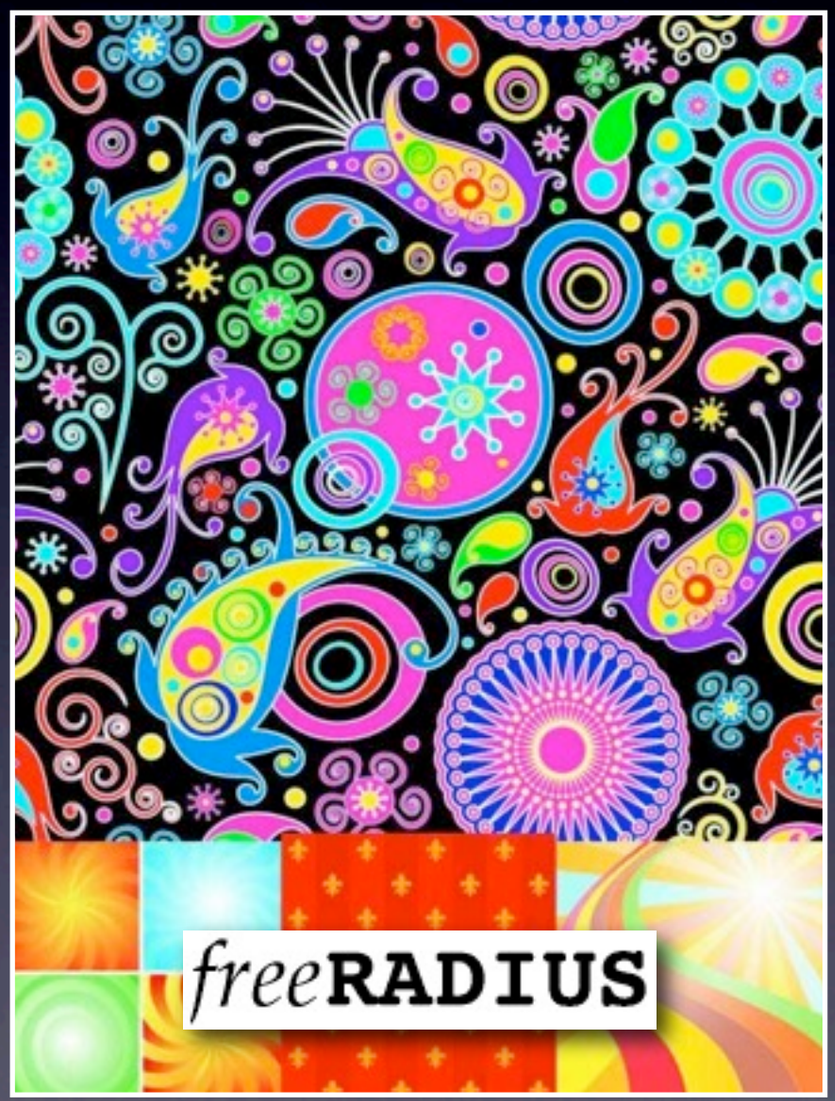
freeRADIUS

Serveur RADIUS libre, performant et modulaire

mais pas vraiment simple

Aurélien Geron, Wifirst, 7 janvier 2011

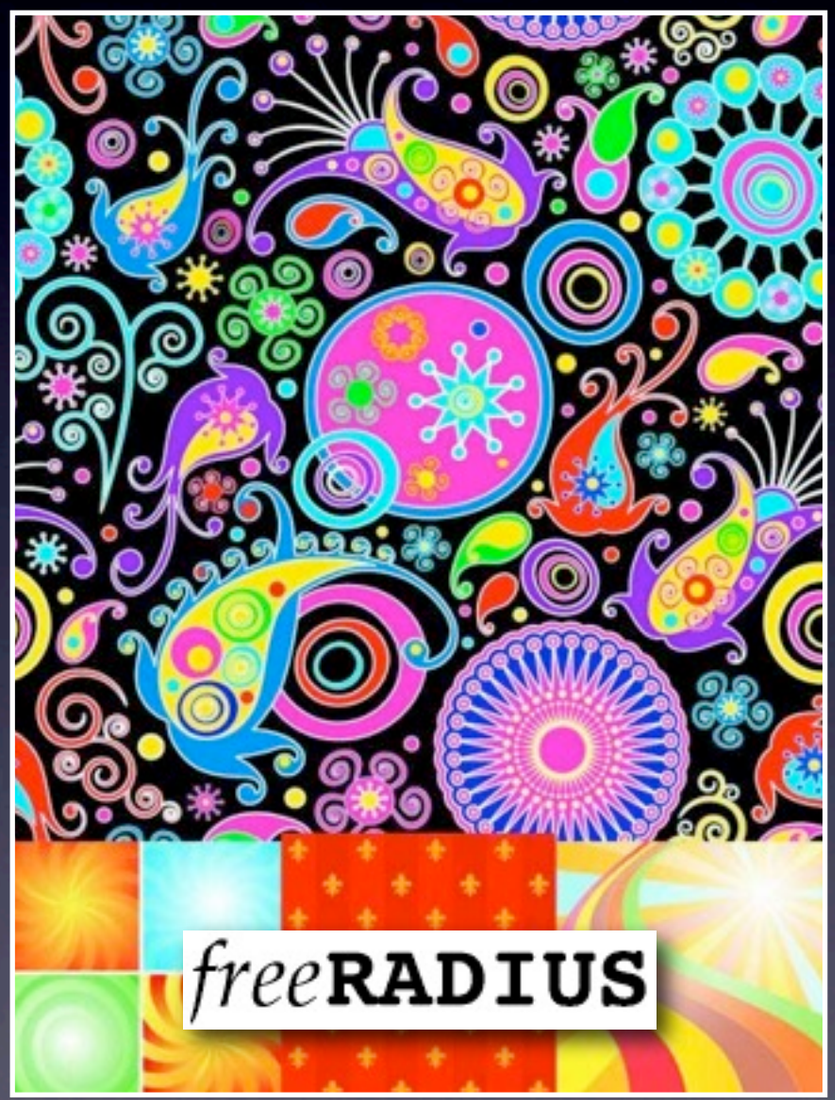
freeRADIUS c'est...



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

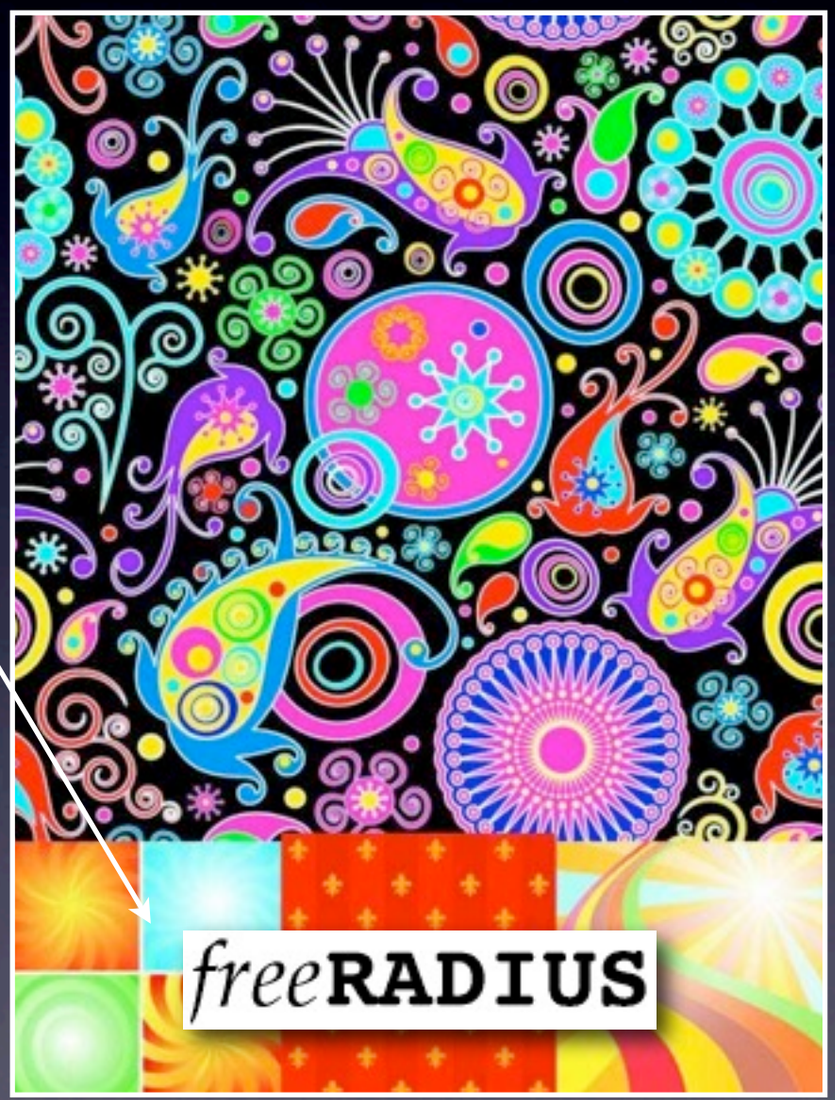
- Plusieurs protocoles : RADIUS, EAP...



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

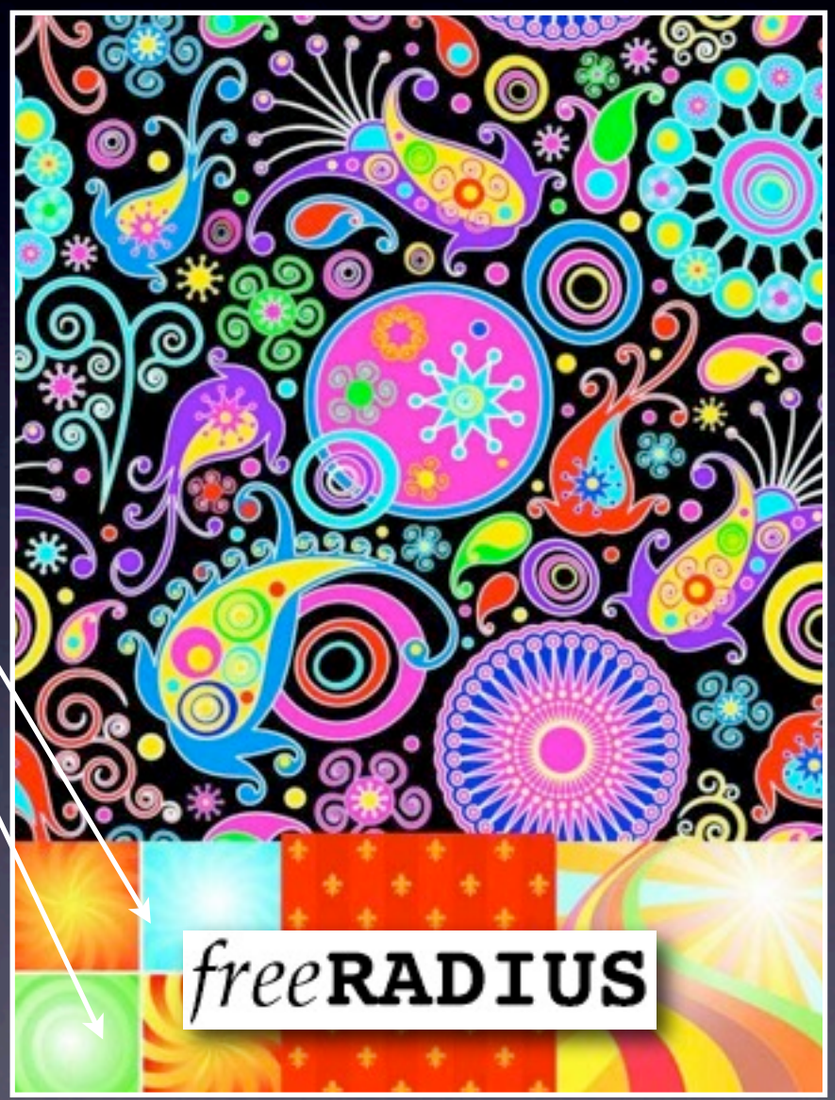
- Plusieurs protocoles : RADIUS, EAP...



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

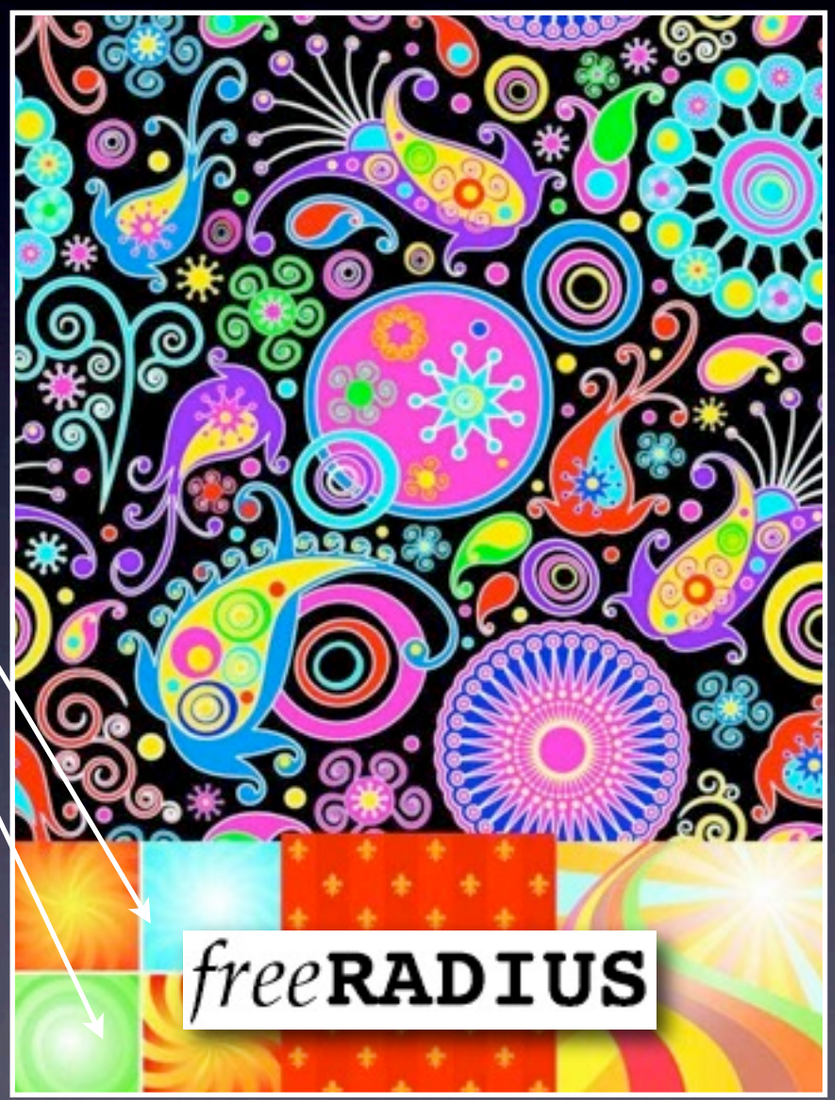
- Plusieurs protocoles : RADIUS, EAP...



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

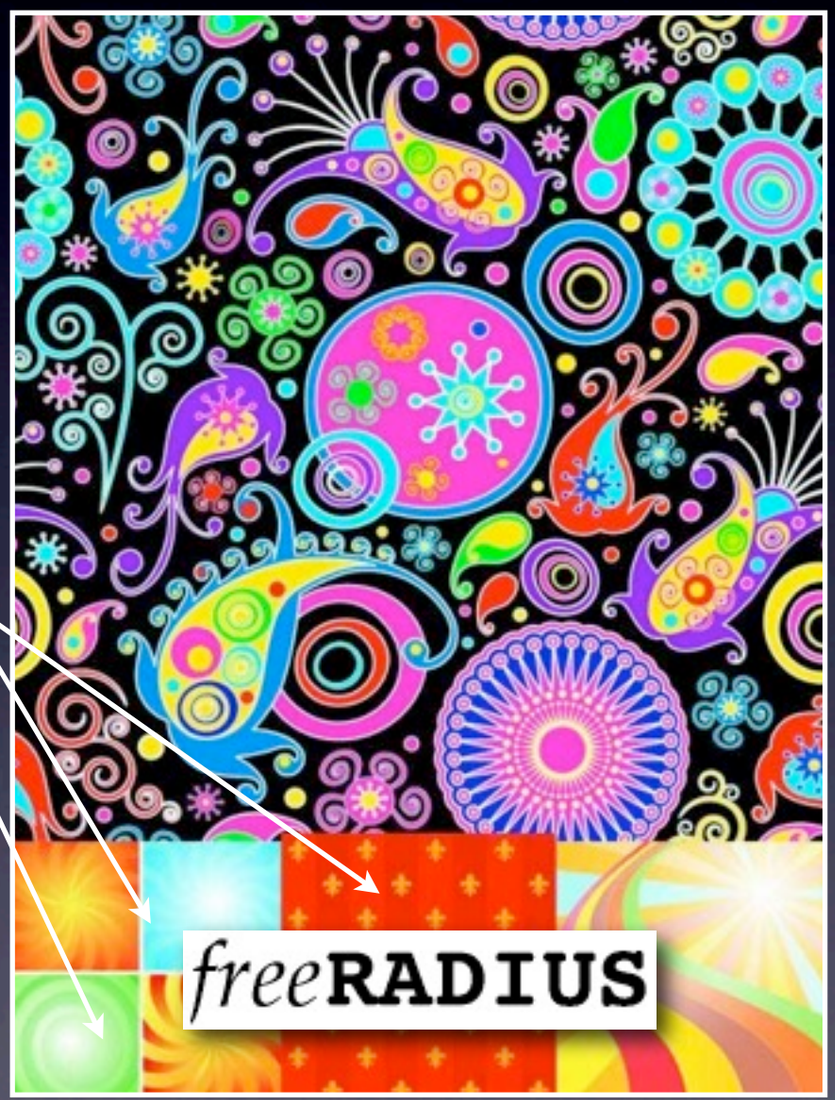
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

