Comment installer un réseau mesh

Introduction

De nos jours, de plus en plus d'entreprises souhaitent disposer d'un réseau wifi pour une question de mobilité. Or, un simple routeur ne suffit pas pour couvrir tout un site. C'est pourquoi, il existe différentes techniques et possibilités pour répondre à ce genre de besoin.
Le mode Mesh consiste à faire communiquer tous les nœuds d'un réseau par le Wifi. Même s'il n'est pas souvent implémenté, sa conception peut se révéler très pratique. Nous allons dans un premier temps définir les généralités du mode Mesh, nous traiterons par la suite le mode WDS, technologie du Mesh. Puis, nous verrons concrètement comment déployer un tel réseau en entreprise à travers un guide d'installation.

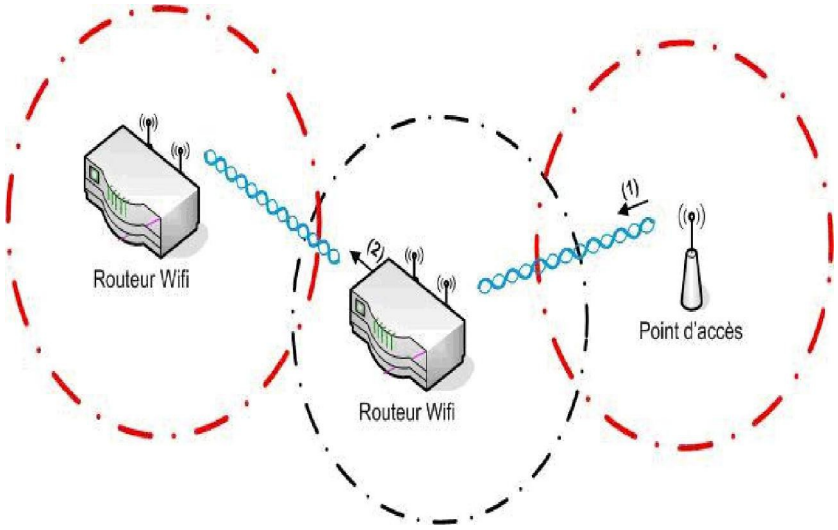
1 Le principe du Mesh

Tout d'abord, il faut savoir que le principe du Mesh est de remplacer tout câblage dans un réseau quel qu'il soit. On connaît tous un réseau wifi composé de plusieurs points d'accès connectés en filaire. Au contraire, le Mesh a pour ambition de supprimer le câblage entre les points d'accès. L'idée est que chaque périphérique sans fil se comporte comme un point d'accès pour ses voisins. C'est-à-dire que tout le monde peut communiquer avec tout le monde par l'intermédiaire de son voisin. Il n'y a pas de différence au niveau logique entre une carte PCMCIA de type mesh network et un point d'accès que ce soit en intérieur tout comme en extérieur. Le réseau Mesh est donc constitué de « mailles » permettant la communication d'un périphérique vers un autre.
Ainsi, pour qu'un réseau Mesh puisse exister, il faut que chaque périphérique soit dans la zone de couverture d'au moins un autre. Le mode Mesh peut être implémenté de plusieurs manières :

- ~~Réseau maillé dynamique~~ : Tous les périphériques sont en « Ad Hoc », ce qui veut dire que tout périphérique peut faire office de routeur/mailles. Techniquement, c'est un réseau maillé dynamique ou les mailles peuvent se former ou disparaître selon les positions de chaque noeud.

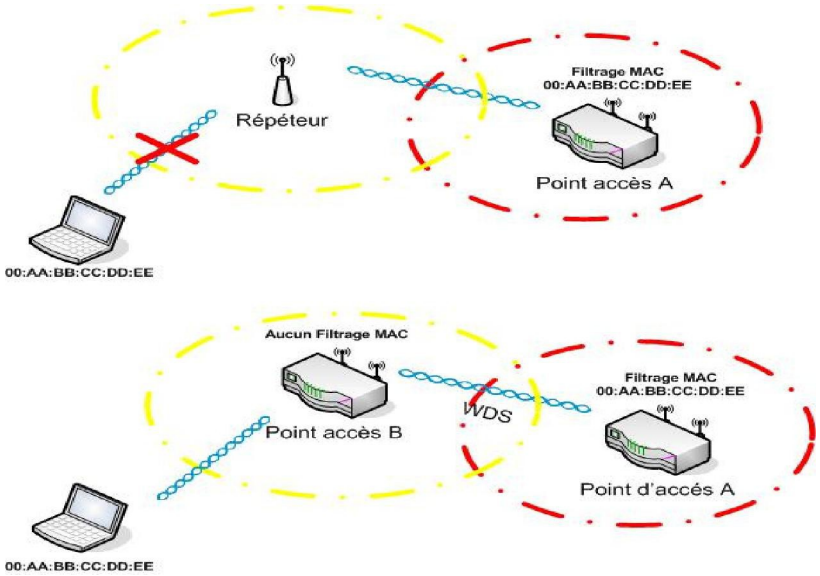
- ~~Réseau maillé statique (mode WDS)~~ : Les points d'accès communiquent entre eux par l'intermédiaire du wifi, et sont les seuls à jouer un rôle de routeur. Le mode WDS peut être considéré comme un réseau maillé statique.

Dans cet article, nous nous intéresserons plus au mesh orienté point d'accès, plus adapté pour le déploiement d'un site fixe.



2 Le mode WDS

Le mode WDS (Wireless Distribution Service) est une configuration qui consiste à faire communiquer plusieurs points d'accès par wifi tout en permettant aux clients sans fils de s'y connecter. A l'inverse d'une configuration ou tous les points d'accès sont connectés par câble, le mode WDS s'avère très pratique puisqu'il supprime toutes les contraintes qu'une installation filaire pourrait poser.
Dans une configuration simple (2 points d'accès), on a l'habitude de dire que le deuxième point d'accès répète le signal du premier.
On aurait donc, un premier point d'accès (Maître) qui diffuse le signal wifi ainsi qu'un deuxième point d'accès (Esclave) faisant office de répéteur du signal émis par le premier. Or, dans une configuration un peu plus complexe (plus de 2 points d'accès), on assimile le mode WDS à un mode permettant de faire communiquer tous les nœuds du réseau par wifi.
On comprend alors que le fait de parler de répéteur est un abus de langage. Effectivement, il ne fait que récupérer et remettre un signal de façon passive.
Ex :
Un point d'accès A est configuré en filtrage d'adresse MAC. Si un client non autorisé se connecte sur le répéteur du point d'accès A, il sera alors rejeté.
A l'inverse, si on connecte un point d'accès B sans filtrage d'adresse MAC sur l'AP A en mode WDS, lorsqu' un client non autorisé se connecte sur le point d'accès B, il sera alors autorisé et aura accès au point d'accès A.
On peut donc en conclure qu'en mode WDS, chaque AP reste maître de lui-même.

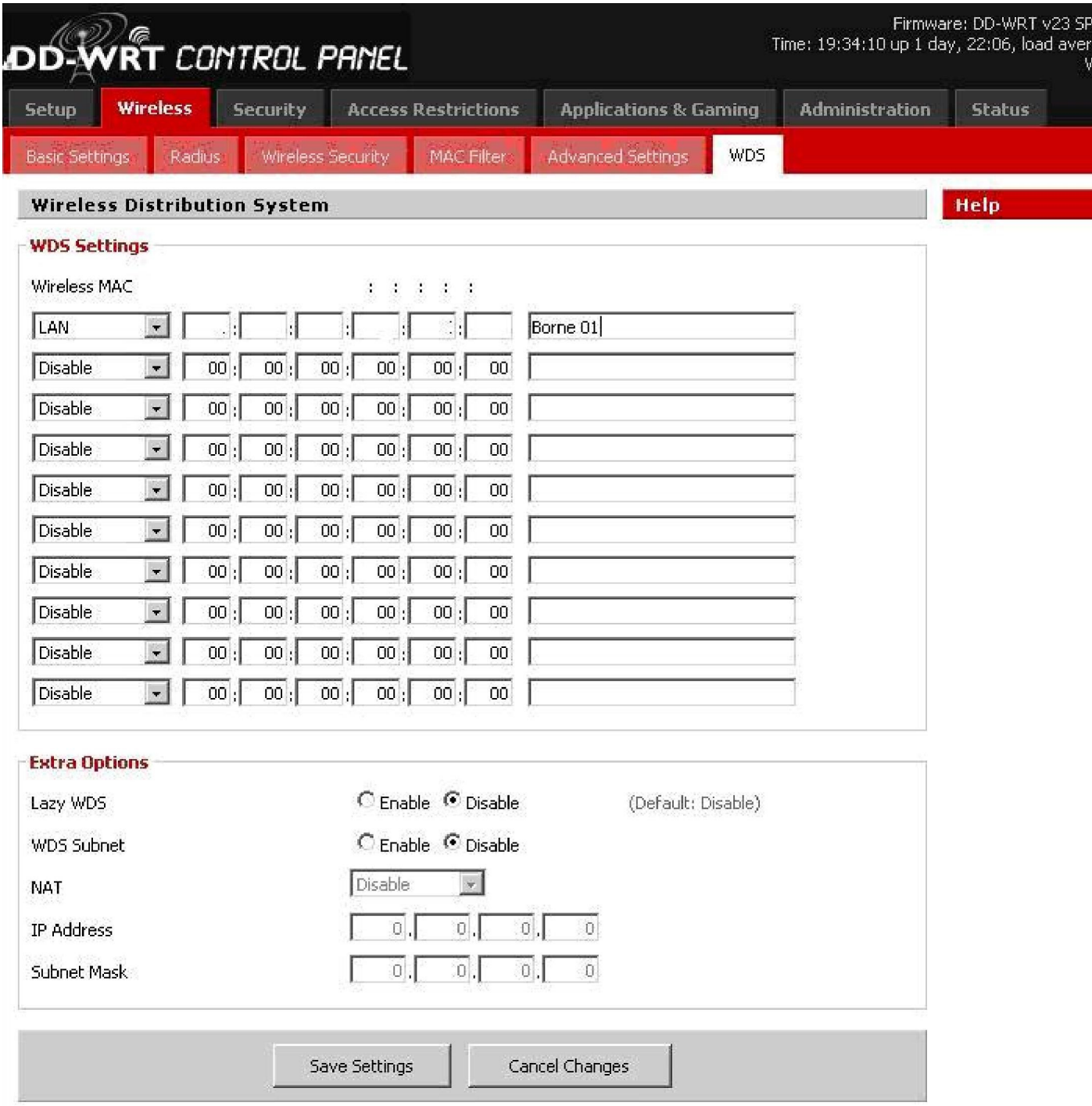


Par ailleurs, on peut distinguer deux méthodes de fonctionnement du WDS :

