

Dokumentasi Pembuatan Edurom



Kelompok :

Muhammad Fachrizal Lisnawan (14523039)

Sumarjianto (14523123)(ketua)

Teknik Informatika

Universitas Islam Indonesia

I. Skenario Edurom

Eduroam (education roaming) adalah layanan roaming internasional untuk pengguna dalam penelitian, pendidikan tinggi, dan pendidikan lanjut. Hal ini memberi peneliti, dosen dan siswa akses jaringan yang mudah dan aman saat mengunjungi institusi lain. Otentikasi dilakukan oleh institusi asal mereka, menggunakan kredensial yang sama seperti saat mereka mengakses jaringan secara lokal, sementara otorisasi untuk mengakses internet dan kemungkinan sumber daya lainnya ditangani oleh institusi yang dikunjungi. Dan hal lainnya adalah pengguna tidak harus membayar untuk menggunakan eduroam.

Eduroam yang akan kita buat menggunakan nama universitas “unpar” dan “unlam”. Sebagai mahasiswa UNPAR dan UNLAM, kita harus bisa mengakses jaringan institusi kita sendiri dan institusi lain yang bertujuan agar mempermudah kita dalam belajar secara roaming. Untuk membuat eduroam sendiri, kita membutuhkan :

1. Software Backend FreeRadius yang digunakan sebagai server .
2. OpenLDAP yang digunakan sebagai identitas server.
3. Dua buah server yang digunakan sebagai backend Universitas UNPAR dan UNLAM.
4. Memastikan FreeRadius bekerja dengan REALM.
5. Eduroam menggunakan EAP (Extensible Authentication Protocol).

II. Dokumentasi Proses Setup

- Langkah pertama adalah mengupdate linux kita, agar installer yang kita butuhkan bisa terdeteksi.

```
root@upr-VirtualBox:/home/upr# apt-get update
```

- Kita akan menginstall freeradius dengan versi 3.0.

```
root@upr-VirtualBox:/home/upr# add-apt-repository ppa:freeradius/stable-3.0
```

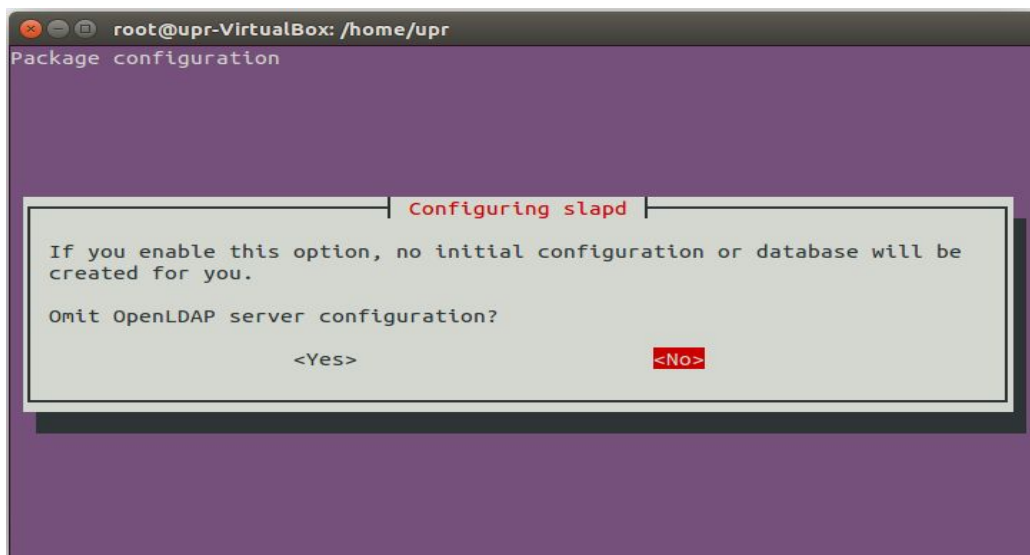
- Kita juga perlu menginstal openLDAP untuk membuat server.

```
root@upr-VirtualBox:/home/upr# apt-get install slapd ldap-utils
```

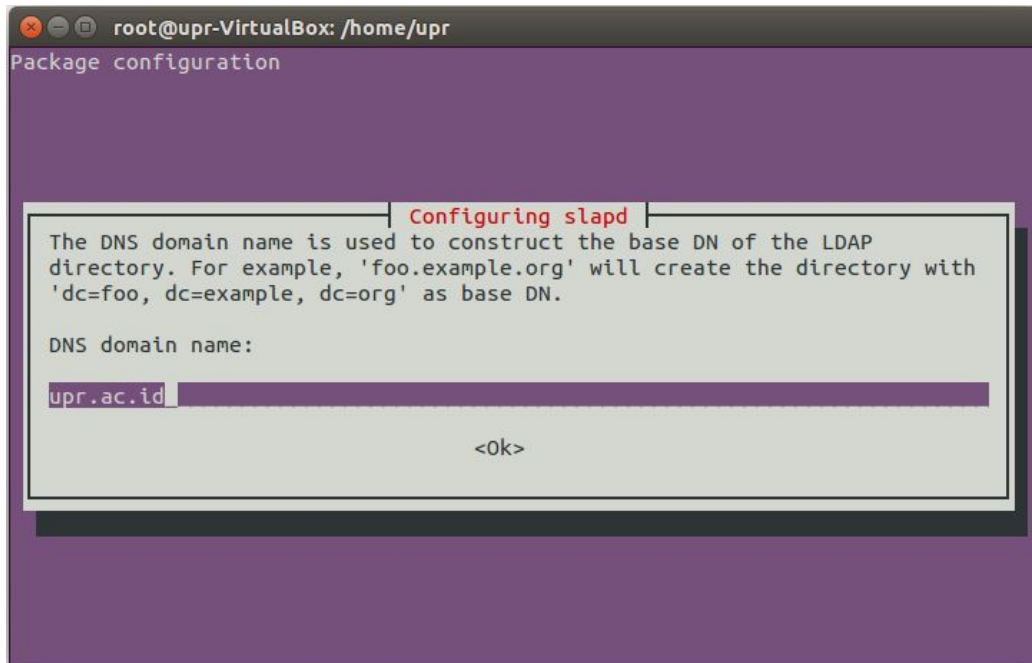
- Setelah mendownload openLDAP tadi, kita akan melakukan penginstallan dengan menggunakan dpkg.

```
root@upr-VirtualBox:/home/upr# dpkg-reconfigure slapd
```

