Noureddine BOUHADDAOUI
Adrien GOSSEAUME
Mustapha MOURI
Julien VEHENT

Architecture Wifi

sécurisée sous Cisco

Master Management de la Sécurité des
Systèmes Industriels et des Systèmes d'Information

Mars 2007

Sommaire

Introduction

L'objectif de ce rapport est de présenter les résultats de nos travaux sur les points d'accès Aironet 1131 AG pour mettre en place une architecture wifi sécurisée.

Dans un premier temps, nous étudierons succinctement les risques qu'encours généralement les réseaux sans-fil. Cette analyse des risques nous permet d'orienter nos travaux vers des solutions qui agirons sur les critères DIC (Disponibilité, Intégrité, Confidentialité).

Puis, dans un second temps, nous détaillerons la mise en place technique d'une architecture wifi simple, non sécurisée, à laquelle nous intégrerons dans une troisième partie le protocole de chiffrement WPA. Ce dernier permet de résoudre la problématique de confidentialité, partiellement, et d'intégrité, complètement.

Enfin, nous orienterons nos points d'accès vers un système d'authentification, radius, et vers un protocole d'itinérance des postes clients, la technologie Roaming.

Analyse de risques

Types de risque	Risque	Commentaire
Disponibilité	Brouillage radio	Les ondes radio sont très sensibles aux interférences, c'est la raison pour laquelle un signal peut facilement être brouillé par une émission radio ayant une fréquence proche de celle utilisée dans le réseau sans fil. Un simple four à micro-ondes peut ainsi rendre totalement inopérable un réseau sans fil lorsqu'il fonctionne dans le rayon d'action d'un point d'accès.
	Mobilité de connexion	Un équipement se déplaçant physiquement dans le réseau doit être capable de passer d'un point d'accès à un autre de façon transparente pour l'utilisateur. Ceci est communément appelé le ROAMING
Intégrité	Modification de données	Un attaquant peut facilement se placer entre un client et un point d'accès en se faisant passer pour le point d'accès, vis à vis du client, et pour le client, vis à vis du point d'accès. Cette technique très efficace est communément appelé Man-In-The-Middle. Elle permet à l'attaquant de modifier les données transmises « au vol », comme par exemple lors d'un échange de clé Diffie Hellman.
Confidentialité	Interception de données	Du fait des propriétés intrinsèques des ondes radio, le vol d'information est facilité. Un pirate peut facilement récupérer les trames circulant entre les clients et les points d'accès.
	Accès illicite	Un attaquant ayant accès au réseau sans fil peut, de fait, accéder à l'ensemble des ressources réseaux de l'architecture. cela constitue une faille importante dans la politique d'accès au système d'information.

Étude d'impact

Note	***Impact***	***Potentialité***
0	aucun impact	Improbable
1	Impact très faible	peu probable
2	Impact moyen	moins fréquent
3	Impact important	fréquent
4	Impact grave qui met en cause la pérénité de l'entreprise	Sûr

Table des gravité

I \ P	***0***	***1***	***2***	***3***	***4***
0	G = 0	G = 0	G = 0	G = 0	G = 0
1	G = 0	G = 1	G = 1	G = 2	**G = 3**
2	G = 0	G = 1	G = 2	**G = 3**	**G = 3**
3	G = 0	G = 2	**G = 3**	**G = 3**	**G = 4**
4	G = 0	**G = 3**	**G = 3**	**G = 4**	**G = 4**

G = 1 : Pas grave
G = 2 : Niveau de gravité de risque moyen
G = 3 : Niveau de risque élevé, doit être intégré dans des plans d'amélioration
G = 4 : Niveau de risque insupportable, exige des mesures urgentes hors des cycles de budget habituels

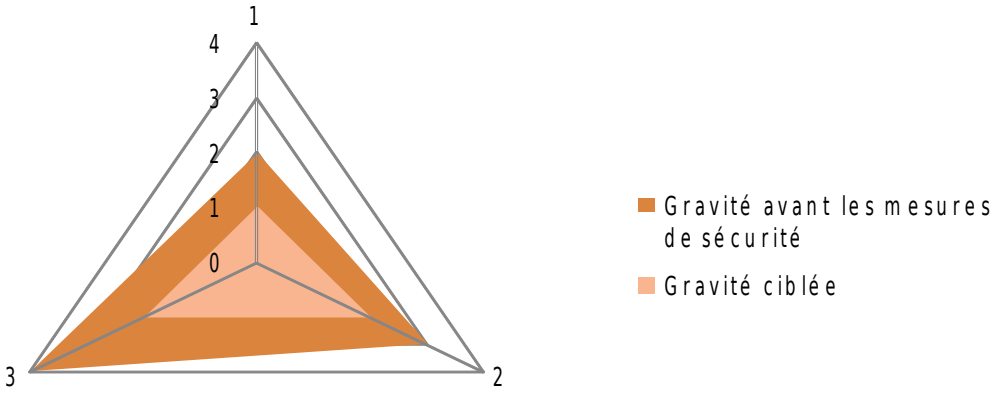
Matrice de gravité actuelle du système

On évalue l'impact et la potentialité de chaque menace à laquelle est exposé notre réseau. Ensuite on se réfère à la matrice détaillée ci-dessus pour noter la gravité de chaque menace.

critère	**Menaces**	**Impact (0 à 4)**	**Potentialité (0 à 4)**	**Gravité (0 à 4)**
Disponiblité	M1- Brouillage radio	1	2	1
	M2- Mobilité de connexion	1	3	2
Intégrité	M3- Modification de données	3	2	3
Confidentialité	M4- Interception de données	3	2	3
	M5- Accès illicite	3	4	4
	M6- Accès malveillant des utilisateurs	2	3	3

A partir de la matrice de gravité, on prend la note maximale de chaque critère, puis on cible un niveau de gravité que l'on souhaite atteindre après la mise en place de certaines solutions. Il faudra bien sûr tenir compte de la matrice de gravité : par exemple on ne peut pas atteindre un niveau de gravité inférieur à 2 en terme de confidentialité parce que l'impact atteint 3 et on ne peut jamais réduire la potentialité de survenance d'une menace à 0.

Risques	**Disponibilité (0 à 4)**	**Intégrité (0 à 4)**	**Confidentialité (0 à 4)**
Gravité avant les mesures de sécurité	2	3	4
Gravité ciblée	1	2	2



Proposition de solution à mettre en place

Menaces	Mesures à mettre en place
M1- Brouillage radio	Vu la faiblesse du niveau de risque que présente cette menace, on ne va pas la traiter dans un premier temps.
M2- Mobilité de connexion	Le Roaming est une des solutions qui peuvent répondre à cette problématique
M3- Modification de données	On doit utiliser des mécanismes de cryptage (WEP,WPA) aujourd'hui WPA est le plus fiable.
M4- Interception de données	WPA répond également à cet aspect.
M5- Accès illicite	Il faut utiliser un système d'authentification des utilisateurs, RADIUS par exemple
M6- Accès malveillant des utilisateurs	Il faudra cloisonner les applications et les services pour empêcher un utilisateurs de se connecter sur des ressources et des données qui ne les concernent pas (VLAN).

Architecture Wifi simple

802.11G

La norme IEEE 802.11 est un standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN). Le nom Wi-Fi (contraction de Wireless Fidelity) correspond initialement au nom donnée à la certification délivrée par la Wi-Fi Alliance, anciennement WECA (Wireless Ethernet Compatibility Alliance), l'organisme chargé de maintenir l'interopérabilité entre les matériels répondant à la norme 802.11. Par abus de langage, le nom de la norme se confond aujourd'hui avec le nom de la certification. Un réseau Wifi est en réalité un réseau répondant à la norme 802.11.

