# WiFi et réseaux locaux sans fil concepts et mise en œuvre

## Travaux pratiques
### Mise en œuvre de mécanismes de sécurité

**Frédéric Weis**
frederic.weis@univ-rennes1.fr

-

*Octobre 2018*

Au cours de ce TP, nous allons :

1. Démarrer un AP Cisco, et l'intégrer à un réseau Ethernet
2. Créer un SSID WiFi, d'abord « caché » puis « public »
3. S'associer une première fois à ce SSID dans ces deux versions
4. Utiliser le WPA « Personal » (chiffrement TKIP ou AES + authentification par mot de passe)
5. Utiliser le WPA « Enterprise » (chiffrement TKIP ou AES + authentification 802.1x EAP-TLS et EAP-PEAP)

## 1. Démarrage

Vous êtes connectés à un commutateur Ethernet commuté.

Chaque groupe dispose donc d'un PC Ethernet et d'un AP WiFi. Le routeur et le commutateur ont été configurés au préalable avant le démarrage du TP. Les adresses IP des AP WiFi ont été également paramétrées pour chaque groupe.

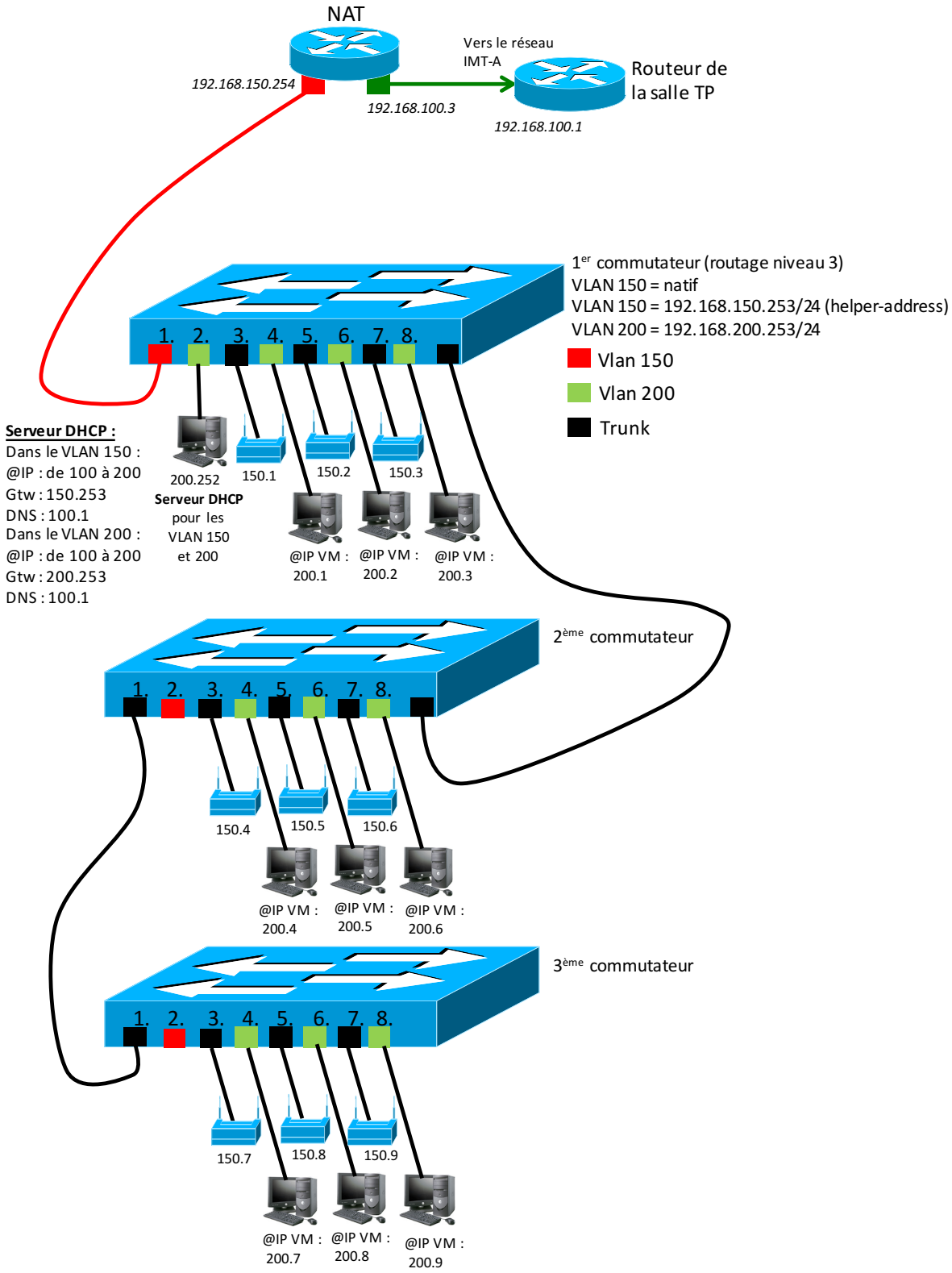
**Remarque 1** : X (1, 2, 3 …) correspond au numéro de chaque groupe.

**Remarque 2 :** Toutes les copies d'écran dans le sujet vous sont données « à titre d'exemple ». Vous devez bien entendu les adapter en fonction des paramètres que vous cherchez à configurer (utiliser les « bonnes » @IP, les « bons » numéros de VLANs etc.).

Un serveur DHCP se trouve dans le VLAN 200 et distribue des adresses dans la classe 192.168.200.X/24. Il est également capable de distribuer des adresses IP dans la classe 192.168.150.X/24 pour le VLAN 150.

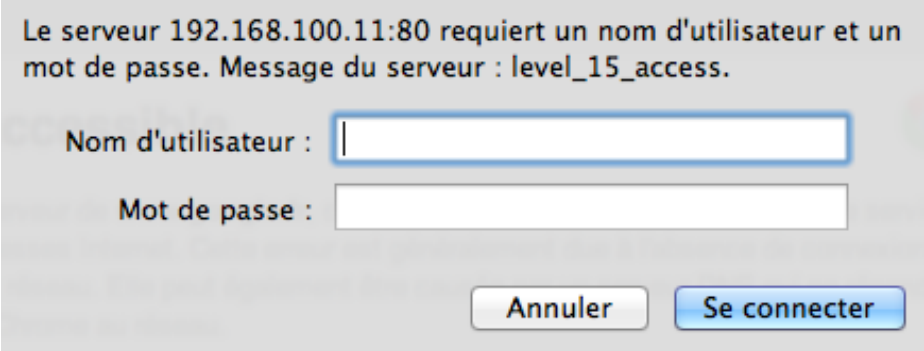
Le PC (PC groupe X sur la figure suivante) dont vous disposez va exploiter une machine virtuelle Linux qui va jouer le rôle de serveur Radius pour l'authentification WiFi. La configuration de cette machine virtuelle sera abordée dans la suite du TP.

La configuration peut être résumée de la manière suivante : (pour 9 binômes)


NAT
192.168.150.254
192.168.100.3
Vers le réseau IMT-A
Routeur de la salle TP
192.168.100.1
1er commutateur (routage niveau 3)
VLAN 150 = natif
VLAN 150 = 192.168.150.253/24 (helper-address)
VLAN 200 = 192.168.200.253/24
Vlan 150
Vlan 200
Trunk
1. 2. 3. 4. 5. 6. 7. 8.
Serveur DHCP :
Dans le VLAN 150 :
@IP : de 100 à 200
Gtw : 150.253
DNS : 100.1
Dans le VLAN 200 :
@IP : de 100 à 200
Gtw : 200.253
DNS : 100.1
200.252
Serveur DHCP pour les VLAN 150 et 200
150.1
150.2
150.3
@IP VM : 200.1
@IP VM : 200.2
@IP VM : 200.3
2ème commutateur
150.4
150.5
150.6
@IP VM : 200.4
@IP VM : 200.5
@IP VM : 200.6
3ème commutateur
150.7
150.8
150.9
@IP VM : 200.7
@IP VM : 200.8
@IP VM : 200.9

Configurez l'interface Ethernet de votre PC en configuration automatique DHCP, puis vérifiez qu'une configuration IP vous a bien été attribuée par le serveur DHCP du VLAN 200. Vérifiez ensuite que vous accédez bien à votre AP et « au reste de l'Internet » à partir de votre PC.

