----Lexique----débuter en Wifi ?----Quel wifi choisir?----architecture réseau----les antennes----Astuces Wifi

Configurer mon ordi pour être client du réseau

Configurer mon wifi pour être membre du réseau en sécurité

Le wifi n'est en fait qu'une norme de communication réseau remplaçant les traditionnels câbles.

Pour réaliser une liaison Wifi avec accès haut débit au net, il faut :

Solution 1 :

Un **modem ethernet** ADSL ou Câble(Noos pax ex) branché sur un **Point d'accès Wifi (AP)**. Le(s) **ordi**(s) communiqueront en wifi avec celui-ci. Ils doivent donc être munis des adaptateurs réseau Wifi idoine **(carte PCMCIA, adaptateur USB ou PCI**)

Solution 2 :

Un **modem USB** branché sur un **ordi à demeure**. Cet ordi servira de relais vers soit un Point d'accès Wifi (avec lequel communiquent les autres ordis), soit directement vers les autres ordis sans passer par un Point d'accès (dans ce cas, ne pas espérer traverser plus de 2 ou 3 cloisons). Il en résulte l'économie du point d'accès. Tous les ordis doivent être munis d'un **adaptateur wifi**. Cette structure sans AP s'appèle un **réseau Adhoc**

La solution la plus stable et pratique reste la 1ere.
La 2eme demande à ce que l'ordi connecté au modem USB soit constamment allumé, afin que les autres ordis puissent accéder au net.

Les antennes, souvent bricolées car tout aussi efficaces que celles proposées par des fabricants et parfois 10x moins cher, permettent un partage de la connection web entre voisins d'un immeuble ou d'une rue, voire plus. Attention cependant à la règlementation qui n'autorise que des puissances très limitées. Une petite antenne perso risque très vite de dépasser ces limites (100mw de pire).

Pour ce qui concerne la santé, la puissance est limitée à 100mw. A comparer avec un téléphone GSM qui à lui seul diffuse une puissance de 2w (20x plus). Il n'y a pas de risque particulier avec le Wifi.

Le seul moyen de savoir si un voisin peut partager votre accès web est de tester la liaison. En effet, cages d'ascenceurs, fours micro-onde, béton armé, etc...peuvent altérer le signal. On peu dire que traverser 2 étages (parquets, brique), ou quelques murs (brique) n'est pas un problème. Au delà, il faut tester.

Le matos :

Une carte PCMCA pour ordi portable coûte entre 60 et 12O euros, selon le magasin et la marque. Un adaptateur USB ou PCI coûte sensiblement le même prix
Si un Point d'accès Wifi est nécessaire, il faudra compter entre 110 et 250 euros, toujours selon le magasin et la marque.

Les magasins :

Charlie12 fais de bons prix (en face de surcouf) http://www.charlie12.fr/)

Hflan (http://www.hflan.com) permets de se procurer des connecteurs pour antennes, des antennes, et les câbles tout faits (**pigtail**).
Un simple coup de fil ou Email et il vous conseillera sur le connecteur, l'antenne ou le câble à prendre.

Les marques :

Linksys et Dlink sont les plus appréciées des wifistes : Qualité, prix, fréquences des mises à jour, facilité d'utilisation.

Pour info, un AP (acces Point) DI 614+ de chez Dlink se trouvera à plus de 220 euros chez Surcouf, et à moins de 140 euros chez Charlie12.

Labon : Thu, 3 July, 2003 **Back**

Quelle norme wifi choisir ? a, b ou g

Le 802.11b

Devenu un standard appelé Wifi, il communique sur la bande des 2,4 ghz.
C'est le matèriel qui à permis la naissance de ce système de communiquation de nonnées pour le grand public
Autrefois (et toujour en France) utilisé par l'armée, son usage fut soumis à autorisation.
Maintenant il ne faut une autorisation que si vous comptez émettre sur le domaine public (rue par ex).
Tout matèriel labellisé Wifi est compatible avec du matèriel wifi, quelque soit sa marque.
Le débit théorique est de 11mbps, descandant à 1mbps avec la distance et les obstacles.

Le 802.11b+

Proposé par la plupart des fabricants, il permets une communication à 22mbps entre matèriels compatibles.
Je ne sais pas si un matèriel D-link acceptant ces débits pourra communiquer à 22mbps avec un matèriel Linksys ou autre pouvant tourner à 22mbps.
Il y a de fortes chances que la communication s'établisse à 11 mbps (standard).
Le 802.11b+ ne change rien à la portée globale du réseau sans fil établi.
Au mieux, on pourra constater un débit un peu supèrieur entre une borne 802.11b+ et un client fonctionnant en Wifi (b)

Le 802.11a

Né aux US, ce standard (il me semble que la norme "a" a été définie comme un standard) fonctionne sur la fréquence des 5ghz.
Pas de compatibilité avec le wifi (b), débits de 54mbps et portées bien inférieures au wifi.
On trouve des AP intégrant du "b" et du "a" mais à des prix supèrieures au wifi.
La présence du "a" en France est marginale.

Le 802.11g

Dernier né, la plupart des fabricants ont sorti du matèriel fonctionnnant en "g"
Totalement compatible avec le "b", conctionnant à 54mbps, et d'une portée légèrement infèrieure au wifi (b), fonctionnant sur la bande des 2,4 ghz comme le "b", il n'y a pas de problème avec la règlementation française.
Il semble que ce soit LE standard à venir, un peu comme USB 2 par rapport à l'USB1

.Voilà, si vous achetez du matos en ce moment, il peut être judicieux de prendre du 802.11g.

Apple à sorti en grande pompes du nouvel Airport (Arport Extreme) fonctionnant en "g", donc s'intégrant dans les installations existantes et à venir.
D-link en sort aussi, Linksys aussi, etc...
A vous de voir si vous préférez du matèriel éprouvé (b) ou du high tech (g) fonctionnant avec les standards.

Labon : Thu, 3-07-2003 18:55

Structures types de reseaux Wifi

Back

Ci-dessous les liens des pages explicatives de chaque config type

petits schémas simplifiés d'agencement matèriels vous permettant de mettre en place des solutions wifi selon vos besoins et objectifs accompagnés de leurs réglages logiques et leurs difficultés. Ces schémas peuvent être modifiès à loisir selon vos besoins

1- **Modem Ethernet, 1 ordi, Un AP**

1 ordi, connection Wifi au net pour plus de liberté. Pas de partage de connection. Solution évolutive vers le partage de la connection filaire vers d'autre ordi, ou d'ordi en ordi suivant le mode ADHOC (d'ordi en ordi par leurs adaptateurs WIFI USB, PCI ou PCMCIA)

2- **Modem USB ou Ethernet , 1 ou plusieurs ordis**

1 ordi connecté au modem, une liaison Wifi pour d'autre ordi.
Partage de la connection vers d'autre ordis, suivant le mode AD-HOC (d'ordi en ordi par leurs adaptateurs WIFI USB, PCI ou PCMCIA) ou via un AP, en activant le partage web sur l'ordi connecté au modem. Ordi à demeure pouvant servir de serveur Web, et serveur d'authentification des clients Wifi.

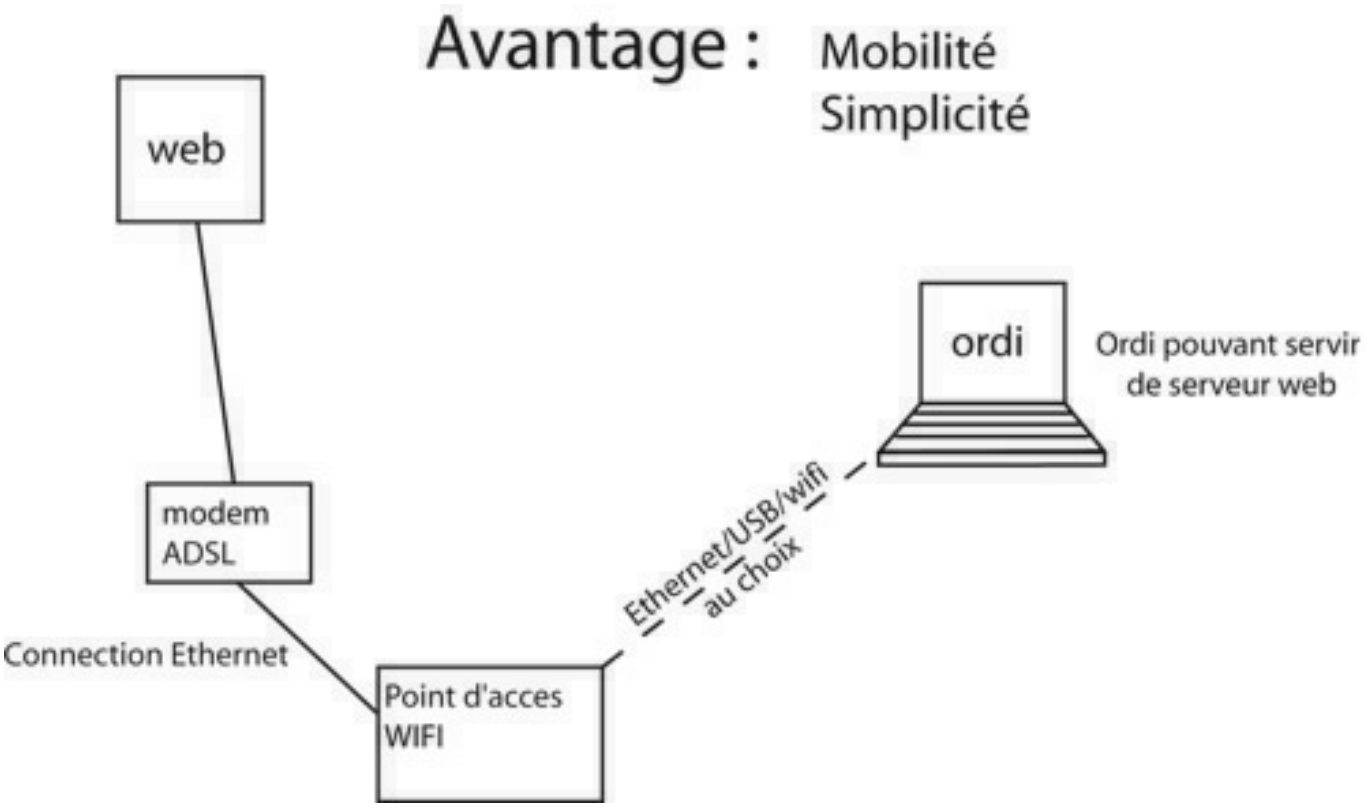
3- **Modem Ethernet, AP serveur DHCP/firewall, Plusieurs ordis** : **ma config**

Solution pratique et simple pour partager sa connection Internet avec plusieurs ordis mobiles ou fixes.
Le routeur s'occupe de sécuriser le réseau grâce à un Firewall qui autorise ou refuse les accés et les échanges de données réseau/réseau (lan/lan), réseau/web (lan/wan), web/réseau (wan/lan).
Tout cela par un paramétrage simple mais astucueux.
Ce point d'accés peut aussi faciliter la gestion du réseau par un adressage dynamique des clients Wifi (DHCP)

Labon:
Thu, 3
July,
2003

Back

1 ordi, 1 modem Ethernet, 1 AP Wifi simple (Ethernet>wifi)



**1 ordi, liaison Wifi au net pour plus de liberté. Pas de partage de connection.
Solution évolutive vers le partage de la connection vers d'autre ordi, ou d'ordi en ordi suivant le mode AD-HOC (d'ordi en ordi par leurs adaptateurs WIFI USB, PCI ou PCMCIA) en activant le partage web sur l'ordi d'origine.**

La config :

Sur l'AP, commencez par attribuer un mot de passe admin différent de ceux d'origine.1- Configurer le point d'accès afin qu'il puisse se connecter au web via le modem ADSL. Entrer les réglages donnés par le Fournisseur d'accès au net (FAI).
Pour ce faire, suivez le guide fourni avec votre AP.
L'idéal étant une configuration par l'intermédiaire de votre navigateur web (HTTP). Pas de driver, solution multiplateforme, configuration à distance font partie des avantages de ces points d'accès.

Bien se renseigner avant d'acheter même si la plupart des AP se configurent de cette façon.Si cet AP n'est réellement qu'un simple convertisseur Ethernet>Wifi, il est possible que les réglages donnés par votre FAI ne soient à mettre que sur votre modem/routeur ou votre ordi, au niveau des réglages TCP-IP de votre interface réseau (Carte WIfi ou carte Ethernet).

Ne possèdant pas d'AP simple (sans DHCP ni Firewall) Ce tutoriel est plus théorique qu'issu d'une certaine expérience. La config de l'AP peut être différente de la procédure que je décris.