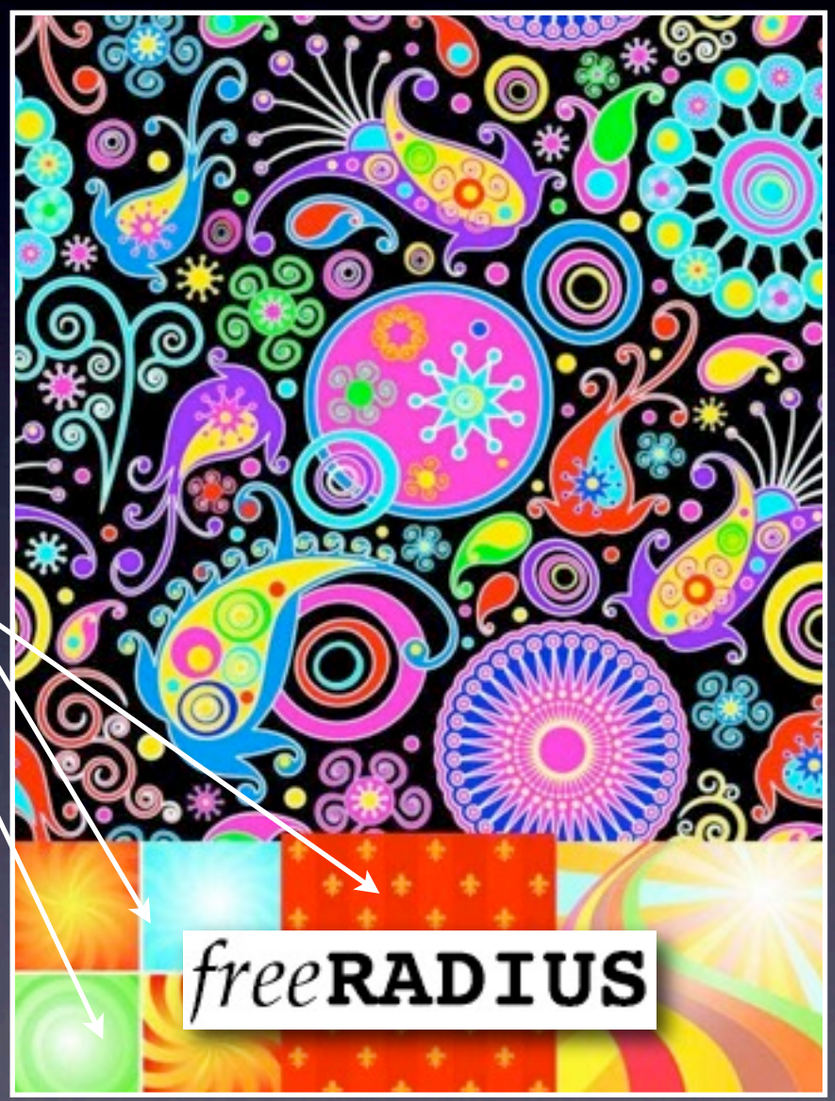
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

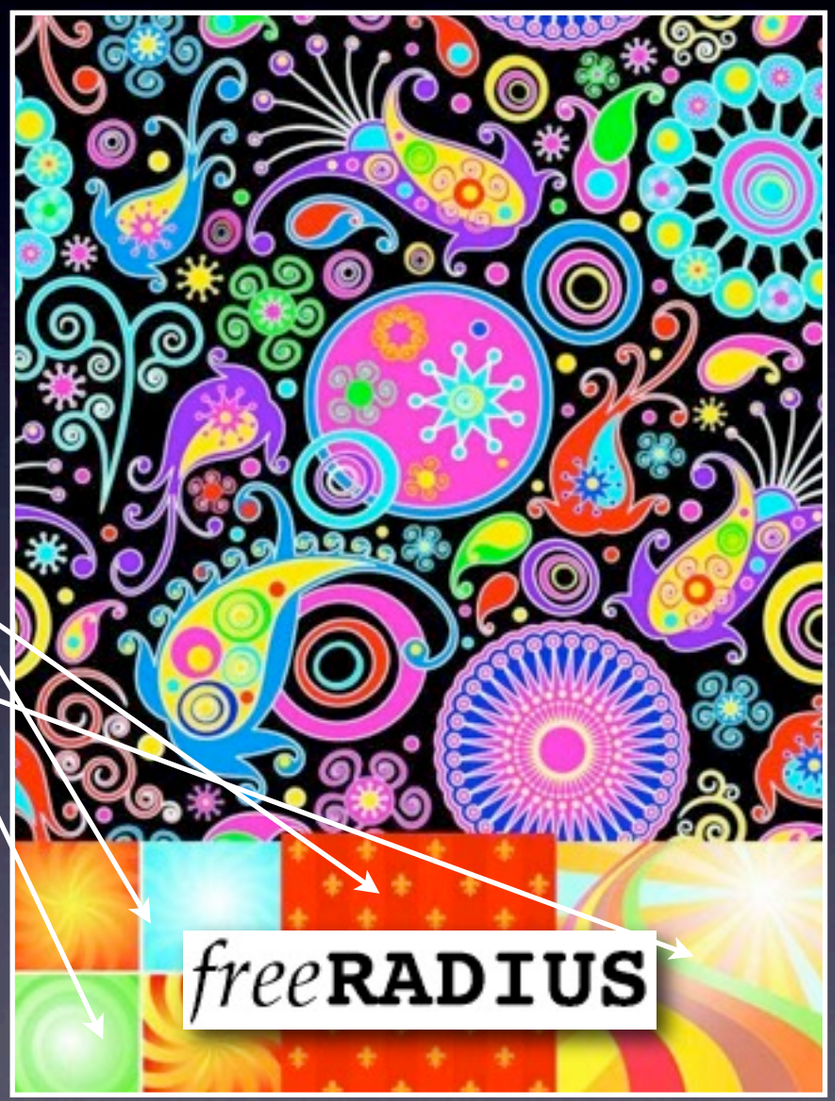
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

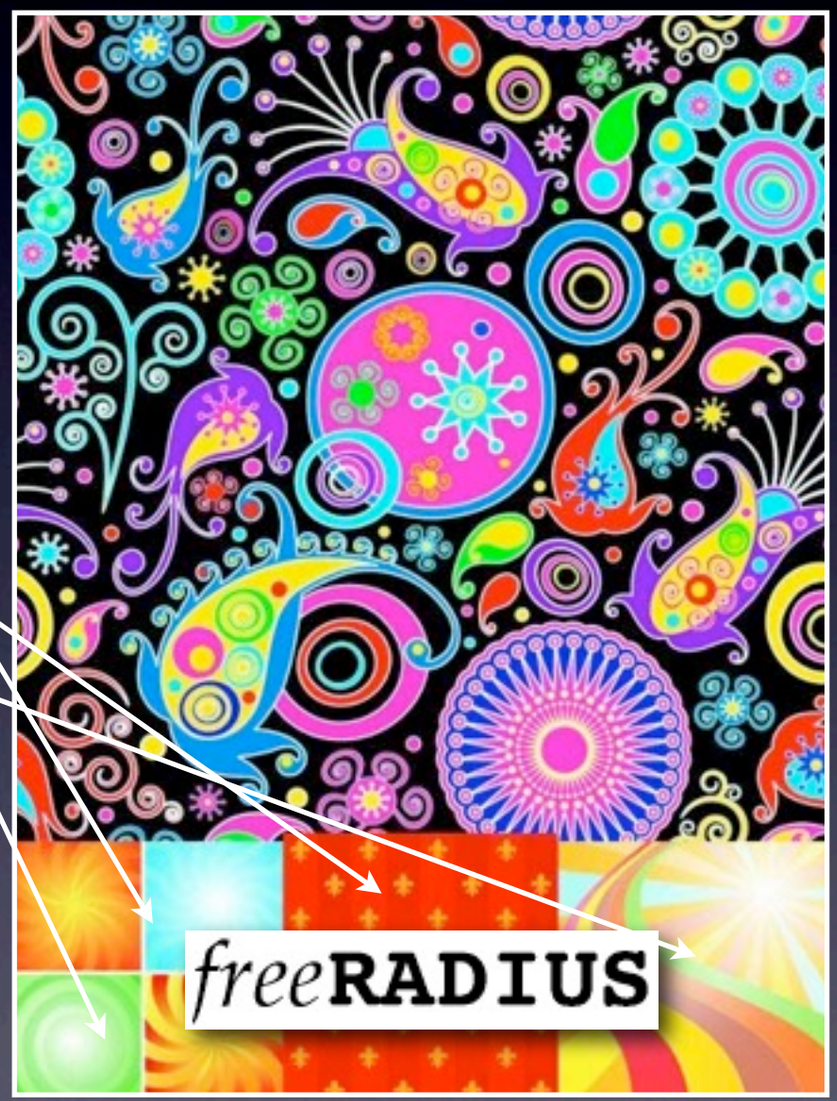
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

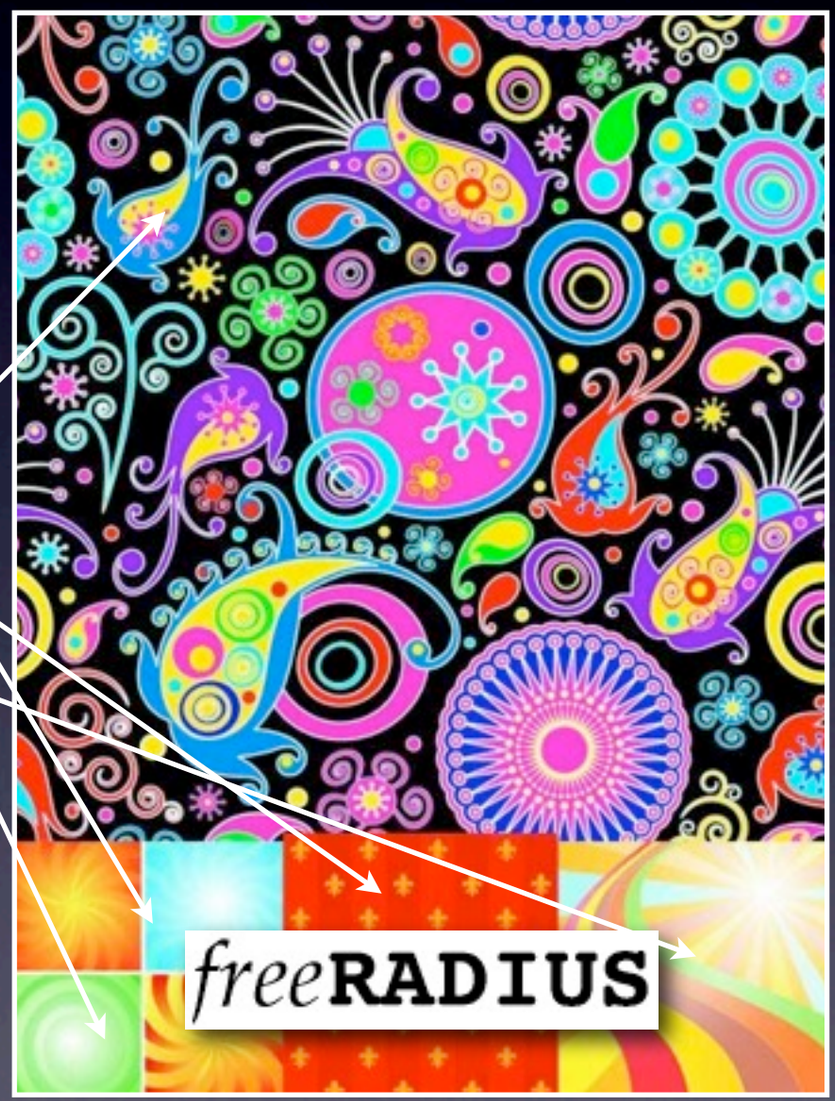
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

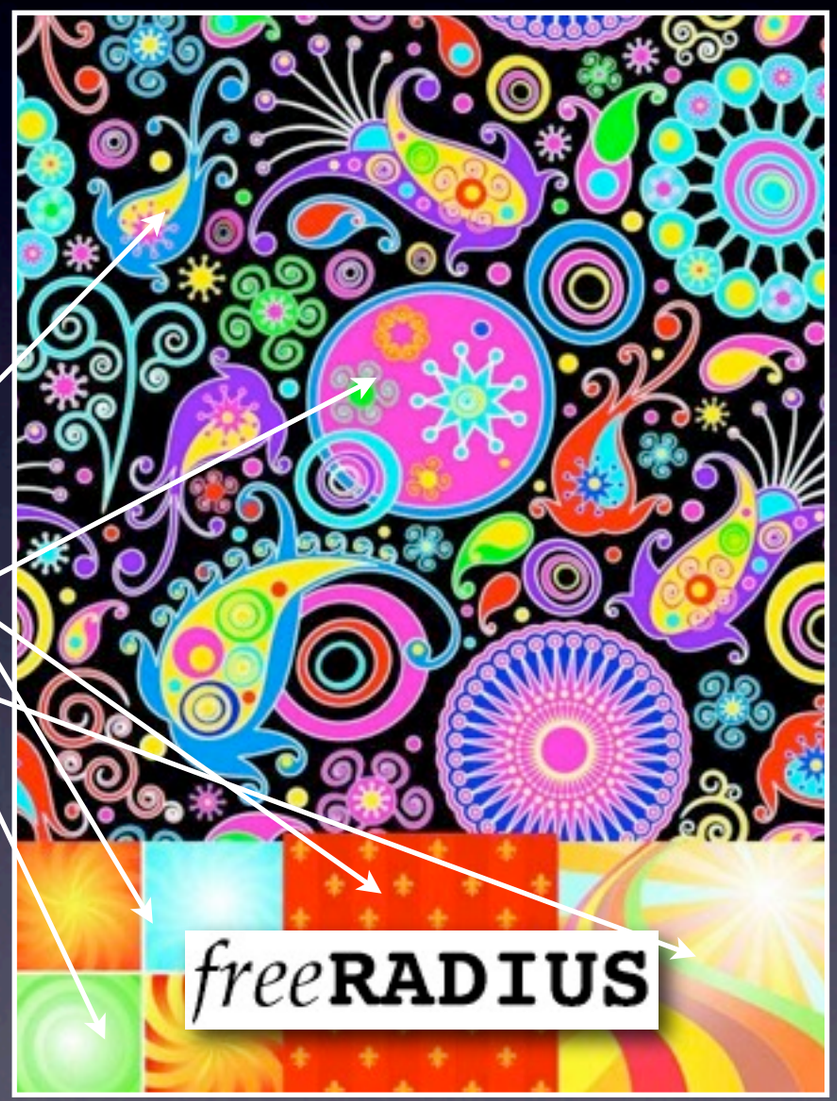
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

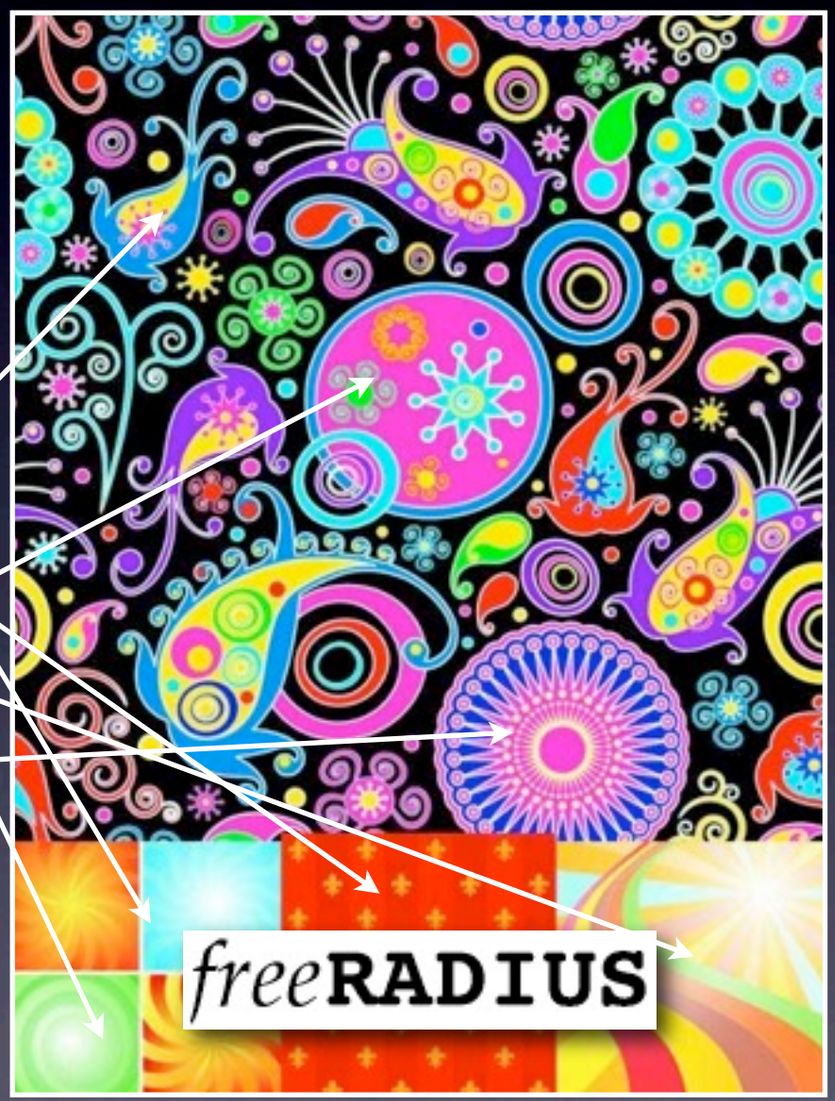
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

