

PROXY - ROUTEUR - NAT - FILTRE

LE PROTOCOLE TCP-IP & INTERNET

MISE EN PLACE D'UN RESEAU (Rappel)

MISE EN PLACE D'UN PROXY

MISE EN PLACE D'UN ROUTEUR NAT PC + SOFT

MISE EN PLACE D'UN ROUTEUR AUTONOME

ACCELERATION DE LA CONNEXION A INTERNET

LE PROTOCOLE TCP-IP & INTERNET

1. *Introduction*
 2. *Le protocole IP*
 3. *L'adresse IP*
 4. *Les différents types de réseaux*
 5. *La subdivision en sous-réseaux*
 6. *Le routage des paquets IP et le protocole TCP*
 7. *Le système de désignation de noms (DNS)*
 8. *Résumé et exemples*
-

1. Introduction

Quelques mots d'abord sur le protocole TCP-IP.

TCP-IP est un ensemble de logiciels développés au fil des années (à partir des années 70 déjà) qui constituent un "langage universel" de communication informatique à travers le monde. Le protocole devait posséder les qualités suivantes :

- une bonne reprise après panne
- la capacité à gérer un taux élevé d'erreurs
- une faible surcharge des données
- la capacité de se prolonger sans difficultés dans des sous-réseaux
- l'indépendance par rapport à un fournisseur particulier ou un type de réseau

A partir du 1er janvier 1983, seuls les paquets TCP-IP ont été transmis sur le réseau Arpanet (précurseur d'Internet). 1983 est donc en quelque sorte l'année de naissance d'Internet.

Il faut encore rajouter que TCP-IP se compose de deux protocoles distincts, IP et TCP, dont j'explique plus loin les rôles respectifs.

2. Le protocole IP

Le Protocole Internet ou **IP (Internet Protocol)** est la partie la plus fondamentale d'Internet. Si vous voulez envoyer des données sur Internet, vous devez les "emballer" dans un **paquet IP**. Je parlerai plus loin (voir la partie accélération de votre connexion à Internet) de ces paquets IP. Il faut savoir pour l'instant que ces derniers ne doivent pas être trop gros; la plupart du temps, ils ne peuvent pas contenir toute l'information qu'on voudrait envoyer sur Internet, et cette dernière doit par conséquent être fractionnée en de nombreux paquets IP.

Les paquets IP, outre l'information, sont constitués d'un en-tête contenant l'adresse IP de l'expéditeur (votre ordinateur) et celle du destinataire (l'ordinateur que vous voulez atteindre), ainsi qu'un nombre de contrôle déterminé par l'information emballée dans le paquet : ce nombre de contrôle, communément appelé *en-tête de total de contrôle*, permet au destinataire de savoir si le paquet IP a été "abîmé" pendant son transport.

3. L'adresse IP

Une des choses les plus étonnantes du protocole TCP-IP est d'avoir attribué un numéro fixe, comme un numéro de téléphone, à chaque ordinateur connecté sur Internet; ce numéro est appelé l'**adresse IP**. Dans le cadre du standard actuel - IPv4 -, les adresses sont codées sur 32 bits. Ainsi, tout ordinateur sur Internet, par exemple le vôtre lorsque vous vous connectez par l'entremise de votre Provider, se voit attribuer une adresse de type a.b.c.d (où a.b.c.d sont des nombres compris entre 0 et 255), par exemple 202.15.170.1. Dès ce moment, vous êtes le seul au monde à posséder ce numéro, et vous y êtes en principe directement atteignable.

Un rapide calcul vous montre qu'il y a, en théorie, un maximum de $256^4 = 4'294'967'296$ adresses possibles, ou, en d'autres termes, d'ordinateurs directement connectables, ce qui est plus que suffisant même à l'échelle mondiale (du moins à l'heure actuelle !). En fait, il y a *beaucoup* moins d'adresses que ce nombre impressionnant, car de nombreux numéros IP ne sont pas autorisés ou sont utilisés à des fins "techniques".

Pour l'ordinateur, cette adresse IP est codée en binaire ($4 \times 8 \text{ bits} = 32 \text{ bits}$).

Par exemple,

202	15	170	1
11001010	00001111	10101010	00000001

Il est plus facile de retenir **202.15.170.1** que **11001010000011111010101000000001** !

4. Les différents types de réseaux

L'adressage a été structuré logiquement dans une architecture de réseaux et de sous-réseaux. N'importe qui ne peut s'approprier librement une adresse IP : ces dernières sont régies par un organisme international, l'INTERNIC, qui délivre les différentes adresses ou plutôt les classes de réseaux.

- **Dans un réseau de classe A**, le NIC fixe les 8 premiers bits (dits bits de poids fort) sous la forme 0xxxxxxx; les 24 autres bits sont laissés à l'administration de l'acquéreur du réseau de classe A. Dans un tel réseau, les adresses IP sont donc de type F.b.c.d où F (fixé par le NIC) va de 0 à 126, les valeurs b, c et d étant laissées librement administrables par l'acquéreur. De grandes sociétés ont ce type de réseau; par exemple, Hewlett-Packard possède le réseau 16.b.c.d (qu'on note aussi 16.0.0.0). Vous noterez que seuls 127 réseaux de ce type sont disponibles.
- **Dans un réseau de classe B**, le NIC fixe les 16 premiers bits sous la forme 0xxxxxxx yyyyyyyy, ce qui donne des réseaux de type F.G.0.0 où F (128-191) et G (0 à 255) sont fixés par le NIC.
- **Dans un réseau de classe C**, le NIC fixe les 24 premiers bits sous la forme 110xxxxx yyyyyyyy zzzzzzzz, ce qui donne des réseaux de type F.G.H.0 où F (192-223), G et H (0-255) sont fixés par le NIC.
- Tout le réseau 127.0.0.0 (qu'on peut voir comme un réseau de classe A) n'est pas attribué par le NIC, car l'adresse 127.0.0.1, dite *adresse de boucle*, est réservée à des fins techniques. Dommage, car 24 millions d'adresses sont ainsi perdues !
- De plus, le NIC n'attribue pas non plus certains réseaux qui sont laissés à des fins privées. Ces plages d'adresses généralement non routées par les fournisseurs d'accès, en d'autres termes des plages attribuables tout à fait légalement pour des réseaux internes, vont
de 10.0.0.0 à 10.255.255.255
de 172.16.0.0 à 172.31.255.255
de 192.168.0.0 à 192.168.255.255
 Typiquement, si vous créez votre propre réseau local en TCP-IP, vous utiliserez pour vos ordinateurs ce type d'adresses. Je reparle de ce cas dans la partie sur la façon de configurer un réseau local et le connecter à Internet.

Il me faut encore rajouter que **certaines adresses d'un réseau quelconque ne sont pas attribuables** à un ordinateur précis, mais joue un rôle "technique" dans TCP-IP.

Prenons l'exemple d'un réseau de classe C comme 192.168.0.x, x pouvant varier entre 0 et 255.

Cette plage d'adresses doit être indiquée de manière officielle, et on utilise pour cela **l'adresse générale 192.168.0.0**, ce qui veut dire "toutes les adresses comprises entre 192.168.0.0 et 192.168.0.255". Remarquez que cela signifie que vous ne pourrez jamais attribuer l'adresse 192.168.0.0 à un ordinateur précis, puisque cette dernière fait référence à tout le réseau.

Il existe une autre adresse IP réservée : *l'adresse de diffusion (broadcast)*. C'est la dernière adresse du sous-réseau, dans notre cas 192.168.0.255. Il s'agit de l'adresse que vous utilisez pour diffuser un message vers chaque ordinateur du sous-réseau concerné.

Finalement, ce qui sera l'objet du paragraphe 6, vous devez réserver une *adresse IP du routeur par défaut* : c'est l'adresse "passerelle" qui permettra à des paquets IP de "quitter" votre sous-réseau.

5. La subdivision en sous-réseaux

Comment un ordinateur transmet-il l'information (les paquets IP) à son destinataire ? Une partie de la réponse se trouve dans le fonctionnement du protocole IP.

Généralement, un ordinateur ne peut transmettre directement un paquet IP qu'à un ordinateur situé sur le même sous-réseau. Par exemple, un ordinateur possédant l'adresse IP 192.168.0.2 pourra directement envoyer de l'information à un ordinateur "voisin" d'adresse 192.168.0.20, mais il ne pourra pas le faire avec un ordinateur d'adresse 194.38.175.55. Pour simplifier, on dira en première approche qu'un ordinateur ne peut communiquer directement qu'avec un ordinateur possédant les trois premiers nombres de l'adresse IP identiques. Cette remarque n'est malheureusement pas théoriquement juste (même si en pratique, c'est assez souvent le cas pour des réseaux simples). En fait, c'est le concept de **masque de sous-réseau** qui définit ce qu'un ordinateur peut "voir" ou ne pas voir.

Le masque de sous-réseau que vous avez peut-être eu l'occasion d'utiliser, si vous utilisez TCP-IP pour un réseau local, est 255.255.255.0. Ce masque veut dire que l'ordinateur concerné peut "voir" (ou communiquer avec) tous les ordinateurs possédant les trois premiers nombres de l'adresse IP identiques, comme je l'ai indiqué à l'exemple précédent. Comment fonctionne ce système à première vue aussi compliqué ?

