TP1 Installation et configuration de base de Freeradius

Objectifs
1- installer freeradius freeradius-utils, freeradius-ldap, freeradius-mysql
2- Arreter le serveur freeradius
3- créer des comptes à des utilisateurs dans le fichier /etc/freeradius/users
4- Demarrer freeradius en mode debug
5- utiliser l'utilitaire radtest pour tester en local
6- créer un compte à un point d'acces WIFI
7- Parametrer un point d'acces WIFI en mode de securité WPA-entreprise pour l'utilisation de radius
8- Parmetrer des terminaux windows, Linux et android pour se connecter sur AP securisé avec la methode d'authentification PEAP

TP RADIUS 2

Objectifs de ce TP
1- Savoir Configurer des VLAN sur un swicth
2- Savoir créer des comptes dans le fichier users de freeradius pour la prise en charge des VLAN dynamiques
3- Savoir activer et parametrer sur une carte reseau d'une machine la prise en charge du protocole 802.1x
4- Savoir activer sur un switch cisco le protocole 802.1x
5- Savoir activer sur un switch cisco la prise en compte du protocole 802.1x et le Vlan Dynamique
6- Savoir configuerer un serveur radius pour la prise en charge des comptes dans une base de données relationnelle
7- Savoir gerer des informations de VLAN dynamique dans une Base de donnees relationnelle

1- Configuration des comptes utilisateurs avec leur VLAN dans le fichier users qui se trouve dans le dossier /etc/freeradius

```
toto Auth-Type := EAP,User-Password := "passer"
        Service-Type = Framed-User,
        Tunnel-Type = "VLAN",
        Tunnel-medium-Type = "IEEE-802",
        Tunnel-Private-Group-Id = 10
bouki Auth-Type := EAP,User-Password := "passer"
        Service-Type = Framed-User,
        Tunnel-Type = "VLAN",
        Tunnel-medium-Type = "IEEE-802",
        Tunnel-Private-Group-Id = 20
```

2- **Configuration du switch 2950**

2.1 Parametrer les elements TCP/IP au switch pour qu'il puisse communiquer avec le serveur radius

switch# conf t

```
switch(config)#int vlan 1
switch(config-if)# ip add 192.168.1.10 255.255.255.0
switch(config-if)# no sh
```

2.2 Configuration de la prise en charge du protocole 802.1x par le switch

```
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#aaa authorization network default group radius
Switch(config)#radius-server host 192.168.1.20  auth-port 1812 acct-port 1813
key passer123
```

