



Nom de l'entreprise : IUT de Caen, Campus III

Adresse : Rue Anton Tchekhov 14123 IFS

Tél. : 02.31.52.55.00

Fax : 02.31.52.55.22

Du lundi 21 janvier 2013

Au vendredi 22 février 2013

Sommaire

Présentation de l'entreprise	2
Organigramme	3
Introduction	4
Description de l'activité	5-25
Remerciements	26
Conclusion	27
Annexe	28

IUT de Caen, Campus III

Rue Anton Tchekhov

14123 IFS



L'Université de Caen Basse-Normandie est implantée sur plusieurs campus de l'agglomération caennaise et sur 6 sites universitaires qui maillent le territoire régional :

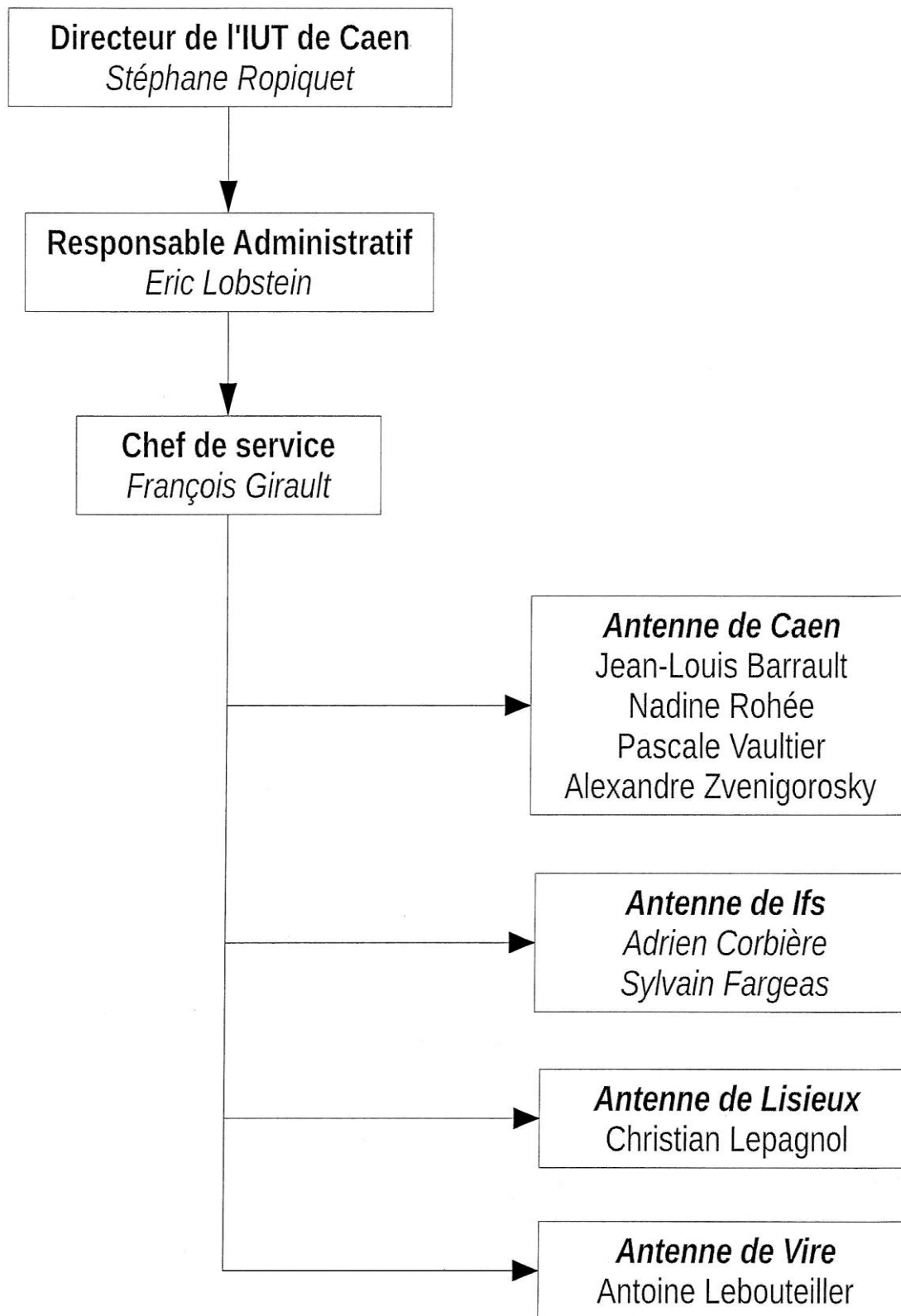
- Caen
- Alençon
- Cherbourg-Octeville
- Lisieux
- Saint-Lô
- Vire

L'université de Caen est divisée en 6 campus : campus 1-2-3-4-5-IUFM centre de Caen

C'est en 1996 que le campus III a vu le jour par l'installation des départements "Information Communication" et "Informatique", puis en 2002 l'ouverture du département "Génie des Télécommunications et Réseaux" et enfin en 2009 la création de la Licence professionnelle "Audit et Sécurité des Réseaux" à IFS.

Organigramme du service informatique de l'IUT de Caen

Maj 21.02.2013



Ma mission était de mettre en place une authentification forte pour avoir une sécurité plus accrue sur un réseau.

Le principe est d'authentifier une machine qui se branche sur le réseau afin de lui autoriser ou refuser l'usage du réseau.

L'authentification sert à :