- Le point to point
- Le multipoint (appelé LAN)

La méthode point to point (P2P) permet au point d'accès de communiquer seulement avec un autre. A l'inverse, le multipoint lui permet de communiquer avec plusieurs points d'accès se trouvant dans sa zone de couverture. De plus, la méthode P2P permet de faire communiquer deux réseaux différents. Par exemple : 192.168.0.0 et 192.168.1.0 en 255.255.255.0. Au contraire, la méthode LAN oblige à ce que les deux points d'accès soient dans le même réseau.

En terme de configuration, le mode WDS doit être configuré sur tous les points d'accès ou routeurs du réseau mesh. Mais attention à bien s'assurer à ce que le matériel soit compatible WDS.
Cette compatibilité n'est pas matériel mais plutôt orienté logiciel (firmware).
Elle peut être différente selon le constructeur et la gamme du routeur ou point d'accès.
Par la suite, nous utiliserons le routeur WRT54GL de chez linksys et le firmware DD-WRT v23 SP1 qui est, à l'heure actuelle celui qui propose le plus de fonctionnalité et de stabilité.



Les configurations requises sur les 2 routeurs doivent être les suivantes :

- Même SSID (nom du réseau)

- Même Canal
- Même cryptage et même clé
- Chaque AP devra connaître l'adresse MAC de son voisin.
- Les nœuds seront dans le même réseau

Techniquement, le WDS fonctionne au niveau de la couche 2, 3 et peut générer des collisions au sein du réseau étant donné que tous les points d'accès fonctionnent sur le même canal. Autre fait important est que la bande passante est divisée par 2 étant donné que l'AP doit gérer les clients et les connexions inter-APs. A savoir aussi que le WDS supporte le roaming. Le client pourra alors se déplacer d'une borne à une autre sans perdre la connectivité.

D'autre part, il est important de noter que le mode WDS ne marche seulement avec les normes standardisées. C'est-à-dire le 802.11b et 802.11g. Il ne peut pas marcher avec la technologie MIMO implémenté sur les routeurs 802.11 pre-n. A l'heure actuelle, il faut savoir aussi que le mode WDS ne fonctionne pas avec les Box proposés par les différents fournisseurs d'accès.
Autre fait important, le WDS permet d'éviter les problèmes liés aux installations complexes du câblage. Sachant que dans une entreprise, les câbles doivent rester discrets, il est parfois obliger de les faire passer sous terre. Or une installation aussi complexe augmente le coût du réseau.
Maintenant que nous avons vu le fonctionnement du mode WDS, nous pouvons passer à son déploiement en entreprise.

3 Etendre son réseau sans fil en dix étapes

Tout d'abord, je tiens à préciser que cette partie est très théorique mais qui rassemble toutefois les principales étapes nécessaires au déploiement du réseau mesh.

Avant de commencer quoi que ce soit, vous devez bien réfléchir aux attentes de l'entreprise et des utilisateurs.
Il faut aussi être sur que le mesh sera adapté aux besoins de l'entreprise.
Et pour cela, certaines exigences sont à prendre en compte :

- Eviter le transfert de gros fichier sur le réseau.
- La connexion Internet ne devra pas se trouver au delà de 4 nœuds pour les utilisateurs.

(Effectivement, le nombre de sauts entre le client et la connexion Internet ne devra pas dépasser 4 routeurs)

- Recourir au mesh lorsque les points d'accès ne peuvent pas être raccordé par câbles.

Si toutes ces conditions sont respectées alors vous avez la possibilité de déployer un réseau mesh.

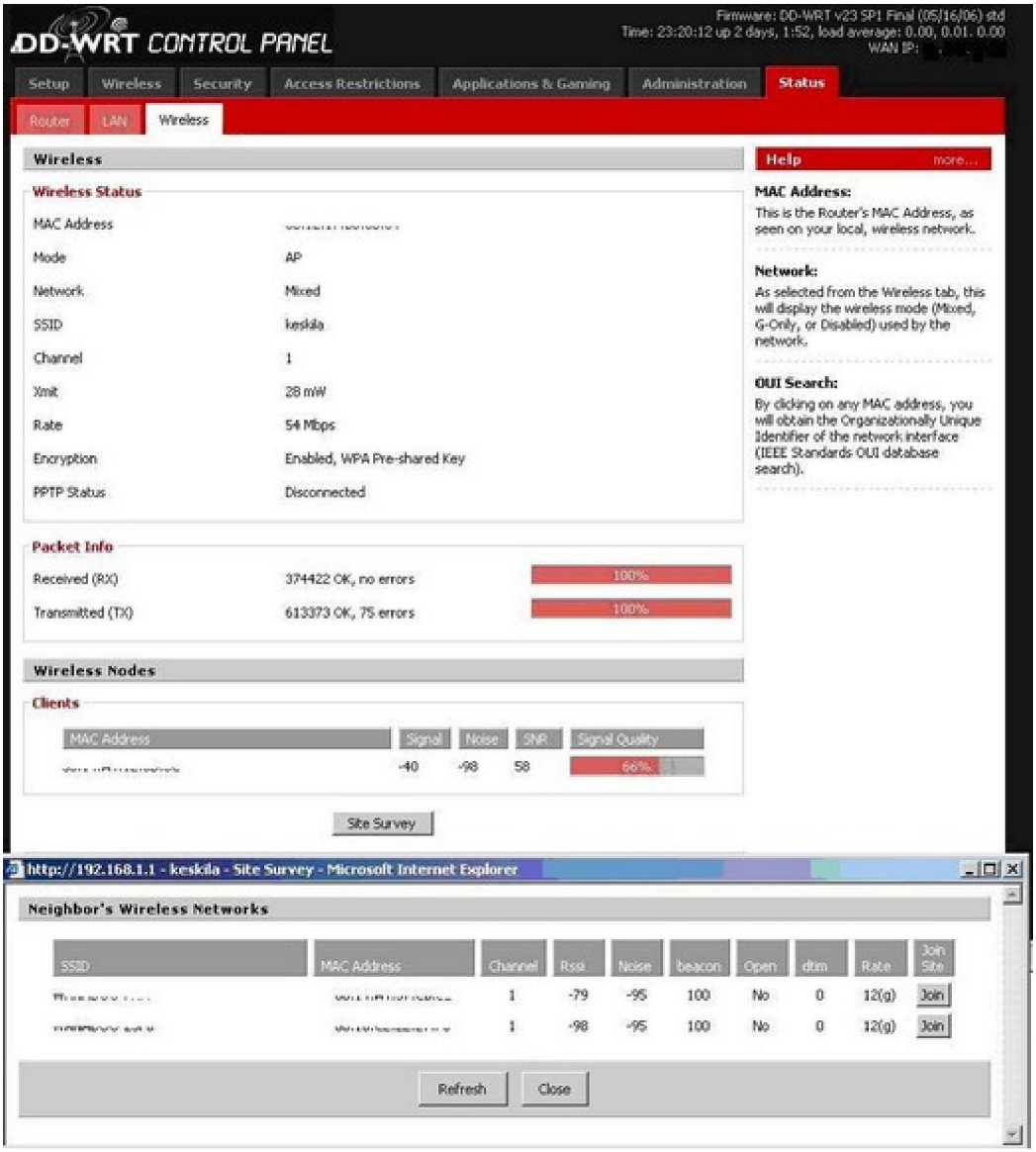
Le premier objectif est de choisir le matériel wifi.
Pour cela, vous devez commencer par analyser le comportement des ondes wifi dans la société.
Vous devez alors vous munir d'un plan des locaux, de l'épaisseur et de la nature des murs de la société.

~~1ère étape : Choix du can~~al

Avant toute chose, vous devez analyser les réseaux avoisinant et plus particulièrement, les canaux qu'ils empruntent. Vous devinerez alors le canal le moins encombré, et donc le moins susceptible aux interférences des autres réseaux. Toutefois, sachez que pour ne subir aucune interférence, le canal utilisé par votre réseau devra être éloigné d'au moins 5 canaux des réseaux avoisinants.
Une fois le canal choisi, vous pouvez commencer vos tests.