Il faut parametrer le port 2 en 802.1x

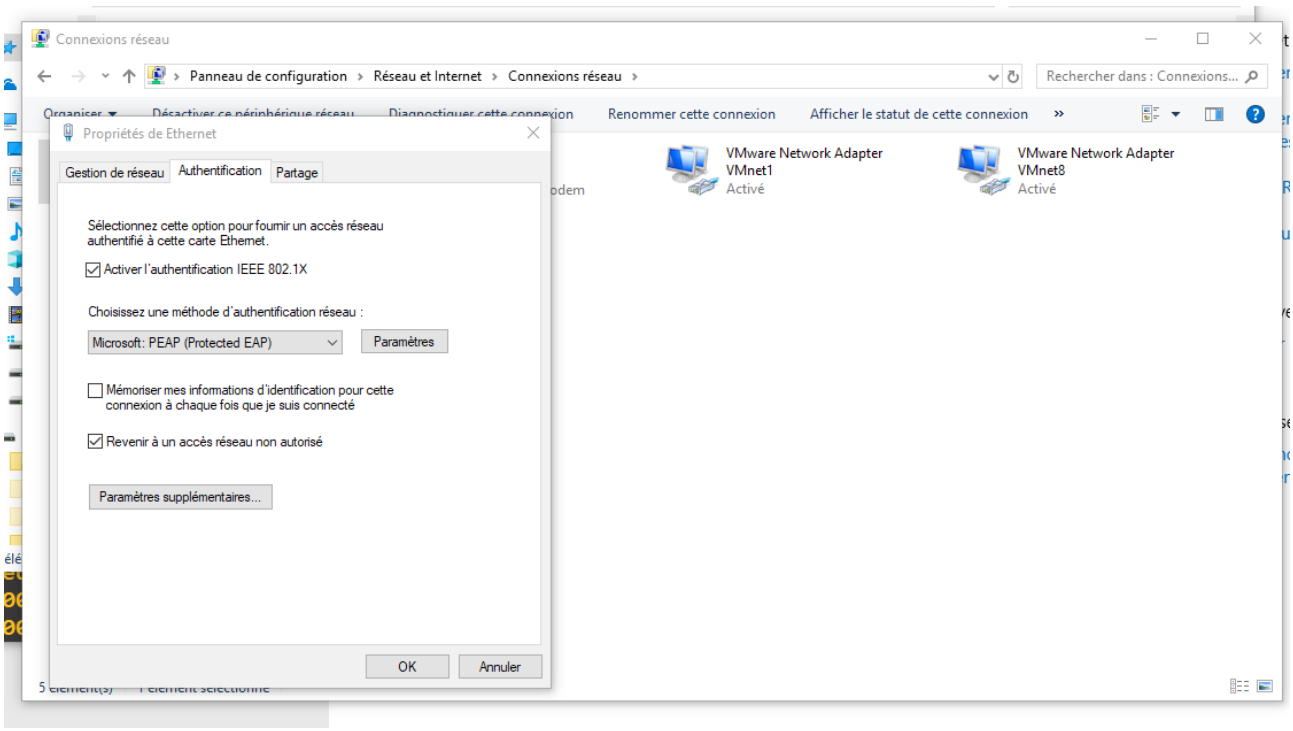
```
swicth# int fa0/2

switch(config-if)# switchport mode access

switch(config-if)# dot1x port-control auto

switch(config-if)#dot1x guest-vlan  40
```

NB : Dans notre cas, le serveur freeradius a pour adresse IP 192.168.1.20

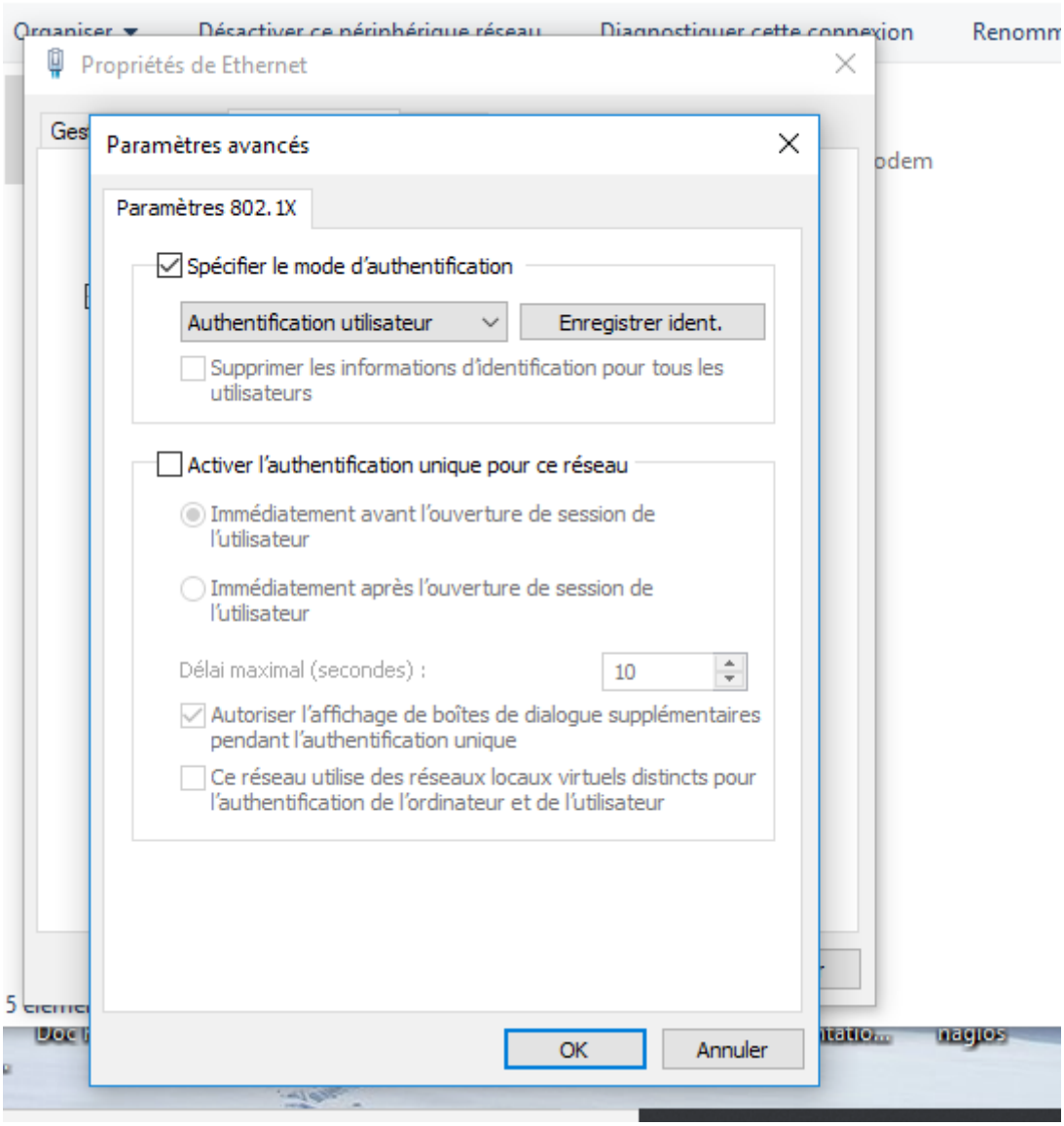
3. Configuration du supplicant Windows 10

