Implementation of Bandwidth Management Authentication

Aulia Rahman[a,1], Haviluddin[b,2]

[a] *ICT Researcher, Universitas Mulawarman, East Kalimantan - Indonesia*
[b] *Faculty of Computer Science and Information Technology, Universitas Mulawarman, East Kalimantan - Indonesia*
[1] *auliarahman@ict.unmul.ac.id;* [2] *haviluddin@unmul.ac.id*

ARTICLE INFO

Article history:
Received
Revised
Accepted

Keywords:
Bandwidth
RADIUS
AAA
LAN
Wi-Fi

ABSTRACT

An internet traffic service mechanism includes monitoring and network security is indispensable. The main purpose of network monitoring is bandwidth optimizing and maintaining network security. This paper has described and implemented Remote Authentication Dial-In User Service (RADIUS) protocol and Authentication, Authorization and Accounting (AAA) server integrated with Mikrotik. The purpose of this article deal with the implementation of bandwidth management, which includes LAN (Local Area Network) and Wi-Fi (Wireless Fidelity) in Universitas Mulawarman. Based on experiment, the system is simple and easy to be used that controls and allocates bandwidth to users (lecturers, staff, and students) as they authenticate with LAN and Wi-Fi. Furthermore, network security perspective shows that users who are not registered to use the internet at the Universitas Mulawarman could be maintained as well.

2016 International Journal of Computing and Informatics (IJCANDI).
All rights reserved.

I. Introduction

Nowadays, an internet is playing a crucial role in providing service activities in modern organizations includes universities. An internet service at the university is dedicated to support the teaching and learning process with users includes lecturers or researchers, staff, and students. Furthermore, the traffic control mechanisms regulate in order to run internet properly is required.

Currently, Universitas Mulawarman has a bandwidth of 500 Mbps. This bandwidth leased from PT. TELKOM which consists of Astinet products with a bandwidth of 100 Mbps and IP Transit products with a bandwidth of 400 Mbps. Furthermore, the bandwidth is distributed to the faculties, institutes and units which managed by the ICT department through wired and wireless networks. Then, the network backbone topology are using a combination of bus and ring topologies with users includes lecturers or researchers of 1.500, staff of 1.200 and students of 35.000. Therefore, the traffic control mechanisms of internet services is indispensable. The main purposes of this mechanism is bandwidth more optimal and network more secure.

Many researchers have also conducted experiment on bandwidth management. Lu, et.al. (2014) Remote Authentication Dial-In User Service (RADIUS) and AAA authentication users was used to campus network security. This research was used Cisco AAA to set the certification, award, and billing safety. The research showed that the internet management much optimized and makes legal users visit all kinds' campus net resource safely [1]. Another researchers recommended that Radius have been controlled the user's limitation of bandwidth that used wireless access points (APs). This study confirmed that the bandwidth quota can be used effectively and efficiently by using RADIUS [2]. Andersson, et.al (2010) presented that a new mobility management scheme for heterogeneous wireless networks consists of mobile nodes, access networks and one home network. Any user has assigned one IP address in the home network and uses only this IP address regardless to attach the Internet. This paper have been used an Authentication, Authorization and Accounting (AAA) server in the home network maintains mappings of user names to IP addresses along with user credentials and other per-user data. The results of this paper was shown that bandwidth savings could reach 30% at the physical layer for VoIP type of applications when compared to existing standard Mobile IP architectures [3]. Islam and Atwood (2006) proposed that a framework to deploy AAA protocols. This study have been successfully to ensure revenue generation by controlling access to network resources using Authentication, Authorization and Accounting (AAA) protocols [4].

Therefore, this paper will study bandwidth implementation using Remote Authentication Dial-In User Service (RADIUS) protocol and Authentication, Authorization and Accounting (AAA) server integrated with

Mikrotik in order to address the issue of bandwidth management at Universitas Mulawarman. This paper consists of four sections. Introduction section is the motivation to do the writing of the article. Next, the methodology is describe the system. Third section is the analysis and discussion results, and finally conclusion section is research summaries.