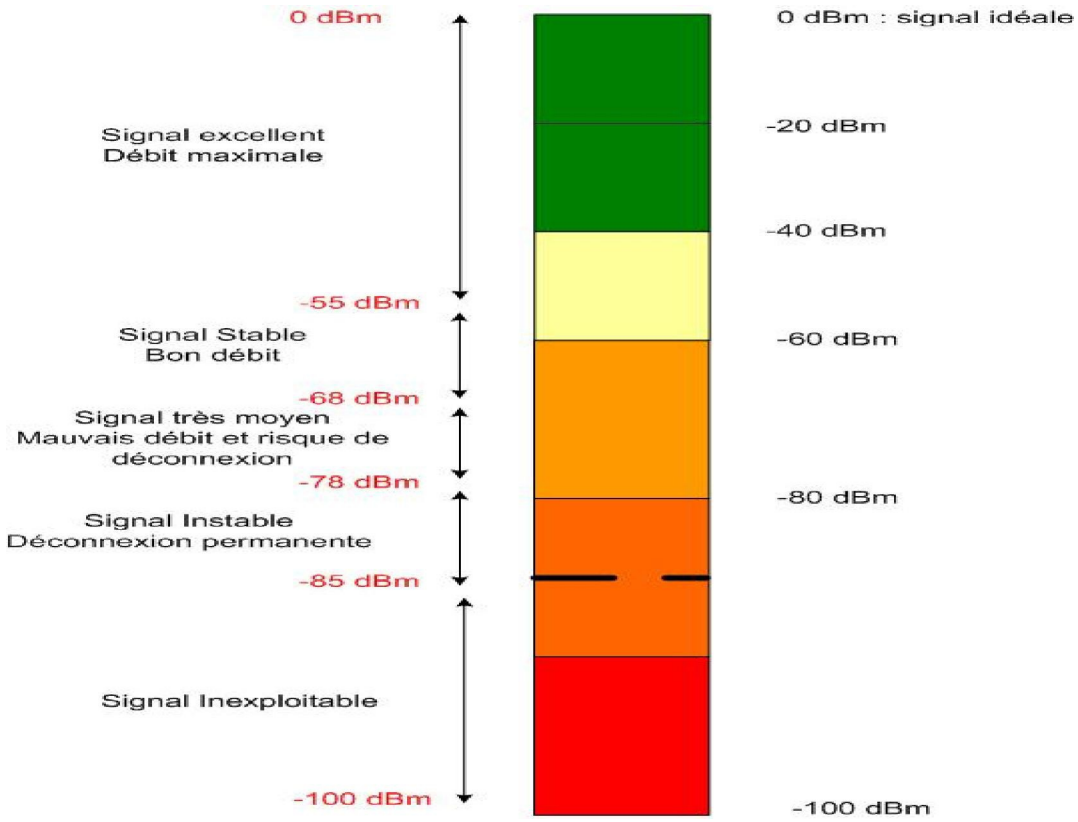
~~2ème étape : Test de réception du sig~~nal

Déplacez vous dans toute l'entreprise avec deux routeurs, l'un comme émetteur et l'autre comme récepteur.
Eviter de faire les tests avec une carte wifi ou encore votre ordinateur portable, ce qui fausserait les résultats.
Vous partirez de l'emplacement où se trouve la connexion Internet, puis vous vous déplacerez jusqu'aux endroits ou vous voulez rendre accessible le réseau wifi. Si vous voulez déployer le réseau dans toute l'entreprise et que celle-ci se trouve assez vaste, vous devrez alors alterner la communication inter-APs wifi/filaire.
En ce qui concerne les tests de qualité du signal, vous utiliserez l'outil « Site Survey » du routeur récepteur.



La qualité du signal est donnée par la colonne « Rssi » en dBm. Celui-ci pouvant aller de 0 à -100 dBm (Sachant que 0 caractérise la réception idéale sans perte).
Dans le but de vous donnez un ordre de grandeur, un lien entre 2 nœuds est stable jusqu'à -68 dBm.
Et elle devient inexploitable à partir de -85 dBm.

Voici une échelle qui vous aidera à distinguer la qualité d'un signal entre deux nœuds :



~~3ème étape : Réalisation de la topolo~~gie

Une fois les tests effectués, vous pouvez alors simuler la topologie de l'entreprise (nombre et positions des routeurs).
La topologie devra respecter les règles suivantes :

- Avoir le moins de nœuds possibles.
- La réception entre chaque nœud devra être au moins de -68 dBm.

Si les réceptions sont plus ou moins bonnes, n'oubliez pas qu'il existe des antennes à fort gain pour remplacer les antennes d'origines.

La création de la topologie est très importante puisqu'elle va vous permettre d'observer l'installation dans sa globalité. Vous en profiterez pour faire le bilan de tous vos tests faits précédemment.
Cette réalisation est une étape cruciale car ce document sera considéré comme un point de départ qui sera mis à jour tout au long de l'installation du réseau. De plus, elle vous aidera par la suite à estimer le coût de celle-ci.
Nous verrons tout au long de cet article qu'il vaut mieux prévoir assez large en terme de matériel plutôt que pas assez.

~~4ème étape : Choix du matériel~~

Une fois la topologie établie, vous pouvez alors vous lancer dans le choix du matériel.
Si vous avez choisi d'utiliser des antennes, pensez à acheter des routeurs avec antenne détachable.
Mais attention, ne prenez pas n'importe quelle antenne.
Vous devrez choisir des antennes discrètes et qui s'adaptent en fonction du lieu.
(Par exemple, optez pour une antenne qui a la même couleur que le ton de la pièce ou du mur ou vous voulez la mettre. Si la pièce présente un faux plafond, choisissez alors une antenne patch).
Elles n'ont pas toute le même gabarie, vous devez alors vous interroger sur la place qu'elle pourrait prendre.

Quel est le meilleur choix, omnidirectionnelle ou directive ?

L'antenne directive est plus efficace lorsqu'il y a besoin d'établir un lien entre 2 bâtiments éloignés de plus de 50 mètres. Etant donné qu'elles émettent dans une seule direction, elles sont beaucoup utilisées pour le point à point. Si vous voulez couvrir plusieurs zones en même temps, il est recommandé de choisir une omnidirectionnelle.

Antenne Patch omnidirectionnelle

Antenne omnidirectionnelle

Antenne parabolique

Antenne omnidirectionnelle à fixer directement sur le routeur

Quel gain choisir ?
Le gain est exprimé en dBi, plus il est élevé et plus il y a de chance d'améliorer la réception.
Pour connaître concrètement l'amélioration apportée par une nouvelle antenne, faire la différence entre le gain de l'antenne d'origine et de la nouvelle antenne, vous aurez alors l'amélioration du signal en dBm.
(Par exemple, vous captez avec l'antenne d'origine un signal de -70 dBm. A savoir que l'antenne d'origine est de 2 dBi. Si vous optez pour une nouvelle antenne de 10 dBi, pour le même test vous obtiendrez en théorie -62 dBm).
Sachez aussi qu'il est possible d'améliorer la réception en augmentant la puissance d'émission du routeur.
A l'origine, celle-ci est réglée à 28 mW mais elle peut être élevé jusqu'à 250 mW selon le matériel.

La loi Française :

Pour respecter la loi française, il est obligatoire de respecter une certaine puissance nommée « PIRE » fixé par l'état. « PIRE » correspond plus précisément à la puissance isotrope rayonnée équivalente d'un système.
Elle est calculée selon la puissance d'émission du routeur, la perte dans les câbles et la puissance de l'antenne.
PIRE = Puissance d'émission (dBm) – Perte dans le câblage (dB) + Puissance de l'antenne (dBi)
Voici ses limites :

	Intérieur	Extérieur
Canal 1 à 7	100 mW (20 dBm)	100 mW (20 dBm)
Canal 8 à 13	100 mW (20 dBm)	10 mW (2 dBm)

Par exemple, la puissance d'émission de mon routeur est de 30 mW (15dBm) sur le canal 6, mon câble qui relie mon routeur à mon antenne est de 6 mètres à 0,58 db de perte par mètre de câble. L'antenne utilisée est une antenne omnidirectionnelle de 8 dBi.

PIRE = Puissance d'émission (dBm) – Perte dans le câblage (dB) + Puissance de l'antenne (dBi)
PIRE = 15 - (0,58*6) + 8
PIRE = 19,52 dBm
La limite légale étant de 20 dBm sur le canal 6, nous sommes donc dans la légalité.

D'un point de vue santé, il est recommandé de ne pas vivre à moins de 2 mètres d'une source wifi.
(Voir le site AFFSET le rapport "Téléphonie mobile & santé (juin 2005)" et de lire pour le wifi à la page 20 le chapitre 4.2, la remarque sur la distance du wifi en bas de page 22 et le tableau page suivante puis à la page 82 le chapitre 7.2)
http://www.afsse.fr/index.php?pageid=671&parentid=619

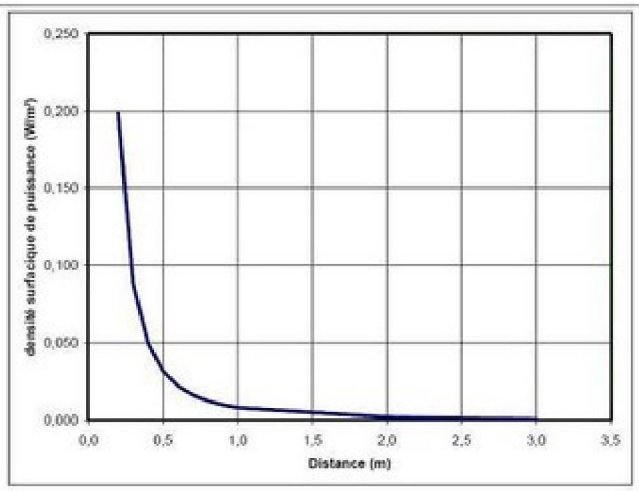


Figure 4 . Décroissance théorique de la densité surfacique de puissance d'un système WiFi en espace libre pour une PIRE maximale de 100 mW

Sachez toutefois que les téléphones portables émettent entre 1 et 2 W contre 28 à 100 mW pour les appareils wifi. Etant donné qu'il est très rare de se balader avec un routeur wifi dans la poche, le téléphone portable présente 15 fois plus de risque pour la santé que les appareils wifi.