Sur l'interface Ethernet de la machine, on active le protocole 802.1x

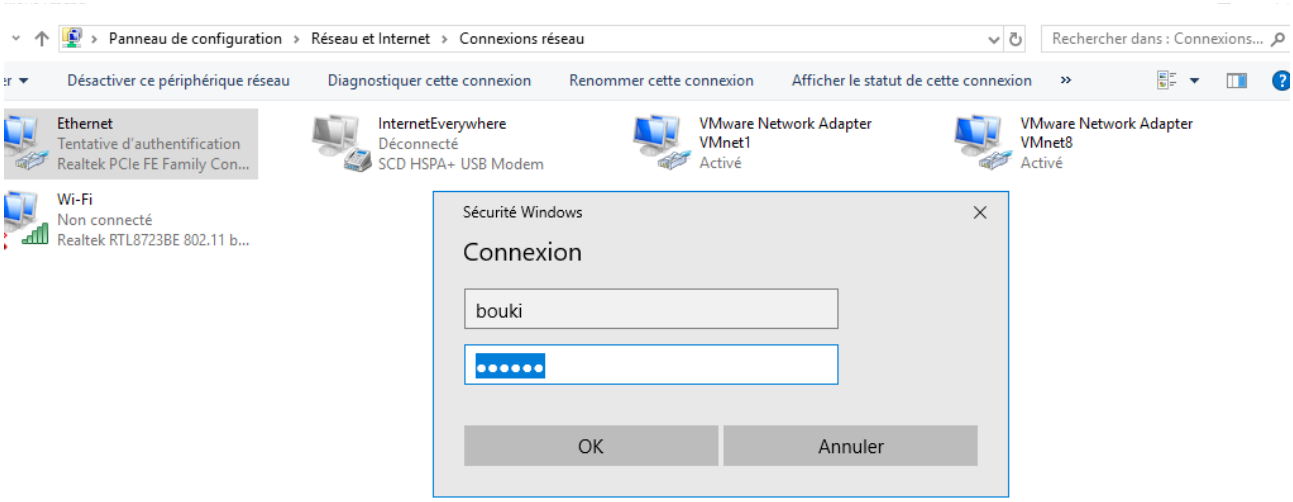
Dans authentification :



Puis on clique sur parametres supplementaires pour choisir le mode d’authentification utilisateur



Après validation, on obtient l'écran d'authentification suivant :



