Implementasi Freeradius Berbasis Lightweight Directory Access Protocol Pada Management Infrastruktur Jaringan Internet Service Provider

Danang Widyatmoko[1], Umniy Salamah[2]
Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana
Jl. Raya Meruya Selatan, Kembangan, Jakarta, 11650
danang.widyatmoko@gmail.com[1],
umniy.salamah@mercubuana.ac.id[2]

Abstrak **-- Internet Service Providers as a provider networks and the internet certainly has a network infrastructure that is scattered everywhere. The greater an internet service provider is certainly the more infrastructure owned. The infrastructure need to be managed and accessed to be configured to function as desired. In managing all these devices we need a legitimate authentication and authorization to gain access to the device. Problems in a large internet service provider which has been very much the number of devices, device management becomes an issue. Conventional System authentication and authorization which user database is stored on each device would be inefficient for any network administrator. The need created system permissions settings centrally to facilitate performance of network administrators in monitoring the network conditions. In this final project-based system freeradius ldap using LDAP as a directory of data can be accessed over a network. Then it will be made an analysis of the LDAP-based FreeRADIUS. After analysis of the FreeRADIUS LDAP-based, it can be concluded that in order to help streamline access rights be integrated to be made in the system centrally**

Keywords : **Autentication, Autorization, Radius, LDAP.**

Abstrak -- Internet Service Provider sebagai penyedia jaringan dan internet tentunya memiliki infrastruktur jaringan yang tersebar dimana-mana. Semakin besar sebuah internet service provider tentu semakin banyak pula infrastruktur yang dimiliki. Infrastuktur tersebut membutuhkan untuk dimanage dan diakses untuk dikonfigurasi agar dapat berfungsi seperti yang diinginkan. Dalam memanage semua perangkat tersebut kita membutuhkan otentikasi dan otorisasi yang sah untuk mendapatkan akses ke perangkat. Permasalahan dalam sebuah internet service provider yang besar dimana jumlah perangkat sudah sangat banyak, managemen perangkat menjadi sebuah issue. System otentikasi dan otorisasi konvensional dimana database user tersimpan disetiap perangkat tentu akan menjadi tidak efisien untuk setiap administrator jaringan. Maka dari itu perlu dibuat system pengaturan hak akses secara terpusat untuk memudahkan kinerja network administrator dalam monitoring kondisi jaringan. Dalam proyek akhir ini dibuat system freeradius berbasis ldap dengan menggunakan LDAP sebagai data directory user dapat diakses melalui jaringan. Kemudian akan dibuat analisa terhadap freeradius berbasis LDAP. Setelah dilakukan analisa terhadap freeradius berbasis LDAP tersebut, maka dapat disimpulkan bahwa untuk membantu mengefektifkan hak akses menjadi terintegrasi harus dibuat di dalam sistem secara terpusat.

Kata Kunci: **Autentication, Autorization, Radius, LDAP.**

I. PENDAHULUAN

A. Latar belakang

Saat Saat Semua perangkat di dalam jaringan internet service provider memiliki fungsi yang sudah ditetapkan dalam sebuah desain network. Person yang memegang hak akses ke perangkat jaringan adalah orang yang memahami topologi desain dan fungsi-fungsi dalam jaringan. Oleh karena itu salah satu hal yang paling penting untuk menjaga agar semua perangkat dapat berfungsi dengan sebagai mana mestinya adalah memastikan agar perangkat tersebut hanya bisa diakses oleh orang yang memiliki wewenang. Hak akses tersebut adalah otentikasi dan otorisasi yang sah untuk mendapatkan akses ke perangkat. Dalam software perangkat tersebut didefiniskan user dan kewenangannya berdasarkan kebijakan-kebijakan perusahaan. Jadi, di setiap memori perangkat tersimpan database user.

Permasalahan baru yang penulis hadapi adalah dalam sebuah internet service provider yang besar dimana jumlah perangkat sudah sangat banyak, managemen perangkat menjadi sebuah issue. Sistem otentikasi dan otorisasi konvensional dimana setiap database user tersimpan disetiap perangkat tentu akan menjadi tidaklah efisien dalam manajemen perangkat. Permasalahan-permasalahan yang sering ditemui ketika menggunakan system otentikasi dan otorisasi konvensional adalah :

1. Tidak efisien dalam mengelola hak akses karena system tidak terpusat.
2. Factor manusia (human error) adalah celah keamanan karena terlalu banyaknya jumlah perangkat sehingga terkadang lepas dari pengawasan.
3. Bila ada karyawan baru atau karyawan resign harus membuat/menghapus hak akses di masing-masing perangkat, baik itu router, switch, server, dan intermediate device lainnya. Situasi ini sangatlah tidak efisien.

Setelah melihat permasalahan tersebut maka dalam proyek akhir ini akan mengangkat tema "Impelementasi freeradius berbabis ldap pada management jaringan infrastruktur internet service provider" yang bertujuan meningkatkan tingkat akses keamanan jaringan menjadi semakin baik.

Proyek akhir menggambil gambaran studi kasus pada internet service provider yang memudahkan bagi network administrator untuk pengaturan hak akses secara terpusat.

B. Rumusan Masalah.

Berdasarkan latar belakang penyusunan proyek akhir yang telah diuraikan sebelumnya, permasalahan yang dihadapi dirumuskan sebagai berikut:

1. Bagaimana cara membuat user untuk hak akses perangkat secara terpusat menggunakan FreeRADIUS berbasis LDAP ?
2. Bagaimana cara mengupdate user untuk hak akses perangkat secara terpusat menggunakan FreeRADIUS berbasis LDAP ?
3. Bagaimana cara menghapus user untuk hak akses perangkat secara terpusat menggunakan FreeRADIUS berbasis LDAP ?