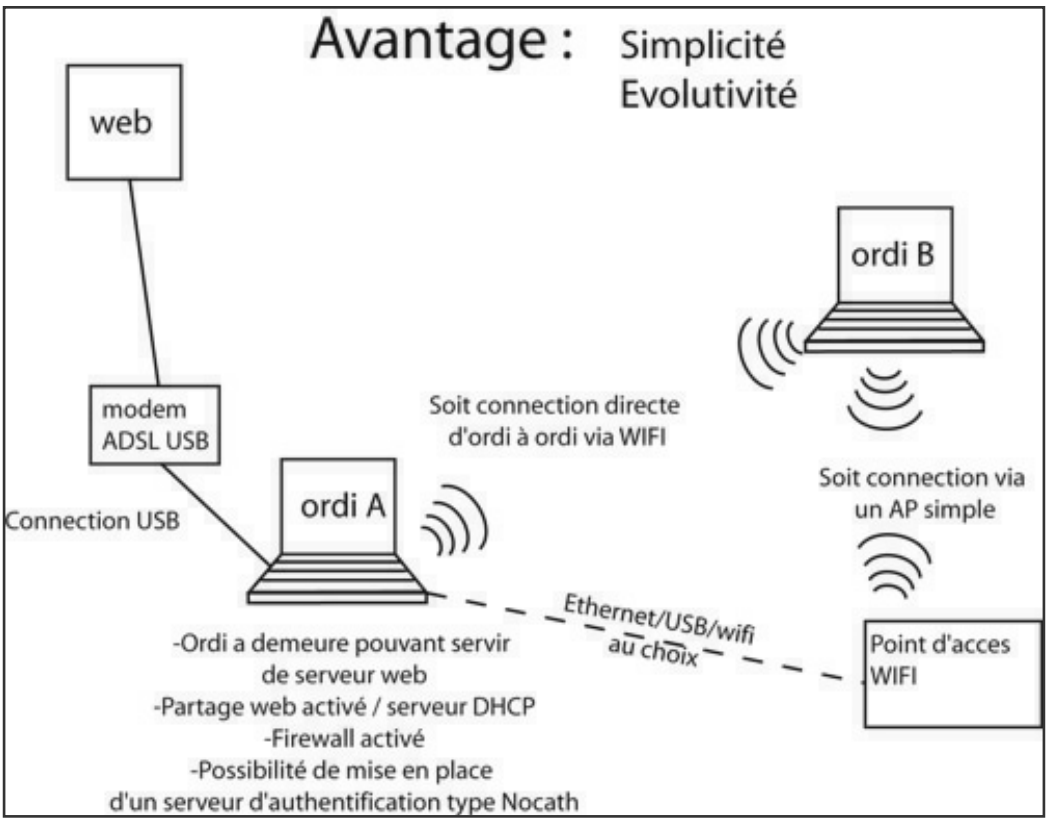
Back

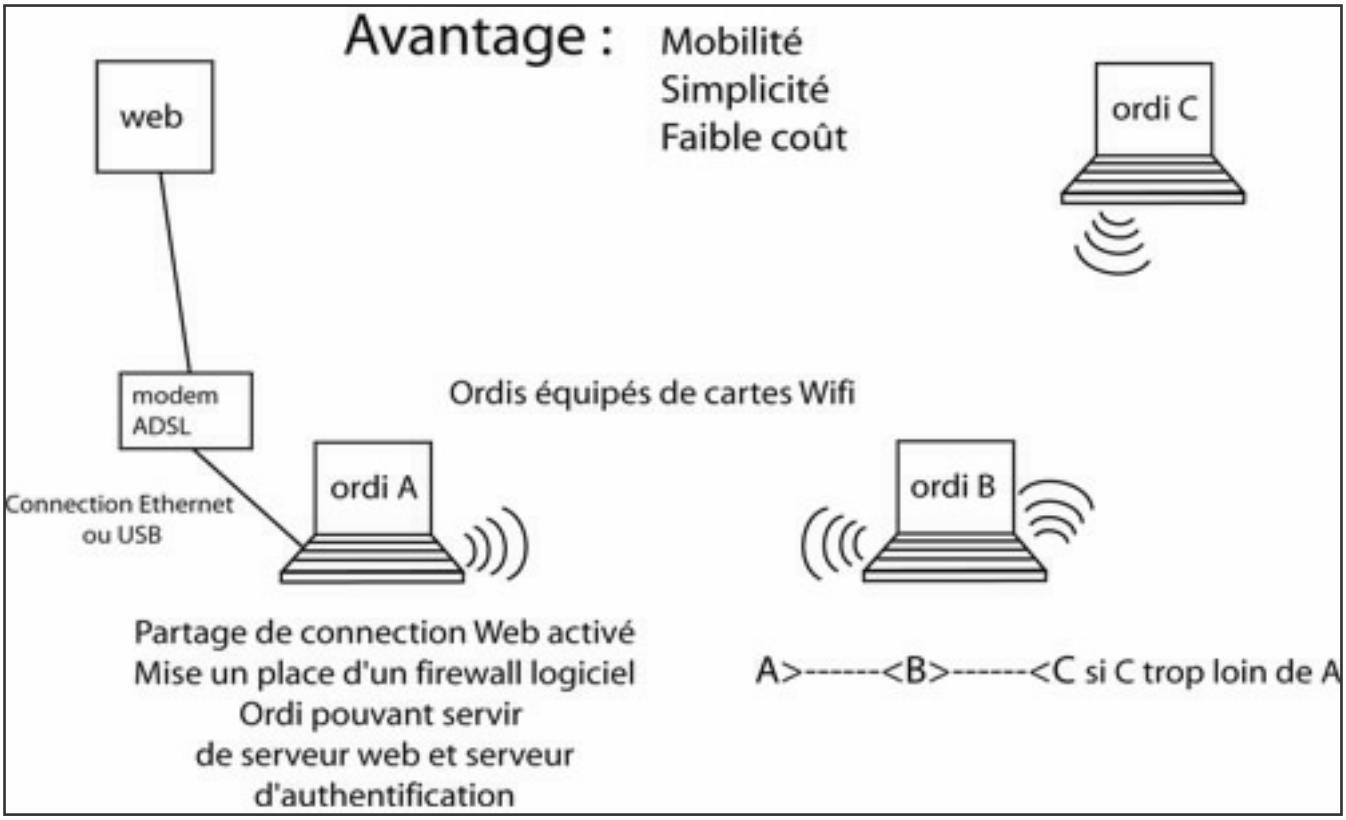
Labon
: Thu,
3
July,
2003

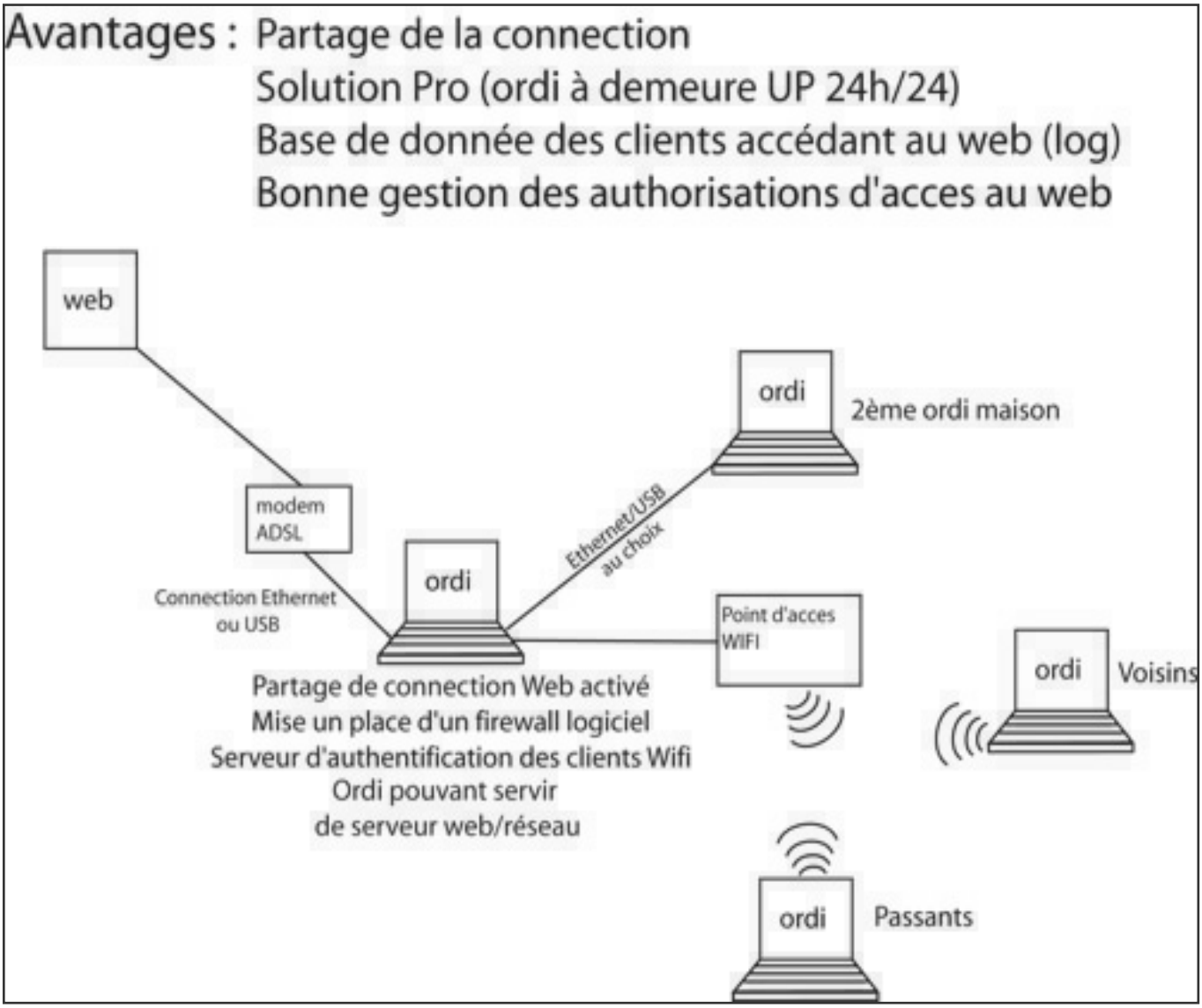
2

Back

1 modem USB, 1ordi, évolutions vers plusieurs ordi
Possible avec 1 modem Ethernet




Avantage :
Mobilité
Simplicité
Faible coût
web
ordi C
modem ADSL
Ordis équipés de cartes Wifi
Connection Ethernet ou USB
ordi A
ordi B
Partage de connection Web activé
Mise un place d'un firewall logiciel
Ordi pouvant servir de serveur web et serveur d'authentification
A>------<B>------<C si C trop loin de A



1 ordi à demeure, liaison Wifi au net des autre ordis pour plus de liberté.
Partage de la connection vers d'autre ordis, suivant le mode AD-HOC (d'ordi en ordi par leurs adaptateurs WIFI USB, PCI ou PCMCIA) ou via un AP, en activant le partage web sur l'ordi connecté au modem.Le mode Ad-hoc est intéressant car pas de point d'accès, donc réduction des coûts.
Par contre, à moins d'utiliser des antennes perso, les distances de liaison peuvent être limitées.
Sans augmentation de la puissance du signal, n'éspérez pas traverser plus d'un mur ou deux.
Un ordi peut toujours servir de relai signal entre deux ordis.

La configuration :

Une fois l'ensemble modem USB et ordi A configurés pour accéder au net (en suivant les indications du fabricant du modem et du fournisseur d'accès), on peut permettre à d'autres ordis de partager la connection via un système Wifi.

Selon le mode Ad-hoc :

L'ordi A devient une borne d'accès Wifi au même titre qu'un AP, mais au signal moins puissant. Chaque ordi se mettra en relation avec l'adaptateur WIFI de l'ordi A, qui distribuera des adresses IP selon le mode DHCP. L'ordi A devra aussi jouer le rôle de Firewall (intégré au système ou de tierce partie), protégeant le réseau du web, et protégeant aussi le réseau comme l'accès internet de clients WIFI indésirables.Mais attention, le mode Adhoc n'est interressant que si vous cherchez une connection pour votre appart. Au-delà de 2 cloisons, le signal peut être perdu. Si vous cherchez à traverser plus d'obstacles et/ou plus de distance, il vous faudra un AP ou une bonne antenne.

Avec un AP :

L'ordinateur A communique avec un AP soit en Wifi soit en Ethernet.
L'ordi reste, du fait du partage internet, un serveur DHCP. L'AP ne fait ici qu'augmenter le signal, si besoin grâce à une antenne à fort gain (voir les antennes maison) bien placée.En partique, l'ordi A devient une passerelle entre le web (une adresse IP) et un réseau local connecté sur une autre interface réseau (carte Ethernet, carte Wifi, réseau USB, etc.), donc une autre adresse IP interne au réseau.
Lors du partage internet, il convient donc de spécifier quelle est l'interface du réseau local, et son adresse IP, de même que le masque de sous réseau (en général 255.255.255.0).
L'adresse IP du réseau local de l'ordi A sera considérée comme l'IP du serveur par les autres machines du réseau.Avec certains logiciels de Firewall/partage de connection internet, chaque client devra être configuré manuellement au niveau des paramètres TCP-IP. Donc, attribution manuelle d'une adresse IP pour chaque client, et renseignement des DNS fournis par le FAI. C'est mon cas, j'utilise Brickhouse sur Mac OS 10.2.3.
Si le serveur (ordi A) à une adresse réseau local type 192.168.0.1, les clients auront la même mais avec un incrément de +1 : Client 1 : 192.168.0.2, Client 2: 192.168.0.3, Client 3: 192.168.0.4, etc...
L'adresse IP de l'AP, sera comprise dans ces adresses. Même si l'AP à sa propre adresse IP, il devient transparent pour les clients WIFI.

Solution Serveur

Par ailleurs, il est possible d'installer sur l'ordinateur A un serveur d'authentification type Nocat. Mais c'est délicat pour un novice. On rentre ici dans des notions très poussées de gestion réseau, éventuellement de base de donnée des clients.
La ligne de commande devient vitale. Le grand intérêt est ici de permettre à tout client de se connecter au web après s'être enregistré auprès du serveur. L'administrateur peut ainsi savoir qui s'est connecté et quand.
Si la justice vous reproche d'avoir pénétré dans le réseau de la banque de France, vous pourrez toujours savoir quel client est à l'origine de cette infraction.Je m'y suis essayé sans parvenir à quoi que ce soit de probant.

Ce système marche, mais faut savoir le faire marcher.

Quelques notions de réseau...
Site recensant les développement de solutions serveur : http://sourceforge.net/
How To pour Nocat : http://cterix.free.fr/Reseau/NoCatAuth
Administration Serveur et BDD (base de donnée) par Webmin : http://www.webmin.com/
Apache et les formulaires Put ou Post : http://www.apacheweek.com/features/put
Doc MySQL : http://dev.nexen.net/docs/mysql/annotee/manuel_toc.php
Mac OS X et les solutions serveur (Tomcat, Apache, SSH, PHP, MySQL, etc.) : http://www.simonganiere.ch/mac/
Manuel PHP 4 : http://dev.nexen.net/docs/php/annotee/manuel_tocd.php
Tutoriels Serveurs et BDD pour Jaguar (OS X) : http://www.projectomega.net/
Solution Nocat : http://nocat.net/Pourtant, en configurant bien le firewall, on peu limiter sans problème les accès des clients non souhaités
Il suffit pour cela d'empécher les communications des ordis ayant des adresses IP non utilisées par le réseau vers le réseau et le web.
D'autre part, il est possible sur l'AP Wifi, d'activer un filtrage des adresses MAC (adresse physique de l'interface réseau du client). Ainsi seul les ordi étant autorisés pourront accéder au réseau et au net.Un bon hacker saura toujours, en y passant le temps nécessaire, contourner ces limitations,
mais vous limitez grandement les risques d'intrusion.Quand au criptage Wep, il peut aussi être activé, mais il faut savoir que certains logiciels permettent de trouver les clefs de criptage et donc, se connecter au réseau.