Quels sont les connecteurs à choisir ?

Faire attention à ce que le type de connecteur entre le routeur et l'antenne soit le même. Il n'existe pas de format universel mais 3 formats fonctionnant à la fréquence du wifi 2.4 Ghz.

Connecteur N :
Le connecteur N est celui que l'on retrouve sur les antennes à fort gain.

N Femelle N male

Connecteur RP-TNC
Le connecteur RP-TNC est celui de quelques routeurs comme ceux de la gamme Linksys.

RP-TNC Male RP-TNC Femelle

Connecteur RP-SMA :
Le connecteur RP-SMA est le plus souvent présent sur les cartes wifi.

RP-SMA Femelle RP-SMA Male

Attention, RP signifie “Reverse Polarity”, il est donc normal que le connecteur femelle soit celui qui possède la petite pointe. Le phénomène est inversé.
Lors de l’achat d’une antenne, le câble n’est pas toujours fournit. C’est pourquoi si vous en achetez un a part, vous ferez attention de sa perte par mètre de câble (Db/m). Ne pas dépasser 6 dB de perte pour un câble.

Bien évidemment, ne choisissez pas le câble avant d'avoir trouvé le routeur approprié.
En ce qui concerne le choix du routeur/Ap voici les critères de qualité pour le mesh :

- Faites attention aux nombres d'utilisateurs supportés.
- Son esthétisme : Il vaut mieux choisir un routeur petit et discret.
- Les firmwares proposés pour celui-ci. Si vous voulez faire du monitoring, vérifier qu'il propose bien les fonctions « syslog » et « snmp ». Vérifier aussi sa compatibilité WDS. Attention, renseignez vous sur le mode WDS ! Certains firmwares ne permettent pas de l'utiliser complètement. Chez certaines marques, il n'est utilisable seulement avec le cryptage WEP, ce qui est impensable dans le monde de l'entreprise. De plus, certaines fois il est limité à 2 nœuds, ce qui restreint alors le réseau.

~~5ème étape : Etude du coût du réseau~~

Maintenant que vous connaissez le type, le nombre de routeurs, d'antennes sans oublier les câbles. (Topologie)
Vous pouvez alors déterminer le coût de votre réseau. Vous devez prévoir large, si jamais le matériel prévu au début ne venait pas à suffire. Il est vrai qu'au final, le coût reste le même mais il vaut mieux faire des économies à l'entreprise.

~~6ème étape : Achat du matériel~~

Le choix du matériel doit se faire en 2 temps. Vous ne devez pas tout commander en une seule fois.
Effectivement, si vous avez du matériel en trop, ce serait considéré comme du gâchis.
Vous devez alors faire une première commande avec l'essentiel du réseau (3/4 de ce que vous avez prévu) et de tester le matériel aux emplacements décidés (Par exemple, évitez d'acheter les mêmes antennes lors de la première commande, les tests vous diront si vraiment la deuxième antenne serait vraiment utile).
Puis dans un second temps, vous pourrez alors faire la deuxième commande si besoin est.

~~7ème étape : Montez une partie du réseau avec la première commande~~

Une fois la première commande reçue, vous pouvez commencer une partie de l'installation du réseau.
Vous mettrez alors le firmware des routeurs à jour et y configurer le WDS.
Placez les routeurs/APs suivant la topologie et tester la qualité de chaque lien (routeur à routeur).

Tester le signal émis : Si l'émission est assuré par une antenne fixé sur le routeur, c'est le routeur que vous devrez positionné pour que le routeur qui reçoit profite du meilleur signal. Ce qui reste un inconvénient puisque l'emplacement où l'on réceptionne le mieux n'est pas toujours l'emplacement ou il est possible de fixer le routeur. A chaque déplacement du routeur, vous devrez tester le signal sur celui qui reçoit.

Si le signal est émis par une antenne externe, le choix de l'emplacement du routeur n'aura pas d'importance.
Vous devrez placer l'antenne le plus haut possible et la tester à la verticale et à l'horizontale.
Vous ferez de même pour les routeurs/APs qui reçoivent.

Si vous avez le choix entre plusieurs firmwares, sachez que la qualité de réception n'influe pas mais le débit lui peut varier d'un firmware à un autre.

Maintenant que tous les liens sont configurés, il est important de tester le réseau.

~~8ème étape : Tester la stabilité du réseau~~

Il est important de tester la stabilité du réseau, il doit être tout le temps opérationnelle et le client ne doit être en aucun cas déconnecté du réseau.
Vous pouvez commencer les tests par la commande « ping ». Vous vous placerez d'une extrémité du réseau et pinger l'autre extrémité afin de tester le plus de nœud. Ces tests seront réalisés pendant 24h.

Vous avez aussi la possibilité de transférer de gros fichiers entre 2 extrémités du réseau afin de connaître ses réelles performances.

Vous devez aussi prévoir le plantage de n'importe quel routeur, pour cela, vous devez toujours avoir la possibilité de vous relier en filaire à celui-ci (Par exemple, si un de vos routeurs se trouvait dans un faux plafond, un câble RJ-45 doit toujours y être relié et se trouver à portée de main.)

~~9ème étape : La sécurité~~

La sécurité des réseaux sans fil en entreprise doit être vraiment pris au sérieux.
Elle doit être choisie en fonction de la politique de sécurité de l'entreprise.
Avant tout, il faut se poser quelques questions :

- Quels seront les utilisateurs du réseau wifi ?
- Le réseau sert il pour l'accès à Internet ou pour l'échange de données entre utilisateurs ?
- Les utilisateurs partagent t'ils des données confidentielles ?

Voici les différentes sécurités que nous allons traités :

-WPA2 (AES)
- Filtrage d'adresse MAC
- Serveur radius

Tout d'abord, la première sécurité est le cryptage « WPA2 Pre-Shared Key AES ».
Le WPA2 est une sécurité de base empêchant aux utilisateurs externes à la société de se connecter.
Pour pouvoir accéder au réseau, il faut connaître la clé partagée. Celle-ci peut se décrypter après 1 semaine de calcul pour les processeurs actuels. On peut donc conclure que le WPA2 est une sécurité très pointue mais qui peut être franchis par quelques crackers.

Il est possible de n'autoriser seulement les utilisateurs que l'on veut. Cette solution opère au niveau des adresses MAC. Il suffit de recenser tous les utilisateurs du réseau et de les rentrer dans une liste d'adresse MAC.
Une méthode très lourde mais qui peut être aussi contournée. Un cracker peut très bien se faire passer par un utilisateur autorisé.

Le WPA2 et le filtrage d'adresse MAC sont des méthodes assez simples en configuration.
Maintenant, si les données circulant sur le réseau sont vraiment confidentielles, il est possible d'implémenter un serveur radius mais les compétences demandés ne sont plus les mêmes. La plupart des serveurs radius étant implémenté sous linux, il est recommandé d'avoir de solides bases dans ce domaine.
Le serveur radius propose plusieurs types de sécurité dites « EAP » et laisse la possibilité à l'administrateur de choisir la ou les plus adaptées.

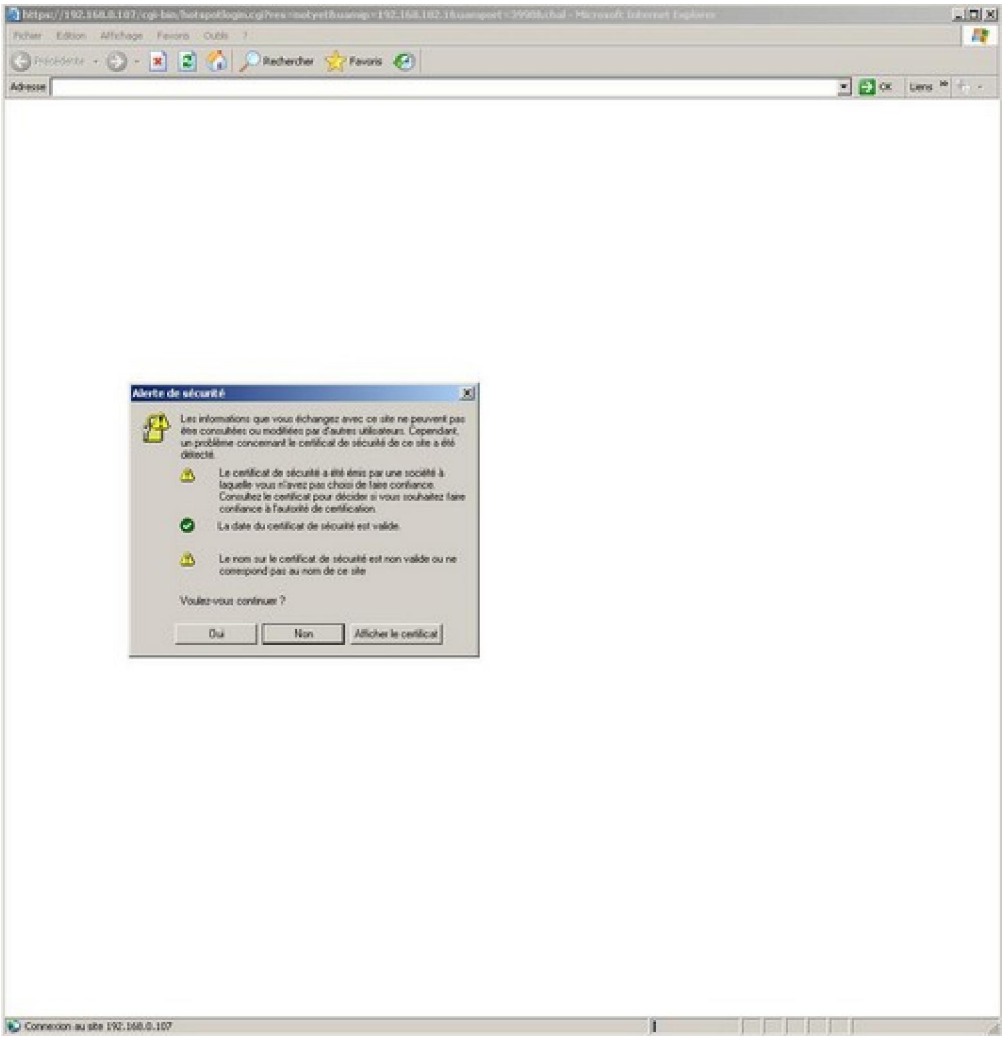
- EAP/MD5 : Une fois connecté, chaque client devra rentrer un login, un mot de passe pour avoir accès à Internet. La méthode d'authentification repose sur CHAP ou le dialogue entre l'AP et le serveur Radius est crypté selon l'algorithme MD5. Par contre, les mots de passe dans la base de donnée sont stockés en clair.
- EAP/MS-CHAP: Même principe que EAP/MD5 sauf que les mots de passes de la base de donnée sont cryptés.
- EAP/TLS : Le client et le serveur Radius dispose tous les deux d'un certificat pour se reconnaître. Lorsque tous les deux dialoguent, cela revient à établir un tunnel crypté généré par une clé symétrique. Le souci est que chaque client doit posséder un certificat, une méthode de sécurité très lourde à déployer.
- EAP/PEAP : À l'inverse de EAP/TLS, seul le serveur possède le certificat. Cette méthode peut être couplé à une autre telle que EAP/MD5, MS-CHAP, MS-CHAP v2. Une solution beaucoup moins lourde que TLS.
- EAP/TTLS : Une méthode quasiment identique à EAP/PEAP. La seule différence avec TTLS est que le serveur d'authentification peut exiger une configuration précise du client. Ex : À la connexion, le client devra activer son firewal.