II. Methodology

The bandwidth management is a set of techniques and tools that aimed to critical segments reducing within the network which includes data compression, bandwidth prioritization based on certain criteria, blocking, traffic shaping, traffic controlling, and others. The purposes of bandwidth management is to optimize network performance in order to be secured [1, 3]. In this study, internet service management of LAN (Local Area Network) and Wi-Fi (Wireless Fidelity) and integrated with network security by applying user traffic limitation mechanism using the Radius protocol and Authentication, Authorization and Accounting (AAA) server to implement bandwidth management has been proposed.

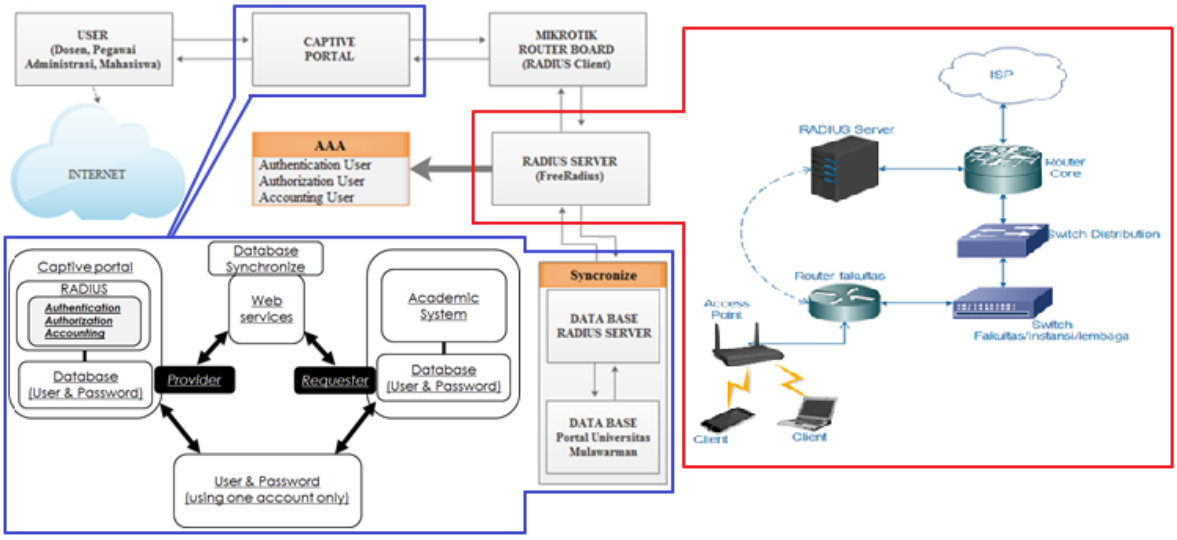


Fig. 1. Scenario of user authentication and Radius server topology

In this scenario, the user identity (username and password) need to fill in through a captive portal web page before access the internet is required. This process consists of two schemes, namely provider and requester web services. The scheme provider web service is to determine the function of public information data sources such as database connections and data name (i.e. resource parameters, and input-output format). Meanwhile, the scheme requester web service is a user identity requested in captive portal web page and Radius server via XML web service. Then, the user identity will be matched in the Radius server and university portal databases through Mikrotik. If correct identity, the user is allowed to access the internet. Otherwise, incorrect identity or no identity (no registered) in the Radius sever and university portal databases, then the user is not allowed to access the internet. The scenario of user authentication and Radius server topology that integrated of internet web services management can be seen in **Fig. 1**.

Next, we will discuss the bandwidth management supporting packets and services that open source (non-proprietary) software in the following five sub-sections. The first deals with Mikrotik as router operating system, the second deals with Linux Slackware64 13.37 as an operating system for Radius server, the third deals with Apache, PHP and MySQL as a web server packets, the four deals with freeRadius as a packet to build Radius server, and the five deals with daloRadius and MySQL daloRadius export data to radius table in Radius server as a radius administrator web template management. In this study, bandwidth management success is also measured in several ways includes user authentication request response time to Radius server, user authentication compatibility into Radius server, and user authentication success in using captive portal. Furthermore, the bandwidth management measurement software are using NTRadPing Test Utility, Radius server console, and web browser.