Apres authentification, on castate sur ‘interface du serveur radius qu’il a authentifié bouki et a doné l’ordre au switch de mettre l’utilisateur boui dans le vlan 20

```
[peap] Success
[peap] Using saved attributes from the original Access-Accept
        Service-Type = Framed-User
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "20"
        User-Name = "bouki"
[eap] Freeing handler
++[eap] = ok
+} # group authenticate = ok
# Executing section post-auth from file /etc/freeradius/sites-enabled/default
+group post-auth {
++[exec] = noop
+} # group post-auth = noop
Sending Access-Accept of id 44 to 192.168.1.10 port 1812
        Service-Type = Framed-User
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "20"
        User-Name = "bouki"
        MS-MPPE-Recv-Key = 0xaddddc00840f82dd9a617daa42d15f5586309922bc39d0c3712cb5e9471d4ecb
        MS-MPPE-Send-Key = 0x6faf61b7be494f5ff260de1a959c137adfdc64afc67069e4ba67bf9031ba71ca
        EAP-Message = 0x03080004
        Message-Authenticator = 0x00000000000000000000000000000000
Finished request 8.
```

Sur le swich , on saisit : sh vlan

Switch# sh vlan

Et on constate que le port fa0/2 a été mis effectivement dans le VLAN 20

COM9 - PuTTY

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Gi0/1
                                                Gi0/2
2    VLAN0002                         active
3    VLAN0003                         active
10   VLAN0010                         active
20   VLAN0020                         active    Fa0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
--More--
```

4- Utilisation d ‘une base de données mysql avec freeradius

4.1 on active la prise en charge de mysql par freeradius

On edite le fichier /etc/freeradius/sites-availables/inner-tunnel

Dans la section authorire, on decommente sql comme suit :

```
        #
        #  Look in an SQL database.  The schema of the database
        #  is meant to mirror the "users" file.
        #
        #  See "Authorization Queries" in sql.conf
        sql

        #
```

Dans la section session du meme fichier, on decommente sql comme suit :

```
#  Session database, used for checking Simultaneous-Use. Either the radutmp
#  or rlm_sql module can handle this.
#  The rlm_sql module is *much* faster
session {
        radutmp

        #
        #  See "Simultaneous Use Checking Queries" in sql.conf
        sql
}
```

Dans la section post-auth, on decommente sql comme suit :

```
#  Post-Authentication
#  Once we KNOW that the user has been authenticated, there are
#  additional steps we can take.
post-auth {
        # Note that we do NOT assign IP addresses here.
        # If you try to assign IP addresses for EAP authentication types,
        # it WILL NOT WORK.  You MUST use DHCP.

        #
        #  If you want to have a log of authentication replies,
        #  un-comment the following line, and the 'detail reply_log'
        #  section, above.
#       reply_log

        #
        #  After authenticating the user, do another SQL query.
        #
        #  See "Authentication Logging Queries" in sql.conf
        sql

        #
        #  Instead of sending the query to the SQL server,
        #  write it into a log file.
        #
#       sql_log
```

4.2 On cree une base de donnees radius et on importe les tables necessaires grace au fichier schema.sql qui se trouve :

```
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql# ls
admin.sql     cui.conf  dialup.conf  ippool-dhcp.conf  nas.sql     wimax.conf
counter.conf  cui.sql   ippool.conf  ippool.sql        schema.sql  wimax.sql
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql#
```

```
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.7.26-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> create database radius;
Query OK, 1 row affected (0,00 sec)
```

On importe maintenant les tables :

```
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql# mysql -u root -p radius < schema.sql
Enter password:
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql#
```

On se connetce à la base radius, comme suit :

```
root@ubuntu-ESPRIMO-E500:/etc/freeradius/sql/mysql# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.26-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Et on insere un user dans la table des comptes
par la commande

