards). The team set up all the routers, a switch, and PCs in EVE-ENG software to obtain this purpose. The Solution the team are adopted here is just an example for Authentication, Authorization and Accounting. AAA could be used for different scenarios and purposes. There are many examples where AAA is using such as utility top-up, mobile top-up and contactless card transaction even online shopping. But the team have wrapped all the scenarios in this practical work to illustrate the real AAA and its benefits. This project has been designed for BBS (Bright Better ICT Solutions) company that provides hotspot internet services.

**TABLE OF CONTENTS**

[1.0 INTRODUCTION 5](#_Toc92298090)

[1.1 Context of the project 5](#_Toc92298091)

[1.2 Rationale of the project 6](#_Toc92298092)

[1.3 Research Problem 7](#_Toc92298093)

[1.4 Dissertation aims and objectives 7](#_Toc92298094)

[1.5Structure of dissertation 8](#_Toc92298095)

[2.0 RESEARCH 9](#_Toc92298096)

[3.0 PROPOSED ARTEFACT 10](#_Toc92298097)

[4.0 BUSINESS MODEL 11](#_Toc92298098)

[4.1 Initial Classification, Installation and Hypothesis 11](#_Toc92298099)

[5.0 Athentication, Authorization and Accounting(AAA) Practical Implementation 17](#_Toc92298100)

[5.1 AAA server Installation and Configuration 19](#_Toc92298101)

[5.2 Ethernet Connections 20](#_Toc92298102)

[5.3 Accessing the Mikrotik router 21](#_Toc92298103)

[5.4 Installing Aaa Package: 22](#_Toc92298104)

[5.4 Making Profile: 23](#_Toc92298105)

[5.5 Adding NAS ( NAS means the Mikrotik which is providing Hotspot services on the LAN network) 23](#_Toc92298106)

[5.6 Configuration of NAS Router 24](#_Toc92298107)

[5.7 Hotspot configuration: 24](#_Toc92298108)

[5.8 Radius Configurations 26](#_Toc92298109)

[5.9 Management PC Installation: 28](#_Toc92298110)

[5.10 TEST: 29](#_Toc92298111)

[6.0 SECURITY ANALYSIS 29](#_Toc92298112)

[7.0 PERFORMANCE ANALYSIS 29](#_Toc92298113)

[8. CONCLUSION 30](#_Toc92298114)

[8.1 Summary of Project 30](#_Toc92298115)

[8.2 Summary of Results 32](#_Toc92298116)

[8.3 Discussion of the Extent to Which the Aims Have Been Met 32](#_Toc92298117)

[8.4 Discussion of the Extent to Which the Problem Addressed Has Been Solved 34](#_Toc92298118)

[8.5 Future Work 35](#_Toc92298119)

[8.6 Acknowledgment 35](#_Toc92298120)

[References 36](#_Toc92298121)

# 1.0 INTRODUCTION

The wired and wireless network is the backbone of connectivity throughout the world, while the team use them in different scenarios and purposes like LAN and WLAN [1]. The difference between teamen WLAN and LAN is that the WALN just needs a device between teamen router or switches, either a wireless router or an Access point that provides wireless connectivity to devices (Mobile and Laptops). Wired is quite simple and just using a wire directly connected to the device such as a laptop while Wireless is relatively complicated as it uses different technologies to propagate signals [2]. WLAN typically uses IEEE 802.11 technology standards. The main purpose to introduce WLAN is to facilitate the users to use it on Mobile devices and laptops. As before the trending devices the team computer desktops, while it is possible to move around with the networked device without hindrances in connectivity. So, the team can implement AAA on such networks (WLAN and Wired) but not limited, even the team can use it worldwide as the team but the team would implement the public network for it as public network communicate work wide and can be accessed from any corner of the world [3]. AAA system is nowadays very popular, as it is used everywhere in the world, today transaction authentication and accounting use different AAA systems. For Example, if a person travels by tube in London, if a person goes by bus in London, if a person buys something from a shop, if a person does online shopping and even if a person travel by Airlines, they use the AAA system for different purposes, requirements and scenarios.

## 1.1 Context of the project

The three functions (Authentication, Authorization, and Accounting) are abbreviated as AAA. Authentication refers to a process that allows a user to be identified by his data, for example, by login (username, phone number, etc.) and password [19]. Authorization is a process during which the authorization of an identified user to access certain network resources is determined. The term accounting for the used network resources is already quite informative in itself. The primary data that is transmitted over the RADIUS protocol are the volumes of incoming and outgoing traffic during data transmission, and the duration of the conversation and the dialled number when using IP telephony. In addition to the standard attributes (parameters) defined in the protocol, the protocol provides for the use by the equipment manufacturer (vendor) of its own attributes [20]. In the English language literature, they are called Vendor Specific Attributes or VSA. RADIUS is currently used to access virtual private networks (VPNs), wireless (Wi-Fi) access points, Ethernet switches, DSL, and other types of network access. Thanks to its openness, ease of implementation, and continuous improvement, RADIUS is now the de facto standard for remote authentication [21].

If the network is small and has a small number of users, it is easy to monitor access and security, and often a single network administrator is responsible for this [23]. But if an organization has a large-scale corporate network or it is a telecom operator's network with a large number of subscribers, then it becomes impossible to manually track what has access to what. In this case, AAA comes to the rescue, a mechanism that allows for authentication, authorization and accounting of users, that is, control access and record the actions performed [24]. Password authentication is the method that relies on the user to provide a username and password to successfully identify and authenticate to the system. Accounting is a stage parallel with authentication and authorization, which records the success or failure of these processes in the log, whether a person was able to enter the room or not, whether the user gained access to a network device and, if so, what actions he performed on it. This process is important from the point of view of security and access control, as it allows identifying potential threats and look for holes in the system. RADIUS is the IETF standard for AAA [25]. It has been in use since the early 1990s and was originally used for dial-up modem connections. RADIUS is widely adopted and supported by most device manufacturers and software developers.

## 1.2 Rationale of the project

The main purpose for AAA is to reduce human efforts by Authorization, Authentication and Accounting mechanism. A couple of decades ago, buying something from a shop included physically going to the shop and making the purchase through hard cash. Whereas, network digitisation has now enabled this time-consuming process to be compacted in few clicks. This is only possible due to advancements made in the network authentication and authorization technology, as it provides a secure purchase network for all users without intermittent lags in the system. Information and release the purchased item and follow the procedure to be delivered. The same AAA has setup for a person utility facility at home i.e., Gas, Electricity and water [1]. They authenticate, authorize and accounts for a person billing and then provides a person service account to the profile they have designed or at the rate of money as same as a quota system. For example, if a person top up 30 pounds in a person gas meter and a person started using it will be charged from the first flame of fire and it’s called pay as a person go system but still they have given a person a quote for Gas at the rate of 30 pounds, either a person can use it in one month, one day or one-year account to the gas mathematically conversion, I don’t have the all those gas meters and banking stuff to demonstrate this project, So I am using VMware and EVE-NG (network simulator) to put all the project’s requirements together in one place.

This project consists of different software and brands (routers and switches) to be used such as Mikrotik and Cisco and virtual PC. Let me clarify that all the devices and equipment used here will be in real-time but virtually. The firmware and OS will be the same as a physical device, so mean to say that the project would be a real project through the virtualization process. The team will implement the AAA concept on Wi-Fi hotspot services with AAA billing server and Hotspot router. A quick introduction to all equipment’s tasks is: AAA will be doing Authentication, Authorization and Accounting Hotspot router will provide the login page to the users where these all devices are mutually connected in same Network prefix and PCs representation either as a mobile device or laptops etc., the team will be using two Cisco L3 switches as the team to maintain and establish connectivity between teamen these devices. This project has also many security measures, depending on the configuration of the device and the parameters a person uses for the configuration of the routers and switches. So, this kind of internet service is not just limited to hotspot services but also can be implemented in ISP (Internet Services Providers) who may have commercial and domestic users, it may connect, discount, provoke and suspend a user according to the profile settings in the AAA system. The rest of the work would be demonstrated in practice and all the configurations the team have set it up. AAA deliver a great opportunity to provide secure authentic, authorized and accounted services to the end-user. It’s been calculated with any errors.

## 1.3 Research Problem

In this research paper, the team will be discussing the search that the team have done about the current and previous status of AAA and hotspot and the whole process of investigation throughout the research. The growing development and use of hotspot, either in public or in other places (commercial or personal) became the demanded technology providing the high-level security and availability of the services. Before, in 2000 there was dialup system using the AAA system [4]. The dialup just uses the windows feature to be connected to services. The first RADIUS server was designed in 1991 for a university to connect and authenticate the users and later on, after a considerable number of meetings, the real Radius was introduced in 1997 and then converted to a standard arena and there is no end of AAA Radius server, as propounded by Merit and John Vollbrecht [4]. AAA is the accounting and auditing system that audit and apply a few policies to overcome the need of commercial and computing filed in term of Internet access. The team can use AAA with radius manager in various platform over Routing, Switching and V-LANs, it is heavily dependent on the need of the user, as the team also can use it over the V-LANs with Cisco V-LAN Trunking protocol for reliable and flexible communication as, the use of routing in any network makes the network fast and more reliable. Therefore, using hotspot with AAA could be used at any environment. It asserted that in AAA the team can use different radius software such as Aradial, Radius manager etc. Aradial uses a wide range of Telecom field i.e., GSM, ISP Management, HTTX and other services that provide high security [3]. The Radius software actually depends on the requirement and many other features that every Network Engineer should compare. The whole system is a set of rules and configuration that a person has to follow and configure according to a person requirement. For example, a person may have a big ISP network and a person have to set all a person network from manual setup to AAA a person may have to add client in the AAA and design a profile for each client or same profile for the same demander clients. The Radius AAA might have many features but some of the core features are client, the overall network security, reliable authentication mechanism and extendable protocol [5]. In this research I have observed that it’s not just about AAA radius server but, the brand like cisco has its own AAA service for big size network like campus network and it’s called TACACS+ servers on other hand there is Mikrotik brand that holds User-Manager services as AAA.

