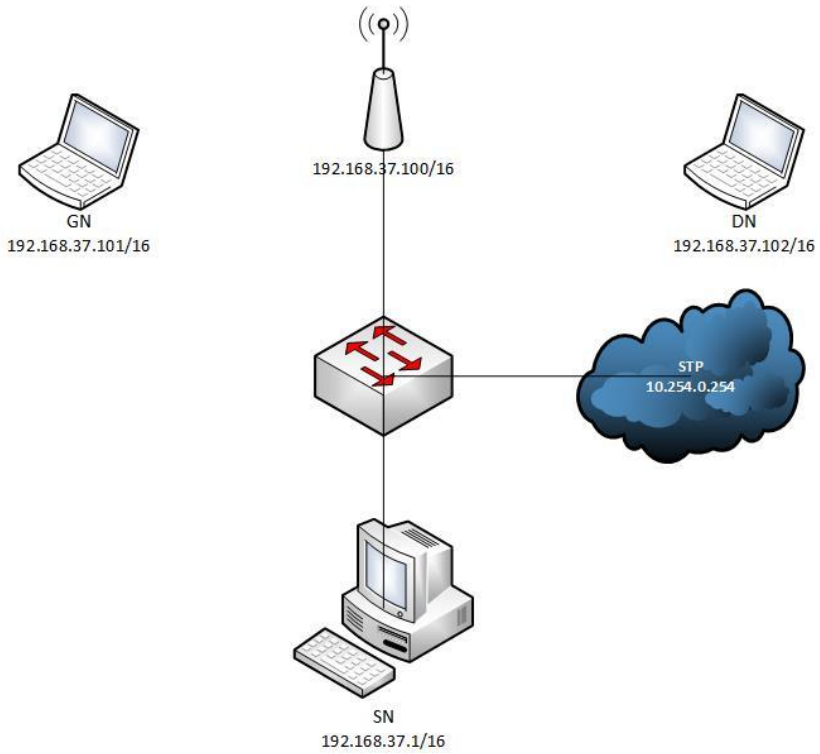
Introduction

Le Wifi (Wireless Fidelity) est une norme de communication destinée à créer des réseaux sans fil en utilisant des ondes radioélectriques. Aujourd'hui les besoins en wifi sont grandissants, la technologie propose en effet d'énormes avantages pour les entreprises comme la mobilité. Mais elle possède aussi quelques inconvénients comme une bande passante limitée ou encore la sécurité. Nous verrons donc au cours de ce TP le fonctionnement de cette nouvelle technologie ainsi que la sécurisation basique de ce genre d'architecture.

PARTIE 1- Mise en place du réseau

Systèmes d'exploitation : Windows XP



1.1 Test de connectivité

On peut observer la bonne connectivité à STP en utilisant sur le poste Sn la commande :

→ **Ping 10.254.0.254**

1.2 Reset du point d'accès

Pour remettre à zéro le point d'accès il faut appuyer sur le bouton reset et alimenté l'AP. Quand la LED jaune s'allume on peut relâcher le bouton. La configuration d'usine est alors rétablie.

1.3 Tableau des adresses MAC

Postes	Interfaces	Adresses MAC
S27	ETH0	00 : 04 : 75 : EF : 96 : 0A
	ETH2	00 : 04 : 75 : EF : 94 : F6
	WIFI	00 : 0F : CB : FA : D3 : 31
D27	ETH0	00 : 19 : B9 : 29 : FB : 74
	WIFI	00 : 0F : CB : F9 : D7 : F7
G27	ETH0	00 : 19 : B9 : 2F : 5F : AF
	WIFI	00 : 0F : CB : FA : D1 : F8
Borne WIFI	BVI1	00 : 17 : 95 : 49 : 11 : 10
	DOT11 RADIO 0	00 : 17 : 0F : 82 : 44 : 30
	DOT11 RADIO 1	00 : 17 : 0F : 86 : 44 : 10
	DOT11 RADIO 1.22	00 : 17 : 0F : 86 : 44 : 10
	DOT11 RADIO 1.23	00 : 17 : 0F : 86 : 44 : 10
	FA0	00 : 17 : 95 : 49 : 11 : 10
	FA0.1	00 : 17 : 95 : 49 : 11 : 10
	FA0.23	00 : 17 : 95 : 49 : 11 : 10

Il y a donc quatre adresses MAC sur le point d'accès pour les interfaces, Fa0, Dot11radio0, dot11radio1 et BVI1.
Fa0 représente l'interface Ethernet pour relier l'AP au réseau.
BVI1 (Bridge Virtual Interface 1) représente l'interface web pour administrer le point d'accès via un navigateur, elle fait la corrélation entre l'interface Filaire et les interfaces Wi-Fi.
Les Dot11radio0 et 1 représente les interfaces wifi.

De plus nous possédons un port «Console», qui permet d'effectuer la première configuration via HyperTerminal de la borne Wi-Fi (adresse ip, nom, mot de passe) et également une configuration avancée de la borne mais pour cela il faut très bien connaître toutes les commandes à utiliser.

1.4 Configuration par défaut du point d'accès

Pour accéder dans un premier temps à l'AP il faut rentrer le mot de passe par défaut qui est « Cisco », ensuite on peut observer la configuration de base du point d'accès.

On peut observer sur l'extrait de la commande « **sh run** » l'état des interfaces :

```
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown

interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown

interface FastEthernet0
```

```
 no ip address

interface BVI1
ip address dhcp client-id FastEthernet0
```

L'interface web BVI1 est active, l'adresse IP configuré en DHCP client de l'interface filaire.

L'interface 802.11a (Dot11Radio1) est inactive, elle ne possède pas d'adresse IP, on n'observe pas non plus de SSID de base.
Grâce à la commande « **sh controller** », on peut voir que le DFS (Dynamic Frequency Selection) est inactif par défaut.

```
Current Frequency : 0 Mhz Channel 0
```

PARTIE 2 - Première Configuration de votre point d'accès en ligne de commande

Configuration à mettre en place :

→ Adresse IP : 192.168.37.100

```
Ap>enable
Ap#conf t
Ap(conf)#int BVI1
Ap(conf-if)#ip add 192.168.37.100 255.255.0.0
```

→ SSID : poste27
Le SSID est le nom du réseau wifi que l'on verra apparaître sur les clients wifi.

```
Ap>enable
Ap#conf t
Ap(conf)#int dot11radio1
Ap(conf-if)#ssid poste27
```

→ DFS
Le mécanisme de DFS configure le choix du canal pour qu'il soit en conformité avec la réglementation française.

```
Ap>enable
Ap#conf t
Ap(conf)#int dot11radio1
Ap(conf-if)#dfs band 3 4  block
```

Apres cette commande l'interface radio utilise la bande de fréquence 2 qui va de 5.250 à 5.350 GHz et choisi un canal dans cet espace de fréquences.
La première fois que nous avons effectué cette manipulation la borne à choisi un canal étant déjà utilisé dans la salle, il a donc fallut refaire la manipulation pour obtenir un canal libre.

→Activation de l'interface radio :

```
Ap>enable
Ap#conf t
Ap(conf)#int dot11radio1
Ap(conf-if)#no sh
```

On peut voir désormais que la borne est configurée comme il nous l'a été demandé, comme le montre la commande suivante :

```
Ap>enable
Ap#sh run

Current configuration : 1585 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$y53y$pYsPaaTRnbZfsGhzjMC14/
!
ip subnet-zero
!
!
no aaa new-model
!
dot11 ssid poste27      //ici on voit le nom du ssid
!
power inline negotiation prestandard source
!
!
username Cisco password 7 00271A150754
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 shutdown // on remarque que l'interface dot11radio 0 est désactivée contrairement à l'interface
             dot11radio 1 qui est active puisqu'elle ne porte pas la mention shutdown
 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
 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
```