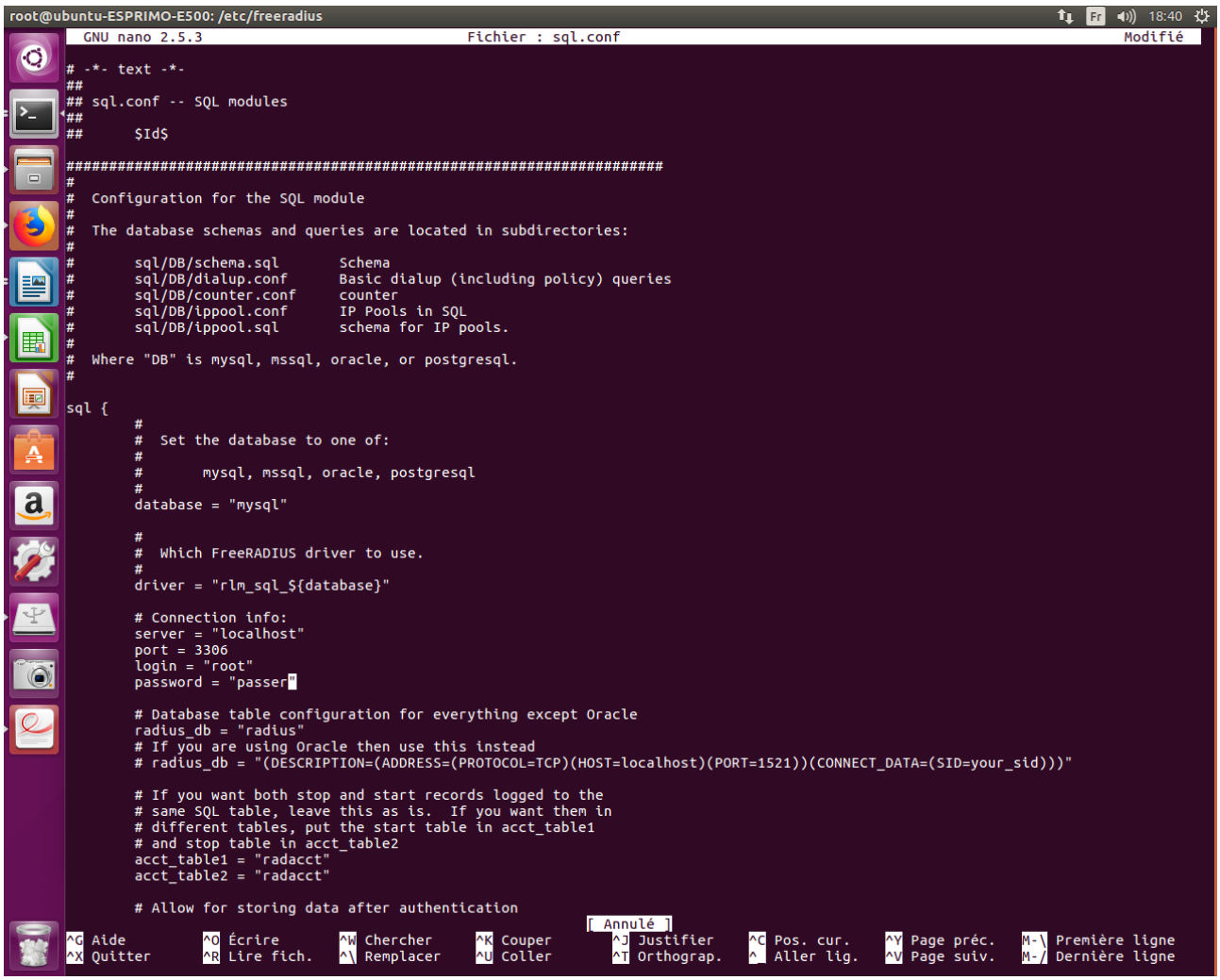
```
insert into radcheck (username,attribute,op,value) values ("babadi","Cleartext-Password",":=","passer");
```

```
mysql> insert into radcheck (username,attribute,op,value) values ("babadi","Cleartext-Password",":=","passer");
Query OK, 1 row affected (0,05 sec)
```

Ensuite , on insere les 3 attributs replyitems concernant babadi

```
mysql> insert into radreply (username,attribute,op,value) values ("babadi","Tunnel-Type","=","VLAN");
Query OK, 1 row affected (0,05 sec)

mysql>  into radreply (username,attribute,op,value) values ("babadi","Tunnel-Medium-Type","=","IEEE-802");
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the righ
t syntax to use near 'into radreply (username,attribute,op,value) values ("babadi","Tunnel-Medium-Type' at line 1
mysql> insert into radreply (username,attribute,op,value) values ("babadi","Tunnel-Medium-Type","=","IEEE-802");
Query OK, 1 row affected (0,06 sec)

mysql> insert into radreply (username,attribute,op,value) values ("clem","Tunnel-Private-Group-Id","=","10");
Query OK, 1 row affected (0,04 sec)

mysql>
```