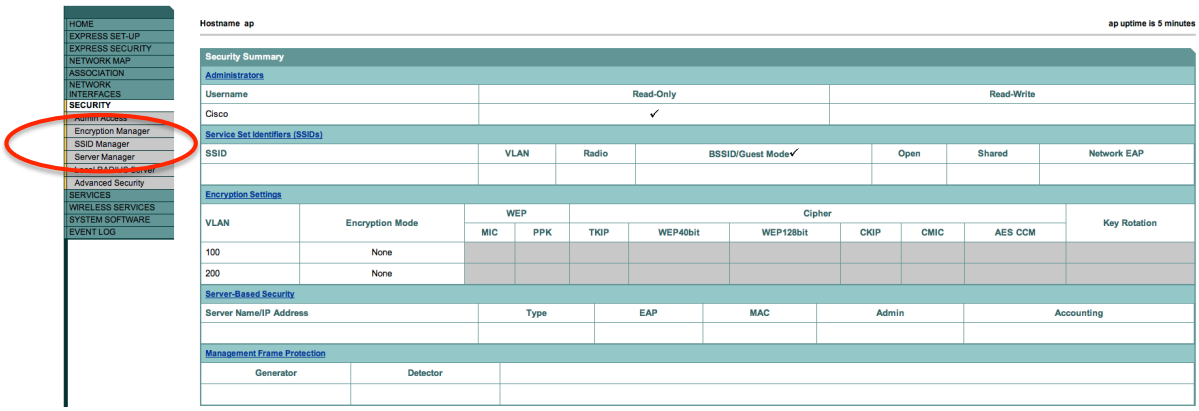
Connectez-vous, depuis votre PC, au serveur WEB interne de l'AP, en utilisant l'URL *http://192.168.150.x/*, login Cisco, mdp Cisco :



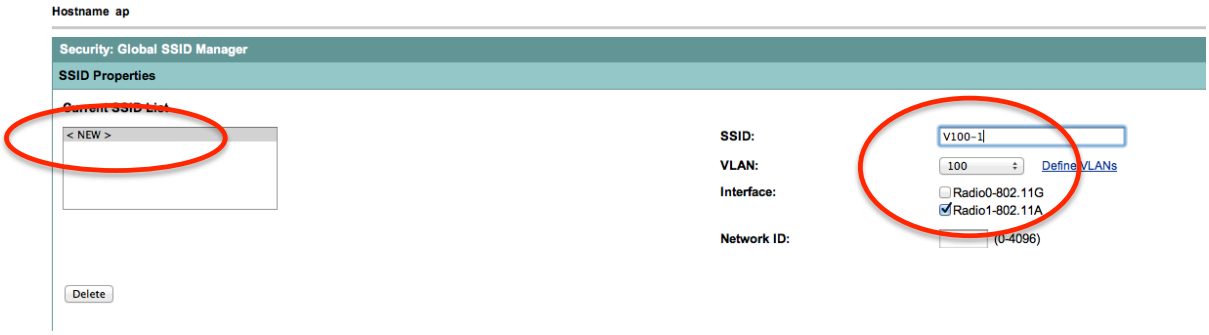

## 2. Gestion du SSID et premier rattachement

### 2.1. Création du SSID « caché »

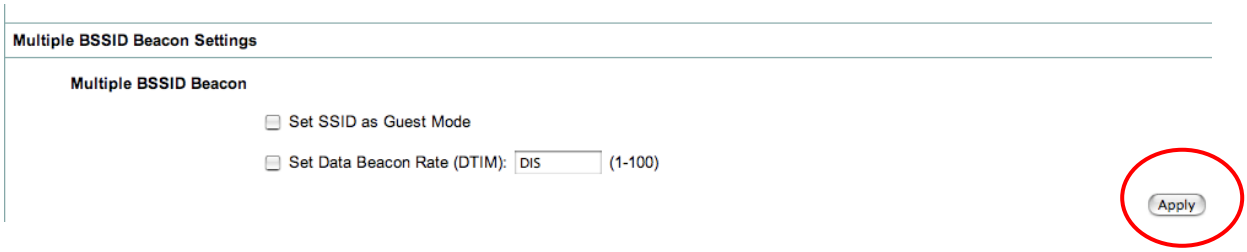
Définissez le SSID V150-X via l'onglet « Security -> SSID manager », en mode open, et sans chiffrement :




Ce SSID doit être lié au VLAN 150, que vous devez également définir dans l'AP (attention, la copie d'écran suivante est donnée à titre d'exemple). Notez bien qu'il s'agit d'un VLAN « natif ».

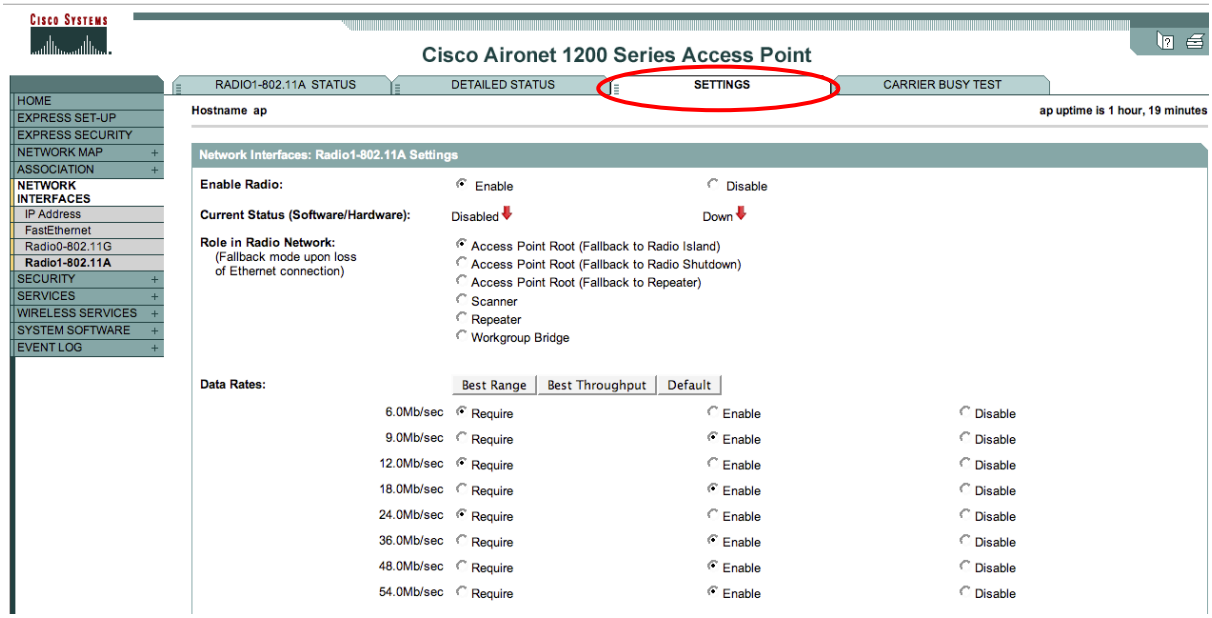



Descendre plus bas dans la page, et valider ces déclarations, en sélectionnant le bouton « Apply ». Attention, ce bouton est assez bas dans la page.

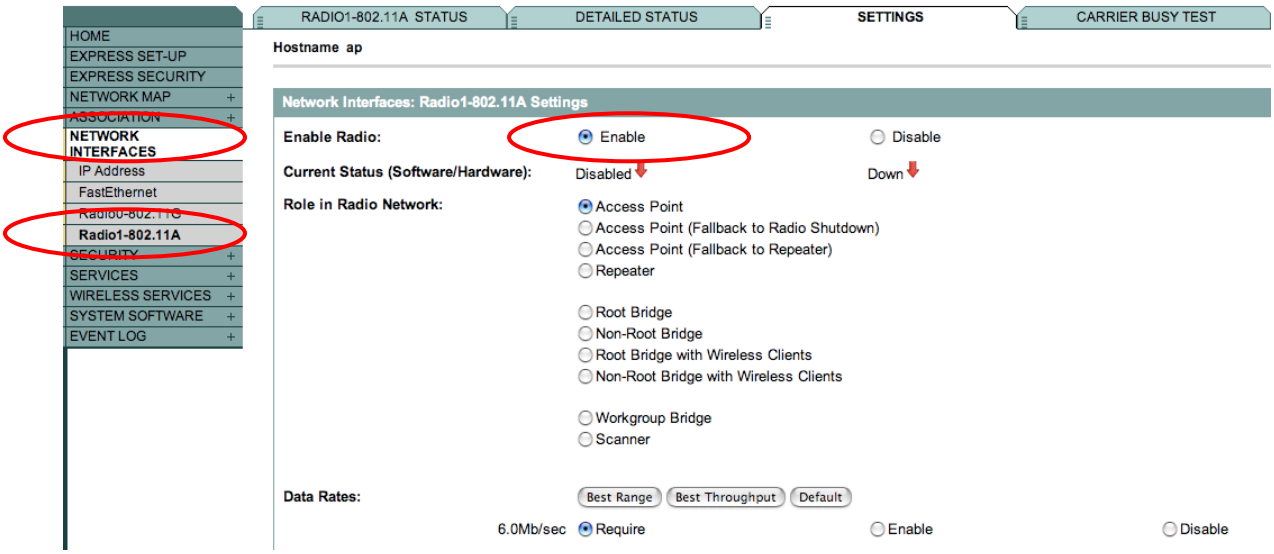



Il vous reste enfin à activer l'interface radio. Via l'onglet « Network Interfaces », activez l'interface radio 802.11a ou 80211b (en fonction du modèle de l'AP). Réduisez la puissance d'émission sur l'interface (si cela est possible).