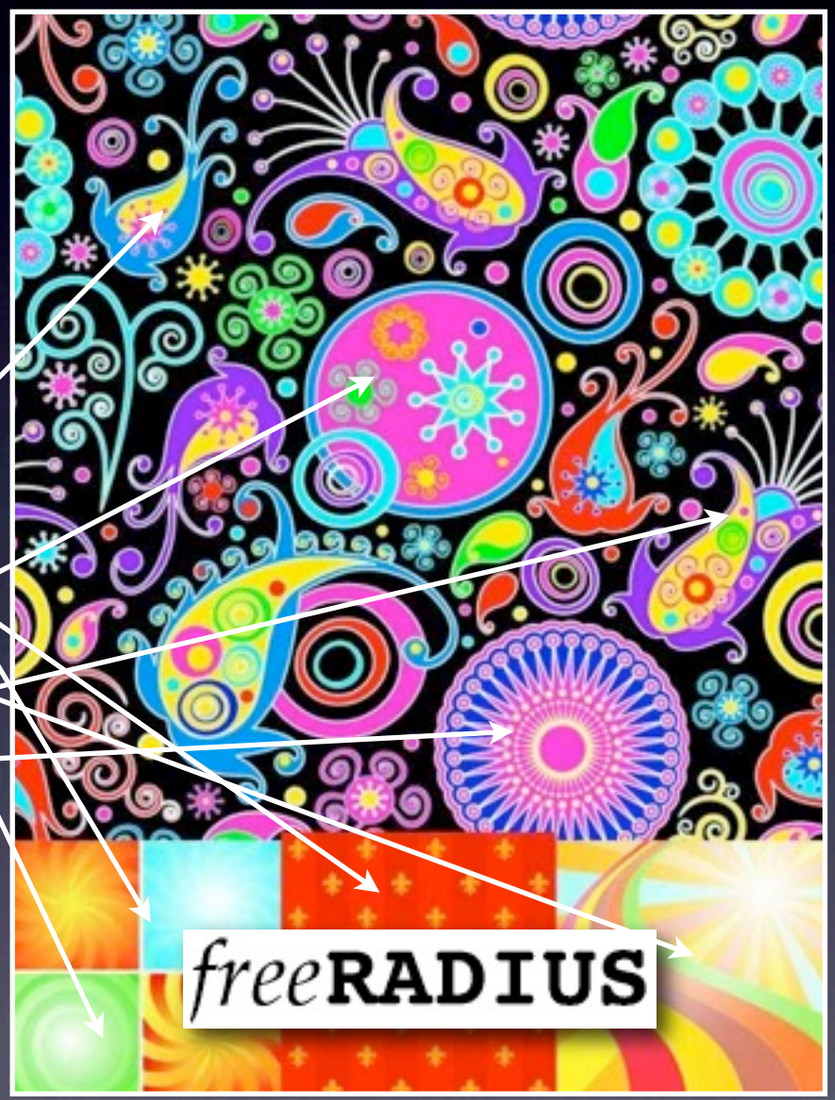
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

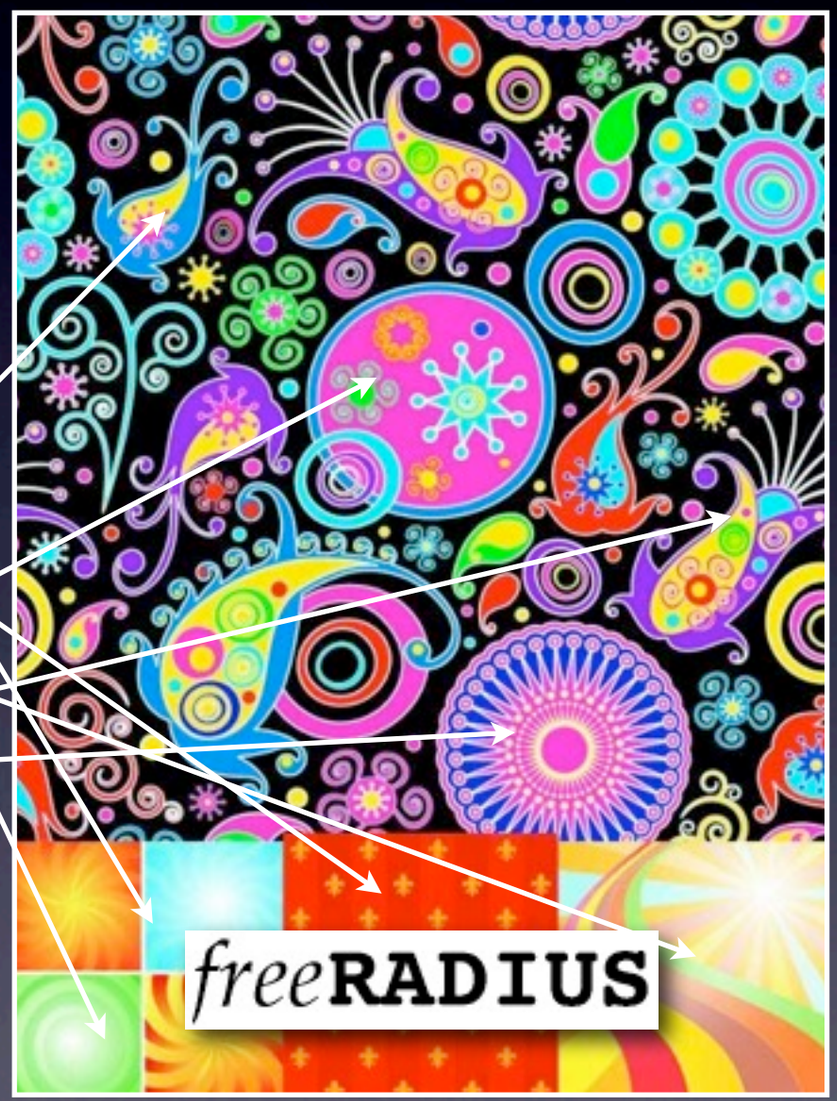
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

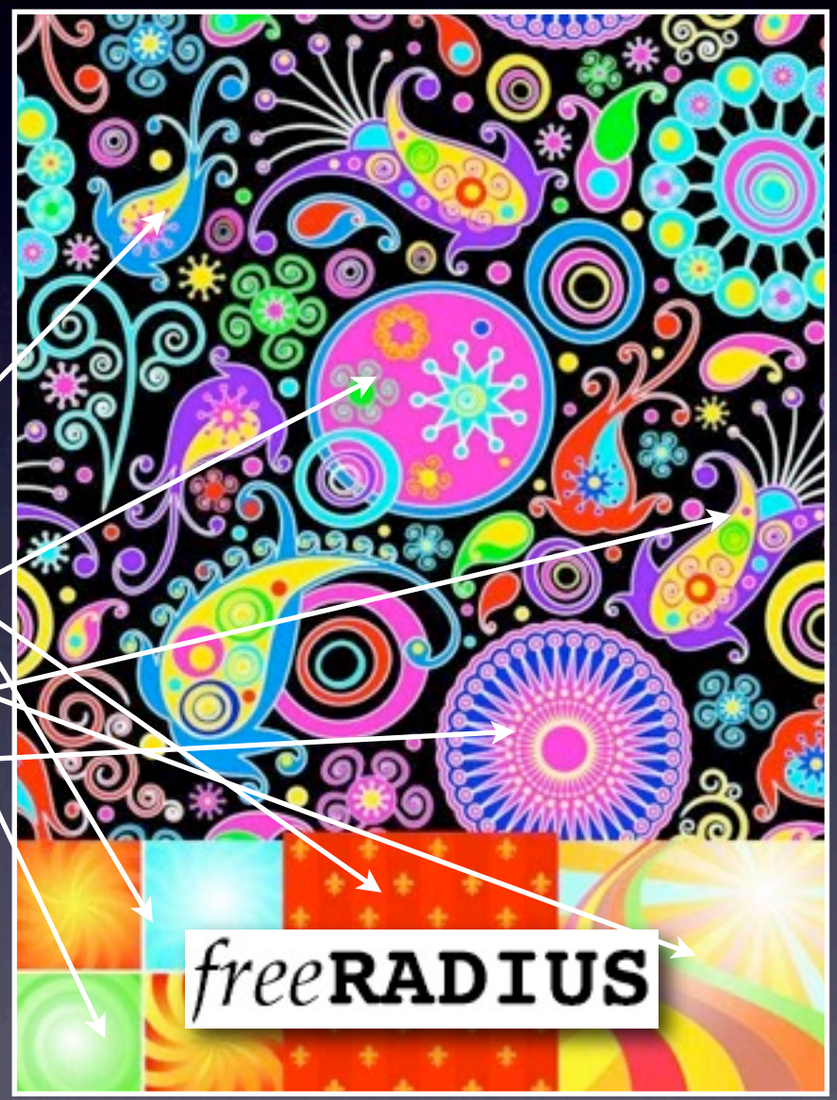
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules
- Un peu un sac de noeuds



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

freeRADIUS c'est...

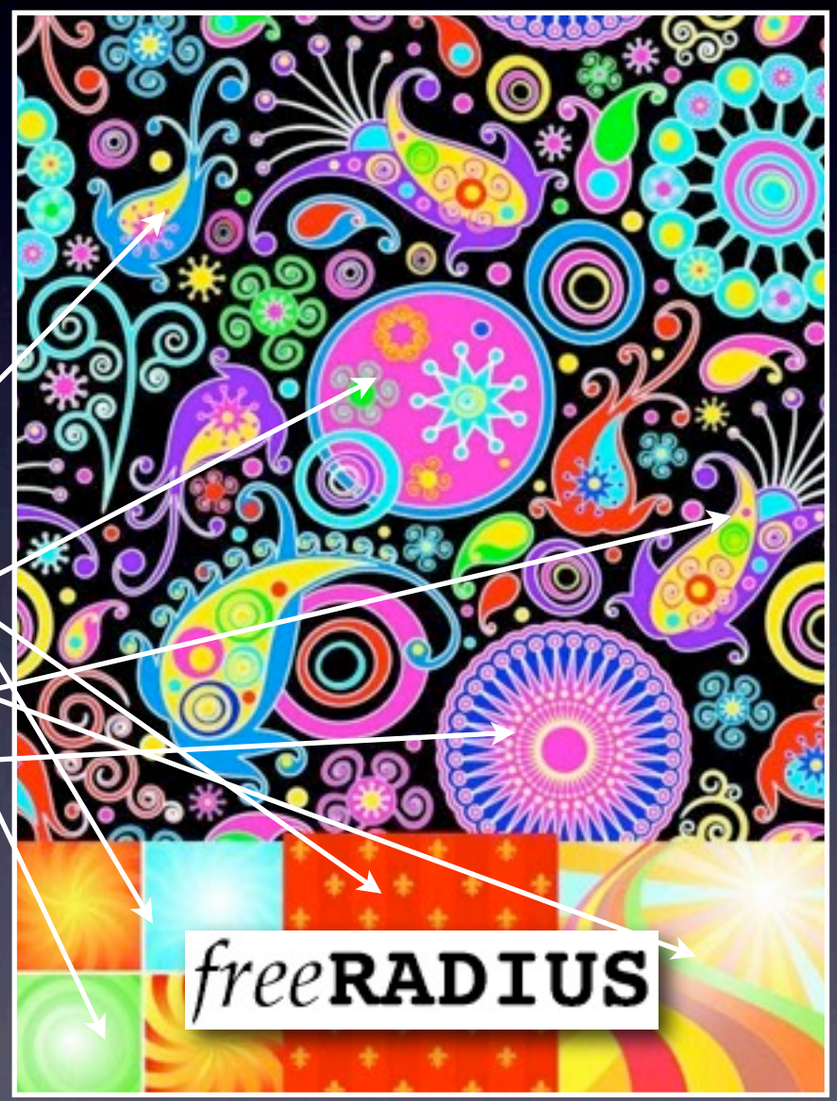
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules
- Un peu un sac de noeuds



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

Plan

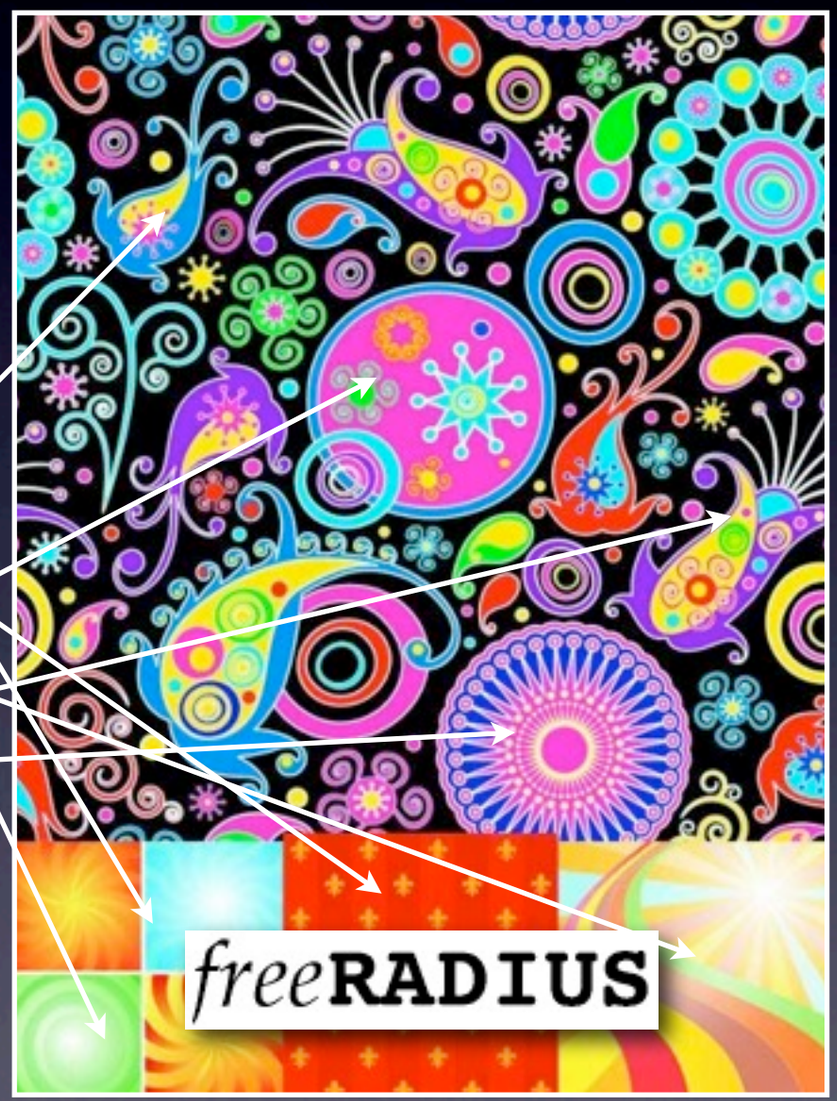
- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules
- Comment écrire un module ?



Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

Plan

- Plusieurs protocoles : RADIUS, EAP...
- Un serveur sous GPLv2
- Un système de configuration puissant
- Une multitude de modules
- Comment écrire un module ?

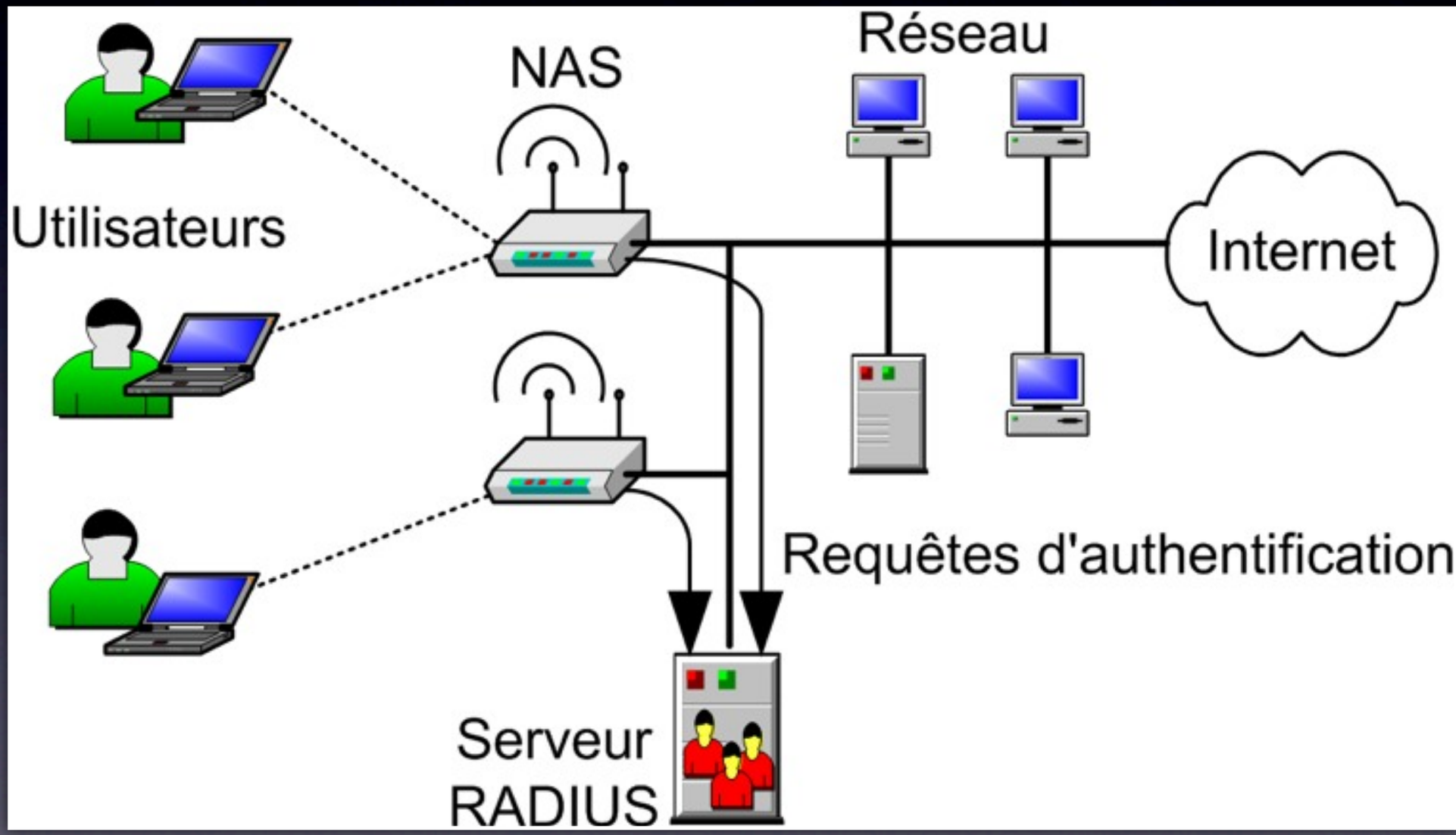


Source image: http://crshare.com/abstract-backgrounds-vector-clipart/

Avant de commencer avec freeRADIUS...