II. LANDASAN TEORI

A. LDAP

Menurut Cartealy (2013, p75), Lightweight Directory Access Protocol (LDAP) merupakan protokol yang mendefinisikan bagaimana data directory dapat diakses melalui jaringan. LDAP biasa digunakan untuk menyimpan berbagai informasi terpusat yang dapat diakses oleh berbagai macam mesin atau aplikasi dari jaringan. Penggunaan LDAP di dalam sistem akan membuat pencarian informasi menjadi terintegrasi dan sangat mudah. sebagai contoh, LDAP seringkali digunakan untuk menyimpan nama pengguna dan sandi yang terdapat di dalam sistem secara terpusat

B. RADIUS

RADIUS merupakan singkatan dari Remote Acces Dial in User Service. Pertama kali di kembangkan oleh Livingston Enterprises. Merupakan network protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar. RADIUS didefinisikan di dalam RFC 2865 dan RFC 2866. RADIUS biasa digunakan oleh perusahaan untuk mengatur akses ke internet bagiclient.RADIUS merupakan singkatan dari Remote Acces Dial in User Service. Pertama kali di kembangkan oleh Livingston Enterprises. Merupakan network protokol keamanan komputer yang digunakan untuk membuat manajemen akses secara terkontrol pada sebuah jaringan yang besar. RADIUS didefinisikan di dalam RFC 2865 dan RFC 2866. RADIUS biasa digunakan oleh perusahaan untuk mengatur akses ke internet bagiclient.

III. ANALISA DAN PERANCANGAN

Pada bab ini akan dilakukan analisis kebutuhan dan perancangan dalam pembuatan proyek akhir "Implementasi freeradius berbasis ldap pada management infrastruktur jaringan internet service provider". Berikut adalah analisis dan perancangan dari proyek akhir ini

A. Pengumpulan Data

1. Pencarian referensi yang berhubungan dengan cara kerja dan penggunaan radius menggunakan freeradius
2. Pencarian referensi yang berhubungan dengan cara kerja dan penggunaan ldap menggunakan openldap dan phpldapadmin..
3. Pencarian refrensi tentang pengintegrasian radius berbabis ldap dengan perangkat cisco switch, router dan mikrotik dalam hak akses.

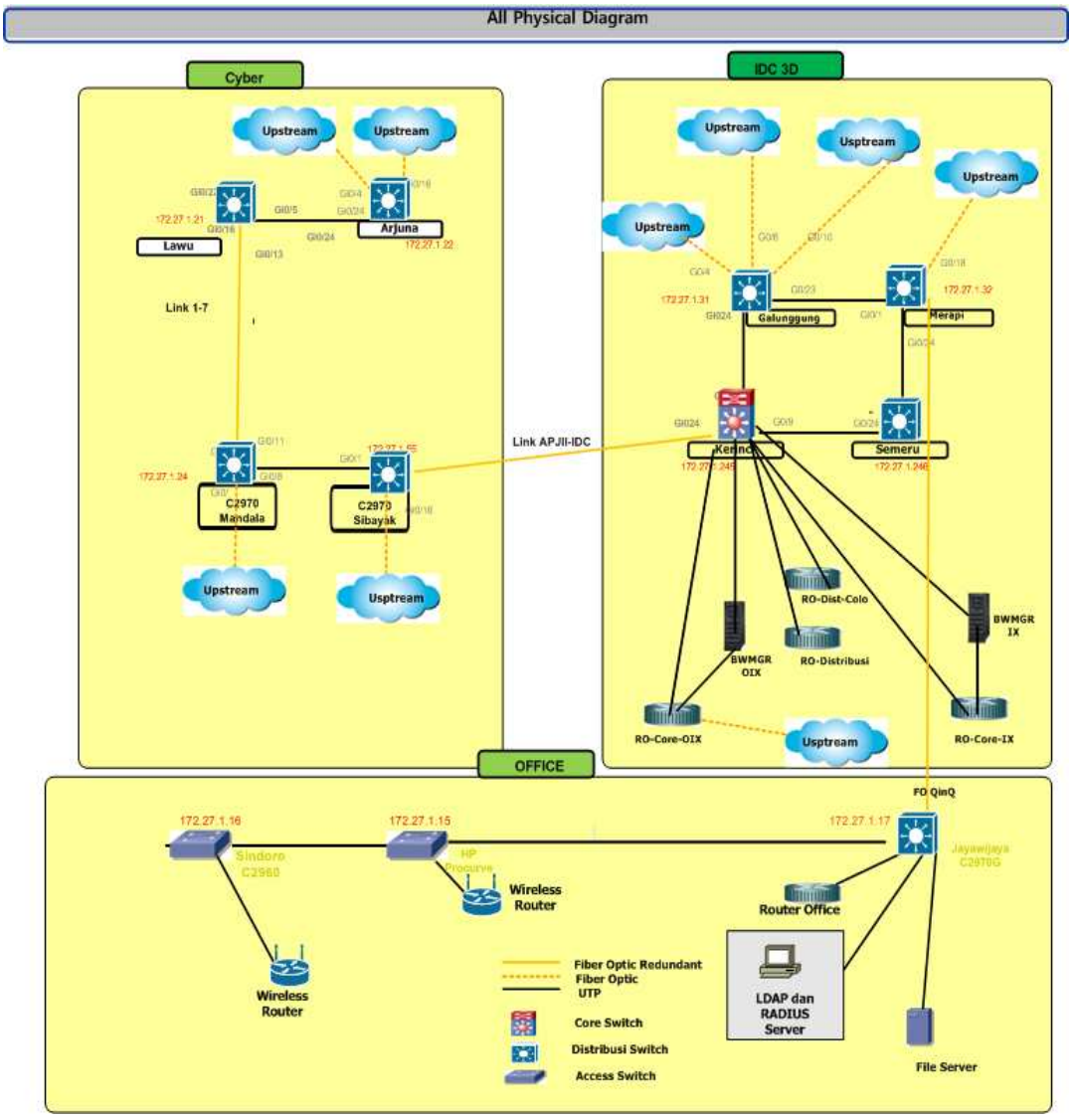
B. Analisa Sistem Berjalan

Berdasarkan hasil pengamatan penulis pada system yang berjalan di internet service provider untuk database user masih tersimpan disetiap perangkat tentu akan menjadi tidaklah efisien dalam manajemen perangkat. Hal ini bisa menimbulkan banyak kendala yang membuat pekerjaan menjadi tidak optimal. Sebagai contoh :

1) Tidak efisien dalam mengelola hak akses karena system tidak terpusat.
2) Bila ada karyawan baru atau karyawan resign harus membuat/menghapus hak akses di masing-masing perangkat, baik itu router, switch, mikrotik, dan intermediate device lainnya. Situasi ini sangatlah tidak efisien.