En fait, admettons que l'ordinateur A d'adresse IP 199.34.57.10 veuille envoyer un paquet IP à l'ordinateur B d'adresse IP 199.34.57.20. A priori, A ne sait pas s'il peut communiquer directement avec B. Pour cela, il utilise le masque de sous-réseau 255.255.255.0 qu'on lui a imposé. Il "convertit" le tout en binaire, ce qui donne :

11111111	11111111	11111111	00000000	masque sous-réseau
11000111	00100010	00111001	00001010	adresse de A
11000111	00100010	00111001	00010100	adresse de B

L'ordinateur A doit s'assurer que partout où le masque de sous-réseau a une valeur de 1, la valeur binaire de son adresse IP corresponde à celle de B. Dans l'exemple ci-dessus, il n'est pas difficile de voir que c'est le cas; finalement, les 8 derniers bits de valeur 0 indiquent que le dernier nombre de l'adresse IP est indifférent pour A : ce dernier verra donc tous les ordinateurs d'adresse 199.34.57.x, x étant compris entre 0 et 255.

Cet exemple paraît trivial, pourtant de nombreux réseaux comportent des masques de sous-réseaux moins compréhensibles (pas uniquement des 0 et des 255), comme par exemple 255.255.255.224. Si vous refaites le même raisonnement, vous verrez qu'avec un tel masque, l'ordinateur 192.168.0.2 ne peut directement communiquer avec l'ordinateur 192.168.0.100 ! En fait, les 256 adresses de ce réseau de classe C seront comme subdivisées en 8 sous-réseaux de 32 ordinateurs.

Ainsi, les ordinateurs 192.168.0.0 à 192.168.0.31 pourront communiquer entre eux, de mêmes que :

les ordinateurs 192.168.0.32 à 192.168.0.63,
 les ordinateurs 192.168.0.64 à 192.168.0.95,
 les ordinateurs 192.168.0.96 à 192.168.0.127,
 les ordinateurs 192.168.0.128 à 192.168.0.159,
 les ordinateurs 192.168.0.160 à 192.168.0.191,
 les ordinateurs 192.168.0.192 à 192.168.0.223,
 et les ordinateurs 192.168.0.224 à 192.168.0.255,

mais ces sous-réseaux ne pourront pas communiquer directement entre eux.

Cette subdivision d'un réseau de classe C en plusieurs sous-réseaux peut être utile pour un fournisseur d'accès. Vous pouvez calculer aisément les masques de sous-réseaux suivants selon le nombre de sous-réseaux que vous souhaitez créer.

nombre de sous-réseaux	IP par sous-réseau	masque de sous-réseau
1	256	255.255.255.000
2	128	255.255.255.128
4	64	255.255.255.192
8	32	255.255.255.224
16	16	255.255.255.240
32	8	255.255.255.248

En fait, nous avons vu au paragraphe précédent que pour chaque sous-réseau **il faut déduire trois adresses IP non attribuables à un ordinateur** :

1. **l'adresse de sous-réseau** (généralement le premier IP du sous-réseau), par exemple a.b.c.0 pour un réseau composé d'un seul sous-réseau, ou a.b.c.64 pour le troisième sous-réseau d'un réseau divisé en 8 sous-réseaux.
2. **l'adresse de diffusion** (généralement le dernier IP du sous-réseau), par exemple, en reprenant les deux exemples précédents, a.b.c.255 ou a.b.c.95.
3. **l'adresse du routeur** par défaut dont je parle un peu plus loin, par exemple a.b.c.1 ou a.b.c.65.

Chaque sous-réseau "perd" donc trois adresses IP; il s'ensuit qu'une subdivision excessive d'un réseau n'est pas avantageuse (on divise rarement au-delà de 8 sous-réseaux).

6. Le routage des paquets IP et le protocole TCP

Revenons à notre ordinateur A d'adresse 192.168.0.2 (mettons-lui un masque de sous-réseau de 255.255.255.0). Admettons qu'il veuille envoyer un paquet IP à ordinateur B d'adresse 192.170.0.4. En utilisant le masque de sous-réseau, A comprend qu'il ne peut atteindre directement B. Que fait-il donc ? Il envoie sans réfléchir le paquet IP à l'adresse du routeur par défaut (disons que ce dernier a été défini comme 192.168.0.254).

Qu'est-ce que ce *routeur* ? Le routeur est une machine pouvant "jouer sur plusieurs sous-réseaux" en même temps. Typiquement, si on utilise un ordinateur, ce dernier possédera deux cartes réseaux, l'une connectée sur l'un des sous-réseaux (dans notre cas, disons qu'elle possède l'adresse 192.168.0.254), l'autre connectée sur l'autre sous-réseau (disons 192.170.0.192). S'il utilise le bon logiciel, un tel ordinateur est capable de faire transiter des paquets IP du réseau 192.168.0.0 vers le réseau 192.170.0.0, et inversement bien sûr.

Deux petites remarques s'imposent. Tout d'abord, vous l'aurez compris, c'est donc grâce à des routeurs que différents sous-réseaux d'un réseau de classe C peuvent communiquer entre eux, par exemple l'ordinateur 192.168.0.2 avec l'ordinateur 192.168.0.120 d'un réseau de classe C subdivisé en 8 sous-réseaux (masque de sous réseau 255.255.255.224). La seconde remarque est d'ordre plus pratique : vous retiendrez que Windows 95 n'est pas capable de faire du routage, bien qu'il soit tout à fait possible d'installer deux cartes réseaux (avec des IP différents) dans un ordinateur tournant sous ce système; par contre, Windows NT 4.0, même en version Workstation, est capable d'une telle fonction.

Question pertinente : pourquoi subdiviser et ne pas faire de "méga" réseaux ?

Les deux points suivants expliquent en partie pourquoi on procède ainsi.

1. Limiter le trafic sur un tronçon donné. Imaginons deux réseaux locaux A et B séparés par un routeur. Lorsque des ordinateurs de A discutent avec des ordinateurs de B, le routeur a pour rôle de transmettre l'information du réseau A vers le réseau B (et inversement). Par contre, si des ordinateurs de A s'échangent entre eux des données, il n'y a pas de raison qu'ils encombrant inutilement le trafic sur le réseau B, et c'est bien pour cette raison que les réseaux A et B sont distincts.
Autre évidence : si le réseau A tombe en panne, le réseau B n'en est pas affecté. C'est d'ailleurs l'avantage principal de subdiviser : éviter qu'un ennui technique qui pourrait rester localisé ne perturbe la totalité du réseau
2. Autre aspect non négligeable : le **broadcast** (diffusion). Vous ne le savez peut-être pas, mais dans votre dos, les ordinateurs sont de grands bavards : ils ne cessent de causer entre eux pour signaler leur présence ou se mettre d'accord sur les protocoles qu'ils sont capables de comprendre. Pensez un peu si Internet n'était constitué que d'un seul segment : le broadcast seul des ordinateurs utiliserait l'intégralité de la bande passante avant même qu'un seul octet de données ait pu être transmis ! Pour cette raison, le travail des routeurs est non seulement de faire transiter les paquets IP, mais aussi de **filtrer** le broadcast local qui n'intéresse pas la planète entière. Vous comprendrez par là que les routeurs jouent un rôle essentiel pour éviter la saturation du trafic.

Disons encore quelques mots sur l'acheminement des paquets IP. Vous comprenez maintenant que lorsqu'un ordinateur doit acheminer un paquet IP, il vérifie tout d'abord s'il peut le transmettre directement (grâce au masque de sous-réseau); s'il ne peut pas, il l'envoie bêtement, sans réfléchir, au routeur par défaut. Et ainsi de suite, le routeur regarde s'il peut transmettre directement le paquet à son destinataire (n'oublions pas que le paquet IP contient les adresses IP de l'expéditeur et du destinataire !), et, s'il ne peut le faire, le transmet à son routeur par défaut, etc.

Or le protocole IP néglige un point crucial : il ne vérifie nullement le bon acheminement des paquets IP. En d'autres termes, l'ordinateur expéditeur, dans le protocole IP, ne fait qu'envoyer le paquet IP plus loin; il ne s'intéresse pas du tout de savoir si le paquet a bien été reçu ou s'il a été endommagé pendant le transfert !

Qui doit donc assurer l'intégrité point à point, si ce n'est IP ? La réponse : son copain, TCP.

Le protocole de contrôle de transmission ou **TCP (Transmission Control Protocol)** vérifie donc le bon acheminement d'un paquet IP. Cela se fait de la façon suivante. Admettons que A veuille transmettre un paquet IP à B (connexion "directe"). A envoie (un peu à l'aveugle) son paquet IP à B, un peu comme une bouteille à la mer. Tant que A ne recevra pas un accusé de réception de B lui indiquant que ce dernier a bien reçu le paquet IP dans son intégrité (grâce à l'en-tête de contrôle), il renverra à intervalles réguliers le même paquet IP à B. Il n'arrêtera d'envoyer ce paquet qu'à la confirmation de B. Ce dernier agira ensuite de même s'il doit transmettre le paquet plus loin. Si B constate que le paquet qu'il a reçu est abîmé, il n'enverra pas de confirmation, de manière à ce que A lui renvoie un paquet "neuf".