Mise en place de l'installation :

Afin de répondre aux besoins de couverture Wifi, le point d'accès Wifi doit être bien placé.Au centre de vos locaux par ex, si votre réseau Wifi ne concerne que votre local/immeuble.Sur votre Toit, si vous souhaiter émettre dans tout un quartier (interdit par l'ART) Pointé en direction d'un ami avec qui vous souhaitez partager votre connection
internet (autorisé s'il est dans le même immeuble).Dans tout les cas, si vous êtes amenés à utiliser une antenne externe pour accroître le signal dans une direction ou dans toutes les directions, réduisez au maximum la longueur du câble reliant l'AP à l'antenne. Plus celui-ci sera long, plus vous aurez de pertes de puissances importantes.Pour un câble de 6mm de diam, évitez les longueurs de plus de 1,5 m
Pour un c,ble de 10-11mm, évitez de dépasser les 6-7 m.Comment mettre son antenne sur le toit sans perdre toute la puissance par un câble d'antenne trop long ?En mettant l'AP sur le toit !!!!! et pour l'alimentation électrique, on la fait passer par le câble Ethernet reliant l'AP au Modem ou à la machine serveur. cela s'appèle le POE (Power Over Ethernet)Quelques liens pour ce type d'installationAlimentation de l'AP par Ethernet : http://www.nycwireless.net/poe/
Mise en boîtier étanche de l'AP : http://www.nycwireless.net/articles/enclosure/

Matèriel type :

Les fabricants de matèriel Wifi les plus réputés chez les wifistes :
Linksys : http://www.linksys.com/
D-link : http://www.dlink.com/
MacSense : http://www.xsense.com/product/broadband/wireless.html

Perso, Je trouve le matèriel D-link tout à fait satisfaisant. Je n'ai eu aucun problème particulier pour l'installer.
Le DI 614+, Connecté directement au modem, fera office de Firewall, serveur DHCP et routeur (avec ses 4 ports réseau en plus vous permets une installation mixte Filaire/wifi) autonome pour moins de 140 euros
Le DWL900AP+ vous permettra une conversion Filaire vers Wifi, avec Serveur DHCP. Il peut aussi jouer le rôle de borne relais, vous permettant d'augmenter la couverture de votre réseau.
Beaucoup de personnes sont aussi assez satisfaites du matèriel Lynksys, notament le WAP 11. Cependant, à service égal, le matos Lynksys me semnle un peu plus cher. Certains raportent quand même que la portée des Lynksys est légèrement supèrieure aux D-link. Mais si vous comptez mettre votre propre antenne, cette remarque ne compte pas.
Equivalent DI 614+ chez lynksys : BEFW11S4 (170 euros)
Equivalent DWL900AP+(135 euros) chez lynksys : WAP 11 (169 euros)Pour les cartes PCMCIA ou adaptateurs PCI et USB, le Wifi étant une norme internationnale, tout matos wifi peut communiquer avec n'importe quel matos Wifi. Le reste n'est qu'une question de réglages réseau (DHCP, IP fixe, filtrages MAC, etc...) qui peuvent évnetuellement empécher toute comunication.
Il est à noter que certains fabriquants proposent du Wifi amèlioré communiquant à 22 mbps au lieu de 11.
Si vous voulez bénéficier de tels services, mieux vaut avoir un matèriel uniforme en terme de gamme et de marque (gamme Airplus chez Dlink par ex)Les magasins Françcais pouvant vous procurer AP, Adaptateurs, Cables, connecteurs
Hflan : http://www.hflan.com/index.html
Au bon micro : http://www.aubonmicro.com/
Chez Charlie 12 : http://www.charlie12.fr/entreprise.asp
Chez Infracom, http://online.infracom.fr/
Chez Cyclades, en face de la gare de Lyon à Paris

Mon ancienne config (12/2002-modem USB)

Le modem usb branché sur mon mac.
Le logiciel Firewall "Brickhouse" me sert de firewall et de logis de partage de connexion.
Activation du partage web via l'interface wifi du mac en question dans brickhouse.
Réglage de l'adresse IP de cette interface wifi (Airport dans mon cas)
Cette adresse IP sera considérée comme l'adresse du serveur par les autres ordi.
En l'occurrence 192.168.10.1
Masque de sous réseau réglé sur 255.255.255.0
Dans une autre pièce, mon AP D-link 614+
IP adresse du lan : 192.168.10.10 par exemple
Masque de sous réseau idem que pour le mac.
Définition d'un SSID en mon adresse email donnée par Paris sans fil (node813@paris.....)
Pour le DHCP, j'ai défini une plage de 2 adresses IP pour d'éventuelles connections depuis la rue par des inconnus. mais en fait, ça marche pas vraiment (voir plus loin)
Mon mac et l'AP communiquent en wifi. Pas de câble.
Pour les autres ordi en câble branchés sur le 614+ ou en wifi depuis le 614+
TCP-IP : Manuellement.
Adresse du serveur : 192.168.10.1
Adresse IP : 192.168.10.2, 3, 4, etc...
Masque de sous réseau : 255.255.255.0
DNS : Les réglages fournis par mon fournisseur d'accès internet. Voila. quand mon mac est connecté au web, les autres ordi peuvent se connecter.
A savoir : C'est une solution temporaire et contraignante pour moi.
Mon ordi ne bébéficie pas du wifi, et je ne peu pas réèlement ouvrir mon accès internet aux autres.
Un client ne pourra pas surfer s'il n'a pas les DNS de mon fournisseur d'accès web configurés.
D'autres part les drivers du modem ont tendance à figer mon unix made in apple (Jaguar).

Sinon, un autre réglage plus souple qui marchait

Activation du partage de connexion intégré au système (10.2.3) sur mon port Ethernet. Via la carte Airport ça marchait que en mode Adhoc (sans AP), d'ordi à ordi
(à voir sous windows, je connais pas)
Branchement filaire à l'AP
Ap avec une adresse IP fixe je crois (je me souviens à moitié)
Réglage en mode DHCP sur les autres ordi.
Voila, mon mac s'était transformé en routeur/AP

Mais comme il fallait que je me connecte par un câbleà mon AP, ça me convenait pas.

Pour moi, l'idéal est d'avoir un modem Ethernet branché directement sur l'AP. Pas de drivers éventuellement plantogènes, accès web ouvert 24h/24 sans ordi allumé, liberté totale de tous les postes, serveurs ou non. C'est mon install actuelle (04/2003)

J'espère que ce descriptif de mon install peut en aider certains dans leur config.

Back

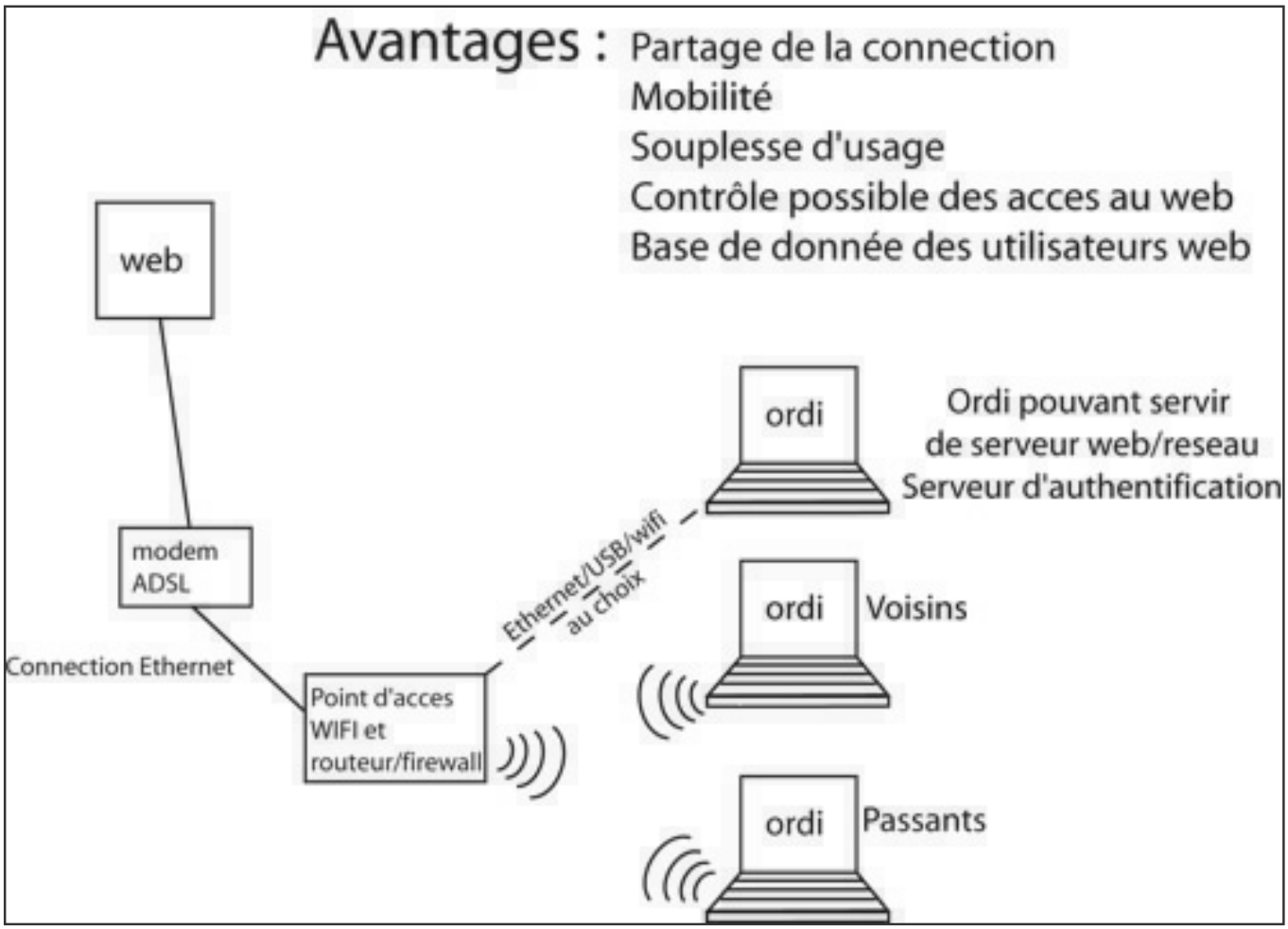
Labon
: Thu,
3
July,
2003

3

Back

1 modem Ethernet, 1 AP serveur DHCP/Firewall, plusieurs ordis mobiles.

Ma config



Solution pratique et simple pour partager sa connection Internet avec plusieurs ordis mobiles ou fixes.

Le serveur DHCP distribue les adresses IP aux clients, et le Firewall sécurise l'ensemble en autorisant ou refusant les accès et les échanges de données réseau/réseau (lan/lan), réseau/web (lan/wan), web/réseau (wan/wan).

Tout cela par un paramétrage simple mais astucieux.
Il est aussi possible d'avoir un réseau de clients habituels ayant des IP fixes et communiquant entre eux, ainsi que des clients de passage se connectant via DHCP, mais n'ayant pas accès au réseau d'IP fixes.
Il suffit là encore de bien paramétrer le Firewall.
Vous pouvez aussi faire en sorte qui les clients DHCP ne soient que des personnes vous ayant fait une demande de connection, en activant le filtrage par adresses MAC des clients DHCP.
En Pratique, on aura **UN AP** ayant l'IP 192.168.10.1. La plaque tournante du réseau, et le lieu de la plupart des réglages.
Les clients habituels auront par exemple les adresses 192.168.10.2 à 192.168.10.5 s'ils sont 4. Ces clients ne sont pas limités dans leur usage du net (P2P, FTP, Mail, Contrôle à distance, VPN, etc...) Ne pas oublier de spécifier un masque de sous réseau. 255.255.255.0 est le réglage couramment utilisé, mais libre à vous d'en changer.Les clients de passages, fonctionnant en DHCP auront par exemple les adresses 192.168.10.10 à 192.168.10.12.
Ainsi vous limitez votre accès à 3 clients en même temps, 10, 11, et 12.
D'autre part, dans les règles du Firewall, vous spécifiez que les adresses de 192.168.10.10 à 12 ne peuvent utiliser que le port 80 (web). Ils ne pourront pas faire de P2P et autre usages parallèles du web.
Vous bloquez aussi tout trafic réseau/réseau (Lan/lan) entre les adresses 10 à 12 vers le reste des adresses possibles du réseau, sauf celle de la borne Wifi (192.168.10.1) ou d'un serveur local (ftp local par ex).Quelques règles de Firewall auront donc suffit à bien sécuriser votre accès wifi. Ajoutez un filtrage des adresses MAC et votre système devient réellement difficile d'accès pour 99,99 % des possesseurs d'ordinateurs.

Adjoindre un Serveur d'authentification n'est nécessaire que si l'accès DHCP est ouvert à toute machine (pas de filtrage des adresses MAC). Dans le cas d'un accès libre de voisinage, ou d'un réseau urbain, ce type de serveur peut être vital à la réussite du projet. Encore faut il savoir manipuler ce type de chose..Quelques infos à ce propos données par un visiteur:

Solution pour installer un serveur (web mail news etc... avec mysql, php ...) il conseille SME/e-smith http://www.sme-fr.homelinux.net/ c'est une distib linux qui donne un server clef en main (pas besoin de connaitre linux) entierement parametrable par page web http://edocs.mitel.com/6000_SME_Server/smeserveruserguide/French/admin.html Il utilise ca chez lui et c'est vraiment puissant (selon son mail) voici le lien vers son site : www.chevrier.info

Un serveur d'authentification des clients Wifi (Nocath par ex)
devra se trouver entre le modem et l'AP (si j'ai bien compris).
Si vous voulez , vous pouvez installer sur l'un des ordis un serveur Web, FTP ou mail,
il suffira de le spécifier à l'AP Finalement, il est assez simple de paramétrer l'AP, surtout que l'aide fournie par le fabriquant
est souvent bien faite.
Par contre, si vous voulez monter un serveur d'authentification type Nocat, ou bien un serveur web hébergeant du FTP, un forum, une base MySQL, etc ..., les choses se corsent.Voici quelques liens pouvant aider ces aventuriersSite recensant les développement de solutions serveur :
http://sourceforge.net/
Solution Nocat : http://nocat.net/
How To pour Nocat : http://cterix.free.fr/Reseau/NoCatAuth
Administration Serveur et BDD (base de donnée) par Webmin : http://www.webmin.com/