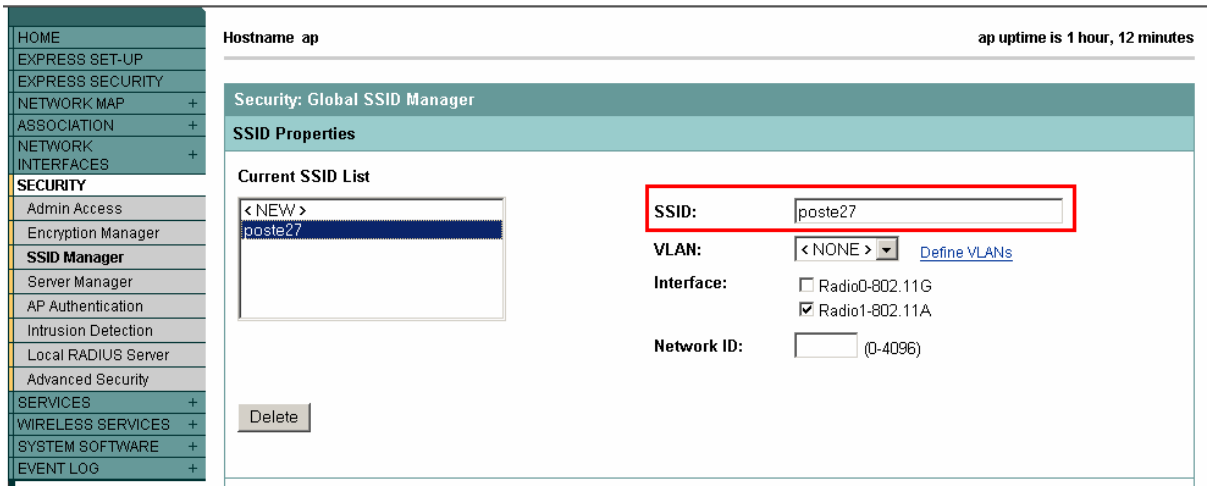
```
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 !
ssid poste27   //ici on voit le nom du ssid
 !
dfs band 3 4 block  //On voit que l'on bloque les espaces de fréquence  3 et 4 et donc que l'on
                    utilise le 1 et 2
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 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
 hold-queue 160 in
!
interface BVI1
ip address 192.168.37.100  255.255.0.0  //adresse ip que l'on a configurée pour la console Web
 no ip route-cache
!
ip http server // serveur web pour la configuration de l'AP dans un navigateur.
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag

control-plane
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
!

Ap>enable
Ap#sh controllers

interface Dot11Radio1
Radio AIR-AP1131A, Base Address 0017.0f86.4410, BBlock version 0.00, Software ve
rsion 5.90.8
Serial number: ALP10160881
Number of supported simultaneous BSSID on Dot11Radio1: 8
```

Carrier Set: ETSI (OFDM) (EU)
Uniform Spreading Required: Yes
Current Frequency: 5180 MHz Channel 36 (DFS enabled) **//Utilisation du canal 36 à la fréquence de 5180 MHz**
Allowed Frequencies: 5260(52) 5280(56) 5300(60) 5320(64)
Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) **5180(36)** 5200(40) 5220(4
4) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64) 5500(100) 5520(104) 5540(108) 55
60(112) 5580(116) 5600(120) 5620(124) 5640(128) 5660(132) 5680(136) 5700(140) 57
45(149) 5765(153) 5785(157) 5805(161) 5825(165)
DFS Blocked Frequencies:
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
Current Rates: basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Active Rates: basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Allowed Rates: 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates: basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates: basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-24.0 bas
ic-36.0 basic-48.0 basic-54.0

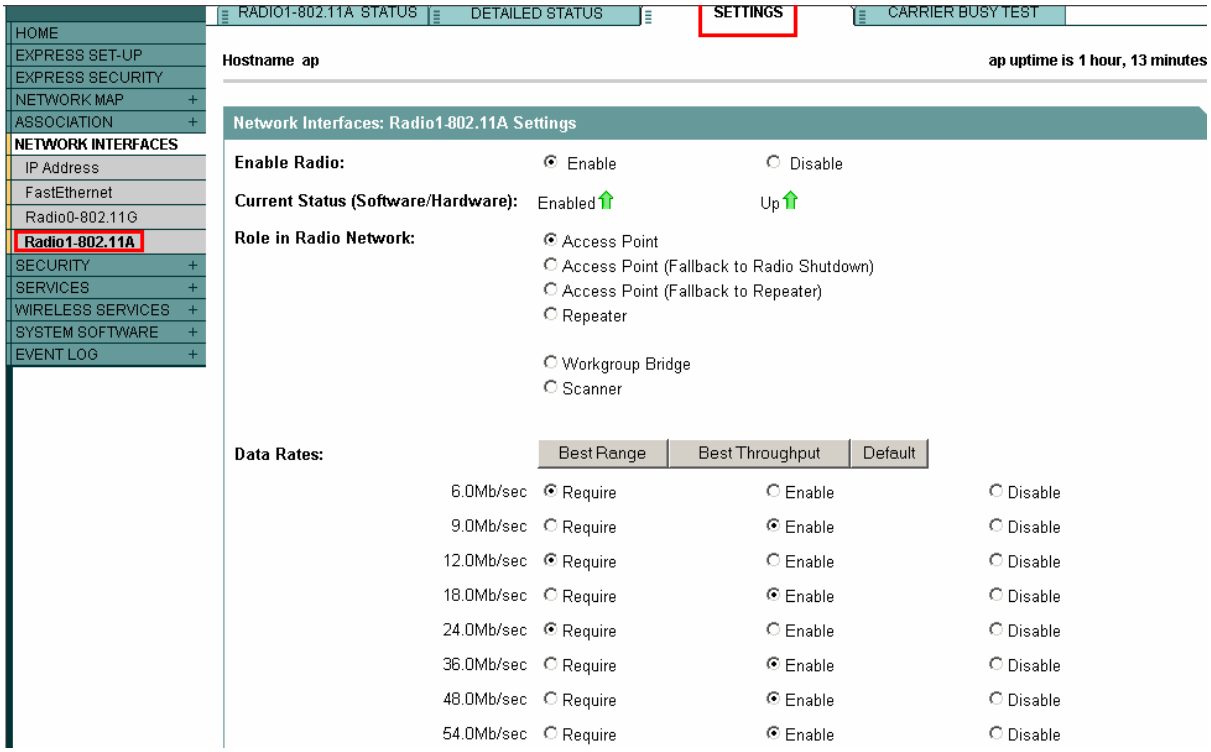
PARTIE 3 - Configuration du point d'accès par l'interface Web

Pour pouvoir accéder, à l'interface web de l'AP, il faut taper l'adresse IP de BVI1 dans le navigateur du poste Sn (http:// 192.168.37.100).

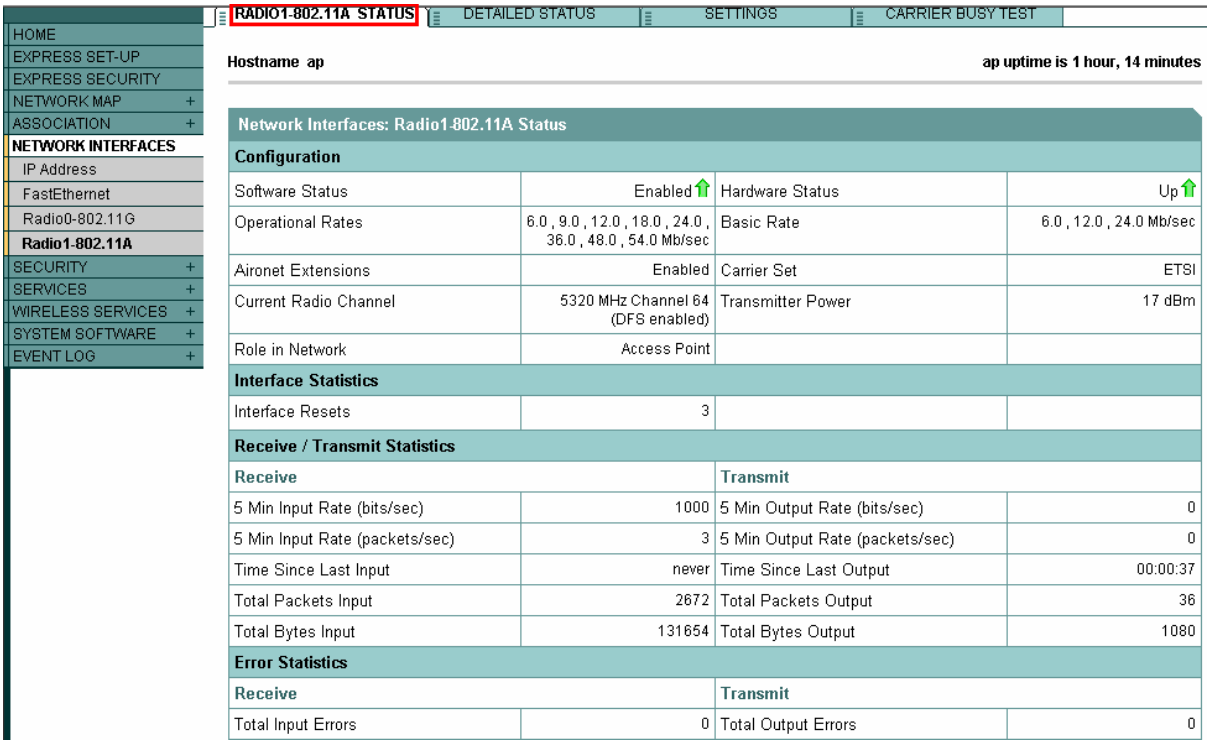
<u>On retrouve dans l'interface Web</u> :
→ La configuration du SSID :