On configure la connexion à la base de données dans le fichier /etc/freeradius/sql.conf
en bien reisignant le nom de la base, le compte utilisateur à utiliser et son son mot de passe



Observez bien les noms des autres tables de la base radius :

```
        # If you want both stop and start records logged to the
        # same SQL table, leave this as is.  If you want them in
        # different tables, put the start table in acct_table1
        # and stop table in acct_table2
        acct_table1 = "radacct"
        acct_table2 = "radacct"

        # Allow for storing data after authentication
        postauth_table = "radpostauth"

        authcheck_table = "radcheck"
        authreply_table = "radreply"

        groupcheck_table = "radgroupcheck"
        groupreply_table = "radgroupreply"

        # Table to keep group info
        usergroup_table = "radusergroup"

        # If set to 'yes' (default) we read the group tables
        # If set to 'no' the user MUST have Fall-Through = Yes in the radreply table
        # read_groups = yes

        # Remove stale session if checkrad does not see a double login
        deletestalesessions = yes

        # Print all SQL statements when in debug mode (-x)
        sqltrace = no
        sqltracefile = ${logdir}/sqltrace.sql
```

En se connectant sur la base radius, on peut observer les differentes tables générées :

```
root@ubuntu-ESPRIMO-E500: ~
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+------------------+
| Tables_in_radius |
+------------------+
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| radusergroup     |
+------------------+
7 rows in set (0,00 sec)

mysql>
```

```
ert into radcheck (username,attribute,op,value) values ("babadi","Cleartext-Password",":=","passer");
```

Dans la fichier /etc/freeradius/radiusd.conf allez dans la session module et decommenter la ligne comme suit :

```
        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        #
        $INCLUDE sql.conf

        #
        #  This module is an SQL enabled version of the counter module.
        #
        #  Rather than maintaining seperate (GDBM) databases of
        #  accounting info for each counter, this module uses the data
        #  stored in the raddacct table by the sql modules. This
        #  module NEVER does any database INSERTs or UPDATEs.  It is
        #  totally dependent on the SQL module to process Accounting
        #  packets.
        #
```

Enfin redemarrez le serveur radius en mode debbug

 # freeradius -X

et verifier que tout bien

Test

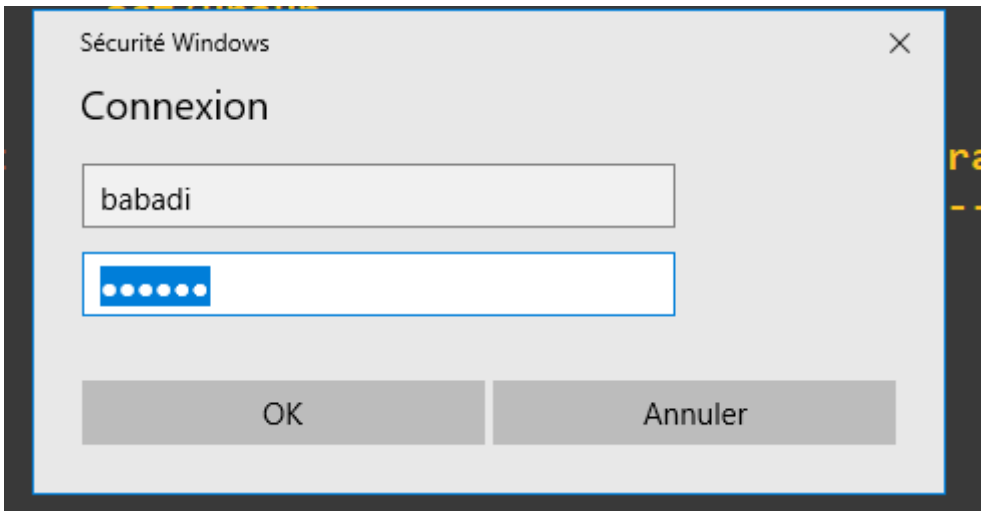
j’ai constaté que j »avais une erreur dans l’insertion de vlan de babadi donc je rectifie comme suit :

```
mysql> insert into radreply (username,attribute,op,value) values ("babadi","Tunnel-Private-Group-Id","=","10");
Query OK, 1 row affected (0,04 sec)
```