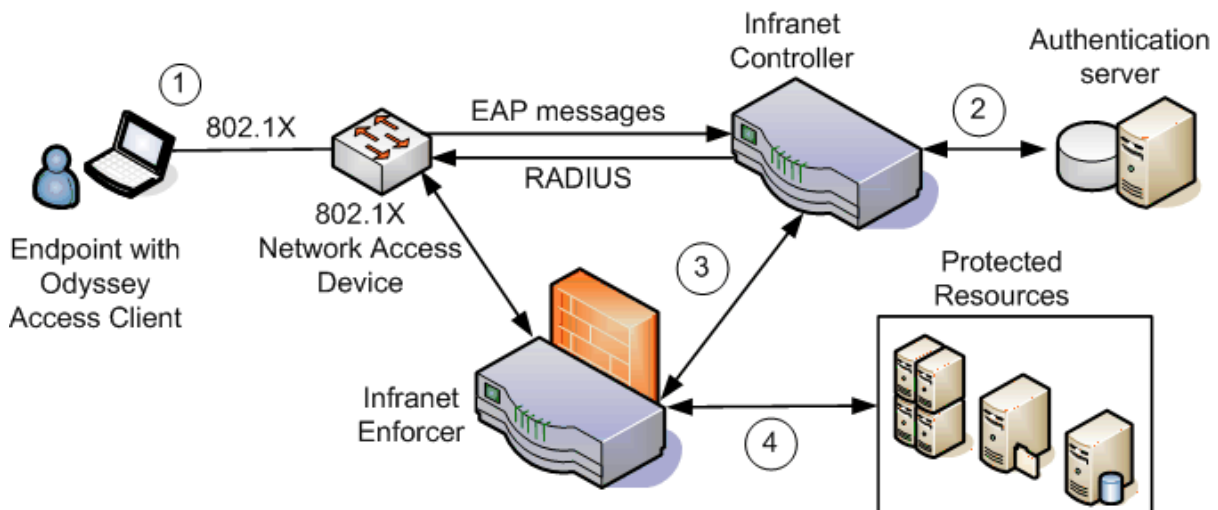
- sécuriser le réseau
- interdire les machines inconnues
- placer les machines connues dans les bons vlans
- savoir quelle machine est connectée et où

Il est possible d'authentifier une machine par son adresse MAC et/ou un utilisateur par le couple d'un login/passwd.

Pour pouvoir authentifier, il faut l'adresse MAC de la carte Ethernet de la machine et/ou une base d'annuaire (ldap,sql,AD etc...) et/ou des certificats (par utilisateurs ou machines).

Il existe deux protocoles d'authentification :

- le protocole propriétaire de Cisco par exemple, mais il permet l'authentification sur adresse MAC uniquement et que en filaire,
- le protocole ouvert avec radius et 802.1x qui permet toute sorte d'authentification comme l'adresse MAC, le login/passwd, certificats etc... et qui se fait en filaire ainsi que sans-fil.



Radius signifie : Remote Access Dial In User Service

Il utilise le port UDP 1812 (anciennement 1645).

Radius est un serveur de type AAA :

AAA (Authentication, Authorization and Accounting) est un protocole qui permet de gérer :

- authentication : consiste à déterminer si l'utilisateur ou l'équipement est bien celui qu'il prétend être, cela se fait grâce à une authentification nom d'utilisateur/ mot de passe, ou grâce à un certificat,
- authorization : consiste à déterminer les droits de l'utilisateur sur les différentes ressources,
- accounting : compte permet de garder des informations sur l'utilisation des ressources par l'utilisateur.

Installation et mise en œuvre d'un serveur Radius

Le matériel nécessaire a été :

- 2 machines de test,
- 1 switch faisant du 802.1x,
- 3 Virtual Machines.



Les trois Virtual Machines sont des serveurs debian 6 à jour comprenant :

- 1 serveur freeradius,
- 1 serveur LDAP,
- 1 serveur SQL.

Freeradius

Freeradius est une implémentation open source du protocole Radius.

Fonctionnalités :

- Support EAP (MD5, SIM TLS TTLS, PEAP, LEAP, GTC, MSCHAPV2)
- 50 dictionnaires vendor-specific
- LDAP, MYSQL, PostgreSQL, Oracle, SAMBA
- Module PAM-radius
- Mod_auth radius pour Apache

Installation des dépendances :

apt-get install **freeradius freeradius-utils freeradius-mysql**

Le démarrage de radius se fait par la commande : service freeradius start ou freeradius -X

La dernière permet de démarrer en mode debug. Mais dans ce cas, il n'y aura aucun log d'enregistré.

Les fichiers de configuration se situent dans /etc/freeradius/

Les fichiers principaux sont : - radiusd.conf,
- Eap.conf,
- clients.conf,
- users.

Configurations particulières : - sql.conf,
- /modules/ldap.

Gestion des certificats : /certs.

Configurations des autorisations : - /sites-enabled/default,
- /sites-enabled/inner-tunnel.

Détail des fichiers de configurations :

Radiusd.conf est le fichier de configuration général de freeradius.

```
# listen: Make the server listen on a particular IP address, and send
# replies out from that address. This directive is most useful for
# hosts with multiple IP addresses on one interface.
#
# If you want the server to listen on additional addresses, or on
# additionnal ports, you can use multiple "listen" sections.
#
# Each section make the server listen for only one type of packet,
# therefore authentication and accounting have to be configured in
# different sections.
#
# The server ignore all "listen" section if you are using '-i' and '-p'
# on the command line.
#
listen {
    # IP address on which to listen.
    # Allowed values are:
    #     dotted quad (1.2.3.4)
    #     hostname   (radius.example.com)
    #     wildcard   (*)
    ipaddr = *

    # OR, you can use an IPv6 address, but not both
    # at the same time.
#   ipv6addr = ::      # any.  ::1 == localhost

    # Port on which to listen.
    # Allowed values are:
    #     integer port number (1812)
    #     0 means "use /etc/services for the proper port"
    port = 0

    # Type of packets to listen for.
    # Allowed values are:
    #     auth      listen for authentication packets
    #     acct      listen for accounting packets
    #
    type = auth

    # Some systems support binding to an interface, in addition
    # to the IP address. This feature isn't strictly necessary,
    # but for sites with many IP addresses on one interface,
    # it's useful to say "listen on all addresses for eth0".
    #
    # If your system does not support this feature, you will
    # get an error if you try to use it.
    #
#   interface = eth0

    # Per-socket lists of clients. This is a very useful feature.
    #
    # The name here is a reference to a section elsewhere in
    # radiusd.conf, or clients.conf. Having the name as
    # a reference allows multiple sockets to use the same
    # set of clients.
    #
    # If this configuration is used, then the global list of clients
    # is IGNORED for this "listen" section. Take care configuring
    # this feature, to ensure you don't accidentally disable a
    # client you need.
    #
#
```

```

        # See clients.conf for the configuration of "per_socket_clients".
        #
        clients = per_socket_clients
    }

    # This second "listen" section is for listening on the accounting
    # port, too.
    #
    listen {
        ipaddr = *
        #
        ipv6addr = ::
        port = 0
        type = acct
        #
        interface = eth0
        #
        clients = per_socket_clients
    }