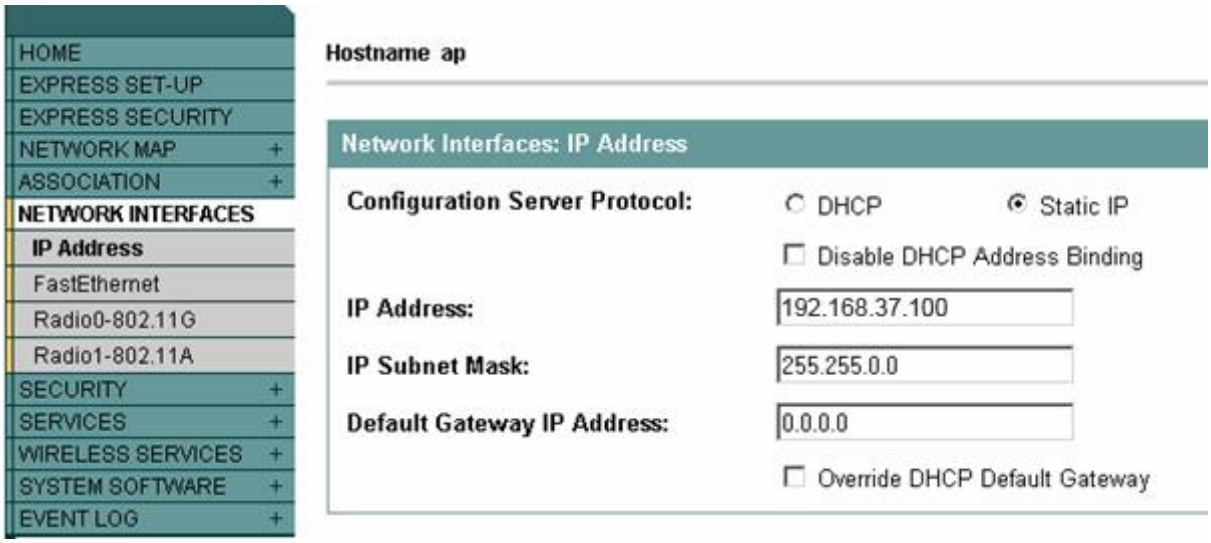
→ La configuration de la partie radio 802.11a:



→ Observation de la configuration radio :



Configuration de l'adresse IP de l'interface Web :

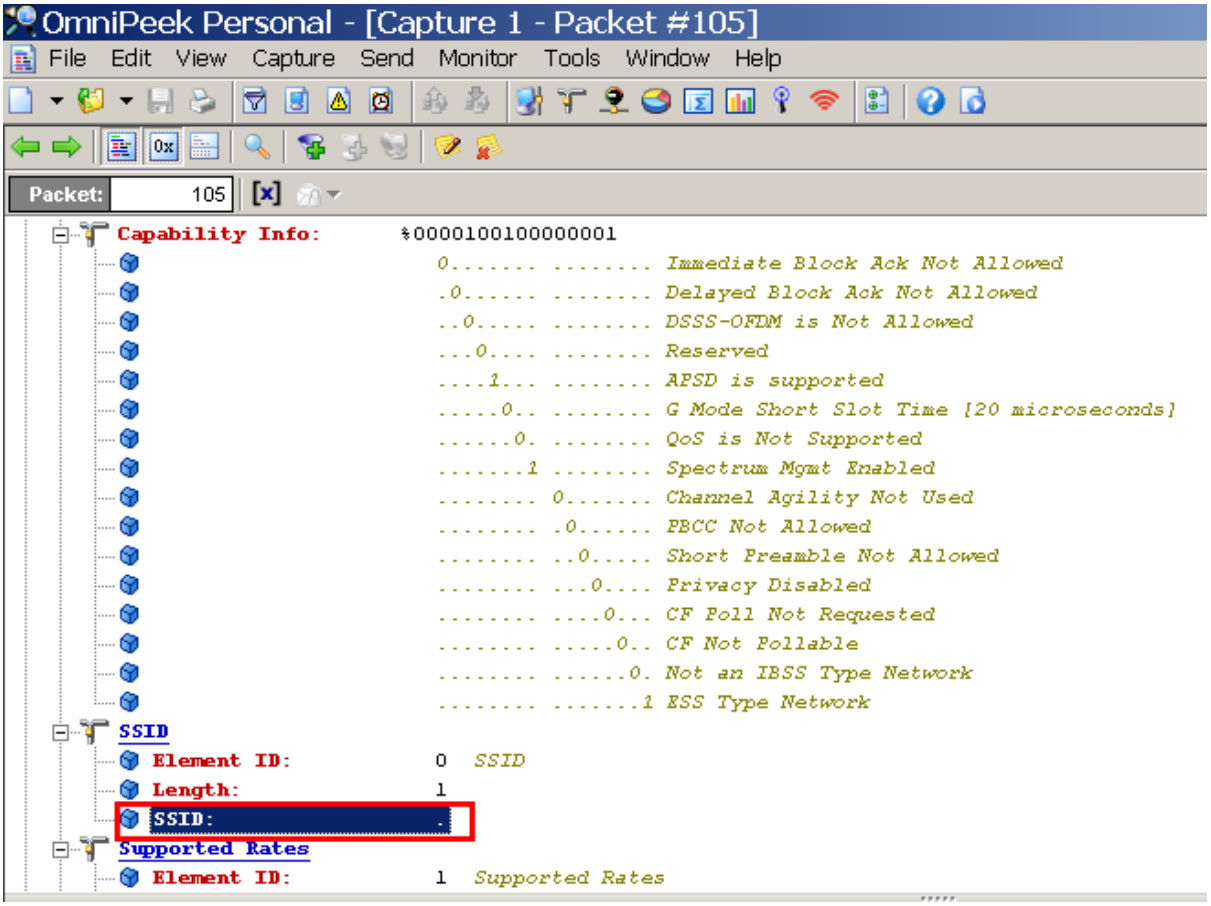


Connexion des postes Gn et Dn clients au réseau Wi-Fi :

Le problème est que les postes ne pas voient le réseau Wi-Fi.

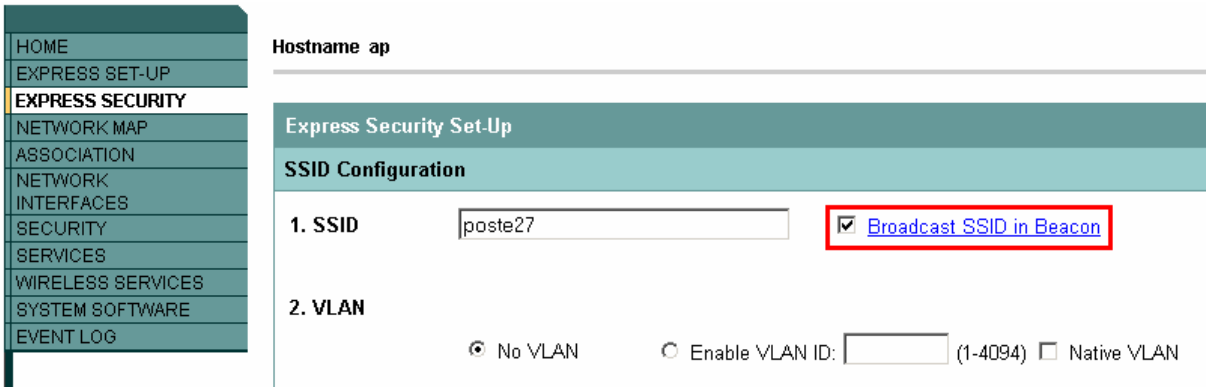
Nous procédons donc à une analyse de trames à l'aide du logiciel « omnipeek personal » sur le poste Sn, pour voir ou se situe le problème et nous analysons plus particulièrement une trame de beacon.

Ceci est réalisable dans la mesure où l'AP se comporte comme un HUB, est donc tous le monde peut observer le trafic.



