

Implémentation d'un réseau Wireless avec 802.1x et EAP/PEAP + WPA/WPA2

Auteur: Gavage, Lionel
Création: 17/10/2006
Modification: 12/11/2006

DRAFT !

Implémentation d'un réseau Wireless avec 802.1x et EAP/PEAP + WPA/WPA2

Sommaire

1. Matériels utilisés
 - Access points
 - Serveurs RADIUS/AAA
 - Cartes Wireless
 - Systèmes d'exploitation
2. Configurations

1. Matériels utilisés

1.1 Access points

Access point Cisco Aironet 1200 (IOS: c1240-k9w7-mx.123-8.JEA)

Modem/routeur Philips (livré avec BelgacomTV)

1.2 Serveurs RADIUS/AAA

FreeRADIUS 1.0.5 Serveur

Cisco Secure Accesss Control Server (ACS) version 3.3 et 4.0

1.3 Carte Wireless

Elsa Airlancer MC11 Wireless PCMCIA Card

Cisco Cards

Intel® PRO/Wireless 3945BG

1.4 Systemes d'exploitation

Microsoft Windows XP Professionnal et Home Edition

Linux (OpenSUSE 10.1 with Gnome and Network Manager Applet)

2. Configurations Access points

2.1 Access Point Cisco Aironet 1200

2.1.1 Encryption Manager

La section **Encryption Manager**, comme son nom l'indique, va concerner tous les paramètres d'encryptage pour chaque réseau défini sur l'access point.

Afin de mettre en place la norme 802.1x, nous devons activer **TKIP (Temporal Key Integrity Protocol)**, utilisé pour le **WPA** signifiant **Wi-fi Protected Access**) ou bien **AES (Advanced Encryption Standard, utilisé pour le WPA2)**. Pour cela :

Security: Encryption Manager

Encryption Modes

None

WEP Encryption Optional

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

Cipher AES CCMP + TKIP

Au niveau des **Encryption Keys**, rien à spécifier vu que tout est dynamique bien entendu. Donc nous avons ceci:

Encryption Keys			
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit ▼
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit ▼
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit ▼
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit ▼

Optionnel mais assez important point de vue sécurité, surtout à l'heure actuelle, nous pouvons activer la rotation des clés en fixant un intervalle. Nous fixons cet intervalle à 300 secondes.

Global Properties	
Broadcast Key Rotation Interval:	<input type="radio"/> Disable Rotation <input checked="" type="radio"/> Enable Rotation with Interval: <input type="text" value="300"/> (10-10000000 sec)
WPA Group Key Update:	<input type="checkbox"/> Enable Group Key Update On Membership Termination <input type="checkbox"/> Enable Group Key Update On Member's Capability Change

Des options spécifiques au **WPA** peuvent être activées.

2.1.2 SSID Manager

Le **SSID Manager** comporte la définition des différents **SSID (Service Set Identifier)** ainsi que les différentes possibilités d'authentification et d'accounting de ces derniers.

Dans cette section, nous pouvons également définir le **Guest Mode SSID**, en d'autres termes le SSID qui sera broadcaster permettant d'être vu de manière automatique par tous les utilisateurs connectés en réseau sans fil.

Le SSID Manager se compose des sous-sections suivantes:

- SSID properties
- Client Authentication Settings
- Client Authentication Key Management
- Accounting Settings
- General Settings

La première sous-section **SSID Properties** nous permet de définir le SSID. Ce dernier est configuré comme étant le **Guest Mode SSID**. Donc en d'autres termes il est vu par tous les utilisateurs connectés en réseau sans fil.

SSID Properties

Current SSID List

< NEW >
protected

SSID:
VLAN: [Define VLANs](#)
 Backup 1:
 Backup 2:
 Backup 3:
Interface: Radio0-802.11G
Network ID: (0-4096)

L'image ci-dessous décrit la sous-section **Authentication Settings**. Celle-ci comporte les méthodes d'authentification à accepter. Dans le cas ici présent, nous devons spécifier de l'authentification **EAP** (vu que nous mettons en place du **EAP/PEAP**). La méthode **Network EAP** est nécessaire dans le cas d'utilisation de carte Wireless **Cisco**.