Analysez rapidement la configuration radio : sélection DFS, possibilité de gestion 802.11d, activation des différents seuils de débits …

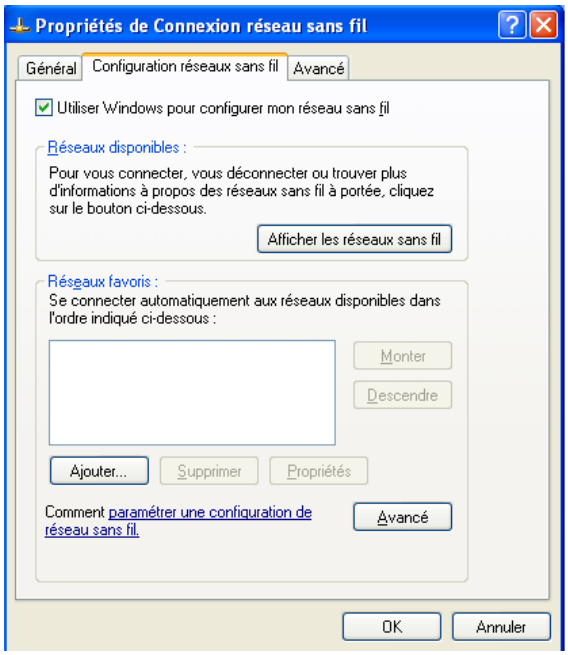



Par exemple, pour « lever » l'interface 802.11a, on sélectionne l'option **NETWORK INTERFACES** du menu gauche. Puis sélectionnez **Radio1-802.11A**, puis l'onglet **SETTINGS**, et sélectionner finalement l'option **Enable**, et le bouton **Apply** se trouvant plus bas dans la page (l'activation de l'interface peut prendre un peu de temps).




### 2.2. Attachement au SSID

Le SSID V150-X est « caché ». Il est donc nécessaire de le déclarer dans les réseaux favoris de votre station mobile à la première connexion. Par exemple, sur une station Windows, vous pouvez le faire par exemple via l'option « Propriétés » sur votre interface WiFi (accessible via un « clic bouton droit » sur cette interface WiFi) :



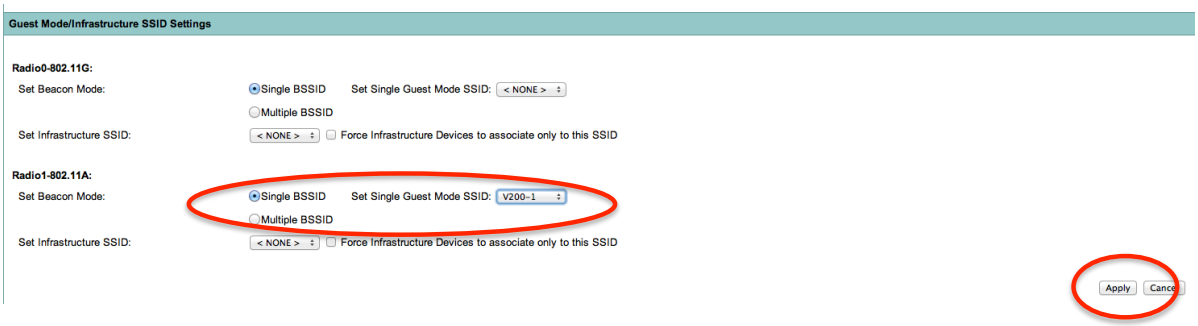

Notez que vous devez déclarer que le SSID peut être accroché « même s'il est caché ». Votre carte WiFi va lancer une série de trames 802.11 « probe request » sur toutes les bandes de fréquence qu'elle supporte, en recherchant le SSID V150-X (qui est dans votre cas son unique réseau favori).

Depuis votre terminal WiFi (Windows, MAC OS, Iphone, Android etc.), vérifiez alors que la connexion est active, et que le serveur DHCP vous a délivré une configuration WiFi dans le VLAN 150 (plage d'@ IP 192.168.150.X/24).

### 2.3. Diffusion du SSID dans les trames balises

Supprimez le SSID V150-X de vos réseaux favoris à partir des propriétés de votre carte WiFi (« oubliez » le réseau WiFi).

Nous allons maintenant déclarer le SSID comme « public ». Autrement dit, on va le diffuser dans les trames *beacon* de l'AP, afin de le rendre automatiquement visible par les clients WiFi. Pour ce faire, procédez comme suit (options se trouvant tout en bas de la page Web) :

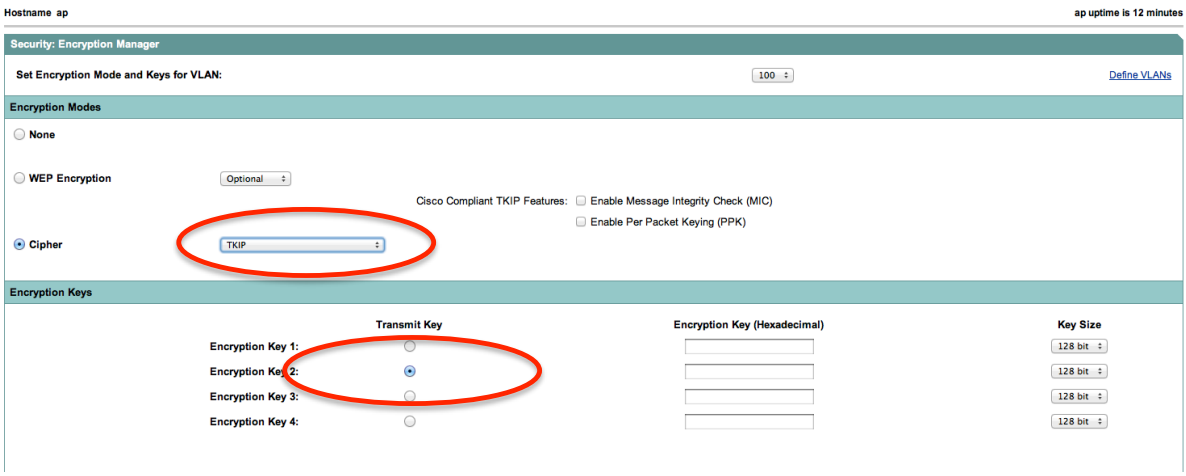



Sans passer par les propriétés de votre carte WiFi, le SSID doit être cette fois-ci visible automatiquement par votre PC. Votre carte va tout simplement scanner l'ensemble des bandes de fréquence qu'elle supporte, et rend visible à l'utilisateur l'ensemble des SSID publics. Cliquez sur le SSID V150-X, et vérifiez que vous l'accrocher correctement.

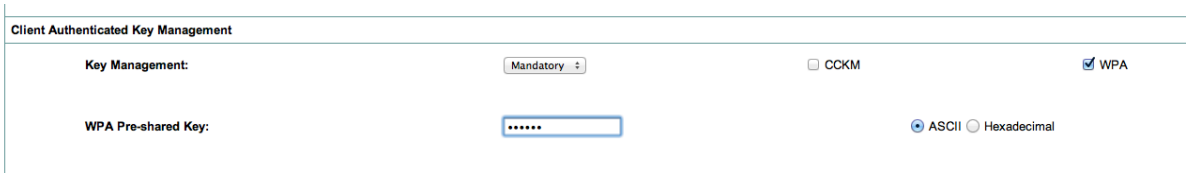
## 3. Mise en œuvre TKIP (WPA personal) sur le SSID V150-X

Nous allons protéger l'accès au SSID V150-X par un mot de passe. Ce dernier sert également à chiffrer la liaison sans fil. C'est de type de protection que vous utilisez sur la *box* de votre domicile.