A. Mikrotik

Mikrotik are tools (i.e. routers, switches, antenna, and other supporting devices) and software (MikroTik RouterOS) based on Linux that serve for internet connectivity. Mikrotik has created by John Trully and Arnis Riekstins in 1996. As simply, Mikrotik is a router operating system that regulates the network activities [5]. In this study, Mikrotik will be used as an operating system that support software and hardware devices for bandwidth management.

B. *Captive portal*

A captive portal or gate portal is a user web page portal that must be accessed before access the internet. In general, captive portals are typically used in places that offer free Wi-Fi hotspot and wired network for internet users. The captive portal has a main component consists of Radius server and router machine that a traffic filter function from internal to external network. The main purpose captive portal is the user forcing fill in their identity (username and password) before the internet access provided and also blocking unwanted connections by the Radius server. In working principle, user will acquire an IP address (DHCP - Dynamic Host Configuration Protocol) after they do verification or fill in the registration (login) form. If the identity is correct then the user could be given access the internet [6]. The scenario of captive portal can be seen in **Fig. 2**.

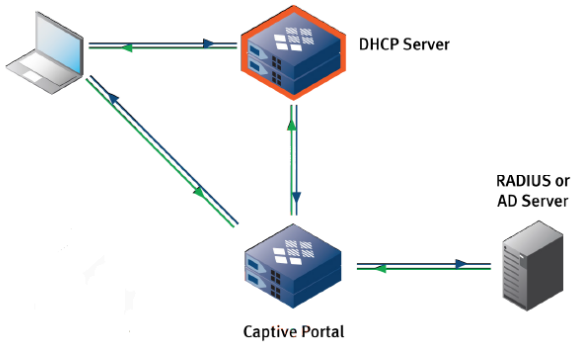


Fig. 2. Scenario of captive portal

C. *Linux Slackware*

Slackware is a Linux distribution free and open source software that has created by Patrick Volkerding in 1993. Slackware has been the basis for many other Linux distributions that the oldest currently being maintained. Slackware aims for design stability and simplicity, provides no graphical installation procedure and no automatic dependency resolution, and available for the IA-32 and x86-64 with a port to the ARM architecture [7]. In this paper, Slackware64 13.37 will be used as operating system.

D. *RADIUS server*

Radius stands for Remote Authentication Dial-In User Service which serves to provide security mechanisms and users management. Security mechanism is a distributed client-server systems with user authentication. Furthermore, Radius is developed for the Authentication, Authorization, and Accounting (AAA), which an access control mechanism that checks and authenticates users by applying challenge or response methods. It means that user management is the user types allocation [8]. An authentication is the checking mechanism and user identity validation to access the network. In general, this process begins with the delivery of a unique codes such as usernames, passwords, pins, finger-prints to the server. On the server side, the system will receive and compare the unique codes in the database. If verified, the server is able to be send the user permissions. Or, not verified, the server should be deny the user permissions. Afterwards, an authorization is allocating any service that users could be accessed on the network. Then, an authorization is eligible when user declared to use the network. Furthermore, an accounting is a process performed by the network access server (NAS) and AAA server that records all user activity in the network, such as duration time (start and terminate), accessed data, and others. Next, all information obtained from the accounting process is stored in the AAA server, and could be used for various purposes such as billing, auditing, or network management [1, 9, 10]. In this study, implementation of bandwidth management will be integrated with Mikrotik.

E. *freeRadius*

freeRadius is a Radius server application. freeRadius has been developed by Daniël de Kok dan Miqual van Smoorenburg in 1999. In general, freeRadius is used to perform remote access using connections such as dial-up, virtual private network (VPN), wireless access points, and Ethernet switches [10]. In this study, freeRadius will be integrated with Radius server.

