eduroam configuring on FreeRADIUS 2.x server

By Fariborz Entezami, August 2014*

eduroam key points:

eduroam: a confederation of federations for unique authentication of Internet access and or other IT resources at the research and education community world wide and is now available in 69 territories world wide.

eduroam authentication: It employs 802.1X standard for access control and functions through a hierarchy of RADIUS proxies.

eduroam In the UK : eduroam is administered on a national level in the UK by JANET.

ORPS (Organizational RADIUS Proxy Server): The server or servers that are the main key point of eduroam in the organization. They take any eduroam requests from APs (Access Point) and forward them to the local authentication servers or their home organizations authentication systems through proxy servers for visiting users. They also receive requests for authentication from the other organizations through proxy servers.

NRPS (National RADIUS Proxy Server): They are the proxy servers at a national level, which accept and forward any proxied requests are destined in organizations who are looking for authenticating a visiting user by user's home organization.
NRPS analyzes the requests and then forwards them along to either other organizations within its realm or passes them along to the higher-level proxies, but they do not accept authentication requests by themselves.

IRPS (International RADIUS Proxy Server): The servers at the top level, which accept proxied requests from any NRPS, and re-directs them to the appropriate NRPS to administer. They do not accept authentication requests.

Set up an eduroam service

To set up an eduroam ORPS follow the instructions:

1.Make a backup of your original configuration

2. File : `/etc/raddb/attrs`

For adding attributes, edit and add the following lines to the file immediately below the `DEFAULT` line:

```
    User-Name =* ANY,
    Operator-Name =* ANY,
    Class =* ANY,
    Calling-Station-ID =* ANY,
    Chargeable-User-Identity =* ANY,
    Acct-Status-Type =* ANY,
    Acct-Session-ID =* ANY,
```

3. File : `/etc/raddb/dictionary`

Edit and add the following lines to the end of the file:

```
   ATTRIBUTE   Operator-Name           126   string
   ATTRIBUTE   Chargeable-User-Identity  89  string
```

4. File `/etc/raddb/clients.conf`

For adding the NRPS to the configuration edit the above file and add the following lines to it:

```
# This is eduroam federation proxy server who accept items fromclient
<IP address>

client Fed_1_Proxy {
       ipaddr = X.Y.Z.W  #Federation IP
       secret = abcdef   #Federation Secret
       shortname = eduroam-nrps #Fed Short Name
      virtual_server = eduroam
    }
```

5. File `/etc/raddb/proxy.conf`

Edit and uncomment the DEFAULT realm and modify it as follows:

```
    realm "~.+$" {
        authhost = X.Y.Z.W:1812 #Federation IP
        accthost = X.Y.Z.W:1813 #Federation IP
        secret = abcdef        #Federation Secret
        nostrip
        }
```

Note: Consider using a secret other than the default **testing123** in standard servers.

6. File `/etc/raddb/policy.conf`

To enable Chargeable-User-Identity (CUI) generation and requesting edit the above file, search for the following lines.

Note: In the steps below, replace `<realm>` with your local domain in FQDN format, e.g. university.ac.uk. The **1** prefix is required as per Section 4.1 of RFC 5580.

Note: replace `<hashkey>` with text of your choice. It will be used as a salt for CUI generation on this server.

Note: Do not use a 32-character hex-string, otherwise CUI generation will fail. This is a bug, which is fixed in FreeRADIUS 3.0.

```
    #  The following policies are for the Chargeable-User-Identity
    #  (CUI) configuration.
    #
    cui_hash_key = "<hashkey>"
    cui_require_operator_name = 1
```

- Replace the **cui_authorize** section with the following:

```
        cui_authorize {
          update request {
               Chargeable-User-Identity = '\\000'
               Operator-Name = "1<realm>"
          }
    }
```

- Insert a new item called **cui_preproxy** as below:

```
    #   The proxy indicates that it needs to do CUI by sending a CUI
attribute
     #  containing one zero byte
     #
     cui_preproxy {
          if ("%{Packet-Type}" == Access-Request) {
               update proxy-request {
                    Chargeable-User-Identity = '\\000'
                    Operator-Name = "1<realm>"
               }
          }
     }
```