## 1.4 Dissertation aims and objectives

The aim the team pursued was implementing the AAA Billing services as said not just limited to Wi-Fi hotspot. It could be used for every AAA concept but in different configuration mechanisms and technologies. The aim here was to develop a service to perform AAA radius services. The current research revolves around the following objectives:

* To develop a AAA framework for a Wi-Fi hotspot environment
* To propose and assess the product development and business models
* To implement the AAA service radius

## 1.5Structure of dissertation

This dissertation is comprised of 5 distinct chapters:

Chapter 1: It includes introduction, contextualisation of the problem, and aims and objectives of the research.

Chapter 2: It involves extensive review of literature on the topic

Chapter 3: It involves proposal of the product artefact

Chapter 4: It is comprised of explication of the business model

Chapter 5: Authentication, Authorization and Accounting (AAA) Practical Implementation

Chapter 6: Is concerned with the security analysis.

Chapter 7: Deals with the performance analysis.

Chapter 8: It is the conclusion chapter which stresses the summary of project, results, discussion along with future work and acknowledgment.

# 2.0 RESEARCH

TACACS+ was developed by Cisco and is a development of the previous versions of TACACS and XTACACS. Despite the similarity of names, TACACS + has been heavily modified and is not backward compatible with TACACS, which is now practically not used anywhere [28]. The main use of TACACS + is in the administration of network devices, however it can be used for some types of AAA when accessing a network. TACACS + uses Transmission Control Protocol (TCP) port 49 rather than UDP because it is more reliable and provides early warning of potential errors thanks to the TCP-RST packet. TCP is a slower protocol, but has additional advantages: the ability to separate authentication, authorization and accounting as separate and independent functions, multiple authorisations after one authentication [29]. The main differences are that TACACS + encrypt the entire contents of the packet, leaving only a simple header. This method protects against attackers eavesdropping on messages transmitted between devices. Also, TACACS + implements AAA functions separately, which allows putting each of them on a separate server or even use a different protocol (not TACACS +).

RADIUS allows some of this capability, but not as well or as flexible as TACACS +. TACACS + also supports several other non-IP protocols such as AppleTalk, NetBIOS, NetWare Asynchronous Service Interface (NASI), and X.25, but these have been phased out in modern networks [28]. When using the TACACS + protocol, there cannot be a firewall between the client and the server, since the server must receive a request from the client with its IP address, and not with the brand wall address. For RADIUS, the client's IP address is also contained in the packet itself, which allows the AAA server to get it from there. But the biggest drawback of TACACS + is that Cisco developed this protocol for its own needs, and therefore it was the network devices of this company that received the widest support for it [27] However, the situation is gradually changing, and other manufacturers also began to support TACACS +. If it is device administration TACACS + will be the best option and if its network access more versatile and faster - RADIUS.

There are many more brands and AAA servers, some are cheap and some are expensive depending on the current budget and financial strength. The key point about the AAA Radius server is meant to be the same as other but the team have research on the standard key point to illustrate the exact task of AAA. AAA dependent on client interaction and client communicate with AAA service depending on the time a person setting. I could be 1 minutes or 5 minutes to talk to each other. The NAS router and AAA Radius billing system update each other as same as OSPF routing protocol updates the routing table published by O'Reilly Media, Inc.

# 3.0 PROPOSED ARTEFACT

This architecture supports the Wi-Fi hotspot services in airlines, public places, and hotel etc. to provide secure and seamless connectivity to the end-user with different package, profile and speed accordingly, moreover it gives a person the facility to generate a batch of cards that contain the username and password with different prices and quota system provided in the practical. Figure 1 illustrates the architecture design overview.

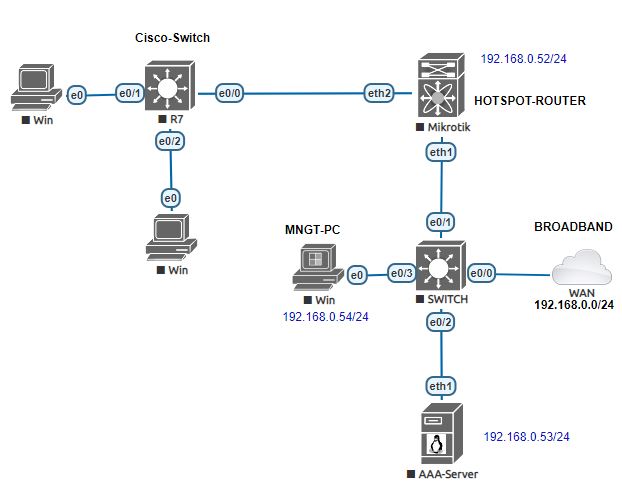


Figure 1. AAA Hotspot network architecture design overview.

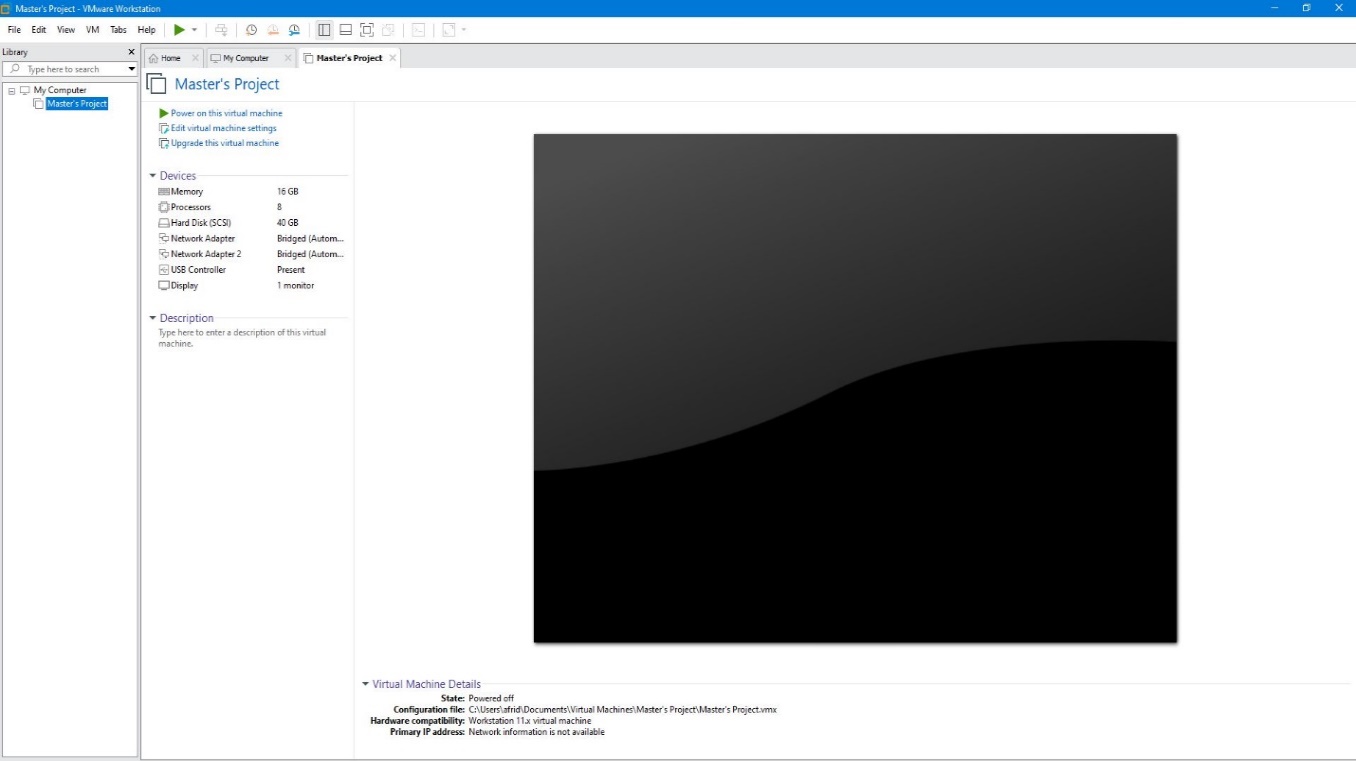
According to the architected design, there are two Miktotik router used, one is NAS and Other as AAA. The Broadband network used as backbone with default Ip prefix provided by virgin media. Moreover, there are two cisco switches, the one providing connectivity to the client PCs and other one connected to NAS-Router, AAA and Management PC. The management PC will manage all the devices operating in the radius on network. The AAA has ability for generate a batch of cards that contains “Username” and “Password” to put in the login page in end user device (could be laptop or mobile device). The whole combination of router and switches and the scenario represents AAA mechanism (*Will be practically demonstrated to supervisor*). For example, a person while walking in a park runs out of cellular data but internet is needed. In such case, the person would search for nearby Wi-Fi connection. The connectivity, generally would not ask for password as it’s already protected and secured by the AAA. He will be then connected to the Wi-Fi after all DHCP process (request, acknowledgment and offer dhcp IP to the end user), A login page will pop up and will ask for user name and password, the person will put the username and password in the login page after buying a scratch card for the service. *(The whole scenario will be discussed in detail with images to demonstrate the architecture in details*)

# 4.0 BUSINESS MODEL

AAA is not limited to use it as a free Wi-Fi but it can be used as business as the team, a person need to pay a certain amount to get access to the service. If a person travel and a person want to user internet service in Aeroplan there may be given a person different option free service as it may have a quota system of max 12MB with a variation of speed. If a person finish his 12MB then they offer 50Mb or 100MB quota to buy. While it is not a business but also a facility on such crucial condition and yes more expensive than normal service. I had made a network architecture for British Military and NATO in Afghanistan from 2013 to 2021 by the time I worked for a Company there. User have to pay for certain service in the public park, airport and different places via they credit card or debit card or may be cash. The subscription may have different price totally depending on the package a person want to buy. The functionality could encompass in a variation of packages that are provided at varying prices. A person may get free air time etc. depending on designed digital marketing.

