The implementation of radius server for wifi pass using the mechanism of access point controller in Department of Electrical Engineering building, Bali State Polytechnic

K A T Indah[1], I N K Wardana[1]

[1] Department of Electrical Engineering, Politeknik Negeri Bali, Kampus Bukit Jimbaran, Bali, Indonesia

Email: triana_indah@pnb.ac.id

Abstract. The problem in accessing the internet network in the Department of Electrical Engineering is that there is no security for WLAN, only normal login page to access to the network. In its application wifi pass requires Radius Server to authenticate against remote network access using Virtual Private Networking (VPN), wireless access points, ethernet switches. Radius Server can protect wireless networks from spoofing MAC Address and also WEP/WPA crack using free Radius authentication. Another problem is to monitoring access points in the area still manually done by IT administrators. With the application of the Radius Server which is a means of wifi pass application, and the access point controller application for monitoring all access points. It will facilitate IT administrators in the operation and maintenance of existing internet networks. Based on the measured QoS table, the hotspot network at the Department of Electrical Engineering for the largest parameter is AP Signal 53 dBm, Bandwidth 1036 bytes, throughput 198,735 bytes, 14 ms delay, jitter 36,777 ms and packet loss 3 percent. The technology used is 802.11 G Wi-Fi that uses DDWRT which has an Extensible Authentication Protocol (EAP) system that supports the implementation of facilities at Radius Server.

1. Introduction

In its application wifi pass requires a container called Radius Server. Radius Server has now been implemented to authenticate against remote network access using connections other than dial-up, such as Virtual Private Networking (VPN), wireless access points, ethernet switches, and other devices. With this authentication server can protect wireless networks from MAC Address spoofing and also WEP/WPA crack, that is by using free Radius authentication.

2. Computer networks

To support information technology in the delivery of information, telecommunications technology is needed to communicate between computers with each other. The telecommunication technology is a computer network. Visitors will still get information through a wifi or WLAN network. At this time in Bali State Polytechnic has not used security for the WLAN, only using the normal login page to access it. In the case of the application of wifi pass requires a container called the Radius Server. In terms of monitoring access points in the area, it is still manually done by IT managers which makes it not efficient

in monitoring access points. Therefore, with permission from the IT Manager, you will build a Radius Server and access point controller using the The Dude Application. By making an access point controller it can facilitate to monitoring and knowing which access point is problematic with the centralized. The following are the system components in infrastructure development implementation of Radius Server for WiFi [1].

2.1. Server

A server is a device that has been equipped with a series of programs and a protocol wherein it has provided various types of services intended to be used by other computer devices. In a world term computer network, there are two programming models, namely basic client and server, where the server program can be interpreted as a program in charge of fulfilling and waiting for requests from a client on a network. In information technology, a server (usually called an application server) is an application program that receives a response. An application server can be run on the same computer as the client that uses the server or can be connected through a computer network. Some examples of servers are file servers, database servers, backup servers, print servers, mail servers, web servers, FTP servers, application servers, VPN servers, DHCP servers, DNS servers, WINS servers, logo servers, security servers, domain controllers, proxies servers, firewalls, etc [2].

2.2. Radius

Radius stands for dial in user service remote authentication, a computer security protocol that is used to centrally authenticate, authorize, and register user accounts to access the network. Radius is defined in RFC 2865 and RFC 2866, which was originally used to authenticate remote network access using a dial-up connection. Radius has now been implemented to authenticate against remote network access using connections other than dial-up, such as Virtual Private Networking (VPN), wireless access points, ethernet switches, and other devices. The Radius server provides a security mechanism by handling user authentication [3]. When the client computer connects to the network, the Radius server will ask for a user identity (username and password) and then match the data in the Radius server database to determine whether the user is permitted to use services in the computer network. If the authentication process is successful, then the reporting process is carried out, namely by recording all user connection activities, calculating the duration of time and the number of data transfers carried out by the user.

2.3. Server Radius

Radius server is a server that provides a security mechanism by handling user authentication and connection authorization. When the client computer connects to the network, the Radius server will ask for the user identity (username and random code that appears) and then match the data in the Radius server database to determine whether the user is permitted to use services in the computer network. If the authentication and authorization process is successful, the reporting process is carried out, namely by recording all user connection activities, calculating the duration of time and the number of data transfers carried out by the user. The reporting process carried out by Server Radius can be in the form of time (seconds, minutes, hours, etc.) or in the form of large data transfers (Byte, Kbyte, Mbyte). Radius Server software used in this study is Free Radius which is modular and has many features. Free Radius is an open source and GPL-licensed server software [3].