- Replace the **cui_postauth** section with the following:

```
     cui_postauth {
          if (FreeRadius-Proxied-To == 127.0.0.1) {
               if (outer.request:Chargeable-User-Identity && \
                  (outer.request:Operator-Name                                  ||
!("${policy.cui_require_operator_name}"))) {
                    update outer.reply {
                         Chargeable-User-
Identity:="%{md5:${policy.cui_hash_key}%{User-
Name}%{outer.request:Operator-Name:-}}"
                    }
               }
          }
          else {
               if (!("%{control:Proxy-To-Realm}") && \
                   Chargeable-User-Identity && \
                   !(reply:Chargeable-User-Identity) && \
                   (Operator-Name                                               ||
!("${policy.cui_require_operator_name}")) ) {
                    update reply {
                         Chargeable-User-
Identity="%{md5:${policy.cui_hash_key}%{User-Name}%{%{Operator-Name}:-
}}"
                    }
               }
          }
          update reply {
               User-Name-="%{reply:User-Name}"
          }
     }
```

6. File `/etc/raddb/eap.conf`

`Edit and` change all instances of `copy_request_to_tunnel` and `use_tunneled_reply` to `yes`, otherwise CUI generation occurs on the anonymised outer request (i.e. all users from the same home institution will have the same CUI).

7. Modify user authentication

In order to uniform the usernames in eduroam networks and avoid to send any unrelated usernames to NRPS and for organization users to get used to **eduroam**, a RADIUS policy has been enforced that requires any usernames used for authentication to be in the `<user>@<realm>` format, where `<realm>` is in FQDN format. Because **eduroam** functions by checking realms, enforcing such a policy will ensure that there are no problems when your users roam onto an **eduroam** network elsewhere in the world.
The University of Bristol publishes an **eduroam** realm check script, which can be found under Section 11.8 in the Implementing eduroam Roadmap document at JANET.
Download `eduroam-realm-checks.conf` from the University of Bristol and copy it to the `/etc/raddb/` directory.

8. File `/etc/raddb/sites-available/default`

Edit and modify the above file as:

- In the **authorize** section, add the following lines at the top of the section:

```
    #  Add a request for CUI + add operator name
    #
    cui_authorize
    #  Implement the eduroam username-realm filter
    #
    $INCLUDE eduroam-realm-checks.conf
```

- In the **post-auth** section, add the following lines at the top of the section:

```
    #  Get a CUI
    cui_postauth
```

- In the **pre-proxy** section, add the following lines at the bottom of the section:

```
   #     Request the Chargeable-User-Identity attribute from the upstream/home server
    cui_preproxy
```

- In the **post-proxy** section, uncomment the line containing

```
    attr_filter.post-proxy
```

9. File `/etc/raddb/sites-available/inner-tunnel`

Edit and modify it as:

- In the **post-auth** section, add the following lines at the top of the section:

```
     #  Get a CUI
     cui_postauth
```

10. File `/etc/raddb/sites-available/eduroam`

Create and modify it as follows:

```
server eduroam {
     authorize {
          auth_log
          cui_authorize
          wimax
          suffix
          eap {
               ok = return
          }
          files
     }

     authenticate {
          #  Comment out the PAP Auth-Type once your eduroam setup is
working
          Auth-Type PAP {
               pap
          }
          #  eduroam only supplies EAP authentication
          eap
     }

     post-auth {
          cui_postauth
          reply_log
          #  authentication failed. eduroam requires you to log these
          Post-Auth-Type REJECT {
               attr_filter.access_reject
               reply_log
          }
     }

     pre-proxy {
          if ("%{Packet-Type}" == Access-Request) {
               attr_filter.pre-proxy
          }
          cui_preproxy
          pre_proxy_log
```

```
    }

    post-proxy {
        post_proxy_log
        attr_filter.post-proxy
        # if you don't proxy LEAP, comment the following line out
        eap
    }
}
```

11. File `/etc/raddb/sites-enabled/eduroam`

Create a soft copy from `/etc/raddb/sites-available/eduroam` to enable the **eduroam** virtual server.