## 4.1 Initial Classification, Installation and Hypothesis

This type of practical would be exorbitant to demonstrate and time consuming as the team, but the team have used the virtualization process to cope and achieve the aim. At initial stage the requirement of PC or machine that a person is going to install such software, should be strong enough and more RAM in the PC as this software runs the OS of router and switches in Realtime and grab as same RAM and processor as a physical device. In the first stage I have installed VMware that provides the Virtual machine scenario from vmware.com, this software provides a person a virtual platform to add virtual router, switches and pcs. After Installation the RAM was specified, as the team as the disk space and processor to the VMware to take RAM, disk Space and Processor from my Laptop. The taken specifies things would not be used by PC anymore it is reserved to the VMware. Figure 2. demonstrated the exact slot reserved to VMware.



Figer 2. Reserved RAM, Disk Space and Processor for VMware

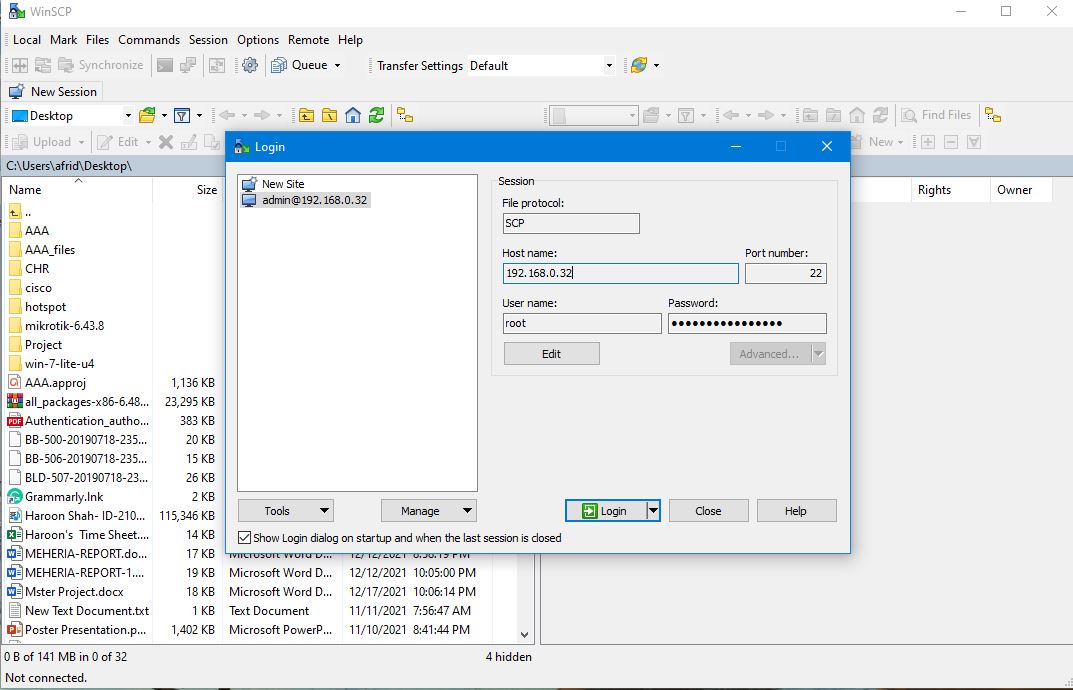
I have allotted 16 GB RM, 40GB Hard Disk and 8 core Processor to VMware from my PC. Moreover, I have bridged the Broadband Internet Wi-Fi to my laptop’s wireless LAN card to provide the same Network access in The VMware.

Sample: Installation VMware, configuration of VMware according to a person need (RAM, Hard Disk and Processor, Auto-Bridge the Wireless LAN to Broadband). The next part is to install EVE-ENG software inside the VMware, it called EVE Community VM. This particular software specially designed for professional network engineer to perform labs and any practical work and reduces having a bunch of physical devices and no financial investment. EVE-NG has capacity to operate many brands equipment such as Cisco, Aruba, FortiGate, Mikrotik etc. in real-time. Open file and select the downloaded EVE community VM and install it in the VMware it will take some time to be installed. Figer 3. shows the exact example of running EVE-NG in VMware



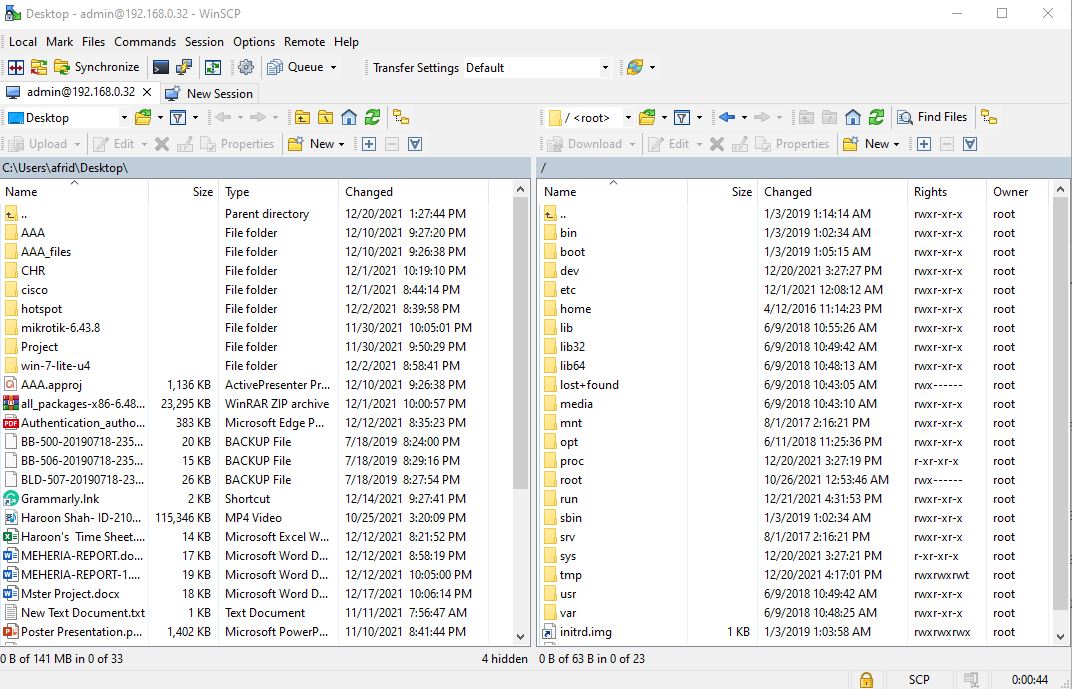
Figer 3. EVE-NG installation in VMware

In this process the EVE-NG will ask a person for root password, admin password and network preferences, either a person want to connect it thru dhcp or static IP, totally up to the person and the person’s requirement. This not just enough to start a person lab in EVE-NG, it’s a long way to get there to start a person 1st lab. After installation successfully, a person needs to upload the firmware and OS (Router, Switches etc.) to the to the EVE-NG’s database in the specified for to be run. For this to perform a person may need a software that transfer the OS to the EVE-NG community, I used WinSCP to transfer IOS to the EVE.NG. a person’s need to access the EVE-NG through root to open its directory and transfer IOS. Figer 4. Shows the setup WinSCP from local disk to EVE-NG.



Figer 4. Shows the setup WinSCP from local disk to EVE-NG

WinSCP is the bridge bet the teamen local drive and the drive the team had selected for EVE-NG. The host Ip is the Ip which had been assigned in the installation process and taken this Ip from the Broadband router through automatic bridge be team laptop’s wireless LAN card and Broadband Wi-Fi. There is a username and password as the team member have setup in the installation of the EVE-NG if a person clicks the login, it will authenticate the username and password and will display EVE-NG directory on a person right and Local PC on a person left. Now a person are able to transfer files. Figer 5. Will show the how to send file through WinSCP.

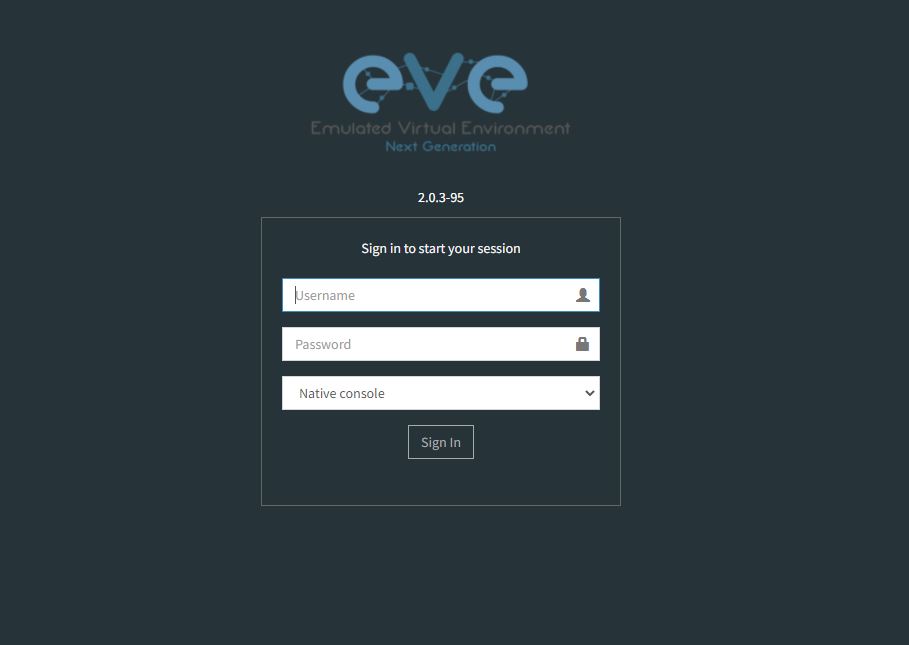


Figer 4. Shows how to send file from local disk to EVE-NG

So, actually the team are transferring file from the local disk to EVE-NG using WinSCP. Windows, and Mikrotik do not requires any configuration as it is a kind of plug and play system but if a person want to add Cisco Files like L2 and L3 switches a person need to wrap it and execute a command to make them work.