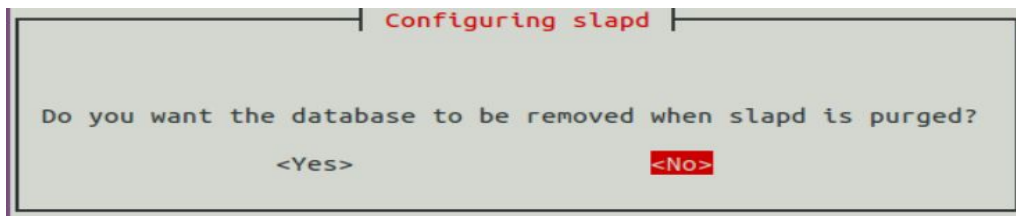
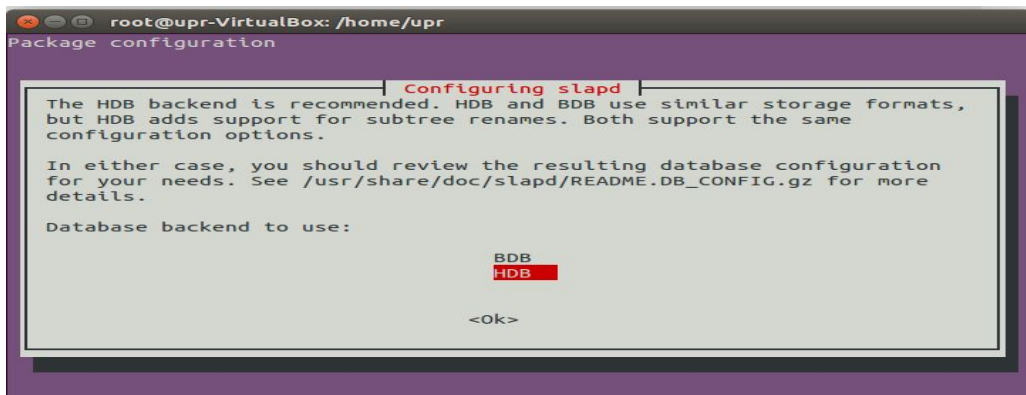
- Disini kita akan melakukan konfigurasi terhadap openLDAP yang akan kita install.



- Kita akan mengkonfigurasi DNS domain name, nama organisasi, dan password administrator yang akan digunakan untuk mengontrol server tersebut.



- Kita juga perlu mengkonfigurasi database backend.



```
Configuring slapd

There are still files in /var/lib/ldap which will probably break the
configuration process. If you enable this option, the maintainer scripts
will move the old database files out of the way before creating a new
database.

Move old database?

<Yes> <No>
```

```
Configuring slapd

The obsolete LDAPv2 protocol is disabled by default in slapd. Programs
and users should upgrade to LDAPv3. If you have old programs which
can't use LDAPv3, you should select this option and 'allow bind_v2' will
be added to your slapd.conf file.

Allow LDAPv2 protocol?

<Yes> <No>
```

- Setelah mengkonfigurasi server tadi, kita harus menginstall phpldapadmin yang digunakan untuk mengkonfigurasi isi dari server.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# apt-get install phpldapadmin
```

- Pertama kita perlu melakukan konfigurasi terhadap alamat server seperti di bawah supaya phpldap admin bisa terhubung dengan openldap .

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# nano /etc/phpldapadmin/config.php

/*$servers->setValue('server','host','127.0.0.1');*/
$servers->setValue('server','host','192.168.1.3');

/*$servers->setValue('server','base',array('dc=example,dc=com'));*/
$servers->setValue('server','base',array('dc=upr,dc=ac,dc=id'));

binds. */
/*$servers->setValue('login','bind_id','cn=admin,dc=example,dc=com');*/
$servers->setValue('login','bind_id','cn=admin,dc=upr,dc=ac,dc=id');

/* Hide the warnings for invalid objectClasses/attributes in templates. */
// $config->custom->appearance['hide_template_warning'] = false;
$config->custom->appearance['hide_template_warning'] = true;
```

- Setelah selesai mengkonfigurasi alamat server, kita harus menginstall apache juga, dan membuat folder dengan nama ssl.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# apt-get install apache2-utils
```

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# mkdir /etc/apache2/ssl
```

- Melakukan sertifikasi.

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

- Setelah itu kita harus memberikan detail sertifikasi server

```
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:yogyakarta
Locality Name (eg, city) []:sleman
Organization Name (eg, company) [Internet Widgits Pty Ltd]:apr
Organizational Unit Name (eg, section) []:apr
Common Name (e.g. server FQDN or YOUR name) []:apr
```

- Kita perlu mengaktifkan modul write yang ada di apache server.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# a2enmod ssl
```

- Kita diharuskan merubah 000-default pada apache server, agar server yang dijalankan sesuai dengan apa yang kita inginkan.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# nano /etc/apache2/sites-enabled/000-default.conf
```

```
#ServerAdmin webmaster@localhost
ServerAdmin webmaster@apr.ac.id
ServerName 192.168.1.3
Redirect permanent /phpldapadmin https://192.168.1.3/phpldapadmin
DocumentRoot /var/www/html
```

- a2ensite digunakan untuk mengaktifkan konfigurasi virtual host yang ada di direktori apache server.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox: /home/upr# a2ensite default-ssl.conf
```

- Kita perlu menambahkan atau merubah isi dari default-ssl.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox: /home/upr# nano /etc/apache2/sites-enabled/default-ssl.conf
```

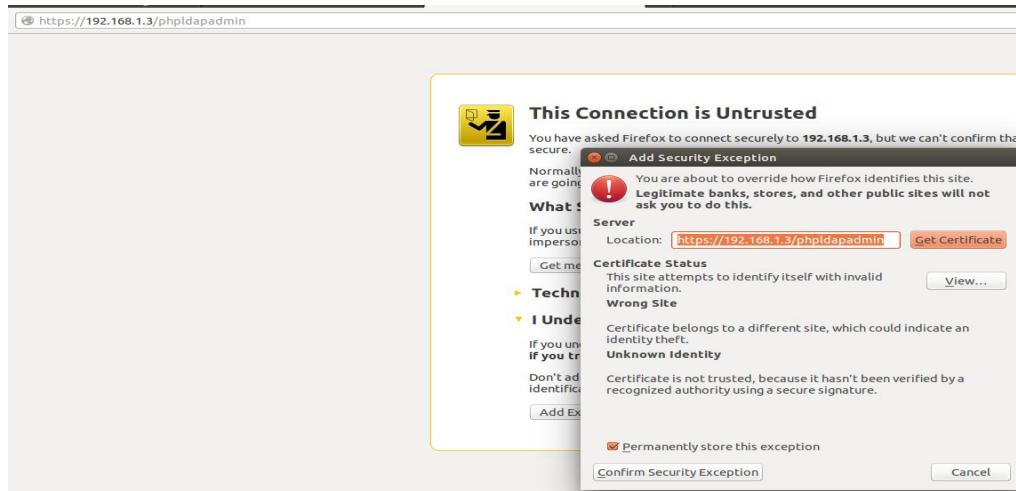
```
<IfModule mod_ssl.c>
  <VirtualHost _default_:443>
    ServerAdmin webmaster@192.168.1.3
    ServerName 192.168.1.3
```

```
# SSLCertificateFile directive is needed.
#SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
SSLCertificateFile /etc/apache2/ssl/apache.crt
SSLCertificateKeyFile /etc/apache2/ssl/apache.key
```