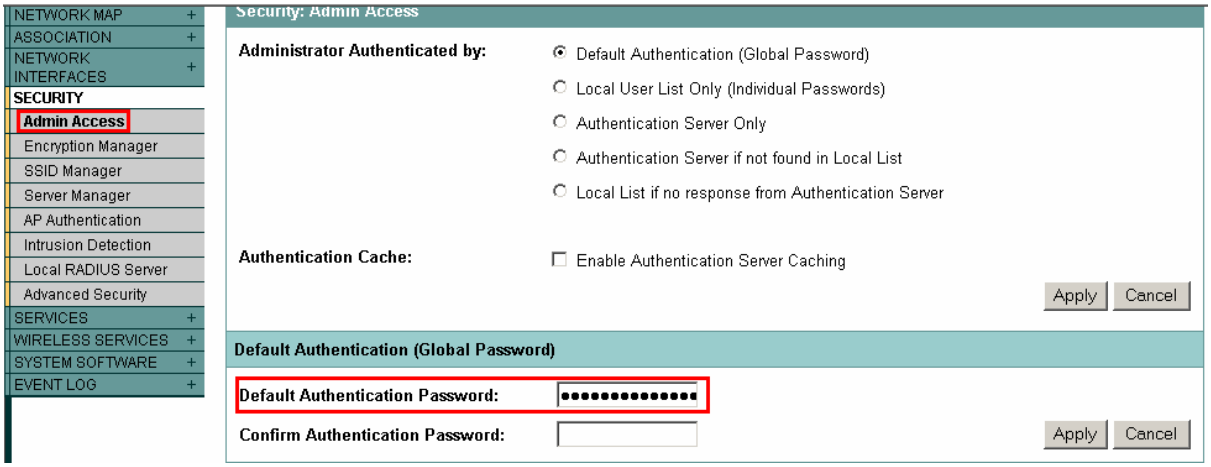
On constate donc que le champ SSID est vide, c'est-à-dire que le SSID n'est pas diffusé par la borne Wi-Fi, c'est donc tout à fait normal que sur les clients on ne voit pas le réseau WI-FI.

Il faut donc compléter la configuration du point d'accès pour corriger ce problème, nous allons donc valider la diffusion du SSID sur le réseau en cochant la case « broadcast SSID in beacon».



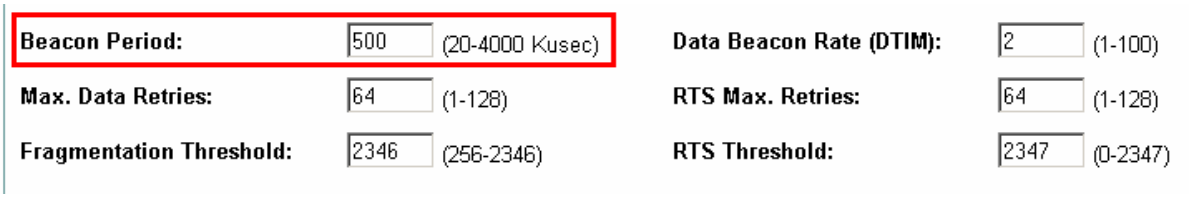
Désormais les clients Gn et Dn voient le réseau SSID poste27, il suffit de double cliquer dessus pour s'y connecter.

Sécurisation de base du point d'accès :
Nous allons maintenant sécuriser le point d'accès en mettant un mot de passe autre que celui par défaut (Cisco).
Pour cela il faut modifier la valeur du champ « default authentification password ».



PARTIE 4 – Analyse de trames entre deux postes Windows XP

Configuration du point d'accès pour la capture de trames :
Dans un premier temps nous réglons à 500 ms l'envoie des trames de beacon.



Pour les différentes captures que nous allons faire, nous prendrons un ping contenant quatre ping request et 4 ping reply, depuis la poste Gn. Nous influerons donc sur les champs fragmentation et RTS ci-dessus, afin d'observer les différents changements.

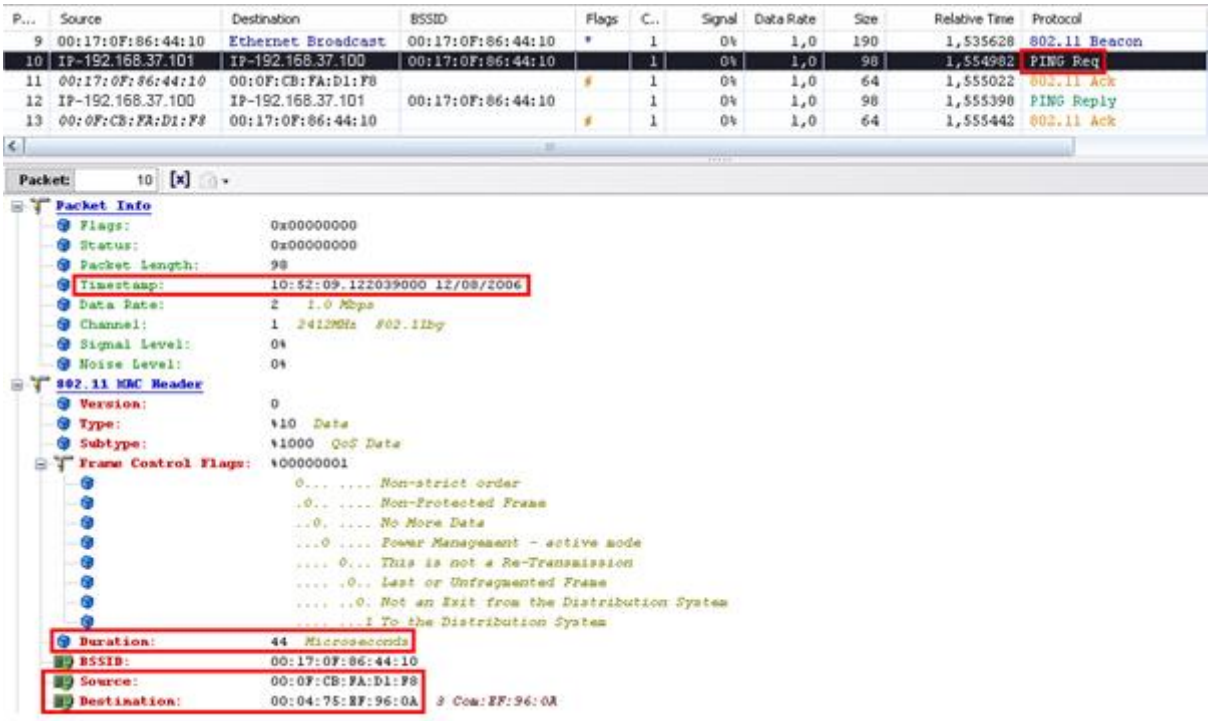
Rappels :
La fragmentation sur les points d'accès, consiste à découper les trames. L'intérêt est de réduire les chances de parasitage, des trames plus petites ont moins de chance d'être parasitées.
Le RTS (Request to Send) est une demande de réservation de « temps de parole » afin d'éviter les problèmes de stations cachées.

Champs de réglages :

Fragmentation Threshold : taille maximale des paquets envoyés (en octets). Il faut noter que plus le paquet est gros et plus les conséquences d'une mauvaise réception de ce paquet seront importantes car il faut alors retransmettre le paquet entièrement.

RTS Threshold : taille d'un paquet de données (en octets) à partir de laquelle l'émetteur va faire une demande de droit de parole afin qu'aucun autre émetteur ne fasse d'émission au même moment, ce qui entraînerait une collision ayant pour conséquence la perte des paquets émis. Cette valeur est à diminuer dans le cadre d'un réseau avec beaucoup de trafic afin d'éviter au maximum les collisions et l'écroulement des débits.

4.1 Capture de Ping entre Gn et Sn sans fragmentation ni RTS/CTS
Valeur du champ Fragmentation : 2346
Valeur du champ RTS : 2347
Les valeurs sont suffisamment hautes ne permettant pas l'activation des mécanismes, dans la mesure où l'on envoi un ping contenant 32 octets de données.



Adresse MAC source	Adresse MAC destination	trame	timestamp	duration
00:0F:CB:FA:D1:F8 (Gn)	00:04:75:EF:96:0A (Sn)	Ping req	10:52:09.122039000 12/08/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:FA:D1:F8 (Gn)	ack	10:52:09.122079000 12/08/2006	0 µs
00:04:75:EF:96:0A (Sn)	00:0F:CB:FA:D1:F8 (Gn)	Ping reply	10:52:09.122455000 12/08/2006	44 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	10:52:09.122499000 12/08/2006	0 µs

Analyse :

Les trames pertinentes de que nous pouvons relevées dans cette capture sont : Ping Req, Ack, PING reply.

Le ping request désigne l'envoi d'une trame sur le poste de destination afin de vérifier la connectivité avec celui-ci (de Gn à Sn).

En retour l'AP acquitte la trame qu'il vient de faire transité, pour préciser au poste initiateur du ping que la trame à bien été envoyer vers poste Sn.

Le poste Sn envoie sa répond au poste Gn c'est le ping reply, qui permet de confirmer au poste Gn que Sn à bien reçue le ping.

Enfin le poste Gn envoi un ACK à l'AP pour confirmer qu'il à bien reçu le reply.