Client Authentication Settings

Methods Accepted:

Open Authentication:
 Shared Authentication:
 Network EAP:

Server Priorities:

<p>EAP Authentication Servers</p> <p> <input type="radio"/> Use Defaults Define Defaults <input checked="" type="radio"/> Customize </p> <p>Priority 1: <input type="text" value="10.1.3.15"/> Priority 2: <input type="text" value=" < NONE >"/> Priority 3: <input type="text" value=" < NONE >"/></p>	<p>MAC Authentication Servers</p> <p> <input checked="" type="radio"/> Use Defaults Define Defaults <input type="radio"/> Customize </p> <p>Priority 1: <input type="text" value=" < NONE >"/> Priority 2: <input type="text" value=" < NONE >"/> Priority 3: <input type="text" value=" < NONE >"/></p>
--	--

Nous définissons également dans la partie **Server Priorities** le ou les serveur(s) d'authentification.

2 types de serveurs possibles:

- Server **RADIUS**
- Server **TACACS+**

Dans notre cas nous utilisons 1 serveur **Radius**.

Dans la partie qui suit nous devons configurer le **Key Management** car nous utilisons le **WPA**.

Client Authenticated Key Management

Key Management: CCKM WPA
WPA Pre-shared Key: ASCII Hexadecimal

Implémentation d'un réseau Wireless avec 802.1x et EAP/PEAP + WPA/WPA2
Par contre nous activons l'**accounting** en spécifiant le serveur **RADIUS** où envoyer les informations de l'utilisation des connexions, ...

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1: 10.1.3.15

Priority 2: < NONE >

Priority 3: < NONE >

Pour le reste, rien de particulier ...

General Settings

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

Association Limit (optional): (1-255)

Call Admission Control: Enable Disable

EAP Client (optional):

Username:

Password:

Multiple BSSID Beacon Settings

Multiple BSSID Beacon

- Set SSID as Guest Mode
- Set Data Beacon Rate (DTIM): (1-100)

Sur l'image ci-dessous, nous pouvons voir comment déclarer le **SSID** en **Guest Mode**:

Guest Mode/Infrastructure SSID Settings

Set Beacon Mode: Single BSSID Set Single Guest Mode SSID:

Multiple BSSID

Set Infrastructure SSID: Force Infrastructure Devices to associate only to this SSID

2.1.3 Server Manager

Le **Server Manager** permet tout simplement de spécifier les serveurs d'authentification et une fois cela effectué de définir les priorités d'interrogation de ces derniers.

Cette section comporte les sous-sections suivantes:

- Backup Radius Server
- Corporate Servers
- Default Server Priorities

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)

Shared Secret:

Dans notre cas, rien à spécifier.

Corporate Servers

Current Server List

RADIUS

< NEW >	Server:	<input type="text"/> (Hostname or IP Address)
10.1.3.15	Shared Secret:	<input type="text"/>
	Authentication Port (optional):	<input type="text"/> (0-65536)
	Accounting Port (optional):	<input type="text"/> (0-65536)

Delete

Dans cette partie, nous définissons le type du serveur, **RADIUS** dans notre cas, ensuite les informations habituelles: adresse IP du serveur, la clé utilisée lors du dialogue entre le client interrogeant le serveur et ce dernier, les ports d'écoute (pour le mécanisme d'authentification ainsi que pour l'accounting).