- Setelah selesai, kita perlu merestart service dari apache server.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox: /home/upr# service apache2 restart
```

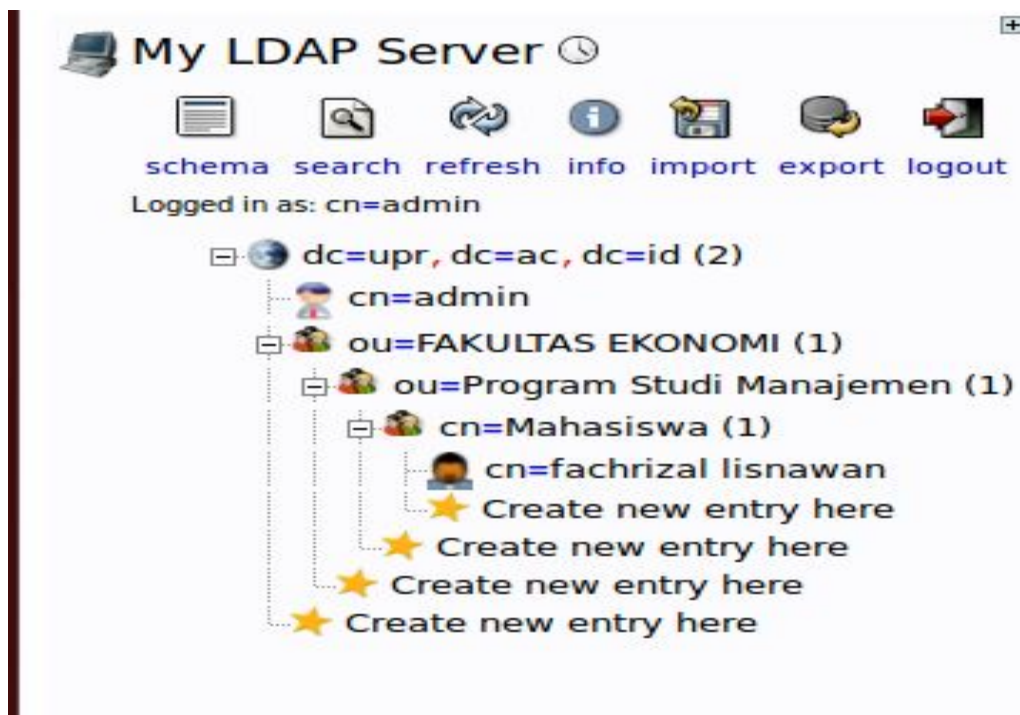
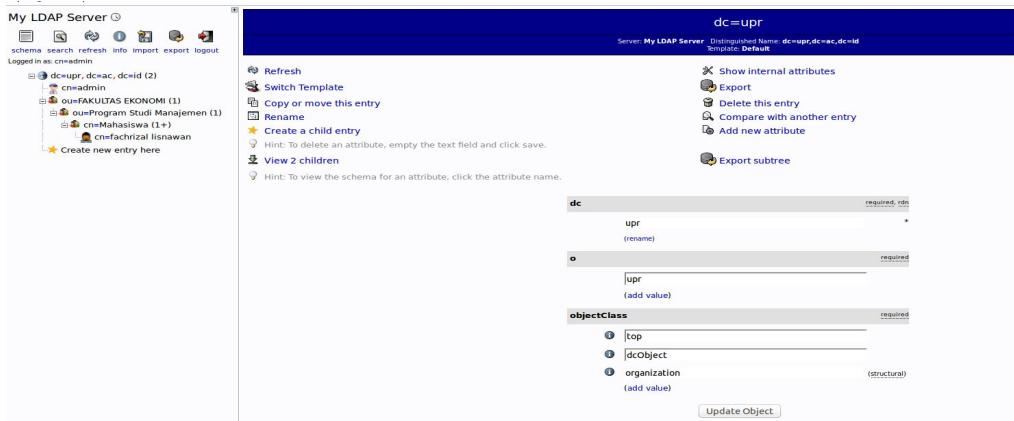
- Lakukan login ke phpldap , maka akan ada peringatan dimana, untuk memasukkan sertifikat di browser



- Login terlebih dahulu.

A screenshot of a web-based login form titled 'Authenticate to server My LDAP Server'. The form is contained within a light gray box. It has two main input fields: 'Login DN:' with the value 'cn=admin,dc=upr,dc=ac,dc=id' and 'Password:' which is masked with seven dots. Below these fields is an 'Anonymous' checkbox which is currently unchecked. At the bottom right of the form is a button labeled 'Authenticate'.

- Kita akan membuat isi struktur dari server ldap seperti dibawah ini.



- Sekarang waktunya menginstall FreeRadius LDAP, pastikan menggunakan versi 3.

```
root@upr-VirtualBox: /home/upr
root@upr-VirtualBox:/home/upr# apt-get install freeradius freeradius-ldap
```

- Kita akan mengkonfigurasi FreeRadius ldap, supaya terhubung dengan ldap ,seperti dibawah ini.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano mods-available/ldap
```

```
# - ldapc:// (Connect to LDAP)
server = '192.168.1.3'
#
# server = 'ldap.rrdns.example.org'
#
# server = 'ldap.rrdns.example.org'

# Port to connect on, defaults to 389, will
port = 389
```

```
# If using SASL + KRB5 these should be commented out.
identity = 'cn=admin,dc=upr,dc=ac,dc=id'
password = tkjku2018

# Unless overridden in another section, the dn from which all
# searches will start from.
base_dn = 'dc=upr,dc=ac,dc=id'
```

- Lakukan link pada konfigurasi ldap, ke folder mods-enable.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# ln -s ../mods-available/ldap mods-enabled/ldap
```

- Kita perlu mengkonfigurasi proxy.conf untuk menghubungkan server sebelah seperti dibawah ini.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano proxy.conf
```

```

proxy server {
    default_fallback = no
}

home_server FLR1 {
    type = auth+acct
    ipaddr = 192.168.1.2
    port = 1812
    secret = tkjku2018
    status_check = status-server
}

#home_server FLR2 {
#    type = auth+acct
#    ipaddr = 192.168.1.3
#    port = 1812
#    secret = tkjku2019
#    status_check = status-server
#}

```

```

realm "~.+$" {
    pool = EDUROAM
    nostrip
}

realm upr.ac.id {
    nostrip
}

```

- Dan jangan lupa untuk mengkonfigurasi clients.conf , tambahkan ip dan secret, untuk bisa melakukan eapol test

```

root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano clients.conf