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- la couche physique, proposant trois types de codages de l'information.
- la couche liaison de données, constitué de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC)

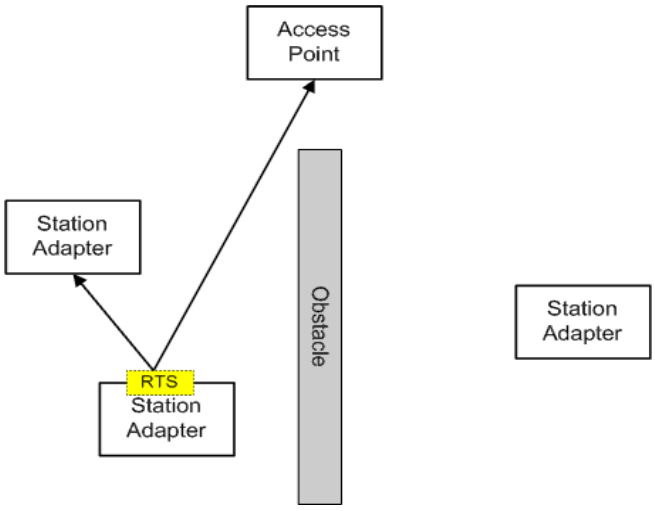
La couche physique définit la modulation des ondes radio-électriques et les caractéristiques de la signalisation pour la transmission de données, tandis que la couche liaison de données définit l'interface entre le bus de la machine et la couche physique, notamment une méthode d'accès proche de celle utilisée dans le standard Ethernet (et son CSMA/CD) et les règles de communication entre les différentes stations.

Il est possible d'utiliser n'importe quel protocole de haut niveau sur un réseau sans fil WiFi au même titre que sur un réseau ethernet.

CSMA/CA

Dans un réseau local Ethernet classique, la méthode d'accès utilisée par les machines est le CSMA/CD (Carrier Sense Multiple Access with Collision Detect), pour lequel chaque machine est libre de communiquer à n'importe quel moment. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine. Si c'est le cas, les deux machines patientent pendant un temps aléatoire avant de recommencer à émettre.

Dans un environnement sans fil ce procédé n'est pas possible dans la mesure où deux stations communiquant avec un récepteur ne s'entendent pas forcément mutuellement en raison de leur rayon de portée. Ainsi la norme 802.11 propose un protocole similaire appelé CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).



Le protocole CSMA/CA utilise un mécanisme d'esquive de collision basé sur un principe d'accusé de réception réciproques entre l'émetteur et le récepteur :

La station voulant émettre écoute le réseau. Si le réseau est encombré, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour Distributed Inter Frame Space), alors la station peut émettre. La station transmet un message appelé Ready To Send (ou Request To Send) noté RTS signifiant prêt à émettre contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un Clear To Send (CTS, signifiant Le champ est libre pour émettre), puis la station commence l'émission des données.

A réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK). Toutes les stations avoisinantes patientent alors pendant un temps qu'elle considère être celui nécessaire à la transmission du volume d'information à émettre à la vitesse annoncée.

802.11G sur Cisco Aironet

Les équipements Aironet permettent de mettre en oeuvre très simplement un point d'accès non sécurisé. En voici les étapes :

Configuration réseau de la borne

La borne est, par défaut, configurée pour prendre une adresse en DHCP. Nous allons lui attribuer une IP statique de la façon suivante :

ap> en *// passe en mode de super user*

Password: 'Cisco'

ap# conf t *// passe en mode configuration*

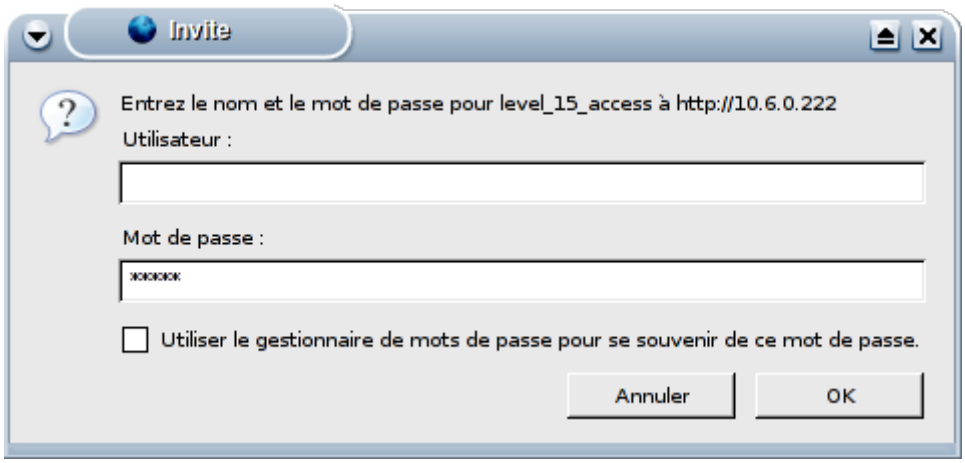
ap(config)# inter bvi1 *// selectionne le bridge ethernet*

ap(config-if)# ip addr 10.6.0.222 255.255.255.0 *// config une adresse ip*

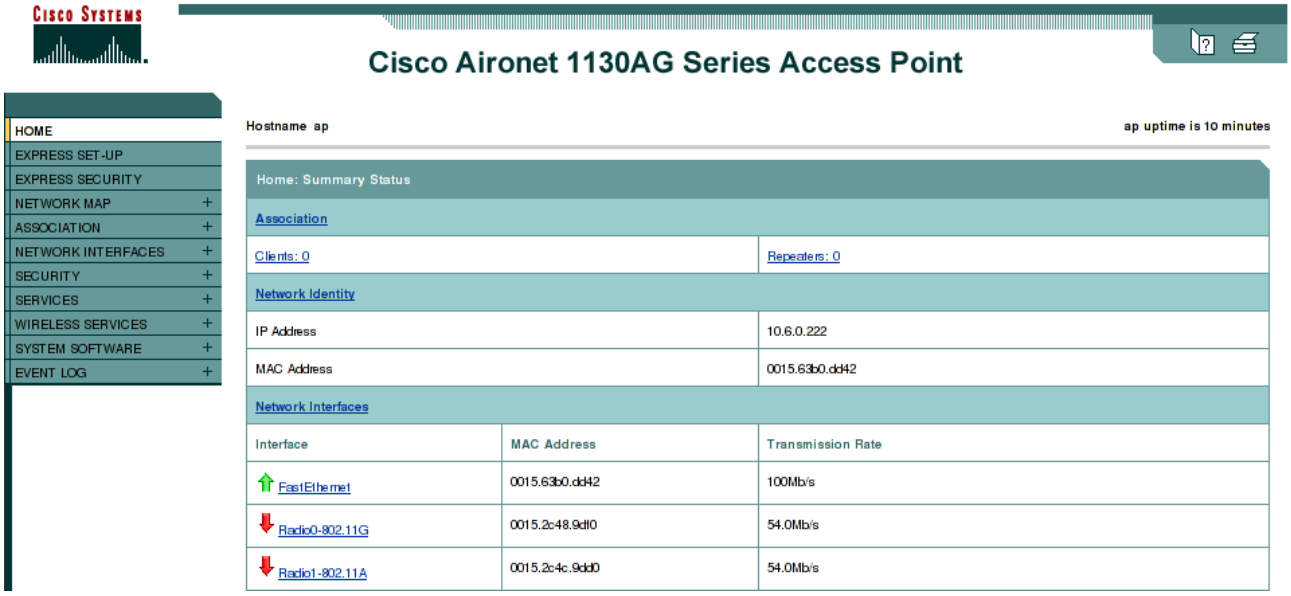
ap(config-if)# no shut *// démarre l'interface*

Accès à l'interface Web

De fait, nous pouvons nous connecter à l'interface web. Il n'y a pas d'identifiant et le mot de passe par défaut est « Cisco ».