Via l'onglet « SECURITY -> Encryption Manager » :

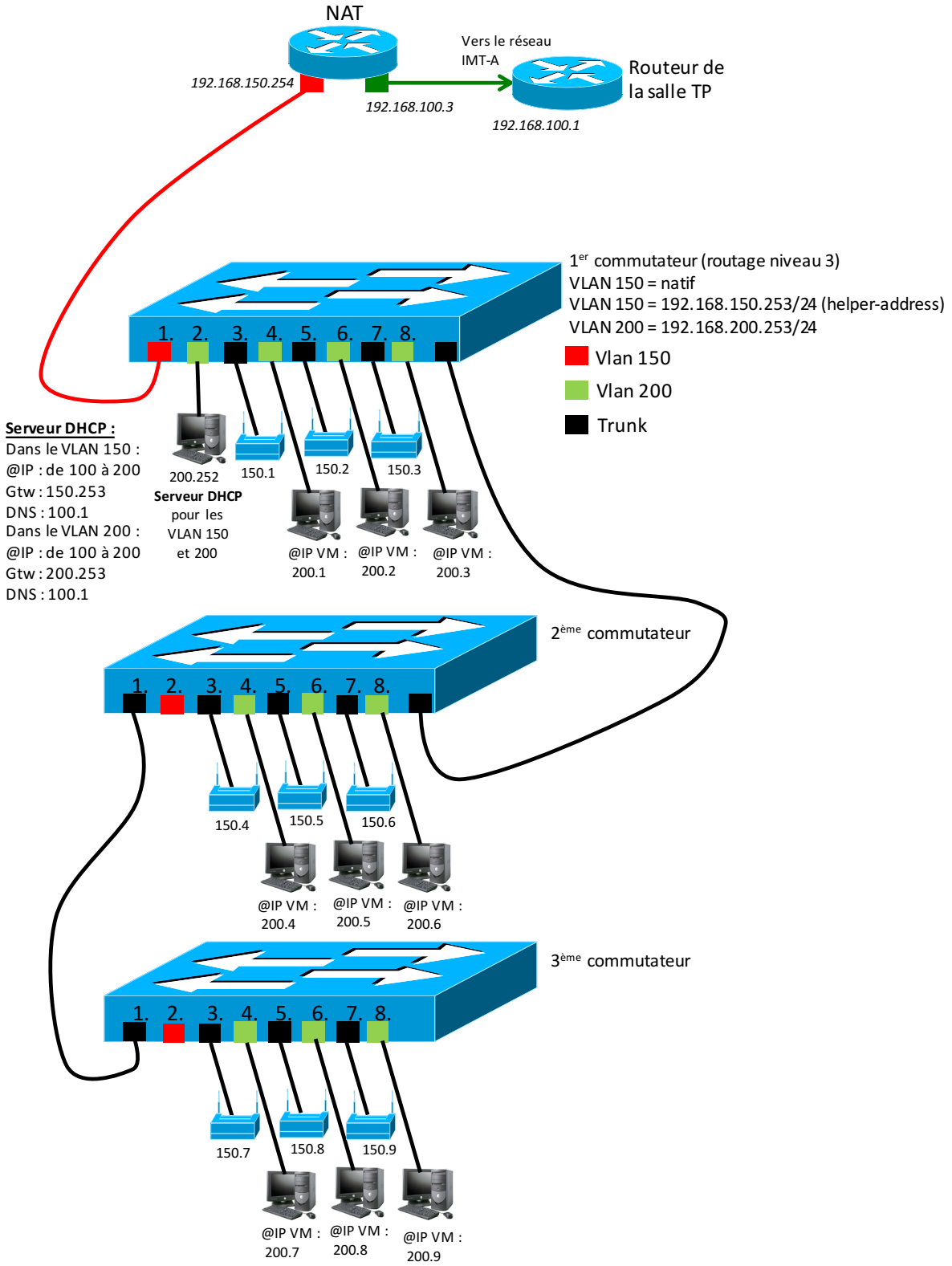



Puis revenir à la configuration de votre SSID à ce niveau :




Le mot de passe sélectionné doit comporter au moins 8 caractères, par exemple `tpsecret`.

Côté




client, vous devez maintenant vous attacher au SSID via WiFi. Un conseil : supprimez le SSID de vos propriétés réseaux sous Windows, et reconnectez-vous. Cela impose à votre ordinateur de « renégocier » les paramètres de sécurité imposés par l'AP.

Comment validez-vous votre configuration ?

## 4. Activation de WPA enterprise (802.1x + chiffrement TKIP) sur le SSID V200-X

Dans ce chapitre, nous allons mettre en œuvre chiffrement TKIP + authentification 802.1x, EAP-TLS dans un premier temps, puis EAP-PEAP dans une deuxième étape.

### 4.1. Un peu de théorie autour d'EAP-TLS

Tout comme le protocole https, EAP-TLS s'appuie sur le protocole TLS pour gérer les mécanismes d'authentification. Cette méthode utilise des **certificats électroniques X.509** côté client 802.11 et côté serveur Radius. Un certificat est un document électronique contenant un certain nombre d'information (nom du propriétaire, période de validité, clef public du certificat, signature numérique (empreinte via hashage + cryptage) du certificat …). Ces informations vont être utilisées par une personne pour prouver son identité.

Plus précisément, on s'appuie sur une autorité de certification (CA). Une autorité de certification est une organisation qui délivre des certificats électroniques à une population. Un CA possède lui-même un certificat (le plus souvent « autosigné », c'est à dire qu'il a généré lui-même), et utilise ce certificat « racine » pour créer les certificats qu'il délivre ensuite.

Une personne se voit donc délivrer un certificat par le CA, qu'elle installe localement. Ce certificat lui permettra de prouver son identité à une entité distante, à condition que cette même entité « fasse confiance » à ce CA. Pour cela, il faut installer localement le certificat « racine » du CA, et déclarer ce certificat comme étant « de confiance ». Et c'est ce couple certificat de la personne + certificat racine du CA « de confiance » qui va permettre de valider le fait que **le certificat reçu a bien été émis par un CA « de confiance »**.

Pour réaliser cette partie, nous avons donc besoin :

1. D'un client supportant EAP-TLS et les certificats X.509
2. D'un serveur Radius supportant EAP-TLS et les certificats X.509
3. D'une autorité de certification (CA) pour générer les certificats X.509 racine, client et serveur

Dans cette partie du TP, nous allons :

1. Générer un certificat « racine » pour le CA
2. Générer des certificats pour le client 802.11 et le serveur Radius
3. Installer les deux certificats (équipement + racine) au niveau du client 802.11 et du serveur Radius
4. Configurer l'AP pour relayer les données EAP vers le serveur Radius
5. Lancer le serveur Radius, et valider le processus d'authentification

Ainsi, via EAP-TLS, chaque partie possède un certificat pour prouver son identité. L'avantage de cette méthode est qu'elle est très sécurisée, les certificats étant échangés via un tunnel crypté. Son principal inconvénient est qu'elle est lourde à mettre en œuvre, notamment au niveau de la gestion des certificats (création, suppression, révocation, distribution …). Tous ces mécanismes reposent sur une « infrastructure de gestion des clefs » (PKI : Public Key Infrastructure), complexe à déployer et à maintenir.

### 4.2. FreeRadius et openSSL

FreeRadius est une implémentation d'un serveur Radius, sous licence GPL, fonctionnant sur la plupart des Unix. Le code source est disponible sur http://www.freeradius.org. FreeRadius supporte la plupart des mécanismes d'authentification EAP, notamment EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP … Pour gérer EAP-TLS, EAP-TTLS et EAP-PEAP, freeRadius a besoin des fonctions offertes par le protocole TLS. Il fait donc appel à un programme externe : openSSL (http://www.openssl.org). OpenSSL est un ensemble de bibliothèques écrit en C, offrant une implémentation des protocoles SSL/TLS, ainsi que des fonctions de manipulation des certificats X.509.

Dans le cadre de ce TP, openSSL sera utilisé

1. Par freeRadius, pour réaliser les appels EAP-TLS
2. Comme autorité de certification pour créer les certificats X.509

Ces deux logiciels vont sont fournis via une machine virtuelle installé sur votre PC. Lancez VirtualBox.

Vous devez ensuite respecter les étapes suivantes :

- Avant de démarrer cette image, assurez-vous que la configuration de l'interface réseau est correcte : 1ère interface de votre PC en mode pont, ce qui vous permettra de disposer d'un serveur accessible comme le serait un OS serveur natif.
- Démarrez la VM.
- Connectez vous : `user` + `bonjour`, puis `sudo su`, mot de passe `bonjour`

Attention, utilisez la commande `halt` si vous souhaitez arrêter cette machine Linux.

- Editez le fichier `/etc/network/interfaces` (utilisez `nano` si vous êtes allergique à l'éditeur `vi`) et validez votre configuration IP : 192.168.200.X/24, routeur par défaut 192.168.200.253.
- Redémarrez votre interface réseau : `/etc/init.d/networking restart`

- Configurez votre serveur DNS dans le fichier `/etc/resolv.conf`, ligne `nameserver`, avec l'adresse 192.168.100.1.
- Vérifiez finalement la connectivité vers Internet : ping www.google.fr

### 4.3. Quelques explications sur le format des certificats

Les certificats X509 peuvent être encodés suivants deux formats : DER et PEM. Le format DER correspond à un certificat encodé en **binaire**, alors que le PEM correspond à un format ASCII éditable. Le format à utiliser (binaire ou ASCII) dépend du logiciel exploitant le certificat. A noter qu'il est possible d'utiliser DER et PEM comme extension pour les certificats.