- Il faut bien comprendre le protocole RADIUS
- ainsi que les méthodes d'authentification EAP, notamment EAP/TLS, PEAP et TTLS

Architecture RADIUS



Terminologie

- User : utilisateur qui cherche à se connecter
- NAS = Network Access Server = Client (!) : contrôleur d'accès au réseau
  - Historiquement, le NAS se situait dans les Points de Présence (PoP) des opérateurs, pour contrôler les connexions RTC (PPP, PPPoE...)
  - Maintenant aussi dans les Base Stations (BS) Wimax (ou d'autres technologies)
  - Mais aussi également dans certains switchs
  - Et surtout dans beaucoup de Point d'Accès (AP) WiFi

Serveur AAA

- Un serveur RADIUS est un serveur de type AAA, car il gère :
  - **A**uthentification (en anglais *Authentication*) : valider que les utilisateurs sont bien qui ils prétendent être
  - **A**utorisation : informer le NAS des droits d'accès de chaque utilisateur qui se connecte
  - ***A**ccounting* : comptabilisation des connexions des utilisateurs (date et heure de connexion, durée, volume envoyé et reçu, adresse MAC...)
- Autres protocoles AAA : Diameter, TACACS

Configuration des NAS

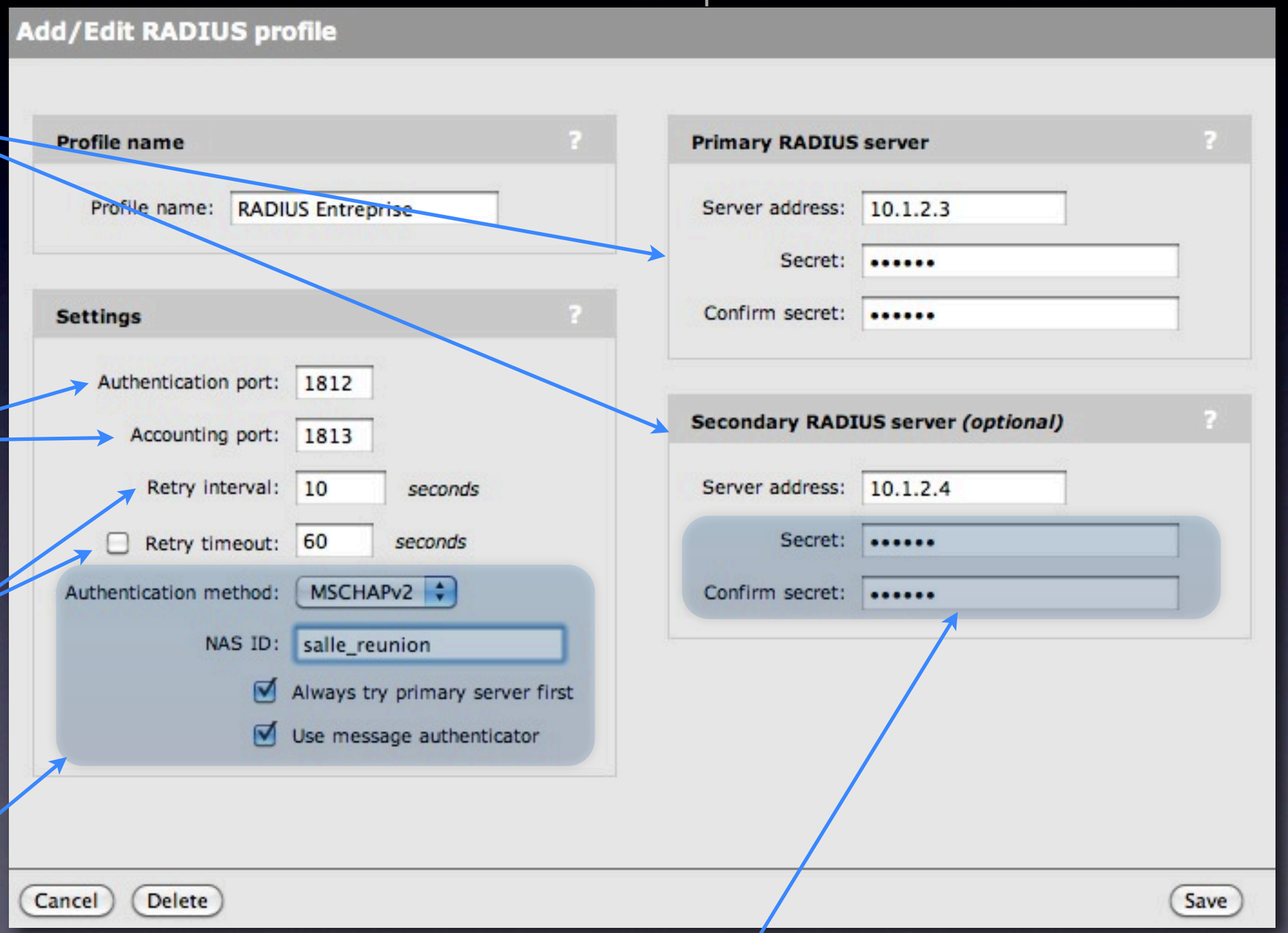
Exemple de l'interface Web d'un AP HP MSM310

Serveurs redondants

Ports UDP par défaut

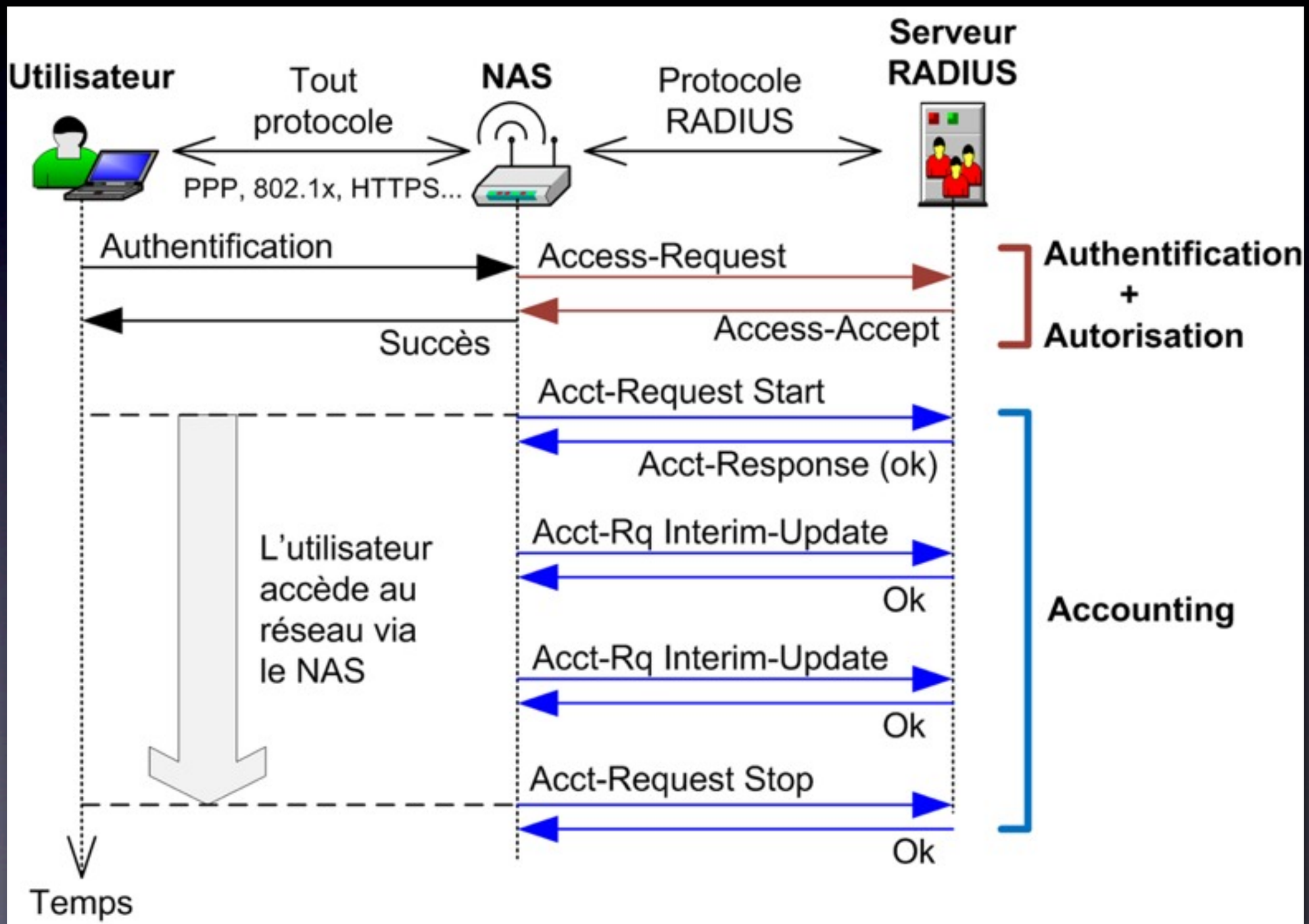
Gestion simple des échecs

Autres détails

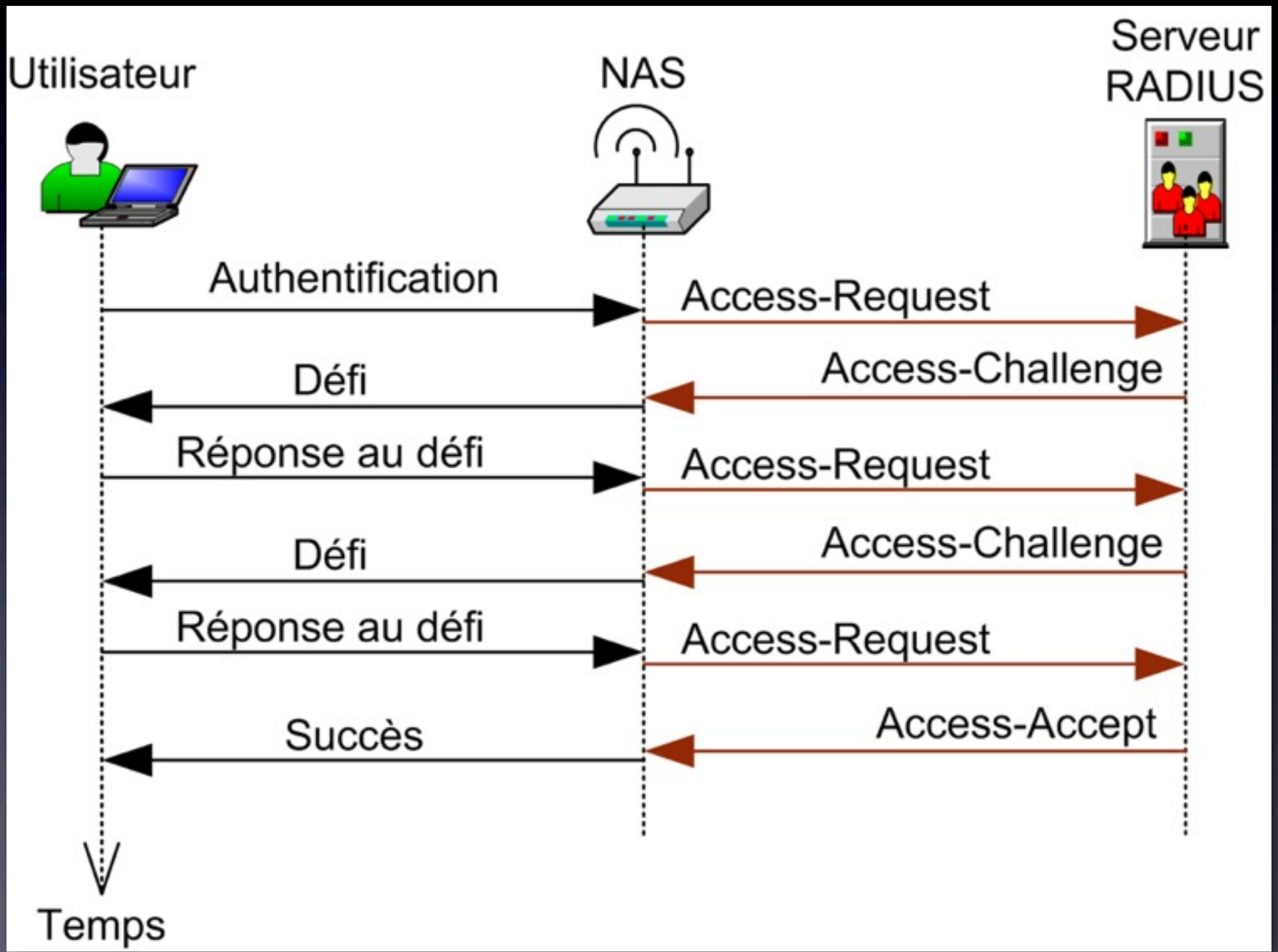


Le secret identifie le NAS auprès du serveur RADIUS

Exemple d'échange



Authentification avec défis



Le protocole RADIUS

- Défini dans plusieurs RFC :
  - RFC 2865 : protocole RADIUS, avec authentification et autorisation
  - RFC 2866 : rajoute l'accounting
  - RFC 2869 : rajoute les méthodes EAP
  - Et bien d'autres : http://freeradius.org/rfc/
- Repose sur UDP, par défaut port 1812 pour l'authentification et 1813 pour l'accounting

Le protocole RADIUS

- Chaque paquet est composé d'un entête qui précise:
  - le type du paquet : Access-Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request, Accounting-Response
  - l'authenticator, qui est une signature des réponses du Serveur RADIUS (voir plus loin)
  - la taille du paquet et son identifiant
- Le corps du paquet est composé d'une liste de paires Attribut=Valeur (AVP ou NVP = NameVP)
  - Exemple : User-Name="alain"

Attribute-Value Pairs

- Les attributs sont définis et numérotés dans les RFC
  - Par exemple l'attribut «User-Name» porte le numéro 1, et son type est une chaîne d'octets (string)
- Dans un paquet RADIUS, le nom et le type d'un attribut n'apparaissent pas, seulement son numéro et sa valeur
- Pour configurer facilement le NAS ou le serveur, il est donc nécessaire d'avoir un dictionnaire qui liste les attributs, leur numéro, leur type, et dans certains cas, leurs valeurs possibles
- Les types de base sont : string (suite d'octets), text (chaîne de caractères encodée en UTF-8), address (IPv4), integer (entier de 32 bits non signé) et time (date et heure). D'autres RFC sont venus compléter cette liste.

Vendor-Specific Attr.

- L'attribut «Vendor-Specific» (numéro 26) peut lui-même contenir une liste d'attributs spécifiques à une société
- Il contient le numéro de la société (délivré par l'IANA), suivi de la liste d'attributs dont les spécifications sont fixées par la société en question
- Souvent, la société ne définit qu'un seul attribut de type «string», puis la valeur elle-même contient une chaîne de caractères au format «attribut=valeur»
  - Exemple de valeur: «login-page=https://a.b.c/»
- Parfois un attribut propriétaire devient très utilisé et fini par être standardisé

Intégrité : Serveur vers NAS

- L'authenticator est une signature du paquet qui permet au NAS de s'assurer que la réponse qu'il reçoit provient bien du serveur RADIUS

Comment ça marche ?

Lorsqu'un NAS envoie une requête, il met un nombre aléatoire dans le champ authenticator.

Au moment de répondre, le serveur calcule un hash MD5 du paquet de réponse + le secret partagé avec le NAS + l'authenticator de la requête. Il renvoie ce hash dans le champ authenticator : c'est une signature électronique que le NAS peut vérifier.

Intégrité : NAS vers Serveur

Par défaut, rien ne permet au serveur de vérifier l'intégrité d'un paquet envoyé par un NAS

- Pour régler ce problème, un attribut «Message-Authenticator» a été défini dans la RFC 2869
- Le NAS peut le rajouter à une requête avant de l'envoyer au serveur : il s'agit d'un *hash* MD5 calculé sur l'ensemble du paquet + le secret partagé.
- Il est recommandé de configurer le serveur pour qu'il rejette les paquets non signés de cette façon.