Dans cet article, nous traiterons le serveur Freeradius implémenté sous Debian Sarges.

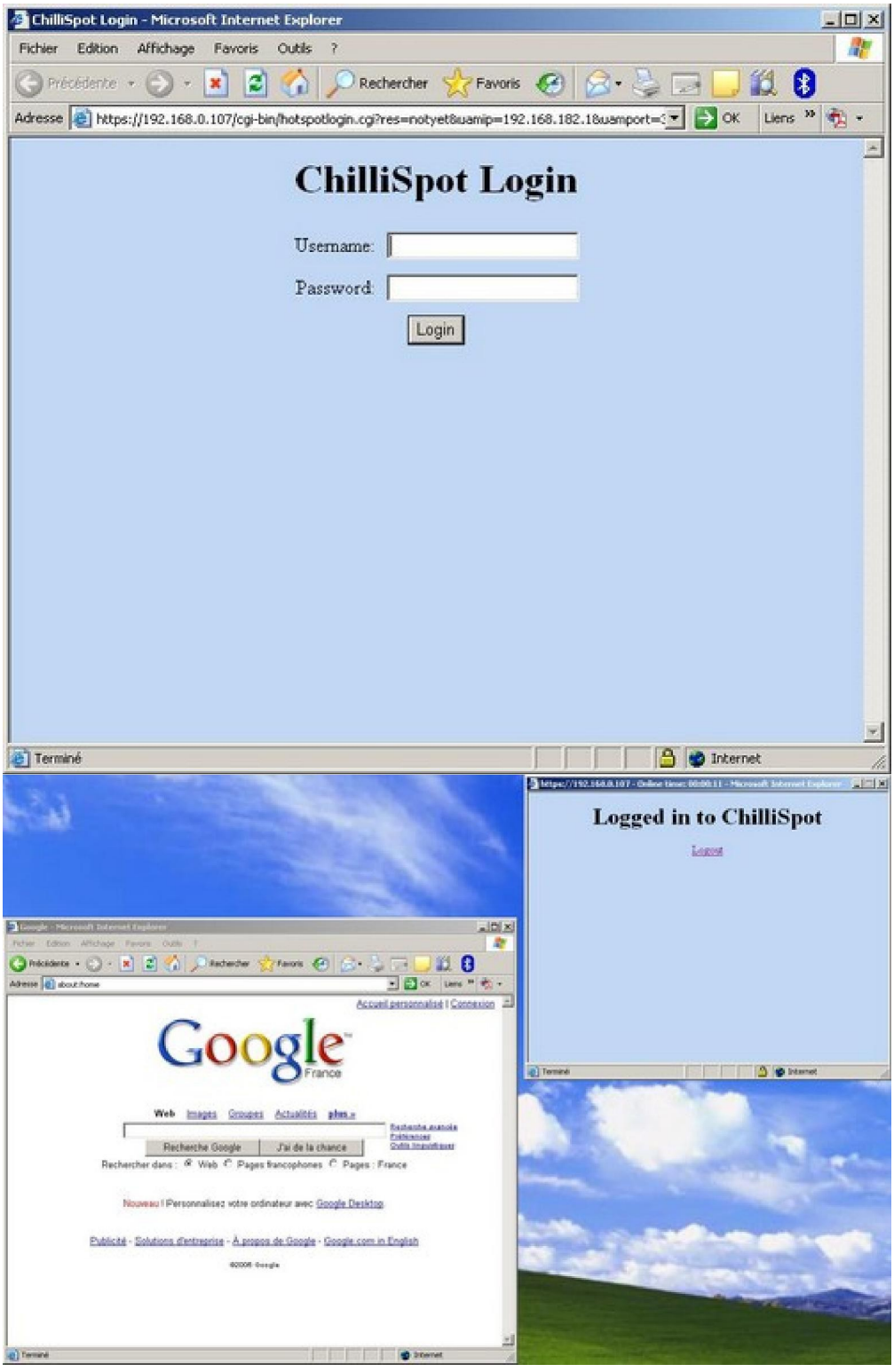
Nous ne verrons pas son installation mais plutôt ces possibilités d'utilisation.
Freeradius peut être considéré comme un serveur d'authentification fonctionnant avec la base de donnée « mysql » et les technologies Internet tel que « apache » et « php » ainsi que le portail captive « Chillispot ».
A partir du moment ou un utilisateur est connecté, il est redirigé automatiquement vers une page web demandant son authentification par login et mot de passe. La gestion des comptes utilisateurs peut être géré par un administrateur via une interface web dites « dialup Admin ».

Interface d'authentification géré par chillispot :

Une fois connecté au réseau, lorsque l'utilisateur ouvrira une page web avec son navigateur, il sera directement redirigé vers l'interface chillispot :



Voici l'interface Chillispot demandant le login et le mot de passe de l'utilisateur :



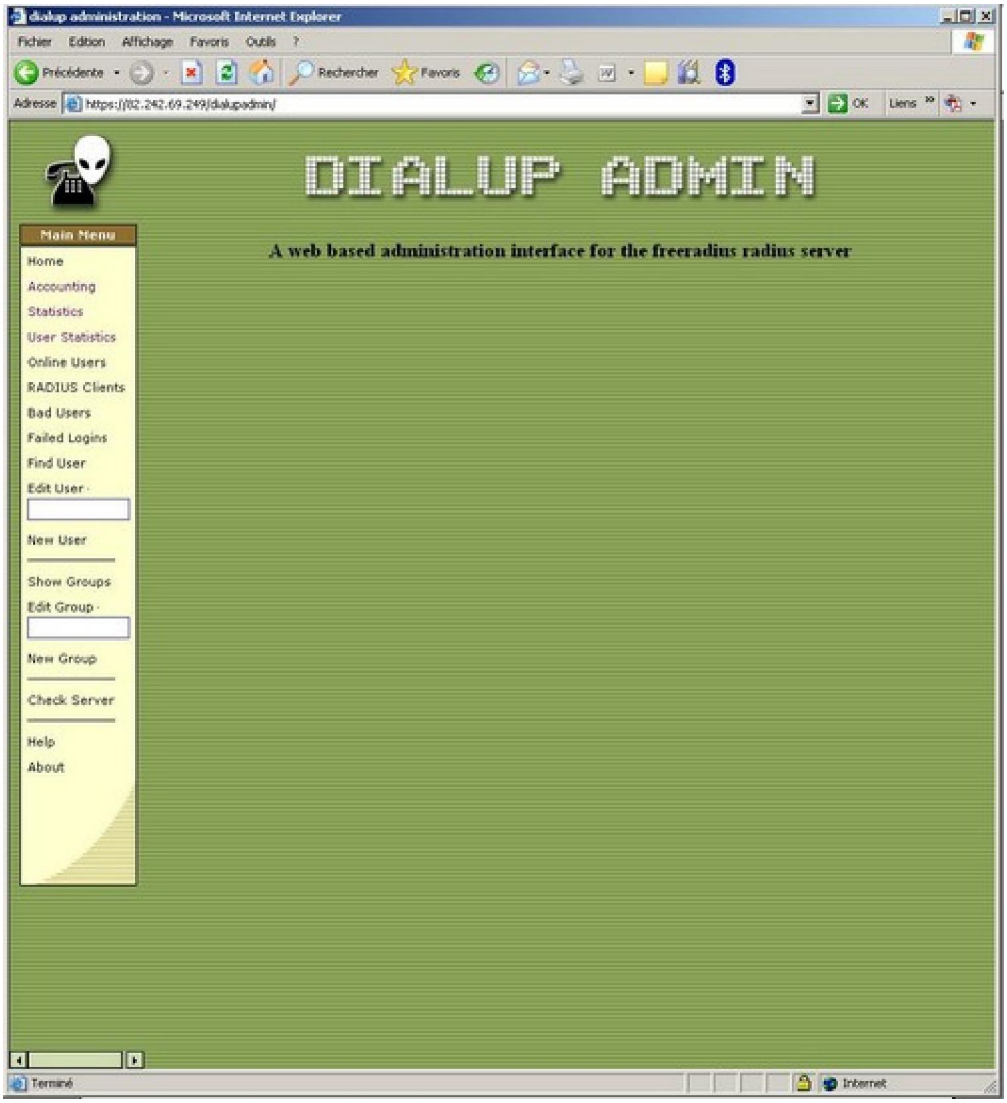
Une fois logué, il apparaît une petite fenêtre affichant le temps de connexion de l'utilisateur. Evidement, il est possible de limiter le temps de connexion pour chaque utilisateur.