```

```

client FLR1 {
    ipaddr          = 192.168.1.2
    secret          = tkjku2019
    shortname       = FLR1
    nas_type        = other
    Operator-Name   = 1unlam.ac.id
    add_cui         = yes
    virtual_server  = eduroam
}

client FLR2 {
    ipaddr          = 192.168.1.3
    secret          = tkjku2018
    # shortname     = FLR2
    # nas_type      = other
    # Operator-Name = 1upr.ac.id
    # add_cui       = yes
    # virtual_server = eduroam
}

```

- Setelah itu setting authorize juga perlu dilakukan misal menggunakan “files” pada eduroam-inner tunnel.

```

root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano mods-config/files/authorize

#laneuser      Auth-Type := Reject
#              Reply-Message = "Your account has been disabled."
testuser@upr.ac.id Cleartext-Password := "tkjku2019"

```

- Konfigurasi terhadap eap, supaya saat login diperlukan autentikasi.

```

root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano mods-available/eap

```

```
GNU nano 2.2.6 File: mods-available/eap
eap {
    default_eap_type = peap
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no

    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_password = whatever
        private_key_file = ${certdir}/server.key
        certificate_file = ${certdir}/server.pem
        ca_file = ${cadir}/ca.pem
        dh_file = ${certdir}/dh
        random_file = /dev/urandom
        fragment_size = 1024
        include_length = yes
        check_crl = no
        cipher_list = "DEFAULT"
    }

    ttls {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "eduroam-inner-tunnel"
    }

    peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = yes
        virtual_server = "eduroam-inner-tunnel"
    }

    mschapv2 {
    }
}
}
```

- pre-proxy juga perlu dilakukan perubahan.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox: /etc/freeradius# nano mods-config/attr_filter/pre-proxy
```

```
root@upr-VirtualBox: /etc/freeradius
GNU nano 2.2.6 File: mods-config/attr_filter/pre-proxy
DEFAULT
User-Name =* ANY,
EAP-Message =* ANY,
Message-Authenticator =* ANY,
NAS-IP-Address =* ANY,
NAS-Identifier =* ANY,
State =* ANY,
Proxy-State =* ANY,
Calling-Station-Id =* ANY,
Called-Station-Id =* ANY,
Operator-Name =* ANY,
Class =* ANY,
Chargeable-User-Identity =* ANY
```

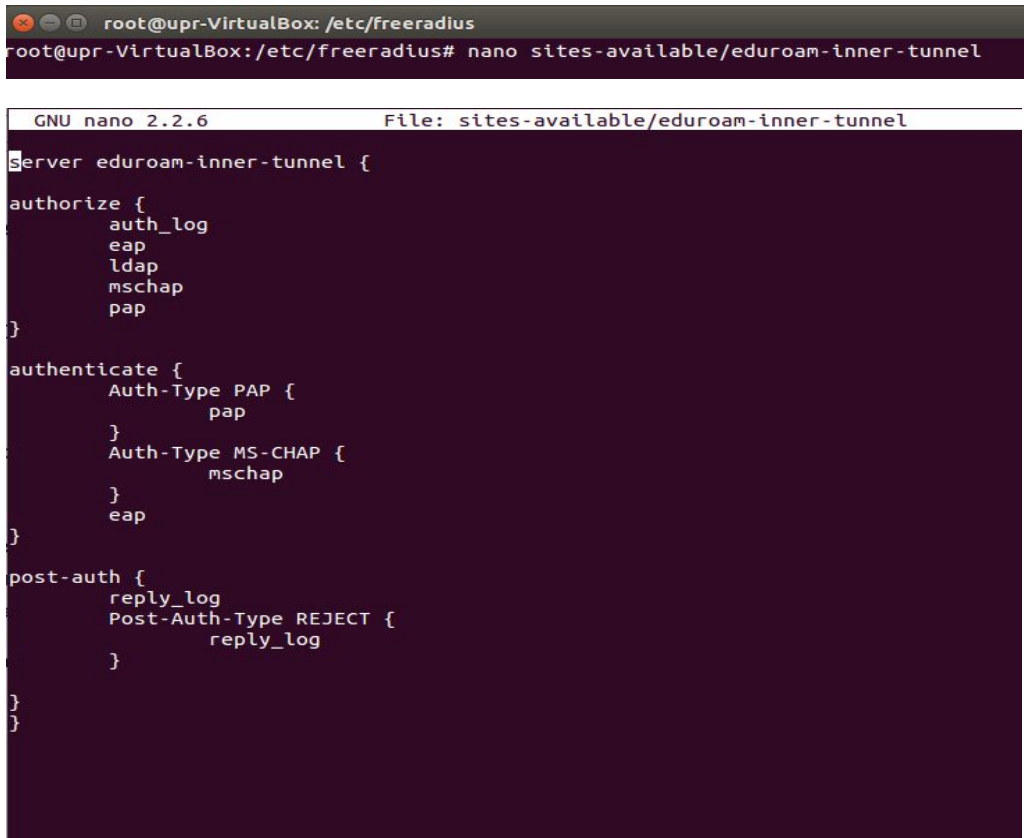
- Melakukan konfigurasi terhadap eduroam, dengan operator name upr.ac.id.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano sites-available/eduroam
GNU nano 2.2.6 File: sites-available/eduroam
server eduroam {
    authorize {
        # only use filter_username from version > 3.0.7 on
        filter_username
        if ("%{client:shortname}" != "FLR1") {
            update request {
                Operator-Name := "1upr.ac.id"
                # the literal number "1" above is an important prefix! Do not change it!
            }
        }
        # if you want detailed logging
        auth_log
        suffix
        ldap
        eap
    }
    authenticate {
        eap
    }
    preacct {
        suffix
    }
    accounting {
    }
    post-auth {
        # if you want detailed logging
        reply_log
        Post-Auth-Type REJECT {
            reply_log
        }
    }
}
```

```
pre-proxy {
    # if you want detailed logging
    pre_proxy_log
    if("%{Packet-Type}" != "Accounting-Request") {
        attr_filter.pre-proxy
    }
}

post-proxy {
    # if you want detailed logging
    post_proxy_log
    attr_filter.post-proxy
}
}
```

- Lakukan editing pada eduroam-inner-tunnel , masukkan ldap pada authorize



```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# nano sites-available/eduroam-inner-tunnel

GNU nano 2.2.6 File: sites-available/eduroam-inner-tunnel
Server eduroam-inner-tunnel {
authorize {
    auth_log
    eap
    ldap
    mschap
    pap
}

authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type MS-CHAP {
        mschap
    }
    eap
}

post-auth {
    reply_log
    Post-Auth-Type REJECT {
        reply_log
    }
}
}
```

- Lakukan link terhadap file eduroam ke folder sites-enable.

```
root@upr-VirtualBox: /etc/freeradius
root@upr-VirtualBox:/etc/freeradius# ln -s ../sites-available/eduroam sites-enabled/eduroam
```

- Lakukan link terhadap file eduroam-inner-tunnel ke folder sites-enable.

```
root@upr-VirtualBox:/etc/freeradius# ln -s ../sites-available/eduroam-inner-tunnel sites-enabled/eduroam-i
nner-tunnel
```