F. *Apache, PHP and MySQL*

Apache HTTP Server or Web Server/WWW Apache is a web server that could be execute on many operating systems such as UNIX, BSD, Linux, Microsoft Windows, Novell Netware and other platforms. Apache HTTP server is useful to serve and execute on a web site that features such as error messages, authentication, and others. Apache is also supported by a number of graphical user interface (GUI) that allows to handling server becomes easy. Next, PHP stands for PHP: Hypertext Preprocessor which HTML-embedded scripting language. PHP is an open-source software, server-side scripting language used to generate dynamic web-pages that integrated with many popular databases. PHP scripts have a file extension is .php*x* (*x* means

version of PHP). Furthermore, MySQL stands for Structured Query Language which is a kind of relational database management system supported by Oracle Corporation. MySQL is one of the most popular open source database server that ideal for both small and large applications, also compiles on a number of platforms. MySQL could be query a database for specific information and have a record-set returned that supports standard SQL [11]. In this study, PHP, MySQL will be used for user web page template interface.

G. daloRadius

daloRadius is a web templates software management for the Radius server that has been built using freeRadius that written in PHP and JavaScript. daloRadius is used a database abstraction layer that supports many database systems such as MySQL, PostgreSQL, SQLite and MSSQL. In general, daloRadius is used to hotspots manage as an internet service provider (ISP) that have features for internet users managing, graphical reporting, accounting, and integrated with GoogleMaps for geo-location (GIS). daloRadius have attributes to assist CRUD (Create, Read, Update and Delete) on the freeRadius database. The purpose using daloRadius is easy to manage Radius server for hotspots and wireless accounts using Linux (i.e. slackware) command (console) by administrator through web browser [12]. In this study, daloRadius-0.9-8 as a virtual machine is used for administrator web page template interface.

H. NTRadPing test utility

NTRadPing is a free Radius client program offered by MasterSoft Inc., developer of the DialWays server. The NTRadPing could be simulate authentication and accounting requests and send them to Radius server as a NAS client [13]. In this study, NTRadPing test utility 1.5 is used as a virtual machine to support Radius server.

III. Results and Discussions

This section describes the process of designing and implementing bandwidth management. The first stage, Radius server were installed and configured. The second stage, Radius server with university portal databases using XML web service was synchronized. This process was created a user group (lecturers, staff, and students). The third stage, Radius client on Mikrotik were installed and configured. The fourth stage, web page template using daloradius-0.9-8 for administrator was designed. The last stage, web page template using PHP and MySQL for user was created.

A. Installation and configuration of Radius server

The first phase, installed and configured of Radius server have been conducted. This scenario explained that the user authenticated of wireless (hotspot) via the login form webpage. The user identify (username and password) to access the network on the Radius server has been received and matched. In this experiment, the user authorization files in the Radius server included `radiusd.conf`, `mysql.conf`, `clients.conf` and `/usr/local/etc/raddb/sites-enabled/default` have been configured. Meanwhile, to active the Radius server (via console) scenario was executed `#/usr/local/sbin/radiusd`.

B. Synchronization of RADIUS server database

The second phase, Radius server and university portal databases using XML web service have been synchronized. In this test, user requested in captive portal web page and Radius server, and university portal databases have been detected and approved by XML web service. On the provider scheme, the user connections could be used wired or wireless in a campus area have been permitted. The configuration of Radius server database synchronized as a display in **Fig. 3**.