-

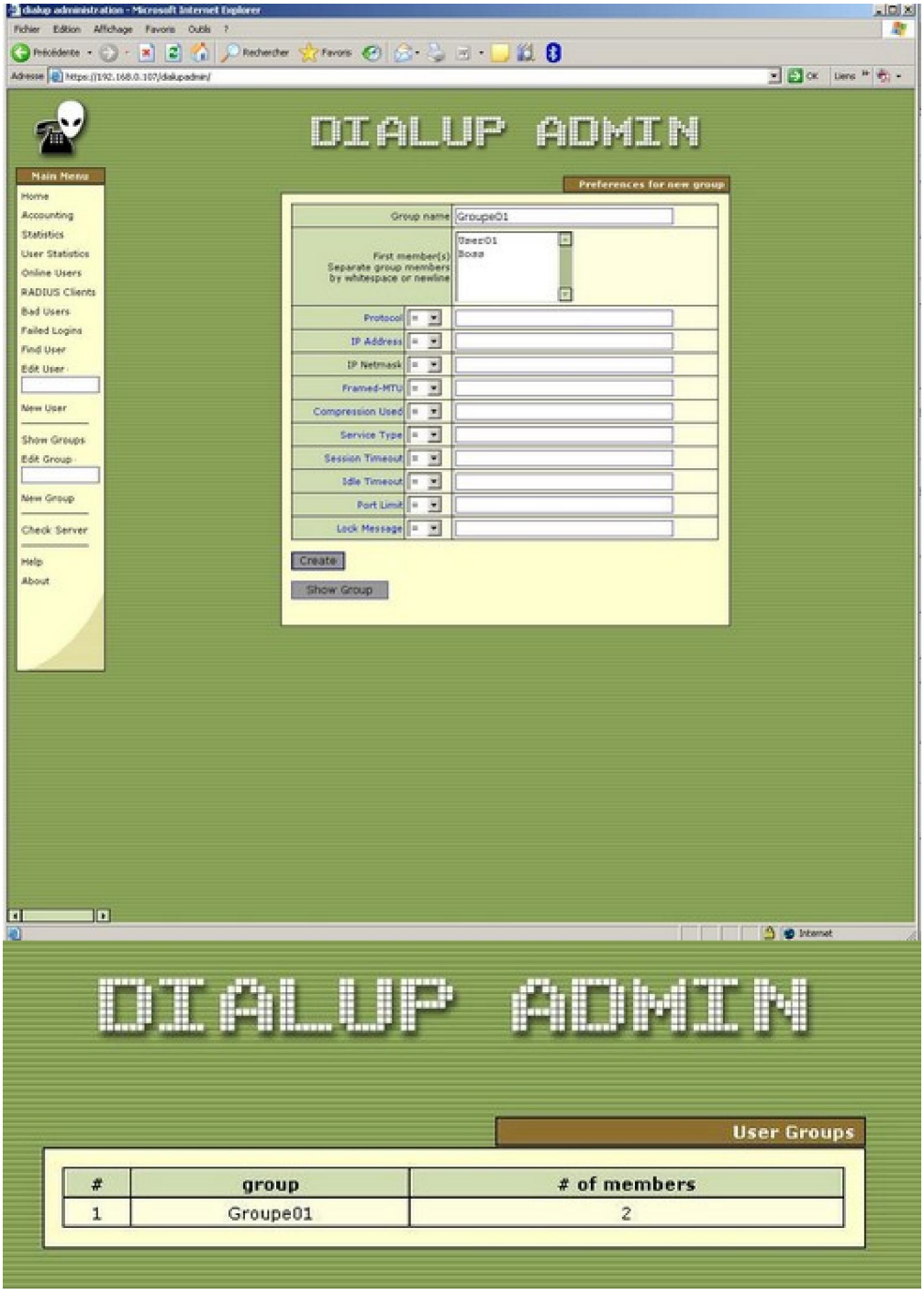
Interface d'administration Dialup Admin :

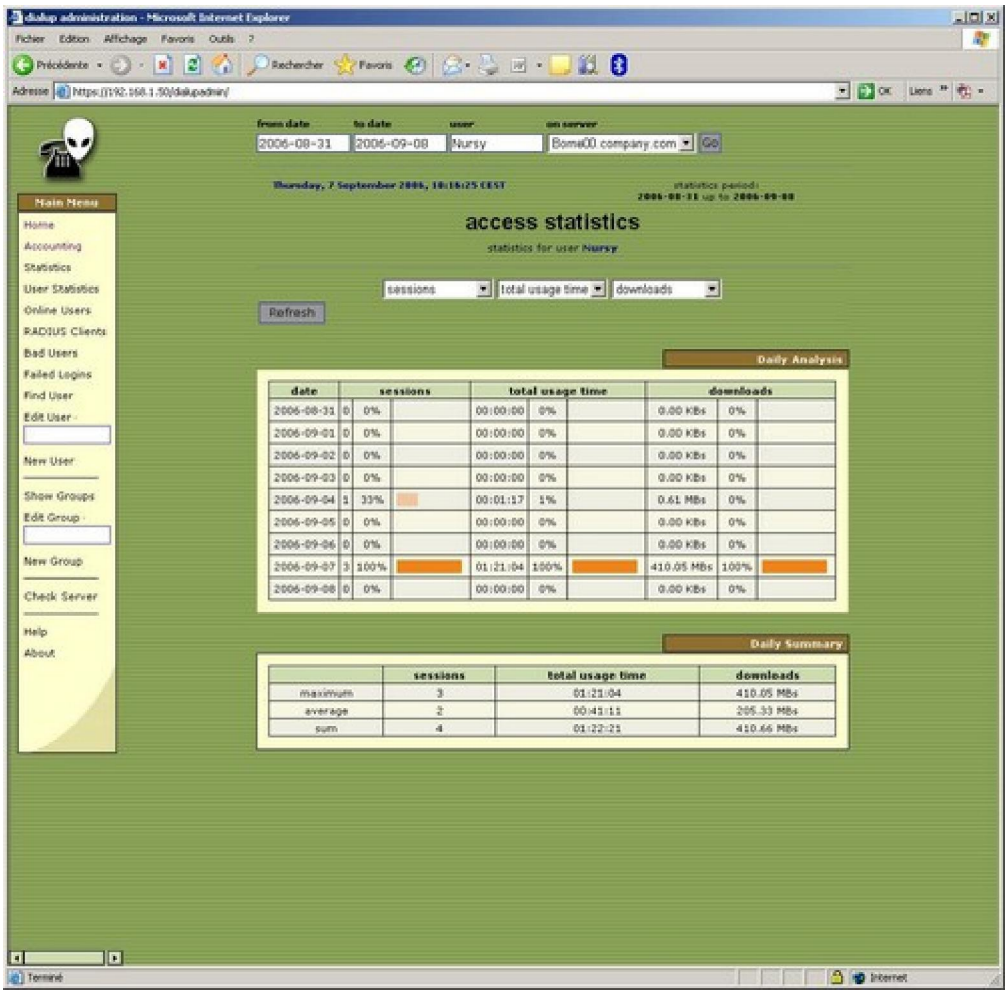
-

L'interface « dialup admin » est une interface web permettant de gérer le les comptes utilisateurs du réseau wifi.



Cette interface plutôt complète donne la possibilité de créer des utilisateurs ainsi que des groupes d'utilisateurs. De plus, elle permet de visualiser les statistiques par utilisateurs comme le download, upload, le temps de connexion consommé, le nombre de sessions ouvertes. D'autre part, il est tout à fait possible de rechercher un renseignement dans les tables SQL.