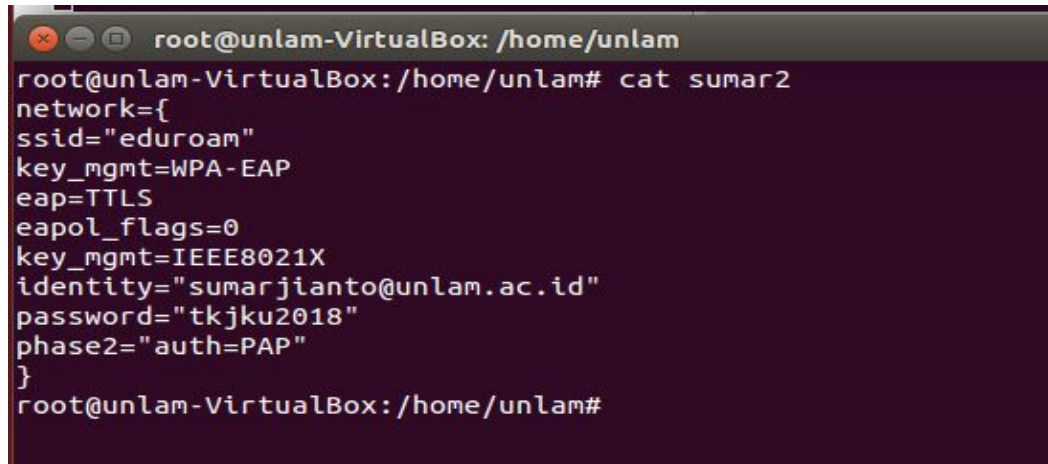
- Lakukan perintah debugging dengan menjalankan perintah ini pada 2 server yang telah disetting, jika terjadi error port telah digunakan lakukan perintah service freeradius restart setelah itu freeradius stop , baru lakukan lagi free radius -X .

```
root@unlam-VirtualBox:/home/unlam# freeradius -X
```

- Konfigurasi hampir sama dengan server unlam dan upr, hanya yang membedakan pada file client, eduroam , dan proxy saja untuk freeradius.
- Hasil perintah debugging dengan server unlam , lakukan juga pada server upr.

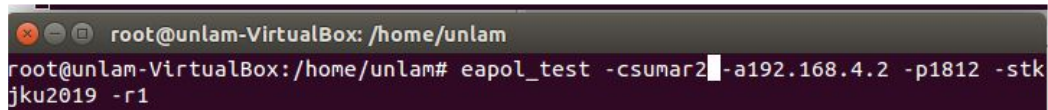
```
root@unlam-VirtualBox: /home/unlam
max_connections = 16
lifetime = 0
idle_timeout = 30
}
}
listen {
  type = "auth"
  ipaddr = 127.0.0.1
  port = 18120
}
Listening on auth address * port 1812 bound to server default
Listening on acct address * port 1813 bound to server default
Listening on auth address :: port 1812 bound to server default
Listening on acct address :: port 1813 bound to server default
Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel
Listening on proxy address * port 38452
Listening on proxy address :: port 44430
Ready to process requests
```


- Buat file untuk melakukan testing seperti ini , testing ini masih pada server unlam



```
root@unlam-VirtualBox: /home/unlam
root@unlam-VirtualBox:/home/unlam# cat sumar2
network={
ssid="eduroam"
key_mgmt=WPA-EAP
eap=TTLS
eapol_flags=0
key_mgmt=IEEE8021X
identity="sumarjianto@unlam.ac.id"
password="tkjku2018"
phase2="auth=PAP"
}
root@unlam-VirtualBox:/home/unlam#
```

- Lakukan perintah untuk mentest freeradius berhasil meotentikasi user dan password pada unlam



```
root@unlam-VirtualBox: /home/unlam
root@unlam-VirtualBox:/home/unlam# eapol_test -csumar2 -a192.168.4.2 -p1812 -stkjku2019 -r1
```

- Berhasil melakukan testing login pada server unlam sendiri .

```
root@unlam-VirtualBox: /home/unlam
(13) Finished request
Waking up in 4.8 seconds.
(0) Cleaning up request packet ID 0 with timestamp +79
(1) Cleaning up request packet ID 1 with timestamp +79
(2) Cleaning up request packet ID 2 with timestamp +79
(3) Cleaning up request packet ID 3 with timestamp +79
(4) Cleaning up request packet ID 4 with timestamp +79
(5) Cleaning up request packet ID 5 with timestamp +79
(6) Cleaning up request packet ID 6 with timestamp +79
Waking up in 0.1 seconds.
(7) Cleaning up request packet ID 7 with timestamp +79
(8) Cleaning up request packet ID 8 with timestamp +79
(9) Cleaning up request packet ID 9 with timestamp +79
(10) Cleaning up request packet ID 10 with timestamp +79
(11) Cleaning up request packet ID 11 with timestamp +79
(12) Cleaning up request packet ID 12 with timestamp +79
(13) Cleaning up request packet ID 13 with timestamp +79
Ready to process requests

root@unlam-VirtualBox: /home/unlam
3 5e 66 2e ab 97 06 fd 45 9c b3 34 71 7a 0d be f0 5d 62 cd
MS-MPPE-Recv-Key (crypt) - hexdump(len=32): a3 45 d2 3d fa f4 08 ca 1f 41
16 16 24 1b df fa 93 7a 86 74 01 2f 07 bf 29 00 d7 db 61 98
decapsulated EAP packet (code=3 id=6 len=4) from RADIUS server: EAP Success
EAPOL: Received EAP-Packet frame
EAPOL: SUPP_BE entering state REQUEST
EAPOL: getSuppRsp
EAP: EAP entering state RECEIVED
EAP: Received EAP-Success
EAP: EAP entering state SUCCESS
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state RECEIVE
EAPOL: SUPP_BE entering state SUCCESS
EAPOL: SUPP_BE entering state IDLE
eapol_sm_cb: success=1
EAPOL: Successfully fetched key (len=32)
PMK from EAPOL - hexdump(len=32): a3 45 d2 3d fa f4 08 ca 1f 41 36 a9 16 1
b df fa 93 7a 86 74 01 2f 07 bf 29 00 d7 db 61 98
EAP: deinitialize previously used EAP method (21, TTLS) at EAP deinit
ENGINE: engine deinit
MPPE keys OK: 2 mismatch: 0
SUCCESS
root@unlam-VirtualBox:/home/unlam#
```

- Buat file untuk melakukan testing login dari server unlam ke server upr.ac.id sebelah.

```

root@unlam-VirtualBox: /home/unlam
root@unlam-VirtualBox:/home/unlam# cat sumar
network={
ssid="eduroam"
key_mgmt=WPA-EAP
eap=TTLS
eapol_flags=0
key_mgmt=IEEE8021X
identity="fachrizal@upr.ac.id"
password="fachrizal"
phase2="auth=PAP"
}
root@unlam-VirtualBox:/home/unlam#