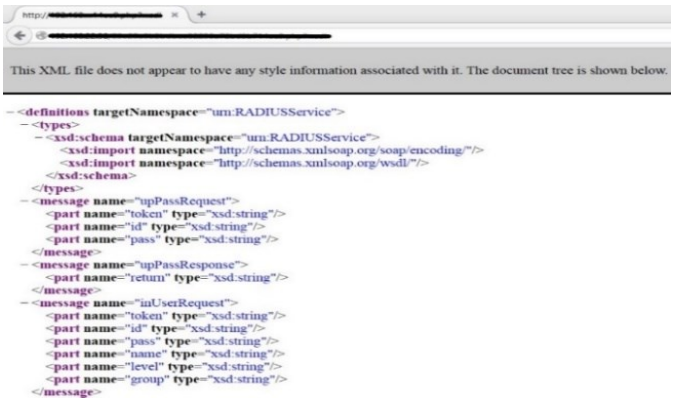


Fig. 3. The configuration of Radius server database synchronize

C. Process of installation and configuration Radius client in Mikrotik

The third phase, Radius client setting on Mikrotik have been configured. In this test, the completed user identity (username and password) in captive portal web page then processed by the Radius server have been required. The configuration syntax of Radius client in Mikrotik, as a follows.

```
import ssl
copy STAR_unmul_ac_id.key and STAR_unmul_ac_id.crt to router
certificate import file-name=STAR_unmul_ac_id.crt
certificate import file-name=STAR_unmul_ac_id.key
copy dir hotspot
       drag n drop hotspot folder to files in router
add radius and walled
/radius add accounting-backup=no accounting-port=1813 address=192.168.xx.xx authentication-
port=1812 called-id="" disabled=no domain="" realm="" secret=xxxxxxx service=login,hotspot
timeout=300ms
/ip hotspot walled-garden ip
add action=accept disabled=no dst-address=192.168.22.0/26
add action=accept disabled=no dst-address=203.130.214.104/29
setting hotspot
addresses per mac = 1
login by = HTTPS, HTTP PAP
radius = Use Radius
ip hotspot set 0,1,2,3,4,5 addresses-per-mac=1
ip hotspot profile set 0,1,2,3,4,5,6 login-by=http-pap,https ssl-certificate=cert1 use-
radius=yes
```

D. Web page template design for administrator

The four phase, administrator web page template interface design using daloRadius-0.9-8 that integrated to Radius server have been proposed. First, the daloRadius-0.9-8 have been installed. Next, administrator database using MySQL daloRadius export data have been created. Second, the administrator web page template interface have been customized, **Fig. 4**. In this test, the administrator menu settings such as the user hotspot, user portal, group hotspot, top user and active user has been configured. The daloRadius-0.9-8 installation process as shown below.

```
root# cd /usr/local/src
wget <URL_daloRADIUS>
http://sourceforge.net/projects/daloradius/files/daloradius/daloradius-0.9-8/daloradius-
0.9-8.tar.gz/download
root#tar -xzvf daloradius-0.9-8.tar.gz -C /var/www
root#mv /var/www/daloradius-0.9-8 /var/www/daloradius
##Tahap pembuatan database radius
root #mysql -u root -p
password: (diisi password mysql)
mysql>create database radius;
mysql>exit
root# mysql -u root -p radius < /var/www/daloradius/contrib/db/fr2-mysql-daloradius-and-
freeradius.sql
password :
root#
##Username yang akan dijadikan untuk authentication:
root#mysql -u root -p
password :
mysql>use radius;
mysql>INSERT INTO radcheck (UserName, Attribute, Value) VALUES ("coba", "Password",
"coba");
mysql>exit
```