Default Server Priorities

<p>EAP Authentication</p> <p>Priority 1: <input type="text" value="10.1.3.15"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>	<p>MAC Authentication</p> <p>Priority 1: <input type="text" value="< NONE >"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>	<p>Accounting</p> <p>Priority 1: <input type="text" value="10.1.3.15"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>
<p>Admin Authentication (RADIUS)</p> <p>Priority 1: <input type="text" value="< NONE >"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>	<p>Admin Authentication (TACACS+)</p> <p>Priority 1: <input type="text" value="< NONE >"/></p> <p>Priority 2: <input type="text" value="< NONE >"/></p> <p>Priority 3: <input type="text" value="< NONE >"/></p>	

Ici, on définit les priorités d'utilisation des différents serveurs d'authentification définis. Dans notre cas cela se résume à définir le seul serveur utilisé

2.2 Access Point Philips ADSL BelgacomTV

2.2.1 Wireless

Dans le menu « Wireless » il faut tout d'abord activer cette fonctionnalité. Sélectionnez pour cela la case « enable » comme sur l'image ci-dessous :

Ensuite nous devons valider votre choix en cliquant sur « save settings ».

2.2.2 Channel and SSID

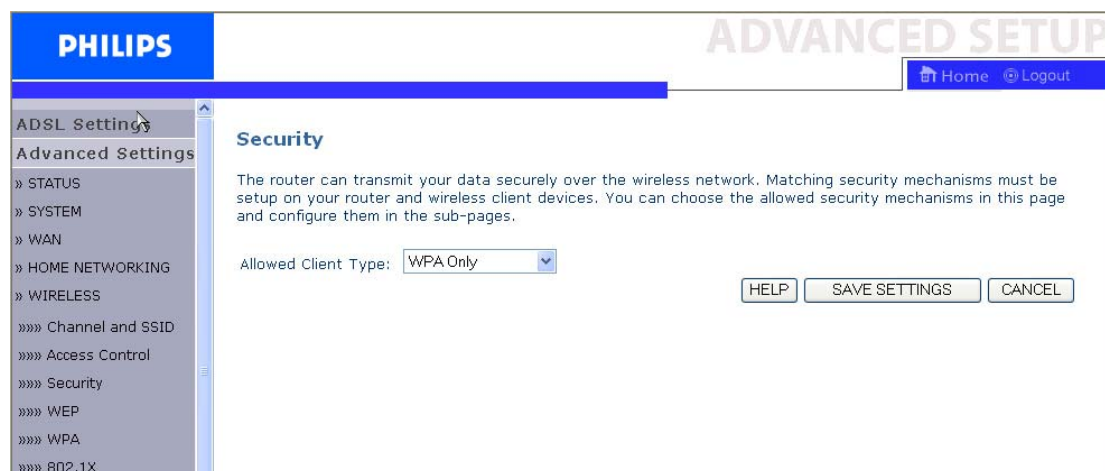
Le menu suivant permet de spécifier le SSID, la possibilité de le broadcaster ou non, le mode Wireless (802.11b/802.11g, 802.11b only, 802.11g only) et enfin le canal qui sera utilisé.

Nous pourrions lire dans pas mal de documentation que le fait de broadcaster le SSID est une faille de sécurité. Mais dans notre cas, ce n'est plus trop vrai au vu des méthodes d'authentification et d'encryption choisies. Il s'agit plus d'un choix personnel.

Ensuite nous devons valider votre choix en cliquant sur « save settings ».