TCP fournit d'autres services sur lequel je ne m'attarderai pas ici.

On résumera rapidement les principales fonctionnalités du protocole TCP ainsi :

- l'établissement d'une liaison
- le séquençement des paquets
- le contrôle de flux
- la gestion d'erreurs
- le message d'établissement d'une liaison

On entend par "contrôle de flux" la capacité de TCP, entre autres, de reconstituer l'information originale à partir de paquets IP arrivés (souvent) dans le désordre le plus absolu.

C'est aussi TCP qui gère la notion de "sockets" (ports d'écoute) dont je parle dans la partie concernant la façon de configurer un réseau local et le connecter à Internet.

7. *Le système de désignation de noms (DNS)*

Maintenant que vous avez compris (j'espère !) comment circulent les paquets IP à travers Internet, il me reste à donner rapidement quelques explications sur le système de désignation de noms, en anglais **Domain Name System (DNS)**. Vous avez vu plus haut que tout ordinateur connecté à Internet possède un numéro IP qui lui est propre. Pour communiquer avec un autre ordinateur, il vous faut connaître son adresse IP. Or, lorsque vous "surfez" sur le net, vous écrivez très rarement de tels numéros dans votre browser. C'est tout simplement que vous faites appel, sans le savoir, à un serveur DNS.

Un serveur DNS est simplement une machine qui associe le numéro IP à une adresse plus facilement mémorisable, bref une sorte d'annuaire téléphonique pour Internet.

Ainsi, la machine qui répond lorsque vous tapez `http://www.microsoft.com` dans votre browser possède en fait l'adresse IP 207.68.137.65. Si vous tapez `http://207.68.137.65`, vous obtiendriez exactement le même résultat. Un (ou plusieurs) serveur DNS se trouvent généralement chez votre Provider; vous avez d'ailleurs sûrement reçu une feuille de configuration vous indiquant un ou deux numéros IP pour ces serveurs lors de la configuration de votre connexion à votre Provider.

Une manière simple de constater l'utilité d'un serveur DNS est d'ouvrir (sous Windows 95) une fenêtre DOS, et de taper `ping 'adresse de l'hôte'`, par exemple `ping www.microsoft.com`. "Ping" est une fonction très utile dans l'établissement de réseau : c'est une commande qui envoie un paquet IP tout simple à un ordinateur et lui demande simplement de répondre. Sous Windows 95, quatre paquets IP sont envoyés, et si vous avez tapé `ping www.microsoft.com` par exemple, votre ordinateur devrait ensuite vous écrire une ligne de type "pinging www.microsoft.com [207.68.137.65] with 32 bytes of data", suivie de quatre lignes de la forme "reply from 207.68.137.65: bytes=32 time=550ms TTL=128". Ces quatre dernières lignes vous indiquent que le serveur Microsoft a répondu (personnellement !) à vos appels et vous montrent le temps total qu'a pris la transaction pour chaque ping (par exemple 550 ms). Vous noterez surtout que le serveur DNS de votre Provider aura fait automatiquement la translation `www.microsoft.com` <-> 207.68.137.65.

PS : J'ai parlé plus haut de l'adresse IP réservée 127.0.0.1, dite adresse de boucle; un ping sur cette adresse correspond à un ping "sur soi-même", ce qui permet de tester la bonne marche de la carte réseau.

MISE EN PLACE D'UN RESEAU (Rappel)

1. *Introduction*
2. *Installation matérielle (hardware)*
3. *Structure du réseau*
4. *Mise en place du matériel*
5. *Configuration logicielle*
6. *Partage des ressources*
7. *Utilisation des ressources partagées*
8. *Mise en place de TCP-IP*

1. Introduction

Voilà ! Vous avez deux ordinateurs ou plus et vous voulez goûter au plaisir de les mettre en réseau pour pouvoir jouer des parties frénétiques de Quake à plusieurs, ou tout simplement pour pouvoir communiquer et partager des fichiers ou des imprimantes. A mon humble avis, il est vraiment dommage de posséder plus de trois ordinateurs et ne pas les relier en réseau afin de:

- Échanger des messages
- discuter en direct
- transférer des fichiers
- partager nos imprimantes
- avoir tous accès à Internet

Le but de ce chapitre est donc de vous expliquer en détails comment mettre en place son propre réseau local sous Windows 95.

2. Installation matérielle (hardware)

Contrairement à une idée reçue, la mise en réseau de plusieurs ordinateurs est extrêmement peu onéreuse. Bien évidemment, à ce prix-là, on n'a pas un réseau "autoroutier-à-100 Mo/s-capable-de-gérer-150-postes" ! Tout dépend de l'utilisation qu'on veut en faire : il est réellement inutile de s'équiper avec du matériel haut de gamme (et passablement beaucoup plus cher) pour un réseau de moins de 15 postes qui n'a pas de but professionnel.

Pour un réseau simple de ce type, le seul hardware dont il faut s'équiper est :

- une carte réseau Ethernet de type NE2000 (jusqu'à 10 Mo/s) sur port ISA ou PCI par poste. A titre indicatif, on trouve de telles cartes à moins de 200 Frs , ce qui n'est pas ruineux.
- des câbles Thin-Ethernet BNC (câble coaxial) pas toujours bon marché. Cela dit, le mieux est de construire soi-même les portions de câbles : on trouve facilement des boutiques qui vendent séparément le câble au mètre et les broches (à visser ou à sertir).



Une alternative au câble BNC est l'utilisation de câble RJ-45, mais cela implique l'acquisition d'un HUB et complique la structure du réseau (voir paragraphe suivant). Cette solution est aussi un peu plus chère.



3. Structure du réseau

Faisons l'hypothèse que vous utilisez du câble BNC. La manière la plus simple de construire un réseau est d'utiliser une structure dite *en bus* :



Les ordinateurs sont simplement connectés les uns après les autres sur une ligne centrale.

Il y a cependant quelques règles à respecter dans ce motif :

- En BNC, chaque carte réseau doit être équipée du traditionnel T, mêmes les cartes en extrémités du bus : on place alors un bouchon ("*terminateur*" Ethernet) sur la partie non connectée.



- Notez bien que le T doit être placé directement sur la carte Ethernet. Très malheureusement, des réseaux de ce type, qui seraient pourtant très pratiques dans leur conception, ne fonctionnent pas pour des raisons d'impédance, comme me l'a remarquablement expliqué un visiteur (électricien !) de ce site.

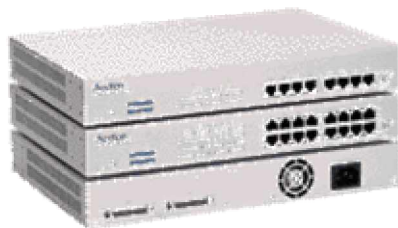


- Dans le même ordre d'idée, on bannit bien évidemment les réseaux "fantaisistes" de type



Les réseaux en BNC sont de loin les moins coûteux. Ils exigent simplement un certain nombre de câbles Ethernet pour relier les différents ordinateurs entre eux et l'achat de deux Terminateurs. Il a par contre un défaut intrinsèque : une coupure du câble (ou une défectuosité quelconque (ce qui peut être fréquent sur des câbles fabriqués "maison")) à un certain endroit peut au meilleur des cas "scinder" le réseau en deux ou au pire paralyser tout le réseau. Le gros désavantage du BNC est la grande difficulté de localiser l'emplacement d'une panne.

L'alternative est d'utiliser du câble RJ-45. Au contraire du BNC, les ordinateurs sont reliés à une unité centrale appelée *HUB* (qui coûte assez cher). Selon la topologie des lieux, cette solution peut s'avérer moins pratique au niveau du câblage qui est plus abondant. Elle a par contre un avantage certain : si un segment est endommagé, le reste du réseau n'en est pas affecté. De plus, le RJ-45 est plus rapide que le BNC, mais cette différence est quasi négligeable avec l'utilisation de cartes NE2000 10 Mo/s.