Command: /opt/unetlab/wrappers/unl­\_wrapper -a fixpermission

After adding the OS in a specific folder in EVE-NG directory from root then a person be able to work and proceed to the practical work. Then, a person can run the OS in the EVE-NG platform and add the OS of the screen that a person added through WinSCP. After adding OS will display in node section of the EVE-NG with blue color (blue color means its clickable and working. But before a person start a person practical a person need to access the team-base. So, the teamb-based EVE-NG platform will be accessible the IP address got by the EVE-NG in initial stage of installation such as 192.168.0.32. The EVE-NG the team-base will show up after putting 19.168.0.32 in the browser. Figer 6. Demonstrate the how it can be achieved



Figer 6. Demonstrated the main login page

A person will exactly get what a person want to see after putting the username and password for EVE-NG and get access to the main screen, wherea person can start a personr practical. The first access of the platform uses the defaul setting in the first page i.e name to the project etc.

Moreover, if a person add a Cisco router or switch or any device in EVE-NG a person need to specify the RAM to the device as a person can not assign all the RAM capacity to just one router, because a person has gotten 16BG RAM to EVE-NG here and a person will dividing the RAM to each and every OS or devices. For Example: I have address L3 cisco switch in the EVE-NG and have the capacity of 16GB RAM in all so I would assign 1GB RAM to L3 switch and I have 15GM RAM in reamaining in total. So, this 15GB RAM, I can use for other OS or devices to be added later accordingly.

# 5.0 Athentication, Authorization and Accounting(AAA) Practical Implementation

AAA is a complex framework that is used for intelligently controlling and regulating access to computer resources, information provision for billing services, policy enforcement, and usage in audit processes etc. [6]. All these processes functioning in close coordination are crucial for efficacious management and security of a digital network. In these processes, the stage of authentication is implemented on the concept of identity verification. Hence, conventional as well as contemporary modes of identity verification could be inoculated at this stage. It provides a digital identity to the user usually through an authenticated user name and password before granting of access permission. However, implementation of authentication mechanism is not sufficient for securing digital security [7]. The step of authorisation is followed in which, the user must gain authorisation to execute certain tasks on the network. Hence, authorisation step is used for policy enforcement, which shape the kind of activities allowed on the network and kind of resources being consumed. Accounting is the final component of the AAA architecture, and it keeps track of how much bandwidth a user uses while on the network. The amount of system time or the quantity of data delivered and received during a session are examples of this. Accounting is done by keeping track of session statistics and consumption data. It's utilised for permission management, billing, trend analysis, resource allocation, and data capacity planning for commercial operations [8]. The ClearPass Policy Manager serves as an accounting server, receiving user accounting data from the Network Access Server (NAS). ClearPass Policy Manager must be configured to use the NAS as an accounting server, and the NAS must deliver appropriate accounting information to ClearPass.

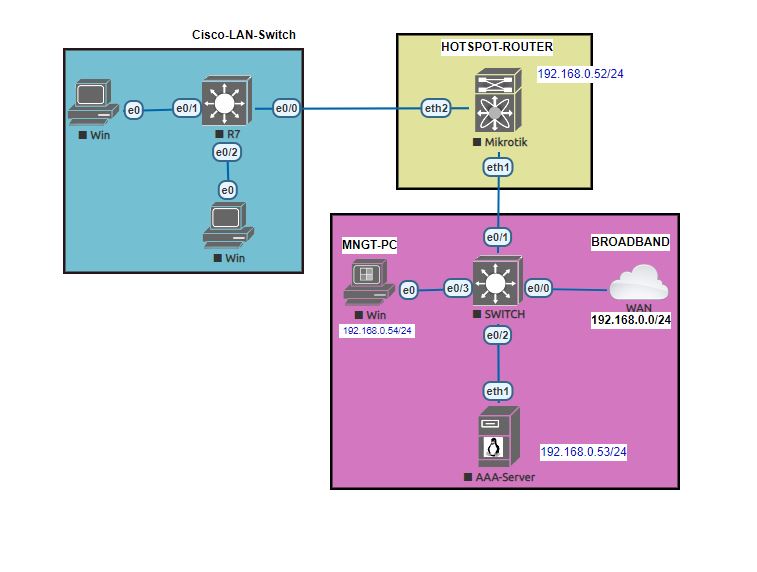
AAA framework could be implemented through either using an external ACS server or using a local database entailing the device. In case of using local data bases associated with the devices, it is necessary to utilise local operating configuration of the routers. Creation of authenticated identities is necessary after which privileges are assigned for each identity according to their access to the network [9]. Whereas, ACS server is a commonly used. When an external ACS server is utilised, it is required to gain confirmation on both the ACS and the router. This step of configuration includes creation of unique user identity, separate customised method list for AAA. Here, the Network Access Server (NAS) conveys and authentication to the ACS server, after which the server takes decision on the basis of the user credentials, whether to allow network resource access to the provided credential or not [9].

This project or Practical is considerably technical and understandable, because a person may have experience with this kind of concept many time while a person travels, visiting any cafe, public parks etc. This practical consist of the same practical and concept to demonstrate how this AAA works in real life, how its authenticate a user, how it authorizes a user and how it account a user. The practical start took place from the initial configuration and setup to make sure everything is the teamll defined to accomplish the desired task. At the first place, may take just 10 minutes to be done and understanding may take more time as usual. It’s basically GUI configuration, easy to deploy. i.e. LAN bridge to local wifi to access to internet inside the EVE- NG by providing the Ip from same prefix, assigning disk space and RAM.

There are different techniques in EVE-NG, the one option for devices to be added to work on and the other is clouds(not online cloud services) basically, cloud refers here the main backbone service to a person EVE-NG such as a personr local broadband etc. here the team use local broadband but in big size networks it could be fiber optic, cloud service or any public network who may work on BGP, OSPF and other Routing protocols.

The connection betthe teamen local physical broadband device and the laptop WLAN are now bridged to each other and the same prefix should be working in EVE-NG.

Bridge connection is directly connected to the CISCO L3 switch, there no special configuration has setup in this switch (a default switch) that connected to AAA radius, Management PC and NAS or Hotspot router. Because the team need to put them all together on single network to make sure there is no complications and easy to understand the concept of AAA. Figer 6. Shows the exact scenario where there are all devices in EV-NG put together and installed.



Figer 6. Shows the entire architecture

The NAS router has always an important role in the concept as NAS always talk to the AAA billing server to update the each other by sending information and data and stores in their directory to use it. It gets expired in a time frame and they withdraw this data and request for a new data to be updated on the time, not just sharing the User data but also they share the TTL (Time To Live) which means AAA is responding or not in a specific tome frame, it could be in mili second (ms). So, AAA and NAS always communicating with each other for a specific reason and share their updates.

There is an other Cisco switch that is connected to NAS which the team can call it LAN switch or Hotspot LAN switch. The purpose of this switch to provide the wifi hotspot service to end user. Actually, EVE-NG could not support Wi-Fi AP (Access Point) to connect the laptop or other devices through Wi-Fi, that’s the reason the team are using LAN switch with Wired connection. AAA concept is not that much easy to implement as it has many features which can not be included in the scope of the current study. The team can use it for the Entire ISP solution, Over routing, with MPLS etc but the team would not go there as it will take bundles to pages to write about them.So, the team have connected virtual computer that obviously run in realtime with windows 7 to the Hotspot LAN switch. In short, cloud as broadband connection to the EVE-NG via bridge terminology, Cisco switch is a default switch to connect all devices in the network together in same prefix network, AAA server will do the Authentication, Authorisation and Accounting for for user, NAS router will be acting to provide login page with username and password boxes , and will alway communicate with AAA to get permission what to do next etc, and Virtual PCs are meant to be as end user or client/ customer to use the service and pay for this particular service. The over all concept has been discussed l,now the team will try to get into the configuration part to discuss the actual infrastructure and mechanisms step by step.

As the team know that and already been discussed the LAN bridging betthe teamen physically broadband and virtually machine. So, the broadband from XYZ company has set the 192.168.0.0/24 as default DHCP pools for the local users and devices.

## 5.1 AAA server Installation and Configuration

Scalability, more flexibility and control, standardised protocols and techniques, and redundancy are all advantages of implementing AAA. For usage in a AAA mechanism, Cisco PIX firewalls support the RADIUS and TACACS+ security protocols [10]. Each procedure has its own set of benefits and drawbacks. An AAA server must be installed and configured in order to take benefit from AAA. Cisco Secure Access Control Server (ACS) is AAA server software that supports TACACS+ and RADIUS protocols at the same time. Basic operations, such as adding users to AAA clients, can be completed after the programme has been installed. Advanced tasks, such as the creation of downloadable access lists and command authorization sets, are also possible. Cisco provides a functionality called cut-through proxy to provide user authentication and permission for user operations over the PIX firewall [11].

Configuration of authentication step is the foremost priority for network managers. The standard configuration method for authentication entails deciding upon a list of authentication methods viable for the network. This is done in the global configuration mode. Meanwhile, application of the list is done in interface configuration mode [12]. However, here, a default method list is treated differently since it is applied to all interfaces automatically by default, except on those interfaces which have named method list particularly defined. Hence, a defined method overrides the default method list. Meanwhile, configuration of authorisation is complicated since it depends upon a myriad of already existing and newly implemented policy frameworks for the system and networks upon which the AAA is being implemented. In this respect, the authorisation step has to be formulated and planned before execution stage so as to ensure that no major room for scotty threat is left unnoticed due to inefficient implementation. Moreover, it is also pertinent to note that authorisation is generally closely associated with the policy guidelines issued by the network stakeholder i.e., the network providing companies [13]. However, the inclusion of all the major stakeholders of the network is regarded as a favourable because each stakeholder may have a different viewpoint about the necessary elements in authorisation step.