```

```

# Regular expressions
#
# These items are set at configure time.  If they're set to "yes",
# then setting them to "no" turns off regular expression support.
#
# If they're set to "no" at configure time, then setting them to "yes"
# WILL NOT WORK.  It will give you an error.
#
regular_expressions      = yes
extended_expressions    = yes

```

```

#Parameters logs
log {
    destination = files
    file = ${logdir}/radius.log
    #requests = ${logdir}/radiusd-%{%{Virtual-Server}:-DEFAULT}-%Y%m%d.log
    syslog_facility = daemon
    stripped_names = no
    auth = no
    auth_badpass = yes
    auth_goodpass = yes
    #
    msg_goodpass = ""
    #
    msg_badpass = ""
}

```

```

proxy_requests = yes
$INCLUDE proxy.conf
$INCLUDE clients.conf
$INCLUDE policy.conf
$INCLUDE sites-enabled/

modules {
    $INCLUDE ${confdir}/modules/
    $INCLUDE eap.conf
    $INCLUDE sql.conf
    $INCLUDE sql/mysql/counter.conf
    #
    $INCLUDE sqlippool.conf
}

```

Clients.conf

Dans ce fichier doivent être référencés tous les clients Radius (NAS) autorisés à interroger le serveur.

```
client localhost {
    ipaddr = 127.0.0.1
    secret = testing123
    shortname = localhost
    require_message_authenticator = no
    nastype = other
}

client 192.168.1.0/24 {
    secret = testing123
    shortname = Accpeter tous le réseau 192.168.1.0
}
```

Users

Le fichier user est la base de données locales. C'est un fichier plat.

Il est constitué d'une succession "d'entrée". Chacune correspondant à un utilisateur ou machine.

Le fichier est parcouru séquentiellement du haut vers le bas.

```
# Config permettant à une machine de s'identifier sans login/mdp (ex : imprimante)
#"90fba6e55a8d" Cleartext-Password := "90fba6e55a8d"
#     Tunnel-Type = VLAN,
#     Tunnel-Medium-Type = IEEE-802,
#     Tunnel-Private-Group-ID = 15
```

```
# Utilisateur locale
"max5" Auth-Type := EAP, Cleartext-Password := "sio"
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-ID = 14

# Ajout de l'unité organisationnelle du LDAP
DEFAULT Ldap-Group := "nom"
    Service-Type = Framed-User,
    Tunnel-Type = VLAN,
    Tunnel-Medium-Type = IEEE-802,
    Tunnel-Private-Group-ID = 16

DEFAULT LDAP-Group != "nom", Auth-Type := Accept
```

Auth-Type: attribut spécial permettant de spécifier le type d'authentification à appliquer à une entrée.

- Reject permet de refuser inconditionnellement une connexion.
- Accept permet d'accepter inconditionnellement une connexion.

Les opérateurs :

- Attribute **==** valeur (*check-item*)
Match si l'attribut est présent et est égal à cette valeur.
- Attribute **!=** valeur (*check-item*)
Match si l'attribut est présent et n'est pas égal à cette valeur.
- Attribute **>** valeur, **>=**, **<**, **<=** (*check-item*)
Match si l'attribut est présent et est > ou >= ou < ou <= à cette valeur.
- Attribute **=~** expression (*check-item*)
Match si l'attribut match l'expression régulière...
- Attribute **!~** expression (*check-item*)
Match si l'attribut ne match pas l'expression régulière.
- Attribute ***=** valeur (*check-item*)
Match si l'attribut est présent dans la requête.
La valeur n'a pas d'importance.
- Attribute **!=** valeur (*check-item*)
Match si l'attribut n'est pas présent dans la requête.
La valeur n'a pas d'importance.
- Attribute **=** valeur (*reply-item*)
Ajoute l'attribut à la liste des reply-items .
- Attribute **:=** valeur (*check-item/reply-item*)
Comme check-item, match toujours et remplace ou ajoute l'attribut aux configuration-items.
Comme reply-item ajoute l'attribut à la liste des reply-items.
- Attribute **+=** valeur (*check-item/reply-item*)
Comme check-item match toujours et rajoute l'attribut au request-item.
Comme reply-item rajoute l'attribut au request-item.

```
Tunnel-Type = VLAN,  
Tunnel-Medium-Type = IEEE-802,  
Tunnel-Private-Group-ID = 16
```

La signification des attributs RADIUS rajoutés pour chaque utilisateur est :

- **Tunnel-Type** positionné à la valeur 13 indique que l'on a un VLAN,
- **Tunnel-Medium-Type** positionné à la valeur 6 indique que la couche physique est de type 802,
- **Tunnel-Private-Group-Id** prend comme valeur du numéro du vlan auquel appartiendra l'utilisateur en question.

Sql.conf

Ce fichier permet de se connecter à la base de données locales ou distante.

```
sql {
    database = "mysql"
    driver = "rlm_sql_${database}"

    # L'adresse IP du serveur
    server = "192.168.1.31"
    # Login permettant de se connecter à la base de donnée
    login = "root"
    # Mot de passe
    password = "sio"

    radius_db = "radius"

    acct_table1 = "radacct"
    acct_table2 = "radacct"

    postauth_table = "radpostauth"

    authcheck_table = "radcheck"
    authreply_table = "radreply"

    groupcheck_table = "radgroupcheck"
    groupreply_table = "radgroupreply"

    usergroup_table = "radusergroup"

    deletestalesessions = yes

    sqltrace = yes
    sqltracefile = ${logdir}/sqltrace.sql

    num_sql_socks = 5

    connect_failure_retry_delay = 60

    lifetime = 0

    max_queries = 0

    readclients = yes
    nas_table = "nas"

    $INCLUDE sql/${database}/dialup.conf
}
```

Eap.conf

```
eap {
    default_eap_type = ttls
    timer_expire     = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no
    max_sessions = 4096

    md5 {
    }

    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        pem_file_type = yes
        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
        CA_path = ${cadir}
        cipher_list = "DEFAULT"
        make_cert_command = "${certdir}/bootstrap"
        cache {
            enable = no
            max_entries = 255
        }
        verify {
        }
    }

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

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

    mschapv2 {
    }
}
```

Module Ldap

```
ldap {
    # L'adresse IP du serveur
    server = "192.168.1.32"
    # DN de connexion
    identity = "cn=admin,dc=ldap,dc=loc"
    password = sio
    basedn = "dc=ldap,dc=loc"
```

Default/Inner-tunnel

```
authorize {
    pap
    preprocess
    chap
    mschap
    files
    digest
    suffix
    sql
    ldap
    eap {
        ok = return
    }
    expiration
    logintime
}
```

Authorization is a process of obtaining information about the user from external source (file, database or LDAP), and checking that the information in request is enough to authenticate user.