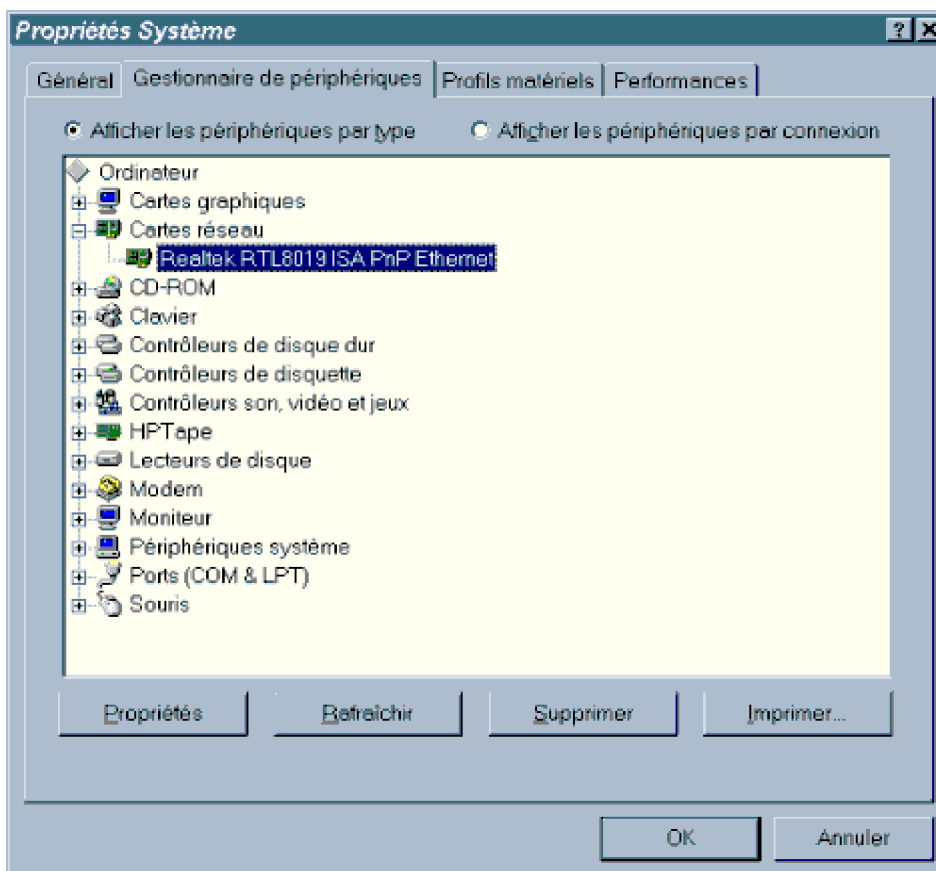
4. Mise en place du matériel

Outre le câblage élémentaire que je vous ai présenté ci-dessus, vous devez bien évidemment installer la carte réseau dans votre ordinateur. Je dirai simplement que ces cartes s'installent aisément sous Windows 95, pour peu qu'elles soient Plug'n Play. Vous pouvez généralement mettre de côté la disquette fournie par le constructeur, Windows95 fournissant des drivers "compatibles NE2000" quasi universels. Ces drivers génériques fonctionnent très bien pour un réseau en BNC, mais ne sont pas toujours performants pour un réseau en RJ-45 (problèmes de collisions dans le HUB); dans ce cas, trouvez des drivers spécifiques à votre carte.

Vous noterez finalement que ces cartes, outre un port I/O, exigent aussi un IRQ libre. J'espère pour vous qu'il en reste au moins un dans votre PC.

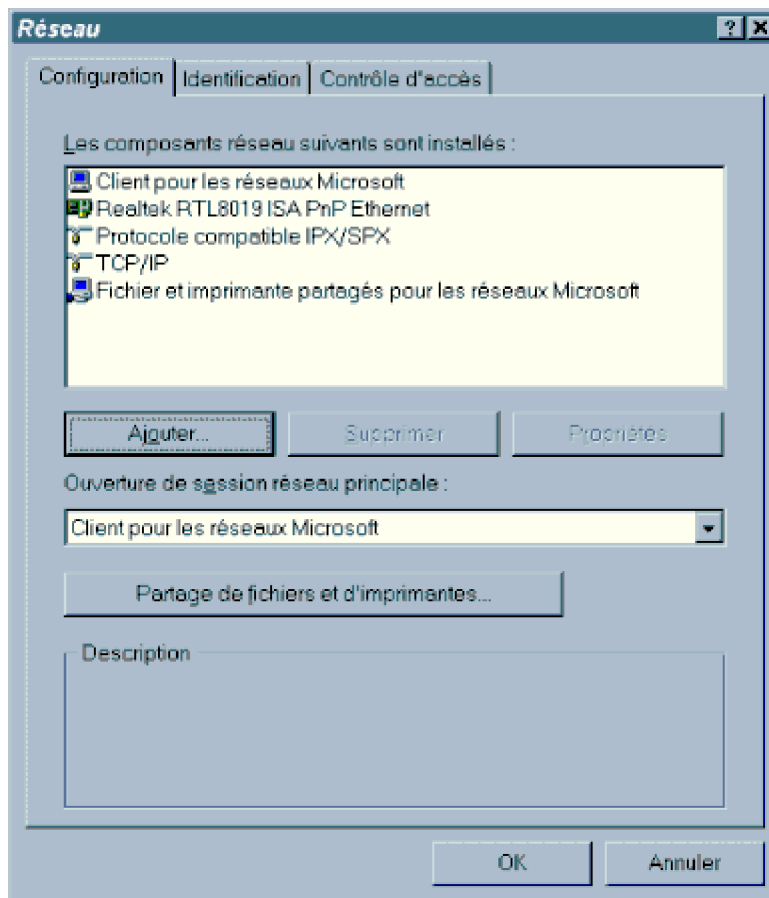
5. Configuration logicielle

Allez maintenant dans le panneau de configuration, puis double-cliquez sur l'icône 'Système'; si votre carte réseau est bien installée, vous devez avoir quelque chose comme cela :

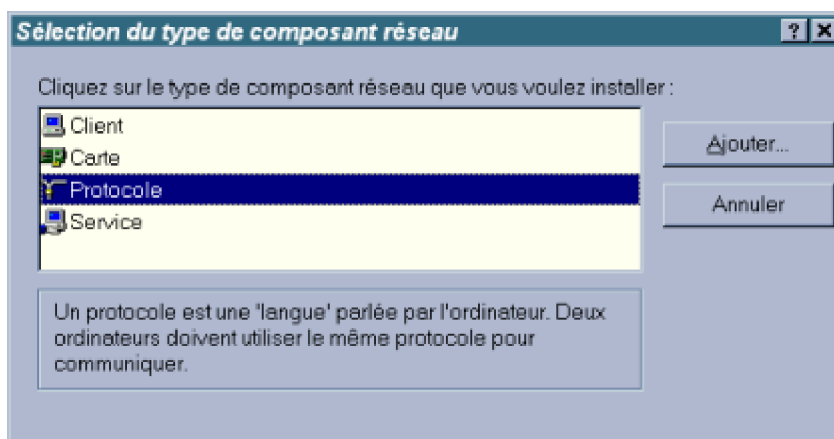


Bien évidemment, votre carte s'appelle peut-être autrement (par exemple, carte compatible NE2000, etc.). S'il y a un point d'exclamation jaune à côté, c'est que la carte est en conflit, probablement d'IRQ, avec un autre périphérique de votre système. Choisissez alors un IRQ libre pour votre carte (sous Windows 95). Si cette dernière n'est pas PnP (ou si elle est en mode jumperless), utilisez l'utilitaire DOS livré avec votre carte Ethernet (en mode DOS, et non sous Windows 95 !) pour forcer la carte à utiliser l'IRQ de votre choix.

Configurez maintenant la partie logicielle; allez sous le panneau de configuration, puis double-cliquez sur l'icône 'Réseau'. Vous obtenez une boîte de dialogue analogue à celle-là :



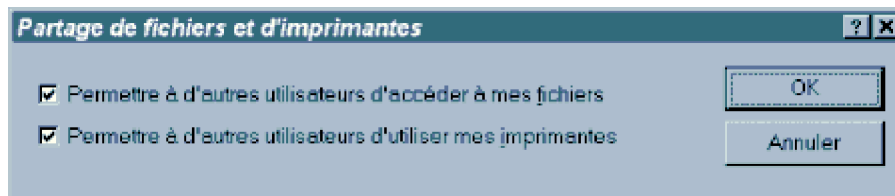
- Si vous créez un réseau local personnel, vous pouvez tout à fait supprimer le client Netware installé par défaut par Windows 95.
- Au niveau des protocoles à installer, je vous recommande la simplicité : IPX-SPX sera le protocole par défaut du réseau local; ce protocole est indispensable pour tous les jeux pouvant se jouer en Network. Si votre LAN risque d'être connecté à Internet, il vous faut installer le protocole d'Internet, à savoir TCP-IP. Vous pouvez ajouter des protocoles en cliquant sur le bouton ajouter, puis sur Protocole.



Les protocoles IPX-SPX, NetBEUI et TCP-IP sont disponibles sous le constructeur Microsoft.

- Par défaut, le protocole NetBEUI est installé.

En-dehors de ça, vous devez indiquer à Windows si vous allez partager des dossiers ou des imprimantes avec le bouton "partager....."; si vous le faites (ce qui est l'intérêt même de construire un réseau !), Windows rajoute automatiquement le service "Fichier et imprimante installés pour les réseau Microsoft" dans les composantes installées.