2.4. Free Radius

Free Radius is a free, high-performance modular Radius Suite developed and distributed under the GNU (General Public License), version 2, and free for download and use. The Free Radius Suite includes Radius Server, a BSD-licensed library of Radius clients, PAM libraries, apache modules, and many additional Radius related utilities and development libraries. Free Radius is the most popular open source Radius Server. It is the most widely used in the world. Supports all common authentication protocols, and servers are equipped with PHP web-based user administration tools. This is the basis for

many commercial Radius products and services, such as embedded systems, Radius equipment that supports Network Access Control and WiMAX.

2.5. Linux Ubuntu

Ubuntu is a Linux distribution based on Debian and has a desktop interface. The Ubuntu project is sponsored by Canonical Ltd (a company owned by Mark Shuttleworth). Ubuntu is a free and open-source Linux distribution based on Debian. Ubuntu is officially released in three editions: desktop, server, and core. All the editions can run on the computer alone, or in a virtual machine. Ubuntu is a popular operating system for cloud computing, with support for OpenStack [4].

2.6. Access point

An access point is a device in a computer network that can create a wireless local area network. The access point will be connected to a router or hub or switch via an Ethernet cable and emit wifi signals in certain areas. To be able to connect with the local network that has been configured, the device must go through the access point [5].

2.7. Wifi pass

Wifi Pass is a wifi login application that requires several tools and support for hardware/software, which is stored in the cloud and on local hotel servers, for tools used by Wifi Pass, it is a recommended tool by IT-Corporate to be setup in buildings or offices. Wifi Pass also requires a local server called the Radius Server to run Radius, proxy and some other software [1].

2.8. The Dude

The Dude is a software/application that makes it easy for a network admin to monitor its network and supports various network protocols, such as SNMP, ICMP, DNS, and TCP. With an application called The Dude we can manage our network. The Dude will automatically read and detect every device connected to a single segment network. In addition, it can also compile from the design of our network topology and can monitor and give information when problems are found on devices connected to our network [6].

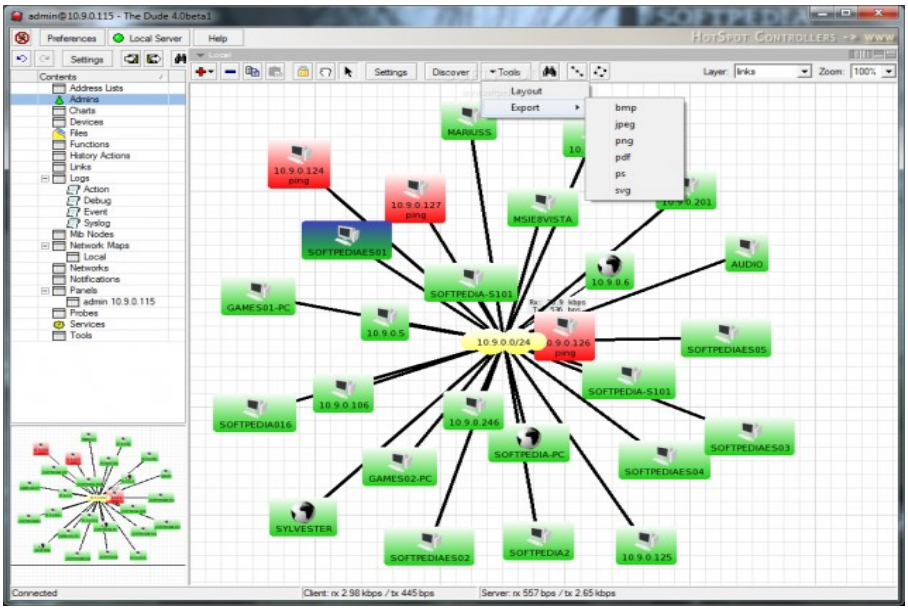

Figure 1. The dude.