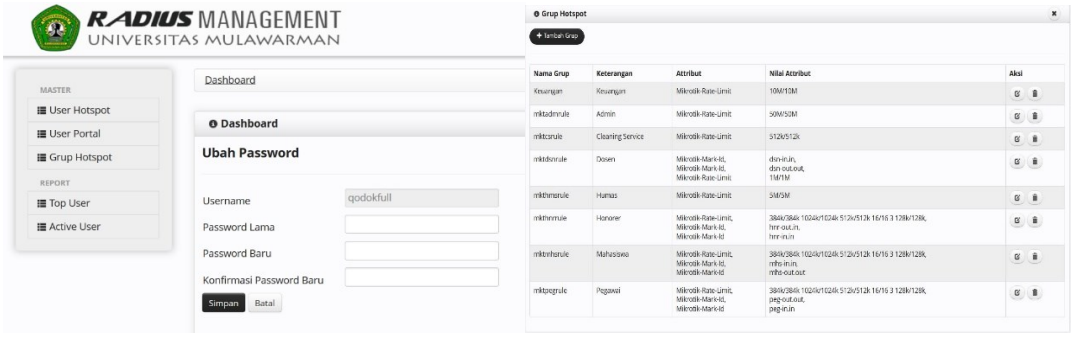


Fig. 4. Administrator web page interface

E. Web page template design for user

The five phase, user web page template interface design using PHP, MySQL, and dreamweaver CS5.5 as an editor have been developed. In this experiment, the web page login interface can be seen in **Fig. 5**.

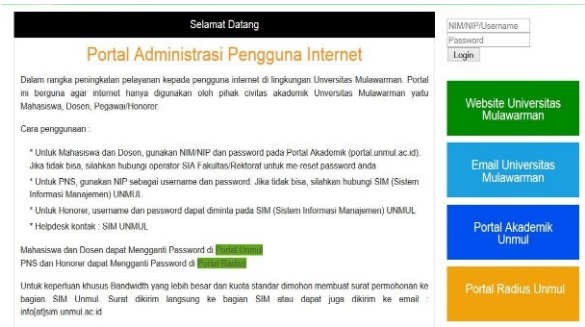


Fig. 5. User web page login interface

F. User authetication testing

In this experiment, user requested response time to Radius server, user identity matched on Radius server and user accessed on captive portal using testing software such as NTRadPing Test Utility, Radius server console, and web browser have also been investigated. In this test, student as a user sample to access the network was used. In **Fig. 6**, user request response time to Radius server using NTRadPing shows that average of 0 – 1000 milliseconds. In **Fig. 7(a, b)**, user identity (username and password) matched on Radius server when access to network indicated that two schemes includes *access-accept packet* and *access-reject packet*. First scheme indicated that user accepted to access the internet. Second scheme indicated that user not accepted to access the internet. In **Fig. 8(a, b)**, user accessed on captive portal scheme shows that user has been automatically forwarded to the http://www.unmul.ac.id website.

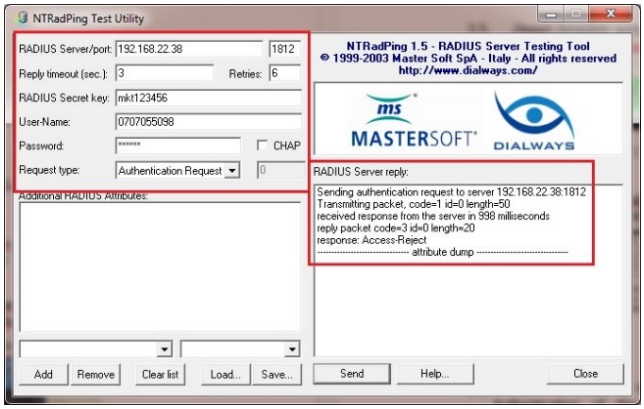
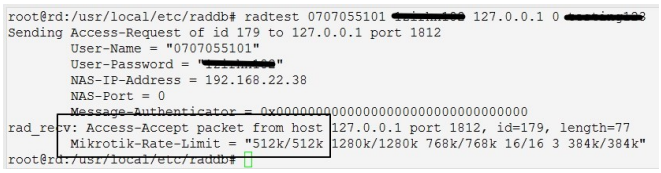
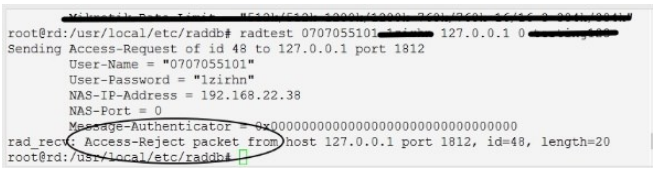