4.2 Capture de Ping entre Gn et Sn sans fragmentation, avec RTS/CTS à 400

Valeur du champ Fragmentation : 2346

Valeur du champ RTS : 400

Adresse MAC source	Adresse MAC destination	trame	timestamp	duration
00:0F:CB:FA:D1:F8 (Gn)	00:04:75:EF:96:0A (Sn)	Ping req	11:04:41.564710000 12/08/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:FA:D1:F8 (Gn)	ack	11:04:41.564752000 12/08/2006	0 µs
00:04:75:EF:96:0A (Sn)	00:0F:CB:FA:D1:F8 (Gn)	Ping reply	11:04:41.565136000 12/08/2006	44 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	11:04:41.565180000 12/08/2006	0 µs

Analyse :

Les trames pertinentes de que nous pouvons relevées dans cette capture sont : Ping Req, Ack, Ping reply.

On observe les mêmes trames que la question précédente, cela s'explique par le fait que le RTS est réglé à 400 octets ce qui signifie que le mécanisme se déclenche uniquement pour les trames supérieur ou égal à 400 octets. Or dans notre cas le ping est envoyée avec la valeur par défaut c'est-à-dire 32 octets. On ne voit donc pas apparaître de trames RTS/CTS dans la capture.

4.3 Capture de Ping de 1200 octets entre Gn et Sn avec fragmentation à 500, avec RTS/CTS à 400

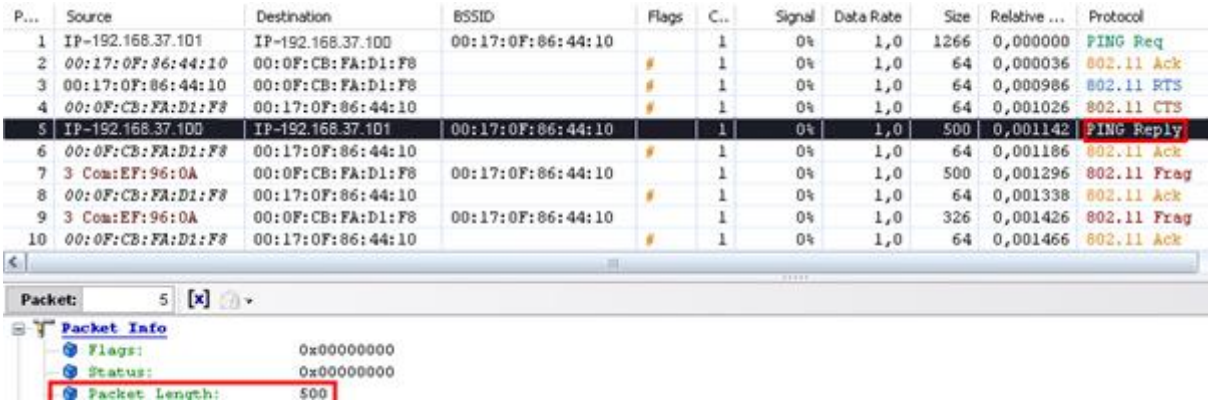
Valeur du champ Fragmentation : 500

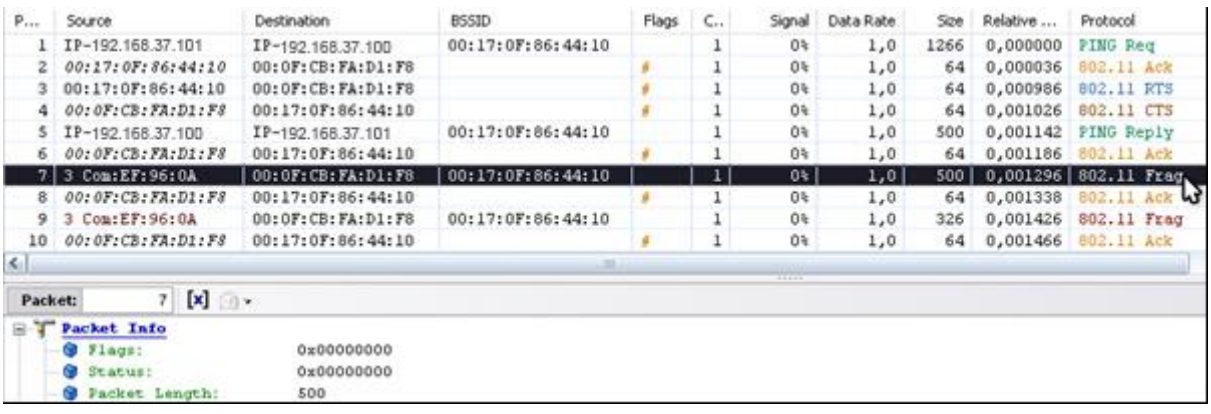
Valeur du champ RTS : 400

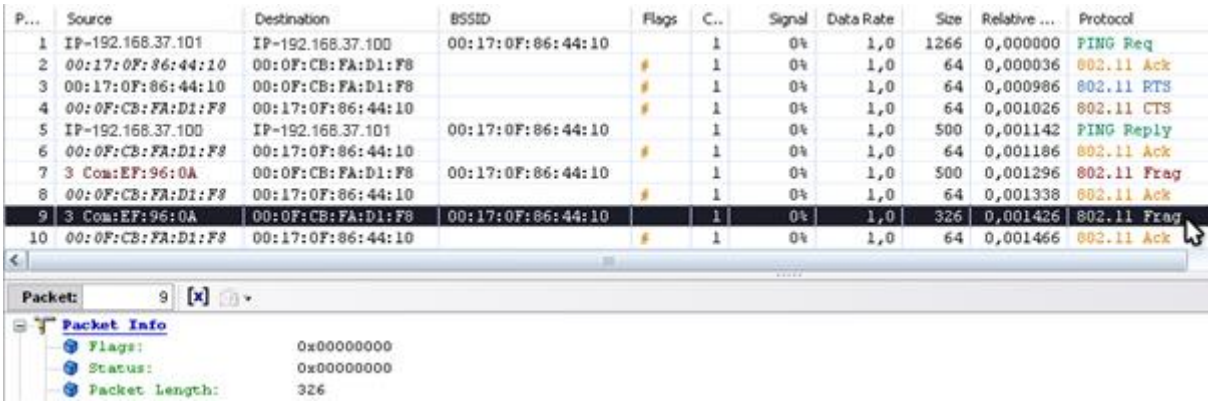
Adresse MAC source	Adresse MAC destination	trame	timestamp	duration
00:0F:CB:FA:D1:F8 (Gn)	00:04:75:EF:96:0A (Sn)	Ping req	11:07:52.415642000 12/08/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:FA:D1:F8 (Gn)	ack	11:07:52.415678000 12/08/2006	0 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:FA:D1:F8 (Gn)	RTS	11:07:52.416628000 12/08/2006	200 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	CTS	11:07:52.416668000 12/08/2006	156 µs
00:04:75:EF:96:0A (Sn)	00:0F:CB:FA:D1:F8 (Gn)	Ping reply	11:07:52.416784000 12/08/2006	200 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	11:07:52.416828000 12/08/2006	156 µs
00:04:75:EF:96:0A (Sn)	00:0F:CB:FA:D1:F8 (Gn)	frag	11:07:52.416938000 12/08/2006	176 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	11:07:52.416980000 12/08/2006	132 µs
00:04:75:EF:96:0A (Sn)	00:0F:CB:FA:D1:F8 (Gn)	frag	11:07:52.417068000 12/08/2006	44 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	11:07:52.417108000 12/08/2006	0 µs

Analyse :

Les trames pertinentes de que nous pouvons relevées dans cette capture sont : Ping Req, Ack, RTS, CTS, PING reply, Frag.







P...	Source	Destination	BSSID	Flags	C..	Signal	Data Rate	Size	Relative ...	Protocol
1	IP-192.168.37.101	IP-192.168.37.100	00:17:0F:86:44:10		1	0%	1,0	1266	0,000000	PING Req
2	00:17:0F:86:44:10	00:0F:CB:FA:D1:F8		#	1	0%	1,0	64	0,000036	802.11 Ack
3	00:17:0F:86:44:10	00:0F:CB:FA:D1:F8		#	1	0%	1,0	64	0,000986	802.11 RTS
4	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		#	1	0%	1,0	64	0,001026	802.11 CTS
5	IP-192.168.37.100	IP-192.168.37.101	00:17:0F:86:44:10		1	0%	1,0	500	0,001142	PING Reply
6	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		#	1	0%	1,0	64	0,001186	802.11 Ack
7	3 Com:EF:96:0A	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		1	0%	1,0	500	0,001296	802.11 Frag
8	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		#	1	0%	1,0	64	0,001338	802.11 Ack
9	3 Com:EF:96:0A	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		1	0%	1,0	326	0,001426	802.11 Frag
10	00:0F:CB:FA:D1:F8	00:17:0F:86:44:10		#	1	0%	1,0	64	0,001466	802.11 Ack

On remarque que le ping request à une taille de 1266 octet, car nous l'avons précisé dans l'envoi de la commande ping (-l 1200).
L'ACK envoyé par l'AP à Gn, confirme l'envoi de cette trame à Sn.
En temps normal, le RTS correspond à la réservation « de temps de parole » du client à l'AP, et Le CTS correspond la confirmation de L'AP du temps de parole du client. Mais dans notre cas ces échanges sont inversés, c'est le point d'accès qui envoi le RTS et le client qui envoi le CTS. Cela s'explique par le fait que la carte wifi 3Com du client wifi, ne gère pas de le RTS/CTS.
On observe sur les différentes captures ci-dessus, que notre paquet de 1200 octets est découpé en trois morceaux, ping reply, frag, frag, grâce à la fragmentation qui découpe les trames à partir de 500 octets.