Authorization modules deal with data sources, so ldap, sql, files, passwd are authorization modules.

```
authenticate {
    Auth-Type PAP {
        pap
    }
    Auth-Type CHAP {
        chap
    }
    Auth-Type MS-CHAP {
        mschap
    }
    Auth-Type LDAP {
        ldap
    }
    eap
    digest
    unix
    files
}
```

Authentication is simply a process of comparing user's credentials in request with credentials stored in database.

Authentication usually deals with password encryption. PAP, CHAP, MS-CHAP are authentication modules. Few modules act as both authorization and authentication. For example, the MSCHAP module is normally authentication one, but it may be used during authorization to verify that request contains MS-CHAP related attribute and only in this case perform MS-CHAP based authentication. LDAP is normally an authorization module, but it may be used for authentication (In this case FreeRADIUS will authenticate user in case he can connect to LDAP server with his account). SQL is only an authorization module, as dial-in users are not normally given passwords to access an SQL server.

Création du serveur LDAP :

Installer les 3 paquets nécessaires :

```
apt-get install openldap-utils  
apt-get install phpldapadmin  
apt-get install slapd
```

Faite un : **dpkg-reconfigure slapd**

- 1°) Voulez-vous omettre la configuration d'OpenLDAP ? **Non**
- 2°) Nom de domaine ? **ldap.loc** (l'extension est obligatoire)
- 3°) Nom d'identité (organisation) ? **Nom de l'organisation**
- 4°) Module de base de données à utiliser : **HDB**
- 5°) Faut-il supprimer la base de données à la purge du paquet ? **Oui**
- 6°) Faut-il déplacer l'ancienne base de données ? **Oui**
- 7°) Faut-il autoriser le protocole LDAPv2 ? **Non**

Puis paramétrer phpldapadmin en fonction de la nouvelle configuration.

Nano /etc/phpldapadmin/config.php

```
$servers->setValue('server','name','Le nom de l'annuaire');  
$servers->setValue('server','host','127.0.0.1'); Dans mon cas, le serveur LDAP est en locale  
sur la machine  
$servers->setValue('server','base',array('dc=ldap,dc=loc')); Se référer à la question 2
```

Enfin dans le navigateur, il faut rentrer l'adresse IP du serveur suivi de /phpldapadmin.

Exemple : <http://192.168.1.32/phpldapadmin>

Création du serveur MYSQL :

```
apt-get install mysql-server
apt-get install mysql-client
apt-get install apache2
apt-get install phpmyadmin
```

En fonction des distributions, le lien symbolique de phpmyadmin n'est pas fait automatiquement dans /var/www.

Dans ce cas : ln -s /usr/share/phpmyadmin /var/www/phpmyadmin

Il faut installer freeradius avec l'utilitaire mysql pour copier certains fichiers.

```
apt-get install freeradius-mysql
```

Création de la base de données

```
echo "create database radius;" | mysql -u root -p
```

Donner tous les droits à l'utilisateur radius

```
echo "grant all on radius.* to radius@%' identified by 'sio'; flush privileges;" | mysql -u root -p
```

Copier les fichiers nécessaires

```
mysql -uroot -p radius < /etc/freeradius/sql/mysql/schema.sql
```

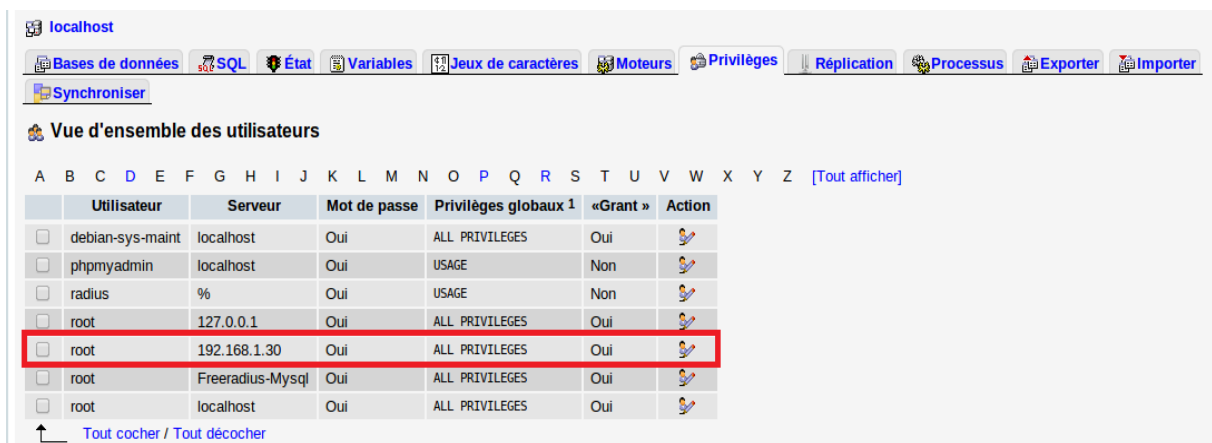
```
mysql -uroot -p radius < /etc/freeradius/sql/mysql/nas.sql
```

Pour pouvoir accéder à distance à un serveur mysql :

Sur la machine serveur mysql, modifier le fichier : /etc/mysql/my.cnf

Puis commenter la ligne : **bind-address = 127.0.0.1**

Rajouter un utilisateur avec **tous les privilèges** avec comme ip de serveur celui du freeradius. Dans notre cas, l'adresse IP est 192.168.1.30.



	Utilisateur	Serveur	Mot de passe	Privilèges globaux 1	«Grant»	Action
<input type="checkbox"/>	debian-sys-maint	localhost	Oui	ALL PRIVILEGES	Oui	
<input type="checkbox"/>	phpmyadmin	localhost	Oui	USAGE	Non	
<input type="checkbox"/>	radius	%	Oui	USAGE	Non	
<input type="checkbox"/>	root	127.0.0.1	Oui	ALL PRIVILEGES	Oui	
<input type="checkbox"/>	root	192.168.1.30	Oui	ALL PRIVILEGES	Oui	
<input type="checkbox"/>	root	Freeradius-Mysql	Oui	ALL PRIVILEGES	Oui	
<input type="checkbox"/>	root	localhost	Oui	ALL PRIVILEGES	Oui	

Script permettant d'ajouter un utilisateur.