Apache et les formulaires Put ou Post : http://www.apacheweek.com/features/put
Doc MySQL : http://dev.nexen.net/docs/mysql/annotee/manuel_toc.php
Mac OS X et les solutions serveur (Tomcat, Apache, SSH, PHP, MySQL, etc.) : http://www.simonganiere.ch/mac/
Manuel PHP 4 : http://dev.nexen.net/docs/php/annotee/manuel_tocd.php
Tutoriels Serveurs et BDD pour Jaguar (OS X) : http://www.projectomega.net/
Mise en place de l'installation : Le centre du réseau, (notre AP/serveur DHCP/Firewall/routeur) devra être placé dans un endroit stratégique.Au centre de vos locaux par ex, si votre réseau Wifi ne concerne que votre local/immeuble.Sur votre Toit, si vous souhaiter émettre dans tout un quartier (interdit par l'ART) Pointé en direction d'un ami avec qui vous souhaitez partager votre connection internet (autorisé s'il est dans le même immeuble).Dans tout les cas, si vous êtes amenés à utiliser une antenne externe pour accroître le signal dans une direction ou dans toutes les directions, réduisez au maximum la longueur du câble reliant l'AP à l'antenne. Plus celui-ci sera long, plus vous aurez de pertes de puissances importantes.Pour un câble de 6mm de diam, évitez les longueurs de plus de 1,5 m
Pour un câble de 10-11mm, évitez de dépasser les 6-7 m.Comment mettre son antenne sur le toit sans perdre toute la puissance par un c,ble d'antenne trop long ?En mettant l'AP sur le toit !!!!! et pour l'alimentation électrique, on la fait passer par le cable Ethernet reliant l'AP au Modem ou à la machine serveur. Cela s'appele le POE (Power Over Ethernet)Quelques liens pour ce type d'installationAlimentation de l'AP par Ethernet : http://www.nycwireless.net/poe/
Mise en boîtierétanche de l'AP : http://www.nycwireless.net/articles/enclosure/Matèriel type : Les fabricants de matèriel Wifi les plus réputés chez les wifistes :
Linksys : http://www.linksys.com/
D-link : http://www.dlink.com/
MacSense : http://www.xsense.com/product/broadband/wireless.htmlPerso, Je trouve le matèriel D-link tout à fait satisfaisant. Je n'ai eu aucun problème particulier pour l'installer.
Le DI 614+, Connecté directement au modem, fera office de Firewall, serveur DHCP et routeur (avec ses 4 ports réseau en plus vous permets une installation mixte Filaire/wifi) autonome pour moins de 140 euros
Le DWL900AP+ vous permettra une conversion Filaire vers Wifi, avec Serveur DHCP. Il peut aussi jouer le rôle de borne relais, vous permettant d'augmenter la couverture de votre réseau.
Beaucoup de personnes sont aussi assez satisfaites du matèriel Lynksys, notament le WAP 11. Cependant, à service égal, le matos Lynksys me semnle un peu plus cher. Certains raportent quand même que la portée des Lynksys est légèrement supèrieure aux D-link. Mais si vous comptez mettre votre propre antenne, cette remarque ne compte pas.
Equivalent DI 614+ chez lynksys : BEFW11S4 (180 euros)
Equivalent DWL900AP+(135 euros) chez lynksys : WAP 11 (169 euros)Pour les cartes PCMCIA ou adaptateurs PCI et USB, le Wifi étant une norme internationnale, tout matos wifi peut communiquer avec n'importe quel matos Wifi. Le reste n'est qu'une question de réglages réseau (DHCP, IP fixe, filtrages MAC, etc...) qui peuvent évnetuellement empécher toute comunication.
Il est à noter que certains fabriquants proposent du Wifi amèlioré communiquant à 22 mbps au lieu de 11.
Si vous voulez bénéficier de tels services, mieux vaut avoir un matèriel uniforme en terme de gamme et de marque (gamme Airplus chez Dlink par ex)Les magasins Françcais pouvant vous procurer AP, Adaptateurs, Cables, connecteurs
Hflan : http://www.hflan.com/index.html (tous connecteurs, câbles, antennes)

Au bon micro : http://www.aubonmicro.com/
Chez Charlie 12 : http://www.charlie12.fr/entreprise.asp (bons prix sur les AP et cartes Wifi)
Chez Infracom : http://online.infracom.fr/
Chez Cyclade, en face de la gare de Lyon à Paris (essenciellement des connecteurs N pour antenne)

Ma Config :

Afin de proposer un accès public soumis à inscription/autorisation.

Afin de protéger mon réseau local Wifi

Afin de pouvoir contrôler mon accès internet, voici ma config.

Avec mon Point d'Accès Dlink DI 614+ branché sur mon modem Ethernet, j'ai :

-Défini des adresses IP fixes pour moi, mon coloc et mes parents. Ces adresses (de 2à9) ont tous les droits, tous les ports dispo.
-Défini une plage d'adresses dispo en DHCP (de 20 à 30 donc pour 11 pers max) qui n'ont accès qu'au port 80 (net)
et qui ne peuvent pas communiquer avec la plage d'adresses IP fixes de mon réseau local.
-Le tout défini via le firewall intégré du Dlink 614+ De plus, un filtrage des adresses MAC a été mis en place.
Toute personne prévoyant de venir se connecter à mon accès depuis le café d'à côté doit s'inscrire via le formulaire mis en place sur la page d'accueil de ce site sur le wifi.Elle me fournit sont adresse MAC, et son nom.
Le mail que je reçoit (issu du formulaire) m'indique aussi l'IP de la personne. Ce qui permets éventuellement de la faire identifier par la justice, si vraiment cela était nécessaire.
J'autorise alors cette personne à se connecter à mon AP. J'autorise en fait son adresse MAC. Je n'ai pas activé de cryptage wep (ca complique la config tu passant, et apporte une sécurité toute relative)
Un log sur mon AP liste toutes les personnes qui se sont connectées et à quelle heure.
Je peux savoir qui fais quoi sur mon réseau (dans une certaine mesure) et peu fournir ces infos sur toute requette judiciaire. Il me semble donc, disposer d'un réseau interne relativement sûr et de proposer un acces web aux passant sans trop de risque (sauf si je croise LE hacker, celui que l'on trouve sur 100 000 utilisateurs d'ordi. Soit 1/100000).
Mais de toute façon, face à ce Hacker, peu de réseaux sont fiables à 100%On est loin du serveur d'authentification sur lequel vous rentrez un login et un mot de passe pour pouvoir surfer, mais c'est économique, simple, et suffisant pour moi.

Back

Quelques antennes rapides qui marchent...en l'air

1 : Le camembert ou autrement appelé

Patch antenna et comtelco :

Les explications données peuvent aussi être trouvées là :

http://www.geocities.com/lincomatic/homebrewant.html

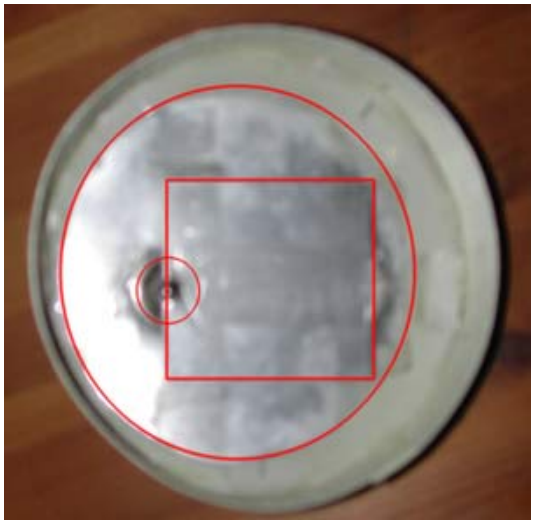
http://www.geocities.com/lincomatic/wifipatchantenna.html

http://reseaucitoyen.be/index.php?AntennePatch

http://devices.planet-wireless.de/comtelco/index.html

Vous y trouverez les plans, puissances, conseils, comparatifs, etc.

Mes remarques : Bonne pour accompagner un portable (un camembert est plus discret sur une table de café qu 'une boite de conserve).
Selon mon expérience, une can est plus puissante, mais plus directive.
C' est pas le même usage, c' est tout.



2 : La boite de conserve ou Cantenna

Après pas mal de butinage sur divers sites de réalisations,
comparatifs et calculateurs de dimensions, j'en suis venu à penser
qu'une can d'un diamètre de 3.25 pouces (82.5 mm) serait la plus à même à :
1 capter les 2.460 Ghz (canaux 10 et sup)
2, mieux marcher qu'une can d'environ 100mm de diam (ricoré). Le seul problème est, comme vous le verrez sur les calculateurs, qu'elle doit avoir une longueur d' environ 150mm.
Difficile à trouver en France. Vous trouverez des boites de café répondant à ce diamètre (83 mm), mais un peu courtes.
Vous pouvez toujours lui adjoindre une boite de maïs du même diamètre et haute d'environ 50 mm afin d'allonger le guide d'onde.

La puissance est grandement améliorée en ajoutant un cône d'environ 7 cm de long et d' un angle compris entre 20 et 30°. Selon mes essais, un angle trop prononcé fais perdre en puissance.

Voici les liens :

http://www.saunalahti.fi/~elepal/antenna2calc.php
http://www.turnpoint.net/wireless/cantennahowto.html
http://www.wifi-montauban.net/communaute/index.php/CaroTenne
http://www.saunalahti.fi/~elepal/antenna2.html
http://www.wireless-fr.org/communaute/index.php?RicoreRJ45
http://www.qsl.net/n9zia/wireless/pics/tincanant.jpg
http://www.turnpoint.net/wireless/has.html
http://www.turnpoint.net/wireless/antennas/performance.html
http://www.turnpoint.net/wireless/antennas/hunts.html
http://www.oreillynet.com/cs/user/view/wlg/1124
http://www.turnpoint.net/wireless/antennas/mypringles.html

http://forums.netstumbler.com/showthread.php?s=&threadid=2750

Bon, je penses que y à assez de lien comme ça pour se faire sa propre idée.

Pour ma part, ma conclusion est la suivante : La Pringle est trop fine et moins performante qu'une ricoré, elle joue dans la même cour que la can 3.25 pouces. Cela se confirme lorsque l'on consulte les calculateurs qui se basent sur le diam de la can, et sur la fréquence de travail désirée.

Pour ce qui concerne les can améliorées type yagi, c'est trop de boulot à mon goût.
Selon moi, ce type d'antenne est quand même plus pratique à demeure que en vadrouille, mais bon, chacun fais ce qu'il veut.
Bientot des chapeaux Cantenna à la mode ? ? je vous laisse immaginer...

3 : La Cantenna Bazooka, enfin...

J'ai trouvé ça sur un seul site

http://www.geocities.com/lincomatic/homebrewant.html à la fin de la page

Mais sur le forum de Paris sans fil.info vous trouverez un lien vers un site commercial fabricant ce bazooka. Rubrique Antennes, sujet Cantenna++ Ok, je suis sympa, le voici
http://www.cantenna.com/whatis.html

Originellement elle est constituée de 2 ou 3 cans. Pour une question évidente de simplicité, et surtout par un grand hasard, je me suis tourné vers l'emballage d'une bouteille de whisky réalisé en acier (plutôt qu'en carton).
Selon les tests dispos sur cette page, elle pulvérise pas mal de records en terme de rapport puissance/prix. A condition d'avoir récupéré l'embalage du whisky. Enfin, le whisky c'est bien bon, et ça peut toujours s'acheter, même si c'est plus cher que de la ricoré que je trouve dégueulasse (-: oui, j'en ai acheté une boite pour en faire une antenne, ça reste à faire, et je ne le ferais pas car j'ai trouvé mon bonheur dans le ....whisky :-)

Pour faire mieux, il faudrait se tourner vers des paraboles, super directionnelles, et plus cher.

Le diam de ma boite est de 87 mm, ce qui reste proche des 83 mm idéaux et loin des 100 mm de la ricoré. Super c'est ce que je veux !
La longueur de la mienne est d'environ 300 mm. On augmente donc la longueur du guide d'onde, ce qui théoriquement augmente la puissance (plus de surface)

Voir les antennes Wavequide, plus elles sont longues plus elles sont puissantes.
http://trevormarshall.com/waveguides.htm

Pour revenir à nos moutons, la longueur n'influe pas ou peu sur la position du connecteur N sur lequel est soudé le petit fil de cuivre.
Il suffit donc dans le calculateur suivant http://www.saunalahti.fi/~elepal/antenna2calc.php d'entrer le diam intérieur de votre boite de whisky et la fréquence centrale autour de laquelle votre antenne sera sensible pour obtenir toutes les dimensions utiles : Position du connecteur N, longueur du fil de cuivre, et longueur idéale de la can, qui ne nous intéresse pas puisqu'on l'augmente (enfin là je dis peut-être un bêtise). Il se peut en effet qu'une longueur double soit plus judicieuse qu'une longueur bâtarde.
Mais j'ai pas été jusque la dans mon antenne.
En fait la Cantenna Bazooka n'est qu'une Cantenna plus longue.
Il ne faut pas oublier de couper la collerette du bord supérieur afin de ne pas avoir de rétrécissement de la boite. Un simple ciseau et une pince coupante m'ont suffit.

Pour ce qui est du cône, si vous avez visité les sites consacrés aux Cantenna, vous avez dû en trouver un qui décrit le schéma du cône.
Pour ma part, j'ai remarqué une puissance accrue si l'angle n'est pas trop fort. 30° me semblent excessif, je pencherai plutôt pour 20-25°.
Une longueur de 7-8 cm semble bonne, mais faudrait faire des essai de cônes plus longs pour voir.

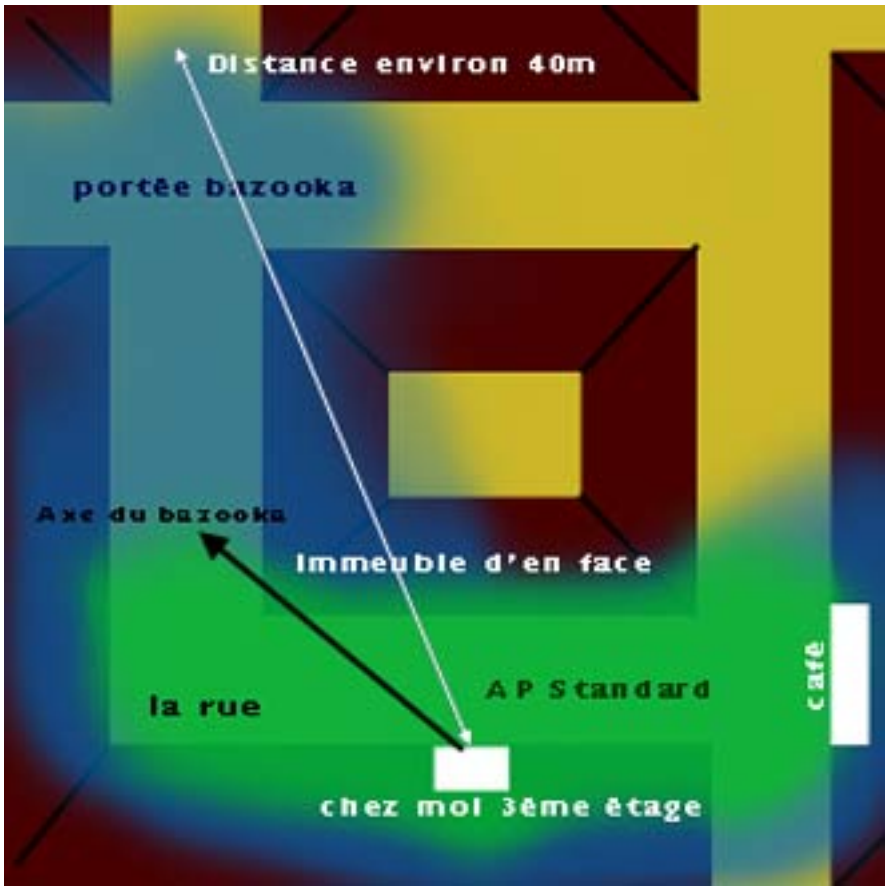
Mon cône est fait de papier épais servant de structure au papier alu plus résistant (c'est marqué sur l'étiquette) collé à la bombe de colle. Pour étanchéifier le tout, la face extérieure est enrubannée de scotch (non, pas le whisky !). L'antenne est ensuite mise dans un sac poubelle pour assurer une étanchéité et la discrétion à ma fenêtre.

les antennes pas chères selon la node 813

4 : Les tests : Camembert vs cantenna simple ou avec cône, elle même vs bazooka cône...