C. Perancangan dan Desain Sistem

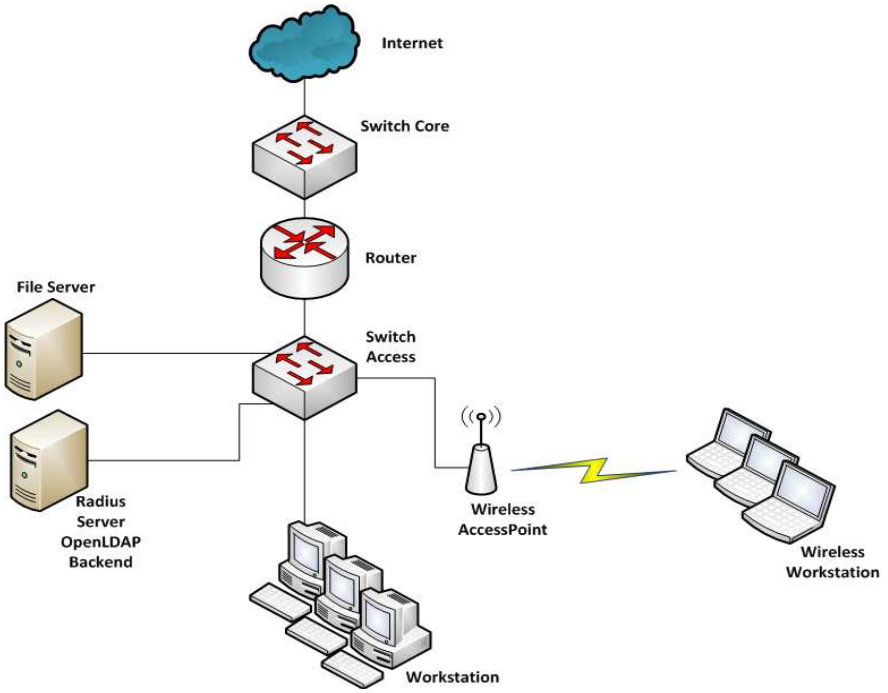
Pada proyek akhir ini akan dibuat sistem radius berbasis ldap untuk hak akses manajemen perangkat secara terpusat. Berikut adalah rancangan topologi fisik jaringan.



Gambar 1. Skema perancangan penambahan RADIUS dan LDAP server dalam topologi fiaik jaringan

Berdasarkan hasil analisis permasalahan di atas, perancangan sistem secara fisik dilakukan dengan penambahan dan pengalihan fungsi server. Penambahan yang dilakukan dengan memasang RADIUS dan LDAP server. Secara fisik kedua server tersebut diletakkan pada mesin server yang sama. Server LDAP berfungsi sebagai direktori untuk menyimpan akun user, sedangkan server RADIUS berfungsi untuk melakukan proses AAA pada sistem perangkat yang ada.

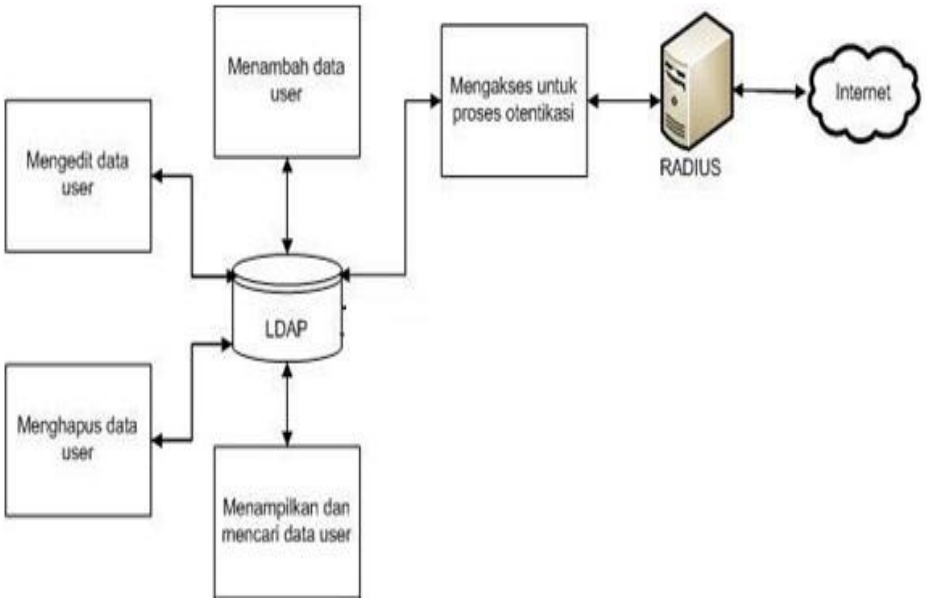
Skema perancangan sistem secara logis disajikan pada Gambar 2.



Gambar 2. Skema Perancangan Sistem secara logis

Perancangan dari Gambar 2 dapat dilihat hubungan antara LDAP dengan RADIUS. Saat user akan mengakses perangkat, user harus memasukkan ID (username dan password) yang akan diproses oleh RADIUS. RADIUS akan mengambil data dari LDAP saat melakukan otentikasi ID user. Setelah ID terotentikasi, RADIUS akan melakukan proses otorisasi pemberian izin akses untuk user.

Diagram ALIR Rancangan Back-end disajikan pada Gambar 3.



.

Gambar 3. Skema hubungan sistem back-end secara umum

Pada sisi back-end, LDAP berhubungan dengan berbagai proses, yaitu menambah data user baru, mengubah data yang sudah ada, menampilkan dan mencari data user, menghapus data user, proses otentikasi RADIUS.

D. Kebutuhan Perangkat Lunak.

Perangkat lunak yang dibutuhkan dalam mebangun sistem ini disajikan pada Tabel 1.