La variable \$1 est la même pour le login et mot de passe car la base de données sert juste pour autoriser les adresses MAC.

```
#!/bin/bash
echo "INSERT INTO radcheck(Username,Attribute,op,Value) VALUES ('$1','Cleartext-Password','=','$1');" | mysql -u root --password=sio radius
```

Pour tester la bonne configuration des fichiers et des utilisateurs, il existe une commande : radtest

A adapter selon ces besoins.

Exemple : radtest login passwd localhost 0 testing123

Login = le nom utilisateur

Passwd = le mot de passe de l'utilisateur

0 = le port nas

Testing123 = la clé partagée

Même si les serveurs sql ou ldap sont distants, il faut rentrer l'adresse IP du serveur radius.

```
radtest xp sio localhost 0 testing123
Sending Access-Request of id 169 to 127.0.0.1 port 1812
  User-Name = "xp"
  User-Password = "sio"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812, id=169, length=42
  Service-Type = Framed-User
  Tunnel-Type:0 = VLAN
  Tunnel-Medium-Type:0 = IEEE-802
  Tunnel-Private-Group-Id:0 = "16"
```

Test avec un faux mot de passe :

```
radtest xp dshfsdh localhost 0 testing123
Sending Access-Request of id 20 to 127.0.0.1 port 1812
  User-Name = "xp"
  User-Password = "dshfsdh"
  NAS-IP-Address = 127.0.1.1
  NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1 port 1812, id=20, length=20
```

Le protocole utilise 4 types de paquets suffisants pour assurer toutes les transactions :

- Access-Request,
- Access-Accept,
- Access-Reject,
- Access-Challenge.

Access Request

Premier paquet envoyé par le client (NAS)

Contient l'identité de l'utilisateur qui se connecte

(username/password ou CN du certificat ou MAC adresse)

Access-Accept

Renvoyé par le serveur Radius pour accepter la requête du client après interrogation de sa base d'authentification.

Ce paquet peut contenir une liste d'attributs correspondant aux services qui sont autorisés (par exemple le vlan).

Access-reject

Emis par le serveur radius pour spécifier au client que sa requête est rejetée.

En principe, ce paquet peut être émis à tout moment pour mettre fin à une connexion, mais certains équipements ne supportent pas.

Access-challenge

Emis par le serveur Radius pour demander soit de réémettre un access-request, soit pour demander des informations complémentaires.

Configuration du switch

Commencer par configurer le AAA.

Pour ce faire, il faut d'abord activer AAA grâce à la commande :

```
aaa new-model
```

These settings create a radius server group called dynaccess.

```
aaa group server radius dynaccess  
server 192.168.1.30 auth-port 1812 acct-port 1813
```

Source from the management address interface you put in network configuration section in the acs server.

```
ip radius source-interface Vlan1
```

These settings point the switch to the appropriate acs (radius) server.

```
radius-server host 192.168.1.30 auth-port 1812 acct-port 1813  
radius-server key testing123
```

These are the AAA settings associated with the above radius server group dynaccess.

```
aaa authentication dot1x default group dynaccess  
aaa authorization config-commands  
aaa authorization network default group dynaccess  
aaa accounting dot1x default start-stop group dynaccess
```

These are the only settings required on the dynamic access MAB enabled interface.

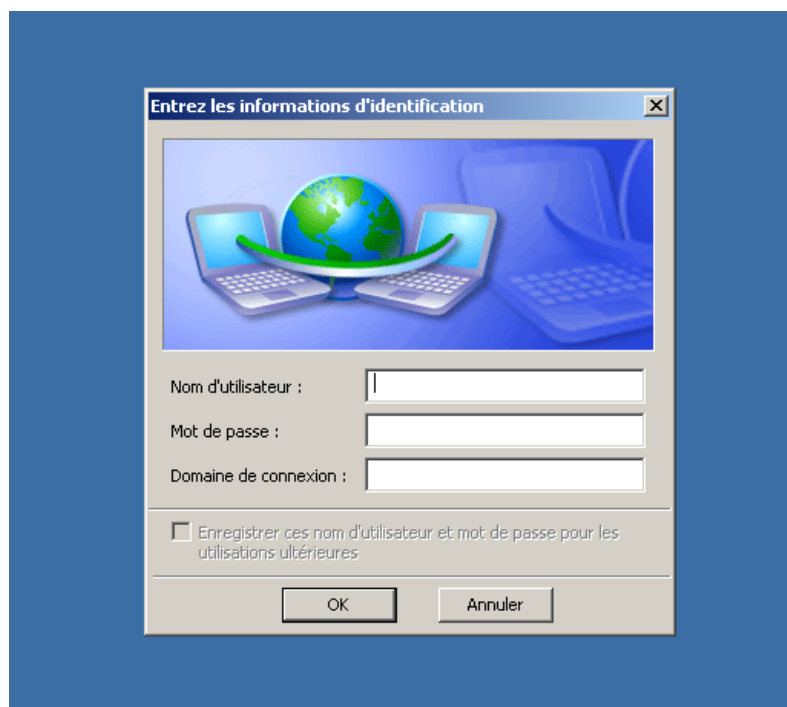
```
interface FastEthernet3/48
description MAB dynamic access enabled interface
switchport
switchport mode access
authentication port-control auto
authentication periodic
authentication timer restart 30
authentication timer reauthenticate 1200
authentication timer inactivity 600
mab
authentication event fail action authorize vlan 40
authentication event no-response action authorize vlan 30
no shut
```

Configuration d'un poste client

Vous devez avoir ouvert une session en tant qu'administrateur pour effectuer ces étapes.

Pour terminer cette procédure, vous devez d'abord activer le service de configuration automatique de réseau câblé, qui est désactivé par défaut.