Confidentialité

Les paquets RADIUS ne sont pas chiffrés

Les données transitent en clair, sauf exception

La valeur de certains attributs est chiffrée

Authentification PAP

- Les deux méthodes d'identification définies initialement par RADIUS sont PAP et CHAP
- En PAP, le mot de passe est chiffré avec un algorithme assez faible (reposant sur le secret partagé), et envoyé au serveur dans l'attribut `User-Password`
- Le serveur déchiffre le mot de passe, vérifie qu'il est bon et répond `Access-Accept` **ou** `Access-Reject`

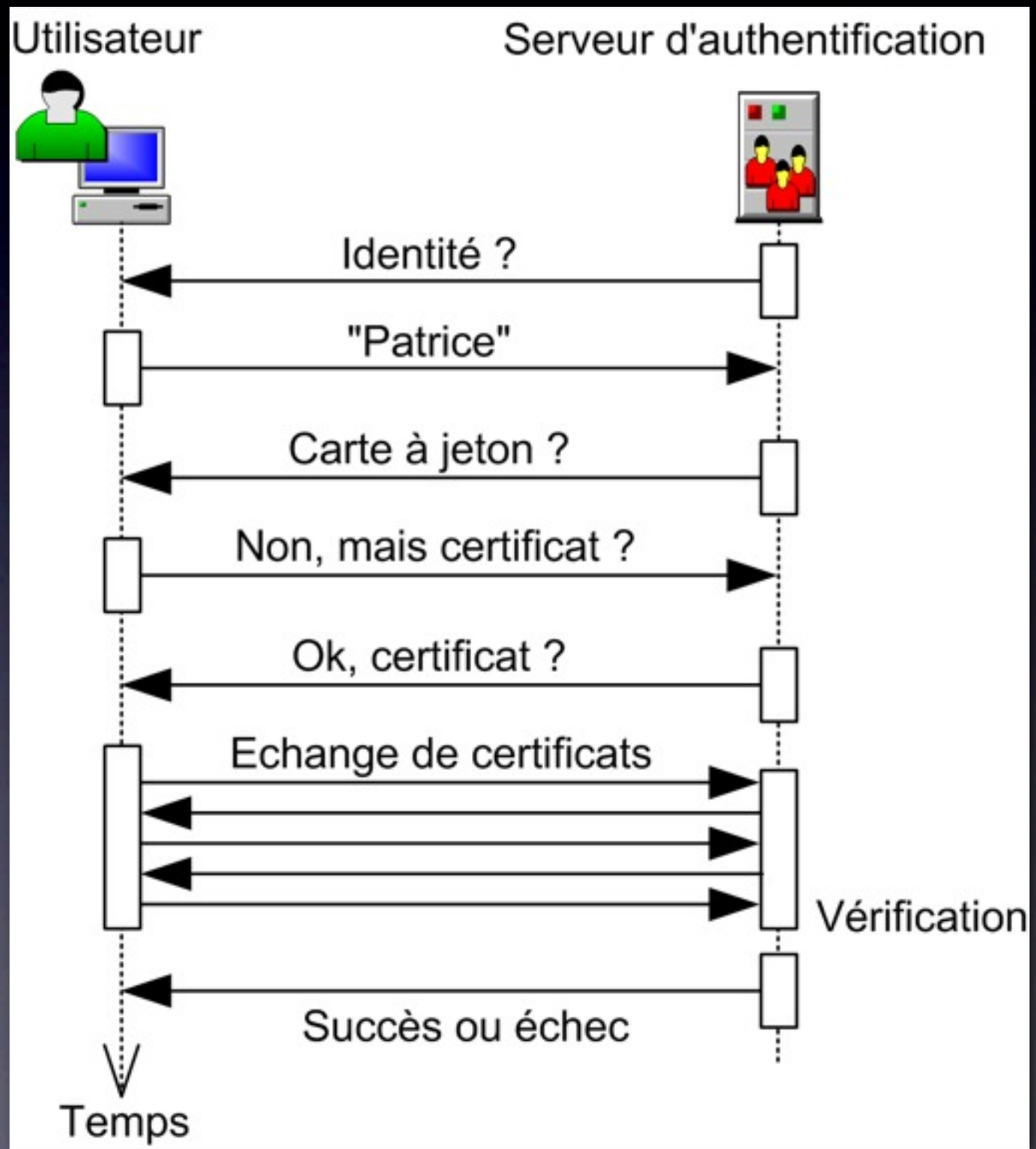
Authentification CHAP

- En CHAP, le NAS fournit un défi (challenge) au système de l'utilisateur
- Le système demande à l'utilisateur son mot de passe, puis calcule un hash MD5 du mot de passe, du challenge et d'un identifiant de réponse CHAP
- Le hash est renvoyé au NAS, qui renvoie ensuite l'identifiant CHAP + le hash au serveur RADIUS dans un attribut CHAP-Password...
- ...accompagné du challenge dans l'attribut «CHAP-Challenge» (ou éventuellement dans l'authenticator si le challenge fait 16 octets)
- Avantage : le mot de passe ne transite plus sur le réseau
- Inconvénient : le serveur RADIUS doit disposer du mot de passe de l'utilisateur en clair pour authentifier le user

Méthodes EAP

- L'Extensible Authentication Protocol a été défini pour permettre plus de souplesse et de sécurité que le PAP et le CHAP
- C'est un protocole indépendant du protocole RADIUS
- L'architecture EAP ne comprend que deux acteurs : l'utilisateur (qu'on appelle ici le «client»), et le serveur d'authentification (dans notre cas, ce sera le serveur RADIUS).
- Lors du dialogue EAP, le client fournit son identité, puis une méthode d'authentification est négociée, et enfin l'authentification proprement dite a lieu.

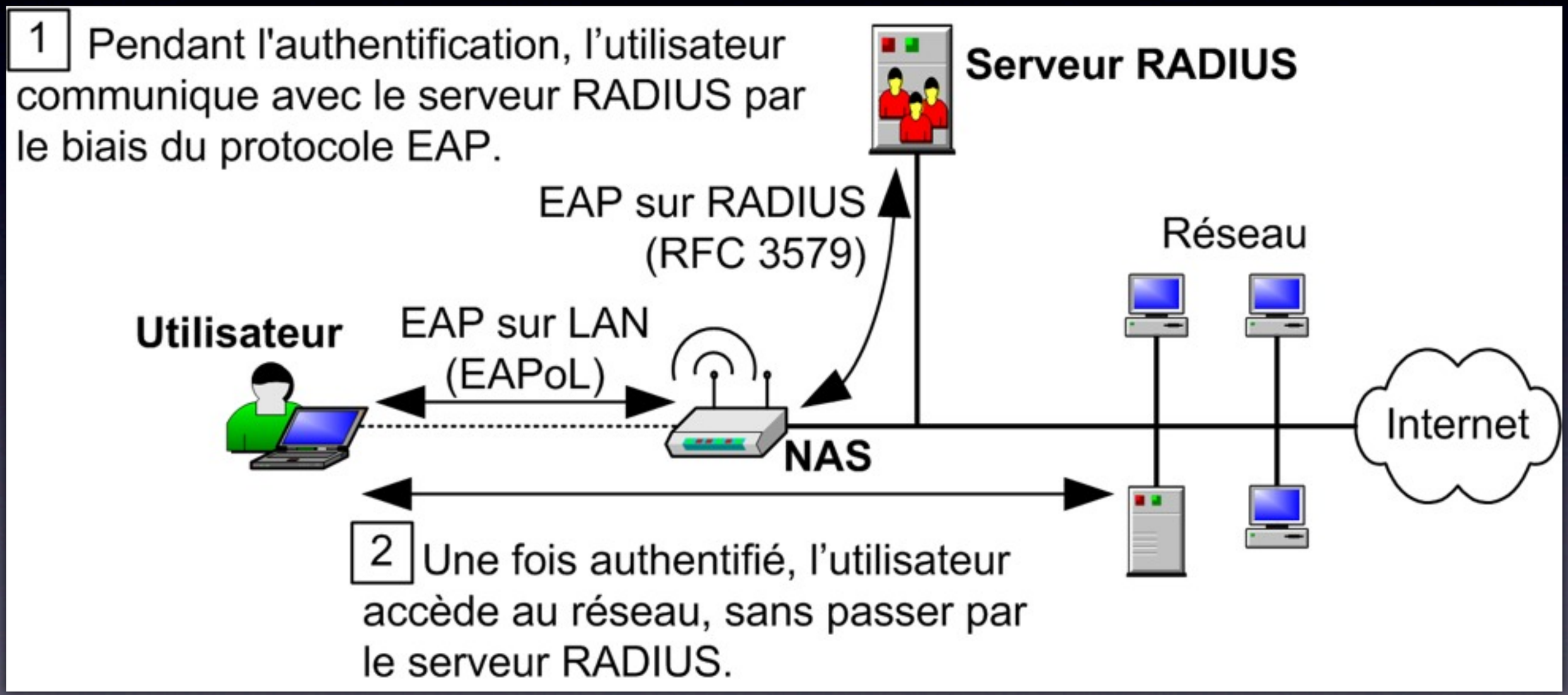
Dialogue EAP



Le protocole 802.1x

- Le 802.1x permet de marier l'architecture RADIUS avec l'authentification EAP pour contrôler les connexions sur un réseau Ethernet (LAN)
- Entre l'utilisateur et le NAS, le protocole EAPoL (EAP over LAN) est utilisé
- EAPoL est une variante de EAP qui rajoute quelques types de paquets, notamment pour que l'utilisateur puisse initier la communication (en EAP classique, c'est le serveur qui parle en premier) et pour permettre l'échange de clés de chiffrement
- Entre le NAS et le serveur RADIUS, la communication repose sur le protocole RADIUS, et les paquets EAP sont transportés dans un attribut EAP-Message

Architecture 802.1x



Principales méthodes EAP

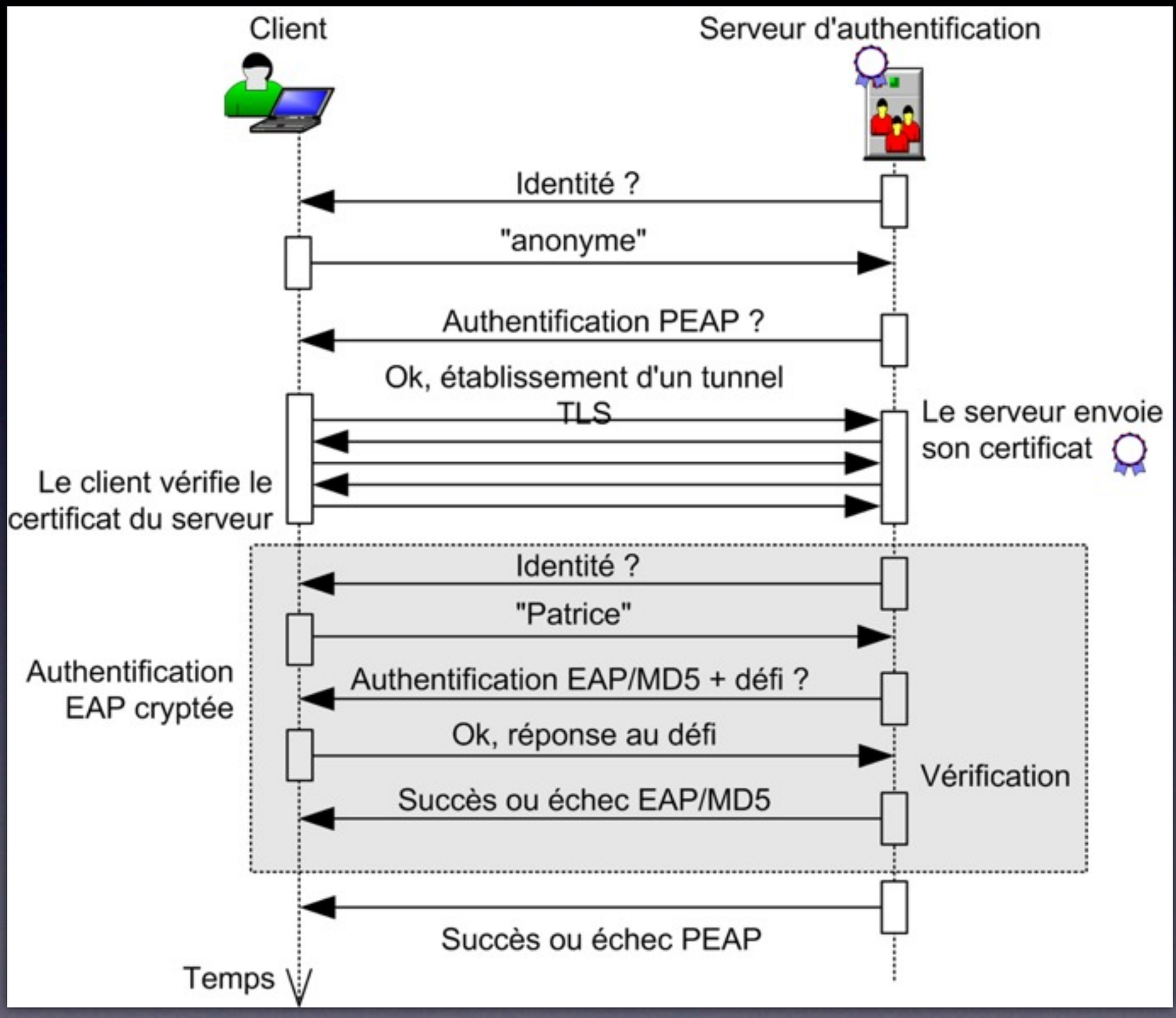
- EAP/MD5 : équivalent à CHAP
- EAP/MS-CHAP-v2 : semblable à CHAP mais n'impose pas au serveur de connaître le mot de passe en clair, mais plutôt un hash du mot de passe.
- EAP/GTC (Generic Token Card) : mécanisme très générique, utilisé pour les cartes d'identification «à jeton»
- EAP/SIM : identification par carte à puce GSM
- EAP/TLS : identification par certificat électronique TLS
- EAP/PEAP : établit un tunnel TLS au sein duquel peut avoir lieu une autre authentification EAP : par exemple EAP/MS-CHAP-v2 (on note alors l'ensemble PEAP/MS-CHAP-v2).

Compatibilité 802.1x

Pour utiliser une méthode d'authentification particulière, il faut:

- que le système de l'utilisateur la gère
- que le serveur RADIUS la gère
- que le NAS soit compatible 802.1x

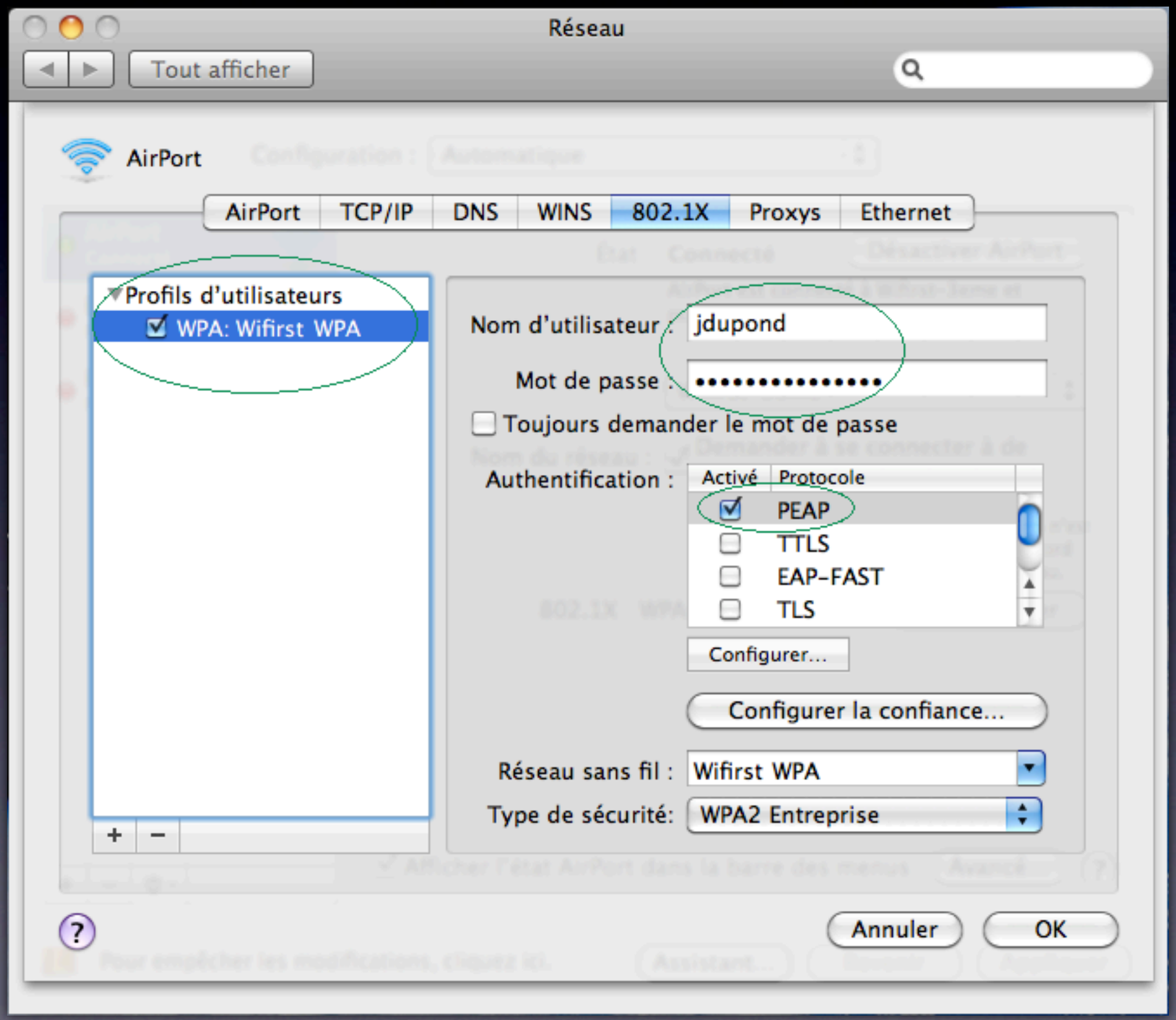
Dialogue PEAP/MD5



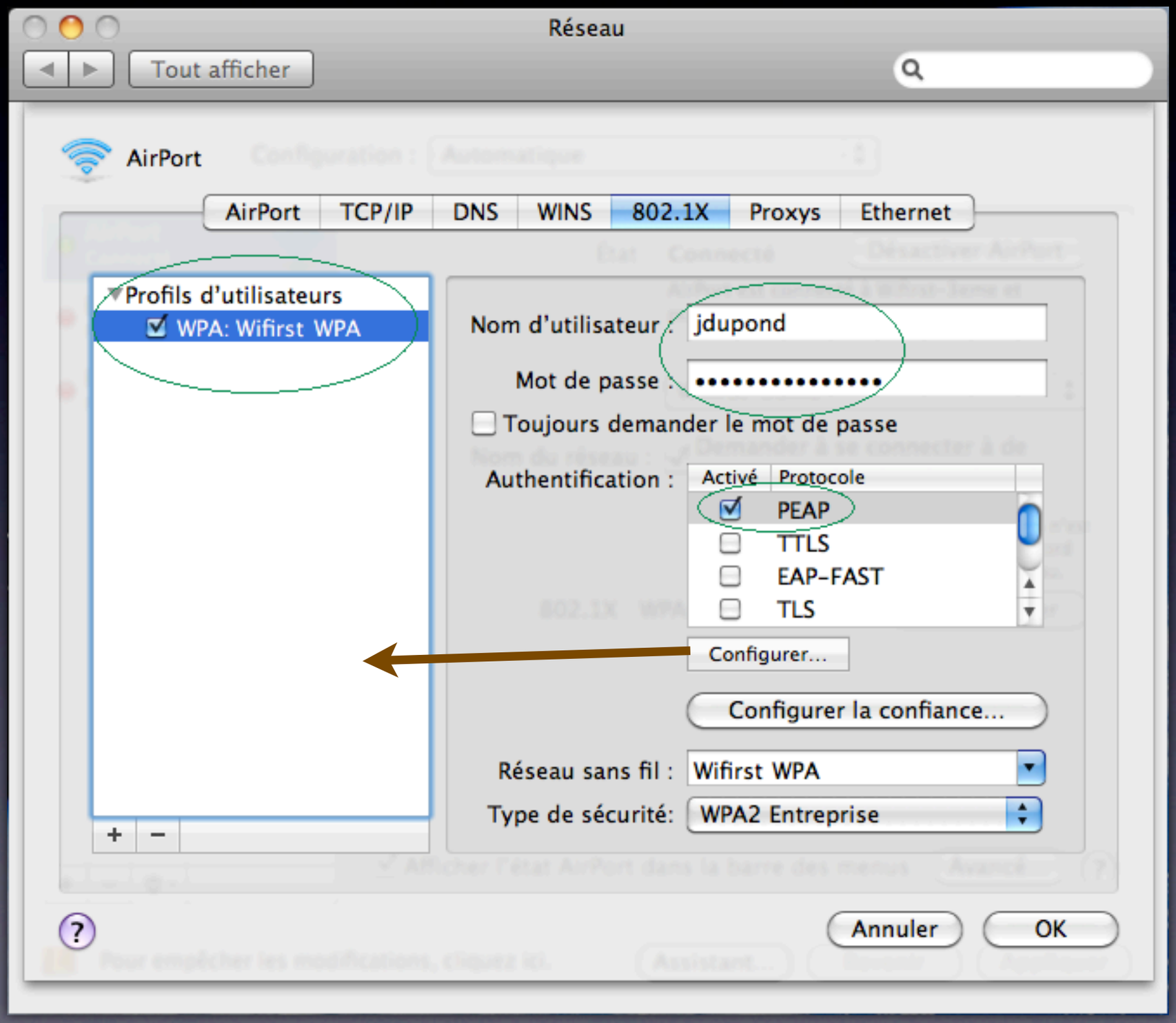
Vérifier le certificat TLS

- L'utilisateur doit absolument vérifier la validité du certificat du serveur, sinon il y a risque d'attaque de type Man-in-the-Middle
- Attention: sous Windows et MacOSX, lorsque l'utilisateur accepte le certificat, il accepte implicitement tous les certificats issus de la même autorité de certification !
- Pour éviter cela, l'utilisateur doit aller modifier sa configuration comme ceci...