Je n'ai pas de mesures en DB ou autres valeurs précises, juste l'indice de réception et de bruit que me donne Macstumbler (sur le site du même nom) quand je suis à telle ou telle distance des antennes, dans telle ou telle position. Mon Power Book G4 possède 2 antennes intégrées de chaque côte de l'ordi. La réception est meilleure quand l'antenne de l'AP se trouve vers l'un des cotés de mon Mac.
Les valeurs que je vais vous donner correspondent donc à la reproduction de conditions X (telle position, telle distance) en changeant l'antenne. Pour info, cet indice atteint 103 quand je colle (sens imagé) une antenne de mon AP sur l'une des antennes du Mac. Le camembert avait à peu de choses prés la même puissance que les antennes standard de mon D-link 614+, en plus directionnelle (+- 60°) :
Indice max 60/103, bruit moyen 4/10La can m'a permis de faire un bond en terme de puissance, mais en la pointant bien précisément vers mon Power Book G4.
Y ajouter le cône m'a permis d'ouvrir le faisceau tout en augmentant fortement la puissance.
Indice max 65/103, bruit moyen 3/10Le bazooka avec un premier cône très froissé
Indice max 75/103, bruit moyen 3/10Le bazooka avec son cône final (2ème)
Indice max 81/103, indice moyen 74/95, bruit moyen 2/10Comme vous pouvez le voir, c'est pas mal. On part de 60 avec une moyenne vers 55 à un max de 81 et une moyenne de 74. En conditions réelles, j'ai

effectué 2 tests. L'un avec les antennes standard de mon AP, l'autre avec le bazooka.
Ma rue fait un angle à 90° à environ 20m à Gauche de ma fenêtre du 3ème.
Le défi est ici de voir quelle sera ma réception une foi que j'aurais tourné à l'angle est que je ne pourrais plus voir mon AP. Plus je vais m'avancer, plus le faisceau aura de pierre, de brique et de bois à traverser pour m'atteindre.Là c'est simple, avec la config de base, à peine j'ai tourné et que je m'avance un peu plus loin, plus rien du tout. Si j'ai le malheur, à l'angle, de me mettre derrière une voiture, pareil, je perds le signal.Avec le bazooka pointé vers l'angle, je peu , une fois l'angle passé, aller au prochain croisement (20m plus loin) et capter encore, faiblement mais je capte. D'autre part, le signal est beaucoup plus stable, même derrière un véhicule.Le comble pour le bazooka (censé être super directif), c'est que de l'autre coté de la rue (à droite de ma fenêtre), derrière le bazooka, je peu capter j'usqu'à 30m.
Au rez de chaussée , je capte aussi (3 étages au lieu de 2 avec le D-link standard) et au 6 ème aussi (3 étages au lieu de 2 avec le D-link standard).
Inutile de vous dire que dans mon appart, ça marche partout alors que le bazooka est toujours dirigé vers le même coin de la rue. Lorsque le bazooka est pointé sur l'immeuble d'en face, je peu, de l'autre coté du pâté de maison, capter le signal. Pas mal non, surtout si je veux partager ma connections NET avec des voisins un peu loin (à 2 immeubles par ex)Bref, plutôt qu'un grosse omni, le bazooka cône, c'est pas mal pour émettre large avec une préférence directionnelle.



Liens vers d'autres types d'antennes maison :

L'anglais est de rigueur dans la plupart de ces liens.

Omnidirectionnelles :

http://reseaucitoyen.be/index.php?AntenneOmni

Collinear :
http://perso.wanadoo.fr/backslash/antenneweb/
http://www.guerrilla.net/reference/antennas/2ghz_collinear_omni/
http://www.guerrilla.net/reference/antennas/2ghz_collinear_omni_lowpwr/
http://www.geocities.com/lincomatic/collinear.html
http://www.tux.org/~bball/antenna/

Slotted Waveguide :
http://www.trevormarshall.com/waveguides.htm
http://reseaucitoyen.be/index.php?SlottedWaveGuide2
http://www.narx.net/~mike/projects/waveguide/
http://seattlewireless.net/index.cgi/SlottedWaveguide
http://www.wafreenet.org/content/hillshub.html
http://reseaucitoyen.be/index.php?SlottedWaveGuide
http://members.iinet.net.au/~clark/FreeNet/

Directionnelles :

plates :
http://www.saunalahti.fi/elepal/antenna1.html

Cones et cornets :
http://www-mo.enst-bretagne.fr/~duflot/courstel/antennes/corele1f.html
http://reseaucitoyen.be/index.php?BoiteDeLait
http://reseaucitoyen.be/index.php?BoiteDeLait2
http://reseaucitoyen.be/index.php?CornetDeCarton
http://ReseauCitoyen.be/GroupeLg/cornet/cornet2.php
http://www.g0mrf.freeserve.co.uk/horn.htm
http://kyleti.aswwc.net/index.php?page=projects

Biquad :
NEW : http://mapage.noos.fr/crockers/site/biquad/biquad.html
http://perso.wanadoo.fr/backslash/antenneweb/
http://www.trevormarshall.com/biquad.htm
http://www.chez.com/f6kio/page19.html

Cans modifiées :
http://www.turnpoint.net/wireless/antennas/mypringles.html
http://www.netscum.com/%7Eclapp/wireless.html
http://www.oreillynet.com/cs/weblog/view/wlg/448

Hélice ou hélicoïdale:
http://www.wireless.org.au/~jhecker/helix/helical.html
http://reseaucitoyen.be/index.php?%41ntenne%48elicoidale2
http://www.chez.com/f6kio/page21.html

Parabollique :
http://www-mo.enst-bretagne.fr/~duflot/courstel/antennes/mirpar0f.html

antennes toutes sortes, portées, sécurité, pages de liens :

http://www.wlan.org.uk/antenna-page.html
http://www.byte.com/documents/s=1422/byt20010926s0002/1001_marshall.html
http://reseaucitoyen.be/index.php?Liege20020401
http://reseaucitoyen.be/index.php?AspectsAntennes
http://www.practicallynetworked.com/tools/wireless_articles_range.htm

Guides de référence :

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/agder_rg.htm
http://www.electronics-tutorials.com/antennas/antenna-basics.htm

Cables et connecteurs :

http://www.saunalahti.fi/elepal/wlancable.html
http://www.paris-sansfil.net/index.php/TechCable
http://nocat.net/connectors.html
http://www.binaervarianz.de/projekte/hardware/mactail/

Back

Back

Les cables d'antenne et connecteurs.

Les cables sont toujours en 50 ohm. Les connecteurs utilisés sont des prises N.

Pour des distances inférieures à 2 m, un cable faible perte d'un diamètre de 6mm suffira.
Pour des distances supérieures et jusqu environ 6 m, il faut passer à du cable faible perte de 10 ou 11 mm de diam.

Au delà, il vaut mieux passer à une solution POE (power over Ethernet) http://www.nycwireless.net/poe/.
Cela consiste à mettre l'AP prés de l'antenne (sur le toit par ex http://www.nycwireless.net/articles/enclosure/) et de faire passer les données comme l'alimentation par le câble Ethernet reliant l'AP au modem ou à la machine serveur.

Vous trouverez des câble 50 ohm et des fiches N à bon pris en face de la gare de Lyon à Paris, chez Cyclades. Mais n'y cherchez pas de connecteurs particuliers, genre SMA, Reverse SMA (pour les AP D-link), etc...
Pour ces connecteurs, il y à Hflan par exemple. Ils peuvent même sur demande (email ou téléphone) vous faire vos pigtails (connecteurs + câbles).

Quoi d'autre.....plus vous multipliez les connecteurs plus vous avez des pertes de puissance, et vu qu'on est déjà bien limité...

Tous les liens >>>>

Crockers : Sun 4 May, 2003 11:39

Une page pour vous faciliter le Wifi.

N'hésitez pas à nous soumettre vos astuces et à compléter celles existantes.

- Pouvoir envoyer ses mails depuis n'importe où - >	En activant un serveur SMTP sur votre ordi >	MAC OS 10.x - Windows - Linux
- Connaitre son adresse MAC- >	plaque d'imatriculation de votre adaptateur Wifi >	La page explicative
- se mettre en DHCP ->	pour surfer sur le réseau	La page explicative
Nous rejoindre sur AIM	Nos profils AIM sont dans le Forum !	Le forum
- Nous rejoindre en Chat sur le channel IRC ->	thématique : serveur >	la page explicative

Objectifs : Faciliter le surf des clients dans tout le quartier par une unification de certains paramètres de votre réseau wifi

-----Afin de faire partie du réseau, nous demandons d'établir votre nom de réseau wifi sur la base suivante :
"www.tdq5-6.fr.st" suivi du nom de votre rue et d'un numéro.

L'idée est ici d'inciter, par le SSID de votre point d'accès wifi, à venir visiter le portail du quartier.
D'autre part, cette uniformisation permets une "présence" du réseau pour le client.

Cela donne par exemple : www.tdq5-6.fr.st-monge1

------Pour le reste de votre installation wifi et réseau :
Afin d'éviter les abus et l'engorgement de votre connexion internet,
nous vous conseillons de limiter l'usage des clients (personnes se connectant depuis la rue)
aux simple consultation/envoi d'email, et à la naviguation web.
Vous pouvez aussi permettre l'utilisation de logiciels de chat AIM par ex.

------En vous enregistrant comme proprio d'AP, vous vous inscrivez à une Mailing list client.
Chaque enregistrement de client donne lieu à l'envoi d'un mail sur cette mailing list.
Y figurent les nom et prénom de même que l'adresse MAC du client.
Ainsi, si vous mettez en place un tel filtrage, il vous faudra renseigner votre AP de l'adresse MAC des clients afin que ceux-ci puissent surfer.

Il vous sera ainsi plus facile de garder trace des surf des clients, au cas ou l'un d'eux fasse des "bétises web"
Dans tous les cas, une centralisation des informations clients est en place sur une boite email et disponible pour toute requête judiciaire.

Comment faire ?

Comment mettre en place mon installation wifi ?

Comment limiter les usages de mon internet ?

Bientôt, les réponses à ces questions

Comment savoir qui se connecte à mon acces internet ?

Quelques liens tutoriaux

Config routeur et partage de connexion sous windows.
Passer à l'ADSL sous macintosh
Comprendre son Routeur/firewall1
Comprendre sou Routeur/firewall 2
Partage de connexion derrière un routeur (avec ou sans wifi)
Quantité de tutoriels macintosh orientés réseau, serveur et programation.
Le filtrage IP facile....

Pour pouvoir se connecter au réseau gratuit et ouvert ToiledeQuartier 5-6 :

1 Remplissez le formulaire destiné aux clients du réseau en précisant bien votre adresse MAC
L'adresse MAC est le numéro d'identification de votre carte réseau Wifi.
Ce numéro existe sur PC, linux, Macintosh, PDA, etc.... pour la trouver

2 Configurez votre carte réseau Wifi pour qu'une adresse IP lui soit attibuée automatiquement.
Autrement dit, mettez vous en DHCP.

Comment faire pour se mettre en DHCP et connaître son adresse MAC

Voilà, c'est fait.
Le temps que le réseau se mette à jour avec vos coordonnées,
vous devriez pouvoir surfer dans tous ces points dans les jours qui suivent.

Bon surf.

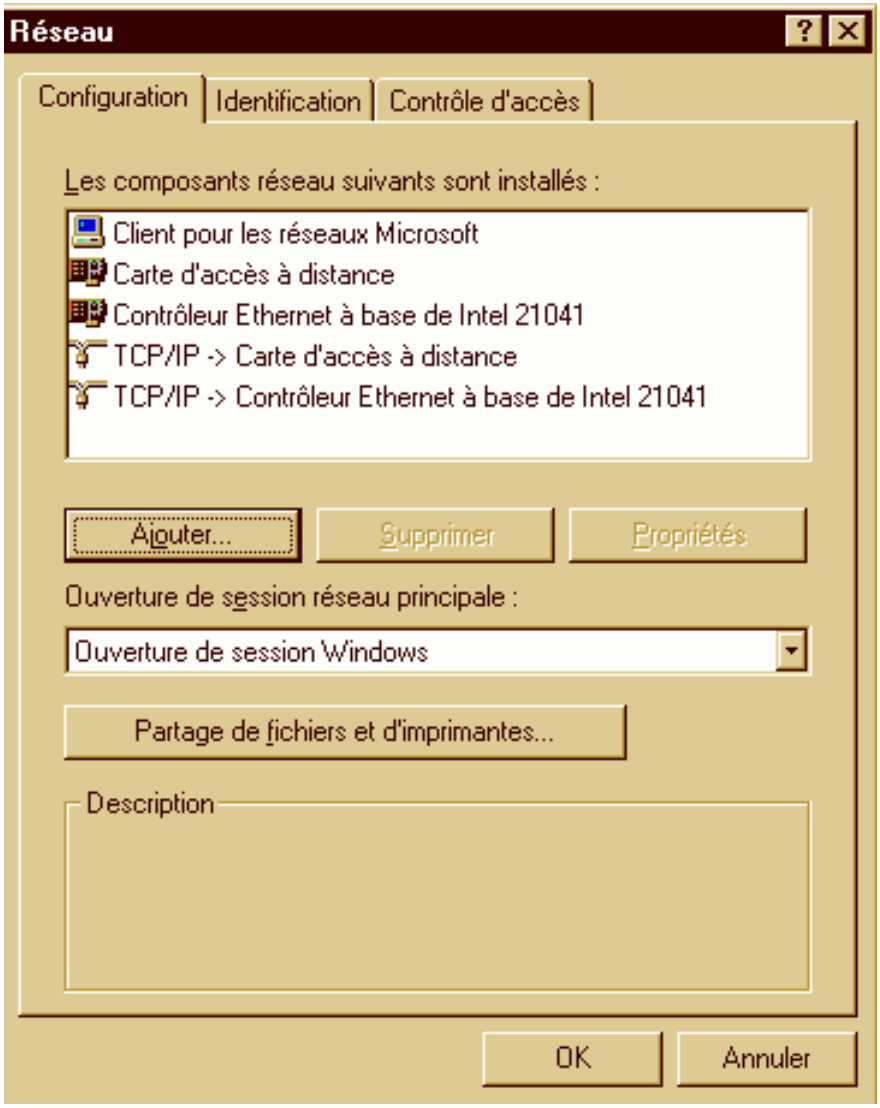
N'hésitez surtout pas à proposer des infos de quartier ou toute suggestion d'évolution du réseau et du portail de quartier.