```

- Lakukan testing login ke server upr dari server unlam.

```

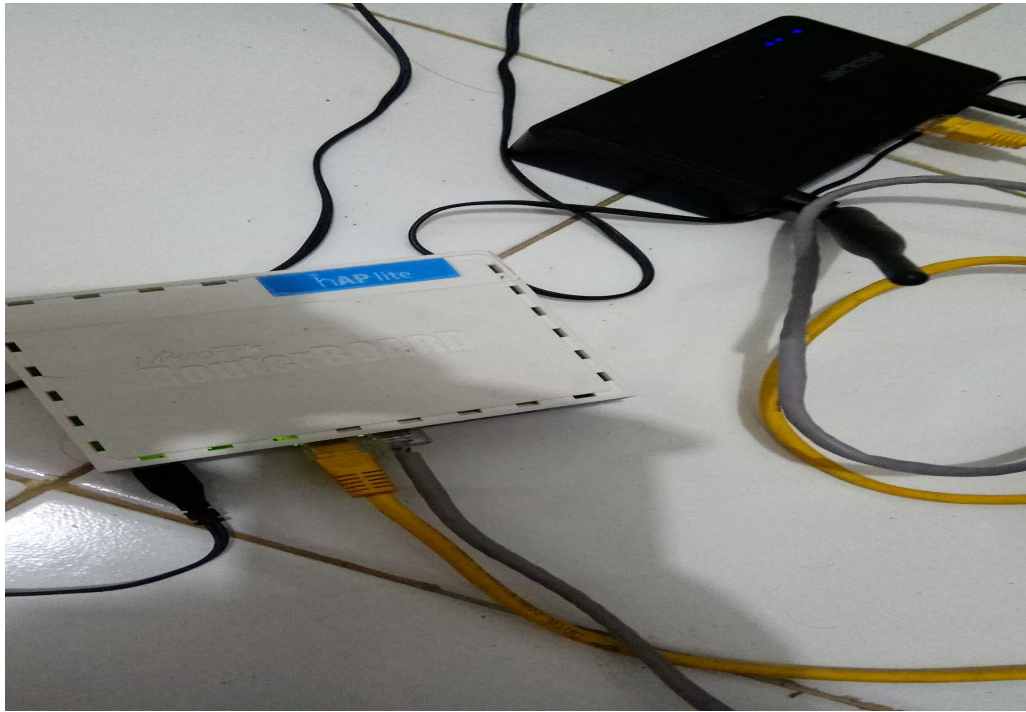
root@unlam-VirtualBox: /home/unlam
root@unlam-VirtualBox:/home/unlam# eapol_test -csumar -a192.168.4.2 -p1812 -stkj
ku2019 -r1

```

- Otentikasi berhasil dilakukan dari server unlam menuju server upr, catatan server kanan unlam dan kiri upr.

The image shows two terminal windows side-by-side. The left window is titled 'root@upr-VirtualBox: /home/upr' and displays a series of log messages from the freeradius server, including IP addresses, timestamps, and authentication status. The right window is titled 'root@unlam-VirtualBox: /home/unlam' and shows the output of the 'eapol_test' command, including hex dumps of EAP messages and the final 'SUCCESS' status. Below the terminals, a portion of a web form is visible, showing a 'User Name' field with the value 'fachrizal@upr.ac.id'.

- Test fisik dengan menggunakan router mikrotik RB 941-2nD hAP lite yang support radius, catatan prolink sebelah kanan untuk digunakan jalur internet dari indihome, menggunakan mode wifi repeater, dan di colok ke port 1 mikrotik, pada port port 2 mikrotik di gunakan untuk server eduroam dari virtual box dengan mode bridge.

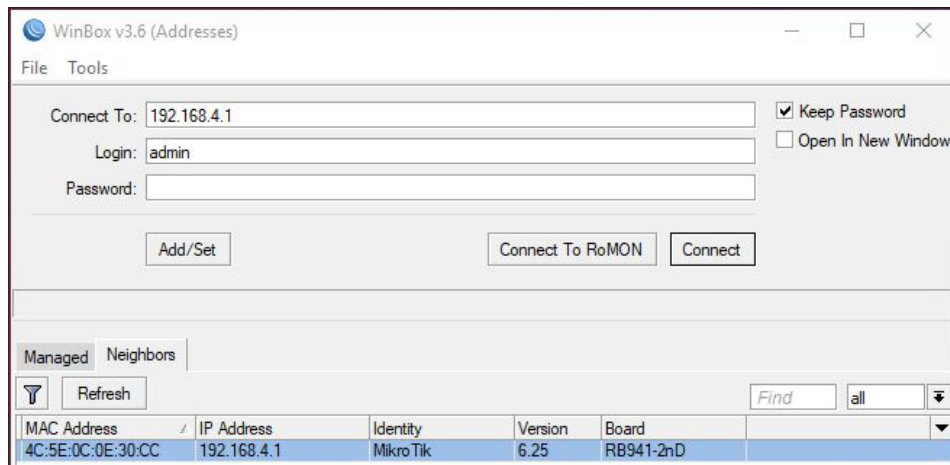


- Tambahkan ip router mikrotik di client.conf pada server unlam, supaya mikrotik bisa mengakses server unlam .

```
root@unlam-VirtualBox: /home/unlam
GNU nano 2.2.6 File: /etc/freeradius/clients.conf

client unlam {
    ipaddr      = 192.168.4.1
    secret      = tkjku2019
}
```

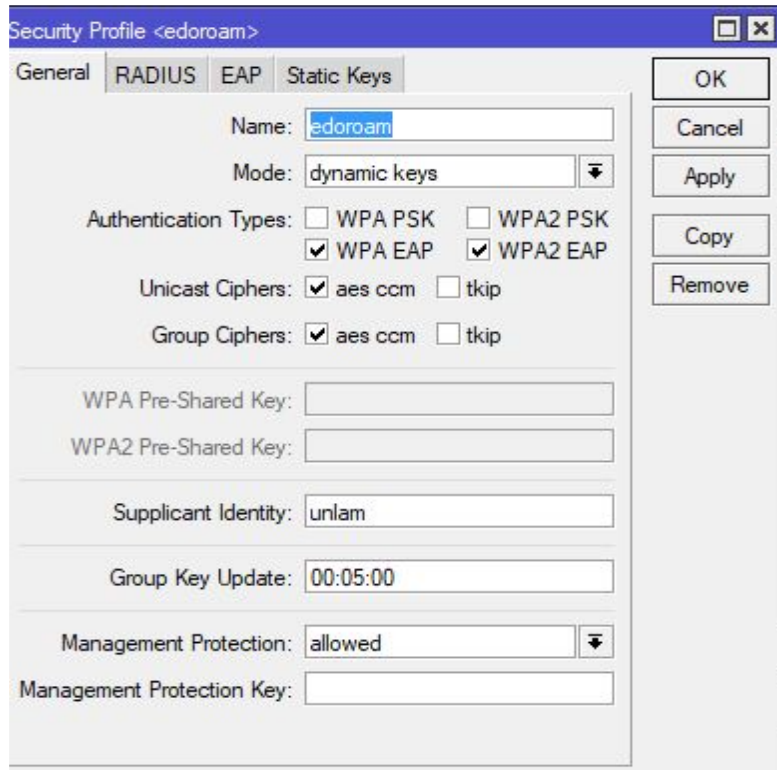
- Lakukan login menggunakan winbox untuk setting wifi mikrotik.