2.2.3 Security

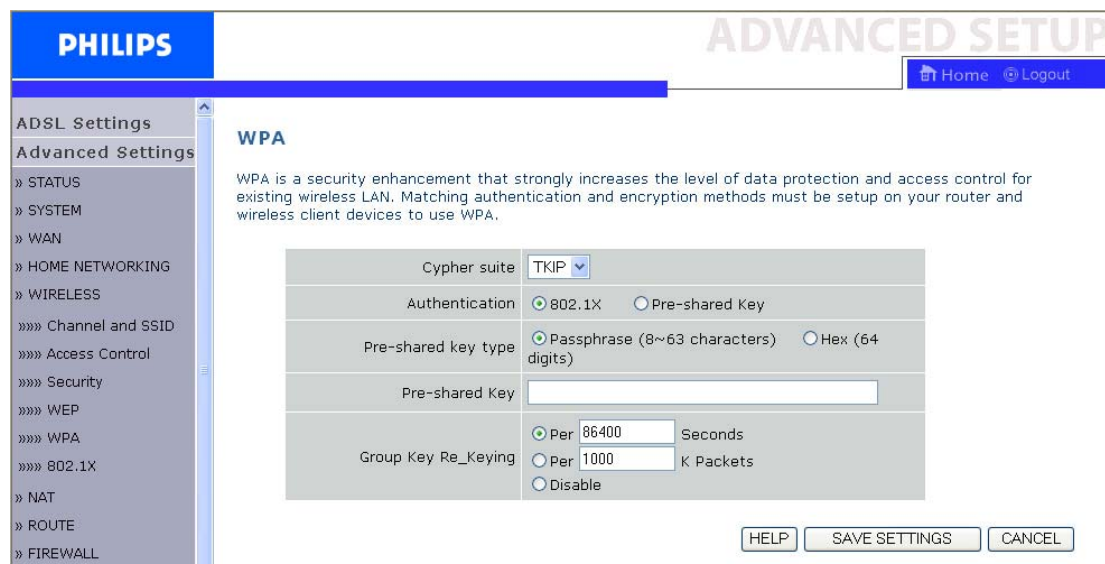
Nous n'appliquons pas de restriction au niveau d'adresses MAC donc nous arrivons au menu « Security ». C'est dans celui-ci que nous spécifions que nous voulons faire du WPA



Ensuite nous devons valider votre choix en cliquant sur « save settings ».

2.2.4 WPA

Ici, nous allons spécifier le mécanisme d'encryption, la méthode d'authentification. Dans notre cas, il s'agit bien entendu de TKIP et de 802.1x comme authentification.



Ensuite nous devons valider votre choix en cliquant sur « save settings ».

2.2.5 802.1x

Nous devons par ce menu, activer la fonctionnalité « 802.1x » et choisir le serveur d'authentification. Ce modem/routeur ne supporte que RADIUS.

Comme pour l'access point Cisco, nous devons entrer l'adresse IP du serveur RADIUS, le port d'écoute de ce dernier ainsi que la « secret key » et un NAS-ID permettant de s'y retrouver dans les logs du serveur.

The screenshot shows the Philips Advanced Setup web interface. The left sidebar contains a navigation menu with the following items: ADSL Settings, Advanced Settings, » STATUS, » SYSTEM, » WAN, » HOME NETWORKING, » WIRELESS, »»» Channel and SSID, »»» Access Control, »»» Security, »»» WEP, »»» WPA, »»» 802.1X, » NAT, » ROUTE, » FIREWALL, » SNMP, and » MAINTENANCE. The main content area is titled '802.1X' and includes a description: 'This page allows you to set the 802.1X, a method for performing authentication to wireless connection. These parameters are used for this access point to connect to the Authentication Server.'

The configuration fields are as follows:

802.1X Authentication	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Session Idle Timeout	0 Seconds (0 for no timeout checking)
Re-Authentication Period	3600 Seconds (0 for no re-authentication)
Quiet Period	60 Seconds after authentication failed
Server Type	RADIUS

RADIUS Server Parameters

Server IP	10 . 1 . 3 . 15
Server Port	1812
Secret Key	••••••••
NAS-ID	ap3

At the bottom right, there are three buttons: HELP, SAVE SETTINGS, and CANCEL.

Ensuite nous devons valider votre choix en cliquant sur « save settings ».

Voilà tout est prêt il nous reste plus qu'à paramétrer notre client !

3. Configurations serveur RADIUS/AAA

3.1 *FreeRADIUS*

3.1.1 *Introduction*

FreeRADIUS est le premier serveur radius open source. Tandis que les statistiques détaillées ne sont pas disponibles, nous (équipe de FreeRADIUS) croyons que FreeRADIUS se positionne bien dans le top 5 du monde entier des serveurs RADIUS, en termes de nombre de personnes qui l'emploient journalièrement pour l'authentification.