1. Cliquez sur le bouton **Démarrer**, puis dans la zone de recherche, tapez **services.msc**, puis appuyez sur ENTRÉE. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.
2. Dans la boîte de dialogue Services, cliquez sur l'onglet **Standard**, puis cliquez avec le bouton droit sur **Configuration automatique de réseau câblé** et enfin sur **Démarrer**.
3. Pour ouvrir Connexions réseau, cliquez sur le bouton **Démarrer**, sur **Panneau de configuration**, sur **Réseau et Internet**, sur **Centre réseau et partage**, puis sur **Gérer les connexions réseau**.
4. Cliquez avec le bouton droit sur la connexion pour laquelle vous souhaitez activer l'authentification 802.1X, puis cliquez sur **Propriétés**. Si vous êtes invité à fournir un mot de passe administrateur ou une confirmation, fournissez le mot de passe ou la confirmation.
5. Cliquez sur l'onglet **Authentification**, puis activez la case à cocher **Activer l'authentification IEEE 802.1X**.
6. Dans la liste **Choisissez une méthode d'authentification réseau**, cliquez sur la méthode à utiliser (dans notre cas, c'est MD5-Challenge).



Si un client veut s'authentifier :

```

max@Max: ~
[sql] expand: SELECT id, username, attribute, value, op FROM radcheck WHERE username = 'xp' ORDER BY id
[sql] expand: SELECT groupname FROM radusergroup WHERE username = '%[SQL-User-Name]' ORDER BY priority -> SELECT
groupname FROM radusergroup WHERE username = 'xp' ORDER BY priority
rln_sql_mysql: query: SELECT groupname FROM radusergroup WHERE username = 'xp' ORDER BY priority
rln_sql (sql): Released sql socket id: 3
[sql] User xp not found
**[sql] returns notfound
[ldap] performing user authorization for xp
[ldap] expand: %{Stripped-User-Name} ->
[ldap] ... expanding second conditional
[ldap] expand: %{User-Name} -> xp
[ldap] expand: (uid=%{Stripped-User-Name}-%{User-Name}) -> (uid=xp)
[ldap] expand: dc=unicaen,dc=fr -> dc=unicaen,dc=fr
[ldap] ldap_get_conn: Checking Id: 0
[ldap] ldap_get_conn: Got Id: 0
[ldap] performing search in dc=unicaen,dc=fr, with filter (uid=xp)
[ldap] Added User-Password = sio in check items
[ldap] No default NMAS login sequence
[ldap] looking for check items in directory...
[ldap] userPassword -> Password-With-Header == "sio"
[ldap] looking for reply items in directory...
[ldap] user xp authorized to use remote access
[ldap] ldap_release_conn: Release Id: 0
**[ldap] returns ok
[eap] EAP packet type response id 2 length 24
[eap] No EAP Start, assuming it's an on-going EAP conversation
**[eap] returns updated
**[files] returns noop
**[expiration] returns noop
**[logintime] returns noop
Found Auth-Type = EAP
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Replacing User-Password in config items with Cleartext-Password. !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!! Please update your configuration so that the "known good" !!!
!!! clear text password is in Cleartext-Password, and not in User-Password. !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
# Executing group from file /etc/freeradius/sites-enabled/default
+- entering group authenticate [...]
[eap] Request found, released from the list
[eap] EAP/md5

```

Et que l'authentification marche, le switch le met dans le bon VLAN.

```

max@Max: ~
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
Switch#
*Mar 1 00:46:14.406: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to down
*Mar 1 00:46:15.407: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
*Mar 1 00:46:18.396: %AUTHMGR-5-START: Starting 'dot1x' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E000000B002A6F
*Mar 1 00:46:20.225: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Mar 1 00:46:24.949: %DOT1X-5-SUCCESS: Authentication successful for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID
*Mar 1 00:46:24.949: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSeF
*Mar 1 00:46:24.949: %AUTHMGR-5-VLANASSIGN: VLAN 16 assigned to Interface Gi1/0/13 AuditSessionID C0A8012E000000B002A646F
*Mar 1 00:46:25.961: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
*Mar 1 00:46:25.987: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E00001

```

VLAN Name	Status	Ports
1 default	active	Gi1/0/1, Gi1/0/2, Gi1/0/3 Gi1/0/4, Gi1/0/5, Gi1/0/6 Gi1/0/7, Gi1/0/8, Gi1/0/9 Gi1/0/10, Gi1/0/11, Gi1/0/12 Gi1/0/14, Gi1/0/15, Gi1/0/16 Gi1/0/17, Gi1/0/18, Gi1/0/19 Gi1/0/20, Gi1/0/21, Gi1/0/22 Gi1/0/23, Gi1/0/24, Gi1/0/25 Gi1/0/26, Gi1/0/27, Gi1/0/28 Gi1/0/29, Gi1/0/30, Gi1/0/31 Gi1/0/32, Gi1/0/33, Gi1/0/34 Gi1/0/35, Gi1/0/36, Gi1/0/37 Gi1/0/38, Gi1/0/39, Gi1/0/40 Gi1/0/41, Gi1/0/42, Gi1/0/43 Gi1/0/44, Gi1/0/45, Gi1/0/46 Gi1/0/47, Gi1/0/48, Gi1/0/49 Gi1/0/50, Gi1/0/51, Gi1/0/52
15 PasDeNon	active	
16 Filaire	active	Gi1/0/13
30 guest-vlan	active	

```

--More--
Aide : CTRL-A Z 9600 8N1 NOR Minicom 2.6.1 VI102 Déconnecté

