



---

# TECHNICAL MANUAL

---

Eduroam Deployment using RADIUS

Nov. 1, 2022

**Ethiopian Education and Research Network , MoE**

**TABLE OF CONTENTS**

Page #

**1. GENERAL INFORMATION Section 1.....1**  
    **1.1 Overview.....1**  
    **1.2 Architecture.....2**  
    **1.3 Installation.....3**  
**SECTION 2.....5**  
**SECTION 3.....7**

## 1. SECTION 1 : GENERAL INFORMATION

### 1.1 Overview

This document contains installation steps for successful deployment of Eduroam's idP on institutional level.

### 1.2 Terminology

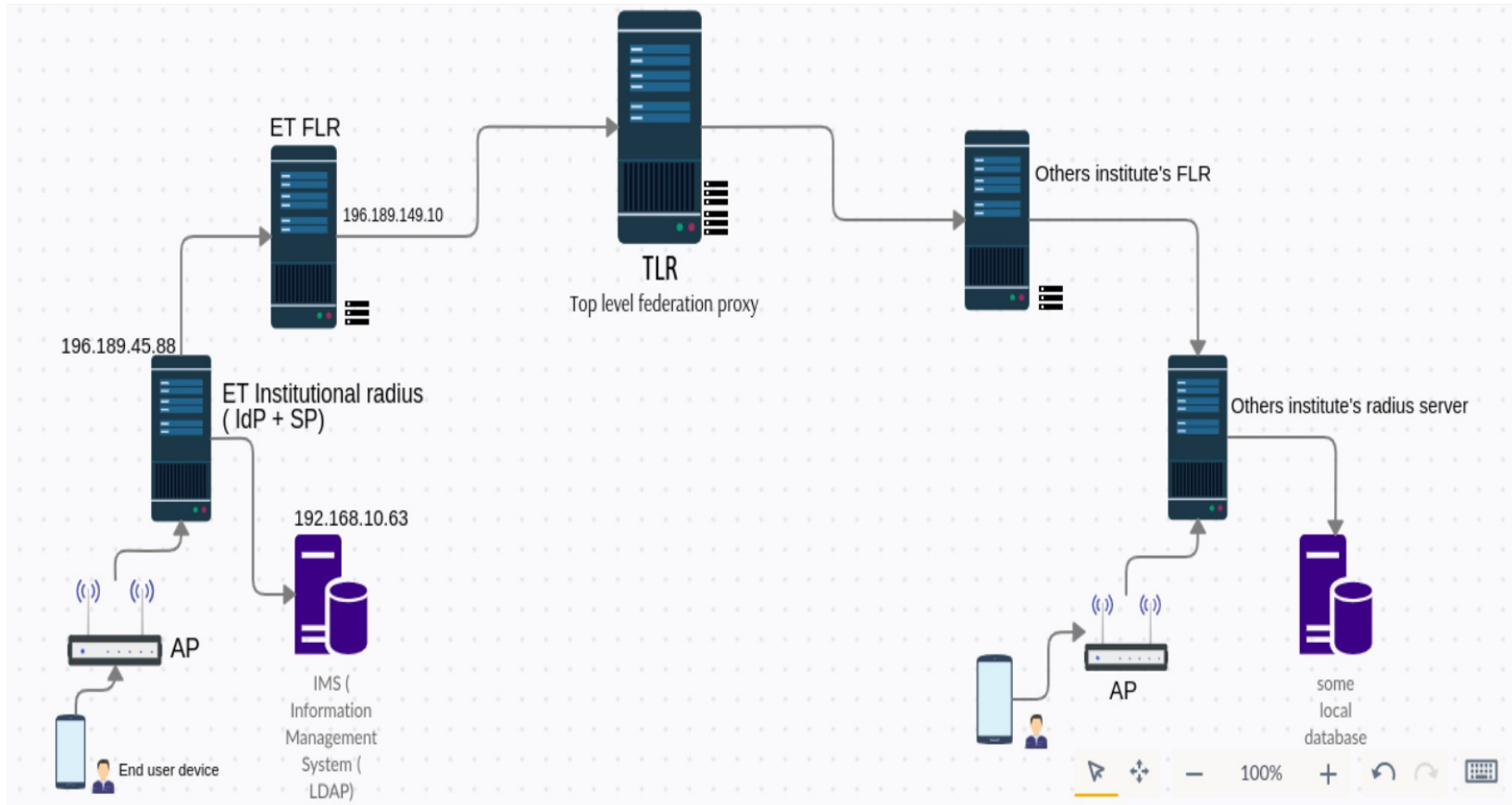
- **Home institution** = Identity provider Provides identity management database  
Authenticates its users
- **Visited institution** = Service provider Provides wireless network to roamers  
Responsible for authorization
- **FLR** – Federated Level Radius
- **TLR** – Top Level Radius

