Eduroam setup on Ubuntu

1. Server Requirements
   RAM at least 1 GB
   HDD at least 20 GB

2. Install Ubuntu

3. Run the following commands after installation of OS
   # apt-get update
   # apt-get upgrade

4. Sudo apt-get install openssl

Freeradius install

5. Install necessary aps
   # apt-get install freeradius freeradius-ldap freeradius-utils

   //freradius-ldap may not be necessary if active diractory already installed.

6. Test Radius
   Syntax: radtest [user] [password] localhost [port (default is 1812)] testing123
   ```
   # radtest first-user supersecret localhost 1812 testing123
   ```
   //it should fail as no users have been added

   Add Test Users
   ```
   # nano /etc/freeradius/users
   ```
   //and add this to the TOP of the file

   //replace username and password with your own.

   Test Radius Again
   ```
   # radtest username password localhost 1812 testing123
   ```
   //It should work this time around.

7. Configure clients.conf file
   //this file defines the networking devices that will need to use freeradius for authentication.
   //such as access points, switches or even other radius servers
   # mv clients.conf clients.conf.original
   # nano clients.conf

```
client localhost {
      ipaddr = 127.0.0.1
      secret          = XXXXXXXXXX
      require_message_authenticator = no
}

# the Zambia top level federation server
client zam-flr1{
       ipaddr   = 41.63.0.19
```

```
        netmask = 32
        secret   =  sharedsecretbetweenzamrenandistitution    #get this from ZAMREN
        shortname = Upstream
        require_message_authenticator = no
        nastype = other
        virtual_server = eduroam
}

# the Zambia top level federation server
client zam-flr2{
        ipaddr   = 41.63.0.20
        netmask = 32
        secret   =  sharedsecretbetweenzamrenandistitution    #get this from ZAMREN
        shortname = Upstream
        require_message_authenticator = no
        nastype = other
        virtual_server = eduroam
}

# Add your individual clients in this manner

client science-lab {
         ipaddr          = 192.168.0.60        //supply your ip of the access point
         netmask         =32
         secret          =  XXXXXXXXXX
         shortname       = Science-lab
         virtual_server  = eduroam
}

client library {
         ipaddr          = 192.168.0.0         //supply your ip of the access point
         netmask         = 24
         secret          =  XXXXXXXXXX
         virtual_server  = eduroam
}
```

8. Test Radius

   //good practice to test radius after each configuration to determine if there are any errors.

   # radtest first-user supersecret localhost 1812 testing123

   //it should work.

9. Configure proxy.conf file

   //controls the servers behaviour towards ALL other servers to which it sends proxy requests.

   # mv proxy.conf proxy.conf.original

   # nano proxy.conf

```
proxy server {
        default_fallback = no
}

home_server firstserver-givename {
        type = auth+acct
        ipaddr = 127.0.0.1
        port = 1812
```

```
        secret = XXXXXXXXXX
#       status_check = status-server
        check_interval = 6
        response_window = 5
}

home_server_pool groupforallservers{
        type = fail-over
        home_server = zam-radius1
}

# National Proxy1
home_server zam-flr1 {
        type = auth+acct
        ipaddr = 41.63.0.19
        port = 1812
        secret =  sharedsecretbetweenzamrenandistitution
#       status_check = status-server
        }

# National Proxy2
home_server zam-flr2 {
        type = auth+acct
        ipaddr = 41.63.0.20
        port = 1812
        secret =  sharedsecretbetweenzamrenandistitution
#       status_check = status-server
        }

home_server_pool zam-flr {
        type = fail-over
        home_server = zam-flr1
        home_server = zam-flr2
}

realm LOCAL {
nostrip
}

realm institution-domain-name.zm{
 nostrip
}

realm NULL {
}

realm "~.+$" {
        pool = zam-flr
        nostrip
}
```

10. Test Radius

    # radtest first-user supersecret localhost 1812 testing123

    //it should work.
    //can add users in file /etc/freeradius/users

11. Configure eap.conf

//??????????????????/

mkdir /etc/freeradius/certs/original-certs

cd /etc/freeradius/certs/original-certs

```
# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
  server.key -out server.pem
```

mv server.key server.pem /etc/freeradius/certs/

cd ../../

mv eap.conf eap.conf.original

nano eap.conf

```
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
          use_tunneled_reply = yes
                virtual_server = "eduroam"
        }
        peap {
                default_eap_type = mschapv2
                copy_request_to_tunnel = yes
                use_tunneled_reply = yes
                virtual_server = "eduroam"
        }
    mschapv2 {
        }

  }
```

12 Test Radius

radtest first-user supersecret localhost 1812 testing123

//it should work.