Il existe des extensions particulières pour désigner les certificats :

- .p12 désigne les certificats PKCS#12. Le certificat contient la clé privée du destinataire du certificat ainsi que le certificat associé. Il peut contenir éventuellement le certificat de l'autorité racine (ce n'est pas le cas dans ce TP).
- .crt et .cert sont des extensions utilisées pour désigner un certificat et peuvent être exigées par certains systèmes d'exploitation. Le certificat peut être encodé au format PEM ou DER.

### 4.4. Génération des certificats X.509 pour le client WiFi et le serveur Radius

Il s'agit ici de reproduire ici quelques mécanismes propres à une PKI. Vous allez générer trois certificats : un pour le client, un pour le serveur Radius, et un certificat racine qui va permettre au client et au serveur de « déclarer » leur confiance à votre autorité de certification.

La manipulation des commandes offertes par openSSL pour créer des certificats X.509 est complexe. Nous utilisons trois scripts de génération : **CA.root, CA.clt et CA.svr** installé dans le répertoire `/etc/certgen`.

Chaque script produit trois certificats : .p12, .pem et .der.

Ces trois commandes exécutées **sans paramètre** vous indiquent en retour quels sont les paramètres attendus en entrée. Commencez par en prendre connaissance.

Vous devez utilisez des mots de passe différents pour protéger les clés privées des différents certificats, par exemple :

- Clé privée de l'AC protégée par « secretAC »
- Clé privée du client protégée par « secretclient »
- Clé privée du serveur protégée par « secretserver »

A noter que les scripts exécutés créent un résumé dans le fichier `RESUME` dans `/etc/certgen`.

Ces trois scripts s'appuient par défaut sur les informations du fichier « openssl.cnf » : nom de l'utilisateur, @mail, nom de l'organisation … Toutes ces informations seront ensuite utilisées pour renseigner les attributs des certificats. Ces scripts sont exécutés à titre d'exemple, dans le cadre de notre autorité de certification. Bien entendu, si on cherche à mettre en œuvre une

véritable PKI, les commandes openSSL peuvent être utilisées en conjonction avec d'autres langages (Php, perl …) et des environnements Web permettant d'assurer la distribution des certificats.

Une fois les certificats créés, la commande `./INSTALL-client` *`nom_du_certificat_client`* installe les certificats pour le client (CA+client) dans le répertoire du serveur FTP (`/home/ftp`) de votre VM. La commande `./INSTALL-serveur` *`nom_du_certificat_serveur`* installe les certificats (CA+serveur) dans le répertoire `/etc/freeradius/certs` du serveur Radius.

Vous devez effectuer les opérations suivantes (en les analysant pour bien les comprendre) :

- Placez vous dans le répertoire `/etc/certgen`.
- Supprimer d'anciens certificats dans ce répertoire via la commande `./PURGE`.
- Créez un certificat serveur de nom `server` et d'identité `server`.
- Créez un certificat client de nom `client` et d'identité `usermobile`.
- Installez les certificats pour l'export FTP et le la configuration du serveur Radius.

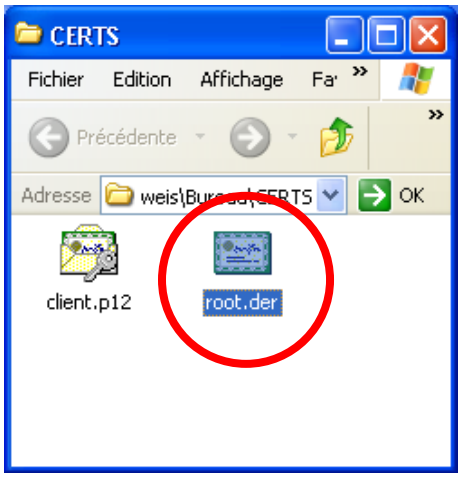
### 4.5. Installation des certificats côté client WiFi

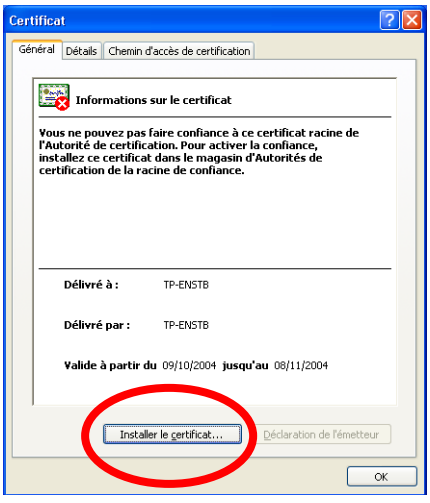
L'exemple d'installation vous est donné ici pour une station Windows. Il peut tout à fait être appliqué sur un Mac, un PC Linux ou sur un Smartphone Android ou Iphone.

Deux fichiers générés par les scripts précédents sont nécessaires côté client Windows ou MAC : **root.der** (certificat du CA), et **client.p12** (fichier contenant les informations nécessaires pour installer le certificat du client). Sous Linux, il faut utiliser les fichiers **root.pem** et **client.p12**, alors qu'Android demande les fichiers root.crt (au format DER) et client.p12.

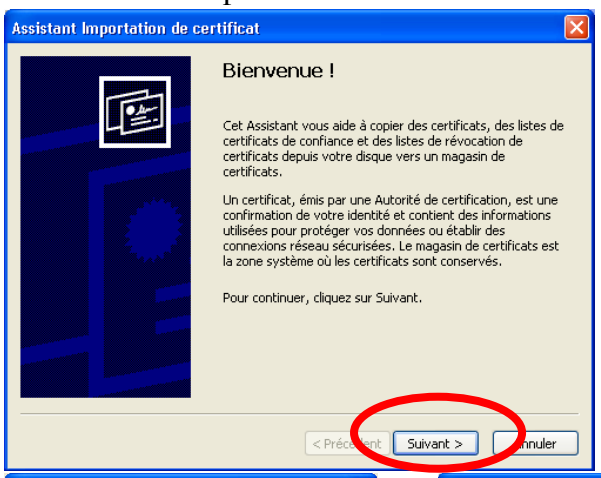
En théorie, ces fichiers doivent être transmis via un canal sûr sur le disque du client : tunnel chiffré, clef USB … Ici, vous pouvez les récupérer via le protocole ftp, et le compte `anonymous` (un ftp public sans mot de passe). Ainsi, lancez une connexion vers l'URL *ftp://@IP de votre serveur* depuis le navigateur de votre PC.

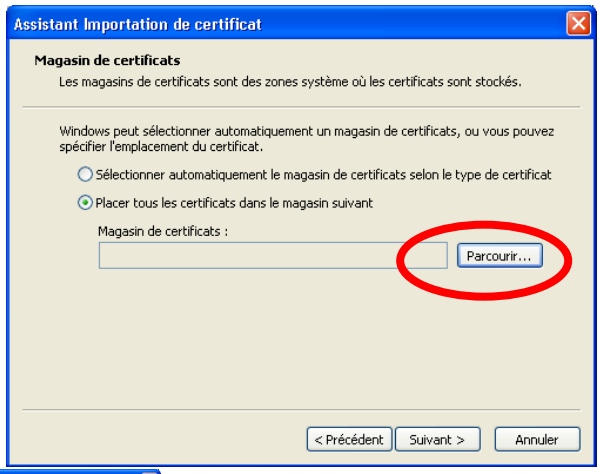
Une fois ces deux fichiers récupérés, cliquez sur le certificat du CA :

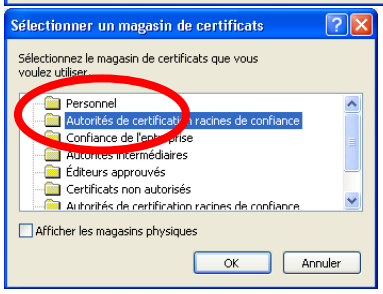


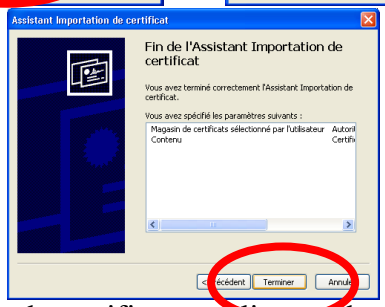



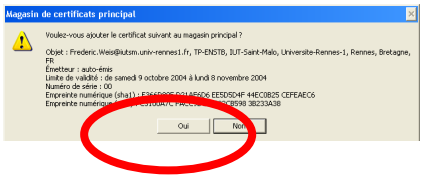
Vous constatez que vous ne faites pas confiance à ce CA. Il faut maintenant installer ce certificat. Les étapes suivantes sont nécessaires :