2.9. Quality of service (QoS) guarantee

The scenarios used for observing QoS parameters are below:

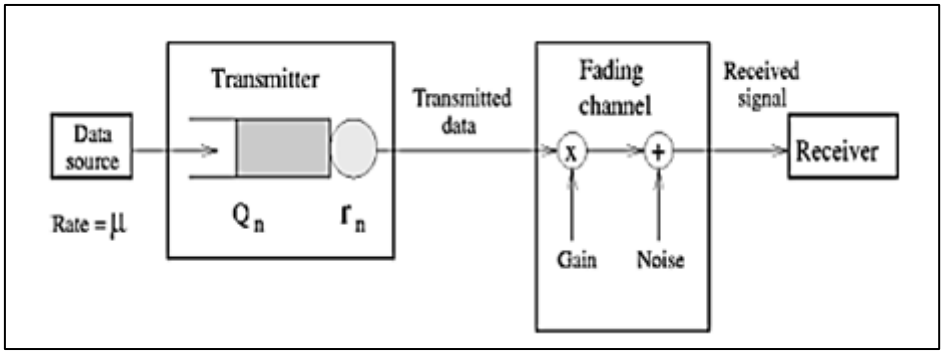

Figure 2. QoS parameter observation scenario utilization/occupancy.

IP technology is connectionless oriented technology, where the process of transmitting information from the sender to its destination does not require defining the path first, as with connection oriented technology. In this case the network utilization/occupancy tends to be directly affected by the traffic that is transmitted over the IP network. As an illustration in the Table 1, shows the amount of bytes needed for the IP application process. Some parameters that are used as a general reference to be able to see the performance of an IP network are utilization/occupancy, package loss, delay and availability [1].

Table 1. Package size in each application [2].

Application	Packet size
Telnet	64 – 1518 bytes
http	400 – 1518 bytes
NFS	64 – 1518 bytes
NetWare	500 – 1518 bytes
Multimedia	400 – 700 bytes

IP Utilization/Occupancy expressed in percent, can be calculated as follows [4]:

$$\text{IP Occupancy} = \frac{Average\ throughput\ of\ IP\ Traffic}{Bandwidht\ capacity\ of\ physical\ link} \quad (1)$$

Along with developments in IP network technology and the need for services running on the network, services on IP networks are no longer just familiar with the best effort class. IP networks can already process traffic according to requests from customers or adjusted to the demand of a service. This traffic management is known as QoS (Quality of Service). QoS on the network can be grouped into several service classes, ranging from the best effort class, real time class (mainly used by services that require real time traffic delivery), classes that divide up guaranteed traffic and best effort. Packet loss is defined as the failure of IP packet transmission to reach its destination. The packet's failure to reach its destination can be caused by several possibilities, including overload of traffic on the network, collision (congestion) in the network, errors that occur on physical media, failures that occur at the receiving end can be caused by overflow in the buffer.

In the implementation of IP networks, the value of packet loss is expected to have a minimum value. In general, there are four categories of decreased network performance based on packet loss values according to the TIPHON-Telecommunications and Internet Protocol Version Over Networks [1], as shown in the following Table 2.

Table 2. IP network performance based on packet loss.

Category degradation	Packet loss
Very good	0
Good	3 %
Medium	15 %
Bad	25 %
Very good	0

Delay is the delay time of a packet caused by the process of transmission from one point to another destination. Packetization delay caused by the time required for the process of forming IP packets from user information. This delay only occurs According to the TIPHON, the amount of delay can be classified as follows:

Table 3. IP network performance based on delay / latency.

Latency Category	Delay Value
Very good	< 150 ms
Good	150 s/d 300 ms
Medium	300 s/d 450 ms
Bad	> 450 m

Jitter is a variation of delay between packets that occur on an IP network. The value of jitter will be greatly influenced by variations in traffic load and the magnitude of collisions between packets (congestion) in the IP network. To get a good network QoS value, the jitter value must be kept to a minimum. There are four categories of decline in network performance based on peak jitter values according to the TIPHON version.

Table 4. IP network performance based on jitter parameters.

Degradation Category	Peak Jitter
Very good	0 ms
Good	0 s/d 75 ms
Medium	76 s/d 125 ms
Bad	125 s/d 225 ms

Link availability is an IP link uptime service. The availability of IP links is stated in the following formula [4].

$$Availability = \frac{Operation\ Time - Down\ Time}{Operation\ Time} \quad (2)$$

3. Research design

The Electrical Engineering Department building has 4 main buildings consisting of approximately 30 rooms. Each building uses an Access Point and LAN Cable. At present, the server in the Department of Electrical Engineering uses the RB1100AHx Microtic Router, for access points at each point using the EnGenius EAP 300 access point, where all internet access from the Access Point and cable lines are connected through a router in the server room located at 2nd floor of Informatics Management Study Program Lab Building. The following Figure 3 is the appearance of network topology conditions in the Electrical Engineering Department.