Sur l’interface de radius, il a donne l’ordre au switch de mettre babadi dans le vlan 10

```
+} # group post-auth = ok
Sending Access-Accept of id 62 to 192.168.1.10 port 1812
        Tunnel-Type:0 = VLAN
        Tunnel-Medium-Type:0 = IEEE-802
        Tunnel-Private-Group-Id:0 = "10"
        User-Name = "babadi"
        MS-MPPE-Recv-Key = 0xf289907d146d4cebb2bdcefb363812a5b9a1ce2d30f3a4ee4ea487a15323ac60
        MS-MPPE-Send-Key = 0xc644d6a91529f01ea15f4b19ceb78873afca63efc06b9b1d9d91cc98b0853f31
        EAP-Message = 0x03080004
        Message-Authenticator = 0x00000000000000000000000000000000
Finished request 8.
Going to the next request
Waking up in 4.7 seconds
```

Sur le supplicant windows, on se connecte sur le port 2 du switch



Sur le swich, on tape : sh vlan et on constate que le port 2 est bien mis dans le VLAN 10 d'appartenance de babadi

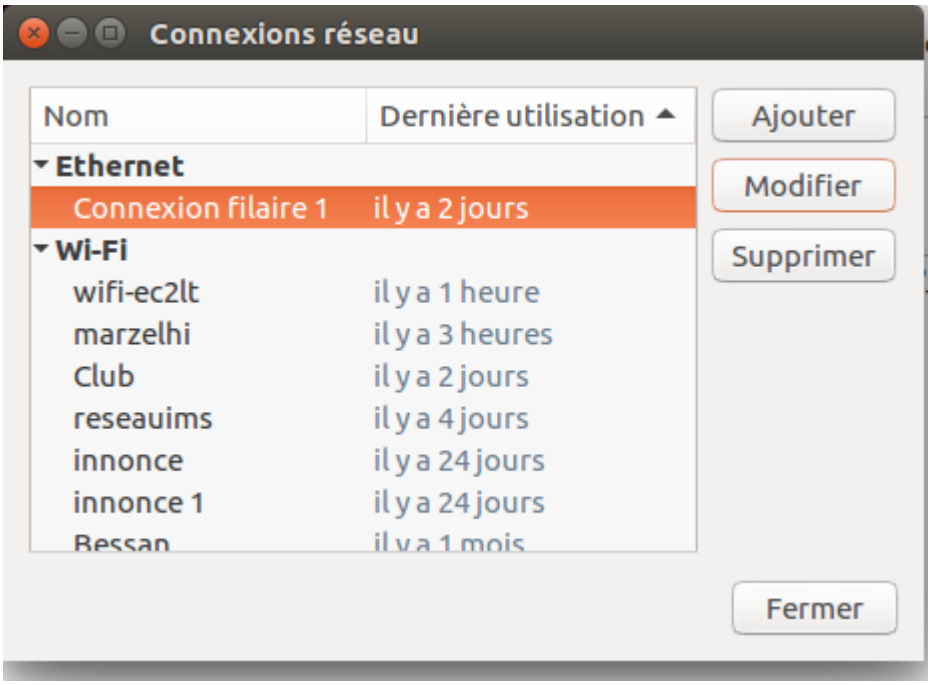
```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Gi0/1
                                                Gi0/2
2    VLAN0002                         active
3    VLAN0003                         active
10   VLAN0010                         active    Fa0/2
20   VLAN0020                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
3    enet  100003     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
 --More--
```