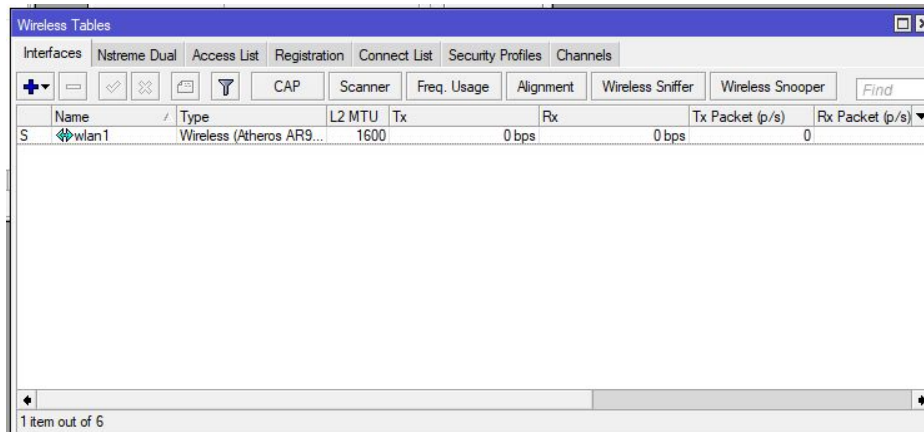
- Masuk ke menu Wirreless , dan masuk ke security profile.



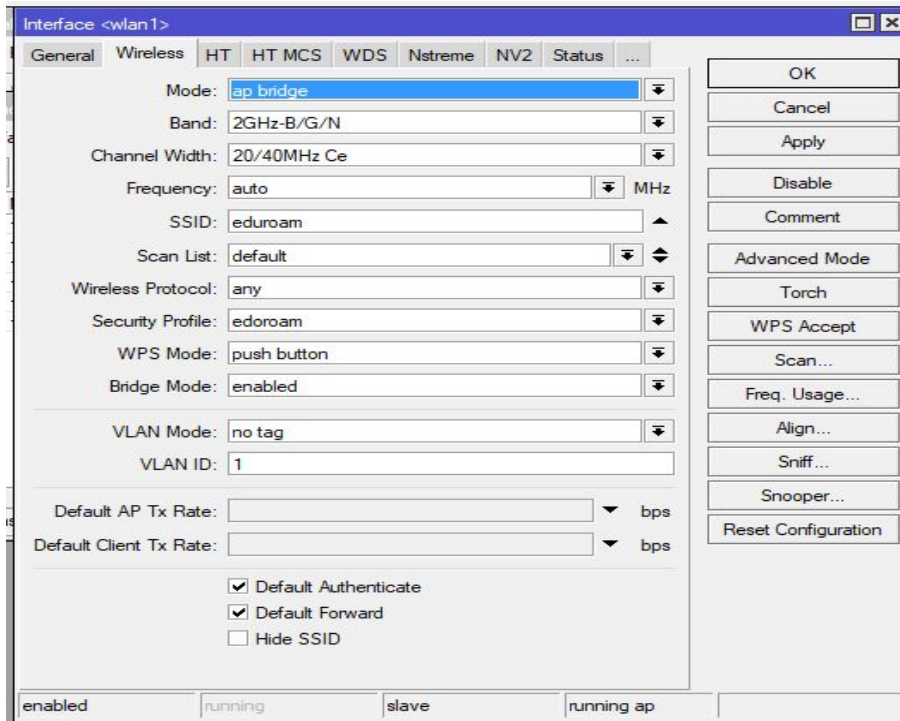
- Lakukan konfigurasi seperti ini.



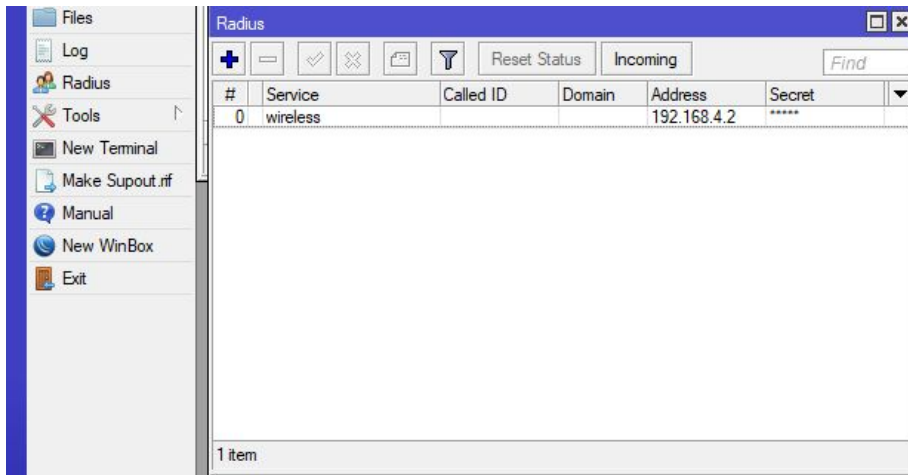
- Masuk ke table interface.



- Pilih security profile eduroam.



- Masuk ke radius dan tambahkan konfigurasi.