## What is it and How it works

In eduroam, communication between the access point and the user's home institution is based on IEEE 802.1X standard; 802.1X encompasses the use of EAP, the Extensible Authentication Protocol, which allows for different authentication methods.

Depending on the type of EAP method used, either a secure tunnel will be established from the user's computer to his home institution through which the actual authentication information (username/password etc.) will be carried (EAP-TTLS or PEAP), or mutual authentication by public X.509 certificates, which is not vulnerable to eavesdropping, will be used (EAP-TLS)

## 1.2 Architecture



## 1.3 Installation

### 1.3.1 Setting up Radius ( freeradius 3.0 )

#### Step 1

Let' make sure we are on the right OS version

```
$ lsb_release -a
```

```
idp@idp:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.5 LTS
Release:        18.04
Codename:       bionic
idp@idp:~$ █
```

#### Step 2

```
$ sudo apt update
```

```
$ sudo apt install freeradius*
```

#### Step 3

Create local users in the users file for testing purposes. Open the users file with your preferred editor (vi or nano) and add the text below at the top of the file (preferably replacing the bob line)

```
$ sudo nano /etc/freeradius/3.0/users
```

```
# The canonical testing user which is in most of the
# examples.
#
bob      Cleartext-Password := "hello"
        Reply-Message := "Hello, %{User-Name}"
█
```

### Step 3

Now restart the freeradius service and test the newly created user. You should get an accept reply.

```
$ sudo service freeradius restart
```

```
$ radtest bob hello localhost 0 testing123
```

```
root@Dev:/etc/freeradius/3.0# radtest bob hello localhost 0 testing123
Sent Access-Request Id 9 from 0.0.0.0:60267 to 127.0.0.1:1812 length 73
  User-Name = "bob"
  User-Password = "hello"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "hello"
Received Access-Accept Id 9 from 127.0.0.1:1812 to 127.0.0.1:60267 length 32
  Reply-Message = "Hello, bob"
root@Dev:/etc/freeradius/3.0# █
```

## SECTION 2

### 3.1 Setting up the Eduroam Server

#### Step 1

Delete all the files in sites-enabled folder. Create two files called eduroam and eduroam-inner-tunnel and paste the contents below to the corresponding files

```
$ sudo rm /etc/freeradius/3.0/sites-enabled/*  
$ sudo touch /etc/freeradius/3.0/sites-enabled/eduroam  
$ sudo nano /etc/freeradius/3.0/sites-enabled/eduroam
```

Paste the following code from the link into edruoam file and save it .

[edruoam file link](#)

Edit “Operator-Name ” and “SP-Country” according to yours.

```
authorize {  
  
    update request {  
        &Operator-Name := "lethernet.edu.et"    # Literal number "1" is important prefix!    }  
}
```

#### Step 2

Create the inner-tunnel file.

```
$ sudo touch /etc/freeradius/3.0/sites-enabled/eduroam-inner-tunnel  
$ sudo nano /etc/freeradius/3.0/sites-enabled/eduroam-inner-tunnel
```

Copy the content of the below code into the “eduroam-inner-tunnel” file we created before

[Eduroam inner tunnel file link](#)

### Step 3

Preserve some variables that overridden by default

```
$ sudo nano /etc/freeradius/3.0/mods-config/attr_filter/pre-proxy
```