TABLE 1.
KEBUTUHAN PERANGKAT LUNAK

No.	Perangkat Lunak	Versi
1.	FreeRADIUS	2.2.8
2.	phpLDAPadmin	1.2
3.	Slapd	2.4.42
4.	Openldapscript	-
5.	Ubuntu	Versi 16.04 LTS
6.	Apache	2.4.18
7.	Smldap-tools	-
8.	Putty	-
9.	Winbox	2.2.18
10.	Mozilla Browser	Versi 47

E. Skenario Sistem

Pada Proyek Akhir ini yang berjudul " Implementasi freeradius berbasis ldap pada management infrastruktur jaringan internet service provider " akan dibuat skenario implentasi dan pengujian sistem, yaitu :

1. Sistem freeradius berbasis ldap ini akan dibuat pada jaringan local area network (LAN) dengan pengalamatan IPv4 dan dibuat berupa *Prototype*.
2. Radius yang akan dipakai sebagai hak akses ke perangkat menggunakan platform *freeradius*.
3. LDAP yang akan dipakai sebagai direktori data user yang akan dipakai menggunakan platform openldap dan phpldapmin.
4. Pada server dibuat *prototype* menggunakan Ubuntu Server dan perangkat cisco switch, router dan miktorik.
5. Komunikasi antara server dengan perangkat menggunakan *local area network*.

IV. IMPLEMENTASI DAN PENGUJIAN

A. Implementasi

Implementasi Free Radius berbasis Idap melalui beberapa tahapan, yaitu:

1. Konfigurasi OpenLDAP

Pada OpenLDAP perlu dilakukan beberapa konfigurasi antara lain :

- Network Configuration

Network Configuration merupakan tahap awal setelah server diinstall operating system, yang berfungsi untuk komunikasi antar network dan penginstalan OpenLDAP. Konfigurasi network seperti berikut:

```
[root@aaa:~]# nano /etc/network/interfaces
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto ens18
iface ens18 inet static
 address 192.168.1.71
 netmask 255.255.255.0
 gateway 192.168.1.50
 dns-nameservers 117.102.253.44 202.6.233.11
 dns-search padi.net.id
```

Setelah itu dilakukan restart network service dengan cara seperti berikut:

```
[root@aaa:~]# /etc/init.d/networking restart
```

Dan terakhir harus dipastikan service network *tersebut auto start on first boot* dengan cara :

```
[root@aaa ~]# Chkconfig network on
```

- Instalasi dan Configure OpenLDAP

Pada tahap awal untuk OpenLDAP adalah instalasi packet. OpenLDAP meliputi slapd (stand-alone LDAP daemon) dan libraries (LDAP protocol , tools dan sample clients). Untuk caranya yaitu:

```
[root@aaa ~]# apt-get install slapd ldap-utils
```

Setelah diinstall perlu mengkonfigurasi beberapa bagian antara lain 'BASE' and 'URI' diganti dengan nama domain dan IP adress. Ini berfungsi sebagai nama domain dan localhost. Untuk konfigurasinya antara lain:

```
# nano /etc/ldap/ldap.conf
#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world writable.

BASE    dc=padi,dc=net,dc=id
URI     ldap://localhost ldap://localhost:666

#SIZELIMIT      12
#TIMELIMIT      15
#DEREF          never

# TLS certificates (needed for GnuTLS)
TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
#include         /etc/ldap/schema/radius.schema
```

Setelah itu lakukan rekonfigurasi slapd melalui:

```
root@aaa:~# dpkg-reconfigure slapd
```

Dan Terakhir harus dipastikan service OpenLDAP Server berjalan dengan cara seperti berikut:

```
root@aaa:~# ldapsearch –x
# extended LDIF
#
# LDAPv3
# base <dc=padi,dc=net,dc=id> (default) with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# padi.net.id
dn: dc=padi,dc=net,dc=id
objectClass: top
objectClass: dcObject
objectClass: organization
o: padinet
dc: padi

# admin, padi.net.id
dn: cn=admin,dc=padi,dc=net,dc=id
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator

# noc, padi.net.id
dn: cn=noc,dc=padi,dc=net,dc=id
gidNumber: 500
cn: noc
objectClass: posixGroup
objectClass: top

# danang widyatmoko, noc, padi.net.id
dn: cn=danang widyatmoko,cn=noc,dc=padi,dc=net,dc=id
cn: danang widyatmoko
givenName: danang
gidNumber: 500
homeDirectory: /home/users/danang
sn: widyatmoko
loginShell: /bin/sh
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
uidNumber: 1000
uid: danang

# search result
search: 2
result: 0 Success

# numResponses: 5
# numEntries: 4
```

• Instlasi phpLDAPadmin

phpLDAPadmin adalah administrasi LDAP berbasis web untuk mengelola server LDAP. Menggunakan phpLDAPadmin dapat menelusuri LDAP tree, LDAP schema, melakukan pencarian, membuat, menghapus, menyalin dan mengedit LDAP entri. Install phpLDAPadmin paket seperti berikut:

```
root@aaa:~# sudo apt-get install phpldapadmin
```

Setelah itu konfigurasi phpLDAPadmin di text editor seperti dibawah ini.

```
root@aaa:~# nano /etc/phpldapadmin/config.php
```

Setelah itu perlu menambahkan rincian konfigurasi yang disiapkan untuk server LDAP. Mencari parameter host dan pengaturan untuk nama domain server atau alamat IP address. Paramater ini untuk mengakses antarmuka web seperti berikut:

```
$servers->setValue('server','name','aaa');

/* Examples:
  'ldap.example.com',
  'ldaps://ldap.example.com/',
  'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
      (Unix socket at /usr/local/var/run/ldap) */
$servers->setValue('server','host','192.168.1.71');

/* The port your LDAP server listens on (no quotes). 389 is standard. */
// $servers->setValue('server','port',389);

/* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
  auto-detect it for you. */
$servers->setValue('server','base',array('dc=padi,dc=net,dc=id'));

/* Five options for auth_type:
  1. 'cookie': you will login via a web form, and a client-side cookie will
    store your login dn and password.
  2. 'session': same as cookie but your login dn and password are stored on the
    web server in a persistent session variable.
  3. 'http': same as session but your login dn and password are retrieved via
    HTTP authentication.
  4. 'config': specify your login dn and password here in this config file. No
  5. 'sasl': login will be taken from the webserver's kerberos authentication.
Currently only GSSAPI has been tested (using mod_auth_kerb).
```

Setelah itu di paramater bind_id perlu menyesuaikan bagian dc lagi, seperti yang dilakukan sebelumnya.

```
$servers->setValue('login','bind_id','cn=admin,dc=padi,dc=net,dc=id');
```

Setelah itu lakukan restart apache service dengan cara seperti berikut:

```
root@aaa:~# service apache2 restart
```