```

Si l'authentification fail, il le met dans un VLAN « poubelle ».

```

max@Max: ~
*Mar 1 00:43:24.274: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dotix' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSeo
*Mar 1 00:43:42.976: %DOTIX-5-FAIL: Authentication failed for client (Unknown MAC) on Interface Gi1/0/13 AuditSessionID
*Mar 1 00:43:42.976: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'dotix' for client (Unknown MAC) on Interface Gi1/0/13 AuditSA
*Mar 1 00:43:42.976: %AUTHMGR-7-FAILOVER: Failing over from 'dotix' for client (Unknown MAC) on Interface Gi1/0/13 AuditSessionID C0A8012E0000A
*Mar 1 00:44:17.117: %AUTHMGR-5-START: Starting 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E00000900270DBA
*Mar 1 00:44:18.129: %MAB-5-FAIL: Authentication failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E00000900270DBA
*Mar 1 00:44:18.129: %AUTHMGR-7-RESULT: Authentication result 'no-response' from 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditA
*Mar 1 00:44:18.134: %AUTHMGR-7-FAILOVER: Failing over from 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E0000A
*Mar 1 00:44:18.134: %AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSesA
*Mar 1 00:44:18.134: %AUTHMGR-5-VLANASSTCN: VLAN 30 assigned to Interface Gi1/0/13 AuditSessionID C0A8012E00000900270DBA
*Mar 1 00:44:19.141: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
*Mar 1 00:44:19.172: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (Unknown MAC) on Interface Gi1/0/13 AuditSesstionID C0A8012E00000000A
Switch#
Switch#
Switch#
Switch#sh vlan
VLAN Name                Status    Ports
-----
1  default                 active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                    Gi1/0/4, Gi1/0/5, Gi1/0/6
                    Gi1/0/7, Gi1/0/8, Gi1/0/9
                    Gi1/0/10, Gi1/0/11, Gi1/0/12
                    Gi1/0/14, Gi1/0/15, Gi1/0/16
                    Gi1/0/17, Gi1/0/18, Gi1/0/19
                    Gi1/0/20, Gi1/0/21, Gi1/0/22
                    Gi1/0/23, Gi1/0/24, Gi1/0/25
                    Gi1/0/26, Gi1/0/27, Gi1/0/28
                    Gi1/0/29, Gi1/0/30, Gi1/0/31
                    Gi1/0/32, Gi1/0/33, Gi1/0/34
                    Gi1/0/35, Gi1/0/36, Gi1/0/37
                    Gi1/0/38, Gi1/0/39, Gi1/0/40
                    Gi1/0/41, Gi1/0/42, Gi1/0/43
                    Gi1/0/44, Gi1/0/45, Gi1/0/46
                    Gi1/0/47, Gi1/0/48, Gi1/0/49
                    Gi1/0/50, Gi1/0/51, Gi1/0/52
15  PasDeNom                active
16  Filaire                 active
30  quest-vlan              active    Gi1/0/13
--More--
Aide : CTRL-A Z | 9600 8N1 | NOR | Minicom 2.6.1 | VT102 | Déconnecté

```

Si le client ne s'authentifie pas, il y a un certain timeout.

```

max@Max: ~
*Mar 1 00:44:58.263: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
*Mar 1 00:44:58.919: %AUTHMGR-5-START: Starting 'dotix' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E000000A00292A
*Mar 1 00:45:00.712: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Mar 1 00:45:03.747: %DOTIX-5-FAIL: Authentication failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID
*Mar 1 00:45:03.747: %AUTHMGR-7-RESULT: Authentication result 'fail' from 'dotix' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessiA
*Mar 1 00:45:22.271: %DOTIX-5-FAIL: Authentication failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID
*Mar 1 00:45:22.271: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dotix' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSeA
*Mar 1 00:45:40.778: %DOTIX-5-FAIL: Authentication failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID
*Mar 1 00:45:40.778: %AUTHMGR-7-RESULT: Authentication result 'timeout' from 'dotix' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSeA
*Mar 1 00:45:40.778: %AUTHMGR-5-VLANASSIGN: VLAN 40 assigned to Interface Gi1/0/13 AuditSessionID C0A8012E000000A00292DDA
*Mar 1 00:45:41.785: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
*Mar 1 00:45:41.811: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E0000A
*Mar 1 00:45:41.811: %DOTIX-5-RESULT_OVERRIDE: Authentication result overridden for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSesstionL
VLAN Name                Status    Ports
-----
1  default                 active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                    Gi1/0/4, Gi1/0/5, Gi1/0/6
                    Gi1/0/7, Gi1/0/8, Gi1/0/9
                    Gi1/0/10, Gi1/0/11, Gi1/0/12
                    Gi1/0/14, Gi1/0/15, Gi1/0/16
                    Gi1/0/17, Gi1/0/18, Gi1/0/19
                    Gi1/0/20, Gi1/0/21, Gi1/0/22
                    Gi1/0/23, Gi1/0/24, Gi1/0/25
                    Gi1/0/26, Gi1/0/27, Gi1/0/28
                    Gi1/0/29, Gi1/0/30, Gi1/0/31
                    Gi1/0/32, Gi1/0/33, Gi1/0/34
                    Gi1/0/35, Gi1/0/36, Gi1/0/37
                    Gi1/0/38, Gi1/0/39, Gi1/0/40
                    Gi1/0/41, Gi1/0/42, Gi1/0/43
                    Gi1/0/44, Gi1/0/45, Gi1/0/46
                    Gi1/0/47, Gi1/0/48, Gi1/0/49
                    Gi1/0/50, Gi1/0/51, Gi1/0/52
15  PasDeNom                active
16  Filaire                 active
30  guest-vlan              active
VLAN Name                Status    Ports
-----
40  auth-fail               active    Gi1/0/13
1002 fddi-default           act/unsup

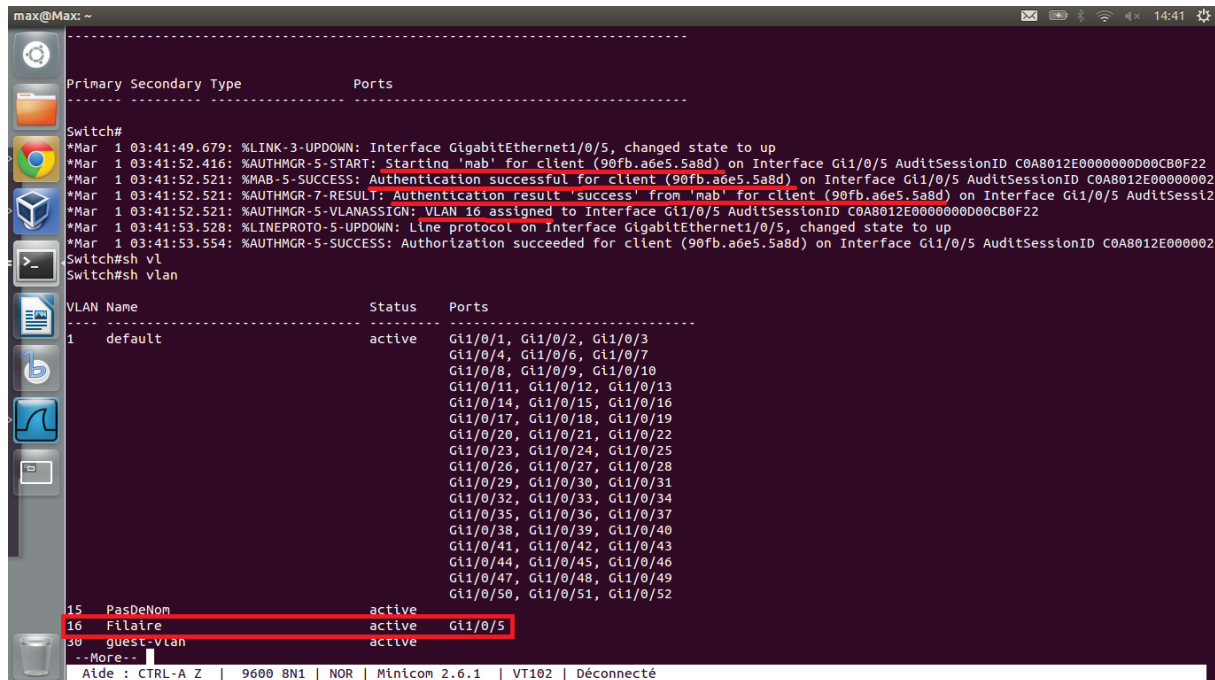
```

Authentification par MAB (Mac Authentication Bypass).