Nous avons installé la version 1.0.5 disponible bien entendu sur le site www.freeradius.org. Cette version supporte les types d'authentification faisant partie de la norme 802.1x (EAP/MD5, EAP/TLS, EAP/TTLS, PEAP, LEAP)

3.1.2 *Installation*

- Téléchargez l'archive .tar.gz ou bien le package généré pour votre distribution.
- Décompressez cette archive (avec gunzip et tar)
- Lancez ./configure avec éventuellement d'autres paramètres
- Lancez make
- En tant que root, exécutez make install
- Editez les différents fichiers de configuration nécessaire suivant vos besoins, ces derniers se trouvent dans le répertoire : etc/raddb/

Dans notre cas, voici notre procédure:

- cd /usr/src
- wget [ftp://ftp.freeradius.org/pub/radius/freeradius-1.0.5.tar.gz](http://ftp.freeradius.org/pub/radius/freeradius-1.0.5.tar.gz)
- tar xzvf freeradius-1.0.5.tar.gz
- mkdir /usr/local/freeradius-1.0.5
- ln -s /usr/local/freeradius-1.0.5 /usr/local/freeradius
- ./configure --prefix=/usr/local/freeradius
- Make
- make install

Nous créons un répertoire portant le numéro de la version de FreeRADIUS, ensuite nous faisons un lien symbolique permettant par la suite d'upgrader de version tout en conservant les anciennes versions...

3.1.3 Configuration

Nous référençons uniquement les directives modifiées par rapport aux fichiers de configuration d'origine. Nous allons détailler l'utilisation du serveur radius sans backend LDAP ainsi que l'utilisation du EAP/PEAP.

/etc/raddb/radiusd.conf

```
log_auth = yes
lower_user = yes
nospace_user = yes
nospace_pass = yes
proxy_requests = no
#$INCLUDE ${confdir}/proxy.conf
snmp = no
#$INCLUDE ${confdir}/snmp.conf
authorize {
eap
}
authenticate {
eap
}
```

/etc/raddb/eap.conf

```
eap {
default_eap_type = tls
tls {
private_key_password = whatever
private_key_file = ${raddbdir}/certs/cert-srv.pem
certificate_file = ${raddbdir}/certs/cert-srv.pem
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
fragment_size = 1024
}
peap {
default_eap_type = mschapv2
}
mschapv2 {
}
```

/etc/raddb/clients.conf

Ici on va définir un exemple montrant l'emploi de la syntaxe, vu que ceci est spécifique à votre range d'adresses IP...

```
client 172.16.8.232 {
secret = SECRETKEY
shortname = ap-cisco-01
}
```

Nous pouvons bien entendu créer un groupe de clients appartenant au même sous-réseau:

```
client 172.16.8.0/24 { ... }
```

/etc/raddb/users

Création d'un utilisateur par exemple:

```
lga User-Password == "mon_mot_de_passe"
```

Pour le « switching VLAN », 3 autres paramètres entrent en compte:

```
Tunnel-Type:1=VLAN  
Tunnel-Medium-Type:1=802  
Tunnel-Private-Group-ID:1=VLAN_NAME
```