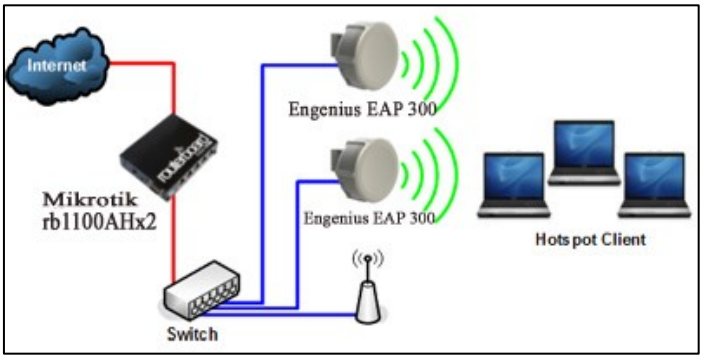

Figure 3. Hotspot network structure in Department of Electrical Engineering.

From the results of field research or hotspots around the fact that the security of wireless networks is still limited to security on the access point and using a normal login page. There needs to be a new device that can be used to overcome the security weaknesses above. Building a Radius Server will provide authentication for users. The Radius server will function to control user authentication. Radius Server will accommodate a wifi pass application that is connected to the system in the Department of Electrical Engineering because it is a server so that the security level can be optimally managed [2]. Based on the above deficiencies, the implementation of the Radius Server will function in accordance with the following rules. Only registered users can connect to the internet network. One user gets one account in the form of a username and password. In this case each user who is in the location will get the username directly in the form of a room number and random password; users who are in the location will get a connection according to the time at the location. In this study, Radius Server was implemented to replace the old security system. System analysis before being implemented with a Radius server application is shown in Figure 4.

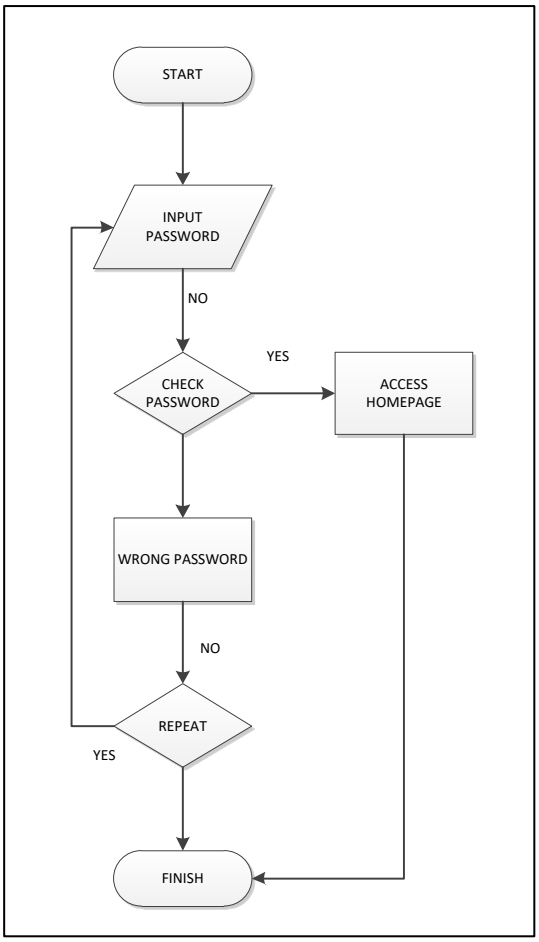

Figure 4. Flowmap hotspot Department of Electrical Engineering.

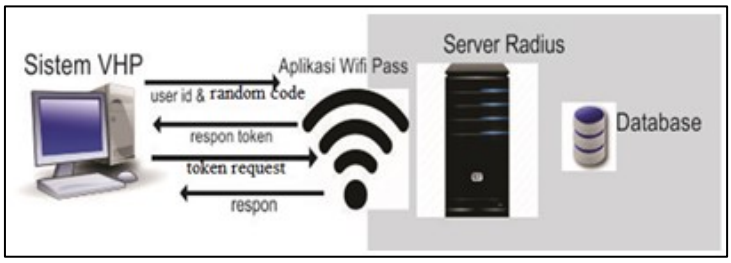

Figure 5. Radius server design.