The Network Policy Server (NPS) allows the network manager to synthesise and enforce an organisation-wide network access policies, which would also enable them to configure the steps of authorisation and authentication according to the nuanced specification of the server and the network. Moreover, the NPS could also be configured to function as a Remote Authentication Dial in User Service (RADIUS) in order to forward the requests for connection to other RADIUS servers and / or to the remote NPS [11]. This feature enables the network manager to load balance connection requests and forward them amend the domain to the subsequent authorisation and authentication.

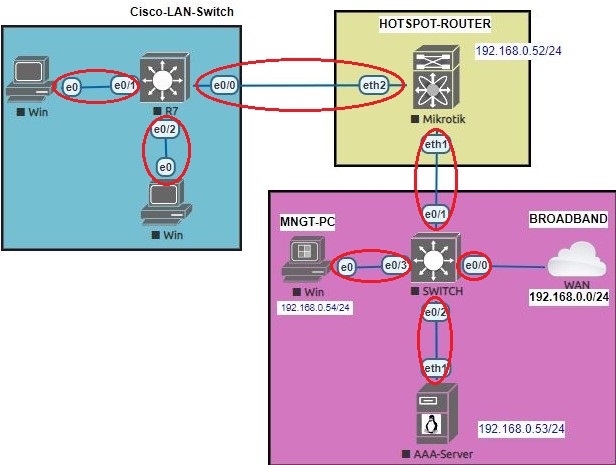
Basically, AAA here , is the Mikrotik router and and same as the team have used for NAS Hotspot. But there is a feature of Mikrotik router that’s called User- Manager or AAA radius manager, the team are using this feature as AAA in the architecture. Obviously a person have put the router on the EVE-NG screen and switch it on, after pothe teamred it on , there is Mikrotik packages, which is by default are not available in the router. The team download the package from the Mikrotik official the teambsite www.mikrotik.com, but make sure check the router OS version and model before downloading the package for it. There may have many model and OS versions this is necessary to check out the model ans OS version first of the router to be the package downloaded for. After downloading the package , make sure a person have winrar to extract the package on a personr local disk drive. A person can access the router from the teamb access, winbox ( official software available from the Mikrotik official site) and telnet or SSH , totally up to the engineers to choose what platform they like to work on.

## 5.2 Ethernet Connections

Ethernet always refers to one of the traditional technology to connect devices through the wired local area network (LAN) and wide area network (WAN). As it helps for enabling the devices especially to develop a connection with each other through the protocol that is a set of rules or within the common network language [14]. Furthermore, ethernet help to elaborate how different network devices have to be formatted and transfer data for the feasibility of the other devices on the similar LAN and on the campus network that recognise, receive, and complete process for the information. However, the ethernet cable is more of the physical wiring that is encased through which traveling of data can be done. Moreover, all the connected devices, which usually use the cables for accessing the geographically localised network, rather than of the wireless connection, use the ethernet. It has been identified that from business to the gamers, more of the diverse end-users completely rely on the benefits of the connectivity by the ethernet and this includes reliability and security [15]. In addition, as compared to the wireless local area network (WLAN) technology, ethernet has been very less vulnerable to all kinds of disruptions. As it offers a high degree of network security and control through wireless technology just because physical cabling is necessary to all the devices for the connection. As such technique resulted by creating difficulties for the outsiders to access someone's network data or hack the bandwidth for any kind of unsanctioned devices [16].

Cloud (broadband) has connected to Cisco switch on E0/0 and Cisco switch has connected to NAS hotspot router via E0/0 and Ether1 and NA hotspot router getting 192.168.0.52/24 Ip from the broadband via Cisco switch. Hence, the management PC connected via E0/3 and e0, with this getting 192.168.0.54/24 Ip from the broadband via the same Cisco switch. So the AAA is getting a DHCP IP from the broadband and AAA connected to the Cisco switch via e0/2 and ether1 and getting 192.168.0.53/24 from the broadband that passed through the cisco switch. Moreover, the NAS hotspot router is further connected to a Cisco switch for the same purpose as the main Cisco switch, it just works as a bridge to provide connectivity betthe teamen NAS router, LAN network, and to end-user devices. NAS router is connected to the Cisco-2 switch via ether 2 to e0/0.

**NOTE**: All devices on this network have gotten IP addresses and have internet access.



The package is being extracted on the local disk drive such as desktop or any other particular partition.

## 5.3 Accessing the Mikrotik router

Mikrotik is one of the operating, which has been established as considering the network router, as it is refer to one of the operating systems and software that has been used for converting all the computers in the reliable network router [17]. The conversion within the computers includes different kinds of features especially for the IP networks and for the wireless network. Hence, such kinds of functions include firewall & Nat, limiter for bandwidth, hotspot, routing, Point-to-point (P to P) tunneling protocol, DNS servers, DHCP servers along with a different number of features. It is further clear that on the network, which has many clients need the complete adjustment of the bandwidth mechanism for preventing the bandwidth over the limit and with this all the clients fairly get their bandwidth. However, bandwidth management is one of the methods that is used to complete all the needs, and limited bandwidth within the Mikrotik hotspot is very important to perform. As wireless hotspots tend to be accessed at any place to whom it has complete access for the policies. The computers that used the Mikrotik router usually did not require high specification and this can be understood throughout the example, it is just considered as the gateway [18]. Hence, if the particular router is used for the complex networks, then it is definite to use adequate specifications. Furthermore, the Mikrotik router board has not needed the computer to run and this is more sufficient for using board, which directly include the Mikrotik router OS and this includes the features such as particularly established for the IP networks and the wireless networks.

As the team knows that the main switch, which is connected to the AAA NAS has not been configured, this switch worked as a bridge to offer DHCP IPs from broadband to the devices connected to this switch. AAA has now the IP and the team are good to go for access. The team can either access this via MAC address or IP address and the team might like to access this AAA server through IP address.

To access the Mikrotik AAA server, open the winbox, put the IP provided, the user name, and password if any, by default AAA has no password, an individual need to set up all the passwords to secure the router, and a person may have to secure the SSH and telnet ports as the teamll for any kind of DDOS attacks.

## 5.4 Installing Aaa Package:

After accessing the router, the port one which is connected to the Cisco switch has not provided the IP address until a person configure the AAA port connected to the Cisco switch, to get into this, the team has to configure the AAA port as DHCP-client to gain dynamic IP address from the broadband as the team did it but it has to be configured as a static as the teamll depending on the network architecture. Hence, the download package of AAA has been already extracted on the desktop and it has many other packages such as teamll, but the team just needs a user-manager to drag from the desktop and drop in the files of the Mikrotik router and reboot the router to take effects. After rebooting, it wrapped up the package and was installed. The main phenomenon here is to access the AAA via browser by putting IP address 192.168.0.53/24 to configure the AAA, make some profiles, rate limiting, users management, scratch card generation, and validation.

## 5.4 Making Profile:

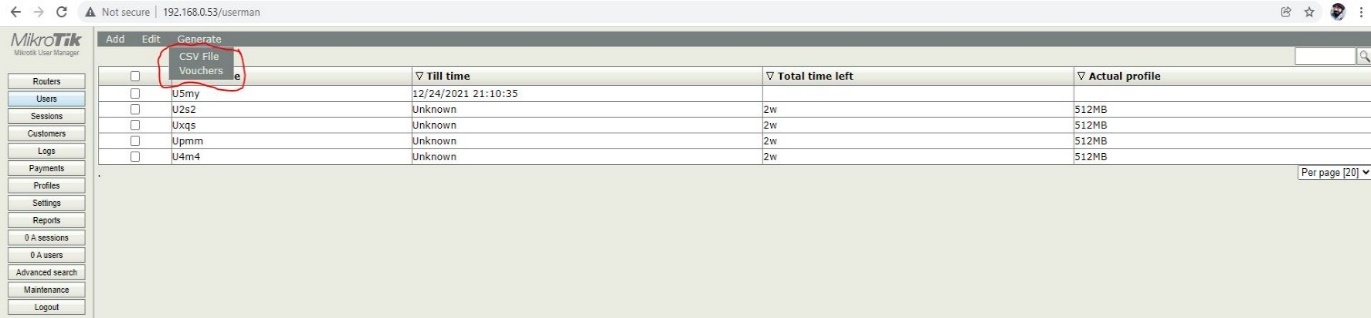
After accessing the AAA through the browser, now a person has access to the AAA GUI interface to configure according to the requirements to be implemented.

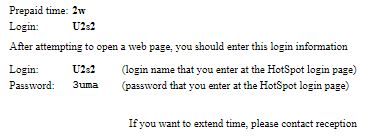
**Profiles design and configuration**

Profile making is one of the main technical thing here to be developed and implement as there comprises of many requirements and demands of services. To make that possible survey has been conducted within the researcher home, where researcher did live from their home-mates. It has been asked from the home-mates that what kind of package they prefer to have especailly when it is all about the internet services. As three of the home-mates stated that data has to be 1GB by the inclusion 1 MBPS transfer rate monthly, and two of the home-mates present their view as data has to be 512MB with the 512KB and 256KB transfer rate. For this particular, design has been made for both of the packages and tested, nevertheless this is not just about the survey, because survey is one of the obvious thing to do when it is about the marketing and to be more competitve for attract more audience and provide offer for good packages. However, according to the survey, researcher decide to make such profiles and configured them by considering all the requirements.

## 5.5 Adding NAS ( NAS means the Mikrotik which is providing Hotspot services on the LAN network)

NAS (Network Access System) is one of the actual router that provides the hotspot services on local area network (LAN) to the end users and communicating with AAA in a specific time frame. NAS and AAA speak to each other when there is a cross over static IP configuration has been done. For Example, NAS IP address is 192.168.0.52 and AAA has IP address is 192.168.0.53, then put NAS or hotspot router IP in AAA and Add NAS section and vice versa. However, the team going to add NAS in AAA radius here to make the system work. Meanwhile, after the configuration of profiles, packages and NAS as a person are done through the AAA radius configuration, and now an individual tend to generate scratches cards or voucher in the form of batch cards or a person has the option to add users manually.