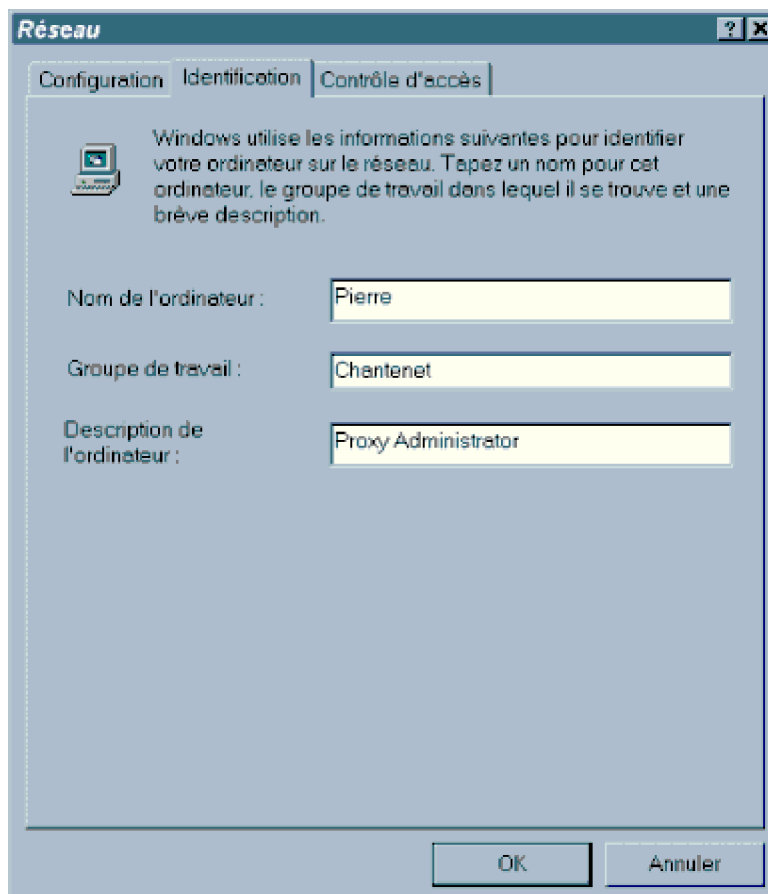


Finalement, remplacez 'Client pour les réseaux Microsoft' (case 'ouverture de session réseau principale' par 'Ouverture de session Windows' **si votre réseau ne comporte que des postes Windows 95**. Cette option vous évite de devoir entrer un mot de passe de session à l'ouverture de Windows 95.

Une autre manière d'éviter cela est de conserver 'Client pour les réseaux Microsoft' et utiliser TweakUI pour que ce dernier remplisse automatiquement à chaque démarrage votre mot de passe utilisateur.

Notez bien que si votre réseau comporte des ordinateurs sous Windows NT, vous ne devez PAS sélectionner 'Ouverture de session Windows' car vous aurez de gros problèmes à accéder aux ressources partagées de l'ordinateur NT qui vérifie l'identité de l'utilisateur qui se connecte à ses ressources partagées.

Allez ensuite à l'onglet 'Identification' et donnez un nom à votre ordinateur sur le réseau ainsi que le nom du réseau. Attention, pour que les ordinateurs puissent "se voir", **le nom du groupe de travail doit être identique pour tous**.



En résumé, les composantes suivantes doivent être installées :

- un client Microsoft
- votre carte réseau (la "carte d'accès distant" correspond à un modem)
- le protocole IPX-SPX ou Netbeui
- le protocole TCP-IP si vous allez vous connecter à Internet
- la gestion du partage des fichiers
- une identification de votre ordinateur sur le réseau

Notez que si vous avez installé l'accès distant, tous les protocoles seront "dédoublés" pour chacune des interfaces, par exemple

TCP/IP -> Carte d'accès distant

TCP/IP -> Carte NE2000

Protocole compatible IPX/SPX -> Carte d'accès distant

Protocole compatible IPX/SPX -> Carte NE2000

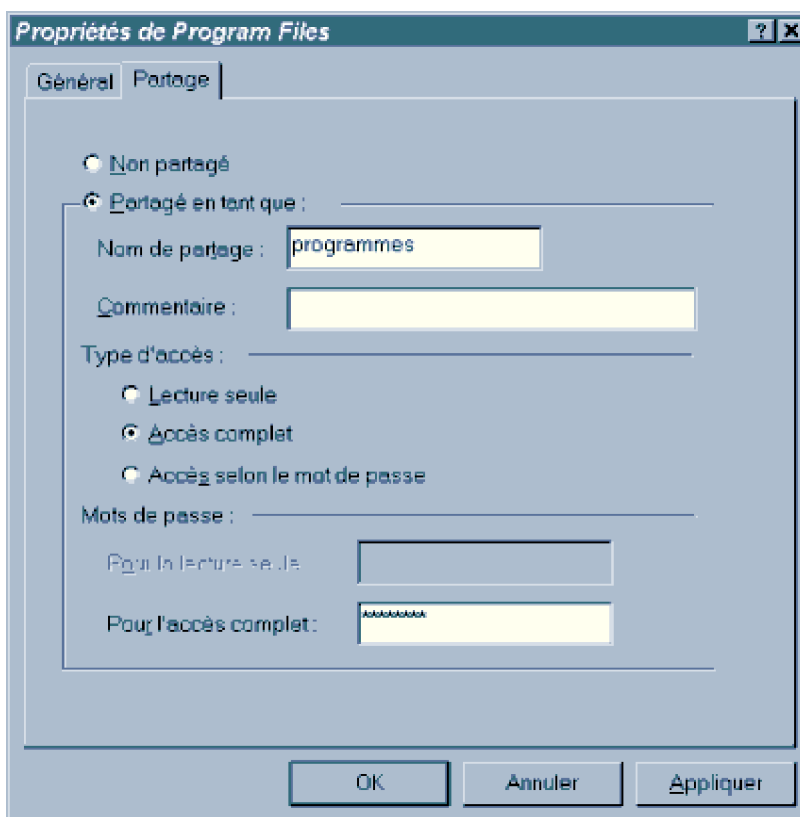
Vous pouvez dès lors supprimer les protocoles qui ne sont pas nécessaires : par exemple, si votre modem ne vous sert qu'à vous connecter à Internet ou envoyer des fax, vous pouvez aisément supprimer pour lui des protocoles comme IPX-SPX ou NetBEUI, car seul TCP-IP est utilisé pour Internet.

Si vous comptez installer TCP-IP sur votre LAN, allez voir le paragraphe 8 où je vous explique comment configurer correctement votre réseau avec ce protocole.

6. Partage des ressources

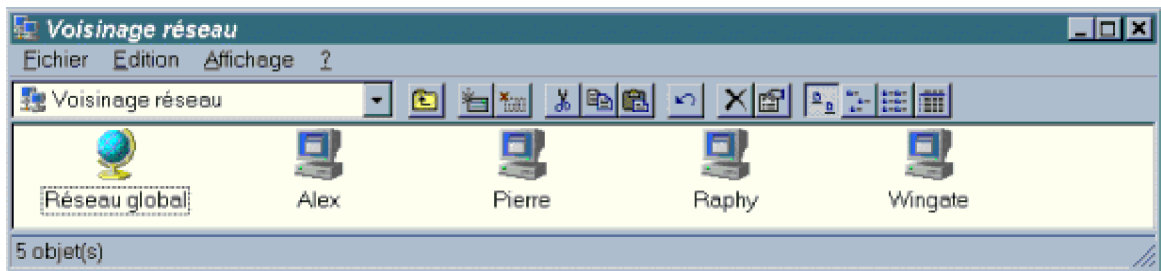
L'utilisation d'un réseau sous Windows 95 est extrêmement simple. Il vous suffit simplement de partager les dossiers et les imprimantes que vous voulez voir accessibles aux autres utilisateurs du réseau.

- En pratique, vous n'avez qu'à vous "ballader" dans l'explorateur Windows, cliquer avec le bouton droit sur le dossier que vous voulez partager et choisir 'partager...'. Dans la boîte de dialogue qui suit, vous pouvez saisir le nom de partage de la ressource ainsi que des permissions basiques (accès selon mot de passe, etc).
- La marche à suivre est sensiblement la même pour le partage d'une imprimante à partir du dossier imprimantes.

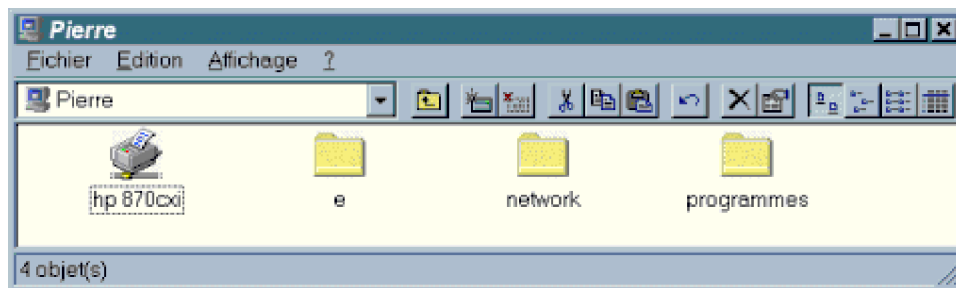


7. Utilisation des ressources partagées

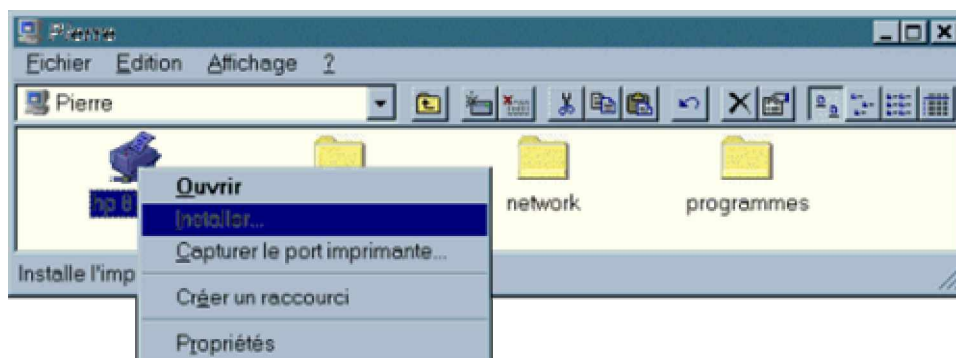
Vous aurez remarqué, après l'installation d'un système de réseau, l'apparition d'un nouvel icône sur votre bureau : le *voisinage réseau*. Un double clic sur cet icône vous montre tous les ordinateurs de votre groupe de travail actuellement connectés.