4.4 Capture de Ping entre Gn et Dn sans fragmentation, sans RTS/CTS

Valeur du champ Fragmentation : 2346
Valeur du champ RTS : 2347 (avec cette valeur on supprime le RTS/CTS)

Adresse MAC source	Adresse MAC destination	trame	timestamp	duration
00:0F:CB:FA:D1:F8 (Gn)	00:0F:CB:F9:D7:F7 (Dn)	Ping req	16:54:49.114187000 12/11/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:FA:D1:F8 (Gn)	ack	16:54:49.114227000 12/11/2006	0 µs
00:0F:CB:F9:D7:F7 (Dn)	00:17:0F:86:44:10 (AP)	Null data	16:54:49.128673000 12/11/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:F9:D7:F7 (Dn)	ack	16:54:49.128713000 12/11/2006	0 µs
00:0F:CB:FA:D1:F8 (Gn)	00:0F:CB:F9:D7:F7 (Dn)	Ping req	16:54:49.128865000 12/11/2006	44 µs
00:0F:CB:F9:D7:F7 (Dn)	00:17:0F:86:44:10 (AP)	ack	16:54:49.128907000 12/11/2006	0 µs
00:0F:CB:F9:D7:F7 (Dn)	00:0F:CB:FA:D1:F8 (Gn)	Ping reply	16:54:49.129185000 12/11/2006	44 µs
00:17:0F:86:44:10 (AP)	00:0F:CB:F9:D7:F7 (Dn)	ack	16:54:49.129225000 12/11/2006	0 µs
00:0F:CB:F9:D7:F7 (Dn)	00:0F:CB:FA:D1:F8 (Gn)	Ping reply	16:54:49.129441000 12/11/2006	44 µs
00:0F:CB:FA:D1:F8 (Gn)	00:17:0F:86:44:10 (AP)	ack	16:54:49.129481000 12/11/2006	0 µs

Analyse :

Les trames pertinentes de que nous pouvons relevées dans cette capture sont : Ping Req, Ack, Ping reply, Null data.
On note dans cette configuration qu'il y a deux requêtes « ping request » et « ping reply » avec leurs ACK respectif. Et également la présence de la trame « null data » avec son ACK. On peut expliquer ces doublons par le fait que le poste Sn qui capture la trame est en dehors de l'échange entre Gn et Dn. Par conséquent il voit une première fois la trame entre GN et l'AP puis une deuxième fois entre l'AP et Dn.

Diagramme des trames échangées dans le cas le plus représentatif (4.3):

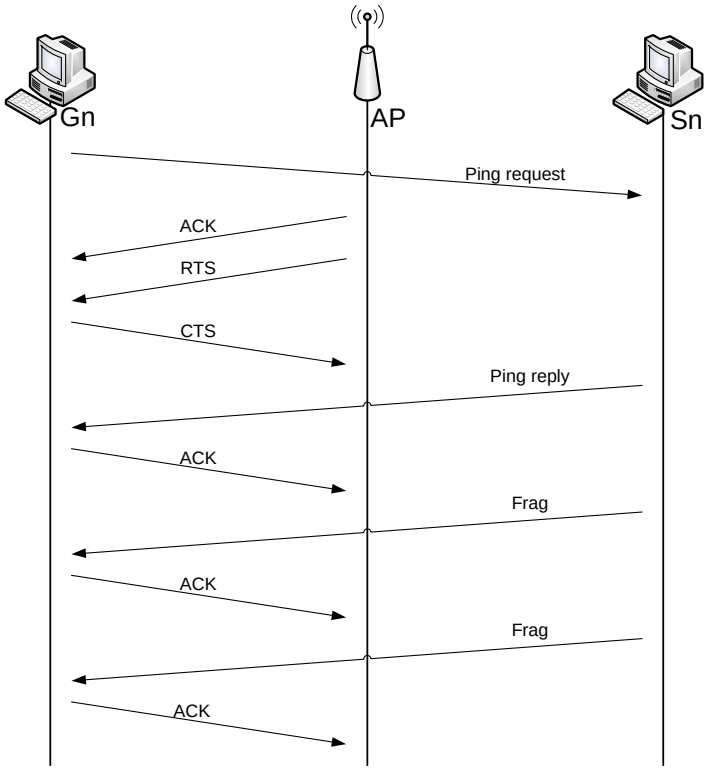
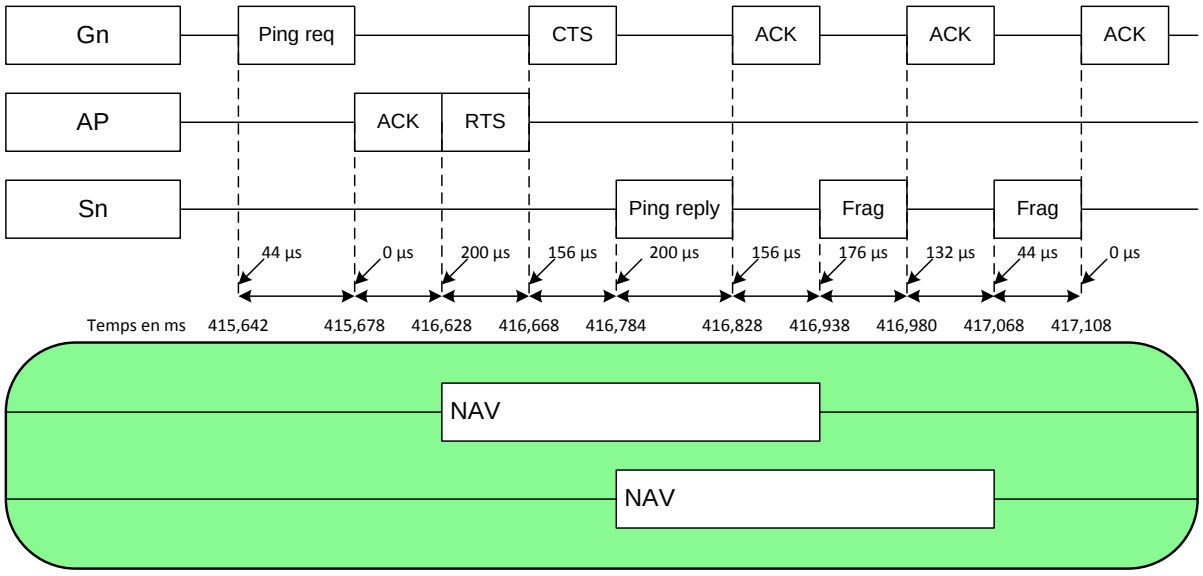


Diagramme de réservation de temps dans le cas le plus représentatif (4.3)



Analyse :

On peut observer sur le diagramme, deux réservations de temps dans la mesure où nous avons trois fragments, et que la taille du dernier est en dessous du seuil minimal du RTS fixé à 400. Il n'y a donc pas de réservation de temps pour ce dernier.

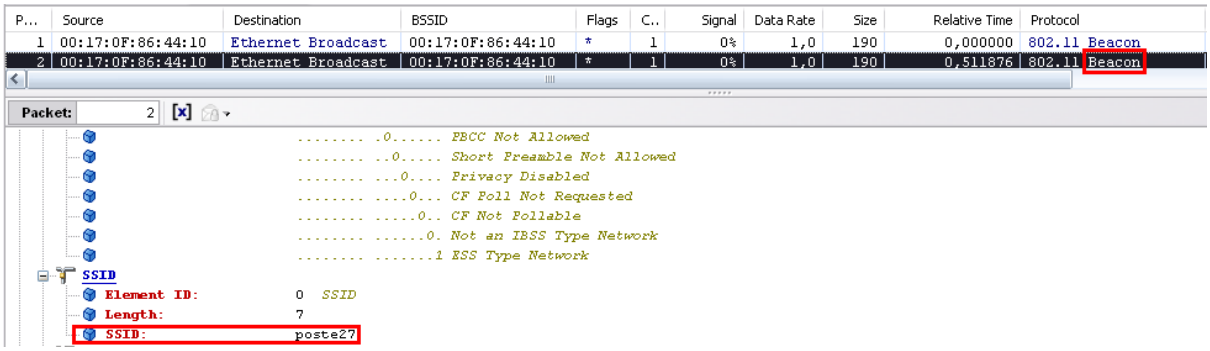
Le rôle de la réservation de temps est d'éviter qu'un client x de l'AP parle en même temps, qu'un autre client y (pour ce faire le client y réserve du temps de parole)

Le processus de réservation de temps : Le client demande au point d'accès s'il peut réserver du temps de parole, le point d'accès lui répond positivement si le media n'est pas occupé. Si le media est occupé alors le client attend réessaye de nouveau.