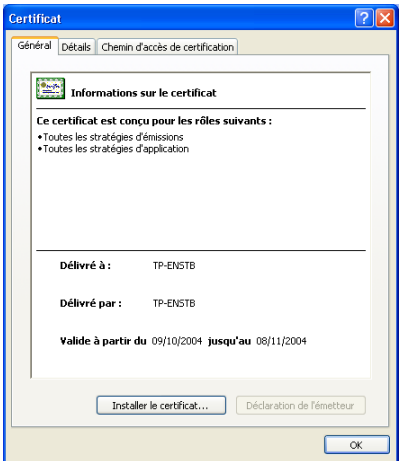



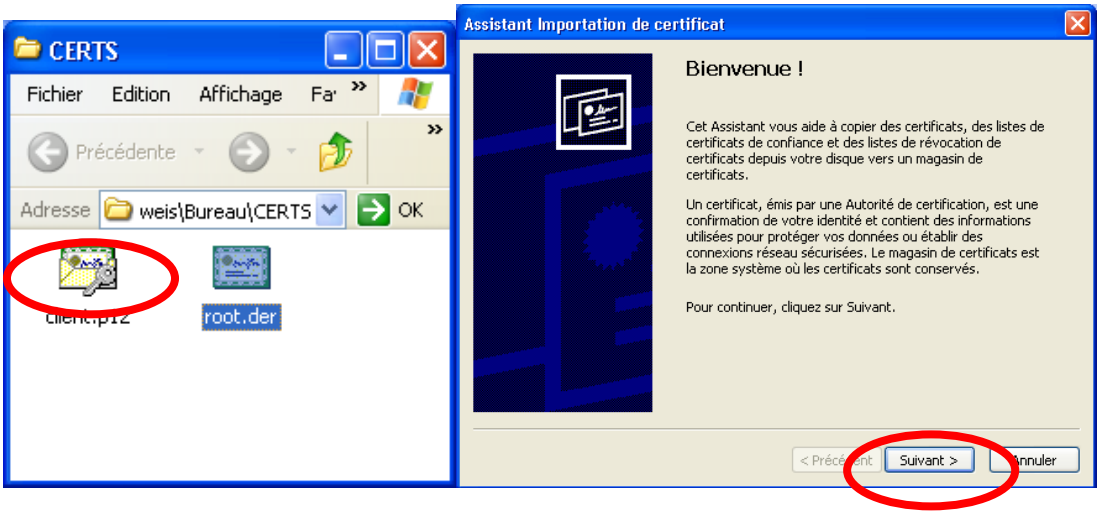



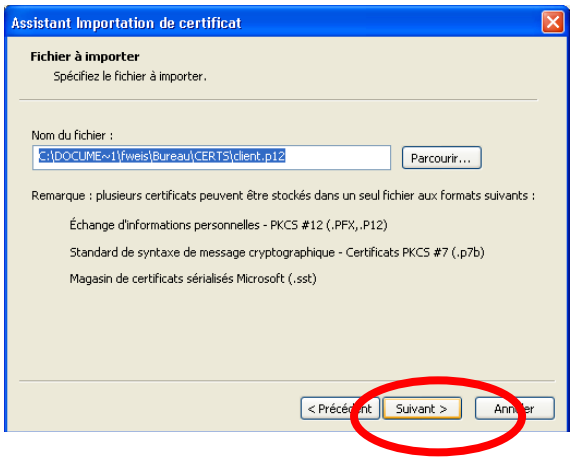



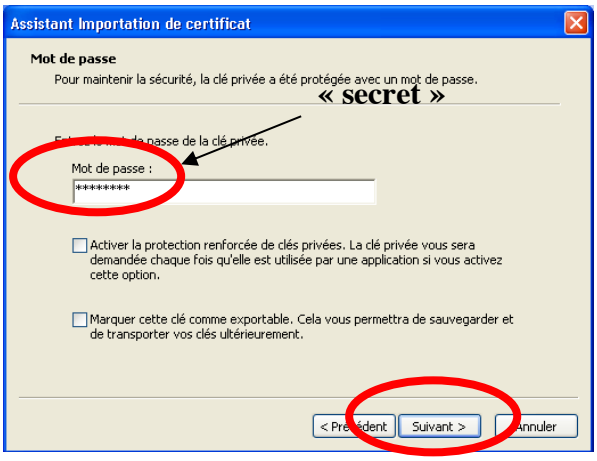

Vous pouvez vérifier l'installation du certificat, en cliquant de nouveau sur « root.der » :

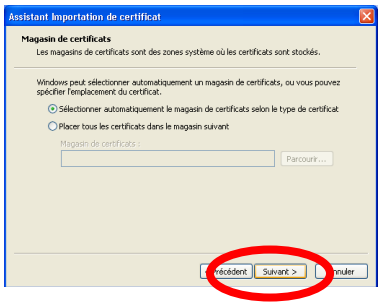


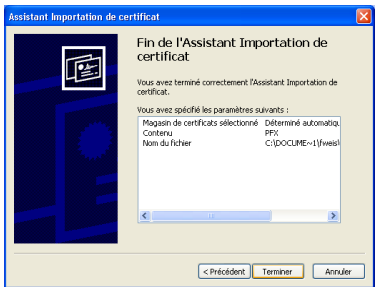

Il faut ensuite installer le certificat client :

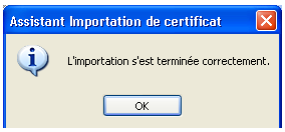


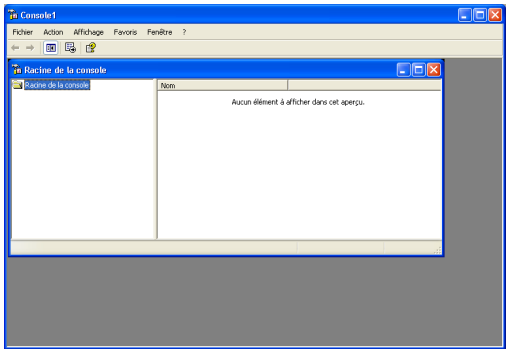



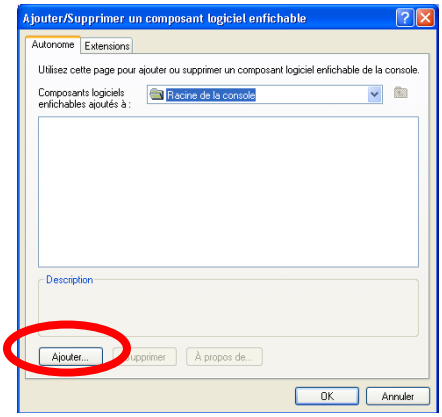



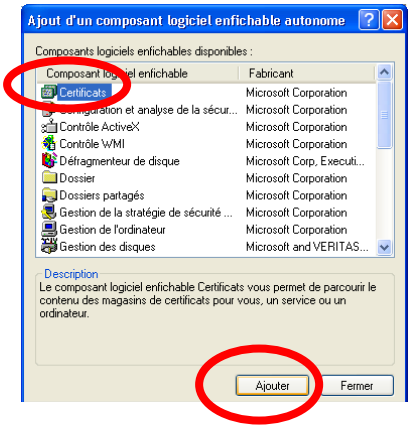



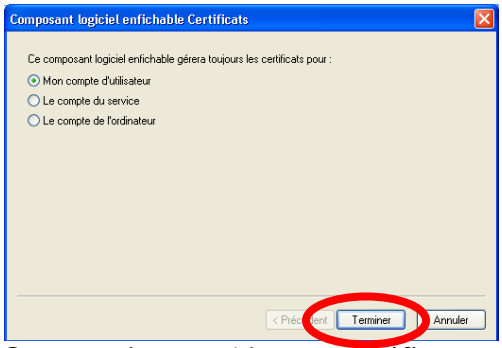

Les certificats installés sous windows peuvent être accédés via la commande « mmc » (lancée comme une commande DOS) :



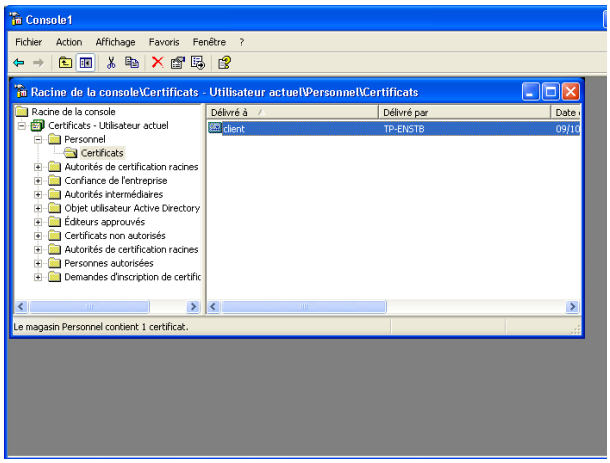
Il faut ensuite choisir le sous-menu « Ajouter / Supprimer un composant logiciel enfichable » :