Parmetrage d'une carte reseau ethernet sous linux en 802.1x

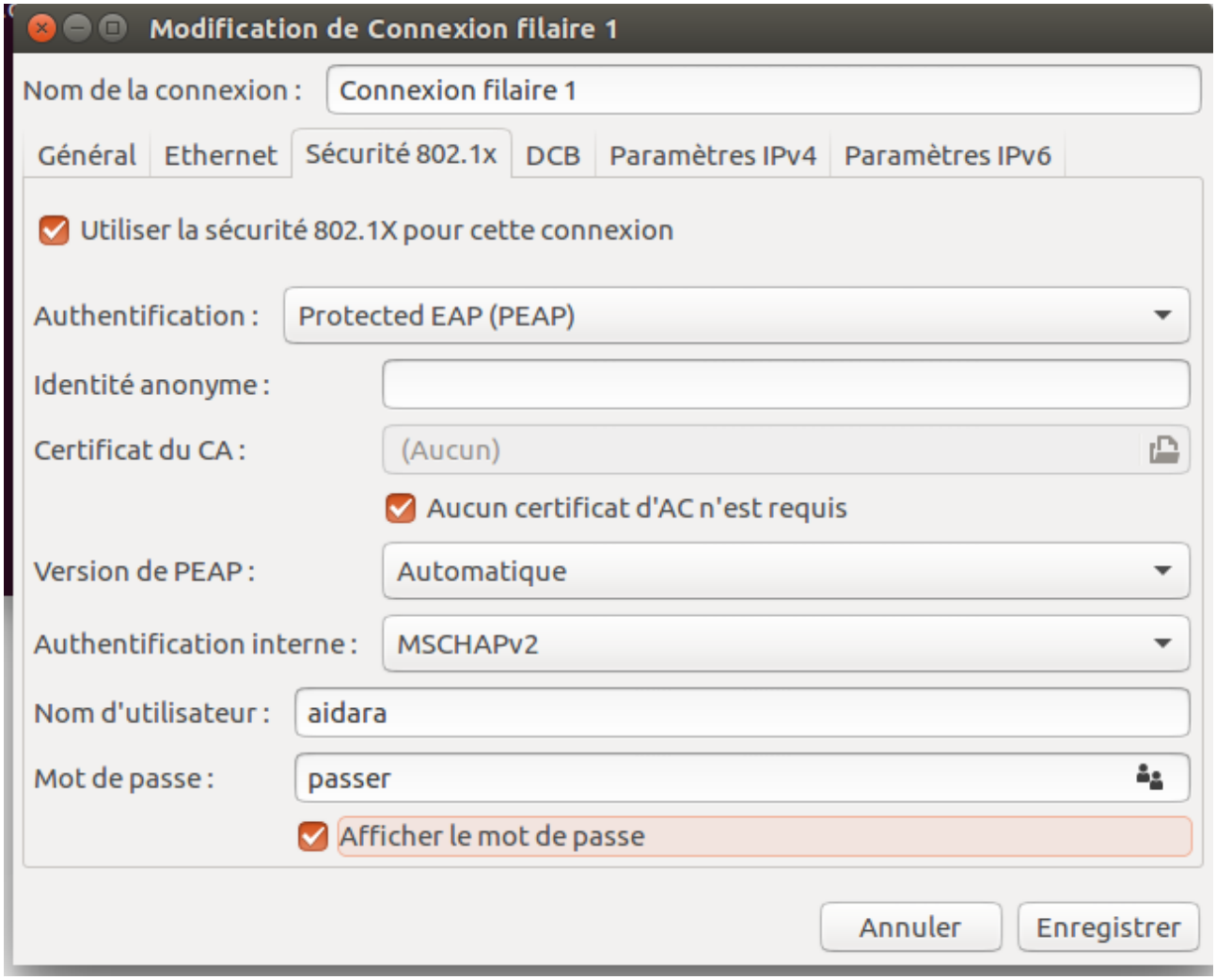
a- En tant que root on lance la commande nm-connection-editor comme suit :

```
root@innonce-Linuxien:~#
root@innonce-Linuxien:~# nm-connection-editor
```

b- on obtient l'ecran suivant :



c- on clique sur modifier pour choisir la methode PEAP et donner les informations de compte



NB : Comme aucun certificat n’est installé au niveau du supplicant Linux, il est important de cocher « aucun certificat d’AC n’est requis »

Dans l ‘episode à venir, on va vous montrer comment générer, installer et utiliser les certificats en vue d ‘utilisation des méthodes TLS, TTLS