****

## 5.6 Configuration of NAS Router

NAS is also a Mikrotik brand router and usually provide hotspot services, as Mikrotik hotspot router is totally dependent on AAA Radius. Similarly, it is not wrong to mention that “AAA radius is King and Mikrotik is Slave”. This is because Mikrotik hotspot router found to be helpless in this case and not able to do anything on by his own, and Mikrotik hotspot has to follow the AAA for choosing the profile and rate limitations. The main task of the NAS router was just to offer and provide DHCP to the local users and provide the login page over the dhcp and the rest Mikrotik hotspot router follows the command from AAA. As the team have the idea that the cross over IP address configuration has made the communication possible betthe teamen AAA and Hotspot router. However, the team had used the same method here as the teamll team had not use static IP address configuration in this case. Moreover, the team use dhcp-client system to gain the IP address from the broadband router in the home as same as AAA did. The Hotspot router have gotten the IP address ( 192.168.0.52/25 ) from the broadband router and having internet access.

## 5.7 Hotspot configuration:

Hotspot configuration always considered as quite easy but tricky as the teamll, a person have to setup various parameters and cope up with issues may be faced. Hotspot is a feature of Mikrotik router and it is quite flexible and consistent solution for low budget ISPs, usually a person has not to pay for the services, because it is free of charge. As a person know after accessing the router via winbox ( Mikrotik software for accessing the routers and switches) a person indirectly see through the GUI interface. There might have many more options but most appropriated and most selected one is the hotspot feature. Hotspot is also a server by itself same as dhcp. DHCP sever provide dynamic IP addresses to the client without any restrictions and authentication. Nevertheless in hotspot, the client take IP address but it redirects a user to the login page to put the username and password, which has been provided by AAA server or generated a batch in AAA server. Configuration of hotspot in the Mikrotik is simple and required to clicks by the selection of the LAN port to the switch or within any other devices. Meanwhile, Hotspot, assign the pool by itself but a person can change it to IP pool, where a person want to configure.

The ports authentication use the port=1813 and port = 1812 on different mechanisms and technology. Authentication port are globally same and unchangeable and the team has configure PAP and CHAP authentication method at same time to get more secure authentication.

**General network configuration:**

### an address on the outside (WAN) interface of the mikrotik

/ ip address add address= 192.168.0.52/24 interface=ether1

### add a gateway

# / ip route add gateway=192.168.0.1

### set the DNS servers

/ ip dns set primary-dns=8.8.8.8 secondary-dns=8.8.4.4

**Radius configuration:**

### add another address for connecting to the radius server

/ ip address add address= 10.5.50.1/24 interface=ether2

### add radius servers for any PPP service on mikrotik

/ radius add service=hotspot address=192.168.0.53/24 secret=1234

timeout=2000ms

/ radius incoming set accept=yes

**Setup masquerading:**

### setup NAT on the outside interface of the mikrotik

/ ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade

### disable masquerading for the radius LAN (10.5.50.0/24)

/ ip firewall nat add chain=srcnat out-interface=ether1

/ src-address= 10.5.50.0/24 action=return

/ ip firewall nat print

/ ip firewall nat move 1 0**Add a pool:**

### add a pool

/ ip pool add name=pool0 ranges= 10.5.50.0/24

**Add a hotspot server profile:**

/ ip hotspot profile add name="prof1" hotspot-address=8.8.8.8 dns-name="hotspot1.al" html-directory=hotspot use-radius=yes radiusaccounting=yes

**Add a hotspot server:**

/ ip hotspot add name="server1" interface=ether2 address-pool=pool1 profile=prof1

**Add a user profile:**

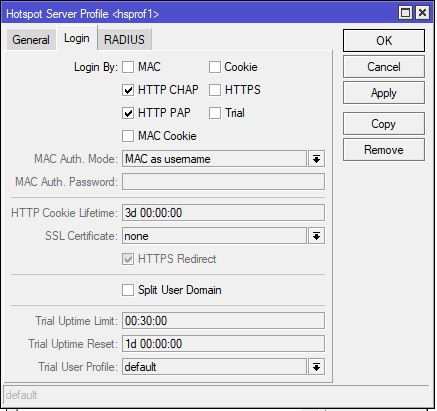
/ ip hotspot user profile add name="userprofile1" address-pool=pool1 transparent-proxy=no**Add a user:**

/ ip hotspot user add server=server1 name="admin" password="admin"profile=userprofile1

PAP: PAP is the authentication protocol that uses for point to point protocol and user validation while:

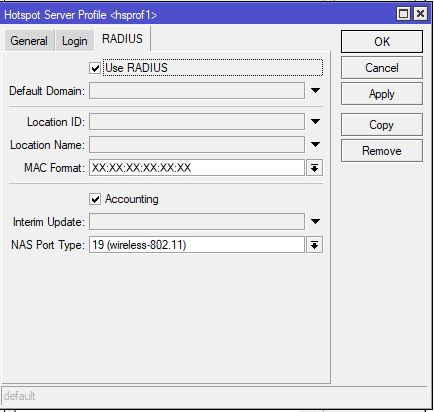
CHAP: CHAP is same as PAP, but CHAP is more secure than PAP.

Using the above protocols , depends on the Network engineer or network administrator.



## 5.8 Radius Configurations

Radius configurations used for enabling the radius in the RADIUS menu of Mikrotik router. Radius belong to AAA, the team has already discussed that the IP address cross over. In addition, later team crossed over the IP addresses, as the team already did in AAA in the configuration time. For this reason, team has put AAA radius server IP address here with a security key. Hence, this key tend to be same on both Mikrotik hotspot router and AAA server, otherwise a person, it has not work in a proper way.



The login page provided refer as one of the default login page by Mikrotik company, but a person have the opportunity to design a personal desired login page and upload to the Mikrotik directory with some advertisements and company profiles. In this case, researched designed this login page for the Bright Better ICT solutions in Afghanistan for British military, and this tend to be adjust in the Mikrotik directory. Hence, Uploading the login page refer same as user manager package drag and drop in the AAA installation and drag the login page from the local folder and drop within the Mikrotik file folder.



## 5.9 Management PC Installation:

Management PC refers to a PC that manages entire devices in the network if the a person are working on a private network. It refer to the campus network with high availability, but there have to be a public IP address if an individual wish to access the local network from out side through VPN site to site connection. So management PC is important to be installed in any size of network. However, in this case virtual PC has been installed to access all kind of the Mikrotik and the Cisco switch for manage from one point. Meanwhile, in the wireless scenario, the team has put the wireless AP controller to manage all the wifi devices in the same network such as Unifi, to manage all wireless access points and Cisco have its own controller for controlling Cisco wireless APs Cisco wireless scenario.





## 5.10 TEST:

It is obvious and certain procedure in information technology to test what a person have done. Testing carries out when the system either works according to defined requirements or it has something more to be updated. The test on this platform has carried out and worked the teamll for us. If there is any updates or modifications need has to be implemented in a little time because the setup has already been done and the modifications could be done remotely.

# 6.0 SECURITY ANALYSIS

In this particular AAA architecture, the end user access the internet services through some pre-defined profiles and related packages/subscriptions. To access the services, the client’s credentials have to pass through a process that possibly make the connection successfully. It is totally up-to the network engineer to configure pre-share keys for Wifi access point because user have to pass through the process in either way to get access to the internet service and this is quite secure connection. For example, if a user want to connect to the wifi, no matter if there is a pre-share key to the wifi it not, still the user needs to go through all the AAA process. The security of AAA is not just limited here, there are three layers of AAA ( Authentication, Authorisation and Accounting). The user need to authenticate his/her credentials if it passes then AAA has granted the profile assigned configuration and account has been started on the first login. AAA also holds data of the current online users (MAC address of the device, IP address offered to the devices from the hotspot router, AP ( Wi-Fi access information to which the user connected to, first login, data usage, remaining data yet to he used and expiration date and time if the voucher). AAA radius provides a huge range to privilege to the network administrators to drop, revoke, suspended and remove the user. The hotspot router is totally dependent by AAA radius server and have to follow the rules, which been provided by AAA.

# 7.0 PERFORMANCE ANALYSIS

This practical totally designed in a virtual platform , the team has not use physical devices as the team have not have that much resources and financial budget to deploy such architecture and implement on physical devices. The team have used VMware and EVE-NG simulator to describe and demonstrate the actual proposition scenario. The team deployed a scenario here to just illustrate the AAA billing service and how to be applied in public. This scenario was not just limited to hotspot internet services but also it uses in different sector e.g banking, trans station contactless card system etc etc. The performance of this architecture was quite excellent and consistent without any delay. The TTL( Time To Live ) was monitored in 0 ms and 1ms, means the communication is fast and reliable. Checked the profile, packages and made a batch of vouchers was working fine and consistent. Further, there has been no critical situation noted in the entire project implementation and evaluation. The installation of this architecture was totally confusing but after researching the team approached this of implementation. Overall the entire solution works the teamll and reliable with zero communication complications. The team the teamre about to install Ubuntu OS to implement this scenario but the device researcher worked on is not much teamful as it consumes the RAM and proecssing the pothe teamr.