Un double clic sur un ordinateur vous permet d'accéder à ses ressources partagées (dossiers et imprimantes) de la même façon que vous accédez aux vôtres.



Pour imprimer sur une imprimante du réseau, il vous faut d'abord l'installer chez vous (comme si vous aviez une imprimante supplémentaire). Le plus simple pour cela est de cliquer avec le bouton droit sur l'imprimante partagée de l'ordinateur distant, et faire 'installer...'. Répondez ensuite aux quelques questions qui vous sont posées et vous aurez dès lors une nouvelle imprimante chez vous sur laquelle vous pourrez imprimer dans n'importe quelle application.



Manipulations

Réalisez 5 groupes de machines référencés sous le nom groupe de travail: **TMSIx** avec x= 1 à 5

Pour chaque machine connectée au groupe TMSIx donnez le nom de l'ordinateur suivant: **PosteRx** avec x= 1 à 22

Pour la description de l'ordinateur spécifiez le type processeur utilisé; par exemple: **Pentium II 133**

Partagez un répertoire et/ou une imprimante.

Localisez les différentes ressources disponibles sur le petit réseau ainsi réalisé.

8. Mise en place de TCP-IP

Vous avez donc décidé d'utiliser le protocole TCP-IP pour votre réseau local. N'oubliez pas que vous DEVEZ installer ce protocole si vous projetez de connecter votre LAN (Local Area Network) à Internet, mais bien entendu rien ne vous empêche d'installer TCP-IP de toute façon; même sans Internet, ce protocole souple possède de nombreuses caractéristiques très intéressantes pour un administrateur réseau.

Si vous avez lu la section que je consacre au protocole TCP-IP, vous comprenez qu'une des bases de ce logiciel est d'attribuer une adresse IP personnelle (comme un numéro de téléphone) à chaque ordinateur du réseau. Un problème se pose : y a-t-il une limitation dans l'attribution de ces numéros ?

En fait, si votre réseau est totalement isolé du reste du monde, vous pouvez mettre les numéros qui vous plaisent. Je vous rappelle qu'une adresse IP se présente sous la forme *a, b, c, d* où *a, b, c, d* sont des nombres compris entre 0 et 255 (par exemple 195.38.55.252). Si vous avez lu ma section sur le sujet, vous savez cependant que pour pouvoir communiquer entre eux, les ordinateurs doivent posséder les 3 premiers nombres de l'adresse IP identiques; par exemple, 192.168.0.4 peut communiquer avec 192.168.0.99, mais pas avec 194.168.0.5.

Par contre, si un ordinateur de votre réseau peut "communiquer plus loin", par exemple s'il est équipé d'un modem et qu'il peut avoir accès à Internet, vous n'avez pas le choix d'utiliser n'importe quelles adresses IP. En principe, en absence de système de routage, vous *pourriez* mettre n'importe quelle IP, car les informations circulant sur votre LAN ne peuvent de toute façon pas "sortir" de votre réseau. Cependant, pour des raisons de sécurité, utilisez toujours les adresses IP suivantes :

de 10.0.0.0 à 10.255.255.255

de 172.16.0.0 à 172.31.255.255

de 192.168.0.0 à 192.168.255.255

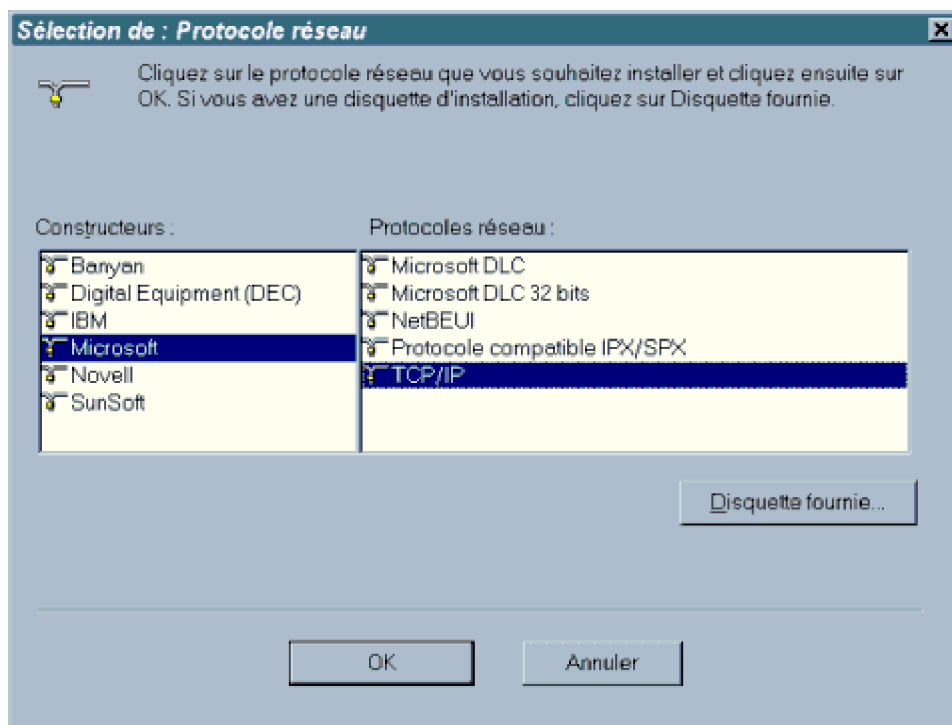
Ces adresses ont été "réservées" par l'INTERNIC et ne seront jamais routées par les Providers Internet. Je parle plus en détails de ces problèmes dans la section mise en place d'un serveur Proxy.

Pour la configuration d'un réseau local simple en TCP-IP, seuls trois points vous intéressent :

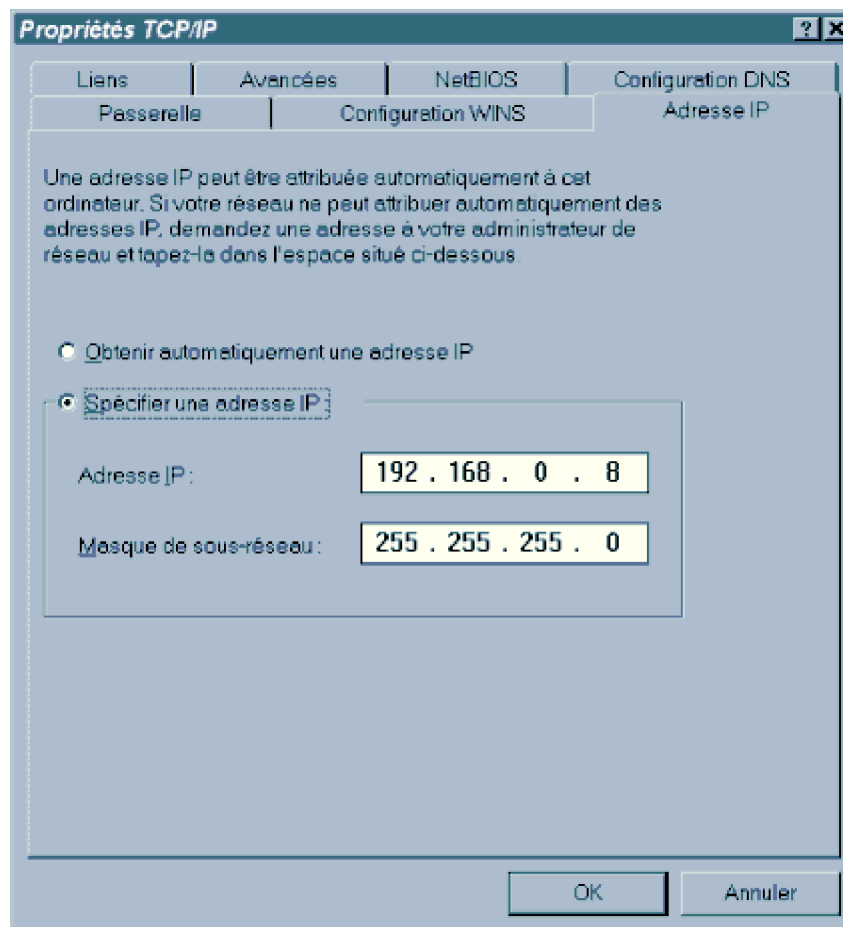
1. l'attribution des adresses IP: je vous conseille vivement d'utiliser les IP 192.168.0.1, 192.168.0.2, 192.168.0.3, etc.
2. le masque de sous-réseau :255.255.255.0
3. un système de désignation de noms de type Host

Reprenons ces points un par un et configurons notre réseau (je suppose pour cela que vos ordinateurs sont correctement connectés les uns aux autres et que les composants réseaux essentielles sont installés).