DIALUP ADMIN

Connection Status for Nursy (-)

User is **online** since	2006-09-07 15:33:02
Connection Duration	00:01:11
Server	**0.0.0.0** (0.0.0.0)
Server Port	2
Workstation	00-14-A4-12-6D-0C
Upload	not available
Download	not available
Allowed Session	user can login for **3 hours, 37 minutes, 59 seconds**
Usefull User Description	-

Check Password

Password [ ] check

Subscription Analysis

-	monthly	weekly	daily	per session
limit	none	20 hours	4 hours	none
used	-	22 minutes, 12 seconds	20 minutes, 55 seconds	00:01:06

day	daily limit	used
sunday	4 hours	0 seconds
monday	4 hours	1 minutes, 17 seconds
tuesday	4 hours	0 seconds
wednesday	4 hours	0 seconds
thursday	4 hours	20 minutes, 55 seconds
friday	4 hours	0 seconds
saturday	4 hours	0 seconds

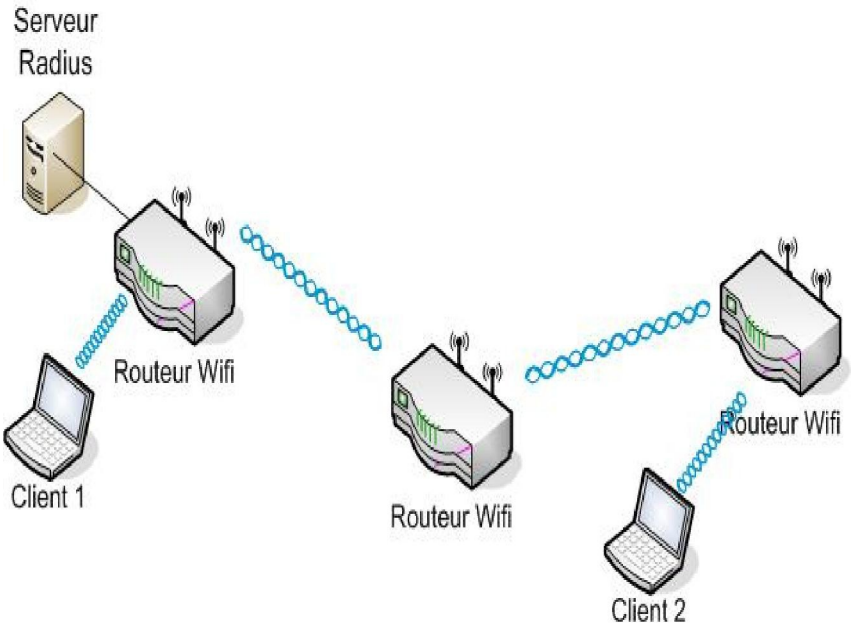
Account Status For The Last 7 Days

Connections	**4**
Online time	**22 minutes, 12 seconds**
Failed Logins	**0**
Upload	5.87 MBs
Download	381.56 MBs
Average Time	5 minutes, 33 seconds
Average Upload	1.47 MBs
Average Download	95.39 MBs

Accounting Report Generator

Accounting Id	Accounting Start Delay	Accounting Stop Delay	CalledStationId	Caller Id	Client IP Address	Download	Login Time	Logout Time	NAS Port	NAS Port Type	Session Id	Session Time	Terminate Cause	Unique Id	Upload	User Name
7	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-14-A4-12-6D-DC	192.168.182.3	12.01 KBs	2006-09-01 19:03:29	2006-09-01 19:03:31	0	Wireless-802.11	44f8668f00000000	2 seconds	User-Request	a19ce838ba98bdd9	3.32 KBs	sparow
8	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-14-A4-12-6D-DC	192.168.182.3	1.57 MBs	2006-09-01 19:04:50	2006-09-01 19:41:20	0	Wireless-802.11	44f866b600000000	36 minutes, 30 seconds	User-Request	4b7c124a0f2e03dc	457.17 KBs	sparow
1	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-14-A4-12-6D-DC	192.168.182.2	1.77 MBs	2006-09-01 17:19:56	2006-09-01 17:57:02	0	Wireless-802.11	44f84dc700000000	37 minutes, 6 seconds	Lost-Carrier	bf4bdae4027c6670	0.52 MBs	Thus0
2	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-90-4B-16-4D-93	192.168.182.100	159.95 KBs	2006-09-01 17:21:35	2006-09-01 17:23:06	2	Wireless-802.11	44f84e3600000002	1 minutes, 31 seconds	User-Request	80da31c5ce982ba5	30.80 KBs	Thus0
3	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-90-4B-16-4D-93	192.168.182.100	178.43 KBs	2006-09-01 17:23:21	2006-09-01 17:25:17	2	Wireless-802.11	44f84f2d00000002	1 minutes, 56 seconds	User-Request	a24dd9ae9409f058	31.93 KBs	Thus0
4	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-90-4B-16-4D-93	192.168.182.100	4.24 KBs	2006-09-01 17:36:29	2006-09-01 17:37:34	2	Wireless-802.11	44f84fb000000002	1 minutes, 5 seconds	User-Request	2e6afd43c77365aa	1.63 KBs	Thus0
9	0 seconds	0 seconds	00-18-39-BF-E5-1A	00-14-A4-12-6D-DC	192.168.182.3	2.93 MBs	2006-09-01 19:41:52	2006-09-01 19:58:35	0	Wireless-802.11	44f86f9300000000	16 minutes, 42 seconds	Lost-Carrier	17e940a21bb9c684	148.15 KBs	Thus0

Le serveur radius est alors une sécurité qui rend strictement confidentielle les données des utilisateurs.

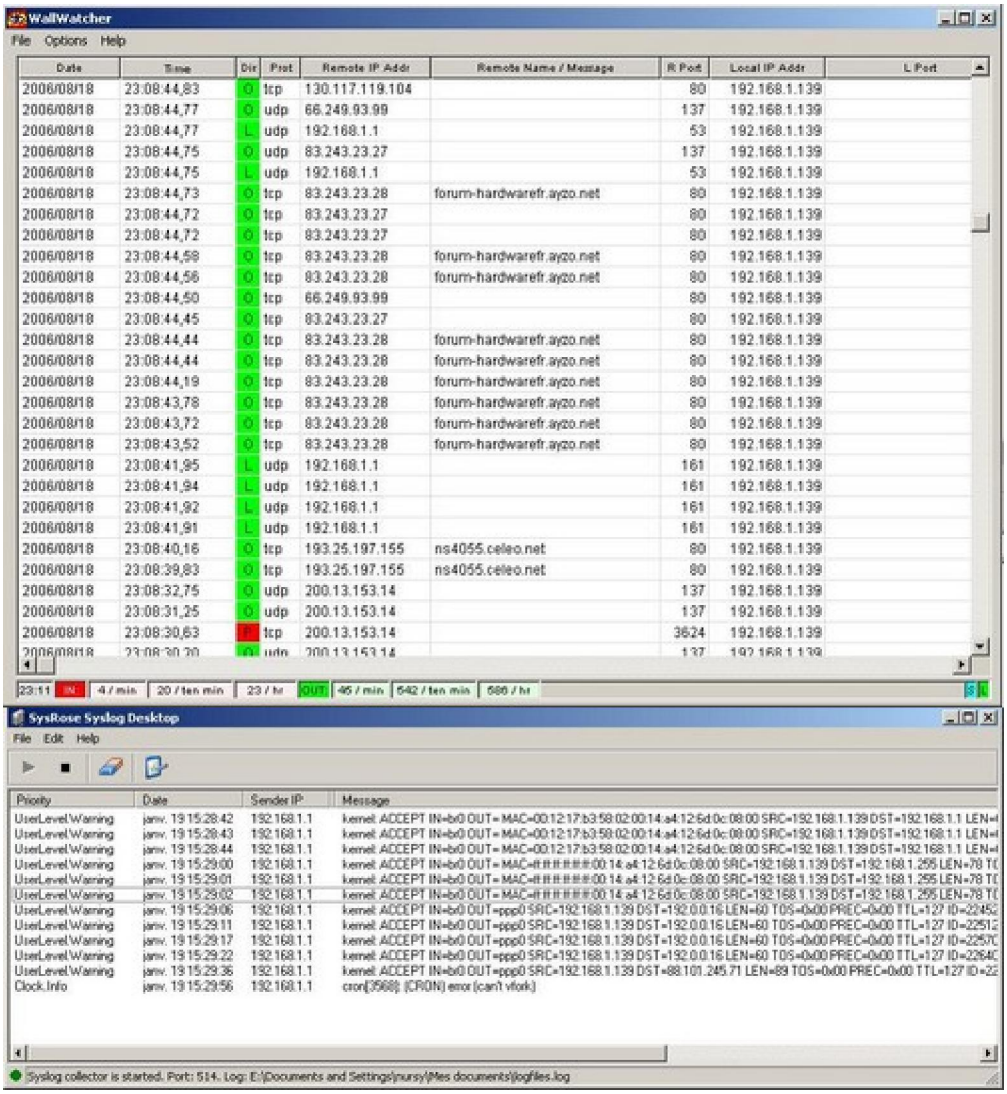


~~10éme étape : Monitoring réseau~~

Dans un souci de sécurité, vous devez mettre en place une solution pour contrôler en permanence le réseau. Vous devez vous assurer que seul les personnes autorisées se connectent au réseau. Evidement vous ne pouvez pas l'analyser en temps réel. Vous devez alors mettre en place un système permettant de faire un bilan de la situation toutes les semaines, voir tous les mois. Pour cela, vous utiliserez deux méthodes de monitoring réseau : SNMP et SYSLOG.
Nous ne traiterons pas ici la configuration de ces deux méthodes mais plutôt de leur utilisation.

SYSLOG va vous permettre d'analyser en temps réel le trafic. Vous aurez alors le descriptif de chaque requête circulant sur votre réseau. Ces données pourront ensuite être réorganisées selon votre choix.
Voici ce que vous propose SYSLOG :

- Alerte en cas de crash d'un point d'accès
- Liste des adresses IP et adresses MAC recensés sur votre réseau.
- Identifier les sites Internet accédés par les utilisateurs



Au contraire, SNMP vous permettra d'avoir une vision plus globale du trafic. Tout d'abord, il faut savoir qu'il fonctionne par interface (WAN, LAN, WLAN ou encore WLAN/LAN). C'est-à-dire que l'on pourra très bien différencié le trafic des clients connectés en Ethernet de ceux connectés en wifi.