Cette option permet l'authentification des clients n'ayant pas de configuration eap (imprimante, ...).

Au bout d'une minute (par défaut), si le switch ne reçoit pas de demande d'authentification eap, il utilise l'adresse MAC du client pour l'authentification.

Cette adresse MAC a été précédemment rentrée dans la base de données sql .



```
max@Max: ~
-----
Primary Secondary Type          Ports
-----
Switch#
*Mar 1 03:41:49.679: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to up
*Mar 1 03:41:52.416: %AUTHMGR-5-START: Starting 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E00000000C0B0F22
*Mar 1 03:41:52.521: %MAB-5-SUCCESS: Authentication successful for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E000000002
*Mar 1 03:41:52.521: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessI2
*Mar 1 03:41:52.521: %AUTHMGR-5-VLANASSIGN: VLAN 16 assigned to Interface Gi1/0/5 AuditSessionID C0A8012E00000000D00CB0F22
*Mar 1 03:41:53.528: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/5, changed state to up
*Mar 1 03:41:53.554: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E0000002
Switch#sh vl
Switch#sh vlan

VLAN Name                Status    Ports
-----
1    default                active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                           Gi1/0/4, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48, Gi1/0/49
                                           Gi1/0/50, Gi1/0/51, Gi1/0/52
15   PasDeNom                active
16   Filaire                  active    Gi1/0/5
30   guest-vlan               active
--More--
Aide : CTRL-A Z | 9600 8N1 | NOR | Minicom 2.6.1 | VT102 | Déconnecté
```

Pour plus de sécurité, il serait préférable d'avoir un **VLAN spécial pour l'authentification MAB**. Car c'est assez simple de voler puis changer une adresse MAC.

Si le serveur radius ne répond plus, il est déclaré dans le switch.

```
*Mar 1 01:07:07.113: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan16, changed state to down
*Mar 1 01:07:07.302: %AUTHMGR-5-START: Starting 'dot1x' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E00000000C003D
*Mar 1 01:07:08.088: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to down
*Mar 1 01:07:12.409: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.252:1812,1813 is not responding.
*Mar 1 01:07:12.409: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.252:1812,1813 is being marked alive.
*Mar 1 01:07:46.042: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.252:1812,1813 is not responding.
*Mar 1 01:07:46.042: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.252:1812,1813 is being marked alive.
*Mar 1 01:07:46.042: %DOT1X-5-FAIL: Authentication failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID
*Mar 1 01:07:46.042: %AUTHMGR-7-RESULT: Authentication result 'server dead' from 'dot1x' for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 Au
*Mar 1 01:07:46.042: %AUTHMGR-5-FAIL: Authorization failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/13 AuditSessionID C0A8012E00000000C0
```


Si le radius veut mettre un client dans un vlan mais que ce dernier n'est pas créé, il y aura une erreur.

```
Switch#
*Mar 1 03:40:05.745: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/7, changed state to down
*Mar 1 03:40:06.746: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/7, changed state to down
*Mar 1 03:40:07.375: %AUTHMGR-5-START: Starting 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E0000000C00C98673
*Mar 1 03:40:07.490: %MAB-5-SUCCESS: Authentication successful for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E0000000C00C98673
*Mar 1 03:40:07.490: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E0000000C00C98673
*Mar 1 03:40:07.490: %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN 16 to 802.1x port GigabitEthernet1/0/5
*Mar 1 03:40:07.490: %AUTHMGR-5-FAIL: Authorization failed for client (90fb.a6e5.5a8d) on Interface Gi1/0/5 AuditSessionID C0A8012E0000000C00C98673
*Mar 1 03:40:09.152: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/5, changed state to up
```

Remerciements

Tout au long de ma formation au sein de l'IUT de Caen, j'ai eu la chance d'être épaulé par Monsieur Sylvain FARGEAS pour avoir répondu à mes questions.

Etant pleinement satisfait de cette expérience professionnelle, je tiens à exprimer ma sincère reconnaissance à Monsieur Adrien CORBIERE, chef du service informatique, pour m'avoir permis d'effectuer cette formation de 5 semaines.

J'ai été très touché par l'invitation au restaurant la dernière journée.

Enfin, je remercie l'ensemble de ses collaborateurs pour leur bonne humeur.

Conclusion

J'ai apprécié ce stage où j'ai été bien accueilli, j'ai su m'intégrer vite et le personnel me trouvait agréable.

Je pense que cette expérience en entreprise m'a offert une bonne préparation à mon insertion professionnelle car elle fut pour moi une expérience enrichissante et complète. Ceci me détermine encore plus dans la poursuite de mes études.

Je garderai un très bon souvenir de ce séjour à l'IUT de Caen où Adrien et Sylvain m'ont accordé un peu de leur temps et ont bien voulu me transmettre une partie de leur savoir.

Annexes

Mon espace de travail



VM Freeradius : <https://docs.google.com/file/d/0B81X-NDKTP0jVFV5Z1V0OC10Z2c/edit?usp=sharing>

VM LDAP : <https://docs.google.com/file/d/0B81X-NDKTP0jc3ZzOHNIYVFIZFE/edit?usp=sharing>

VM Mysql : <https://docs.google.com/file/d/0B81X-NDKTP0jZkRhcfFfaTZVMWM/edit?usp=sharing>

Config Switch : <https://docs.google.com/file/d/0B81X-NDKTP0jTWRxT3B6NkVFZGM/edit?usp=sharing>

Config freeradius : <https://docs.google.com/file/d/0B81X-NDKTP0jY0tWIk3T3JZY1E/edit?usp=sharing>