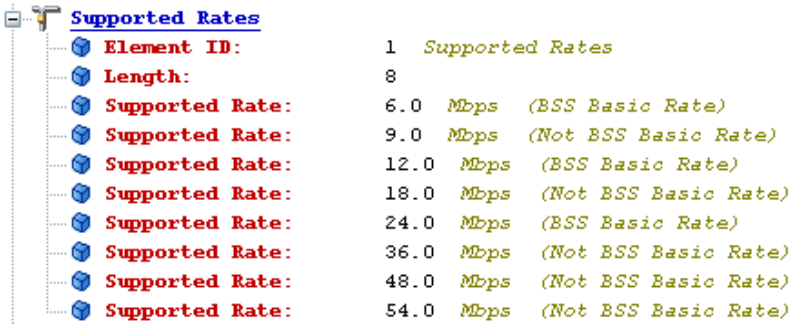
PARTIE 5 – Analyse d'une trame de beacon

Rappel :

Un point d'accès envoie périodiquement des trames de beacon pour annoncer sa présence et relayer des informations, comme le SSID et d'autres paramètres. Les clients écoutent continuellement tous les canaux, ainsi que les trames de type BEACON, qui sont à la base du choix du canal.

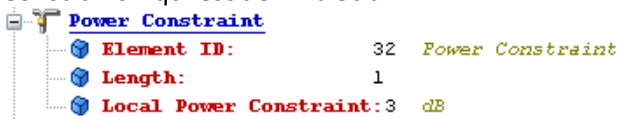


La trame est un broadcast envoyé par le Point d'accès, elle permet entre autre comme on peut le remarquer la diffusion du SSID.

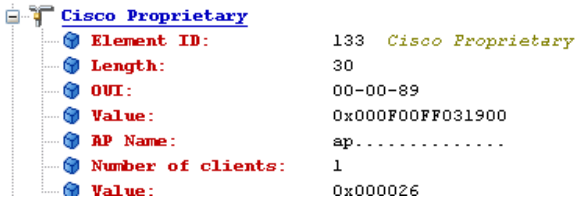


La trame de beacon, contient également des informations sur taux de transmissions que doit posséder la carte cliente.

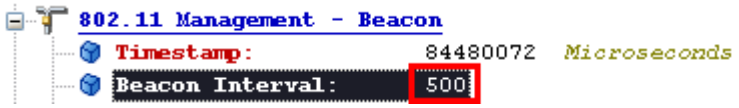
On retrouve également une information concernant la gestion de l'énergie, le « Local Power Constraint » qui est défini à 3db.



Enfin on peut constater que l'on peut relever la marque du point d'accès, à savoir ici Cisco, ainsi que le nom du point d'accès qui est par défaut «ap »



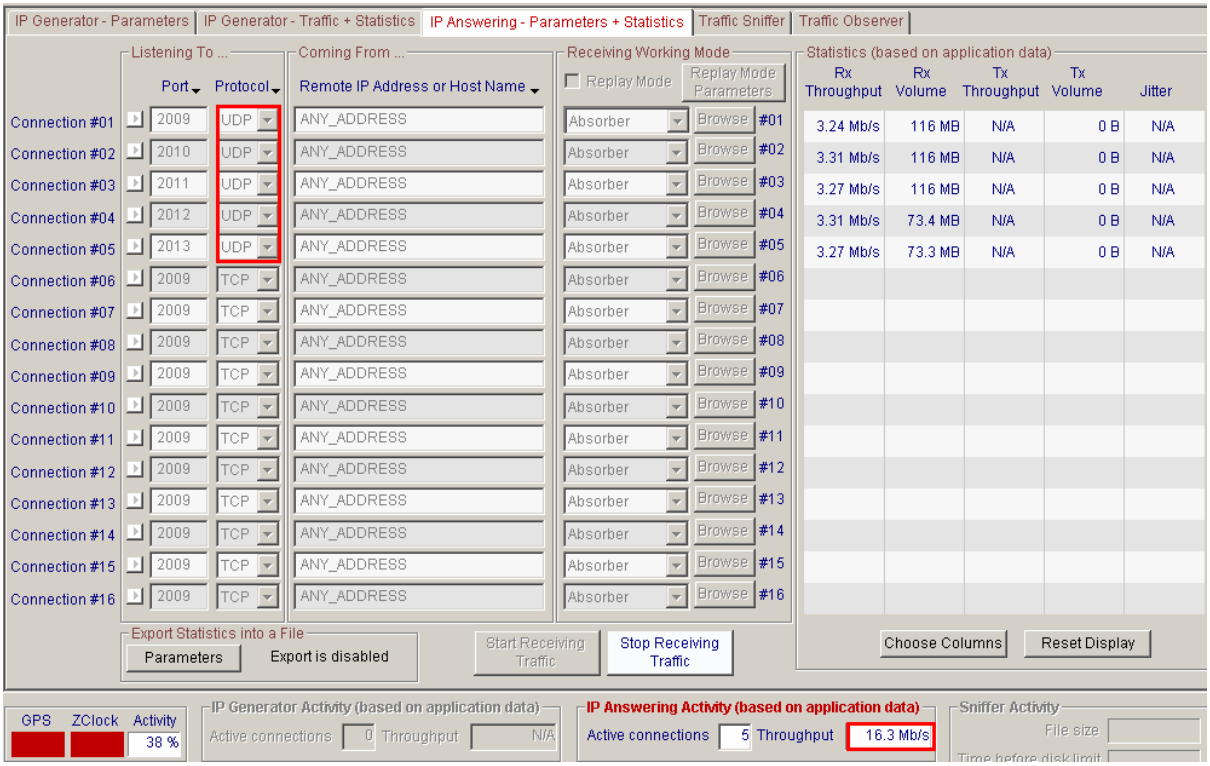
On retrouve également l'intervalle de diffusion des trames de beacon, défini sur le point d'accès à 500 ms.



Enfin on note la présence d'un contrôle à la fin de la trame le FCS, qui vérifie l'intégrité de cette dernière.

PARTIE 6 – Analyse des performances du réseau Wifi

Pour cette partie, nous utiliserons le logiciel IPTraffic qui permet de simuler une charge du réseau. Nous pourrons ainsi observer l'influence des paramètres facultatifs, sur les performances du réseau. Pour ce faire nous configurerons le poste Gn en tant que générateur de 5 trafics UDP de débit 10mbits/s, avec des trame de taille 1460 octets. Les postes Sn et Dn serons « les absorbers ».



Mesure :

Cas	RTS	Fragmentation	Manipulation	débit
1	Non	Non	Client wifi -> PA -> Client Filaire	17,0 Mb/s
2	400	Non	Client wifi -> PA -> Client Filaire	16,8 Mb/s
3	Non	500	Client wifi -> PA -> Client Filaire	16,5 Mb/s
4	Non	1000	Client wifi -> PA -> Client Filaire	16,9 Mb/s
5	400	1000	Client wifi -> PA -> Client Filaire	18,5 Mb/s
6	Non	Non	Client wifi -> PA -> Client Wifi	10,1 Mb/s
7	400	500	Client wifi -> PA -> Client Wifi	7,39 Mb/s

Analyse :

On peut relever que dans le cadre d'un trafic d'un client wifi vers un client filaire, les débits varient peut suivant les réglages facultatifs, sauf pour le cas 5 ou l'on réduit le RTS à 400 et on place la

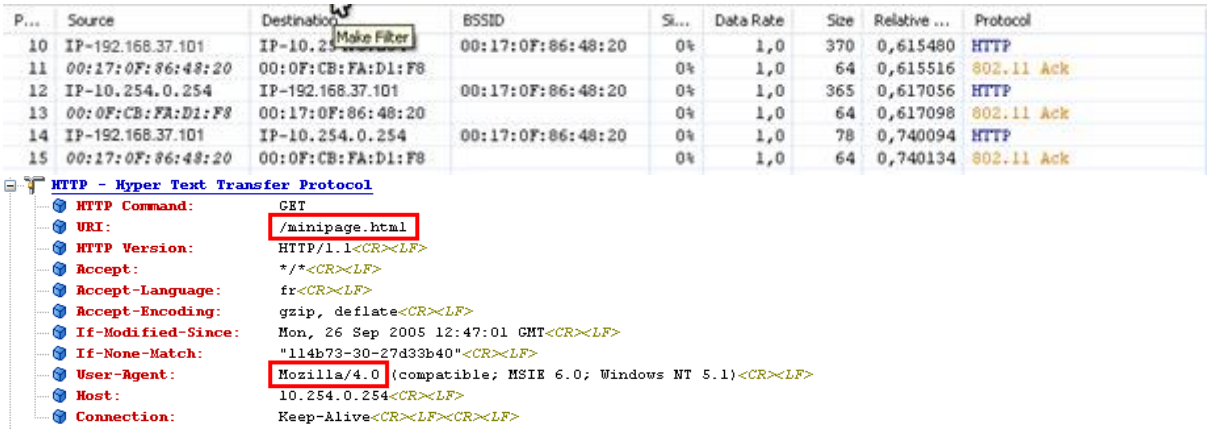
fragmentation à 1000. Cela fait gagner globalement 1,5 Mb/s, c'est la combinaison d'un RTS et d'une faible fragmentation (1000 octets pour 1460 octets dans la trame) qui permet d'offrir de telles performances.