Dans notre cas, nous préférons analyser : (par interface):

- la bande passante
- le taux d'erreur

Les résultats sont donnés sous forme de tableau et de graphique. Ci-dessous, vous pouvez voir l'utilisation de la bande passante sur l'interface WAN :

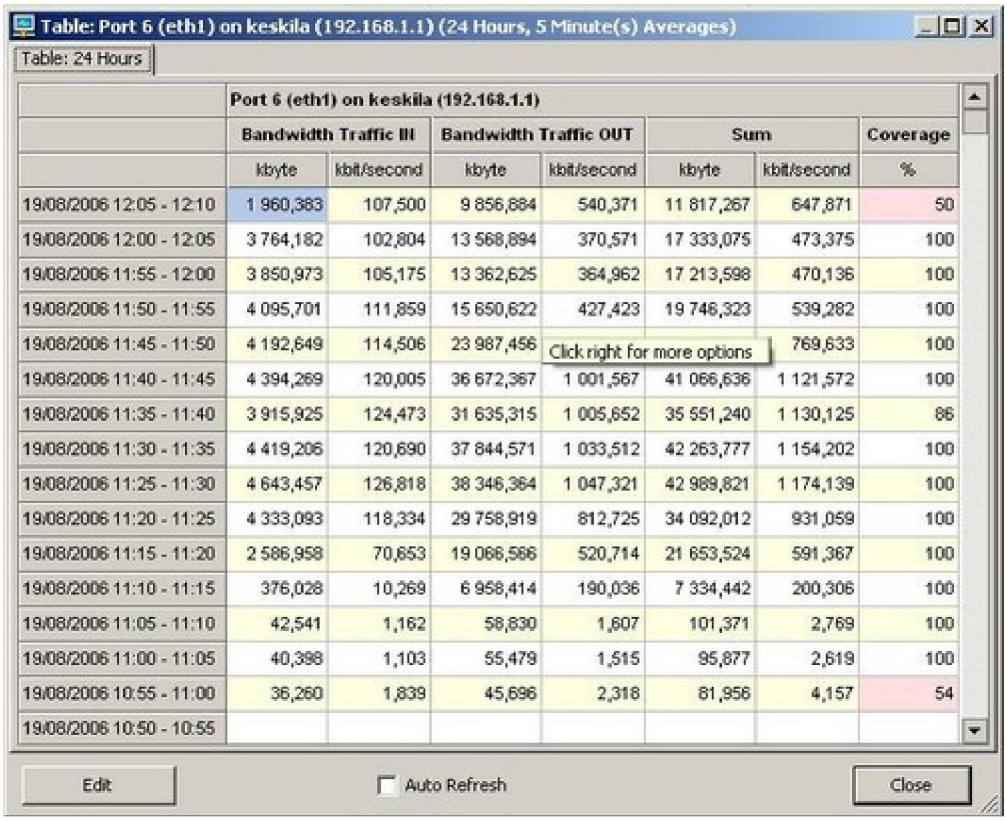
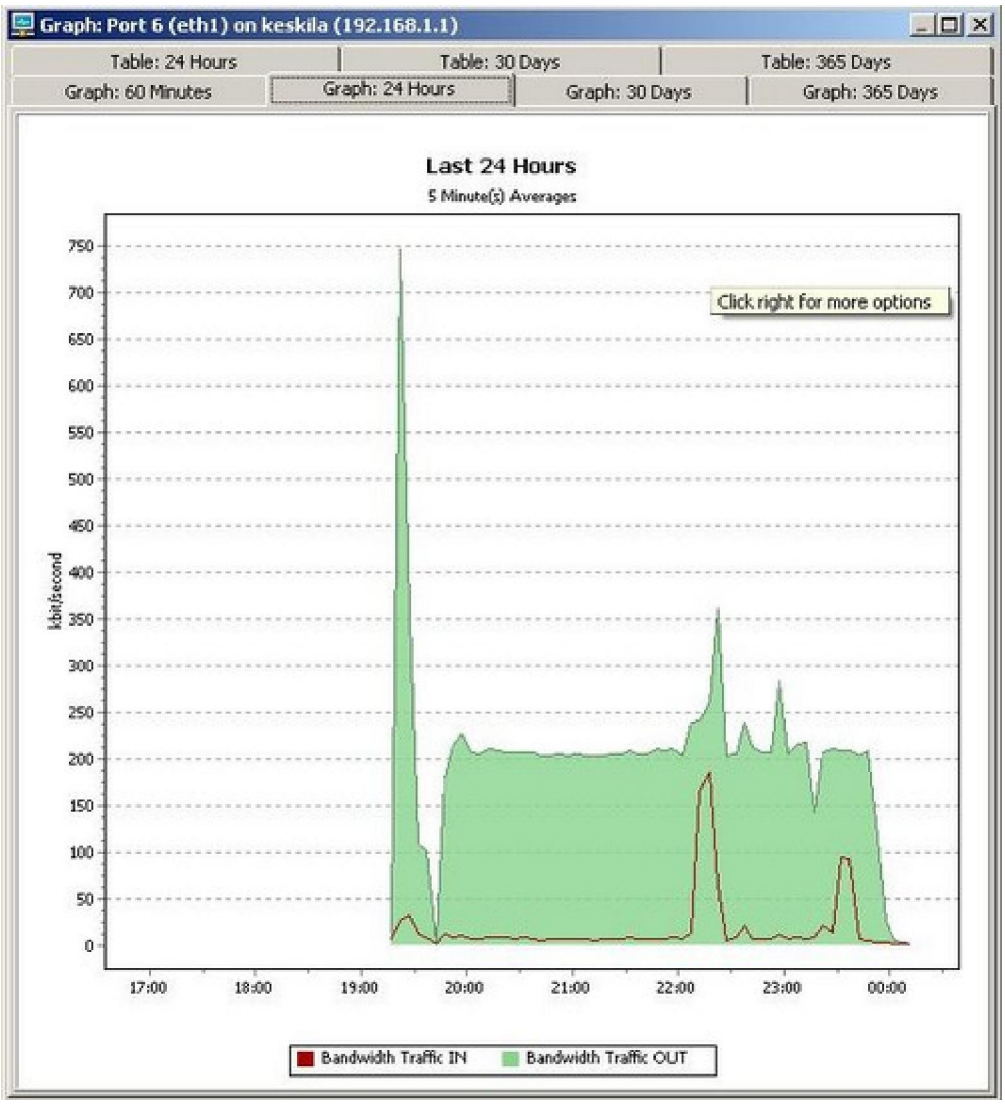


Table: Port 6 (eth1) on keskila (192.168.1.1) (24 Hours, 5 Minute(s) Averages)

Table: 24 Hours

	Port 6 (eth1) on keskila (192.168.1.1)						
	Bandwidth Traffic IN		Bandwidth Traffic OUT		Sum		Coverage
	kbyte	kbit/second	kbyte	kbit/second	kbyte	kbit/second	%
19/08/2006 12:05 - 12:10	1 960,383	107,500	9 856,684	540,371	11 817,267	647,871	50
19/08/2006 12:00 - 12:05	3 764,182	102,804	13 568,894	370,571	17 333,075	473,375	100
19/08/2006 11:55 - 12:00	3 850,973	105,175	13 362,625	364,962	17 213,598	470,136	100
19/08/2006 11:50 - 11:55	4 095,701	111,859	15 650,622	427,423	19 746,323	539,282	100
19/08/2006 11:45 - 11:50	4 192,649	114,506	23 987,456	Click right for more options		769,633	100
19/08/2006 11:40 - 11:45	4 394,269	120,005	36 672,367	1 001,567	41 066,636	1 121,572	100
19/08/2006 11:35 - 11:40	3 915,925	124,473	31 635,315	1 005,652	35 551,240	1 130,125	86
19/08/2006 11:30 - 11:35	4 419,206	120,690	37 844,571	1 033,512	42 263,777	1 154,202	100
19/08/2006 11:25 - 11:30	4 643,457	126,818	38 346,364	1 047,321	42 989,821	1 174,139	100
19/08/2006 11:20 - 11:25	4 333,093	118,334	29 758,919	812,725	34 092,012	931,059	100
19/08/2006 11:15 - 11:20	2 586,958	70,653	19 068,586	520,714	21 653,524	591,367	100
19/08/2006 11:10 - 11:15	376,028	10,269	6 958,414	190,036	7 334,442	200,306	100
19/08/2006 11:05 - 11:10	42,541	1,162	58,830	1,607	101,371	2,769	100
19/08/2006 11:00 - 11:05	40,398	1,103	55,479	1,515	95,877	2,619	100
19/08/2006 10:55 - 11:00	36,260	1,839	45,696	2,318	81,956	4,157	54
19/08/2006 10:50 - 10:55							

Edit | Auto Refresh | Close



Maintenant que nous avons vu ce que nous pouvions faire avec SNMP et SYSLOG, il est possible de créer une stratégie afin de pouvoir surveiller le réseau toute les semaines voir tous les mois.

Puisque nous analysons un réseau sans fil, il serait idéal de pouvoir faire la différence entre les utilisateurs connectés et ceux autorisés à se connecter. Cette analyse peut se faire au niveau des adresses MAC.

Il vous faudra alors 2 documents :

- Les adresses MAC des utilisateurs qui se sont connectés au réseau
- Les adresses MAC des utilisateurs autorisés à se connecter au réseau

Les adresses MAC des utilisateurs connectés au réseau sont conservées dans un log obtenue par SYSLOG.

Par contre, pour recenser les MAC autorisés, vous avez plusieurs solutions :

- Intervenir manuellement sur chaque poste et relever l'adresse MAC de la carte wifi.
- Créer une interface web en php qui relèvera automatiquement l'adresse MAC de l'utilisateur : bien sur, il faudra trouver un moyen d'obliger l'utilisateur d'accéder à l'interface.