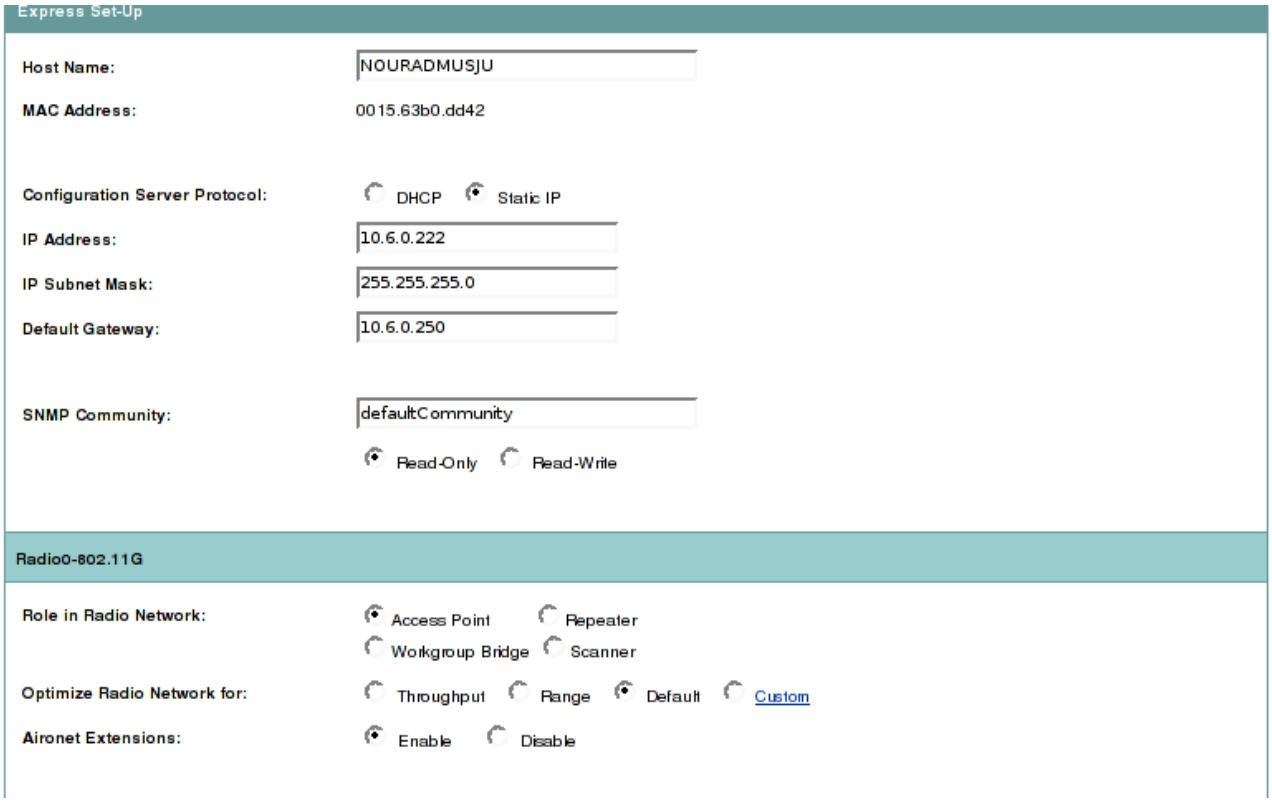


Nous arrivons donc sur la page de résumé du point d'accès :

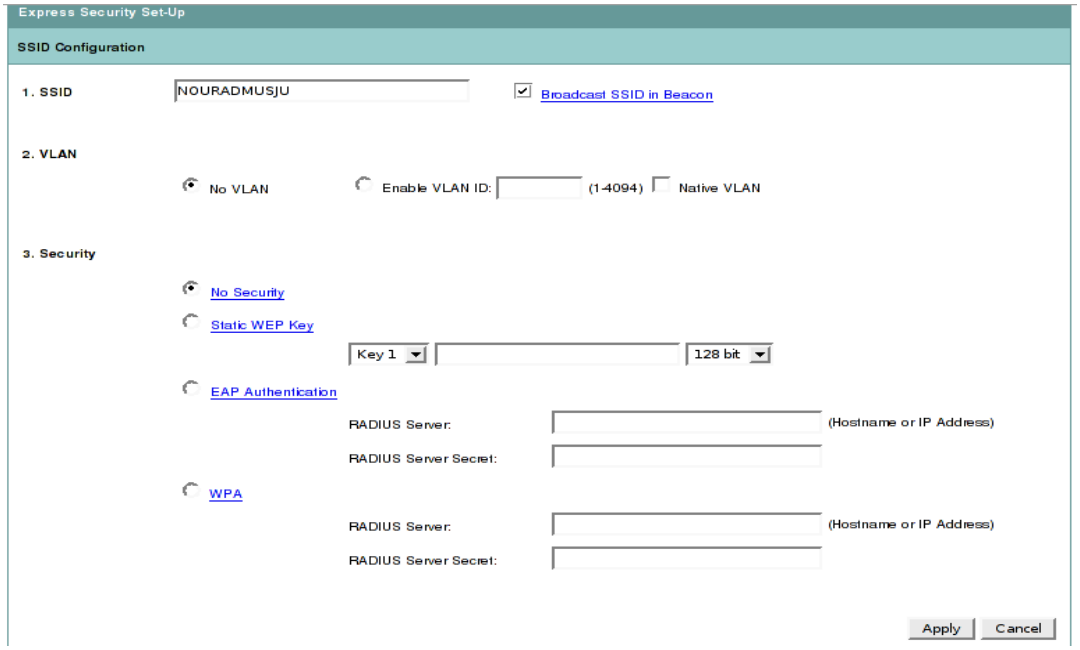


Création d'une configuration rapide

La section *Express Set-UP* dans le menu de gauche pour accéder au paramétrage des options de base de la borne (IP, Masque, Passerelle par défaut, Nom d'hôte, Mode point d'accès ou pont, ...) :



Puis, dans la section *Express Security*, nous configurons un nouveau *SSID* sans activer la sécurité.



Il faut ensuite démarrer l'interface WLAN qui est, par défaut, désactivée. Ceci se fait dans la section *Network Interfaces > Radio0-802.11G > Settings.* Cette section permet de passer l'interface en mode *Enable* et de choisir un channel sur lequel elle va fonctionner, dans notre cas, le channel 4.

Nous ne touchons pas aux autres paramètres.

Test

L'outil *Kismet*, sous Linux, scanne les différents réseaux vus par la carte Wifi. Dans notre cas, l'activation de l'interface entraîne l'apparition du réseau *NOURADMUSJU* dans la liste des réseaux détectés. On voit bien ici que le réseau ne dispose pas de protocoles de sécurité (sections *Privacy* et *Encrypt*).

```
Network Details
Name    : NOURADMUSJU

SSID    : NOURADMUSJU
Server  : localhost:2501
BSSID   : 00:15:2C:48:9D:F0
Carrier : IEEE 802.11g
Manuf   : Unknown
Max Rate: 18.0
BSS Time: 33a918b
Max Seen: 1000 kbps
First   : Tue Mar 20 09:50:17 2007
Latest  : Tue Mar 20 09:51:09 2007
Clients : 0
Type    : Access Point (infrastructure)
Info    : NOURADMUSJU\000\000\000\000\000\000\000\000
Channel : 4
Privacy : No
Encrypt : None
Beacon  : 25600 (26.214400 sec)
Packets : 81
  Data    : 0
  LLC     : 81
  Crypt   : 0
  Weak    : 0
  Dupe IV : 0
Data    : 0B
Signal  :
  Power   : 26 (best 56)
  Noise   : 0 (best 0)
IP Type : None detected
Min Loc : N/A
Max Loc : N/A
Range   : N/A
```

De fait, sous Linux et avec une carte Atheros, on peut se connecter très simplement au réseau via la commande :

```
iwconfig ath0 channel 4 mode Managed \
essid "NOURADMUSJU"
```

La commande iwconfig ath0 renvoie alors la configuration de l'interface.

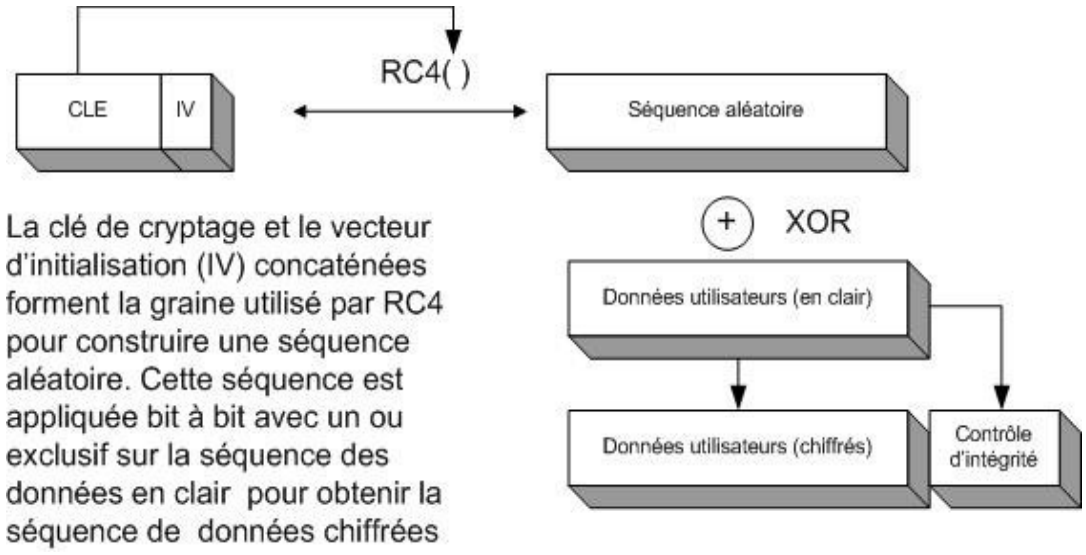
WPA

Le WPA est une version « allégée » du protocole 802.11i, reposant sur des protocoles d'authentification et un algorithme d'échange de clé robuste : TKIP (*Temporary Key Integrity Protocol*). Le protocole TKIP permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité.