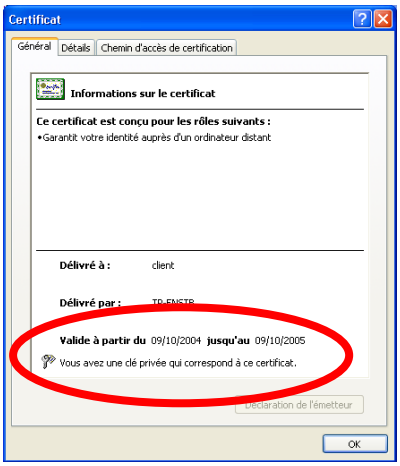


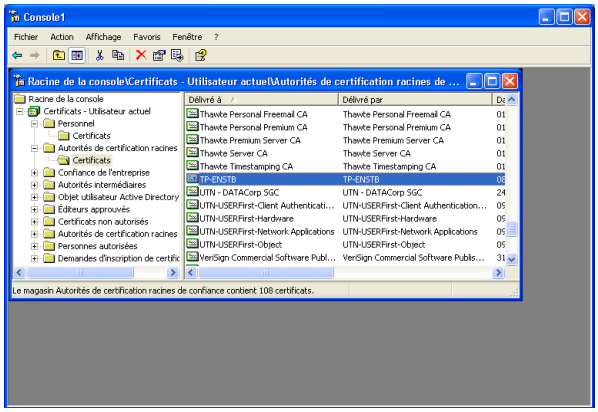



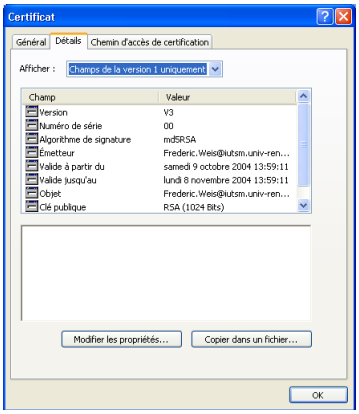




On peut alors accéder aux certificats personnels, ainsi qu'aux autorités de certification de confiance installée sur votre station.



On peut utiliser cet utilitaire pour supprimer les certificats.

### 4.6. Installation des certificats côté serveur, et lancement du serveur radius

L'ensemble des fichiers de configuration du serveur Radius se trouve dans le répertoire `/etc/freeradius`. Les deux certificats serveur et racine (serveur.pem et root.pem) doivent être installés dans le répertoire `/etc/freeradius/certs`. Il faut ensuite modifier trois fichiers du répertoire `/etc/freeradius` :

- **eap.conf** : configuration d'EAP
- **clients.conf** : configuration des APs ou commutateurs relayant EAP et autorisé à contacter le serveur Radius
- **users** : configuration des utilisateurs à authentifier

Dans le fichier **eap.conf**, on spécifie l'emplacement des certificats, et le type de version d'EAP utilisée.

```
default_eap_type = tls
tls {
                        private_key_password = secretserver
                        private_key_file = ${raddbdir}/certs/server.pem
                        certificate_file = ${raddbdir}/certs/server.pem
                        CA_file = ${raddbdir}/certs/root.pem
                        dh_file = ${raddbdir}/certs/dh
                        random_file = ${raddbdir}/certs/random
                        fragment_size = 1024
                        include_length = yes
                        check_crl = no
                }
```

Dans le fichier **clients.conf**, on définit l'AP et le commutateur comme équipement autorisé à relayé des messages EAP vers le serveur Radius. Par exemple :

```
client 192.168.150.0/24 {
        secret          = tp
        shortname       = ap-wifi
        nastype         = other
}
```

Important : le paramètre « secret » (=tp dans l'exemple) est un mot de passe partagé avec l'AP, qui va être utilisé pour chiffrer les messages Radius échangé entre l'AP et le serveur. Il doit donc être configuré avec une valeur identique, au niveau de l'AP WiFi.

Dans le fichier **users**, on spécifie la liste des utilisateurs autorisés à se connecter. Ainsi, pour le certificat « client » généré précédemment, on ajoute la ligne suivante :

```
« client » Auth-Type := EAP, EAP-Type := EAP-TLS
```

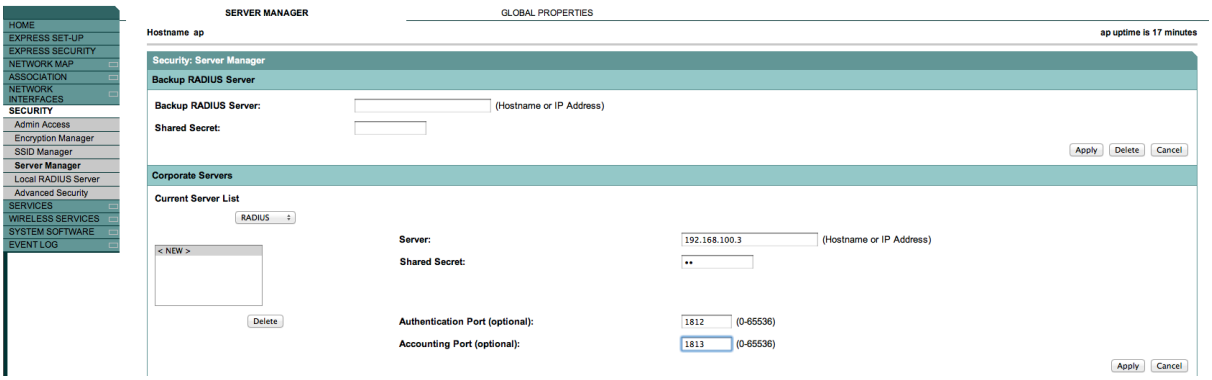
Après cela, vous pouvez lancer le serveur Radius :

`freeradius -X`, le paramètre –X est optionnel et lance les messages de *debug*.

Votre serveur Radius attend maintenant vos demandes de connexion.

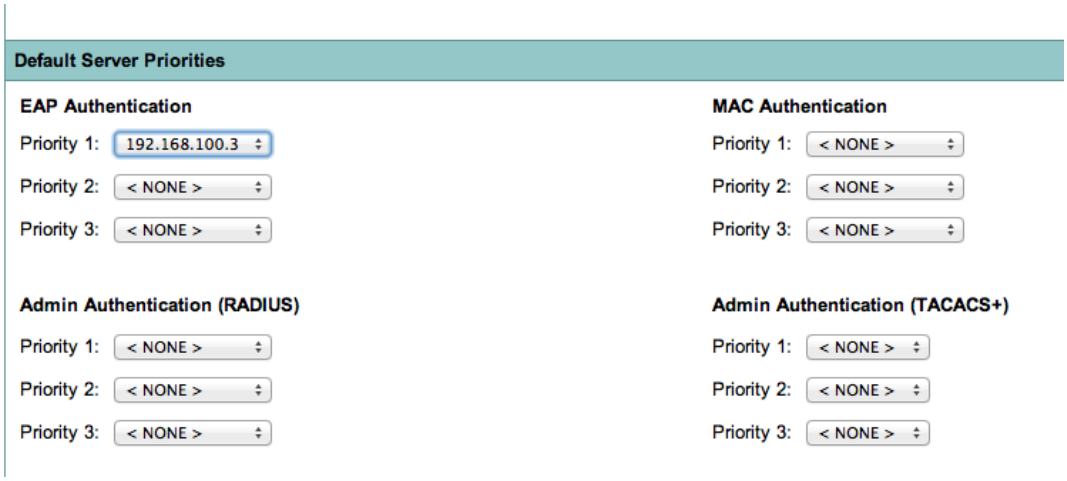
### 4.7. Configuration de l'AP

Au travers de l'interface WEB de l'AP, définissez les caractéristiques du serveur radius (au niveau de l'onglet « server manager ») :