# 8. CONCLUSION

## 8.1 Summary of Project

In the project the team highlighted the overall solution of the AAA billing mechanism and implementation to cope the broadband issue in the public place and business development. The main theme of this project to work on the AAA Radius server deployment over Wi-Fi hotspot services in public places like hotel, restaurants, airlines and parks, even a person can have this service at home from different broadband services. This project was not just limited to internet hotspot services but it can be implemented in various scenarios. As the team have discussed above that AAA is a consistent solution for mobile top-up, e-commerce, bio metric authentication and authorization, national database services etc. The implemented project is just an example to approach for all the above examples. AAA play an important role in deployment to reduce human efforts and make the authentication, authorization and accounting easier and more automatic billing services. The team have used different approach and different brands to make this happen. There have been Mikrotik router, team have used as hotspot NAS and cisco as a default. The team have used multi-protocol label switching system and some routing protocol such as OSPF, RIG and EIGRP but it needs a huge amount of RAM and processing speed. It is possible to deploy this type of virtual concept in HP, Dell and other pothe teamrful server.

Technically, authorization and authentication on the portal consist of several phases: connection, redirection to the portal, authentication and authorization, organization of Internet access. Redirection to the portal is the next phase after connection. The user, using a device that connects to a Wi-Fi network, goes to any resource on the Internet. Technically, the user terminal makes an HTTP request to the server where the requested resource is located. However, the rule set that was passed by the management platform to the VAP-based access point prevents data packets sent from a connected rogue device from reaching the requested resource. The access point intercepts these packets and responds to the request to the user. In the HTTP response, the access point informs the client terminal that the resource has temporarily moved to another server with a different address. This other server is the authorization portal. That is, after a series of HTTP redirects, the user goes to the authorization portal and sees exactly his welcome page in his browser. At the time of forwarding, the access point changes the user's HTTP request and adds standard parameters required for identification on the portal (MAC address of the client device, MAC address of the access point, etc.). Thus, the authorization portal receives information about the connected user.

Authentication and authorization is the stage of the process at which the user is validated their access attributes (login, password). In order to clarify the sequence of actions on the authorization portal, it makes sense to describe the main elements of the portal user interface. Further, in a typical scenario of an authorization portal, the user on the browser screen is shown advertising content in a dynamic or static version. After that, the user is given access to the Internet by going to the pre-configured address of the resource on the Internet. From the point of view of technical interaction, the user is redirected to the Internet through the interaction of the platform API and the authorization portal. The portal gives a command to the platform that the user (client terminal) is authorised and that the access rules need to be changed for him. The platform, in turn, broadcasts this message to the access point to which this terminal is connected. The access point applies the rule and informs the portal through the platform. The visual components of the portal, marketing content and the type of authorization can be changed, for this it provides documentation describing typical possibilities for changing the appearance of the authorization portal.

The portal functionality in the AAA part complements the AAA solution with a custom frontend for authorization in the public Wi-Fi network. The use case is similar to the one above, but it's worth noting that AAA is a separate product and can be used separately from the Wi-Fi network management platform. AAA terminates RADIUS requests from Wi-Fi controllers or control platforms on itself. HTTP traffic, as in the case of vAP, is processed by the frontend of the authorization portal. Further interaction of the portal with the controller or Wi-Fi control platform occurs through integration with AAA via the RADIUS protocol. Typical scenarios for using Portal-vAP, Portal-AAA are different. The portal-vAP link only works with the management platform. The portal functionality is integrated into the platform, which gives an advantage in the speed of service deployment, but limits the scope of application only to the infrastructure with the software. In turn, the portal-AAA link is as independent of the type of Wi-Fi infrastructure as possible and makes it possible to deploy an authorization service on any Wi-Fi network.

However, in this case, the team just virtualized everything to squeeze the result of what the team can derived from the physical devices. The team have used the home broadband as a WAN connection in order to have access to the internet in the virtual devices, cisco switch as default switch with no configuration to connect all devices together. The team also used Mikrotik routers one, as AAA radius services and the other one as hotspot router to provide hotspot service to devices on LAN side. There are some virtual PC as the teamll illustrate the act of the end user devices, it tend to be a mobile and laptop. For Example: A person walking in park or have coffee at coffee shop, suddenly his Data has finished and he wants to use the internet service. He will activate the data again from mobile or he will use the internet in coffee shop, in either way he will pay for the service. If he wants to activate the data from mobile, he needs to make a top up and he will go through the whole process, the top-up voucher will authenticate, authorize and account will provide services, same as if a person have paid as a person go service as home for gas and if a person need to top up for the gas or the team can say prepaid voucher then a person can avail the gas services etc.

## 8.2 Summary of Results

From a practical point of view, it would be convenient to manage Wi-Fi networks by issuing a password to each user. This makes it easier to access the wireless network. Using the so-called WPA2 PSK authorization, in order to prevent access to a random user, the users need to change the key, as well as re-pass the authorization process on each individual Wi-Fi device. In addition, if they have several access points, the key must be changed on all of them. To ensure that only specific individuals could access the wireless network, a special security technology was created. It allows securing the Internet channel from being used by hackers. High-quality data encryption is used to ensure a decent level of protection, and authentication is carried out with a minimum chance of brute-forcing a password.

As the identifier of the authenticated user session which is stored in the server memory or in a database. The session should contain all the necessary information about the user to be able to authorize his requests. As an encrypted and/or signed object containing user data and validity period, this approach allows for stateless server architecture, but requires a mechanism to refresh the session token upon expiration. The two protocols described above are successfully used to authenticate users to websites. But when developing client-server applications using web services (for example, iOS or Android), along with HTTP authentication, non-standard protocols are often used in which authentication data is transmitted in other parts of the request. Using certificates for authentication is much more secure than password authentication. This is achieved by creating a digital signature during the authentication process, the presence of which proves the fact of using the private key in a specific situation (non-repudiation). However, difficulties in distributing and maintaining certificates make this method of authentication inaccessible in wide circles. To better understand the standard itself, consider an example of a web application that helps users plan their travels. As part of its functionality, it can analyse users' mail for booking confirmation emails and automatically include them in the planned route.

The result was quite fine so far, the team have tested all the routers and switches along with the broadband connection and started work on it. There the teamer faced some difficulties to manage all things together but according to the study and research the team copped with it in consistent way. The team have made some voucher and in AAA radius server, after cross-connection betthe teamen AAA and hotspot server. The voucher was made in AAA radius server and tested in the virtual PC, which work very well for the teamll. The voucher username and password sent to hotspot router and hotspot sent back to AAA radius server for authentication and authorization. The accounting will start after the first login. The team have set some rate limits to check what exact speed that the team have offered for client, which was exactly according to the configuration and requirements. The whole projected deployed, implemented and tested and the team got a positive result.

## 8.3 Discussion of the Extent to Which the Aims Have Been Met

The aim the team pursued was implementing the AAA Billing services as said not just limited to Wi-Fi hotspot. It could be used for every AAA concept but in different configuration mechanisms and technologies. The RADIUS protocol is implemented as an interface between the NAS, which acts as a RADIUS client, and the RADIUS server, which is software that can be installed on a computer (server) or some specialized device [22]. Thus, the RADIUS server, as a rule, does not interact directly with the user's device, but only through the network access server. A user sends a request to a network access server to gain access to a specific network resource using an access certificate. The certificate is sent to the network access server via the Link Layer, for example, Point-to-Point Protocol (PPP) in case of dial-up access, Digital Subscriber Line (DLS) in case of using appropriate modems, etc. The NAS then, in turn, sends an access request message to the RADIUS server, the so-called RADIUS Access Request. This request includes access certificates, which are usually in the form of a username and password or a security certificate obtained from the user [23]. In addition, the request may contain additional parameters, such as the network address of the user's device, their phone number.

In simple terms, the AAA principle can be described as follows: in order to perform any action on the network, we must trace who initiates this action or authentication, whether the user has the right to perform this action (authorization) and that all actions that they performed are recorded in the log [26]. Hence, authentication is the identification of the person who is trying to enter the premises. In our example, this can be a fingerprint scan, because each person is unique and can be a guarantor of identity confirmation. In the networked world, standard authentication consists of using a username and password that is generated for each user and allows him to verify his identity. Authorization is the next step after successful authentication [27]. It consists in checking the access rights to the premises of the person who has passed the authentication. Perhaps a person has the right to enter the first room, but it is forbidden to go further. On network devices, access rights most often define a list of commands that an authenticated user can execute [26]. For example, a network engineer with access level 1 is only allowed to view the device configuration using the show command, while an engineer with access level 2 is allowed to make changes. On the AAA servers of telecom operators, the access right can determine the subscriber's membership in any tariff plan. The aim here was to develop a service to perform AAA radius services. The team has no issues with development as the team have reached the aim and the team wanted to implement. But the team must have to do more research on banking sector, bio metric systems and national data bases, may be in a government sector such as police network and carried out authentication of a person by his/her date of birth, validity and expiration dates of driving license and bio metric for the resident permit.

When using this type of authentication, the username and password are included in the web request. Any interceptor of a packet of information can easily recognize classified data. This method is not recommended to be used even in situations where classified data does not carry significant information either for the user or for the Internet resource. This circumstance is due to the fact that most people on the network use the same password for all the services they use. The main advantages of double authentication are convenience; the smartphone is always at hand and security, constant change of the confirmation code. This method also has certain disadvantages. Problems with the mobile network can interfere with the receipt of the confirmation code, and the SMS message itself can be intercepted by hackers. There is also some delay in receiving SMS due to the authentication procedure. When connecting to a wireless network, a user also goes through an authentication process. There are several methods for this type of authentication. They depend on the settings of the router, the number of subscribers, and the type of wireless network home, public, corporate. It is quite secure and suitable for use in various types of networks. Network authentication is something that a large number of Internet users face on a daily basis. Some people are unaware of what this term means, and many are unaware of its existence. Almost all users of the World Wide Web start their working day by going through the authentication process. It is needed when visiting mail, social networks, forums and other things.