- Instalasi SSL Cwetificate

Mengamankan server LDAP dengan SSL dari pihak luar dengan sertifikat SSL.Langkah pertama create directory untuk hold our certificate dan key seperti berikut :

```
[root@aaa:~# mkdir /etc/apache2/ssl
```

Kemudian create key dan sertifikat seperti berikut:

```
root@aaa:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt
```

Setelah itu *create password authentication file* :

```
root@aaa:~# apt-get install apache2-utils
```

Kemudian *create file* dan *username/password* :

```
root@aaa:~# htpasswd -c /etc/apache2/htpasswd admin
New password:
Re-type new password:
Adding password for user admin
```

Langkah berikutnya *enable SSL module* di Apache :

```
Root@aaa:~# sudo a2enmod ssl
```

Kemudian edit konfigurasi apache phpLDAPadmin untuk url lokasi :

```
root@aaa:~# nano /etc/phpldapadmin/apache.conf
# Define /phpldapadmin alias, this is the default
<IfModule mod_alias.c>
   Alias /aaa /usr/share/phpldapadmin/htdocs
</IfModule>
```

Setelah itu konfigurasi HTTP Virtual Host :

```
root@aaa:~# nano /etc/apache2/sites-enabled/000-default.conf
ServerAdmin danang@padi.net.id
      DocumentRoot /var/www/html
      ServerName aaa.padi.net.id
Redirect permanent /aaa https://aaa.padi.net.id/aaa
```

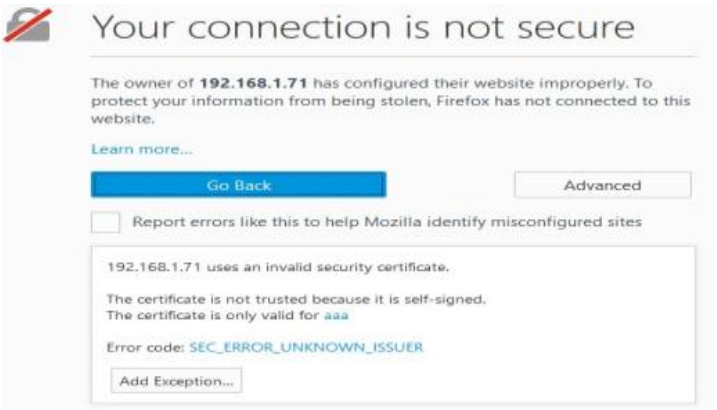
Setelah itu konfigurasi HTTPS virtual host file :

```
root@aaa:~# a2ensite default-ssl.conf
root@aaa:~# nano /etc/apache2/sites-enabled/default-ssl.conf
<VirtualHost _default_:443>
            ServerAdmin danang@padi.net.id
            ServerName aaa.padi.net.id
SSLCertificateFile      /etc/apache2/ssl/apache.crt
```

```
SSLCertificateKeyFile /etc/apache2/ssl/apache.key

<Location /aaa>
    AuthType Basic
    AuthName "Restricted Files"
    AuthUserFile /etc/apache2/htpasswd
    Require valid-user
```

Berikut tampilan web interface phpLDAPadmin dengan *warning SSL certificate* seperti Gambar 4.1



Gambar 4. Interface phpLDAPadmin

1. Instalasi FreeRadius

Server RADIUS merupakan server AAA yang bertugas untuk menangani proses otentikasi, otorisasi dan accounting. Server RADIUS dengan menggunakan aplikasi FreeRADIUS.

- Instalasi FreeRadius dengan OpenLDAP
  Tahapan instalasi FreeRADIUS dengan OpenLDAP

```
# apt-get update
# apt-get install freeradius
# cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema/
# sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \ cn=schema,cn=config dn
# nano schema.conf
# include /etc/ldap/schema/openldap.schema
# mkdir out
# slapcat -f schema.conf -F out -n0 -H ldap:///cn={0}openldap,cn=schema,cn=config -l cn=openldap.ldif
# nano /etc/ldap/schema/openldap.ldif
dn: cn=openldap,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: openldap
# sudo ldapadd -Q -Y EXTERNAL -H ldapi:/// -f cn\=openldap.ldif
# sudo ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b cn=schema,cn=config dn
```

Setelah itu lakukan *Restart network service* dengan cara :

```
[root@aaa ~]# service slapd restart
[root@aaa~]# service freeradius restart
```

Kemudian koneksikan ldap ke FreeRADIUS dengan cara :

```
[root@aaa~]# nano /etc/freeradius/modules/ldap
        server = "localhost"
        identity = "cn=admin,dc=padi,dc=net,dc=id"
        password = adPN741.net
        basedn = "dc=padi,dc=net,dc=id"
        filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
        base_filter = "(objectclass=radiusprofile)"
[root@aaa~]# nano /etc/freeradius/site-enabled/default
         ldap
         Auth-Type LDAP {
         ldap
         }
[root@aaa~]# nano /etc/freeradius/site-enabled/inner-tunnel
```

Berikut pengetesan FreeRADIUS dengan backend OpenLDAP siap digunakan setelah menyatakan *access-accept.*

```
root@aaa:~# radtest danang danang localhost 18120 padinet
Sending Access-Request of id 36 to 127.0.0.1 port 1812
        User-Name = "danang"
        User-Password = "danang"
        NAS-IP-Address = 127.0.1.1
        NAS-Port = 18120
        Message-Authenticator = 0x00000000000000000000000000000000
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=36, length=20
```

2. Konfigurasi Perangkat

Pada perangkat cisco, switch, router dan mikrotik terdapat konfigurasi. Konfigurasi ini berfungsi untuk otorisasi dan otentikasi user ke freeradius dengan backend openldap, untuk konfigurasi seperti berikut :

- Mikrotik Configuration

  Untuk konfigurasi mikrotik dengan cara *network configuration* seperti:

```
[danang@padinet-wifi] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   192.168.1.51/24    192.168.1.0     ether1
[danang@padinet-wifi] /radius> export
# jun/22/2016 21:09:09 by RouterOS 6.27
# software id = AX4D-N8DT
#
/radius
add address=192.168.1.71 secret=padinet service=wireless
            add address=192.168.1.71 secret=padinet service=login
```

Terkahir pastikan pastikan ip address mikrotik bisa terhubung ke radius server :

```
[danang@padinet-wifi] > ping 192.168.1.71
SEQ HOST                                     SIZE TTL TIME  STATUS
0     192.168.1.71                             56  64 1ms
      1    192.168.1.71                            56
```