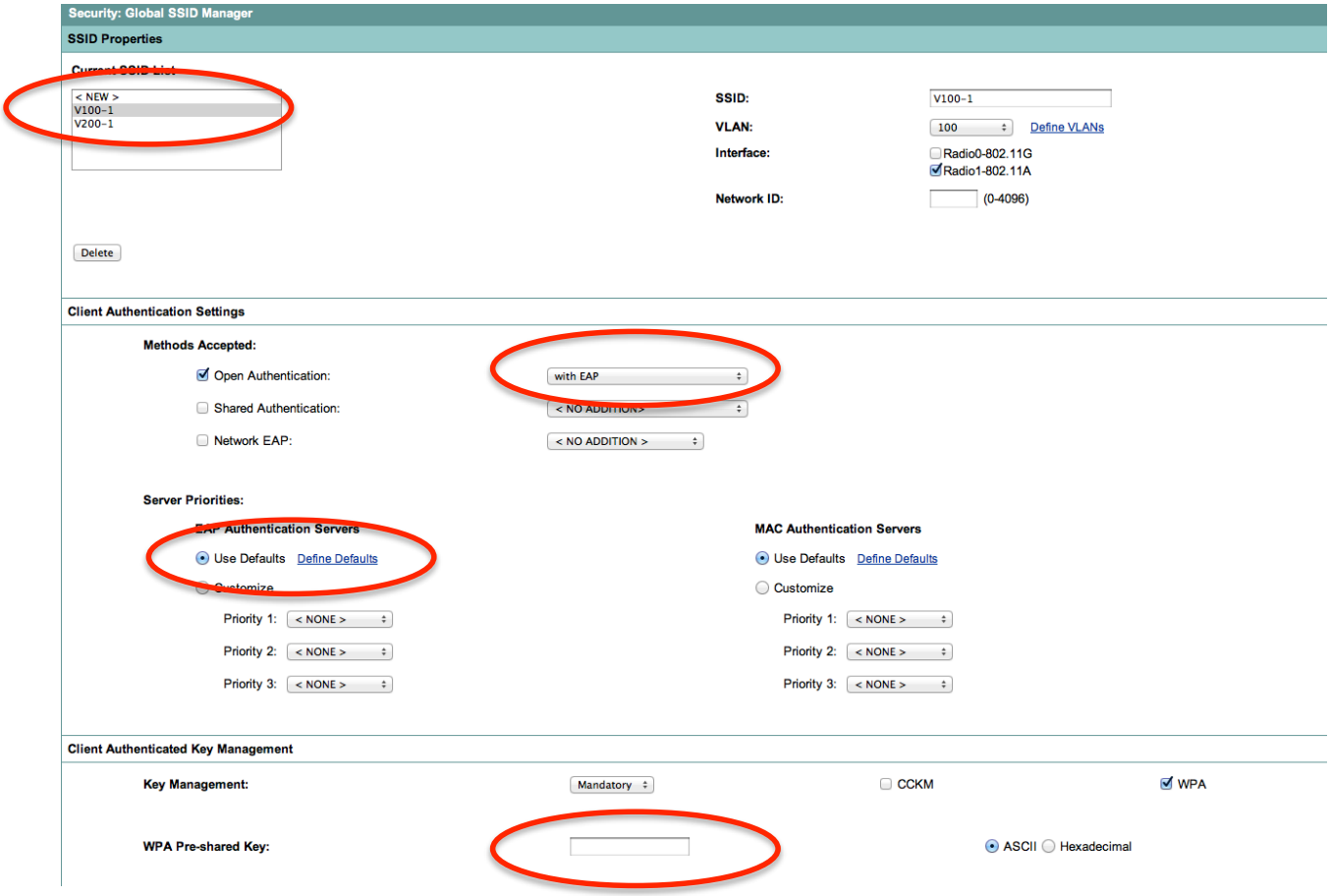



Mettre `tp` comme mot de passe partagé avec le serveur Radius.

Puis validez l'utilisation de ce serveur Radius pour l'authentification 802.1x/EAP :



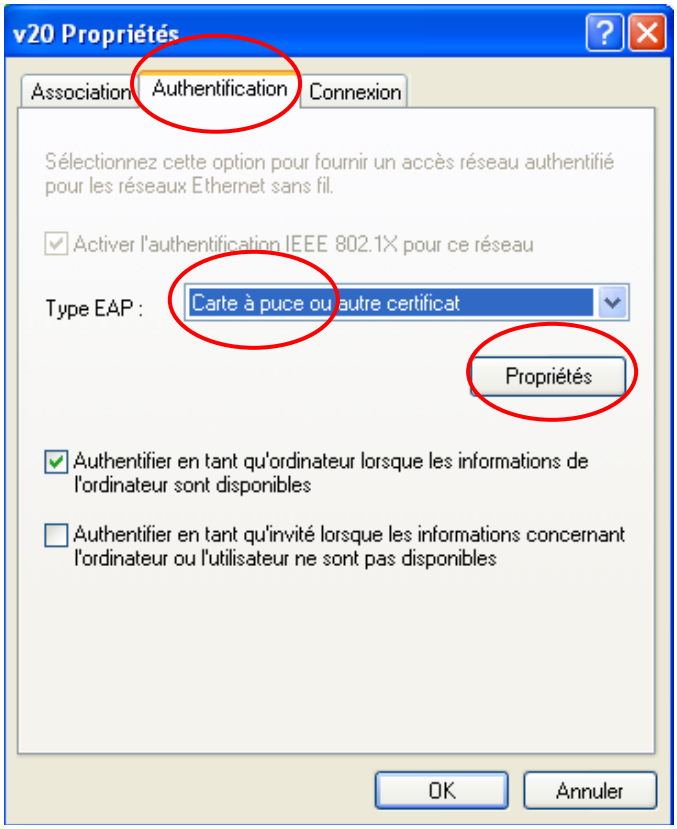

Et enfin, au niveau de la configuration du SSID V200-X attaché au VLAN 200, activez l'authentification « open + EAP », et supprimer la clé TKIP, fournie dynamiquement par le serveur Radius :



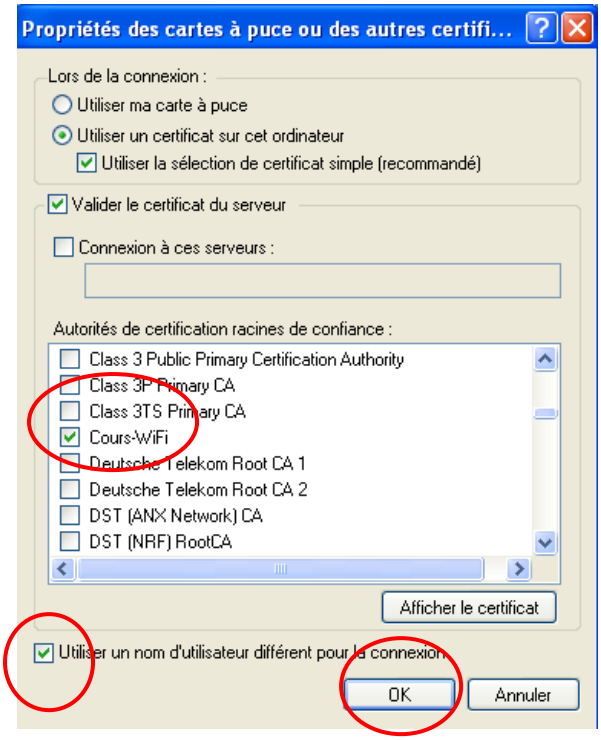

### 4.8. Configuration du SSID

Cliquez sur le SSID V200-X dans les réseaux favoris de votre carte WiFi, afin d'en modifier les propriétés :

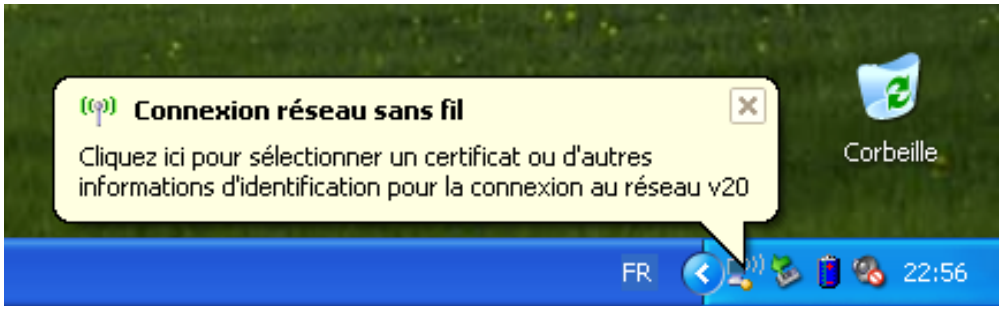
En plus de basculer le SSID en WPA *enterprise*, vous devez paramétrer l'onglet **authentification,** sélectionnez le type EAP retenu, et cliquer sur le bouton **Propriétés** :




Sélectionnez le CA « de confiance » que nous avons généré, et choisissez l'option « Utiliser un nom d'utilisateur différent pour la connexion » (qui permet de bloquer la connexion EAP-TLS et de choisir le nom du certificat « client » envoyé au serveur Radius au moment du rattachement à l'AP). Sortir ensuite des propriétés de la carte WiFi).




Attendre maintenant la reconnexion vers le SSID et cliquer sur la bulle :




Choisir le certificat et observer les *logs* au niveau du serveur radius :