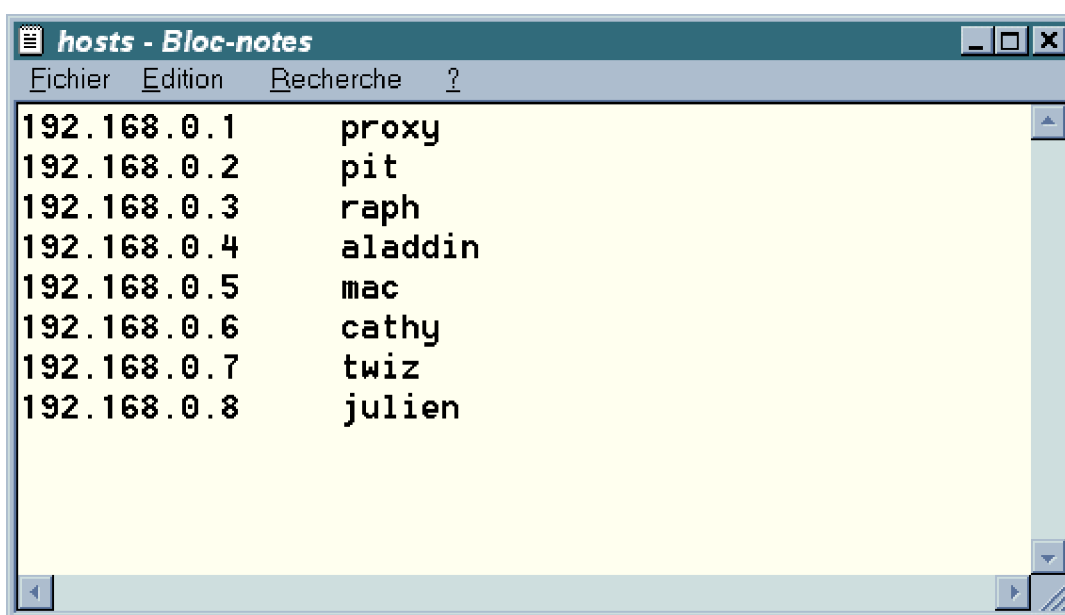
Dans Panneau de configuration Réseau, ajoutez tout d'abord le protocole TCP-IP (en cliquant sur ajouter, puis protocole)



Attribuez ensuite les adresses IP et les masques de sous-réseau. Pour cela, double-cliquez sur 'Protocole TCP/IP' (ou 'Protocole TCP/IP -> votre carte réseau) et allez à l'onglet 'Adresse IP'. Introduisez le numéro IP que vous attribuez à la machine (par exemple 192.168.0.1) ainsi que le masque de sous-réseau (255.255.255.0). N'oubliez pas que chaque machine doit avoir un IP différent (par contre, le masque de sous-réseau est identique partout).



Sur chaque machine, créer un fichier Hosts (*sans extension !*) qui établit une relation entre le numéro IP et un nom, plus facile à retenir, que vous voulez attribuer à l'ordinateur. Voici un exemple de fichier de ce type (à faire avec le bloc-note par exemple) :

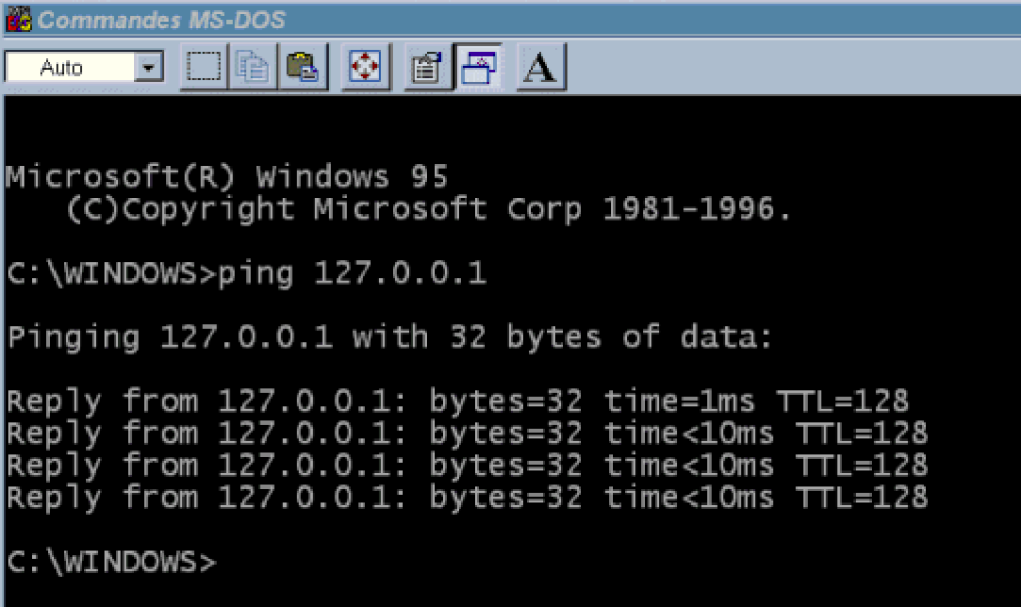


N'oubliez pas le retour de chariot (enter) après la dernière entrée du fichier.

Le fichier doit impérativement résider dans le répertoire c:\windows\, et ce sur tous les ordinateurs du réseau.

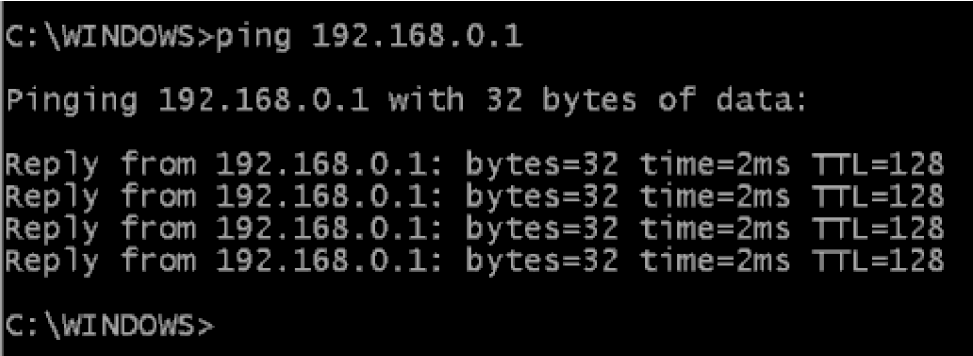
Rebootez tout ce beau monde, et testez votre réseau. Utilisez pour cela la fonction Ping.

- ouvrez une fenêtre DOS et faite d'abord un ping sur votre propre adresse ou l'adresse de boucle (127.0.0.1)



```
Commandes MS-DOS
Auto
Microsoft(R) Windows 95
(C)Copyright Microsoft Corp 1981-1996.
C:\WINDOWS>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time=1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
C:\WINDOWS>
```

- "pingez" ensuite toutes les autres adresses du réseau et vérifiez qu'elles répondent



```
C:\WINDOWS>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
C:\WINDOWS>
```

Si vous obtenez un message de type "Request timed out" ("la requête a expiré"), c'est que votre réseau n'est pas correctement installé; vérifiez votre installation hardware et logicielle.

- testez votre fichier Hosts : au lieu de pinger le numéro IP, "pingez" le nom que vous avez attribué à vos machines; le résultat doit être le même. Au passage, vous verrez que l'ordinateur indique l'adresse IP correspondante.

```
C:\WINDOWS>ping pierre

Pinging pierre [192.168.0.8] with 32 bytes of data:

Reply from 192.168.0.8: bytes=32 time<10ms TTL=128
Reply from 192.168.0.8: bytes=32 time<10ms TTL=128
Reply from 192.168.0.8: bytes=32 time=1ms TTL=128
Reply from 192.168.0.8: bytes=32 time<10ms TTL=128

C:\WINDOWS>ping proxy

Pinging proxy [192.168.0.1] with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128
Reply from 192.168.0.1: bytes=32 time=2ms TTL=128

C:\WINDOWS>
```

Si vous obtenez un message de type "Bad IP address ...", c'est que votre fichier hosts n'est pas correct. Avez-vous bien vérifié qu'il ne porte pas d'extension ? Est-il bien placé dans le répertoire c:\windows\ ? Est-il nommé correctement (hosts et non host) ?

Si tout fonctionne, votre réseau est correctement installé et est donc prêt à être connecté à Internet. Vous pouvez vous attaquer au gros morceau : mise en place d'un serveur Proxy.

Manipulation:

- 1) Pour chaque machine spécifiez les informations suivantes dans Propriétés TCP/IP:

IP = 10.0.0.x (x correspondant au numéro de votre machine)
Masque = 255 . 0 . 0 . 0

- 2) vérifiez votre installation TCP/IP avec l'outil **PING**
- 3) **Créez un fichier Host** contenant les informations suivantes:

IP	Nom de machine
10.0.0.1	PosteR1
10.0.0.2	PosteR2
10.0.0.3	PosteR3
.....

