2ème année 2008-2009

# Le protocole RADIUS

Décembre 2008

**Objectifs**

**Objectifs :** Le but de cette séance est de montrer comment un protocole d'authentification peut être utilisé afin de permettre ou interdire à un utilisateur l'accès à un réseau, que ce soit un réseau local, type Ethernet, ou un réseau d'accès à un fournisseur.

Le protocole RADIUS (*Remote Authentication Dial-In User Service* est un protocole d'AAA (*Authentication, Authorization and Accounting* : identification, autorisation et comptabilité).

La figure 1 montre l'utilisation du protocole RADIUS.

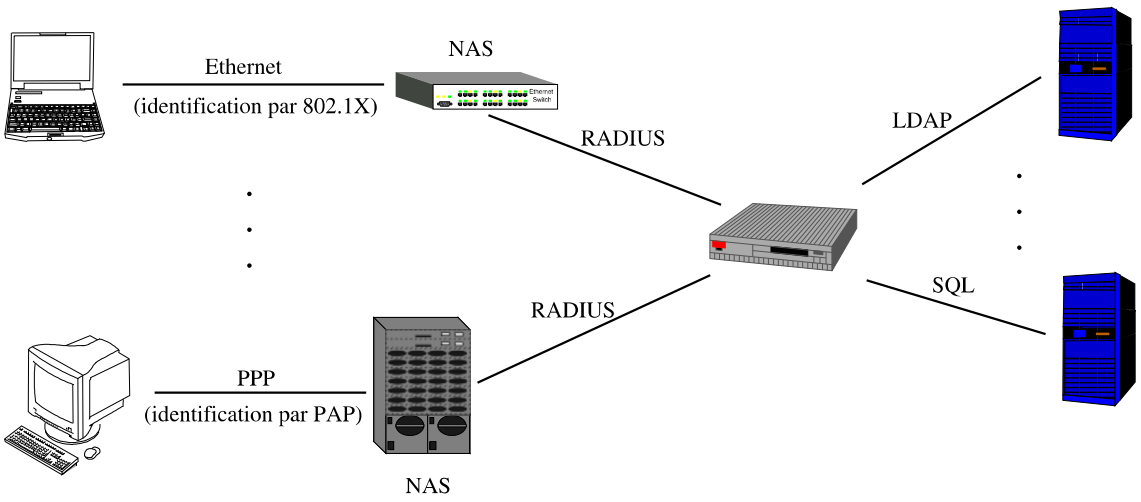


FIG. 1 – Utilisation du protocole RADIUS.

Le protocole RADIUS est utilisé entre un client appelé *authenticator* et un serveur. Le client est par exemple un NAS (*Network Access Server* : un serveur d'accès au réseau) qui doit identifier une entité (appelé *supplicant* désirant accéder au réseau. Les mécanismes d'identification mis en place entre cette entité et le NAS dépendent des protocoles par lesquels ils communiquent, comme nous allons le voir.

Le protocole RADIUS permet donc un accès uniforme à un serveur d'AAA.

Comme l'illustre la figure 1, les informations permettant l'identification pourront à leur tour être stockées sur des serveurs de natures diverses accédés par des protocoles spécifiques.

Une séquence d'identification pourra donc se dérouler de la façon suivante

1. Le NAS découvre la présence d'un client à identifier afin de lui autoriser, ou non, l'accès au réseau.
2. Le NAS demande au client de s'identifier.

3. Le client fournit son identifiant au NAS.
4. Le NAS interroge le serveur d'AAA au travers du protocole RADIUS afin d'identifier (ou autoriser, ou comptabiliser) le client.
5. Le serveur RADIUS consulte la base de données hébergeant ces informations, par exemple au travers du protocole d'annuaire LDAP.
6. Le NAS peut alors authentifier le client grâce à la réponse obtenue du serveur RADIUS.

Nous utiliserons ici RADIUS à des fins d'identification dans deux contextes différents
– l'utilisation d'un réseau local au travers d'un équipement de niveau deux (un commutateur Ethernet) ;
– l'accès à un réseau de FAI (ou d'entreprise) au travers du protocole PPP.

Avant de procéder à chacune de ces deux manipulations, nous devrons mettre en place leur dénominateur commun : un serveur RADIUS.

# 1 Mise en place d'un serveur RADIUS

Dans les deux cas, nous utiliserons un serveur RADIUS disponible sur le système Linux, nommé *FreeRadius*.

Le serveur *FreeRadius* est configuré par un ensemble de fichiers situés dans le répertoire `/etc/freeradius`. Le fichier de configuration principal est le fichier `radiusd.conf`. C'est ce fichier qui définit les différents types d'authentification, et les paramètres associés à chacun d'entre eux. Certains type d'authentification peuvent utiliser des sources distantes au travers d'autres protocoles tels que LDAP.

Le fichier `users` permet de définir localement des utilisateurs ainsi que les méthodes d'identification qui leur est appliquée. C'est ici la base que nous utiliserons à des fins de simplification.

Le fichier `clients.conf` permet quant à lui de décrire les clients (les NAS) susceptibles de communiquer avec le serveur. Chaque méthode d'identification pouvant être utilisée entre le NAS et le serveur RADIUS sera à son tour définie dans un fichier spécifique, tel que `eap.conf` pour le protcole EAP.