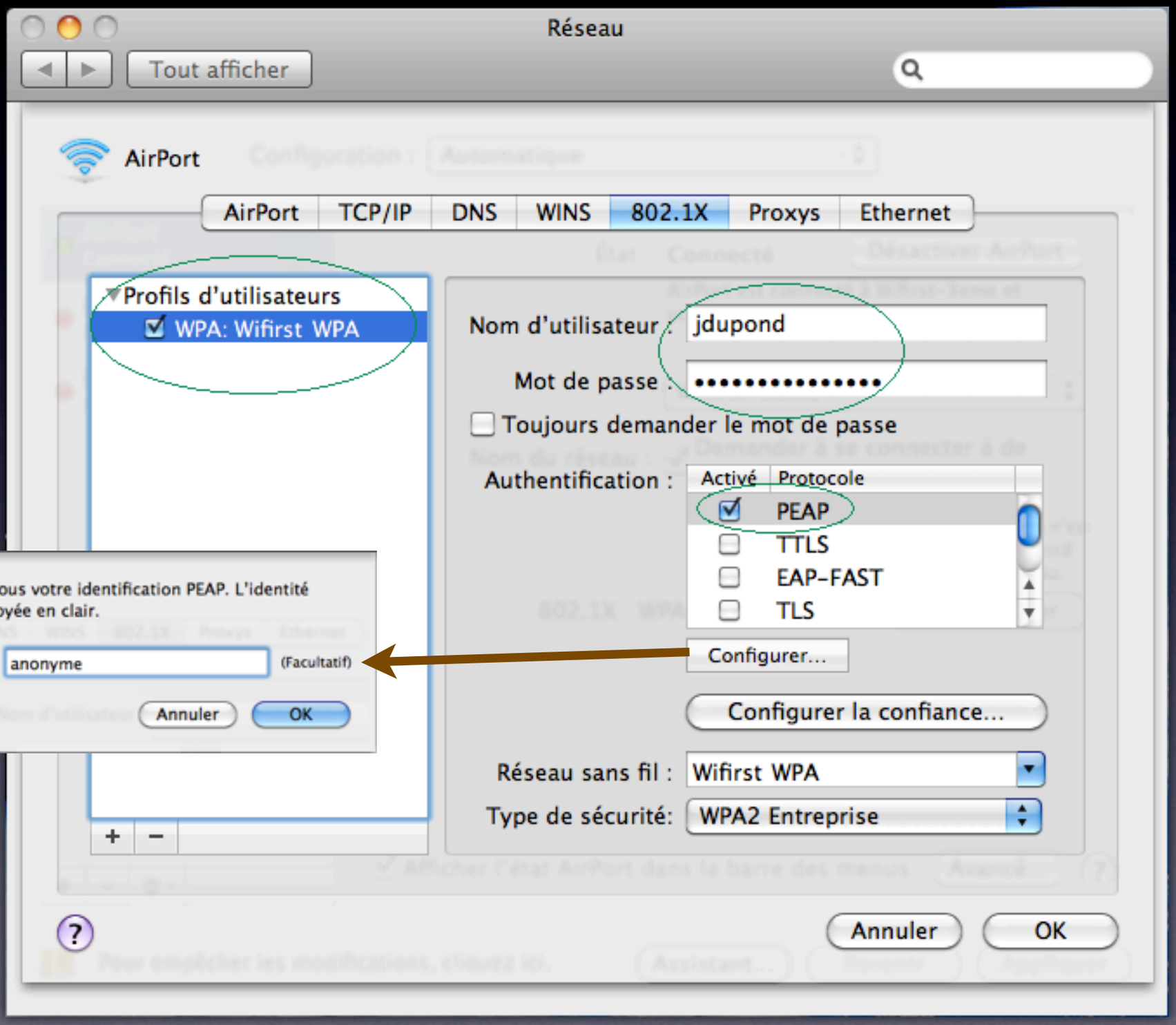
PEAP sous MacOSX



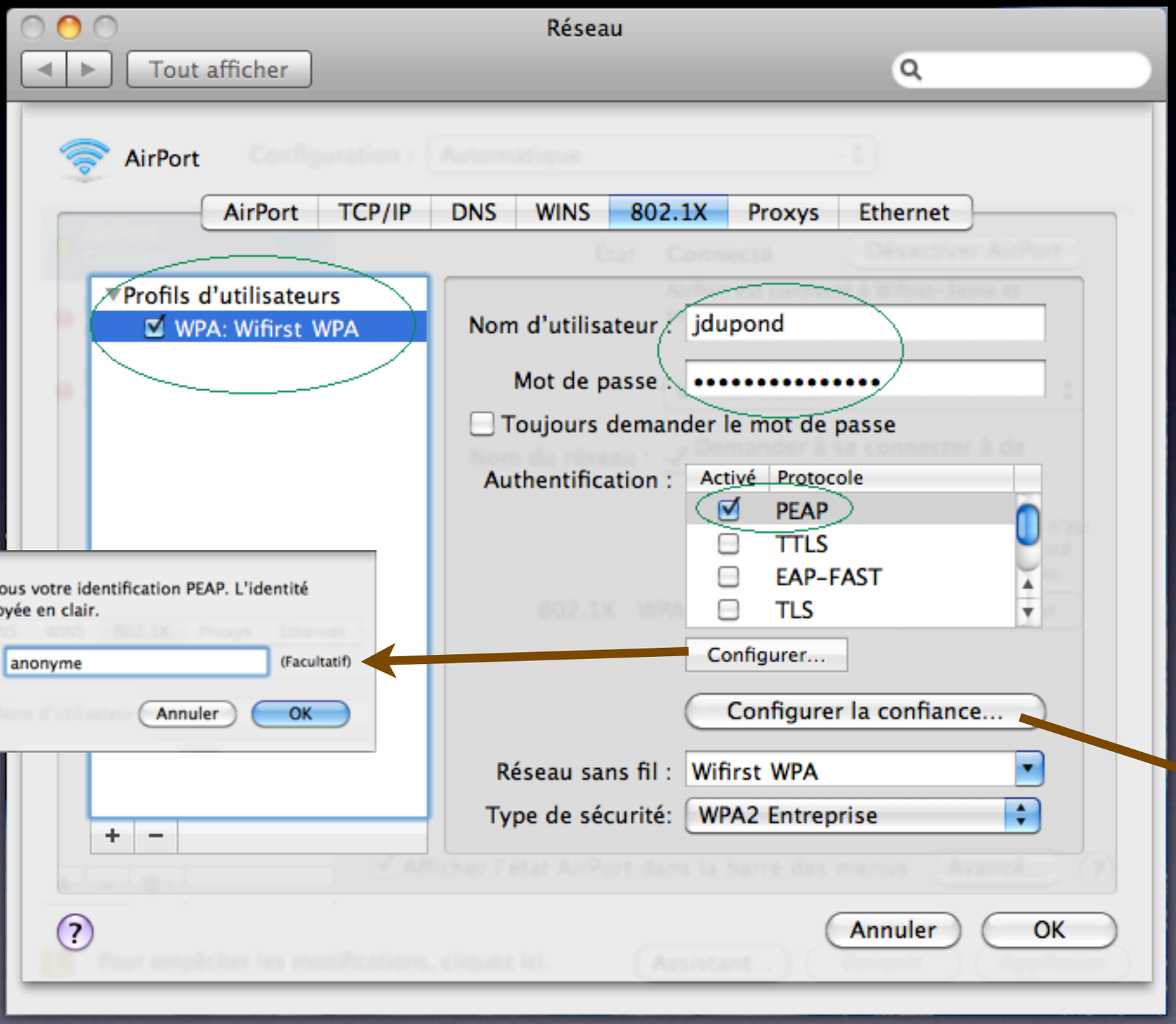
PEAP sous MacOSX



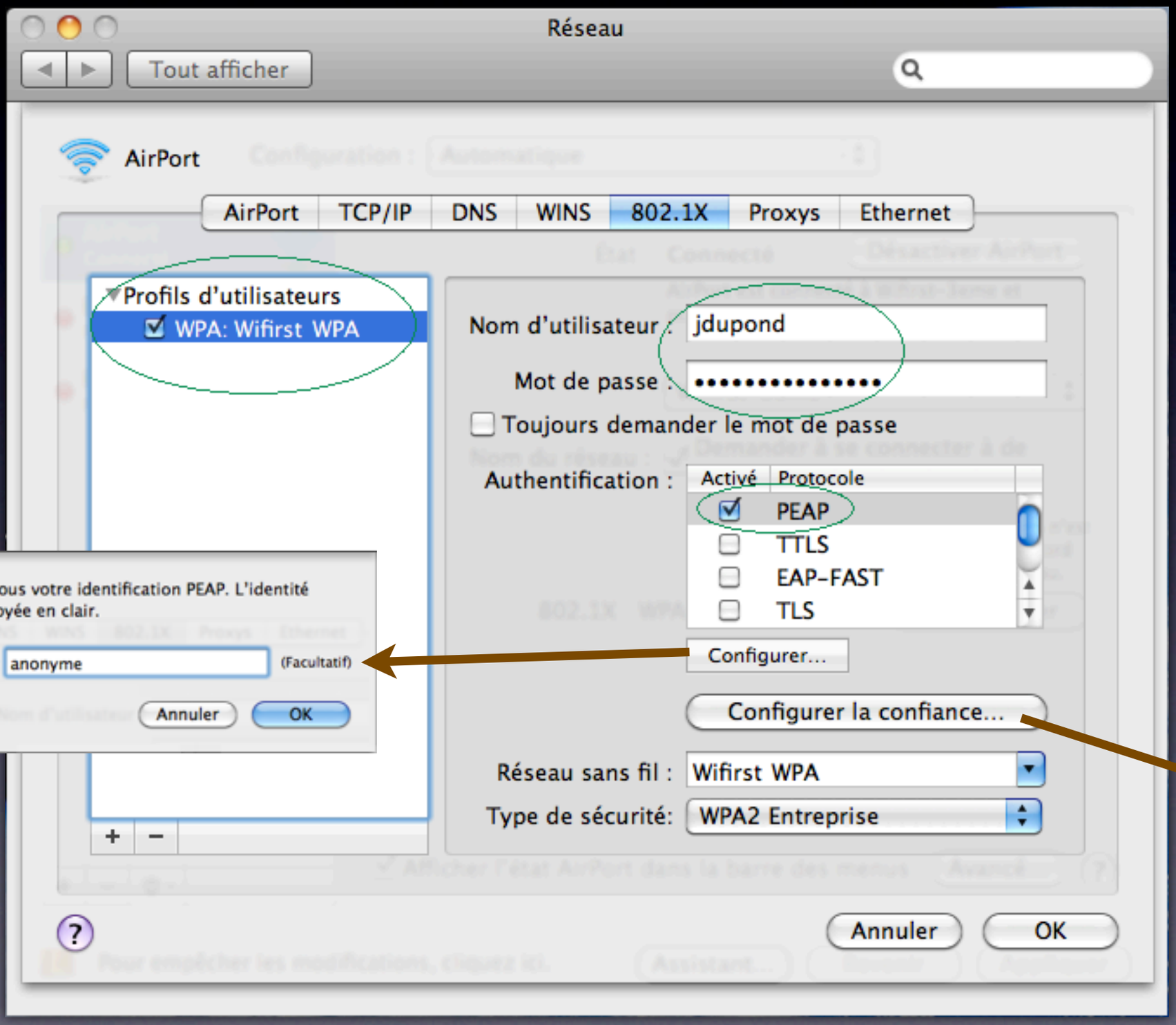
PEAP sous MacOSX



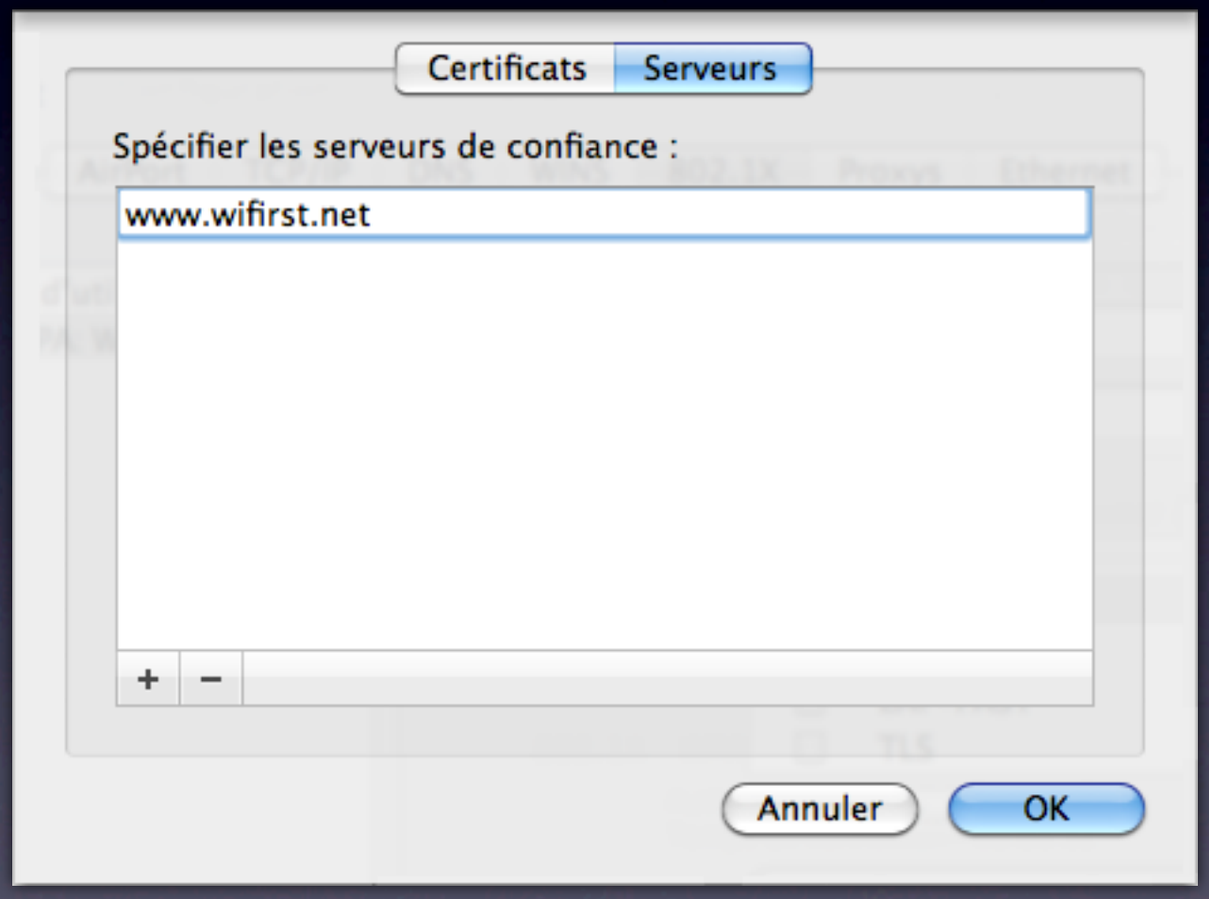
PEAP sous MacOSX



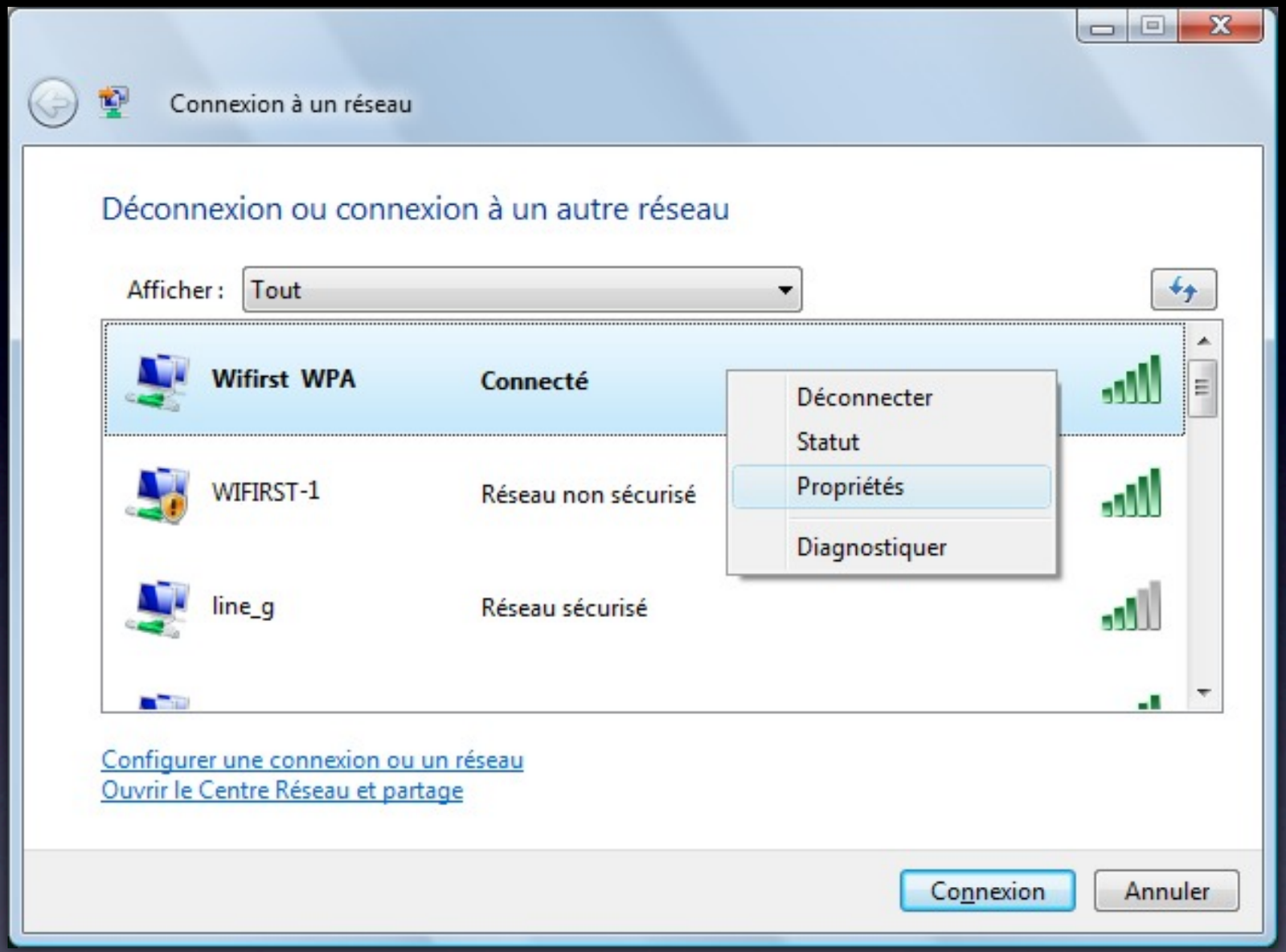
PEAP sous MacOSX



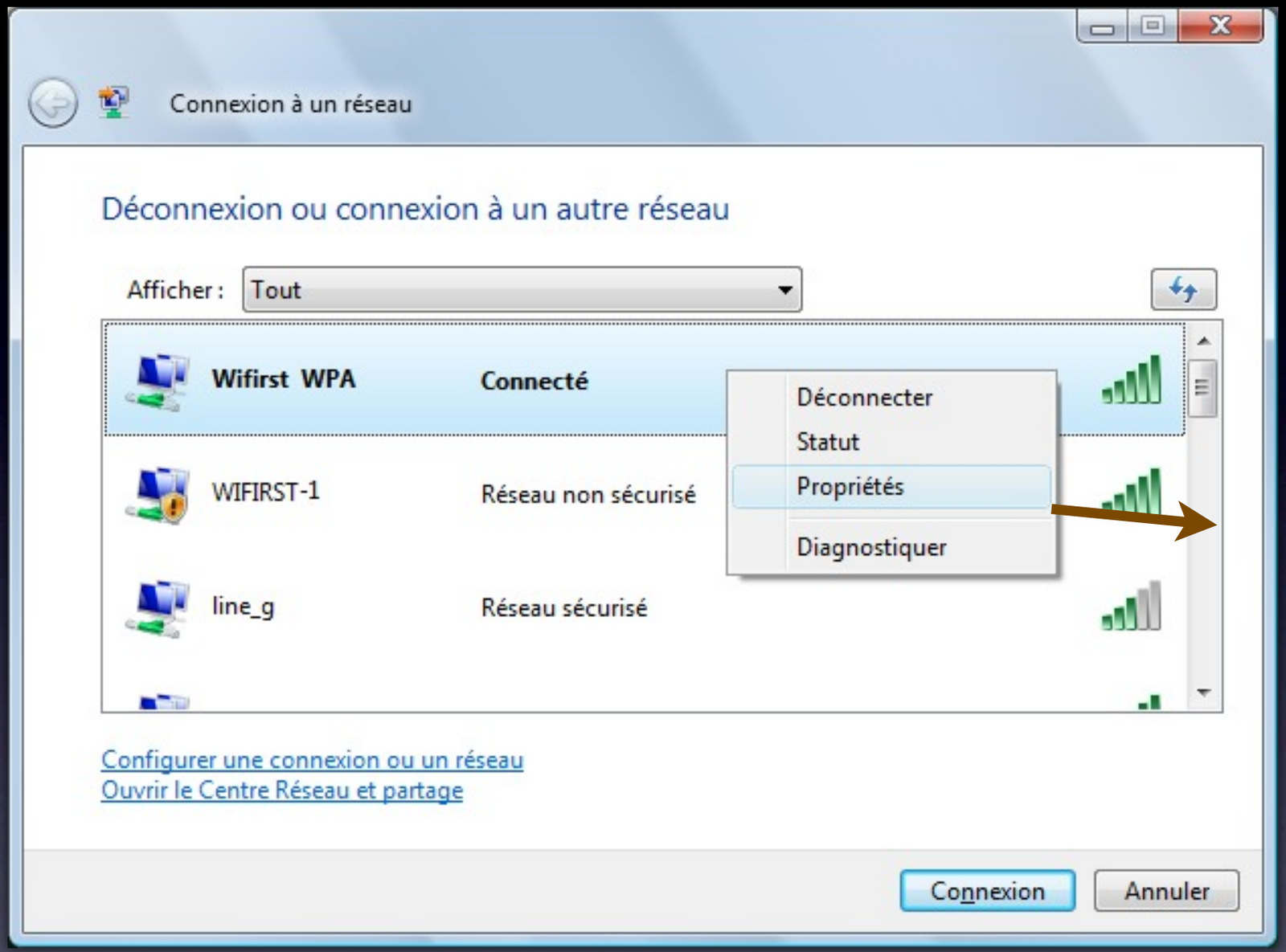
PEAP sous MacOSX



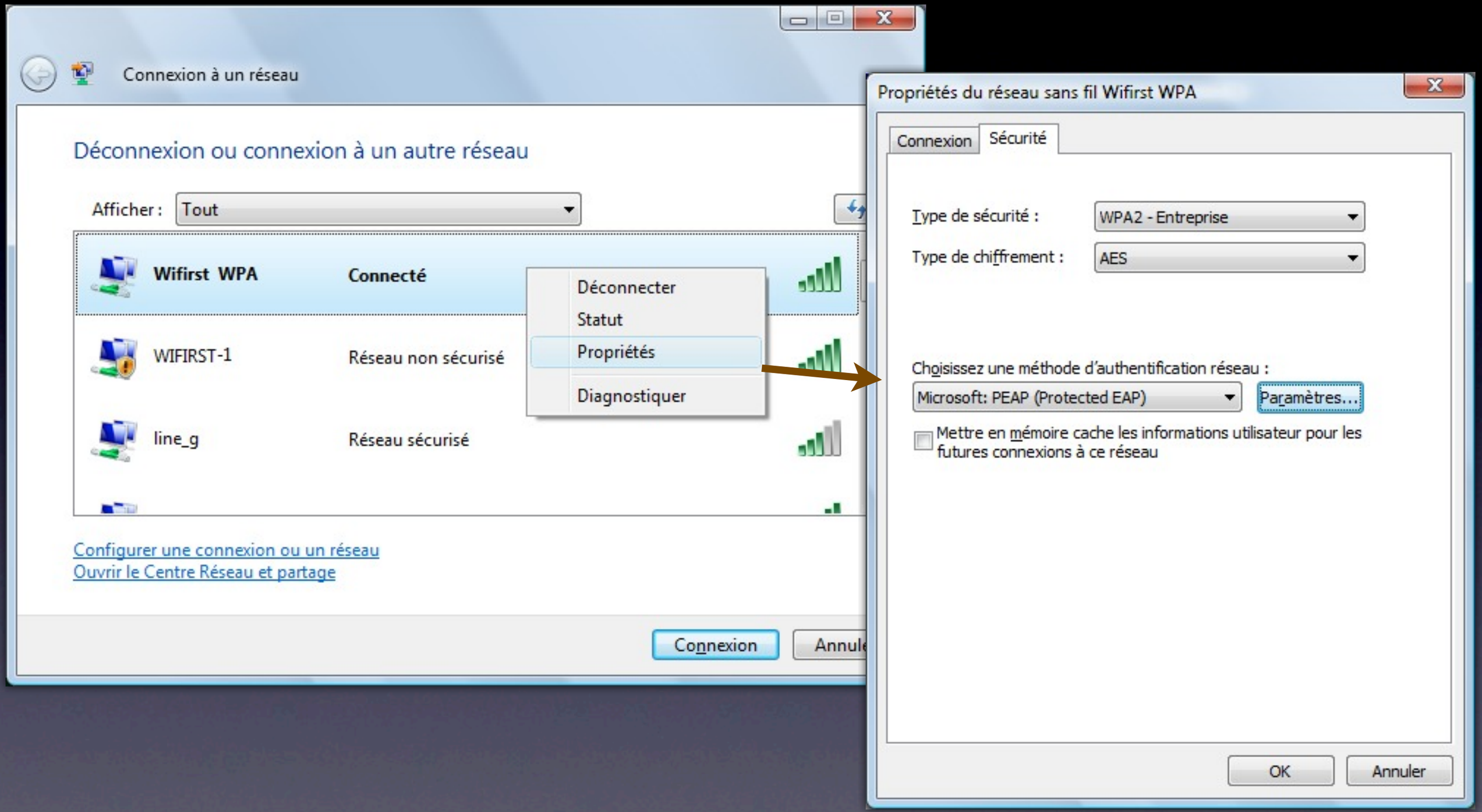
PEAP sous Windows



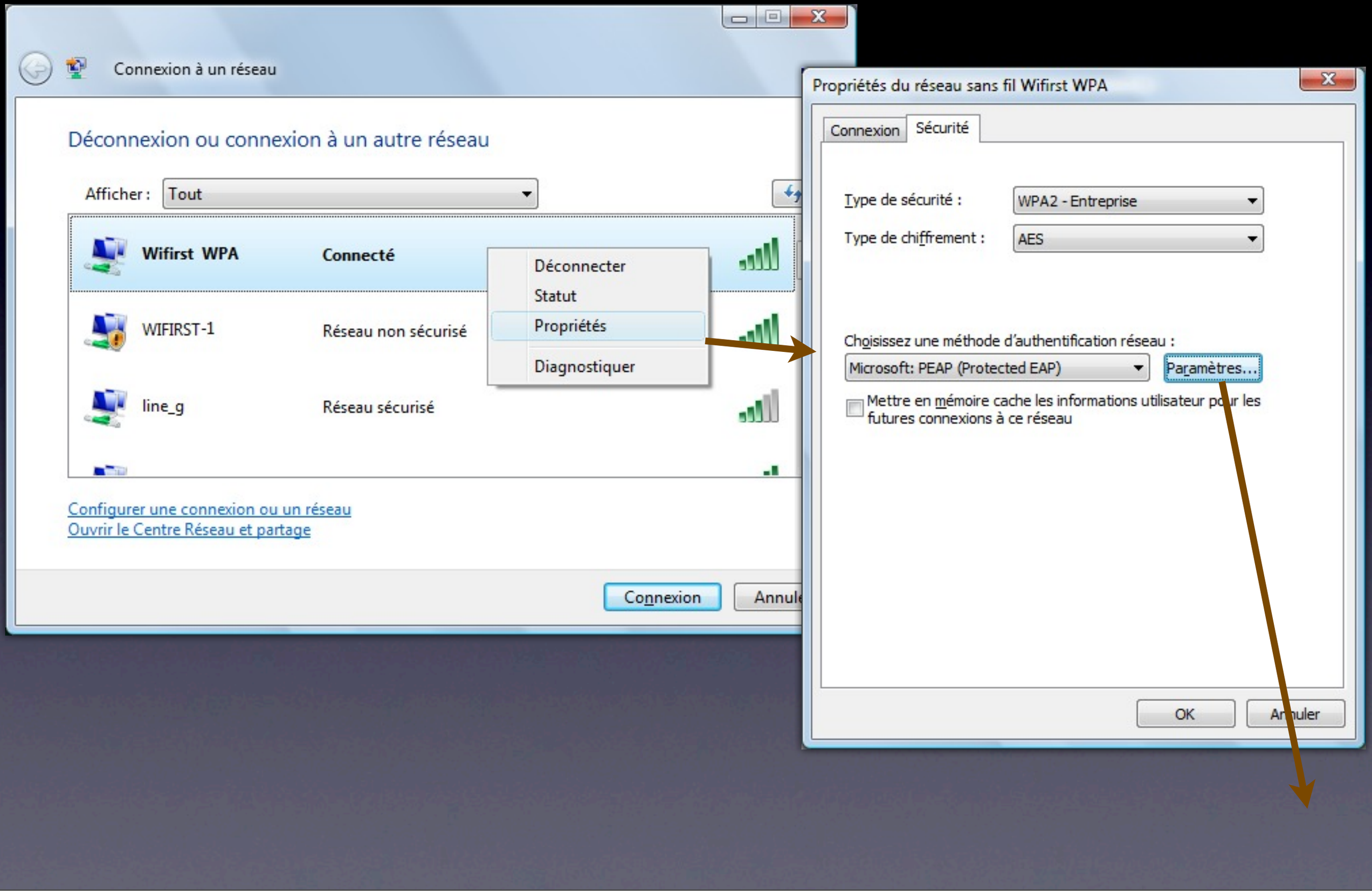
PEAP sous Windows



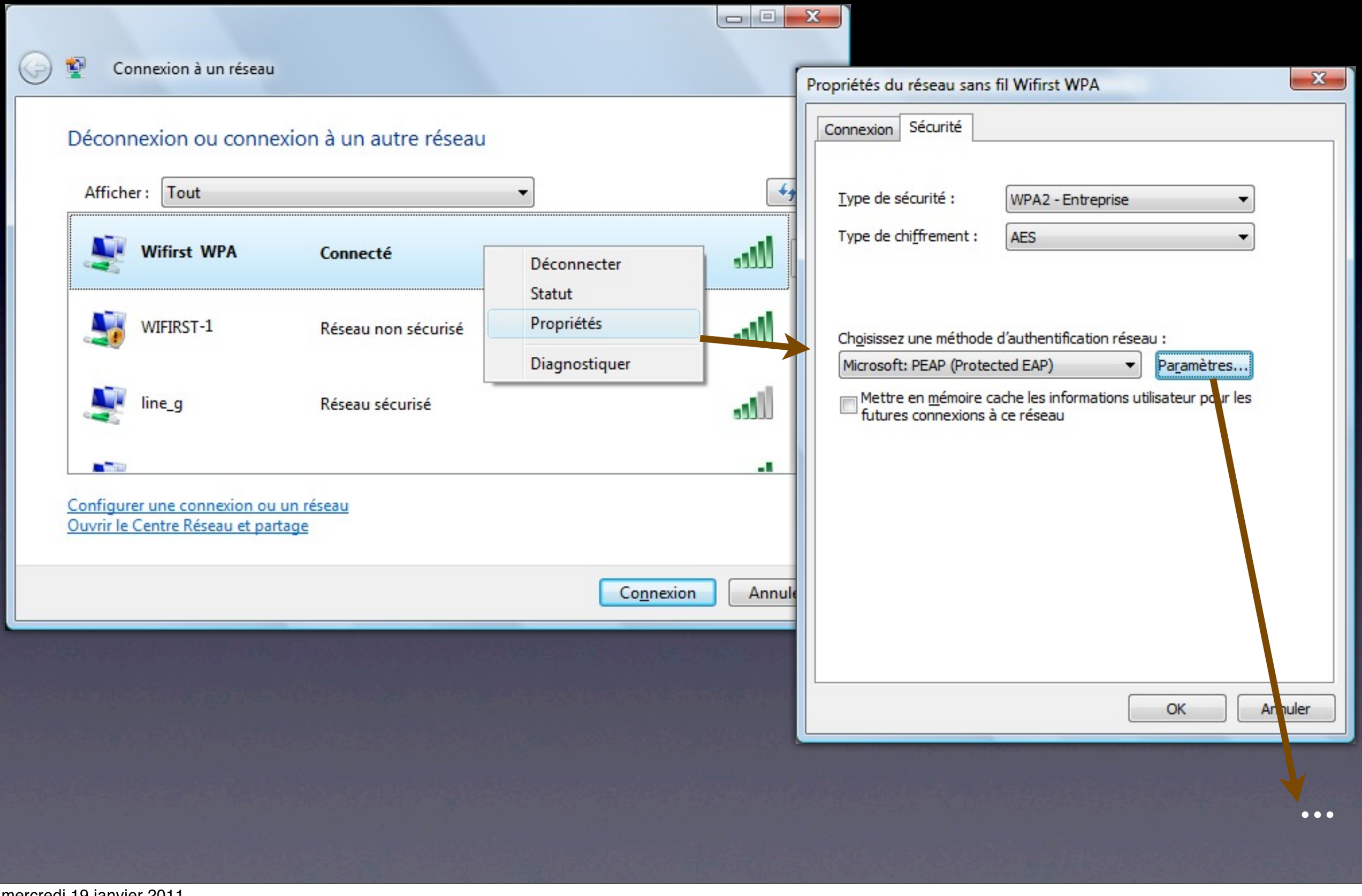
PEAP sous Windows



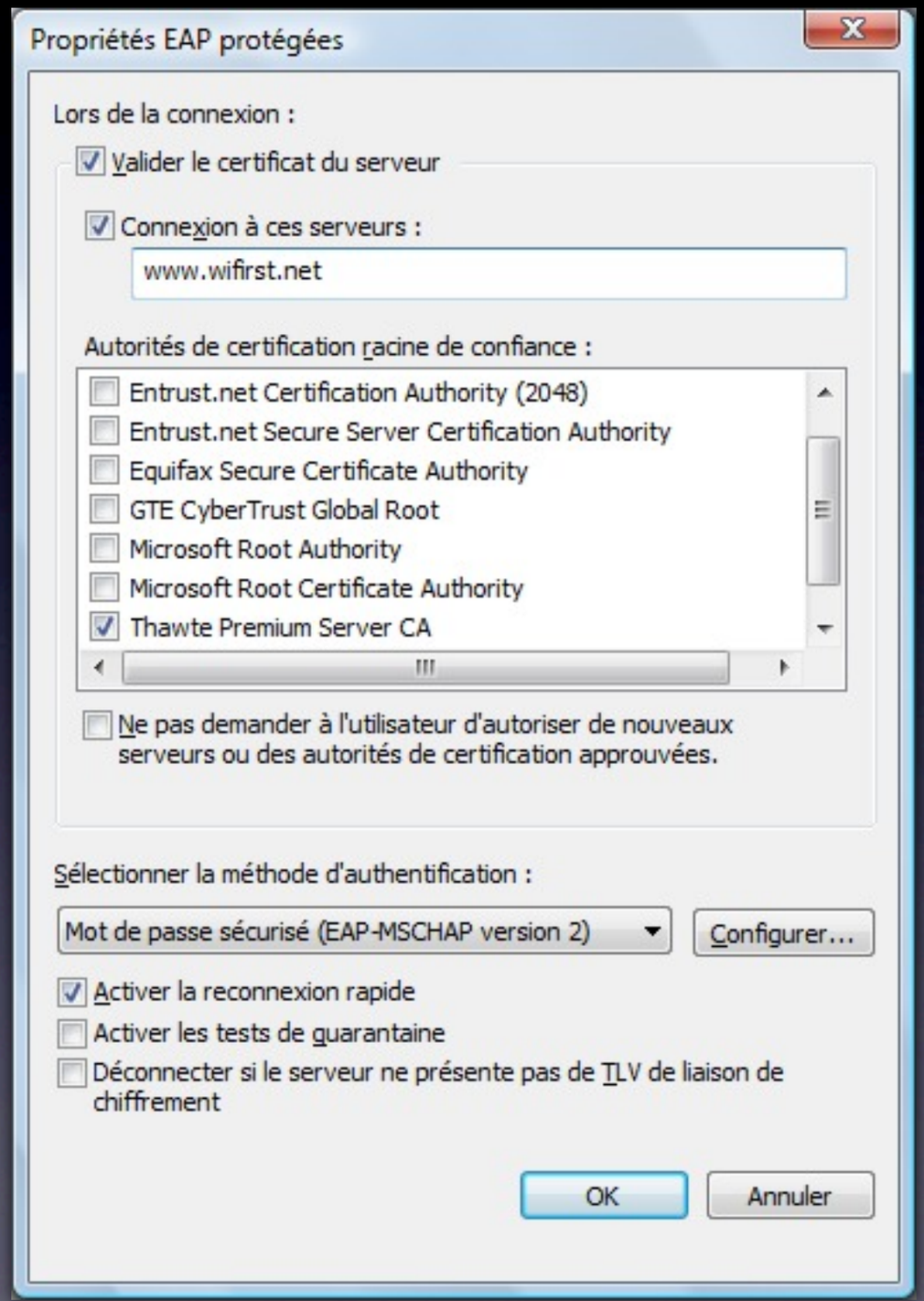
PEAP sous Windows



PEAP sous Windows



PEAP sous Windows



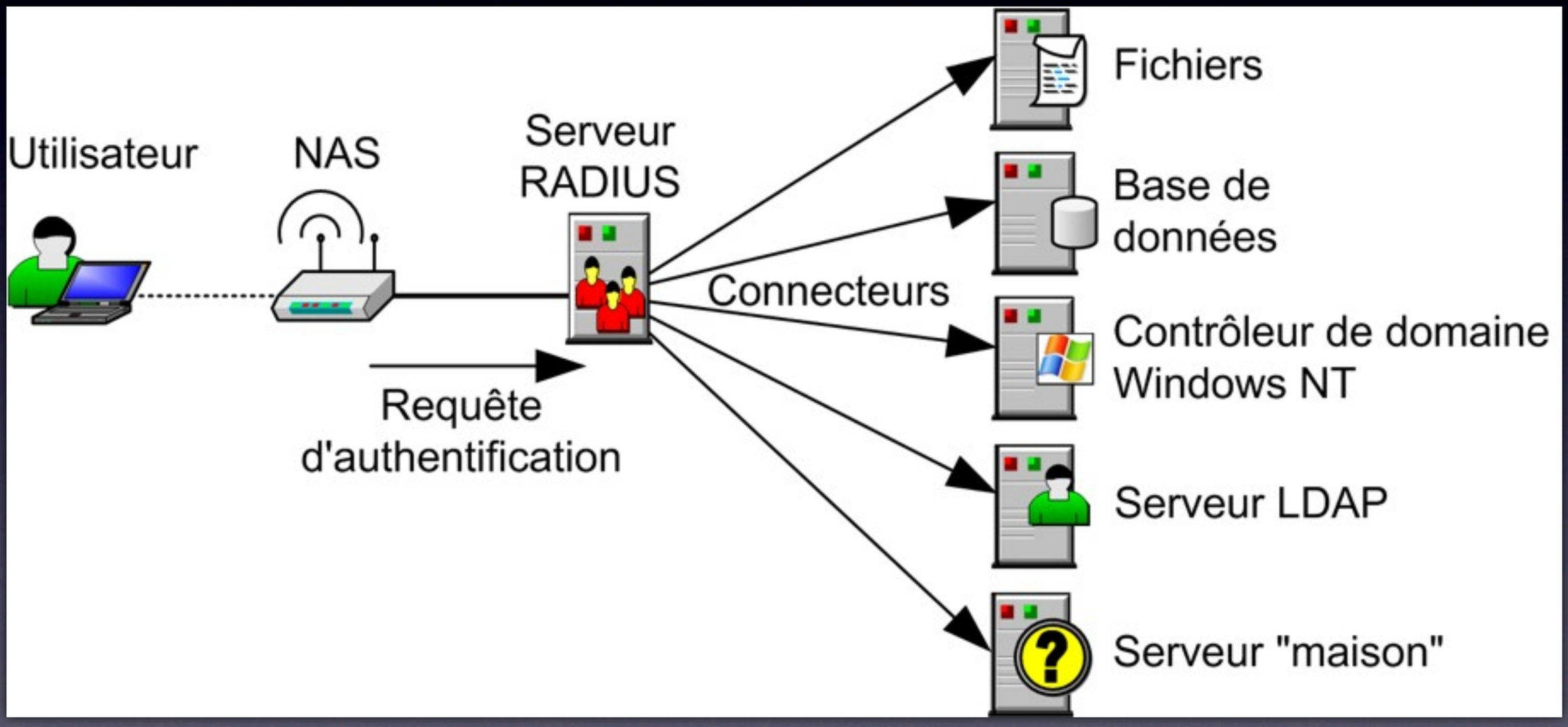
PEAP et accounting

- Le tunnel PEAP ne concerne que l'authentification, pas l'accounting
- L'identité externe est donc celle qui sera utilisée pour l'accounting
- L'attribut Chargeable-User-Identity peut régler ce problème

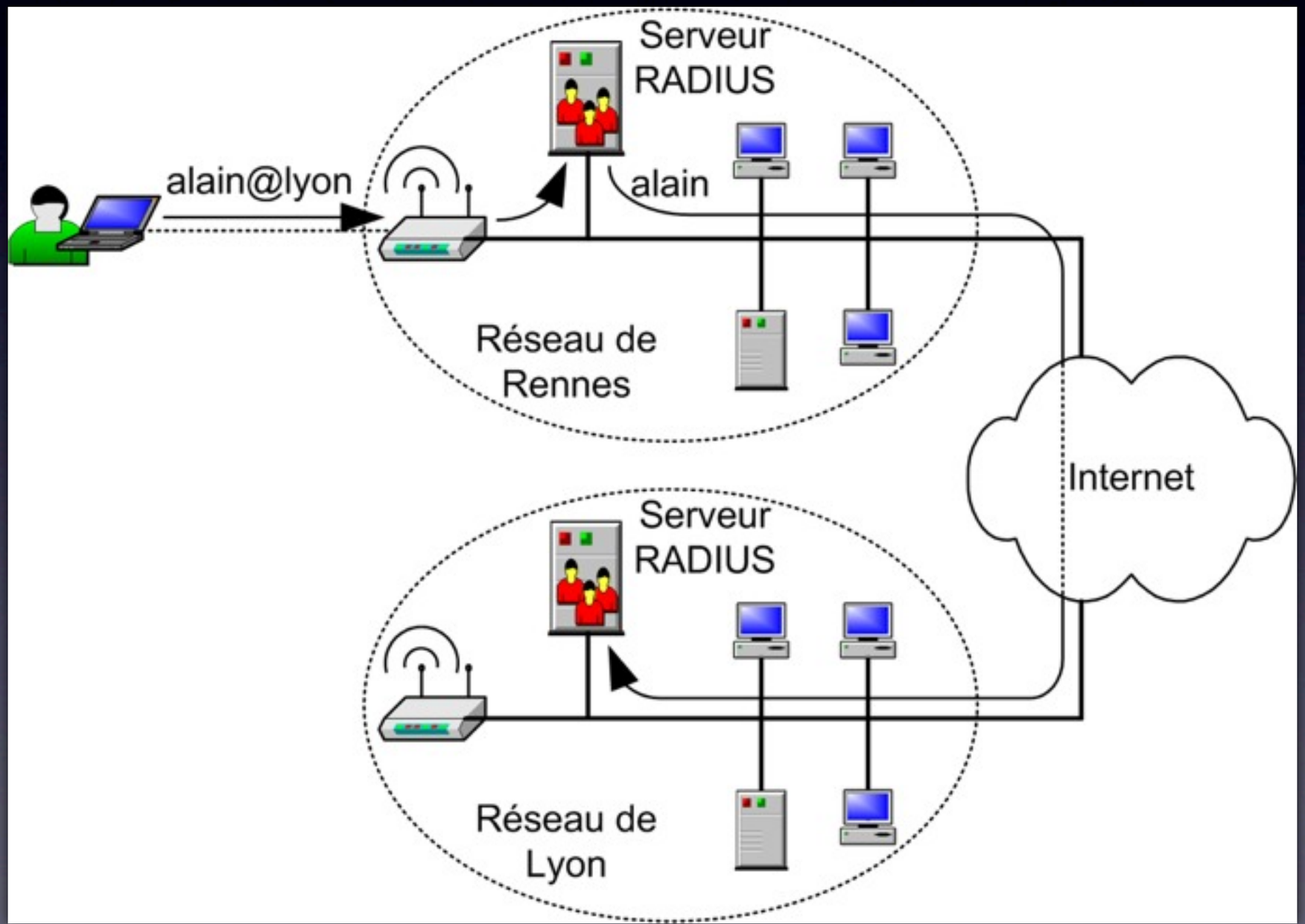
EAP/TTLS

- La méthode d'authentification EAP/TTLS est très similaire à la méthode EAP/PEAP