Open the above file and add / append the following code

DEFAULT

```
User-Name =* ANY,  
User-Password =* ANY,  
CHAP-Password =* ANY,  
CHAP-Challenge =* ANY,  
MS-CHAP-Challenge =* ANY,  
MS-CHAP-Response =* ANY,  
EAP-Message =* ANY,  
Message-Authenticator =* ANY,  
State =* ANY,  
NAS-IP-Address =* ANY,  
NAS-Identifier =* ANY,  
Operator-Name =* ANY,  
Calling-Station-Id =* ANY,  
Chargeable-User-Identity =* ANY,  
Proxy-State =* ANY,  
Called-Station-Id =* ANY,  
Eduroam-SP-Country =* ANY,  
Operator-Name =* ANY
```



## SECTION 3

### 3.1 Configure RADIUS server to forward users to up streams

Let us now configure our RADIUS server to forward all users it doesn't recognize to the federation Proxy Server for Ethiopia (or any other African country). It will now serve as a Service Provider.

#### Step 1

create a back for the original config

```
$ sudo mv /etc/freeradius/3.0/proxy.conf /etc/freeradius/3.0/proxy.conf.original
```

#### Step 2

Receive proxy.conf from the regional ( EthERNET admins) or from your switchboard account put into *etc/freeradius/3.0/*

#### Step 3 : Configure clients

Now let us configure the clients. Again the main contents of the file should be generated and downloaded from the Switchboard or contact EthERNET Admins

put into *etc/freeradius/3.0/*

#### Step 4 : Configure Certificate

Let us now make the certificates used by eduroam. Open the ca.cnf file and edit the file to correspond as specified

```
$ sudo /etc/freeradius/3.0/certs/ca.cnf
```

```
[certificate_authority]
countryName           = ET
stateOrProvinceName  = Ethiopia
localityName          = Ethiopia
organizationName      = EthERNet
emailAddress           = support@ethernet.edu.et
commonName             = "EthERNet certeficate Authority"
```

change the value to this : default\_days = 3650

Now build the ca.pem and ca.der files

```
$ cd /etc/freeradius/3.0/certs/
```

```
$sudo make ca.pem
```

```
$ sudo make ca.der
```

*Step 4 Configure certeficate for server*

Edit the server.cnf file to correspond with the values edited in ca.cnf as shown below

```
$ sudo nano /etc/freeradius/3.0/certs/server.cnf
```

```
[server]
countryName           = ET
stateOrProvinceName  = Ethiopia
localityName          = Addis Ababa
organizationName      = EthERNet
emailAddress           = support@ethernet.edu.et
commonName             = "Ethernet Server Certificate"
```

change the value to this : default\_days = 3650

Then build the server.pem

```
$ cd /etc/freeradius/3.0/certs/  
$ sudo make server.pem
```

We need to now assign the correct file ownership

```
$ sudo chown freerad:freerad ca.*  
$ sudo chown freerad:freerad server.*  
$ sudo chown freerad:freerad index.*
```

Let us configure the EAP by editing the contents of the eap file to correspond as [as shown here](#). Here we are telling the eap file where our certificate is located and setting different configuration to use.

```
$ sudo rm /etc/freeradius/3.0/mods-enabled/eap  
$ sudo touch /etc/freeradius/3.0/mods-enabled/eap  
$ sudo nano /etc/freeradius/3.0/mods-enabled/eap
```

#### **Step 4 testing with rad\_eap\_test**

Let us now setup testing with rad\_eap\_test

```
$ sudo apt install libnl-genl-3-200 libpcsclite1  
$ cd ~/  
$ sudo apt install git  
$ git clone https://github.com/CESNET/rad_eap_test.git  
$ cd rad_eap_test  
$ sudo cp bin/eapol_test /usr/local/bin/
```

Let us now run any of the following tests using any of the users specified in the users file

```
$ ./rad_eap_test -H localhost -P 1812 -S testing123 -u eduroamuname -p eduroampass -m WPA-  
EAP -e TTLS
```