Nous utiliserons justement ici un EAP-MD5 pour l'identification sur un réseau local. En se fondant sur une identification simple, on aura par exemple les lignes suivantes dans le fichier `users`

```
lan     Auth-Type :=EAP , User-Password == "lan308&9"
        Reply-Message = "Hello, %u"

ppp     Auth-Type :=Local , User-Password == "ppp308&9"
        Reply-Message = "Hello, %u"
```

Voici enfin comment un client tel que le commutateur Cisco pourra être configuré dans le `clients.conf`

```
client 192.168.198.8 {
   secret = cisco
   shortname = switch
}
```

### 1.1 Configuration des clients

Les clients RADIUS sont configurés par des fichiers situés dans le répertoire `/etc/radiusclient` et nommé par exemple `radiusclient.conf` qui contient en particulier une ou plusieurs lignes de la forme

```
authserver nomduserveur
```

et

```
acctserver nomduserveur
```

Le fichier `servers` contient quant à lui des couples :

```
serveur clef-partagée
```

permettant aux clients de s'identifier auprès des serveurs.

Nous n'utiliserons pas de client RADIUS lors de cette séance, aussi cette configuration est ici inutile. Elle serait nécessaire pour une utilisation de RADIUS dans le cadre de PPP ou de l'authentifcation PAM sur le poste Linux.

▷ **Exercice 1 : Mise en place d'un serveur** RADIUS

*Configurez un serveur* RADIUS *de sorte à permettre l'authentification de deux clients, nommés* PPP *et* LAN*, par exemple.*

*On utilisera des fichiers locaux au serveur pour stocker les informations sur les clients.* ■

## 2 Identification pour l'accès à un LAN

Le protocole RADIUS peut donc également être utilisé afin de contrôler l'accès à un réseau local, qu'il soit sans fil ou de type Ethernet. La norme 802.1X décrit les mécanismes d'identification permettant l'acceptation ou le refus d'un client (*supplicant*) par un élément de réseau (commutateur Ethernet, point d'accès Wifi, ...).

Ce dernier utilisera le protocole RADIUS pour réaliser effectivement cette identification. Il devra donc être en mesure de contacter un serveur RADIUS.

La configuration d'un commutateur *Cisco* en temps que client RADIUS se fait de la façon suivante

```
cisco$ enable
cisco# conf t
cisco# aaa new-model
cisco# aaa authentication dot1x default group radius
cisco# aaa authentication login default line    pour un login/mdp local en telnet)
cisco# aaa authentication enable default enable          pour un enable/mdp local)
cisco# radius-server host 192.168.198.X port 1812 1813      ports auth acc sur 3750)
cisco# radius server key <le-secret>
cisco# dot1x system-auth-control                          (sur le 3750 uniquement)
cisco# ctrl z
```

La configuration de chaque port pourra alors se faire de la façon suivante

```
cisco$ enable
cisco# conf t
cisco# int FastEthernet0/X
cisco# switchport mode access
cisco# dot1x port-control auto
cisco# ctrl Z
```

On pourra observer la configuration à l'aide des deux commandes suivantes

```
cisco# show radius
cisco# show dot1x
```

▷ **Exercice 2 : Configuration d'un commutateur Ethernet**

*Configurez le commutateur Ethernet de sorte à conditionner l'utilisation de certains ports à une identification préalable par* EAP.

*Vérifiez en essayant d'utiliser ce port grâce à un poste non authentifié.* ■

Le dialogue entre le supplicant et le point d'accès se fait au travers du protocole EAP (*Enhanced Authentication Protocol*).

Un client EAP sur poste Linux est `wpa_supplicant`. On le lancera par exemple de la façon suivante

```
# wpa_supplicant -c/etc/wpa_suppplicant.conf -Dwired -ieth1 -d
```

Ce démon est donc configuré ici par le fichier `/etc/wpa_suppplicant.conf`. On y configurera par exemple le type et la méthode d'authentification.

Un exemple de fichier de configuration vous est fourni dans `/home/admin`.

▷ **Exercice 3 : Accès authentifié à un** LAN

*Configurez un poste de sorte à lui permettre de s'identifier auprès du commutateur Ethernet.* ■

▷ **Exercice 4 : Observation des échanges**

*Utilisez* `ethereal` *pour observer les échanges sur les différents liens et mettre ainsi en évidence les différentes étapes.* ■

## 2.1 Ajout d'informations

Il est également possible d'ajouter des informations complémentaires dans les dialogues RADIUS. Voyons par exemple comment le VLAN dans lequel une machine doit être placé peut être acheminé dans un message RADIUS.

Le serveur RADIUS doit bien entendu être modifié en ce sens. Pour cela, le fichier `users` doit conenir les lignes suivantes

```
Tunnel-Type = VLAN
Tunnel-Medium-Type = IEEE-802
Tunnel-Private-Group-ID = 4832
```

Le switch Ethernet doit, lui aussi, être configuré de sorte à utiliser cette information :

```
cisco$ enable
cisco# conf t
```

`cisco#` **aaa authorization network default group radius**

Le configuration de chaque port est inchangée par rapport à une autorisation “simple”, c’est-à-dire sans configuration du numéro de VLAN.

▷ **Exercice 5 : Ajout du numéro de** VLAN

*Configurez vos équipements de sorte à ce que le numéro de* VLAN *soit fourni par* RADIUS. *Vérifiez le fonctionnement et observez le trafic engendré.* ■