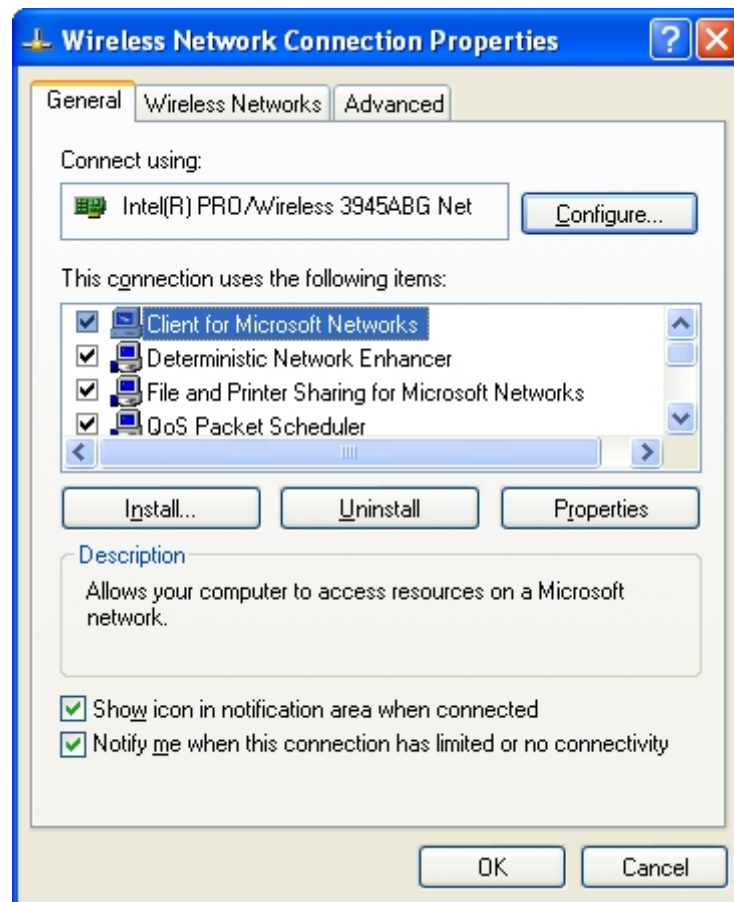
Ces paramètres permettent une fois l'utilisateur authentifié de basculer vers le VLAN indiqué par le group-id.

4. Configurations client Wireless

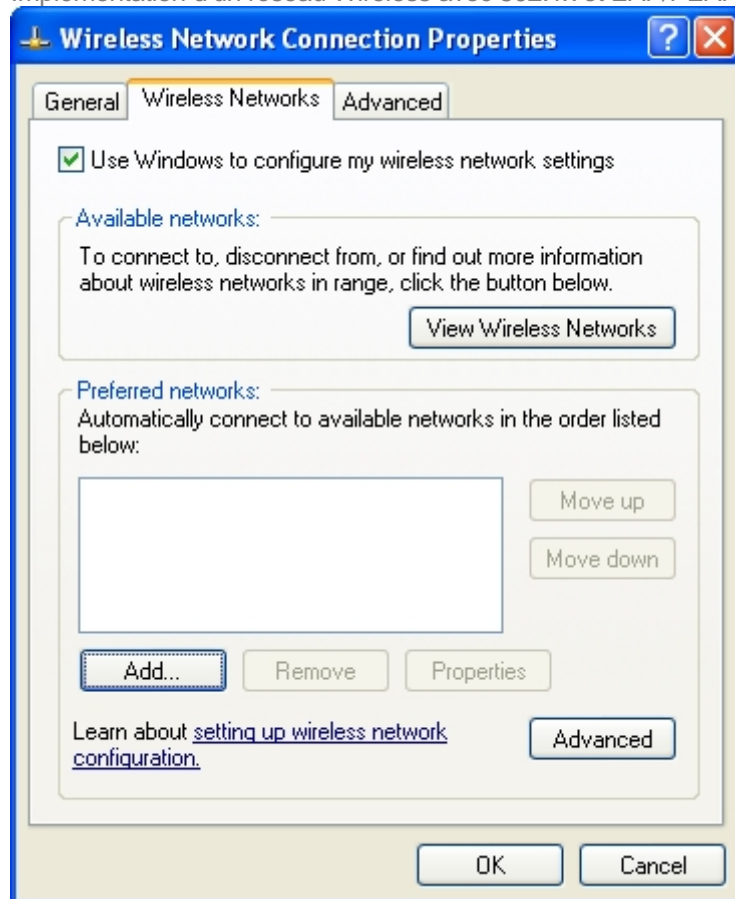
3.1 Microsoft Windows XP (support natif de EAP/PEAP)

La configuration EAP/PEAP + WPA, sous Windows, nécessite des modifications devant être effectuées obligatoirement manuellement. En effet, il faut activer EAP/PEAP, désactiver la vérification de la validité du certificat et soit utiliser le login/password de la session windows ou bien permettre l'encodage manuel de ceux-ci.