Le fonctionnement de WPA repose sur la mise en oeuvre d'un serveur d'authentification (la plupart du temps un serveur RADIUS), permettant d'identifier les utilisateurs sur le réseau et de définir leurs droits d'accès. Néanmoins, il est possible pour les petits réseaux de mettre en oeuvre une version restreinte du WPA, appelée WPA-PSK, en déployant une même clé de chiffrement dans l'ensemble des équipements, ce qui évite la mise en place d'un serveur RADIUS. C'est cette alternative que nous allons, dans un premier temps, mettre en place.

Chiffrement

L'algorithme utilisé par WPA est, comme pour WEP, le RC4. Ce dernier est détaillé dans le schéma ci-dessous :



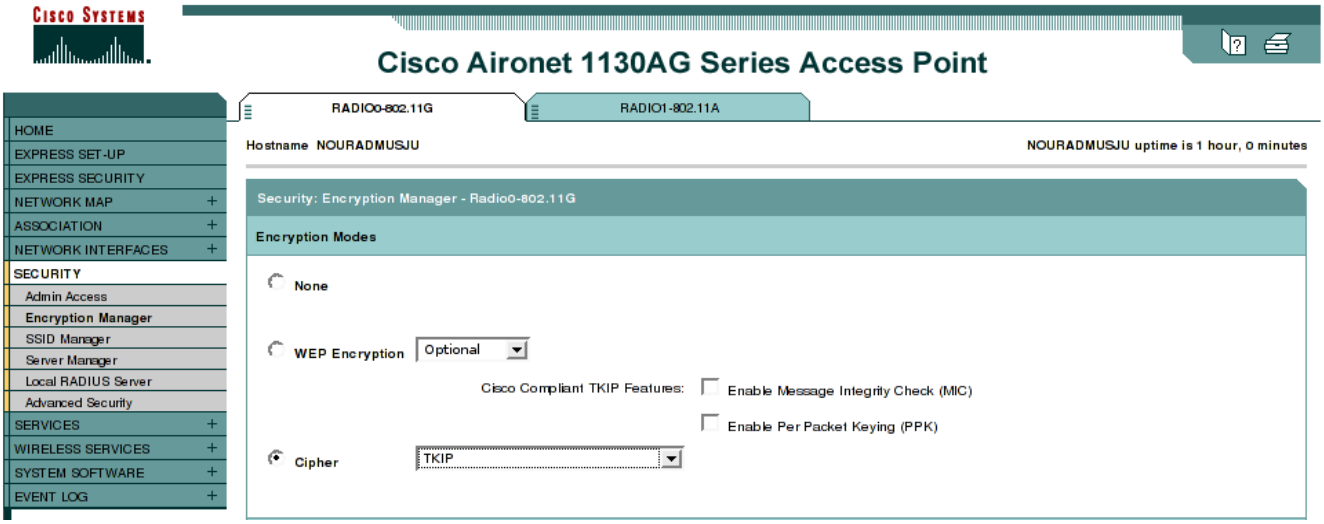
Le renouvellement rapide de la clé permet de pallier au problème majeur du WEP, c'est à dire la redondance de la clé et la transmission en clair du vecteur d'initialisation. Ainsi, il est beaucoup plus difficile de décrypter les messages car le nombre de paquets chiffrés avec une clé est beaucoup plus faible qu'avec le protocole WEP (dans lequel la clé ne varie pas).

WPA sur Cisco Aironet

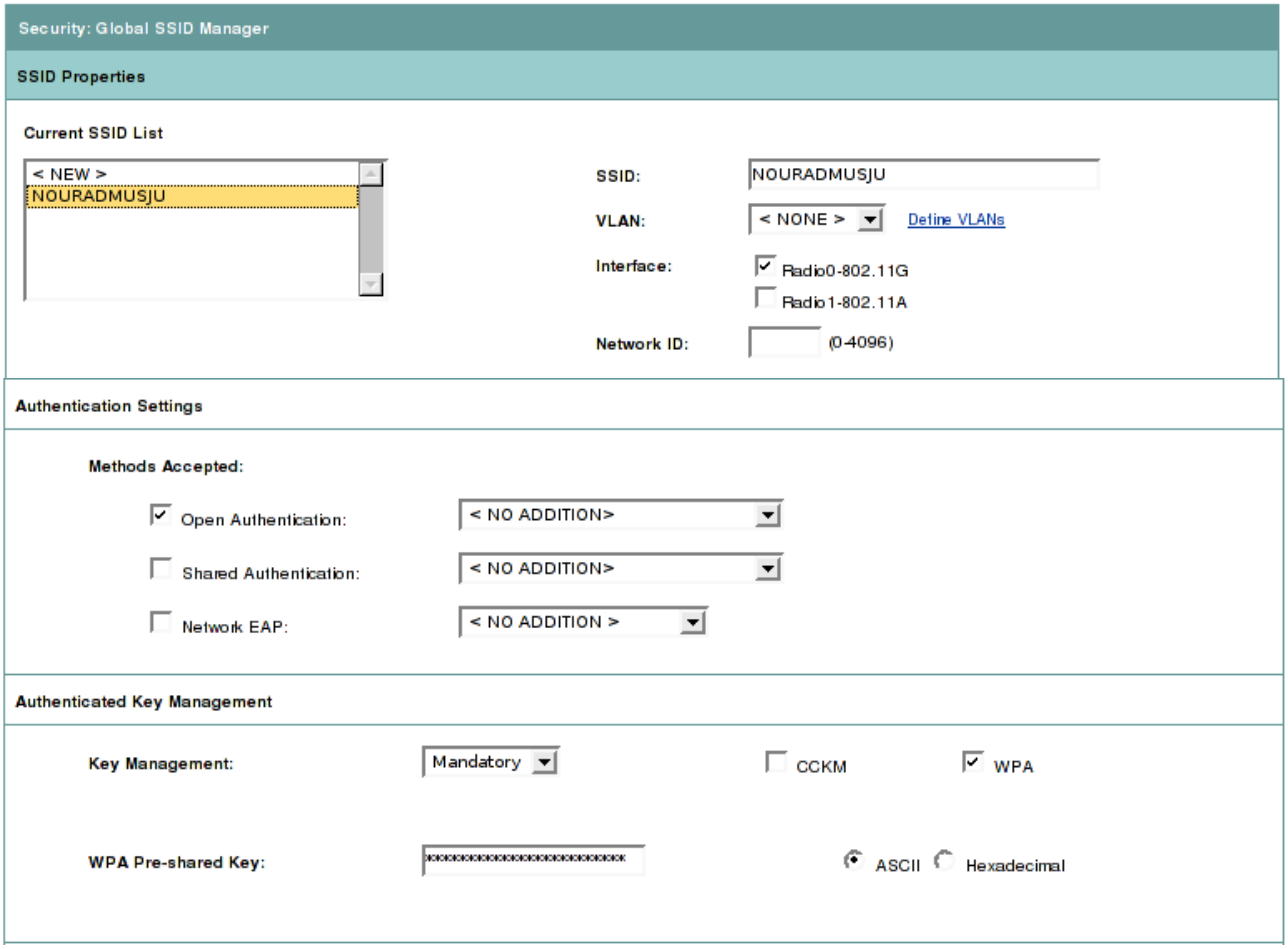
Pour activer le mode WPA, nous allons reprendre la création du SSID dans l'interface web de configuration du point d'accès.

Nous allons créer un nouvel SSID qui, à la différence du premier, utilisera le chiffrement WPA avec un secret partagé (WPA-PSK) et le protocole d'échange de clé TKIP.