Figure 5 explains that every user who transacts through the VHP system will send data from the user and stored in the VHP database, then the Wifi Pass application responds in the form of a username hotspot via Radius Server and stored in the database.

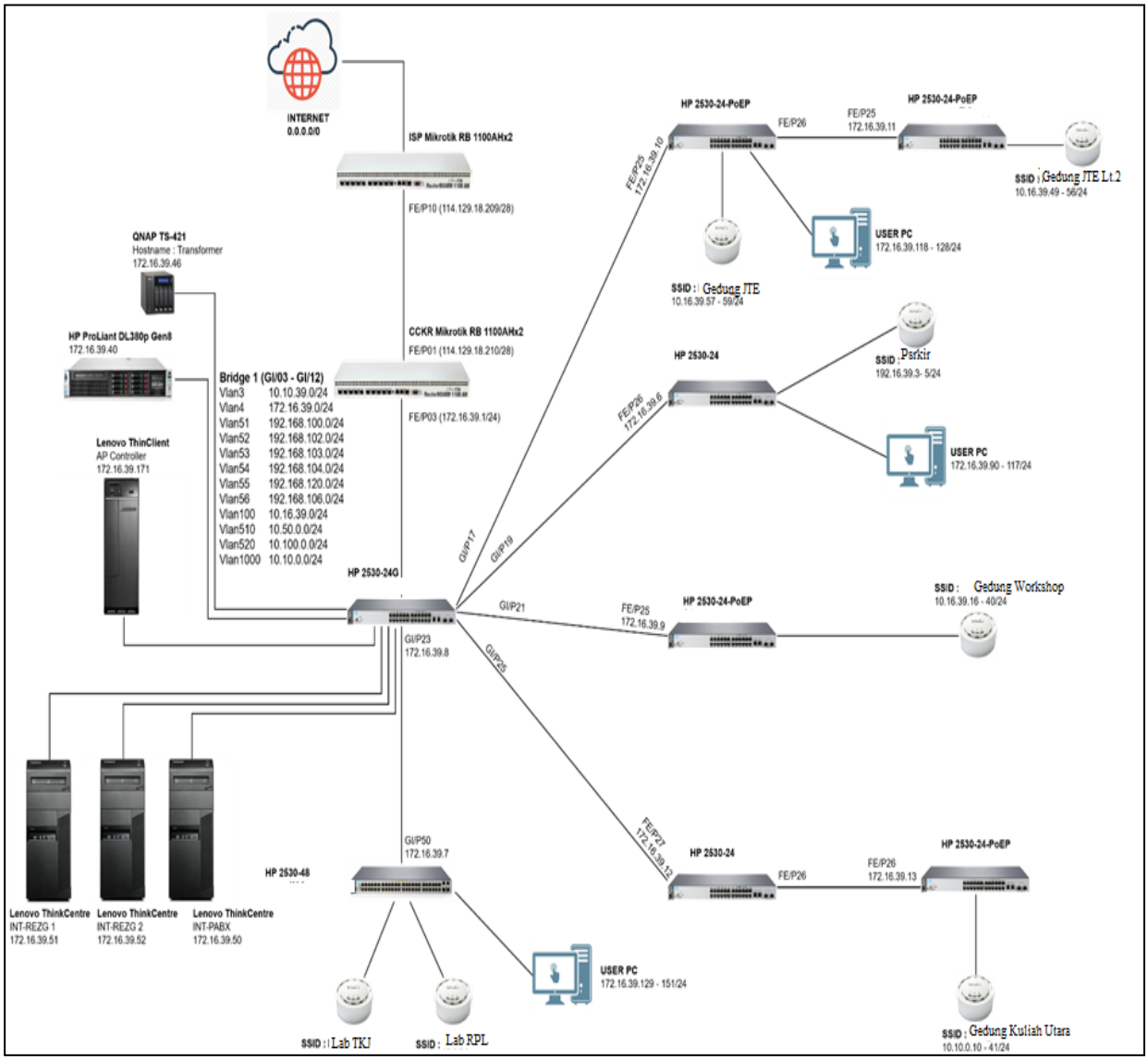

Figure 6. Design of a wifi pass hotspot.