## 8.4 Discussion of the Extent to Which the Problem Addressed Has Been Solved

The current research has been significant in terms of analysing the limitations of Radius and VMware and EVE-NG, EVE-Ng in implementation of AAA on WIFI Hotspot environment. However, the framework developed contains some limitations in further applicability due to highly contextualised environment in which the framework was developed. Hence, its wider real applicability is currently limited. The team has completed a thorough examination of all routers and switches, as well as the broadband connection, and has begun work on it. There were some issues for the team members in managing everything at the same time, but according to the study and research, the team dealt with it in a consistent manner. After establishing a cross link between the AAA and hotspot servers, the team created some vouchers and placed them in the AAA radius server. The coupon was created in AAA radius server and tested in a virtual PC, both of which performed admirably for the team. The voucher username and password are given to the hotspot router, and the hotspot is then authenticated and authorised by the AAA radius server. Modern RADIUS implementations use UDP ports 1812 (authentication) and 1813 (accounting) (ports 1645 and 1646 are also possible). UDP is fast, but it has a number of drawbacks that must be taken into account when using it. When RADIUS was developed, security issues were not as relevant as they are now, so it supports a fairly small number of authentication types (Clear text and CHAP), encrypts only the password field, and generally has moderate security. Furthermore, to tackle the different issues within the project different techniques have been used that lie under the EVE-NG, one of the options that has been opted for the devices was about to add the work on and another option was about the cloud, but not the online cloud services. In simple words, cloud refer to the backbone for the person EVE-NG like person local broadband etc. In this case team has used local broadband, which was very big in the size networks and tend to be considered as the optic fibre, or other services like cloud service or any kind of public network that might work on the BGP, OSPF along with the other routing protocols. Meanwhile, in the wireless scenario team has put the wireless AP controller especially for managing all the Wi-Fi devices within the same network like Unifi, especially for managing all different wireless access points along with the Cisco that has their own controller to control the Cisco wireless APs in the Cisco wireless scenario. As such kind of the analysis within the project and to identify problems and use proper solution helped this project to reach the final results.

The team presented a hotspot design for wireless and wired internet access in WLAN hotspot zones as part of this research. The team demonstrated an AAA network solution that provides safe Internet access to mobile clients and ISPs outside of the LAN, MAN and WAN communication range. Hence, Design makes a significant advance by allowing each mobile client to communicate securely and securely transfer data while still having access to the wired Internet. These two factors are critical for future business potential. To achieve this, the team implemented and set up an AAA radius service to work according to authentication, authorization and accounting mechanism. The team also implemented this scenario and top leading software for virtualization which is VMware and EVE-NG, EVE-Ng support the network devices to virtualize and work alike on real devices. The team also implanted the security for a secure connection and data transfer to make establish a secure connection betthe teamen the Wi-Fi hotspot and client device. The team have use used cisco product and Mikrotik product to achieve this kind implementation and deployments in certain places. Moreover, the team have sued the home’s broadband connection as Wide area network, then merge into the local area network. After the configuration and test, the team finally observed that the team can work on some other project as the teamll with same concept but in different scenario. The advantage of the particular implementation is developed business and often uses in big sized Internet service providers such virgin media, British Telecom etc. The main theme of this project to construct AAA radius server and internet data packages according to the price and quota system as discussed above. This project is also business oriented; a person can develop the hotspot business as according to the people need.

## 8.5 Future Work

The team intend to implement this project in a big size network or a campus networkwith highly availability over load balancing, routing and use of different AAA services as Mikrotik hotspot, Cisco AAA and radius Manager Services. The combination of this all in a single big size network would help the community to reduce the human effort and technical hard work, furthermore, the team looking forward to deploy this system over FTTH (Fiber TO The Home) network.

## 8.6 Acknowledgment

Many Thanks to discuss this concept with Ali Afridi, advised and encouraged me to develop this scenario in VMware and EVE-NG and provide me the Cisco and Mikrotik OS and advised us to read books and articles on AAA.

## References

1. Song S, Issac B. Analysis of WiFi and WiMax and wireless network coexistence. arXiv preprint arXiv:1412.0721. 2014 Dec 1.
2. Lohan ES, Koski K, Talvitie J, Ukkonen L. WLAN and RFID Propagation channels for hybrid indoor positioning. InInternational Conference on Localization and GNSS 2014 (ICL-GNSS 2014) 2014 Jun 24 (pp. 1-6). IEEE.
3. Banerji S, Chowdhury RS. On IEEE 802.11: wireless LAN technology. arXiv preprint arXiv:1307.2661. 2013 Jul 10.
4. Vollbrecht J. Lambda Grid, Grid Computing and AAA. Merit Techical Report. 2004 Apr.
5. Benzekki K, El Fergougui A, Elbelrhiti Elalaoui A. Software‐defined networking (SDN): a survey. Security and communication networks. 2016 Dec;9(18):5803-33.
6. Paolini A, Scardaci D, Liampotis N, Spinoso V, Grenier B, Chen Y. Authentication, Authorization, and Accounting. Towards Interoperable Research Infrastructures for Environmental and Earth Sciences. 2020:247-71.
7. Spinoso V, Grenier B, Chen Y. Authentication, Authorization, and Accounting. Towards Interoperable Research Infrastructures for Environmental and Earth Sciences: A Reference Model Guided Approach for Common Challenges. 2020;12003:247.
8. Yeh LY, Huang JL. PBS: a portable billing scheme with fine-grained access control for service-oriented vehicular networks. IEEE Transactions on Mobile Computing. 2013 Mar 27;13(11):2606-19.
9. Zorn G. Diameter Network Access Server Application. RFC 7155, April; 2014 Apr.
10. Lu YY, Yang Y, Yin ZH, Yu BC. The research and design of campus network security development on Cisco AAA certification. InApplied Mechanics and Materials 2013 (Vol. 411, pp. 662-666). Trans Tech Publications Ltd.
11. Lu Y, Chen XZ, Wang W, Yang Y. Based on the RADIUS and AAA Authentication of the Campus Networks Security System Design and Implementation. TELKOMNIKA Indonesian Journal of Electrical Engineering. 2014 Apr 1;12(4):3040-5.
12. Yan Y, Qian Y, Sharif H, Tipper D. A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials. 2012 Jan 30;14(4):998-1010.
13. Osipov V, Sweeney M, Weaver W. Cisco security specialist's guide to PIX Firewall. Syngress Pub.; 2002.
14. "What Is Ethernet?", *Linksys*, 2022. [Online]. Available: https://www.linksys.com/us/r/resource-center/basics/whats-ethernet/. [Accessed: 04- Jan- 2022].
15. R. Gupta, S. Tanwar, S. Tyagi and N. Kumar, "Tactile internet and its applications in 5G era: A comprehensive review", *International Journal of Communication Systems*, vol. 32, no. 14, p. e3981, 2019. Available: 10.1002/dac.3981.
16. I. Indu, P. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges", *Engineering Science and Technology, an International Journal*, vol. 21, no. 4, pp. 574-588, 2018. Available: 10.1016/j.jestch.2018.05.010.
17. A. Prayogo, I. Riadi and A. Luthfi, "Mobile Forensics Development of Mobile Banking Application using Static Forensic", *International Journal of Computer Applications*, vol. 160, no. 1, pp. 5-10, 2017. Available: 10.5120/ijca2017912925.
18. G. Irawan, M. Djaohar and M. Ficky Duskarnaen, "Perancangan Dan Implementasi Sistem Keamanan Jaringan Menggunakan Firewall dan Web Proxy Berbasis Mikrotik di SMA Negeri 1 Kota Sukabumi", *PINTER : Jurnal Pendidikan Teknik Informatika dan Komputer*, vol. 2, no. 1, pp. 27-32, 2018. Available: 10.21009/pinter.2.1.4.
19. Housley, R., and B. Aboba. Guidance for authentication, authorization, and accounting (AAA) key management. BCP 132, RFC 4962, July, 2007.
20. Wong, Stan, Nishanth Sastry, Oliver Holland, Vasilis Friderikos, Mischa Dohler, and Hamid Aghvami. "Virtualized authentication, authorization and accounting (V-AAA) in 5G networks." In 2017 IEEE Conference on Standards for Communications and Networking (CSCN), pp. 175-180. IEEE, 2017.
21. Abukeshipa, Amna SM, and Tawfiq SM Barhoom. "Implementing and Comprising of OTP Techniques (TOTP, HOTP, CROTP) to Prevent Replay Attack in RADIUS Protocol." (2014).
22. Barhoom, Tawfig Sm. "implementing and comprising of otp techniques totp, hotp, crotp to prevent replay attack in radius protocol." (2014).
23. Péreza, Salvador, Dan Garcia-Carrillob, Rafael Marın-Lópeza, José L. Hernández-Ramosc, Rafael Marın-Pérezb, and Antonio F. Skarmetaa. "Architecture of security association establishment based on bootstrapping technologies for enabling secure IoT infrastructures." (2018).
24. Spinoso, Vincenzo, Baptiste Grenier, and Yin Chen. "Authentication, Authorization, and Accounting." Towards Interoperable Research Infrastructures for Environmental and Earth Sciences: A Reference Model Guided Approach for Common Challenges 12003 (2020): 247.
25. Thakur, Mukesh. "Authentication, authorization and accounting with Ethereum blockchain." (2017).
26. Paniagua Díez, Fidel. "Advanced AAA System for interoperable distributed architectures." (2020).
27. Lopez, Javier, and Juan E. Rubio. "Access control for cyber-physical systems interconnected to the cloud." Computer Networks 134 (2018): 46-54.
28. Paramitha, Ardelia Puri, Adian F. Rochim, and Adnan Fauzi. "Design and Implementation Network Administrators Account Management System Based on Authentication, Authorization, and Accounting Based on TACACS and LDAP." In IOP Conference Series: Materials Science and Engineering, vol. 803, no. 1, p. 012040. IOP Publishing, 2020.
29. Shabalin, A. M., and E. A. Kaliberda. "Development of a Set of Procedures for Providing Remote Access to a Corporate Computer Network by means of the SSH Protocol (Using the Example of the CISCO IOS Operating System)." In 2021 Dynamics of Systems, Mechanisms and Machines (Dynamics), pp. 1-5. IEEE, 2021.