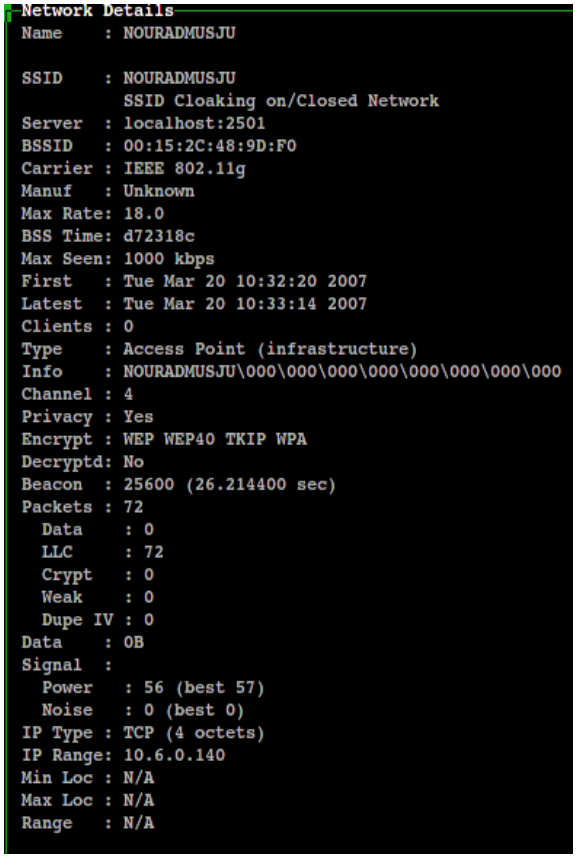
Dans un premier temps, il faut activer le mode TKIP dans les modes de chiffrements :



Ensuite, il faut supprimer le SSID actuel, ce qui se fait très bien dans la section *Express Security*. Puis, dans la section *Security > SSID Manager*, nous créons un nouvel SSID avec les paramètres suivants :



De fait, dans Kismet, nous voyons notre SSID comme protégé (voir ligne Encrypt).



Pour nous connecter, il faut donc utiliser l'outil WPA_Supplicant avec le fichier de configuration suivant :

```
# cat wpa_409.conf
ctrl_interface=/var/run/wpa_supplicant
ap_scan=2
network={
       ssid="NOURADMUSJU"
        proto=WPA
        pairwise= TKIP
        key_mgmt=WPA-PSK
        psk="NOURADMUSJU"
}
# wpa_supplicant -i ath0 \
-c wpa_409.conf  -D madwifi -B
```

Notre interface est active avec la configuration suivante :

```
ath0     IEEE 802.11g  ESSID:"NOURADMUSJU"
          Mode:Managed  Frequency:2.427 GHz  Access Point: 00:15:2C:48:9D:F0
          Bit Rate:54 Mb/s   Tx-Power:16 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:4448-DA8E-6EF2-E1A0-7B03-B370-82C2-024C
          Security mode:restricted
          Power Management:off
          Link Quality=52/94  Signal level=-43 dBm  Noise level=-95 dBm
          Rx invalid nwid:8007  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Nous pouvons observer l'évolution de la clé de chiffrement dans le temps très simplement de la façon suivante :