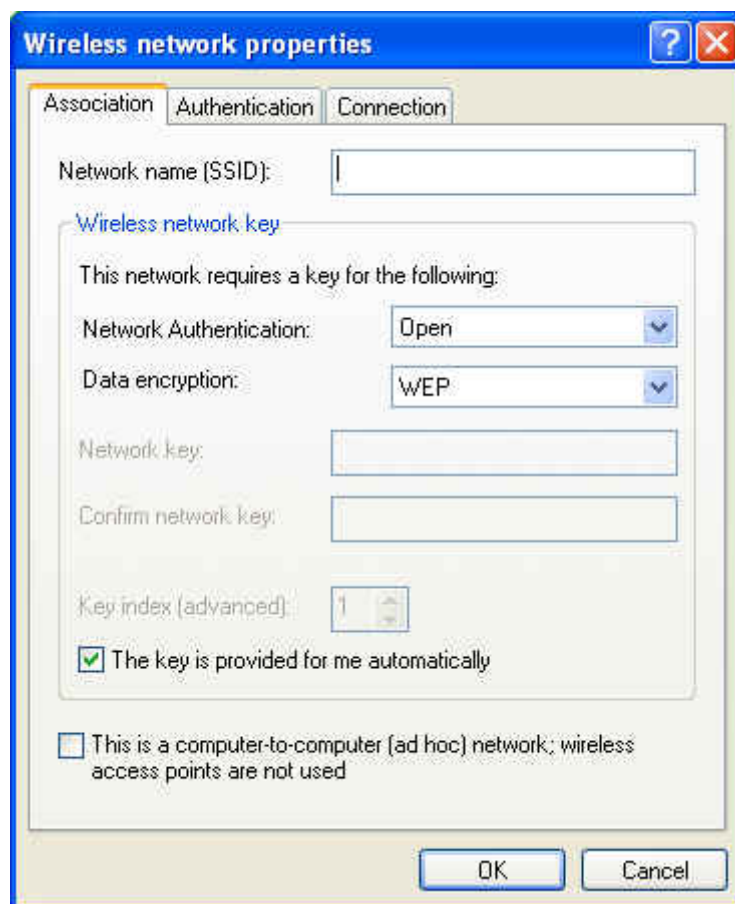
Une fois dans les propriétés de votre carte Wireless (panneau de configuration, ensuite connexions réseau, puis clique droit sur la carte sans fil et choisir « propriétés » dans le menu qui apparaît) nous obtenons la fenêtre suivante :



Nous devons sélectionner l'onglet « Wireless Networks » (« authentification sans fil » dans la version française, de mémoire). Nous arrivons à ceci :



Nous cliquons sur « ajouter » et obtenons la fenêtre suivante :



Nous devons encoder le nom du réseau Wireless, le **SSID**. Dans mon cas il s'agit de « protected ». Ensuite nous devons sélectionner comme « authentification réseau » **WPA**. Pour l'encryption des données, choisissez **TKIP**. **AES** est rien d'autre que le **WPA2** permettant une meilleure sécurité mais une adaptation de la configuration de l'access point est nécessaire.