Comment configurer son adaptateur réseau Wifi en DHCP (addressage IP automatique et dynamique)

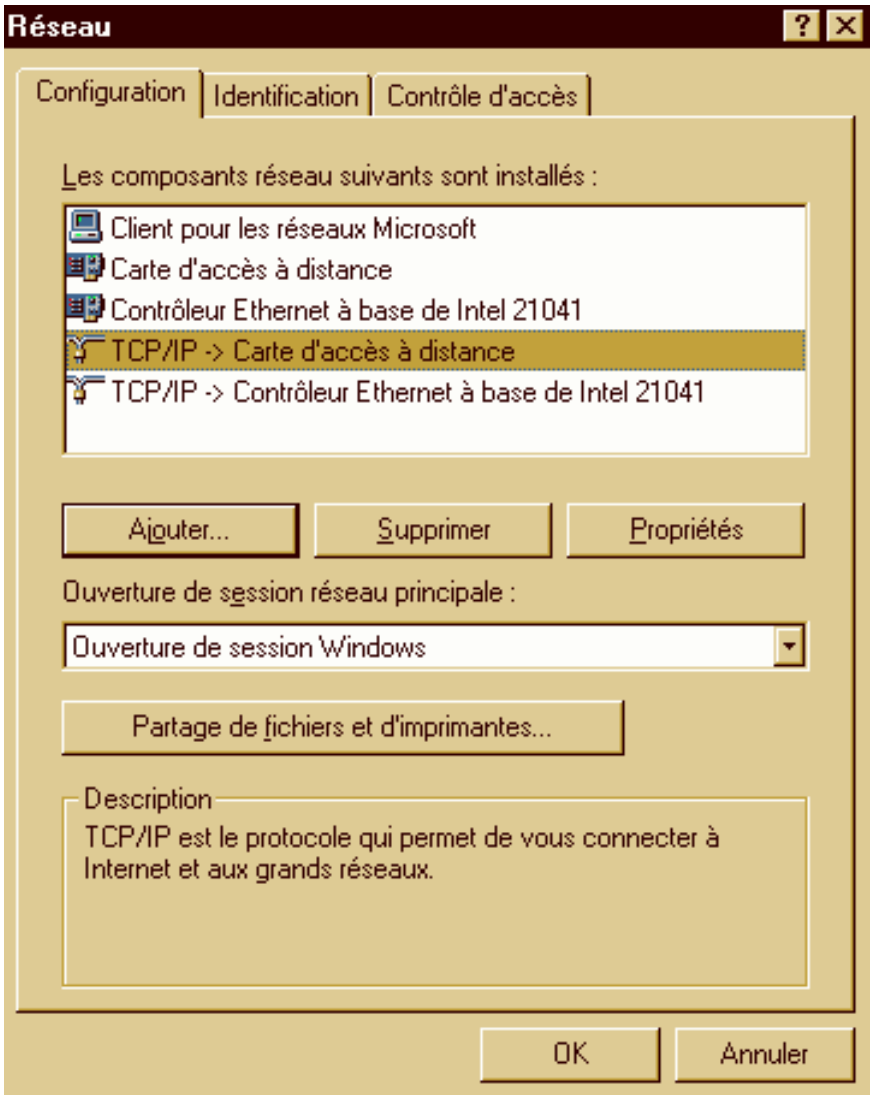
Comment connaître son adresse MAC

Sur PC :

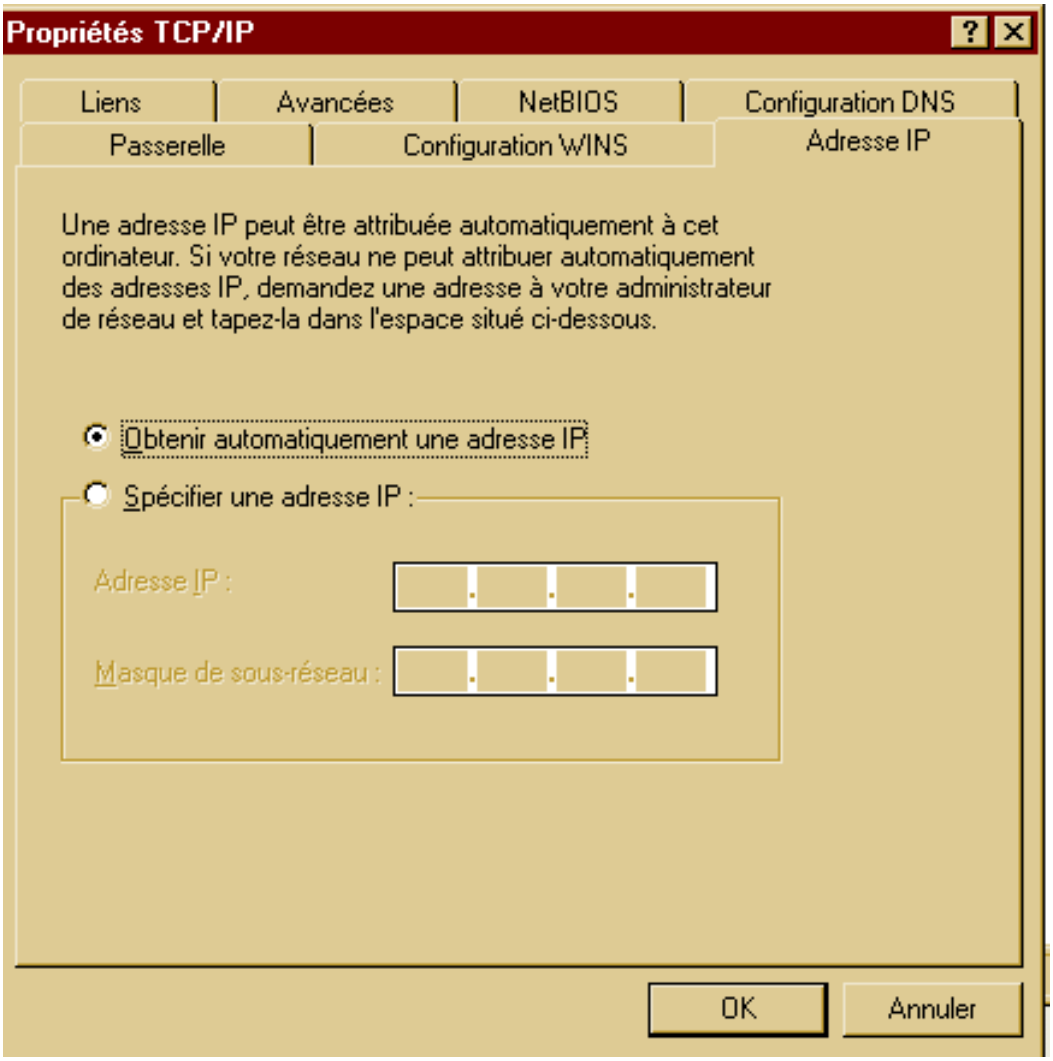
Se mettre en DHCP



Ouvrir "Poste de travail" puis "panneau de configuration" puis "réseau". Vous arrivez à cette fenêtre.



Sélectionner votre carte Wifi puis cliquez sur "propriétés"



Comme indiqué, cocher "obtenir automatiquement une adresse IP"

Connaitre la MAC adresse de votre carte Wifi sous windows

Pour **Windows 2000 et XP (NT4** également, à confirmer), télécharger l'utilitaire" getmac.exe" (604KB) du Kit de Ressources Microsoft

. La syntaxe et des exemples d'utilisation (en anglais) sont décrits dans le document getmac_d.htm qui accompagne l'installation dans le dossier C:\Program Files\Resource Kit\ . Le contenu en est repris ci-dessous:
Getmac.exe: GetMAC

GetMAC provides a quick method for obtaining the MAC (Ethernet) layer address and binding order for a computer running Windows 2000, locally or across a network. This can be useful when you want to enter the address into a sniffer, or if you need to know what protocols are currently in use on a computer.
File Required
* Getmac.exe
Getmac.exe Topics
* GetMAC Syntax
* GetMAC Examples
Getmac.exe Syntax
---

getmac [\\computername] [computername.domain.com]
Where:
\\computername
is the NetBIOS name of a computer accessible across a network (including by using RAS).
computername.domain.com
is the DNS name of a computer accessible across a network (including by using RAS).
Getmac.exe Examples

When you type:
C:\>getmac \\host
you get the following information returned:
Information for machine \\host Transport Address Transport Name
---------- ---------- 00-00-1B-16-78-76 \Device\NetBT_NE32007
00-00-1B-16-78-76 \Device\NwlnkNb 00-00-00-00-00-00 \Device\NetBT_NdisWan5
52-41-53-48-00-01 \Device\Nbf_NdisWan4 52-41-53-48-00-04 \Device\Nbf_NdisWan8
00-00-1B-16-78-76 \Device\Nbf_NE32007
In this example 00-00-1b-16-78-76 is the address of an NE3200 Ethernet card, and 00-00-00-00-00-00, 52-41-53-48-00-01, and 52-41-53-48-00-04 are RAS addresses.
When attempting a connection to a remote computer over the network, the workstation service will use the following order:
NetBT (TCP/IP) over the NE3200
NwlinkNb (IPX) over the NE3200
NetBT over one of the RAS links
Nbf (NetBIOS) over two other remote access server links
Nbf over the NE3200
To change the order in which Windows 2000 attempts connections for the workstation service
1. In Control Panel, double-click Network.
2. Click Bindings.
3. In "Show Bindings For," select "Workstation."
4. Adjust the binding order by using the arrows on the right.

Les utilisateurs devraient télécharger dans ce même Kit de Ressources l'outil WNTIPCFG.EXE... familier aux ex-utilisateurs de Windows 9x, ne serait ce que pour vérifier l'adresse IP attribuée.

Pour **Win9x**, pas glop !? C'est stressant ces Zindows ! Cet OS et ses dérivés ne m'ont jamais convaincu. Utilisateurs de Win9x passez donc à Win2000ProSP4 ! Plus sérieusement des recherches sont en cours. Le résultat vous sera communiqué dès disponibilité.

Sur Macintosh

Sur MAC OS 10.x
Dans le menu pomme, ouvrez les Préférences Systeme, puis "Reseau"

Sur Mac OS 9 et infèrieurs
Dansle menu pomme, ouvrez le "tableaux de bord", puis "TCP/IP"

Selectionnez votre interface réseau Wifi

En face de "Configurer" vous pourrez choisir "Via DHCP"

Vous trouverez votre adresse MAC en bas de la fenêtre.

L'adresseMAC sur MacOS 9

l'utilitaire "Informations système Apple" onglet "Profil système"
permettra de connaire l'adresse MAC de votre carte Airport.
Dérouler la rubrique "Informations réseau" puis" AppleTalk". L'adresse MAC de la carte réseau intégrée au système apparait en
clair à l'intitulé "Adresse".

L'adresseMAC sur Linux

Arpwatch entre autres pourra être utile. Davantage d'informations en suivant le lien :
http://letanou.linuxfr.org/arpwatch/arpwatch.html

Merci à Emmanuel Rihn pour ses compléments d'informations. Il cherche un travail dans les domaines de l'assistance technique systèmes et réseaux et du webmastering. Pour le contacter

Le chanel IRC sur mac : Nous vous suggérons de consulter ce how-to très bien fait.
Vous n'aurez qu'à remplacer les champs par les valeurs suivantes :

-Serveur : irc.action-irc.net
-Port : 6667
Surnom : Ce que vous voulez
Mot de passe : laisser vide

Ensuite, le channel IRC à joindre est le suivant :
Identifiant : projet_serveur_5-6

Voilà, c'est fini. Vous pouvez venir discuter Serveur.....

Le Chanel IRC sur PC : utiliser le logiciel MIRC

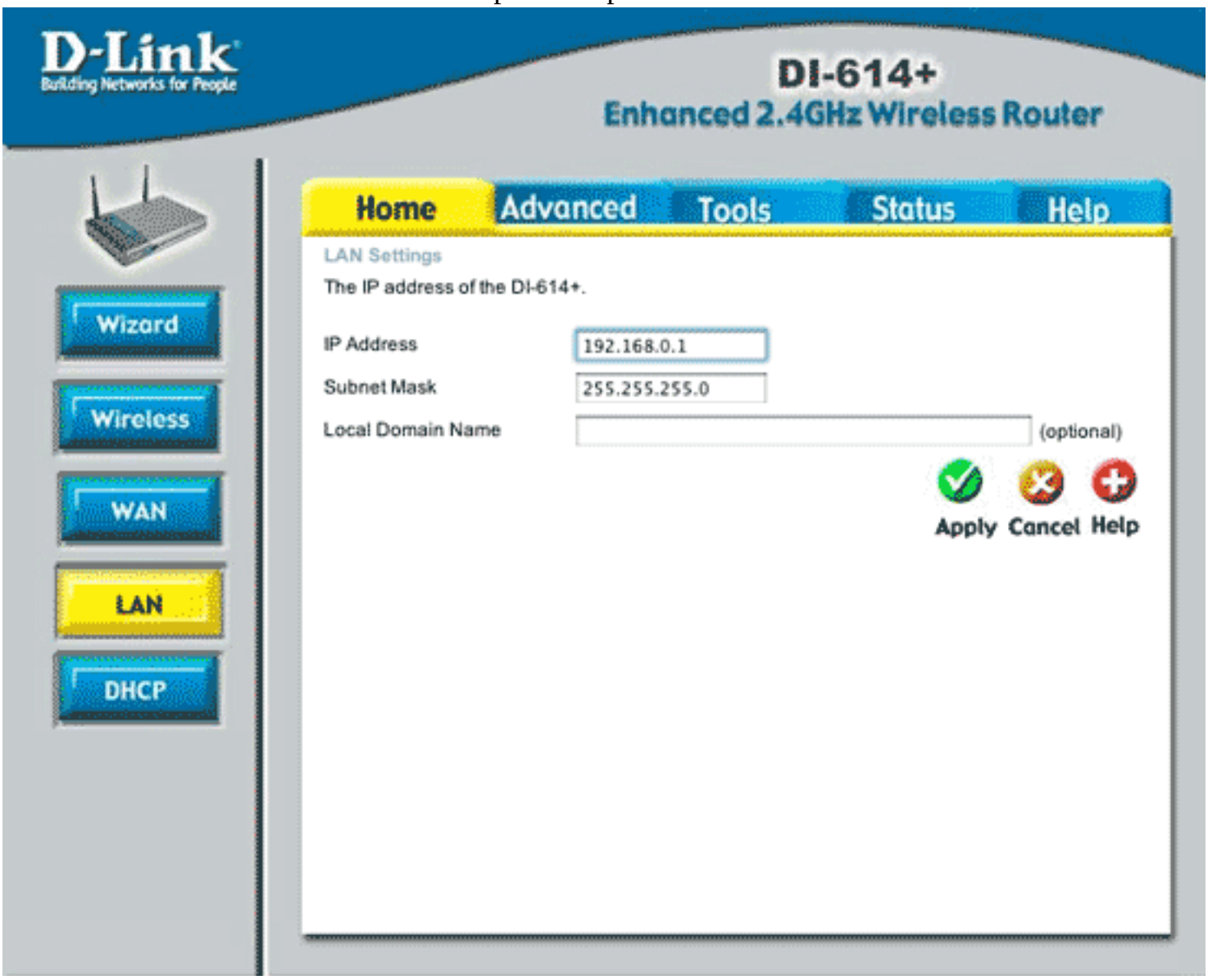
Le Channel IRC sur linux : utiliser le logiciel Xchat

Comment limiter l'usage de mon internet pour les clients ToileDeQuartier?