```
# for ((i=0;i<6;i++));do iwconfig ath0|grep Encryption;sleep 3;done
          Encryption key:4448-DA8E-6EF2-E1A0-7B03-B370-82C2-024C
          Encryption key:A8C3-29F8-2A3D-8FEE-1CBC-7D68-CB88-713F
          Encryption key:35DB-FDF1-9E79-010C-70E3-C4CD-319C-A9E5
          Encryption key:6CE9-F17E-E92D-09ED-6E03-DDA9-7A41-042D
          Encryption key:55D4-9C92-C9B4-7FA8-695E-46FD-2845-E29F
          Encryption key:93F1-B211-4ACC-B675-214E-998D-DAB2-B4FC
```

Le protocole TKIP permet de négocier régulièrement une nouvelle clé de chiffrement entre le client et le point d'accès pour crypter les paquets transmis sur la liaison Wifi. La fréquence de renouvellement de la clé est inférieure à 3 secondes.

Radius

Le protocole RADIUS (Remote Authentication Dial-In User Service), mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

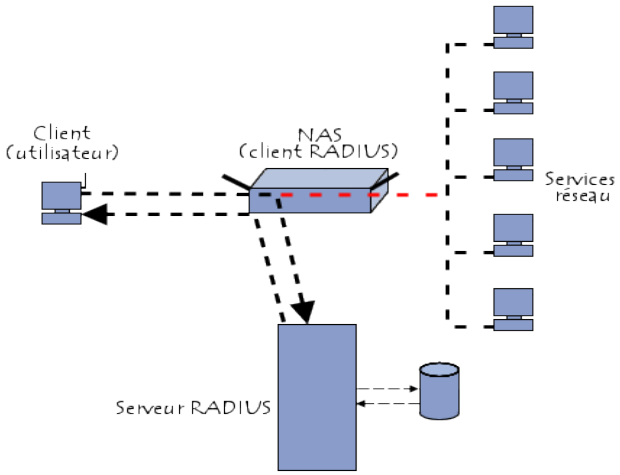
Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

Il est à noter que le serveur RADIUS peut faire office de proxy, c'est-à-dire transmettre les requêtes du client à d'autres serveurs RADIUS.

Fonctionnement de RADIUS

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance
2. Le NAS achemine la demande au serveur RADIUS
3. Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthodes d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :
   - ACCEPT : l'identification a réussi
   - REJECT : l'identification a échoué
   - CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge »)
   - CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe

Suite à cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur.

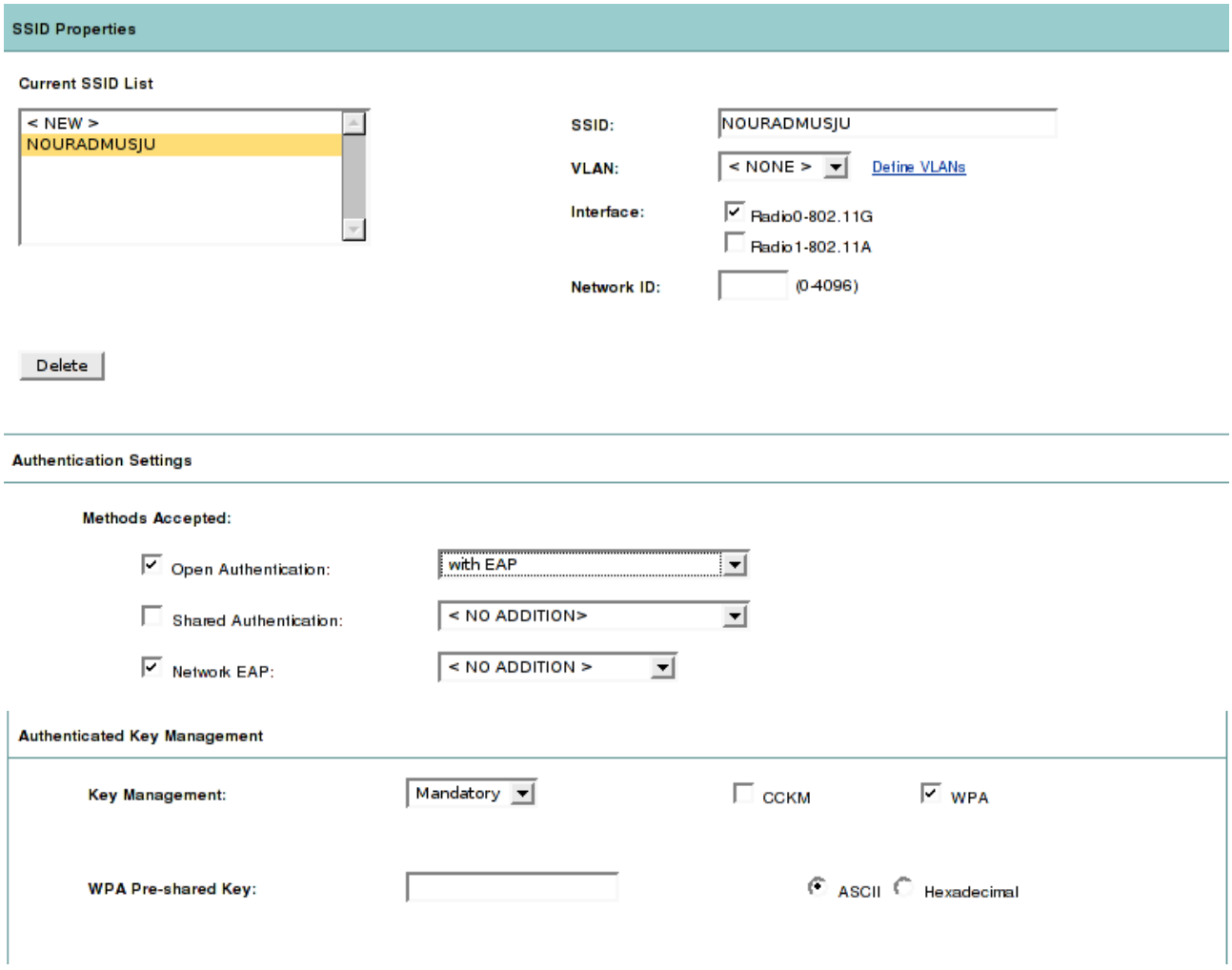


Radius sur Cisco Aironet

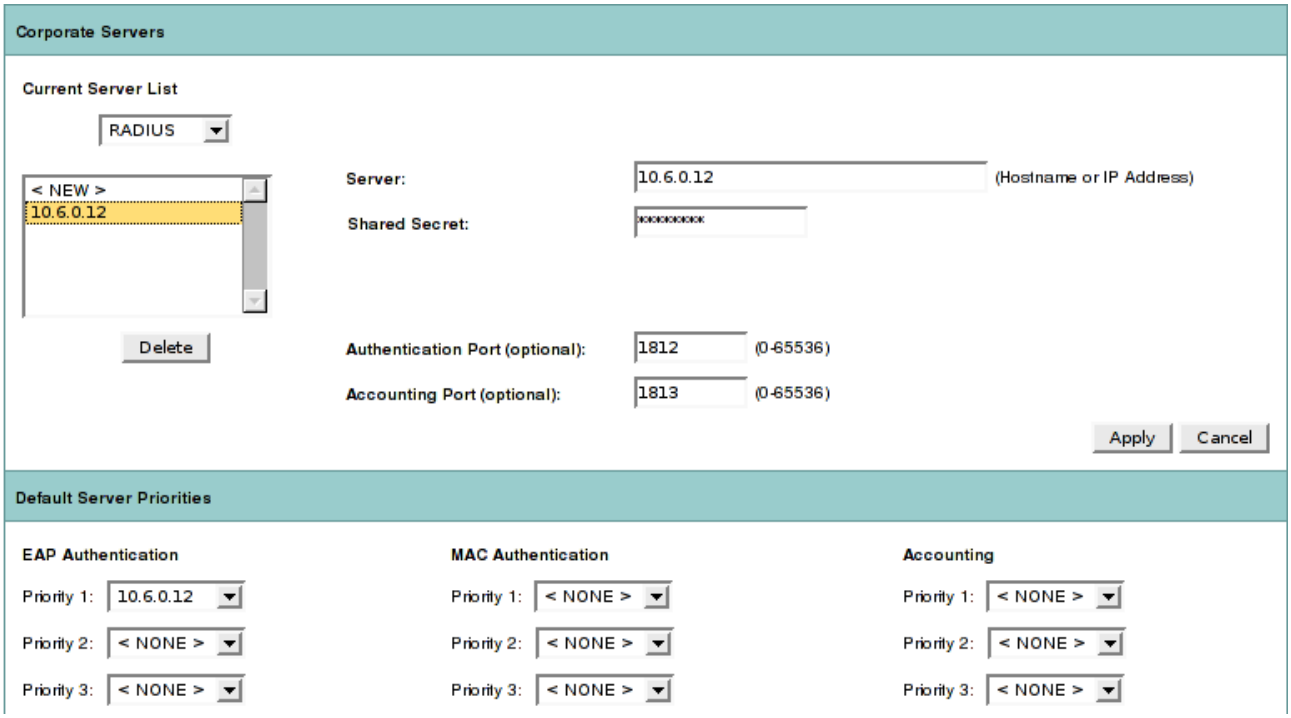
Les points d'accès Cisco Aironet sont conçus pour jouer le rôle de NAS dans les architectures RADIUS. Une machine Windows Server 2003 joue le rôle de serveur RADIUS.

Comme lors de la configuration du WPA, nous utilisons l'algorithme de négociation de clé TKIP dans l'*Encryption Manager*.

Dans le *SSID Manager*, on modifie la configuration comme suis :

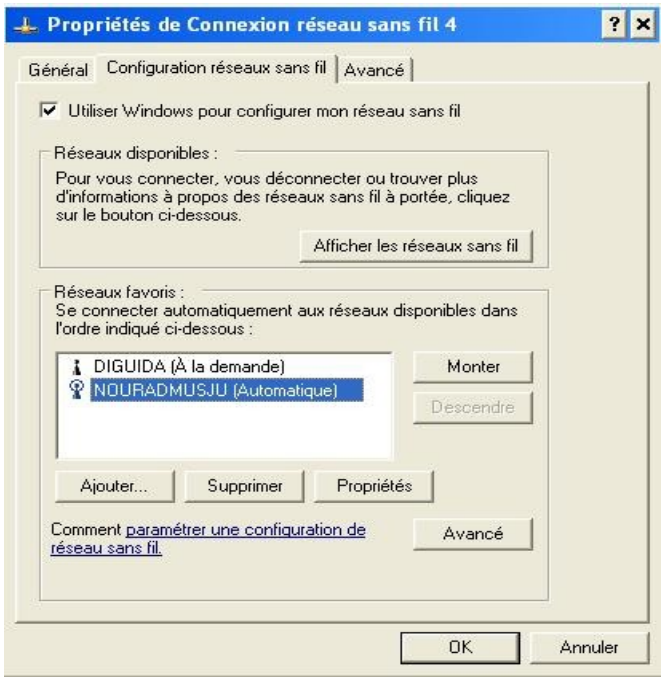


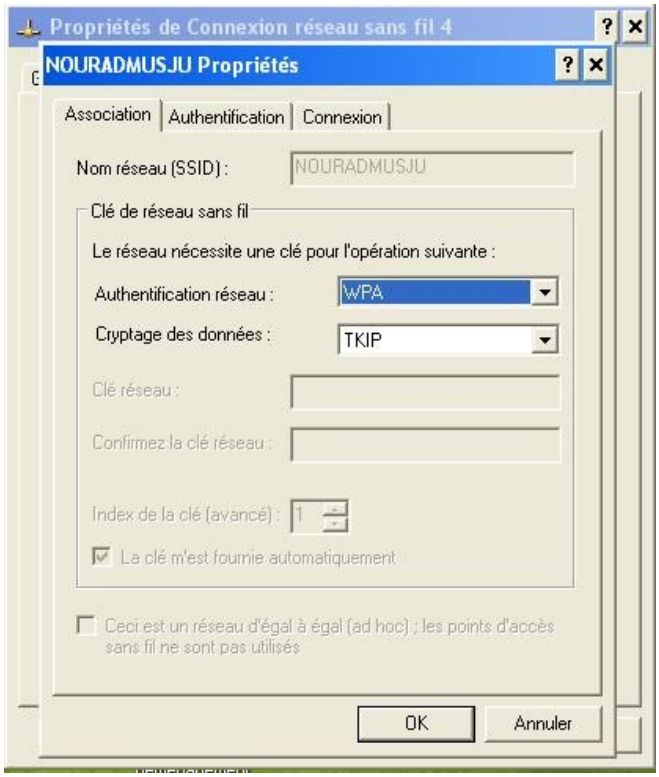
Enfin, dans le *Server Manager*, on créé le NAS en lui passant comme adresse de serveur RADIUS l'adresse IP du serveur Windows (le *Shared Secret* est fournit par Windows).



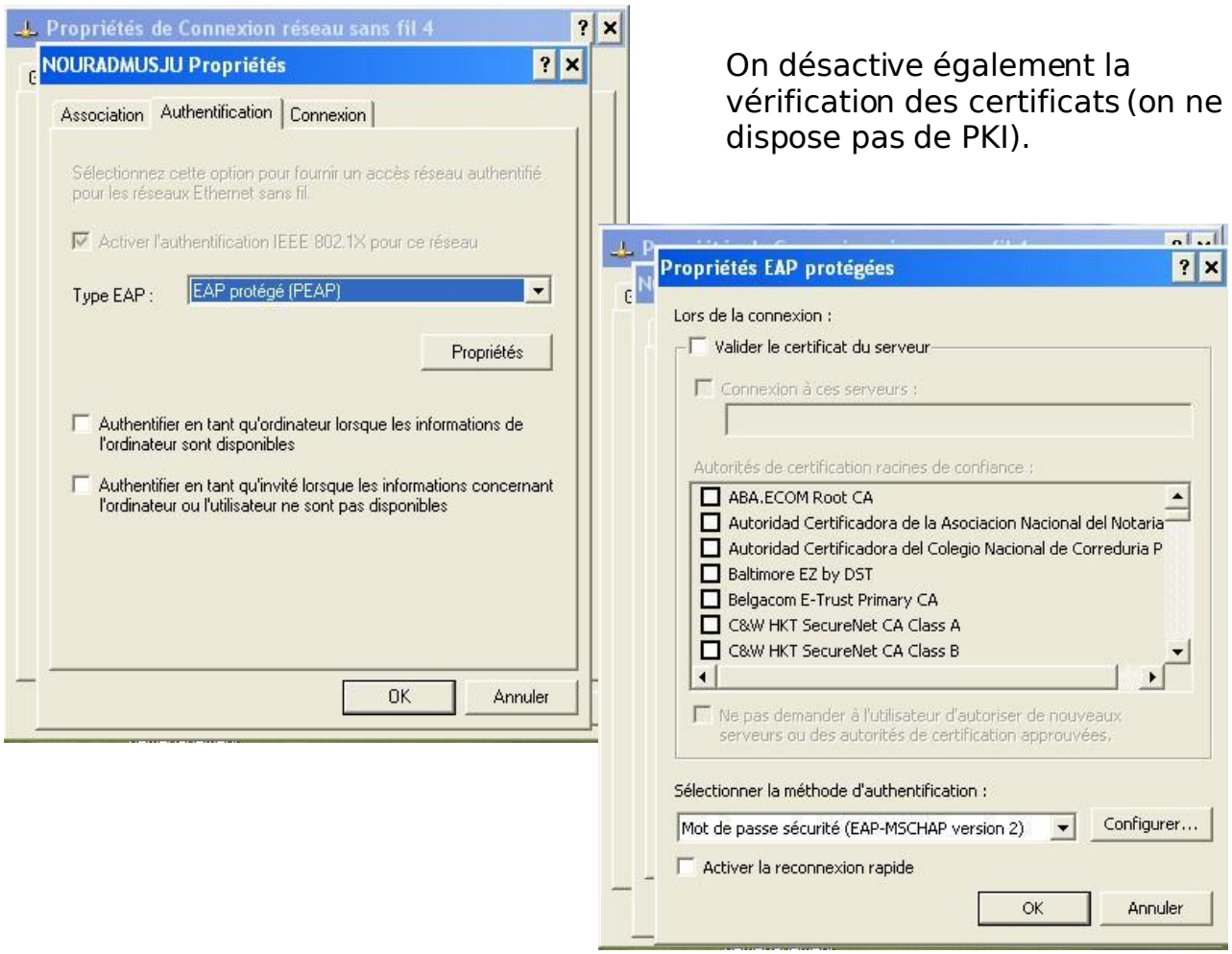
Au niveau du client, nous devons utiliser un poste sous Windows XP car la configuration de WPA2/RADIUS sous Linux n'est pas fonctionnelle. Wpa_supplicant le supporte mal et la documentation n'est pas du tout claire.

Sous Windows, on rentre dans les propriétés de la carte Wifi et l'on change les modes d'authentification et de chiffrement pour le SSID « *NOURADMUSJU* ».





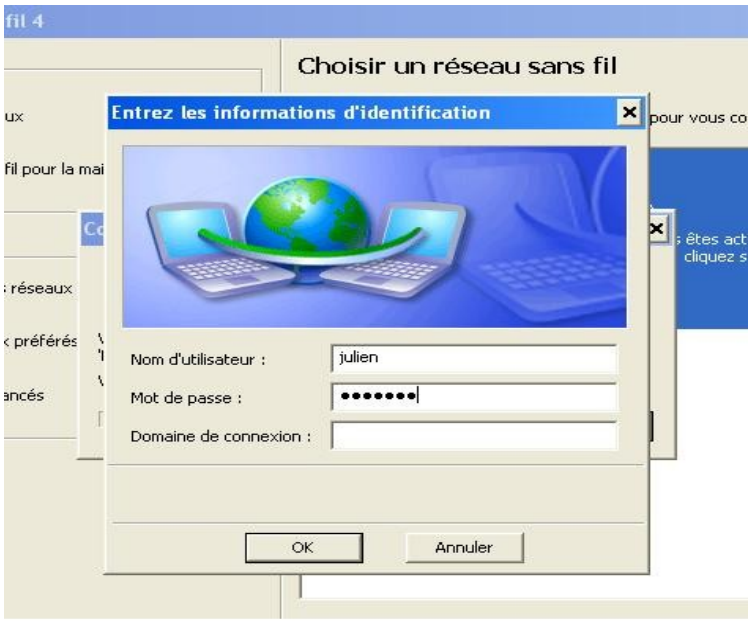
Le mode d'authentification supporté par Windows est PEAP.



On désactive également la vérification des certificats (on ne dispose pas de PKI).

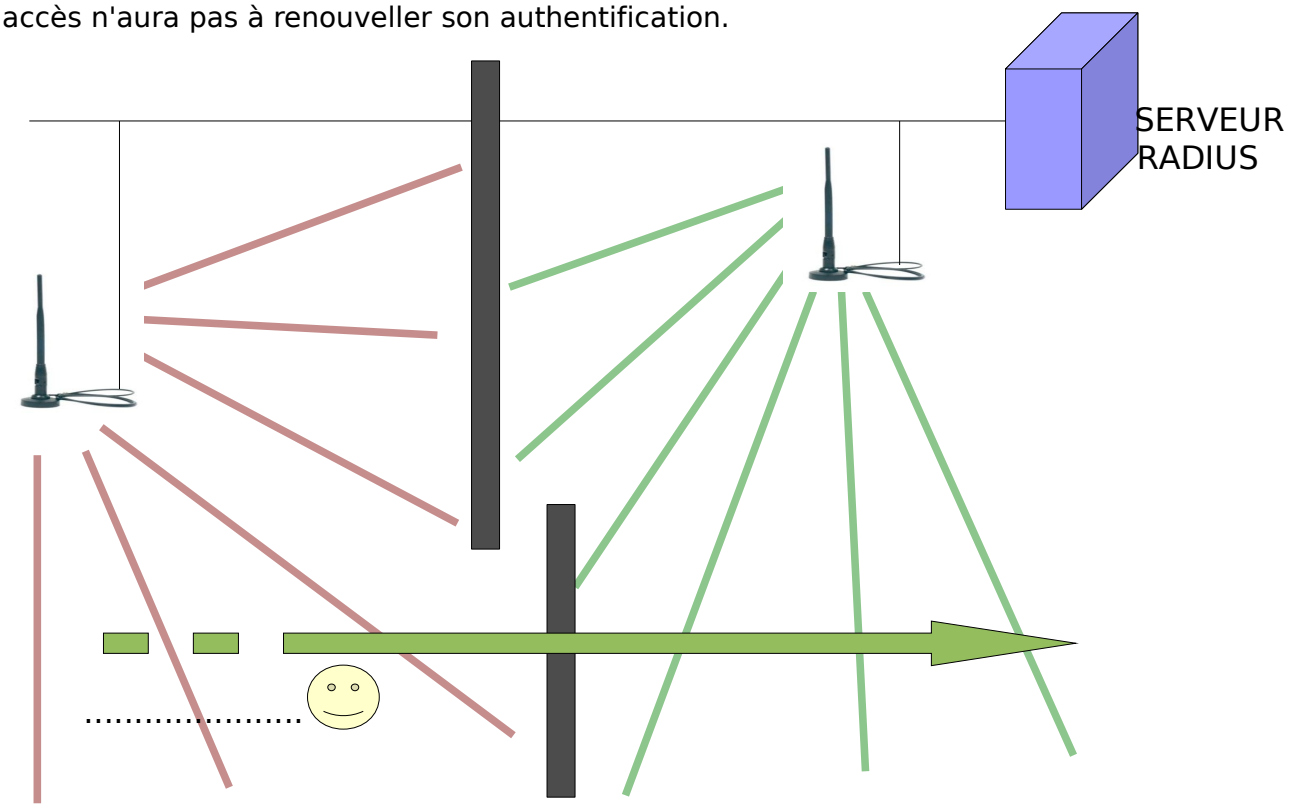
Dans la section *EAP-MSCHAP version 2*, on clique sur « configurer » pour désactiver l'utilisation systématique du compte Windows.

Enfin, lors de la connexion au réseau *NOURADMUSJU*, on saisie le nom d'utilisateur et le mot de passe existant dans le serveur RADIUS. Il faut avoir configuré celui-ci précédemment, mais ce ne sera pas vu dans ces pages.



Roaming

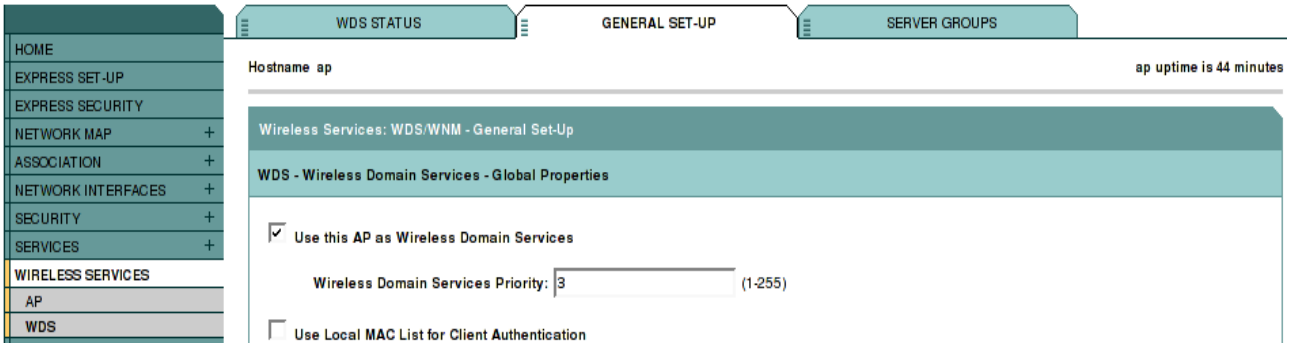
La technologie de Roaming permet de grouper un ensemble de points d'accès travaillant sous un seul SSID pour rendre transparent à l'utilisateur le passage du AP à un autre.