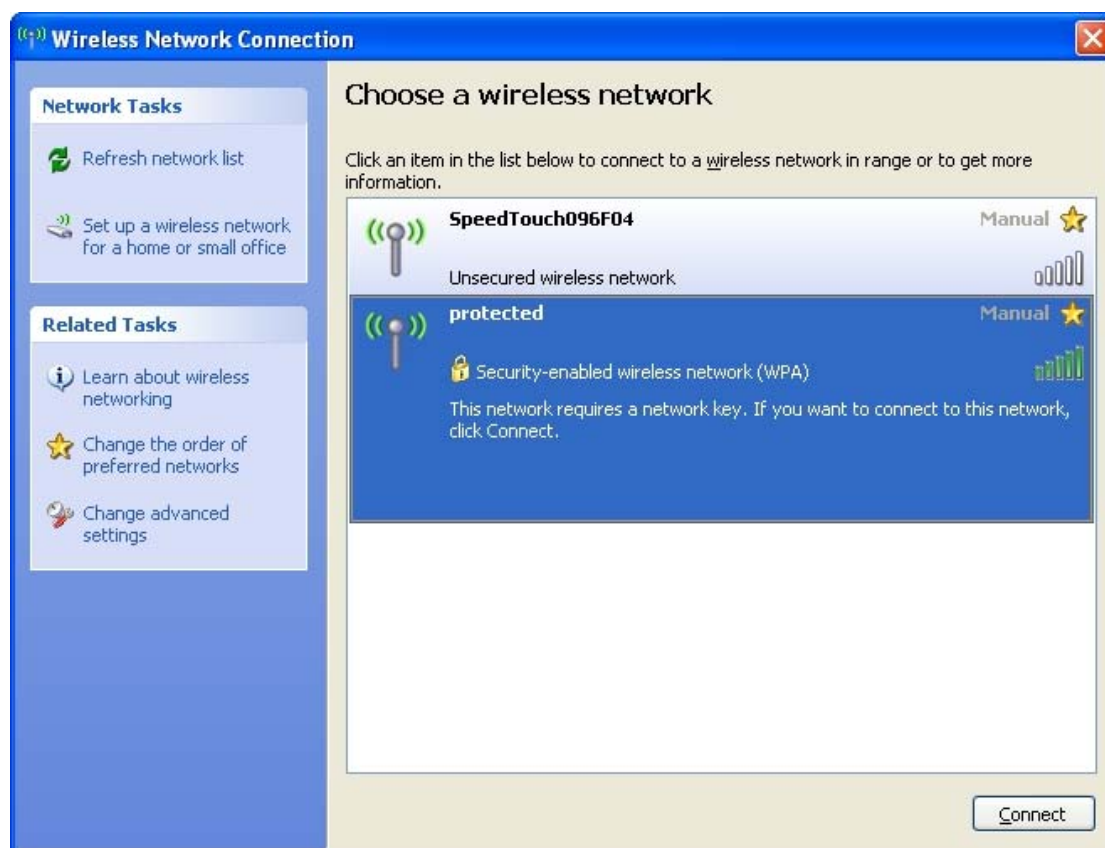
Ensuite dans l'onglet « Authentification » sélectionnez **Protected EAP (PEAP)**. Faites « propriétés ». Décochez la case « Valider le certificat du serveur ». Cochez par contre la case « Activer la reconnexion rapide ». Si nous ne voulons pas employer le login/password de la session windows, il nous suffit de cliquer sur « Configurer » à côté de « Secured Password (EAP-MSCHAP V2) » et de décocher la case dans la fenêtre qui apparaît.

En gros nous avons comme résultat ceci :



Nous validons le tout en cliquant sur « OK » pour fermer toutes les fenêtres.

Lorsque nous cliquons 2 fois sur votre carte Wireless nous obtenons la fenêtre suivante :



Il nous suffit de choisir le réseau auquel nous voulons nous connecter et ensuite cliquer sur « connect » ou bien simplement cliquer 2 fois sur le réseau souhaité.

Si nous n'utilisons pas votre login/password de la session windows un message en bas à droite apparaîtra, nous devons cliquer dessus et la fenêtre suivante s'ouvre :



Bien entendu nous devons entrer votre login/password défini dans le serveur RADIUS/AAA et le tour est joué ;-)