Figure 6 explains the flow of the Wifi Pass hotspot that will run on the Department of Electrical Engineering (JTE) after the Radius Server is implemented as follows: users who are in a JTE location will choose one of the hotspots (SSID for wifi connection) according to where the visitor is located; There are 3 SSIDs that will appear. If a visitor is in the public area, the SSID that appears is JTE_PUBLIC, after connecting the Public Area, then the Public Log Page area will appear with 2 selected options, the first 3 hours season (3 hour session), this session login using a facebook account. Second is 15 minutes session, this session is only to be selected and directly connects to the internet after going through the authentication process. If the user is in the MI Study Program Lab, the user selects SSID: JTE_Lab TKJ and JTE_Lab Multimedia. The visitor selects SSID: JTE_ then the login page will appear as a username and password. The username is the NIP or NIM number and gets a random password from the front office of the process on Server Radius. If the user is in the main JTE Building, the user must log in to the SSID: JTE_Jurusan then the login page appears to enter the password. Password is a voucher that is valid for 6 months. As an easy alternative to monitoring, Mikrotik creates an application called The Dude. With this application we can manage our network. The Dude will automatically read or detect every device connected to a single segment network. For the

access point used in the JTE is the EnGenius Eap300 type access point, this access point is not supported by software for the access point controller, so the author uses The Dude, as an alternative application access point controller.

4. Implementation of research results

The Radius server configuration is done after installing VMware and Ubuntu Server 14.04. After the hardware preparation process is complete and VM ware is installed. the next step to building an authentication server is to install an operating system. This server uses the Ubuntu Server 14.04 operating system. At the installation stage this is quite easy because especially for Ubuntu Linux distributions themselves from version to newer version are made easier and familiar, both in installation and configuration. For the installation phase, just follow the steps, there are also Indonesian choices to simplify the installation process. Ubuntu Server 14.04 is used as an operating system because it is open source. So, it does not need to buy a license. In addition, Ubuntu Server 14.04 supports x64 bits and no GUI for better performance resources. The Radius Server in VMware has been set up, select the setting to extract the Ubuntu server ISO 14.04 file. Select one of these options when installing or later. if you choose to continue, you can manually choose what you want to install later. After Installing OS Linux Ubuntu is complete, continue to Ubuntu system operation [7]. The next step installing the web server and database server is to install the FreeRadius application on Ubuntu can be shown in Figure 7.

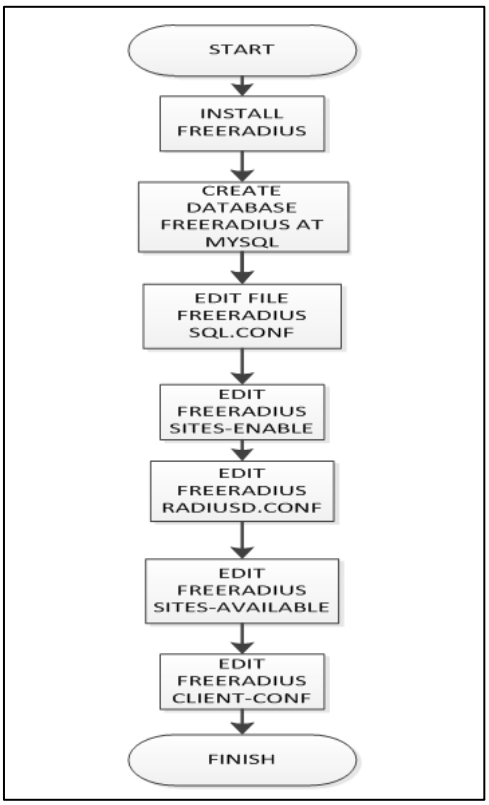

Figure 7. Free Radius configuration flow.

5. Design and analysis of the access point controller

One of the products is the Eap 300 type EnGenius brand access point. Eap 300 is not supported by software access point controller from the EnGenius brand, unlike the case with EnGenius type WDS which is supported by EZ access point controller. Eap300 consists of 3 indicator lights that sometimes light even if they do not emit a wifi signal. The dude is an alternative application because EAP 300 is not supported by the default access point controller from EnGenius [8]. As an easy alternative to

monitoring, Mikrotik creates an application called The Dude. With this application we can manage our network. The Dude will automatically read or detect every device connected to a single segment network.