De fait, un utilisateur qui s'identifie via RADIUS sur un point d'accès et passe à un autre point d'accès n'aura pas à renouveller son authentification.



Roaming sur Cisco Aironet

Nous supposons que les deux points d'accès disposent d'un SSID nommé « 409 » et que ce SSID utilise l'identification RADIUS comme vu au chapitre précédent.

Ainsi, nous allons maintenant créer un WDS (*Wireless Distribution System*) qui va permettre l'inter-connexion des points d'accès.



Le niveau de priorité doit être différent entre les points d'accès pour que ces derniers puissent élire un maître et un backup.
Ceci est fait automatiquement lorsque deux points d'accès ayant le même SSID se voient.
Il est important de noter que les points d'accès proches doivent émettre sur des canaux

différents pour éviter les interférences.

Les élections WDS se font par Ethernet et non en 802.11. Les différents AP ne connaissant pas les adresses IP de leurs voisins, cette discussion doit être précédée d'un Broadcast des informations WDS.
Voici ce que montre l'interface d'un point d'accès WDS Backup :

Wireless Services: WDS - Wireless Domain Services - Status			
WDS Information			
MAC Address	IP Address	Priority	State
0015.63b0.ee40	10.6.0.221	3	BACKUP
Current Active WDS			
MAC Address		Priority	
0015.63b0.dd42		5	

On y retrouve bien le status Backup (priorité 3) et l'adresse MAC du point d'accès Maître (priorité 5).

Etude de risque finale

Après la mise en place des solutions, on procède de la même façon qu'avant pour analyser les risques. Les résultats suivants ont été obtenus.

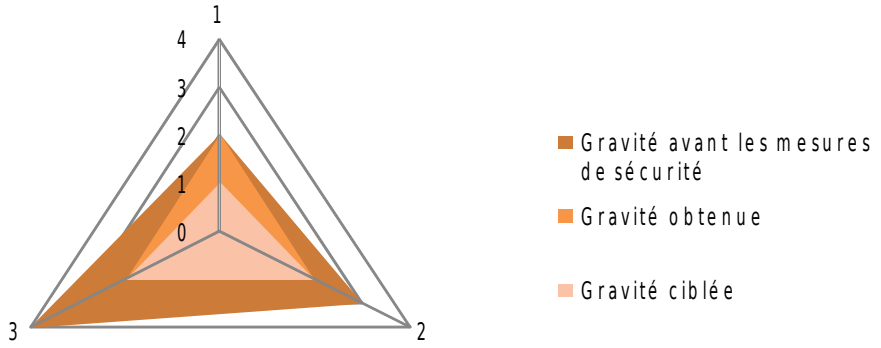
Matrice de gravité obtenue après les mesures de sécurité

Menaces	Impact (0 à 4)	Potentialité (0 à 4)	Gravité (0 à 4)
Brouillage radio	1	2	2
Mobilité de connexion	1	1	1
Modification de données	3	1	2
Interception de données	3	1	2
Accès illicite	3	1	

Résultats globaux

Risques	Disponibilité (0 à 4)	Intégrité (0 à 4)	Confidentialité (0 à 4)
Gravité avant mesures de sécurité	2	3	4
Gravité obtenue	2	2	2

On peut observer l'impact de nos mesures en ajoutant la dimension « gravité obtenue » sur notre radar :



Conclusion

Après la mise en place des solutions définies au début de projet nous avons réussit à ramener le risque d'un niveau critique à un niveau supportable. Il est important de noter que la mise en place de VLAN permettrais d'améliorer d'avantage le niveau de sécurité tant sur le réseau Wifi que sur le réseau filaire traditionnel.

Annexe 1 : Configuration WPA PSK

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname NOURADMUSJU
!
enable secret 5
$1$D9pl$nfxgFgKLdlclB2Pezmxvl.
!
ip subnet-zero
ip domain name Cisco
!
!
no aaa new-model
!
dot11 ssid NOURADMUSJU
   authentication open
   authentication key-management wpa
   wpa-psk ascii 7 0525293A136D6A242C363D27
!
power inline negotiation prestandard source
!
!
username Cisco password 7 00271A150754
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers tkip
 !
 ssid NOURADMUSJU
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0
basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel 2427
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-
24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.6.0.222 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.6.0.250
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/p
rodconfig/help/eag
!
!
control-plane
!
bridge 1 route ip
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 login local
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

Annexe 2 : Configuration RADIUS