En ce qui concerne le trafic d'un poste wifi vers un autre poste wifi, on observe globalement que les performances sont réduites 10,1 et 7,39 Mb/s. Cela s'explique par le fait que les trames subissent deux transmissions radio (Gn → PA et PA→Dn). De plus on observe de meilleures performances sans fragmentation et sans RTS/CTS, on peut expliquer ce résultat car la fragmentation est trop élevée 3 fragments pour 1460 octets et donc plus réservation de temps pour ces fragments.

PARTIE 7 – Sécurisation du réseau Wifi

Nous verrons dans cette dernière partie, les faiblesses en termes de sécurité des réseaux wifi et nous essayerons de l'améliorer un petit peu, en mettant en place un cryptage par clé WEP.

Tout d'abord nous désactiverons la fragmentation ainsi que le RTS/CTS en réglant ces dernières à 2346 et 2347.
Ensuite nous préparons le poste Gn pour qu'il puisse communiquer avec STP, en nous connectant au réseau wifi.
On peut alors désormais afficher la mini page se trouvant sur STP
« http:// 10.254.0.254/minipage.html ».
Nous pouvons donc désormais faire une capture de trame de la visualisation de la page web avec Omnipeek.



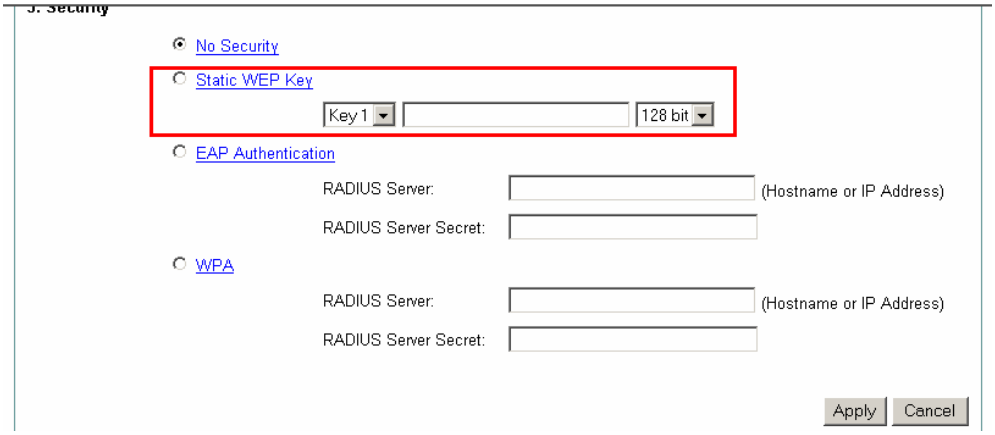
P...	Source	Destination	BSSID	Si...	Data Rate	Size	Relative ...	Protocol
10	IP-192.168.37.101	IP-10.25	00:17:0F:86:48:20	0%	1,0	370	0,615480	HTTP
11	00:17:0F:86:48:20	00:0F:CB:FA:D1:F8		0%	1,0	64	0,615516	802.11 Ack
12	IP-10.254.0.254	IP-192.168.37.101	00:17:0F:86:48:20	0%	1,0	365	0,617056	HTTP
13	00:0F:CB:FA:D1:F8	00:17:0F:86:48:20		0%	1,0	64	0,617098	802.11 Ack
14	IP-192.168.37.101	IP-10.254.0.254	00:17:0F:86:48:20	0%	1,0	78	0,740094	HTTP
15	00:17:0F:86:48:20	00:0F:CB:FA:D1:F8		0%	1,0	64	0,740134	802.11 Ack

Make Filter

HTTP - Hyper Text Transfer Protocol
HTTP Command: GET
URI: /minipage.html
HTTP Version: HTTP/1.1<CR><LF>
Accept: */*<CR><LF>
Accept-Language: fr<CR><LF>
Accept-Encoding: gzip, deflate<CR><LF>
If-Modified-Since: Mon, 26 Sep 2005 12:47:01 GMT<CR><LF>
If-None-Match: "114b73-30-27d33b40"<CR><LF>
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)<CR><LF>
Host: 10.254.0.254<CR><LF>
Connection: Keep-Alive<CR><LF><CR><LF>

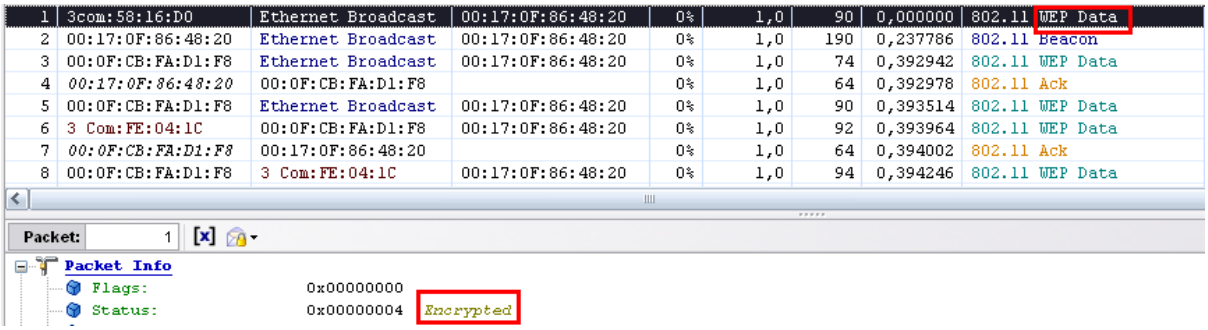
On observe dans la capture des trames http, tout circule donc « en clair » sur le réseau (navigateur, nom de la page). Par conséquent tous le monde peut observer qui fait quoi sur le réseau ce qui représente une faiblesse de ce genre d'architecture.

Maintenant nous allons configurer le Point d'accès avec une sécurisation par clé WEP. Pour ce faire dans l'onglet express security du point d'accès, il faut cocher la case « static WEP key » puis insérer des valeurs de 40 ou 128 bits.



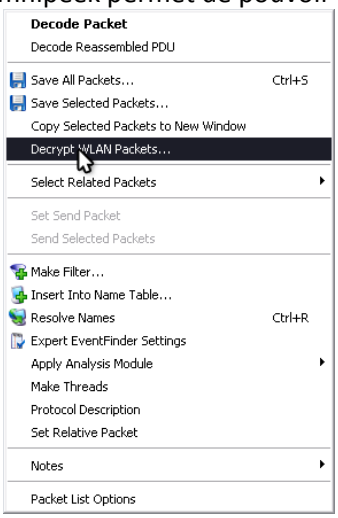
Au niveau du poste client à la connexion sur point d'accès, nous rentrons la clé précédemment entrée, et nous nous accrochons au point d'accès.

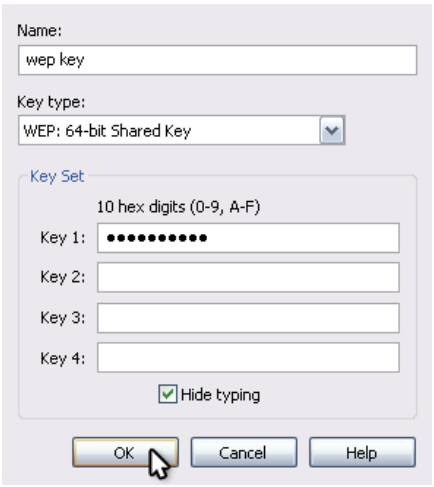
Nous pouvons à présent reprendre une nouvelle capture pour observer les changements.



On constate donc que le protocole http que nous avons vu précédemment en clair n'apparaît plus, et fait place à « WEP data », ce qui signifie donc que les trames de données du réseau sont cryptés.

Le logiciel Omnipeek permet de pouvoir décrypter les paquets en lui précisant la clé WEP :





On peut donc désormais voir les paquets comme si ils n'étaient pas cryptés, et observer les trames http.