- Router Configuration

  Untuk konfigurasi cisco router dengan cara network configuration seperti:

```
Router#show running-config
Building configuration...

Current configuration : 1088 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password 7 044B0A02062F495A
!
aaa new-model
!
!
aaa authentication login default local group radius
aaa authorization exec default local group radius
aaa authorization network default group radius local
!
aaa session-id common
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
ip cef
!
!!
interface FastEthernet0/0
 ip address 192.168.1.115 255.255.255.0
 duplex auto
 speed auto
!
radius-server host 192.168.1.71 auth-port 1812 acct-port 1813 key 7
0216055F02080A35
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
end
```

- Web Server Configuration
  Untuk konfigurasi workstation admin dengan cara network configuration.

```
C:\Users\CISCO>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : 202.6.233.11
   Link-local IPv6 Address . . . . . : fe80::3939:385:d1e6:3117%3
   IPv4 Address. . . . . . . . . . . : 192.168.1.158
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.50
```

B. Pengujian

Pada tahap ini akan dilakukan pengujian seperti pada black box test table. Pengujian Proyek Akhir ini menggunakan phpmailer, telnet, dan email header check. Untuk tahapan pengujian antara lain.ac

1. Pengujian phpLDAPadmin

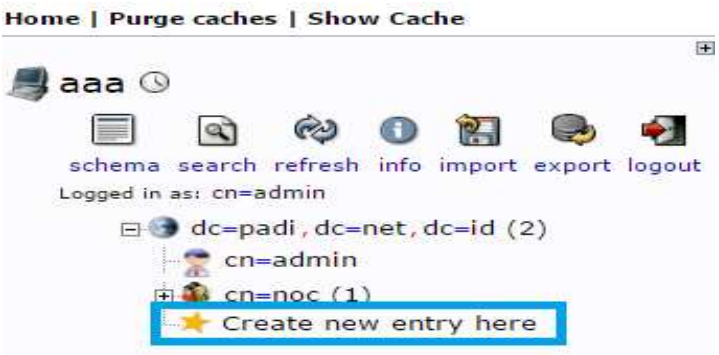
Pada bagian pengujian network connection akan dibagi ketiga tahapan, yaitu sebagai berikut :

- phpLDAPadmin

Untuk pengujian menggunakan phpLDAPadmin. Langkah awal yang harus dilakukan adalah admin login ke site phpLDAPadmin pada server, seperti Gambar 5.

Gambar 5. phpLDAPadmin login

Selanjutnya melakukan create objects yang dengan memilih menu create new entry here, seperti Gambar 6.



Gambar 6. phpLDAPadmin Menu

2. Pengujian create user pada phpLDAPadmin

Pengujian menambah user yang dilakukan adalah mendapatkan hak akses ke dalam perangkat cisco dan mikrotik.

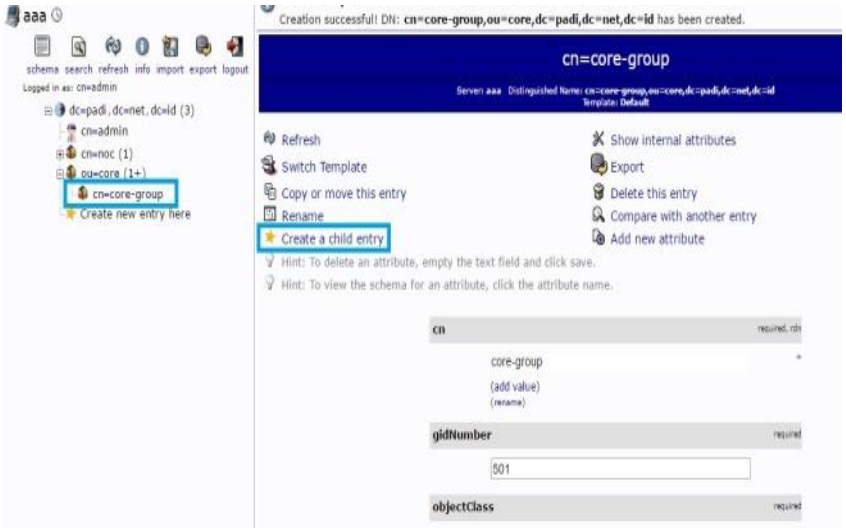
Pengujian yang dilakukan dengan menggunakan dua buah tools yaitu :

a. Telnet

b. Winbox

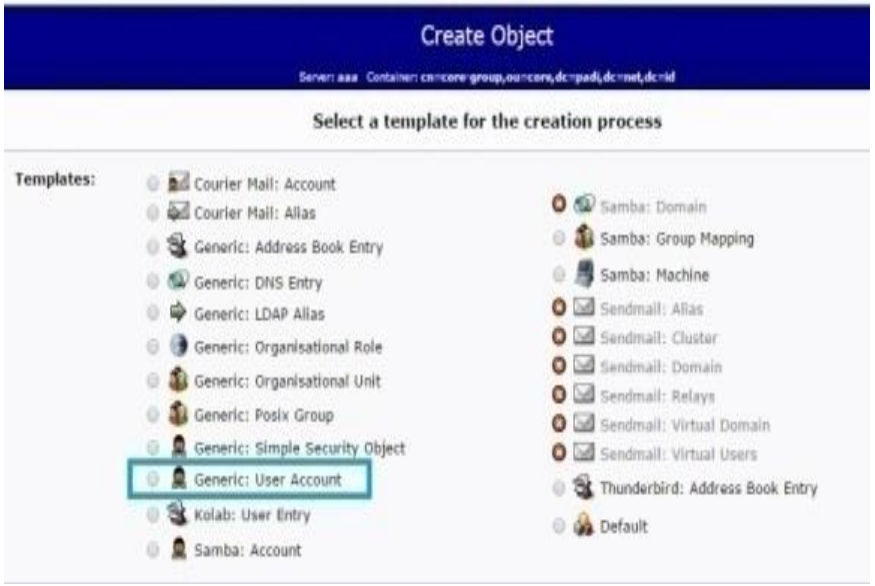
- Create User

Untuk pengujian menggunakan langkah awal yang harus dilakukan adalah pilih core-group dan create a child entry seperti dibawah ini, seperti Gambar 7.