13. Virtual Servers

cd /etc/freeradius/sites-available
nano eduroam

```
server eduroam {
        authorize {
                suffix
                preprocess
                auth_log
                ldap
                chap
                mschap
                pap
                eap {
                        ok = return
                        }
}
authenticate {
        Auth-Type LDAP{
                ldap
        }
Auth-Type PAP{
        pap
        }
Auth-Type MS-CHAP{
        mschap
        }
Auth-Type EAP {
        eap
        }
Auth-Type CHAP {
        chap
        }
eap
}
preacct {
        preprocess
}
accounting {
        detail
        radutmp
        unix
        attr_filter.accounting_response
}
session {
        radutmp
}
post-auth {
        exec
        reply_log
        Post-Auth-Type REJECT {
                reply_log
        }
}
pre-proxy {
```

```
                attr_filter.pre-proxy
                pre_proxy_log
}
post-proxy {
        eap
                post_proxy_log
                attr_filter.post-proxy
        Post-Proxy-Type Fail {
                detail
                }
        }
}
```

14. Configure inner-tunnel file
    //???????????????
        # mv inner-tunnel inner-tunnel.original
        # nano inner-tunnel

```
server inner-tunnel {
listen {
       ipaddr = 127.0.0.1
       port = 18120
       type = auth
}
authorize {
        chap
        mschap
        suffix
        update control {
              Proxy-To-Realm := LOCAL
        }
        eap {
                ok = return
        }
        files
#        ldap     //commented out cause not installed and everywhere else it
appears
        expiration
        logintime
        pap
#######Point of Interest#############
        if (User-Password) {
                update control {
                        Auth-Type := ldap
                }
        }
}
authenticate {

########Point of Interest
        Auth-Type PAP {
#               pap
                ldap
        }
        Auth-Type CHAP {
                chap
        }
        Auth-Type MS-CHAP {
```

```
                mschap
        }
        ldap
        unix
        eap
}
session {
        radutmp
}
post-auth {
        Post-Auth-Type REJECT {
                attr_filter.access_reject
        }
}
pre-proxy {
}
post-proxy {
        eap
}
}
```

15. Create symbolic link in sites-enabled
    //similar to short cut in windows
    # cd ../sites-enabled
    # ln -s /etc/freeradius/sites-available/eduroam eduroam

Authenticating users of eduroam using Active Directory

16. Install Samba
    //samba is used to join the linux radius server to a windows domain. Some tools in samba will be used.
    # apt-get install samba-common winbind
    # apt-get install libnss-winbind libpam-winbind krb5-config krb5-locales krb5-us

Workgroup	DOMAIN
domain	DOMAIN.LOCAL or ZM
DC IP	w.x.y.z

17. Edit smb.conf
    # cd /etc/samba/
    # nano smb.conf

```
[global]

  workgroup = DOMAIN
  security = ads
  password server = w.x.y.z                    //ip of domain controller
  realm = domain.local                         //FQDN
      server string = %h server (Samba, Ubuntu)


;   wins server = w.x.y.z
```

```
  dns proxy = no


;   interfaces = 127.0.0.0/8 eth0

log file = /var/log/samba/log.%m

  max log size = 1000

  syslog = 0
```

Verify the following lines in the [homes] section

```
comment = Home Directories
browseable = no
writable = yes
```

18. Edit krb5.conf

nano /etc/krb5.conf

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = DOMAIN.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false

[realms]
 DOMAIN.LOCAL = {
  kdc = w.x.y.z:88
  admin_server = w.x.y.z:749
  default_domain = domain.local
 }

[domain_realm]
 .domain.local = DOMAIN.LOCAL
 domain.local = DOMAIN.LOCAL

        [kdc]
          profile = /var/kerberos/krb5kdc/kdc.conf

        [appdefaults]
```

```
pam = {
 debug = false
 ticket_lifetime = 36000
 renew_lifetime = 36000
 forwardable = true
 krb4_convert = false
}
```

19. Restart or start the Samba service
    # service samba restart (start)

20. Join the domain
    # net join -U Administrator

    //Administrator is the name of the domain controller admin.
    //Or you can use the name of a user that has rights to join a computer to the domain.
    //Enter your password when prompted.

21. Restart or start the winbindd service
    # service winbind restart (start)

22. Test authentication
    # wbinfo -a [username]
    # wbinfo -u list users
    # wbinfo -g list groups

23. Change permissions
    // add FreeRADIUS user to winbindd group:
        # usermod -a -G winbindd_priv freerad

    // Correct the permission on the Winbind pipe:
        # chown root:winbindd_priv /var/lib/samba/winbindd_privileged/

24. Change the path for ntlm_auth
    # updatedb
    # locate ntlm_auth

    // insert the path to the binary file in the line below and uncomment the line
    # nano /etc/freeradius/modules/mschap

```
ntlm_auth = "/path/to/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%
{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} –nt-response=%{%{mschap:NT-
Response}:-00}"
```

    // change the parts in bold
    # nano /etc/freeradius/modules/ntlm_auth

```
 program = "/path/to/ntlm_auth --request-nt-key --domain=MYDOMAIN --username=%
{mschap:User-Name} --password=%{User-Password}"
```

25. Restart the service
    # service freeradius restart

26. Test MS-CHAP authentication again:
    # radtest -t mschap [username] [password] localhost 0 [testing123]

Configuration of Cisco access points

```
aaa group server radius radsrv
 server w.x.y.z auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group radsrv
aaa authorization network default group radsrv
aaa accounting send stop-record authentication failure
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 15
aaa accounting network default start-stop group radsrv
aaa accounting network acc_methods start-stop group radsrv
!
aaa session-id common
ip domain name domain.zm
!
dot11 ssid eduroam
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa optional
   accounting acct_methods
   guest-mode
!
radius-server host v.w.x.z auth-port 1812 acct-port 1813 key 7 [secret-client-password]
```

****

apt-get install screen
screen -x [name]

****
open onother window to test.
        # freeradius -XXX
****

http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO

****