Literature study data and field studies are obtained by focusing on the parameter variables that will be measured and then analysed that has been formulated in the framework of thinking namely Bandwidth, Throughput, Delay, Jitter and Packet loss, which is assisted by using tools namely NetStumbler, Axis NetTool, and Iperf, on the hotspot [9, 10].

Table 5. Comparison of QoS parameters with a barrier (fresnel zone).

Access Point	AP Signal (dBm)	Bandwidth (byte)	Throughput (byte)	Delay (ms)	Jitter (ms)	Packet Loss (%)
Building A (Department of Electrical Engineering)						
Ground Floor	31	696	184,595	9	7.457	0
Floor 1	46	828	174,658	14	2.297	0
Floor 2	50	758	198,735	10	5.472	0
Parking Area	43	623	39,519	11	18.140	0
Building B (Workshop)						
Ground floor	53	768	78,452	13	3.719	0
Practicum Lab	42	786	35,548	13	8.255	0
Building C (Laboratory)						
Ground Floor	34	453	18,346	14	36.777	3
Floor 2	38	1036	104,369	14	12.382	0
Total						3

Based on the Table 5, the hotspot network QoS at the Department of Electrical Engineering for the largest parameters are AP Signal 53 dBm, Bandwidth 1036 bytes, 198,735 bytes throughput, 14 ms delay, jitter 36.777 ms and packet loss 3%. The current QoS approach is diffServ, by dividing services into classes with a certain priority scale. In the diffServ model, packages are marked according to the type of service they need. When a packet has to be forwarded from an interface with a queue, packages that require low jitter are given priority over other queue packages. Usually, some bandwidth is allocated by default to control packets, while best effort traffic may only be given the remaining bandwidth. To get a good QoS, bandwidth usage settings are needed in the network as best as possible. HTB (Hierarchy Token Bucket) which is the latest technique and is very supportive for DD-WRT applications that are already in the Access Point. In addition, in an effort to maintain and improve the value of QoS, techniques are needed to provide network utilities, namely by classifying and prioritizing each information according to its characteristics.

6. Conclusions

Based on the background, objectives until the implementation of this authentication server, it can draw conclusions as follows. With this authentication server can protect wireless networks from MAC address spoofing and also WEP/WPA crack, that is by using FreeRadius authentication. In addition to improving security, this server also functions for bandwidth management for each user, so that the use of an internet connection is more optimal and is not misused by irresponsible parties. The existence of an access point controller for access point Eap300 using The Dude is very helpful in terms of monitoring existing access points. Based on the measured QoS table, the hotspot network at the Department of Electrical

Engineering for the largest parameter is AP Signal 53 dBm, Bandwidth 1036 bytes, throughput 198,735 bytes, 14 ms delay, jitter 36.777 ms and packet loss 3%. The technology used is 802.11 G Wi-Fi that uses DDWRT which has an Extensible Authentication Protocol (EAP) system that supports the implementation of facilities at Radius.

7. References

[1] Andress J 2011 *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice* (Amsterdam: Syngress Publishing)
[2] Shinder D 2013 *Understanding and Configuring Network Policy and Access Services in Server 2012* (Malta: TechGenix)
[3] Cisco 2016 *Radius Issue Resolution Guide* (California: Cisco Press)
[4] Coleman D D and Westcott D A 2015 *CWNA Certified Wireless Network Ad-ministrator Official Study Guide* (Indianapolis: Sybex)
[5] Cisco 2013 *Quick Start Guide Cisco Aironet 1130AG Access Point* (California: Cisco)
[6] Hucaby D 2016 *CCNA Wireless 200-355 Official Cert. Guide* (Indianapolis: Cisco Press)
[7] Rouse M 2016 *Network Access Control (NAC)* (Atlanta: TechTarget)
[8] Cisco 2013 *Configuration of WPA/WPA2 with Pre-Shared Key: IOS 15.2JB and Later*
[9] Granlund D *Secure and Scalable Roaming Support in Heterogeneous Access Networks* (Sweden: Luleå University of Technology)
[10] Jelinek J, Satrapa P and Fiser J 2015 *IEEE International Workshop of Electronics, Control, Measurement, Signals and Their Application to Mechatronics (ECMSM)*