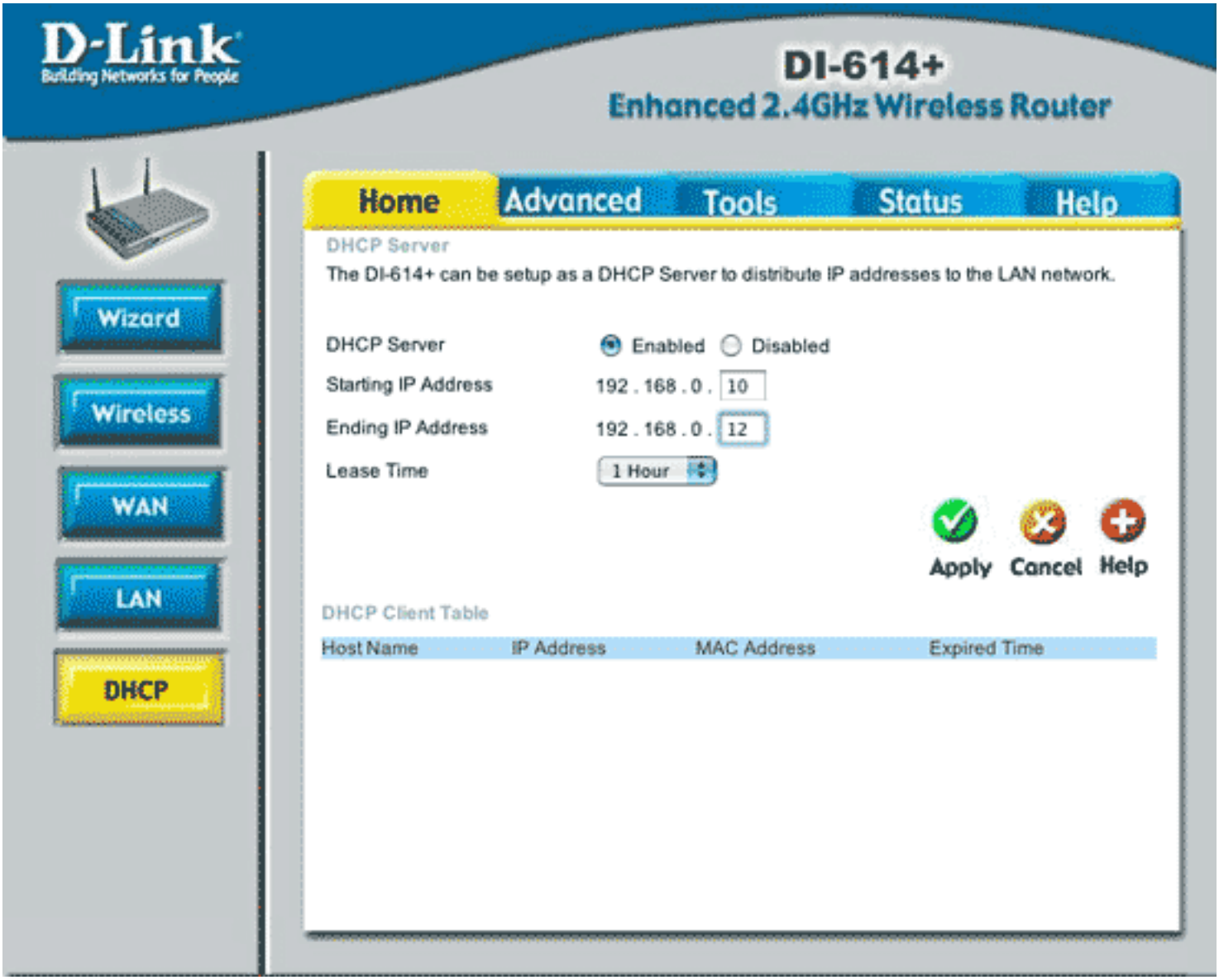
Plage d'IP en DHCP :

Tout d'abord, sur votre routeur, qu'il soit intégré à votre Modem ADSL, votre borne Wifi ou votre serveur, faire en sorte de définir une plage d'IP destinée au DHCP :

Si par exemple la classe d'IP de votre réseau est 192.168.xx.xx
Votre routeur a par exemple l'adresse 192.168.0.1



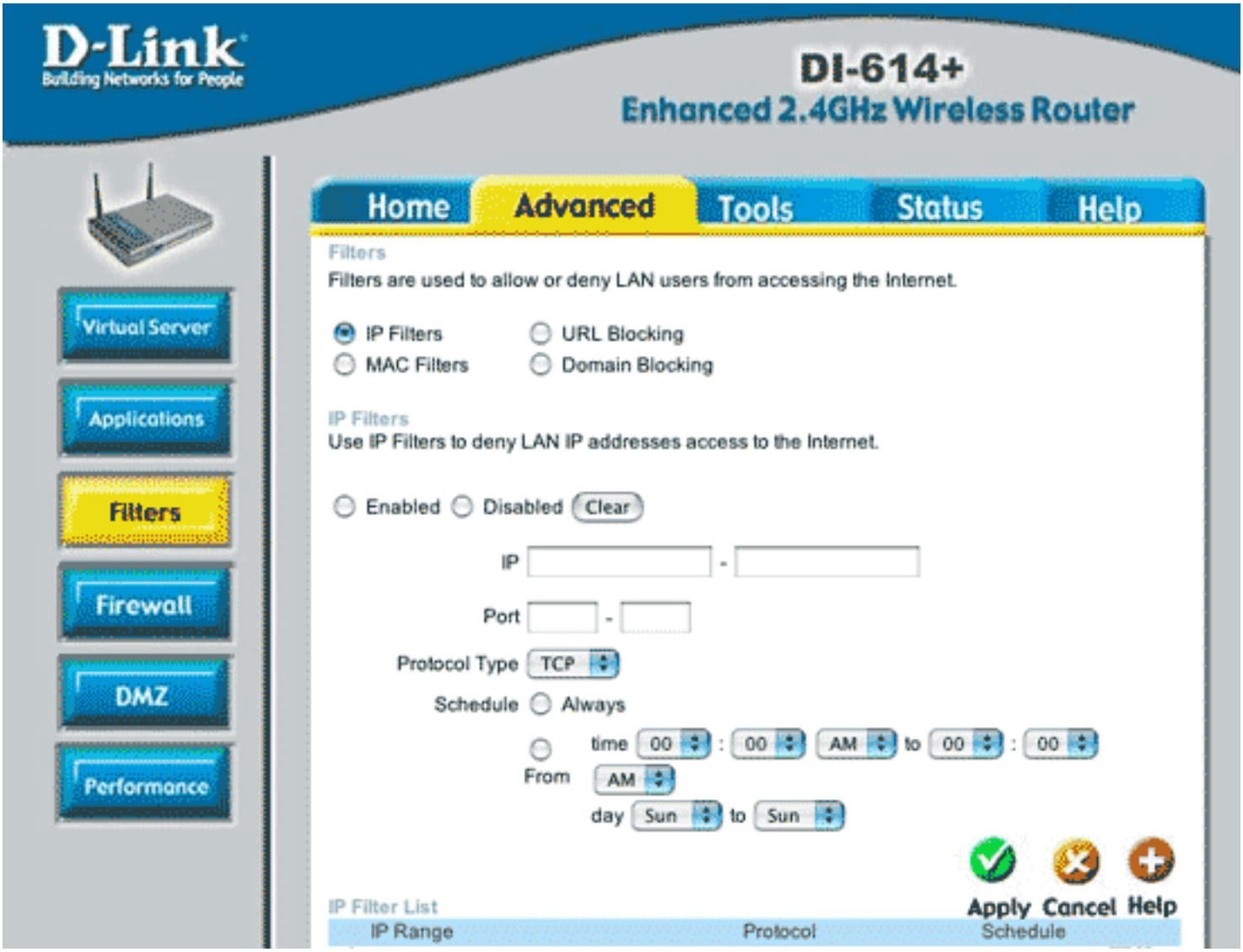
Votre réseau local (vos machines) auront les adresses 192.168.0.2, 192.168.0.3, 192.168.0.4, etc. Ainsi, vous pouvez définir une plage d'IP en DHCP (attribuée automatiquement à la machine qui se connecte) de 192.168.0.10 à 192.168.0.12 si vous ne voulez pas plus de 3 clients en même temps.



Afin de limiter leur temps de présence sur votre réseau, vous pouvez demander à ce que une adresse IP attribuée en DHCP ne le soit que pour un temps défini d'1 heure.

Voila, maintenant, vous pouvez définir des droits différents d'accès au web, pour votre réseau privé et pour les clients qui surfent depuis la rue.

Cela se passe sur le Firewall du routeur, ou sur l'onglet Filtrage IP de l'interface web du routeur.



Voici quelques règles permettant de limiter les abus de votre ligne ADSL et d'éviter l'engorgement.

Dans cet exemple, nous laisseront au client DHCP l'usage du web, du mail et du chat AIM.
Pas d'IRC, ni de Peer to Peer, telnet, etc...

Chacun de ces usages utilise un "port" spécifique. Il suffit donc de bloquer ou ouvrir un port.

Le Filtrage des ports en fonction des IP

Nous allons donc bloquer les ports indésirables pour les adresses IP 192.168.0.10 à 192.168.0.12

Bloquage du FTP et Telnet:
Deny --LAN,--192.168.0.10 -192.168.0.12 -- WAN,* -- TCP,20-23
On bloque donc la plage d'IP en DHCP vers le Web (Wan) toutes IP (*) protocole TCP ports 20 vers 23

Bloquage de tout après le port 1050 sauf AIM :
Deny --LAN,192.168.0.4-192.168.0.9 --WAN,* --IP (0),1050-5189
On bloque tout sauf AIM (port 5190) à partir du port 1050 jusqu'au port 5189

Deny --LAN,192.168.0.4-192.168.0.9 --WAN,* --IP (0),5191-65530
On bloque tout depuis le port suivant AIM (5191) jusqu'au port maximal possible.

On peut aussi faire un blocage plus précis en dessous du port 1050, mais attention à ne pas rendre le surf ou la connexion impossible.

Voici une liste des ports et de leur usage :

exempt http/https (Web)
Port 80

exempt ssh and telnet
22 et 23

exempt imap and smtp (le Mail -envoi)
143 et 25

exempt ftp directory listings
21

exempt aim (Ichat, chat AOL)
5190

exempt msn (MSN)
1863

exempt pop3 (Mail -réception)
110

exempt irc and sirc
6667 et 6668 et 9999

exempt hotline and carracho "listing" ports (client end)
5500 et 6700

exempt hotline and carracho "listing" ports (server end)
5500 et 6700

Il est à noter que ne sont pas listés ici les ports de services, ceux utilisés pour établir une connexion.
On se simplifiera donc la vie en constatant que tous les ports utilisés pour le Download sauvage se situent au dessus du port 1050.
Les ports de service se situent de manière générale au dessous de 1050.

Suite a pas mal d'expériences infructueuses de blocage de ports entre 1 et 24, 26 et 79, 79 à 109, 111 à 420, puis de 500 à 5189 et enfin de 5191 à 65335, j'en suis venu à simplifier et obtenir la configuration conseillée en amont.

Back

Back

Adresse IP :
Adresse délivrée à une machine serveur sous la forme w.x.y.z (w, x, y, z compris entre 0 et 255). L'adressage IP est le moyen de connaître, d'identifier et de localiser toute machine connectée à l'Internet. Plus largement sur les réseaux locaux de classe A, B ou C, les adresses IP permettent de faire communiquer les machines entre elles.

Adresse MAC : Adresse physique
C'est une adresse physique fixe unique dans le monde et qui identifie chaque carte réseau. Elle est composée d'une liste de code héxadécimaux.

ADSL : Asymmetric Digital Subscriber Line
Il s'agit d'utiliser la paire de fils de cuivre torsadée du téléphone pour y faire transiter des informations à haut débit. Pour plus d'info : MacADSL

Airport : Voir WiFi

Bande passante :
C'est le débit d'information qu'il est possible de faire transiter sur un support de transmission.

Bit : Binary Digit
Elément de base d'une donnée informatique prenant la valeur 0 ou 1. Il en faut 8 pour composer un octet.

Bps :
Bit par seconde, unité de mesure pour quantifier un flux d'information binaires. Aussi Kbps (Kilobit/seconde) et Mbps (mégabit/seconde).

Byte :
Voir octet.

DHCP : Dynamic Host Configuration Protocol
Protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Son principal but est de simplifier l'administration d'un réseau. Généralement le protocole DHCP, distribue des adresses IP, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol) qui est utilisé par exemple lorsque l'on installe une machine à travers un réseau (on peut effectivement configurer complètement un ordinateur, et c'est beaucoup plus rapide que de le faire à la main). Cette dernière possibilité est très intéressante pour la

maintenance de gros parcs-machines. Les versions actuelles des serveurs DHCP fonctionne pour IPv4 (adresses IP sur 4 octets). Une spécification pour IPv6 (adresses IP sur 16 octets) est en cours de développement par l'IETF.

DNS : Domain Name Server

Protocole Internet assurant la conversion entre les noms IP (par exemple www.macbidouille.com) et les numéros IP (212.43.222.205) des machines reliées à Internet. Ce système est basé sur l?organisation arborescente du système de nommage de machines utilisé sur Internet. Pour les fanas, dans le Terminal la commande 'nslookup ' permet de demander une traduction. Et pour ceux qui en veulent encore plus, la commande 'dig axfr' permet de voir l'ensemble du mécanisme de traduction...

DSLAM : Digital Subscriber Line Access Multiplexer

Le DSLAM est utilisé dans les liaisons ADSL. Il est l'interface entre le client et l'opérateur. Il est placé dans le central téléphonique, et fait la séparation entre le signal analogique (voix) et numérique (données). Il peut être Alcatel ou ECI.