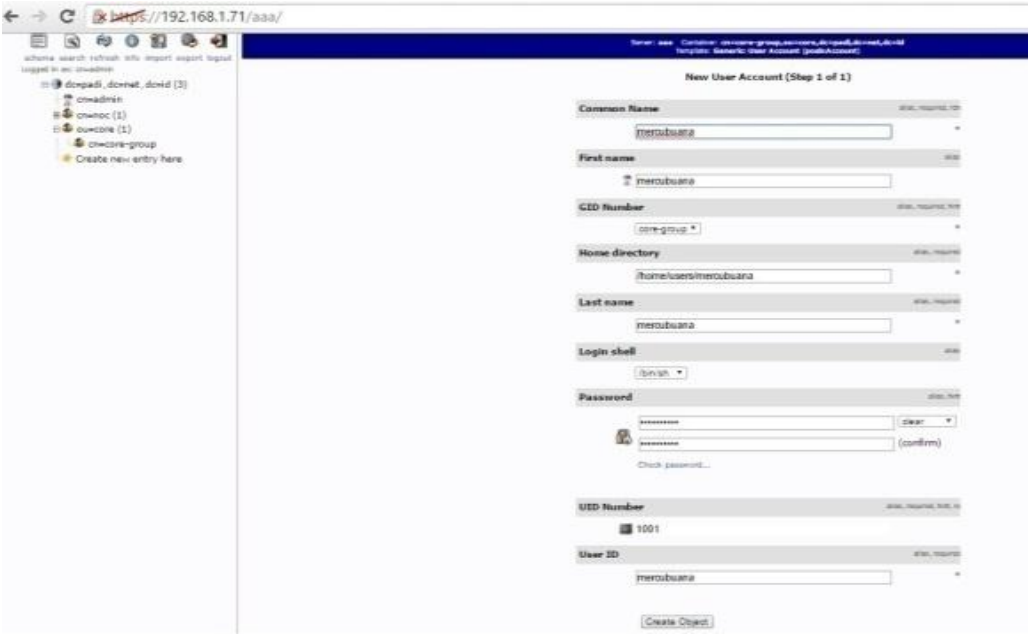
Gambar 7. phpLDAPadmin Menu

Dan selanjutnya dengan memilih menu menu generic user account, seperti Gambar 8.



Gambar 8. Templates create Objects

Jika sudah dipilih maka tampilan halaman akan beralih seperti dibawah ini. Dan perlu diinputkan User ID dan password beserta common name maupun first name. Jika sudah diisi klik tombol create object, seperti Gambar 9.



Gambar 9. New User Account

Tahapan selanjutnya dengan memilih tombol commit, seperti Gambar 10.

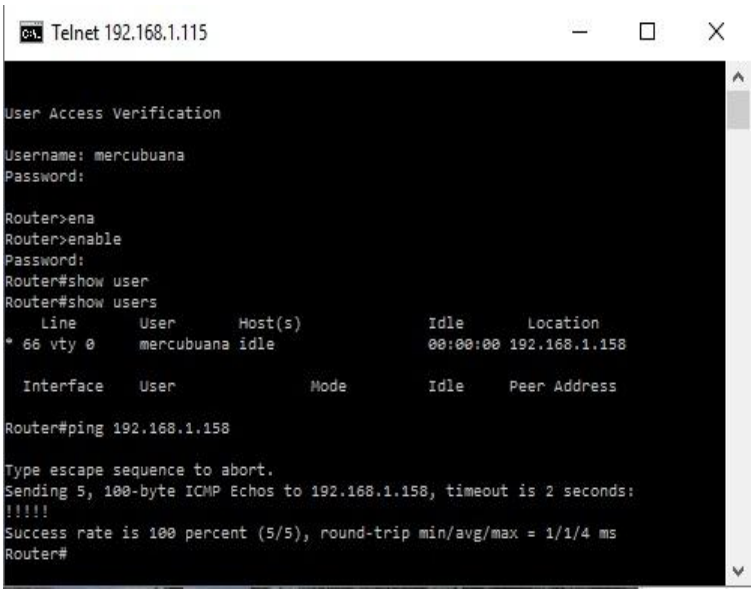
Gambar 10. Create LDAP Entry Commit

Dan terlihat username mercubuana yang sudah di create, seperti gambar Gambar 11.

Gambar 11. User Account phpLDAPadmin

- **Perangkat Cisco Router**

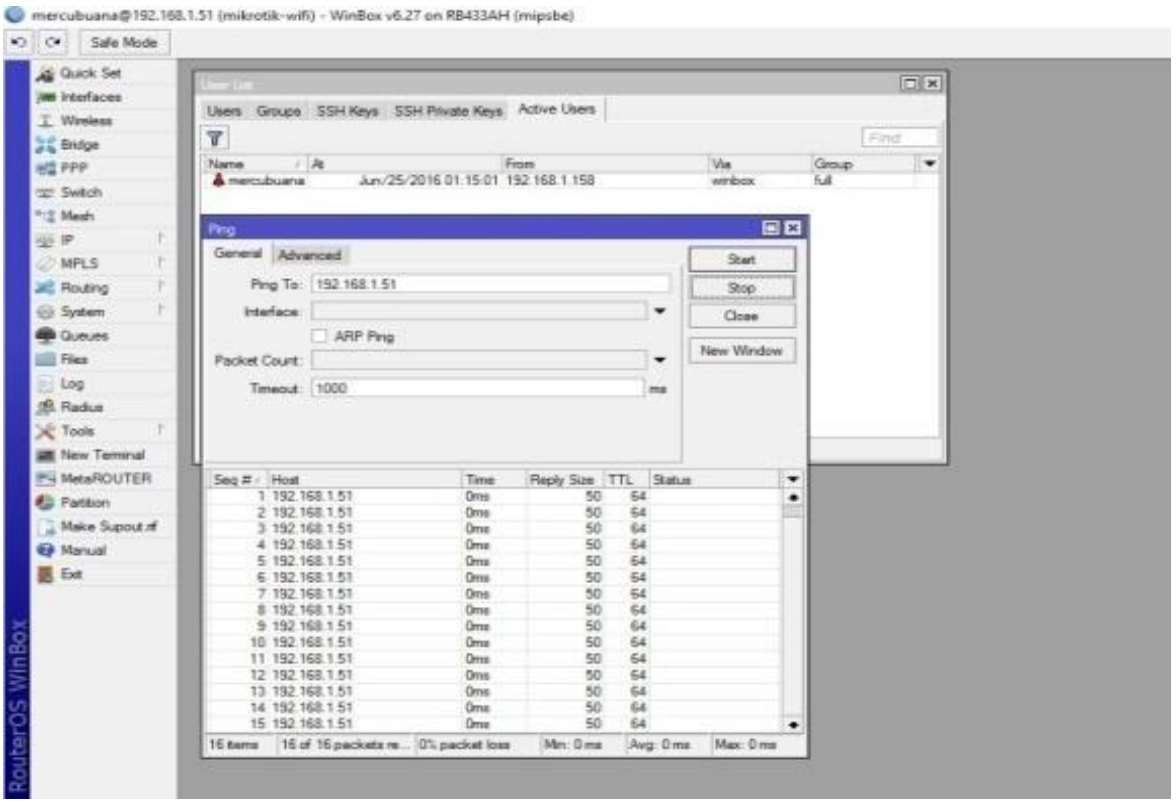
Pengujian yang dilakukan dengan melakukan telnet ke cisco router. Untuk mendapatkan hak akses ke router sehingga user account mercubuana dapat mengoperasi router. Berikut gambar login telnet ke router dengan menggunakan freeradius dengan backend ldap username mercubuana dan password mercubuana