- Masukkan secret dan ip server free radius

Radius Server <192.168.4.2>

General Status

Service: ppp login
 hotspot wireless
 dhcp

Called ID:

Domain:

Address: 192.168.4.2

Secret: *****

Authentication Port: 1812

Accounting Port: 1813

Timeout: 3000 ms

Accounting Backup

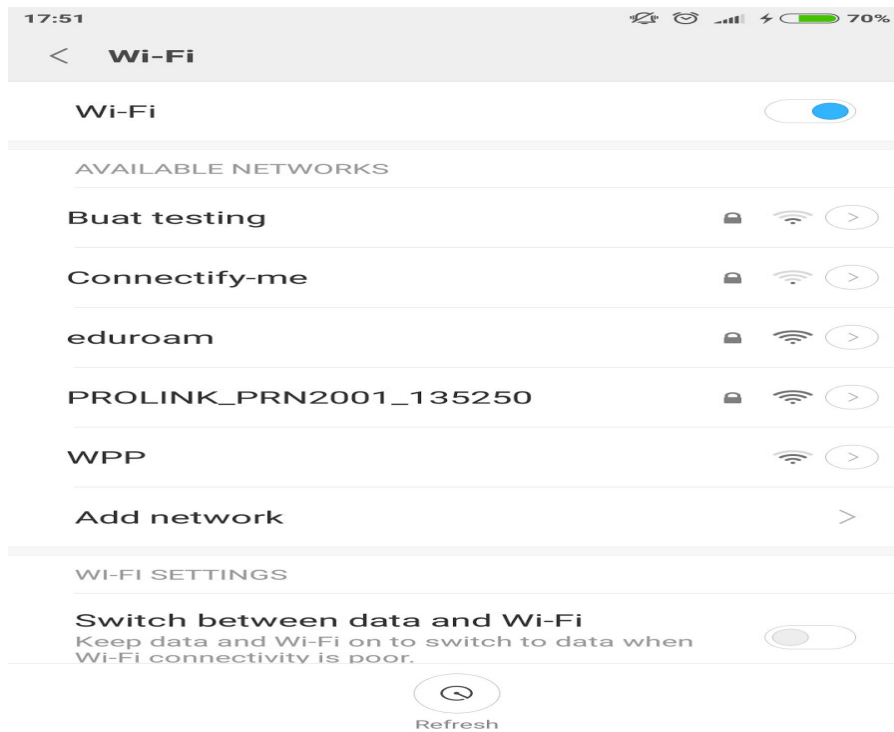
Realm:

Src. Address: 0.0.0.0

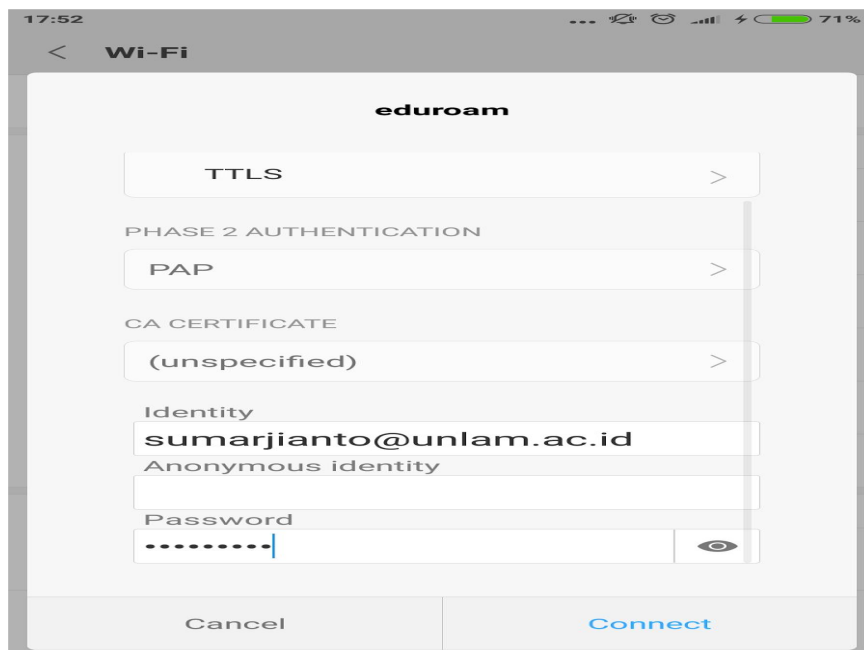
enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

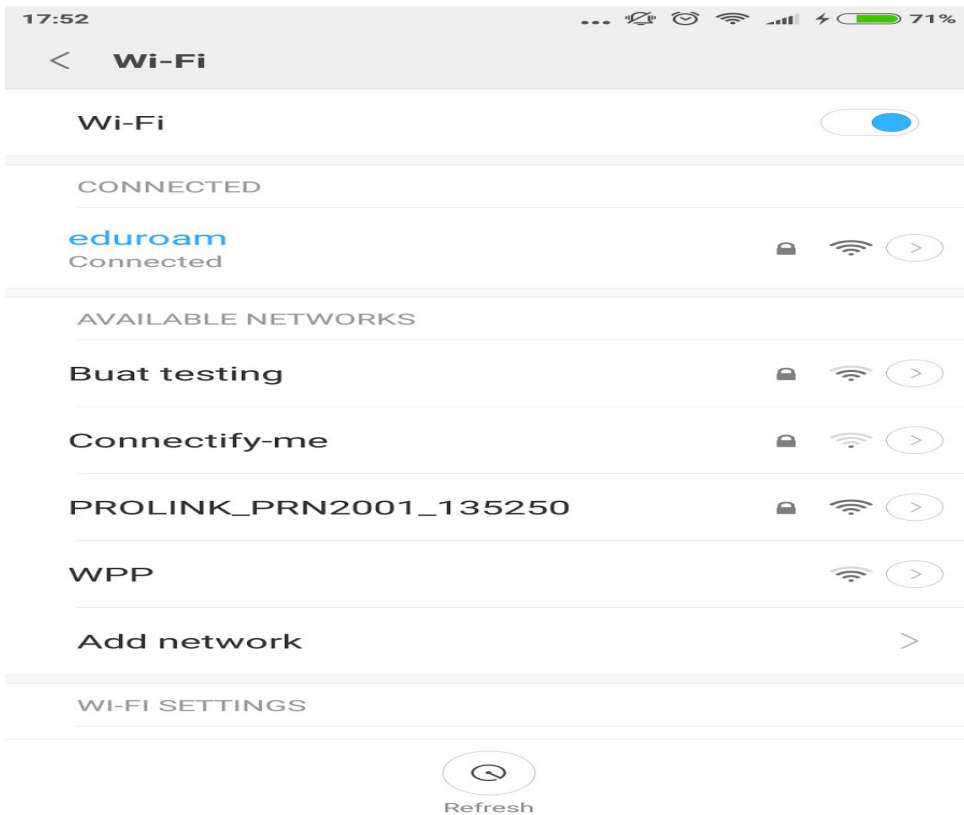
- Testing ini menggunakan smarthphone xiaomi redmi note 4, dan lakukan login wifi eduroam.



- masukkan autentikasi, password , dan identitas



- eduroam sudah bisa terhubung, dan bisa akses internet, untuk testing login ke server upr dari unlam kami tampilkan di video youtube



Sumber :

<https://www.digitalocean.com/community/tutorials/how-to-install-and-configure-openldap-and-phpldapadmin-on-an-ubuntu-14-04-server>

<https://wiki.geant.org/display/H2eduroam/freeradius-idp>

<https://wiki.geant.org/display/H2eduroam/freeradius-sp>

<https://hub.docker.com/r/spgreen/freeradius-eduroam/>

<https://ttboa.wordpress.com/2014/09/26/freeradius-on-debian-7/>

Video Youtube simulasi eduroam :

<https://www.youtube.com/watch?v=Wl9p50hCp9E>