12. Enable more extensive logging

eduroam requires you to log authentication attempts for both visitors and for requests coming from the **eduroam** NRPS. Additionally, JANET and **eduroam** also publish usage statistics with a system called F-TICKS. To enable F-TICKS and other logging mechanisms, do the following:

13. File `/etc/raddb/modules/eduroam_logging`

Create and modify it as follows:

Note: In the steps below, replace `<realm>` with your local domain in FQDN format, e.g. university.ac.uk. The **1** prefix is required as per Section 4.1 of RFC 5580:

```
linelog f_ticks { filename = syslog format = ""
reference = "f_ticks.%{%{reply:Packet-Type}:-format}"
f_ticks { Access-Accept = "F-
TICKS/eduroam/1.0#REALM=%{Realm}#VISCOUNTRY=UK#VISINST=1<realm>#CSI=
%{%{Calling-Station-Id}:-UnknownCSID}#RESULT=OK#" Access-
Reject = "F-
TICKS/eduroam/1.0#REALM=%{Realm}#VISCOUNTRY=UK#VISINST=1<realm>#CSI=
%{%{Calling-Station-Id}:-UnknownCSID}#RESULT=FAIL#" } }
linelog eduroam_log { filename = syslog format = ""
reference = "eduroam_log.%{%{reply:Packet-Type}:-format}"
eduroam_log { Access-Accept = "eduroam-
auth#ORG=%{request:Realm}#USER=%{User-Name}#CSI=%{%{Calling-Station-
Id}:-Unknown Caller Id}#NAS=%{%{Called-Station-Id}:-Unknown Access
Point}#CUI=%{%{reply:Chargeable-User-Identity}:-
Unknown}#MSG=%{%{EAP-Message}:-No EAP Message}#RESULT=OK#"
Access-Reject = "eduroam-
auth#ORG=%{request:Realm}#USER=%{User-Name}#CSI=%{%{Calling-Station-
Id}:-Unknown Caller Id}#NAS=%{%{Called-Station-Id}:-Unknown Access
```

```
Point}#CUI=%{%{reply:Chargeable-User-Identity}:-
Unknown}#MSG=%{%{reply:Reply-Message}:-No                    Failure
Reason}#RESULT=FAIL#"     } }
linelog  inner_auth_log  {       filename  =  syslog       format  =  ""
      reference   =   "inner_auth_log.%{%{reply:Packet-Type}:-format}"
       inner_auth_log    {              Access-Accept    =    "user-
auth#VISINST=%{request:Operator-Name}#USER=%{User-
Name}#CSI=%{%{Calling-Station-Id}:-Unknown                   Caller
Id}#NAS=%{%{Called-Station-Id}:-Unknown                      Access
Point}#CUI=%{%{%{reply:Chargeable-User-Identity}:-
%{outer.reply:Chargeable-User-Identity}}:-Local     User}#RESULT=OK#"
          Access-Reject    =    "user-auth#VISINST=%{request:Operator-
Name}#USER=%{User-Name}#CSI=%{%{Calling-Station-Id}:-Unknown   Caller
Id}#NAS=%{%{Called-Station-Id}:-Unknown                      Access
Point}#CUI=%{%{%{reply:Chargeable-User-Identity}:-
%{outer.reply:Chargeable-User-Identity}}:-Local   User}#RESULT=FAIL#"
     } }
```

14. File `/etc/raddb/sites-available/default`

Edit and modify it:
- In the **post-auth** section, uncomment `reply_log` and insert these lines blow it:
  ```
  f_ticks
  eduroam_log
  ```

- In the **post-auth `Post-Auth-Type REJECT`** section, insert `reply_log`
  ```
  f_ticks
  eduroam_log
  ```

15. File `/etc/raddb/sites-available/eduroam`

Edit and modify it as:
- In the **post-auth** section, insert this line below `reply_log: eduroam_log`

- In the **post-auth `Post-Auth-Type REJECT`** section, insert this line below `reply_log :`
  ```
  eduroam_log
  ```

16. File `/etc/raddb/sites-available/inner-tunnel`

Edit and modify it:
- In the **post-auth** section, insert this line below the commented-out `reply_log` line:
  ```
  inner_auth_log
  ```

- In the **post-auth `Post-Auth-Type REJECT`** section, insert below the `sql` line:
  ```
  inner_auth_log
  ```

Each of these logs generates a single line entry into the syslog, i.e. `/var/log/messages`, while

`reply_log, pre_proxy_log, post_proxy_log, auth_log`, etc. generate a more detailed log of the RADIUS traffic in `/var/log/radius/radacct/<client IP>`.

17. Modify the firewall rules

The ORPS proxy cannot respond to requests from the NRPS for authentication without the following ports being open in firewall of the organization:

- 1812/UDP
- 1813/UDP
- 1814/UDP

* This document has been regenerated based on “Configuring an eduroam FreeRADIUS 2.x server (superceded)” by Stefan Paetow.