Ethernet :

Technologie inventée par Xerox qui permet de relier deux ordinateurs via un cable RJ-45 ou (plus rarement) BNC pour les faire communiquer. C'est la base de la très grande majorité des réseaux actuels. Aujourd'hui, la vitesse atteinte par l'Ethernet est - en théorie - 1000 Mbps

Firewall : Pare-feu en Français.

Ensemble de règles de communications qui permettent de protéger une machine située sur un réseau. Un firewall peut être logiciel ou matériel.

Firmware :

Terme anglophone servant à désigner le microcode embarqué à bord de mémoires de type ROM et qui contient les instructions nécessaires au fonctionnement de l'appareil qui en est équipé.

Flasher : Mettre à jour une mémoire flash

La plupart des périphériques possèdent une mémoire contenant les données qui permettent à l'ordinateur de les identifier et de dialoguer avec eux. Certaines de ces mémoires, dite mémoires flashs, ou firmware, ou bios, peuvent être mise à jour avec des micro-programmes adéquat. L'action de flasher consiste à exécuter cette mise à jour.

Gbits :

Gigabits = 1024 mégabits.

Gif : Graphics Interchange Format

Format graphique répandu sur internet du fait de la faible taille des fichiers qu'il génère. Il est limité à 256 couleurs.

Hacker :
Un hacker est une personne très douée pour l'informatique et la programmation en particulier. Le mot a pris la conotation de "pirate informatique" car ces derniers se sont souvent introduits dans des systèmes "pour le sport" mais sans intention malveillante (à la différence des Crackeurs), mettant souvent, au passage, en lumière les faiblesses de sécurité qui pouvaient exister au sein des sus-dits systèmes.

HTML : HyperText Markup Language
Système de codage permettant de construire des pages destinées à être consultés sur Internet.

HTTP : HyperText Transfert Protocol
Protocole de transfert de données utilisé pour les pages internet principalement, mais aussi pour le téléchargement de certains fichiers.

Hub ethernet :
Un hub ethernet est un petit boitier muni de ports ethernet qui permet de relier physiquement plusieurs ordinateurs dans le but de les mettre en réseau. Un hub ethernet est souvent alimenté par sa propre alimentaion externe pour pouvoir amplifier le signal et ainsi faire transiter les informations sur de longues distances (100 mètres au maximum). A la différence d'un switch, un hub partage le flux de données entre tous les ordinateurs qui lui sont ratachés.

Internet : Réseau public mondial
Réseau mondial basé sur une architecture ouverte constituée d'un ensemble de protocoles pour interconnecter entre-eux plusieurs réseaux (machines idividuelles, réseaux domestiques, réseau locaux, réseaux nationaux....) même s'ils sont totalement hétérogènes. Internet s'appuie notamment sur le protocole IP (Internet Protocole) mais aussi les protocoles TCP, UDP, ICMP, ARP, RARP, DNS, RIP, ainsi qu'un ensemble de protocoles applicatifs permettant notamment l'utilisation de la messagerie electronique et du web: SMTP, POP3, IMAP, HTTP, FTP, TFTP, TELNET, SSH, BOOTP, DHCP...

IPv6 : Internet Protocol, version 6 (actuellement on utilise la version 4)
Prochain standard pour la transmission de données et d'information sur internet. Actuellement une adresse IP est codée sur 32 bits, alors qu'une adresse IPv6 le sera sur 128 bits. Les ameliorations sont importantes: meilleur gestion de la securitée, facilitée d'installation de reseau (plus besoin de DHCP, l'adresse IPv6 peut etre determinée grace a l'adresse MAC), protocole de decouverte du plus petit MTU, pour eviter la frgmentation des paquets... La principale raison du passage a IPv6 est le manque d'adresse IPv4, qui a mené dans un premier temps au recours au NAT.

IRC : Internet Relay Chat
Outil de communication en temps réel.C'est un protocole de communication permettant à des utilisateurs de discuter par écrit et en temps réel sur Internet.

ISP : Internet Serices Provider
Fournisseur d'accès Internet (FAI). Les FAI sont les sociétés qui vous permettent de vous connecter à

Internet.

JPEG : Joint Photographic Expert Group
Norme définissant un mode de compression destructif appliqué aux images.

Kbits :
Kilobits = 1024 bits

Kernel :
Voir noyau.

Kernel Panic : Plantage du noyau.
Le noyau étant le coeur du système, celui-ci ne peut continuer à fonctionner. C'est l'erreur la plus grave pouvant survenir, entraînant l'obligation de redémarrer la machine. Cette erreur survient essentiellement suite à un problème hardware, ou lors de l'utilisation d'extensions noyau douteuses (fichiers .kext : Kernel Extension).

Ko :
Kilo octet = 1024 octets

LAN : Local Area Network
Désigne un réseau dont l'échelle est locale. Par exemple un réseau d'entreprise au niveau d'un unique bâtiment.

Liaison asynchrone :
Mode de transmission ne necessitant pas d'étape de synchronisation dans l'établissement d'une communication.

Liaison synchrone :
Mode de transmission où les données envoyées sont séparées par un intervalle de temps constant fixé par un système de synchronisation tel qu'un signal d'horloge.

LOL : Abréviation de chat
(Anglais) Laughing Out Loudly
Ce qui veut dire : "Rire à pleine gorge tout fort".
Se traduit en Français par MDR.

MacOS : Système d'exploitation des micro-ordinateurs Apple Macintosh.
Système d'exploitation des micro-ordinateurs Apple Macintosh. Celui-ci a connu un tournant avec l'apparition de la version X (MacOS 10) architecturé autour d'un Unix BSD, rompant avec les anciennes générations de systèmes (essentiellement Système 6 et MacOS 7,8,9) qui n'étaient pas des Unix et avaient atteints avec la version 9 des limites technologiques réelles en termes de performances et de

fiabilité.

Mail : Courrier électronique
Désigne le courrier électronique, mais aussi l'application Apple Mail livrée en standard sous Mac OS X pour la gestion du courrier électronique.

Mappage : Action de mapper un port
Mapper un port est l'action de configurer un routeur pour qu'une requête externe sur un port donné soit rediriger vers une adresse IP et un port particulier. Par exemple, configurer son routeur pour que les requêtes qui arrivent sur le port 80 soient redirigées vers l'IP 192.168.1.2 port 80, et que les requêtes qui arrivent sur le port 81 soient redirigées vers l'IP 192.168.1.3 port 80.

MTU : Minimum Transfer Unit
C'est la taille maximale d'un paquet que peut transmettre une interface réseau donnée. Par exemple, pour Ethernet, c'est 1500 octets, pour PPPoE c'est 1492... Si un paquet exède la taille du MTU, la station qui l'envoie devra le fragmenter.

NAT : Network Adress Translation
Protocole utilisé pour creer des sous reseau a partir d'un reseau principal. Du point de vue de l'exterieur, toutes les machines du sous reseau ont l'adresse IP de la machine qui effectue le NAT. A l'interieur du sous reseau, chaque machine a une adresse IP propre. La machine qui effectue le NAT est un routeur, et elle posede 2 adresse IP: une interne et une externe. Ce procedé a ete developpé a cause du manque d'adresses IP.

Octet :
Donnée informatique représentant 8 bits de données.

Open Source :
La base d'un programme, la façon dont il est écrit, son code est appelé source. Le fait que ce source soit ouvert veut dire qu'il est (généralement) fournit avec le programme compilé ou disponible gratuitement. De ce fait tout le monde peut ajouter, modifier, ou emprunter du code source pour son besoin personnel ou celui de la comunauté.

OS : Operating System
Voir Système d'exploitation.

Paquet :
C'est la plus petite unitée d'information pouvant etre envoyé sur un réseau. Un paquet IP par exemple contient de l'information, et aussi un en tête spécifiant des information relatives au contenu, au routage, et à la securitée. Un paquet peut faire de quelques octets à plusieurs kilo-octets.

Ping : Temps en millisecondes que mettent les données pour aller d'une machine à une autre sur un

réseau.

Un ping est caractérisé par une trame (un paquet contenant en général que très peu de données, en général une suite de caractères) qui est envoyée d'un ordinateur vers un autre ordinateur (c'est à dire à une certaine IP) pour que le second renvoie le paquet au premier. Si les données envoyées sont identiques à celles retournées, la connexion est bonne. Le ping se mesure en millisecondes, c'est le temps que le paquet a mis pour être retourné à l'envoyeur. Ainsi un ping de 500ms signifie que l'information a mise 500ms pour faire un aller et retour entre les deux IP. Historique : le mot ping vient des premier prototypes de sonars lors de la guerre mondiale. L'ASDIC (qui était le premier protype) faisait le bruit : Ping, Ping, Ping?

Pixel : De l'anglais PICcture ELement.

Point lumineux bicolore (écran noir et blanc) ou multicolore (écran couleur) constituant l'élment de base de l'image affichée par un moniteur informatique. La définition d'un écran est caractérisée par le nombre de pixels affichés en largeur et en hauteur (exemple : 1024x780).

Plug'n Play : Plug And Play

Technologie qui permet à un péripherique de s'identifier lui même à l'ordinateur. Le périphérique contient dans une petite mémoire l'information à envoyer à l'ordinateur, après une requête, pour se faire connaître. L'ordinateur peut ensuite charger automatiquement le driver nécessaire et configurer le périphérique. Concrètement, c'est ce qui fais qu'en branchant une souris USB elle marche tout de suite, par exemple. Ce terme a été popularisé par Microsoft à la sortie de son système Windows 95 (à l'époque, le fonctionnement aléatoire avait amené certaines personnes à employer plutôt le terme de "Plug'n Pray").

PPP : Point to Point Protocole

PPP est le protocole standard de transmission des paquets IP sur une ligne serie, vous le retrouvez en gros pour établir votre accés internet via un modem classique et une ligne téléphone.

PPPoA : Point to Point Protocole over ATM

protocole point à point sur ATM. Protocole qui permet de faire transiter des données sur un réseau de type ATM tout en authentifiant son utilisateur.

PPPoE : Point to Point Protocole over Ethernet

protocole point à point sur ethernet. Protocole qui permet de faire transiter des données sur un réseau de type ethernet tout en authentifiant son utilisateur. Un standard actuel pour l'ADSL.

PPTP : Point to Point Tunneling Protocole

Protocole Point à Point en Tunnel. C'est aussi un protocole qui permet de faire transiter des données en authentifiant ses utilisateurs. Il appartient à Microsoft et se veut sécurisé car encapsulant une fois de plus les données (il les fait transiter dans un tunnel en quelque sorte). Hélas ses failles de sécurité sont déjà connues.

RJ-45 : Voir Ethernet

Routeur :
Un routeur est un boitier autonome qui permet de partager une connexion réseau. Un routeur peut donc partager votre liaison internet : il sera placé entre votre modem et vos ordinateurs ; il se chargera d'assurer la connexion Internet et de la distribuer aux ordinateurs de votre réseau local.

RTFM : Read The Fucking Manual
Terme issue du language "Geek", pour signifier à une personne posant une question (souvent évidente ou déjà abordée) de se réferer à la documentation existante sur la question.

SMTP : Protocole de transfert de mail
Ce protocole s'occupe de l'acheminement de vos messages mails à travers le réseau.

Socket (au sens logiciel) :
Interface abstraite de communication sur réseau IP d'une machine. Elle est composée d'une adresse IP et d'un numéro de port. Ce numero de port est compris entre 1 et 65535. Les 1024 premiers sont réservés pour des applications connues (les "Well-known services) dont la liste est disponible dans le fichier '/etc/services' de la plupart des systèmes Unix.

Spam :
Désigne les messages electroniques, souvent commerciaux, non désirés.

Système d'exploitation :
Programme informatique s'éxécutant dès le démarrage d'un ordinateur et qui ne s'arrête que lorsque vous éteignez ce dernier. C'est le programme fondamental permettant de gérer l'ensemble des ressources matérielles (écran, processeur, clavier, disque dur, souris, carte réseau...etc etc) et de les distribuer correctement aux autres programmes informatiques.

TAR : Unix Tape ARchive
C'est le format d'archivage employé par les systèmes Unix et dérivés. Il doit son nom au support qui fut longtemps utilisé pour enregistrer de telles archives : la bande magnétique.

TCP/IP : Transmission Control Protocol/Internet Protocol
Ensemble des protocoles utilisés par Internet.

Trojan :
Un trojan est un programme dissimulé dans un autre et qui exécute des commandes sournoises. Il donne généralement un accès à la machine sur laquelle il est installé.

UDP : User Datagram Protocol
Ce prococole sur internet permet à une application d'envoyer un paquet d'information (datagram) à une

autre application mais avec le minimum d'efforts et de moyens, mais contrairement à TCP la délivrance de l'information n'est pas garantie.

Unix : Famille de systèmes d'exploitation
Famille de systèmes d'exploitation dont les principales caractéristiques sont: - multi-tâches préemptif - multi-utilisateurs - mémoire protégée - un ensemble de fonctions en langage C de bas niveau: les primitives systèmes. - ... On distingue quelques grandes sous-familles parmi lesquelles: HP-UX (Hewlet Packard), BSD (Berkeley Software Distribution, MacOS X fait partie de cette famille), Linux (contenant le célèbre noyau de Linus Torvalds), Solaris (Sun Microsystems)...

USB : Universal serial Bus
Bus de communication série pour les périphériques lents (claviers, souris, scanner, imprimante, etc) Il supporte jusqu'a 127 pérphérique et est auto-alimenté (pour les périphériques ne consommant pas beacoup de courant)

WAN : World Area Network
Réseau dont l'infrastructure s'étend sur tout ou partie de la planète. Le téléphone et Internet sont les plus connus de ces réseaux.

WiFi : Norme de communication sans-fils
Nom générique des normes 802.11x, permet la communication en Ethernet sans fils en utilisant une fréquence de 2,4gHz (802.11b alias AirPort et 802.11g alias AirPort Extrème) ou 5gHz (802.11a - incompatible avec les 2 autres)

XML : eXtensible Markup Language
Format de fichier standard pour les échanges de données. Des scripts peuvent être appliqués a ces fichiers pour les afficher sous forme de page internet par exemple. C'est notament le format retenu pour les fichiers de préferences sous mac OS X (.plist).

ZIP : Format de compression
Compression non destructive d'un fichier ou d'un dossier, largement employé sur PC, le plus proche cousin serait peut-être sur MAC le format binhex (.hqx).

Back

Formulaire à remplis par les personnes souhaitant se connecter au réseau ToileDeQuartier5-6.

Merci de vérifier que l'encodage texte par défaut de votre naviguateur soit bien sur Occidental (Mac OS roman) sur safari

Ces renseignements seront fournis aux propriétaires de point d'accés wifi qui vous permettent de surfer sur le net. Ils sont confidentiels.

***Nom** ***Prénom**

Code postal ***N° de tel valide**

***E-mail valide**

***Adresse MAC**

(identité de votre carte réseauWifi.) **comment la trouver ?**

Activité

Commentaires

Reset

Envoyer le formulaire

*Indispensable