```
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname NOURADMUSJU
enable secret 5
$1$D9pl$nfxgFgKLdlclB2Pezmxvl.
!
ip subnet-zero
ip domain name Cisco
!
aaa new-model
!
aaa group server radius rad_eap
 server 10.6.0.12 auth-port 1812 acct-port
1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
 cache expiry 1
 cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server tacacs+ tac_admin
 cache expiry 1
 cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group
rad_eap
aaa authentication login mac_methods local
aaa authorization exec default local
aaa accounting network acct_methods start-
stop group rad_acct
aaa cache profile admin_cache
 all
!
aaa session-id common
!
dot11 ssid NOURADMUSJU
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
!
power inline negotiation prestandard source
!
username Cisco password 7 00271A150754
username 001195f38190 password 7
03540B5A5756744A1D51485C47
username 001195f38190 autocommand exit
!
bridge irb
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 encryption mode ciphers tkip
 ssid NOURADMUSJU
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0
basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 channel 2427
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 speed basic-6.0 9.0 basic-12.0 18.0 basic-
24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.6.0.222 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.6.0.250
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/p
rodconfig/help/eag
ip radius source-interface BVI1
!
radius-server local
  nas 10.6.0.222 key 7
14393D3E3E250E06111B1900
  user NOURADMUSJU nthash 7
1441422A5B52790E76716460074522375659020F0177
7657564D457A0C7600040C
!
radius-server attribute 32 include-in-
access-req format %h
radius-server host 10.6.0.12 auth-port 1812
acct-port 1813 key 7 101F5B4A
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
end
```