- Son gros inconvénient est de ne pas être gérée par défaut par Windows : il faut installer un logiciel appelé le «supplicant TTLS»
- PEAP ne peut «tunneliser» que du EAP. L'avantage de TTLS est de permettre aussi le PAP, ce qui permet au serveur de recevoir le mot de passe en clair. C'est parfois utile, comme nous le verrons.

Les bases de données d'identification



Le principe du *roaming* (itinérance)



Terminologie de roaming

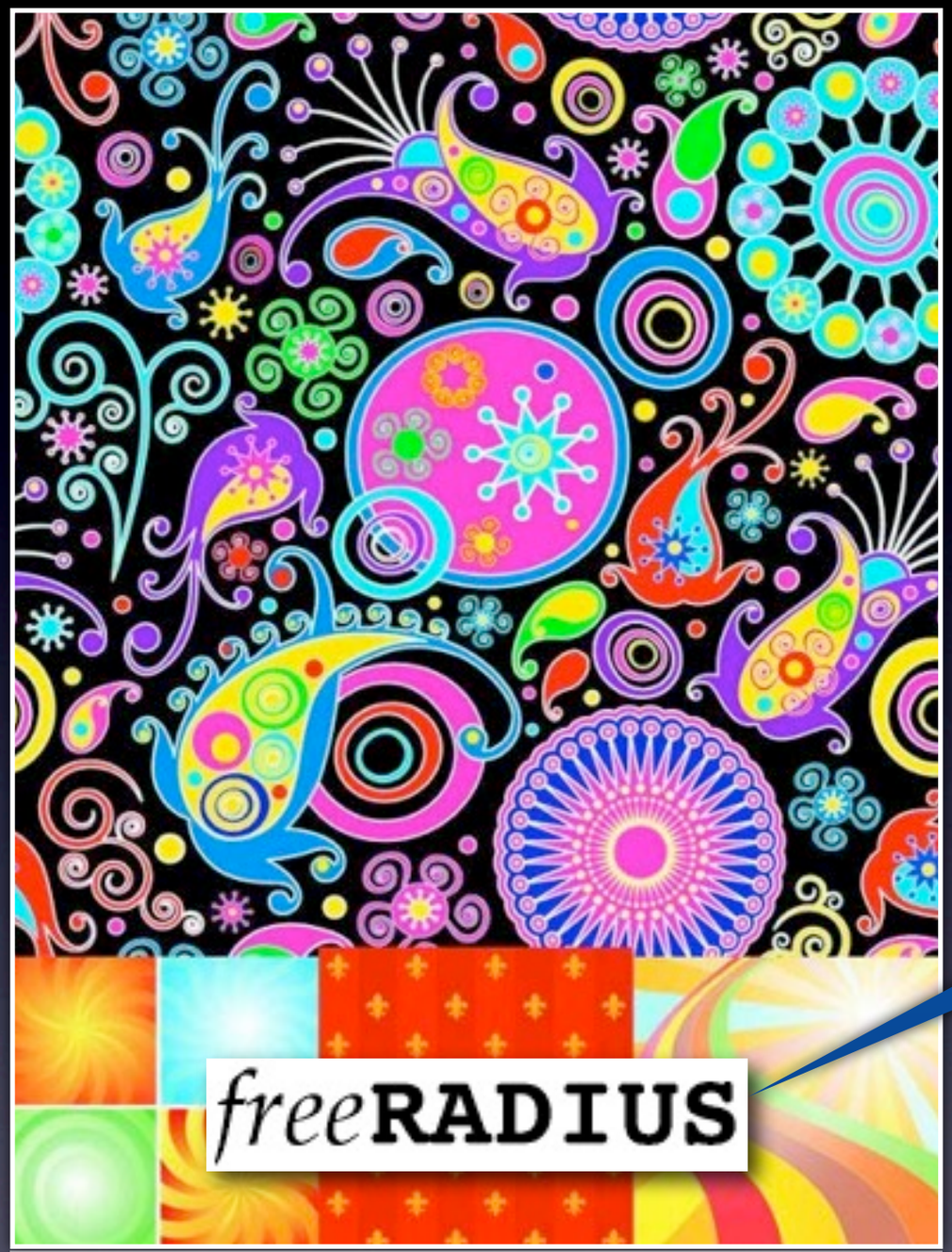
- Visited-Network : le réseau auquel l'utilisateur se connecte
- Home-Network : le réseau de provenance de l'utilisateur (là où son compte est configuré)
- Realm : partie de l'identifiant (*login*) de l'utilisateur qui indique à quel réseau il appartient :
  - `alain@lyon` dans l'exemple
  - mais le format peut être différent : `fti/d9fl3g`
- Home-Server : le serveur RADIUS dans lequel l'utilisateur est configuré
- Proxy-Server : le serveur RADIUS du réseau visité

Terminologie de roaming

- Si nous sommes le gestionnaire d'un réseau X, et que nous avons un accord d'itinérance (*roaming*) avec le gestionnaire d'un réseau Y, alors nous parlerons de :
  - Roaming-in (rentrant) : lorsqu'un abonné de Y se connectera sur notre réseau (Y nous doit des €)
  - Roaming-out (sortant) : lorsque l'un de nos abonnés se connectera sur le réseau de Y (nous devons à Y)
  - Réconciliation : lorsqu'on se mettra d'accord avec Y pour décider combien ils nous doivent et combien nous leur devons (en comparant les historiques)
  - Data Clearing House (DCH) : une entreprise dont le service consiste à s'occuper de la réconciliation

Tunnels et roaming

- Si l'on utilise la méthode PEAP ou TTLS dans un contexte de roaming, alors le Proxy-Server ne voit que l'EAP externe
- L'utilisateur doit donc configurer son identité externe de façon à ce que le Proxy-Server puisse rediriger les requêtes vers le bon Home-Server :
    - par exemple anonyme@lyon
- Si l'identité interne contient elle-même un realm, le Home-Server risquera de rediriger les requêtes internes au tunnel vers un autre serveur RADIUS : les données de ces paquets ne seront alors plus protégées par le tunnel TLS :
    - on désactive donc généralement le «proxying» pour l'intérieur des tunnels TLS.



Questions ?