Gambar 12. Pengujian Cisco Router

- Perangkat Mikrotik (Winbox)

Pengujian yang dilakukan dengan melakukan winbox ke mikrotik. Untuk mendapatkan hak akses ke mikrotik sehingga user account mercubuana dapat mengoperasi mikrotik. Berikut gambar login winbox ke mikrotik dengan menggunakan freeradius dengan backend ldap username mercubuana dan password mercubuana.



Gambar 13. Pengujian Login Winbox Mikrotik

TABLE 2.
BLACKBOX TESTING

No.	Skenario Pengujian	Hasilyang diharapkan	Checklist
FreeRADIUS LDAP			
1.	Create User phpLDAPadmin	phpLDAPadmin dapat menambah user untuk mendapatkan hak ases ke perangkat Cisco dan Mikrotik	Berhasil
2.	Change password user phpLDAPadmin	phpLDAPadmin dapat merubah password sehingga user menggunakan password terbaru	Berhasil
3.	Delete user phpLDAPadmin	phpLDAPadmin dapat menghapus user sehingga user tersebut tidak bisa menggunakan hak akses ke perangkat Cisco dan Mikrotik	Berhasil
4.	Proses Login	Jika user memasukan username dan password dengan benar secara otomatis user dapat mendapatkan hak akses ke perangkat Cisco dan Mikrotik	Berhasil
FreeRADIUS LDAP			
1.	Create User phpLDAPadmin	phpLDAPadmin dapat menambah user untuk terkoneksi ke jaringan melalui WiFi.	Berhasil
2.	Change password user phpLDAPadmin	phpLDAPadmin dapat merubah password sehingga user menggunakan password terbaru untuk terkoneksi ke jaringan melalu WiFi	Berhasil
3.	Delete user phpLDAPadmin	phpLDAPadmin dapat menghapus user sehingga user tersebut tidak bisa terkoneksi ke jaringan melalui WiFi	Berhasil
4.	Proses Login	Jika user memasukan username dan password dengan benar secara otomatis user dapat terkoneksi ke jaringan melalui WiFi	Berhasil

V. PENUTUP

Kesimpulan dari pengujian dan analisa dari penelitian ini adalah :

1. Implementasi freeradius berbasis ldap ini dapat mempermudah proses pendaftaran user untuk hak akses perangkat secara terpusat, sehingga tidak diperlukan lagi pendaftaran user di setiap perangkat.
2. Implementasi freeradius berbasis ldap ini dapat mempermudah proses pengupdatean user untuk hak akses perangkat secara terpusat, sehingga tidak diperlukan lagi pengupdatean user di setiap perangkat.
3. Implementasi freeradius berbasis ldap ini dapat mempermudah proses delete user untuk hak akses perangkat secara terpusat, sehingga tidak diperlukan lagi delete user di setiap perangkat

Saran untuk pengembangan lebih lanjut dari penelitian ini, antara lain :

1. Diharapkan untuk kedepannya dapat dikembangkan untuk menangani proses *privalage* hak akses, sehingga *user* mempunyai hak akses sesuai kewenangannya.
2. Diharapkan untuk kedepannya freeradius berbasis ldap dapat dipergunakan secara *live*.

DAFTAR PUSTAKA

[1] Danny. 2014. *Install OpenLDAP In Ubuntu*. Diambil dari: (http://www.unixmen.com/install-openldap-in-ubuntu-15-10-and-debian-8/, 27 Mei 2016).

[2] Hardana. 2013. *Setting Mikrotik Radius*. Yogyakarta : Andi Offset.

[3] Imam, Cartealy. 2013. *Linux Networking*. Jakarta: Jasakom.

[4] Justin. 2014. *How To Install and Configure OpenLDAP and phpLDAPadmin on an Ubuntu 14.04 Server*. Diambil dari: (https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-openldap-and-phpldapadmin-on-an-ubuntu-14-04-server, 27 Mei 2016).

[5] Prama, Jaka. 2015. CCNA. Diambil dari: (http://www.jakapramana.com/2015/03/download-ebook-belajar-materi-ccna.html, 27 Mei 2016).

[6] Rahul. 2013. *Setup FreeRadius Authentication with OpenLDAP*. Diambil dari: (http://tecadmin.net/freeradius-authentication-with-openldap/, 27 Mei 2016).

[7] Ryaz. 2012. *Freeradius with OpenLDAP authentication in Ubuntu 12.04 LTS*. Diambil dari: (https://ubuntuforums.org/showthread.php?t=1976883, 27 Mei 2016).

[8] Sofana, Iwan. 2012. *Cisco CCNA & Jaringan Komputer*. Bandung: Informatika

[9] Tldp. 2012. *Radius authentication using LDAP*. Diambil dari: (http://www.tldp.org/HOWTO/archived/LDAP-Implementation-HOWTO/radius.html, 17 Mei 2016).

[10] Wahana Komputer. 2014. *Konsep & implementasi jaringan dengan linux ubuntu*. Yogyakarta : Andi Offset.