Fig. 6. User request response time to Radius server using NTRadPing

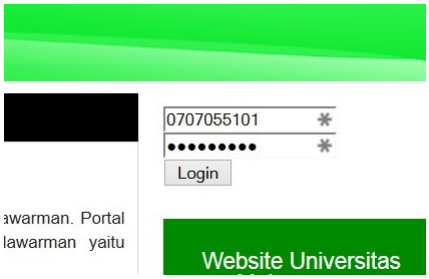


(a)



(b)

Fig. 7. User identity matches on Radius server using console; (a) *access-accept packet*, (b) *access-reject packet*



(a)

(b)

Fig. 8. User access on the captive portal; (a) captive portal web page, (b) http://www.unmul.ac.id website

IV. Conclusions

This paper discusses of user authentication management on the LAN and Wi-Fi at Universitas Mulawarman. All stages, in the bandwidth management by using Remote Authentication Dial-In User Service (RADIUS) protocol and Authentication, Authorization and Accounting server (AAA) that integrated with Mikrotik have been implemented. Based on experiment, the system is simple and easy to be used especially for controls and allocates bandwidth users (lecturers, staff, and students). Hence, the captive portal is able to provide convenience for the administrator in monitoring users who access the internet. Furthermore, network security perspective shows that users who are not registered to use the internet could be maintained as well. Means that it makes legal users visit all kinds' campus net resource (LAN and Wi-Fi) safely.

Acknowledgment

This study has been completed, thanks to the help and support from various parties that cannot be mentioned one by one. Researchers say a big thank you to family of ICT Universitas Mulawarman who has given support to complete this study. Hopefully this research can be useful.

References

[1] Y. Lu, X. Z. Chen, W. Wang, and Y. Yang, "Based on the RADIUS and AAA Authentication of the Campus Networks Security System Design and Implementation," *TELKOMNIKA,* vol. 12, No.4, April 2014, p. 3040 ~ 3045, 2013.
[2] A. Peart and A. Good, "Wireless Bandwidth Management Authentication Improving Quality of Service," *Academic Journal of Manufacturing Engineering,* vol. 10, Issue 3/2012, pp. 6-11, 2012.
[3] K. Andersson, D. Granlund, M. Elkotob, and C. Åhlund, "Bandwidth Efficient Mobility Management for Heterogeneous Wireless Networks," in *the IEEE CCNC 2010*, 2010.
[4] S. Islam and J. W. Atwood, "A Framework to Add AAA Functionalities in IP Multicast," in *International Conference on Internet and Web Applications and Services (AICT/ICIW 2006)*, 2006.
[5] T. Shahaf, "Mikrotik Router OS - Setup and Configuration Guide for Aradial Radius Server," vol. July 2012, ed: © 2012 Aradial & Spotngo, 2012.
[6] S. Note, "Captive Portal (Authenticated DHCP)," ed: 2013 Infoblox Inc. All Rights Reserved, 2013.
[7] D. de-Kok. (2008). *Slackware Linux Basics: For Slackware Linux 12.0*.

[8] L. Wang, M. Song, Y. Zhang, Y. Man, P. Wang, and J. Song, "Research on the Hierarchy AAA Scheme for Interworking Authentication in Heterogeneous Networks," in *2008 International Conference on MultiMedia and Information Technology*, 2008, pp. 586-589.
[9] A. Peart and M. Adda, "Quality of Service: Dynamic Authentication Bandwidth Management for the Wireless Environment," in *The 1st International Conference on Information Science and Engineering (ICISE2009)*, 2009, pp. 5366-5369.
[10] RADIUS, "The FreeRadius Technical Guide," 2014.
[11] E. S. Walia and E. S. K. Gill, "A Framework for Web Based Student Record Management System using PHP," *International Journal of Computer Science and Mobile Computing,* vol. 3, Issue. 8, August 2014, pp. 24 – 33, 2014.
[12] L. Tal, "Virtual Machine daloRADIUS Administrator Guide Version 0.9-9," 2011.
[13] S. H. Kim, "Setting up SiteMinder Radius Authentication," 2010.