- 4) Vérifiez la reconnaissance des noms avec PING

MISE EN PLACE D'UN PROXY

1. *Un serveur Proxy, mais pour quoi faire ?*
2. *Préparatifs pour connecter un LAN à Internet*
3. *Installation de Wingate*
4. *Configuration de Wingate*
5. *La notion de ports d'écoute*
6. *Configuration des applications*
7. *Conclusions*

1. Un serveur Proxy, mais pour quoi faire ?

Supposons que vous ayez suivi les quelques notions que je vous expose aux chapitre mise en place d'un réseau local et le protocole TCP-IP et Internet, vous avez retenu ceci :

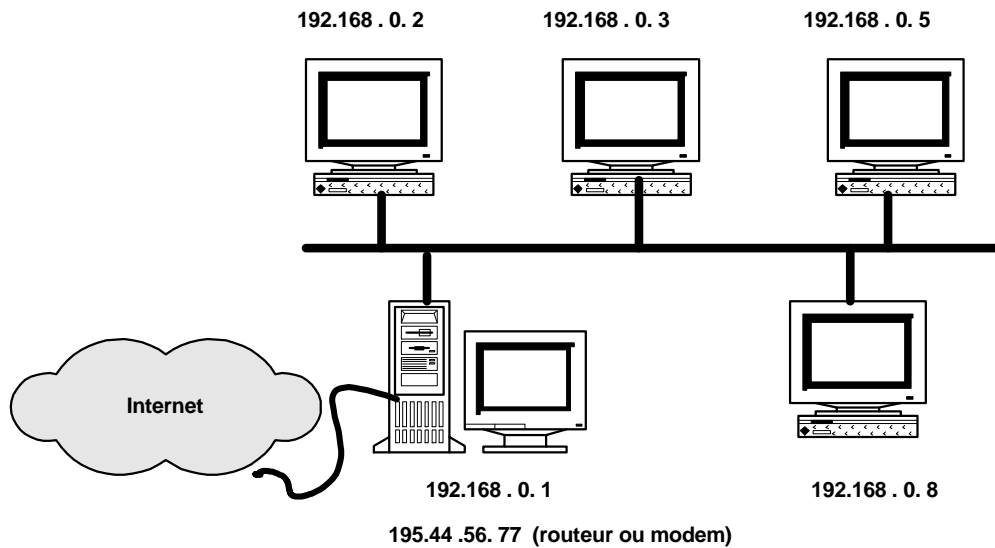
1. Comme TCP-IP est le langage d'Internet, vous avez correctement configuré votre LAN sous ce protocole après avoir assigné à chaque ordinateur une adresse IP propre de type 192.168.0.1, 192.168.0.2, etc... (masque de sous-réseau : 255.255.255.0) et créé le fichier Host adéquat sur chaque ordinateur.
2. Vous savez que votre ISP (Internet Service Provider) vous attribue une et une seule adresse IP lorsque vous vous connectez à Internet.
Cette adresse est souvent fixe (on dit "statique") dans le cas d'un câble opérateur, et variable (on dit "dynamique") dans le cas d'une connexion par modem (votre ISP a une fourchette d'adresses IP disponibles et vous en attribue une de libre lorsque vous vous connectez).
3. Vous avez retenu que les paquets IP que vous envoyez ou recevez sur Internet contiennent les adresses IP des l'expéditeur et du destinataire.

Si vous réfléchissez un peu à ces trois points, vous comprenez tout doucement le gravissime problème qui va se poser : Vous ne pouvez pas identifier de manière univoque tous vos ordinateurs sur Internet, ce qui est une condition obligatoire (puisque le paquet IP doit contenir l'adresse de l'expéditeur et/ou du destinataire).

En effet, seul l'ordinateur de votre LAN qui est connecté directement à Internet (l'ordinateur sur lequel le modem est connecté) possède un "numéro de téléphone" valable sur Internet (l'unique adresse IP attribuée par votre ISP). Les autres ordinateurs de votre LAN ont des adresses "bidons" de type 192.168.0.x qui sont sûrement utilisées par des milliers d'autres utilisateurs dans le monde qui, comme vous, ont créé un réseau local chez eux. C'est bien pour cela que ces adresses ne sont pas routées par les ISP.

Vous pourriez vous croire malin en attribuant la même adresse IP à tous les ordinateurs. Vous devriez cependant vous rendre compte qu'un tel système n'est pas possible, car une information entrante sur votre IP ne "saurait" quel ordinateur du LAN rejoindre. De toute façon, **Windows interdit d'attribuer une même adresse IP à plus d'une machine sur un même réseau**; le problème est donc réglé.

Vous vous retrouvez donc avec une architecture de ce type :Exemple

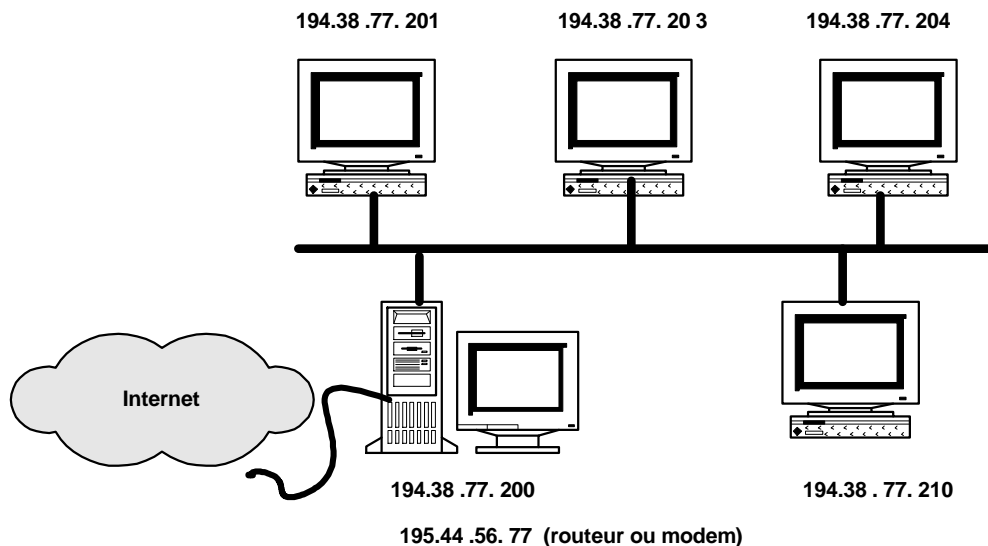


Vous constatez que la machine avec la tour est "à cheval" sur deux réseaux :

1. le réseau "interne" 192.168.0.0
2. Internet 195.44.56.0

Cet machine un peu particulière qui est capable de jouer sur les deux réseaux est appelée le **Gateway**.

- Si votre ISP vous offrait une brochette d'adresses IP valables sur Internet (disons une distincte pour chacun de vos ordinateurs),



vous pourriez simplement faire du "routage", c'est à dire que l'ordinateur à cheval sur les deux réseaux n'aurait qu'à faire transiter les paquets IP du réseau Internet sur le réseau interne, et inversement. Les ordinateurs du LAN ayant des adresses IP bien attribuées sur le réseau Internet, les paquets IP n'auraient pas de peine à retrouver leur chemin.

- Mais comme votre ISP ne vous attribue qu'une adresse IP valable sur Internet, et comme les IP de vos ordinateurs "internes" ne correspondent à rien sur Internet, **le Gateway doit être capable de diriger sélectivement l'information provenant d'Internet (sur votre unique adresse IP) vers un ordinateur précis du LAN.**

Cette machine indispensable peut être soit un *routeur NAT* soit un *serveur Proxy*. C'est de ce type de serveur que nous allons parler ici.

La manière la moins chère de mettre en place un tel serveur est l'installation d'un logiciel idoine sur un ordinateur possédant une carte réseau (pour le LAN) et un modem (pour Internet), ou deux cartes réseaux (une pour le LAN, l'autre pour Internet) dans le cas d'une connexion par câble.

Il existe de nombreux logiciels "Proxy". Pour le reste de ce chapitre, je vais uniquement parler de **Wingate** (<http://www.wingate.net>), logiciel remarquable par son interface graphique accueillante et sa configuration aisée. Wingate 2.1d (la première version 2.1 réellement stable) se décline en deux versions : l'une tournant sous Windows 95, l'autre sous NT. Je ne saurais que trop vous recommander d'acquiescer Windows NT pour le serveur Proxy; Wingate sous NT est la seule solution stable (dans les systèmes Microsoft). En effet, Windows 95 n'est pas un bon système pour les réseaux et vous aurez inévitablement des crashes assez fréquents du système Proxy si vous utilisez ce système d'exploitation. Sachez que la version 3.0 est disponible depuis le 12/1998

2. Préparatifs pour connecter un LAN à Internet

Avant d'installer Wingate, je suppose que vous êtes en ordre avec les points suivants :

1. Vous avez configuré correctement votre LAN sous TCP-IP, avec des adresses IP de type 192.168.0.1, 192.168.0.2, etc... (masque de sous-réseau : 255.255.255.0)
2. Une de vos machines peut se connecter à Internet :
 - soit par modem (dial-up); dans ce cas, vous voyez le protocole TCP-IP dédoublé pour chacune des interfaces dans la partie "Réseau" du panneau de configuration :

TCP/IP -> Carte NE2000

TCP/IP -> Carte d'accès distant

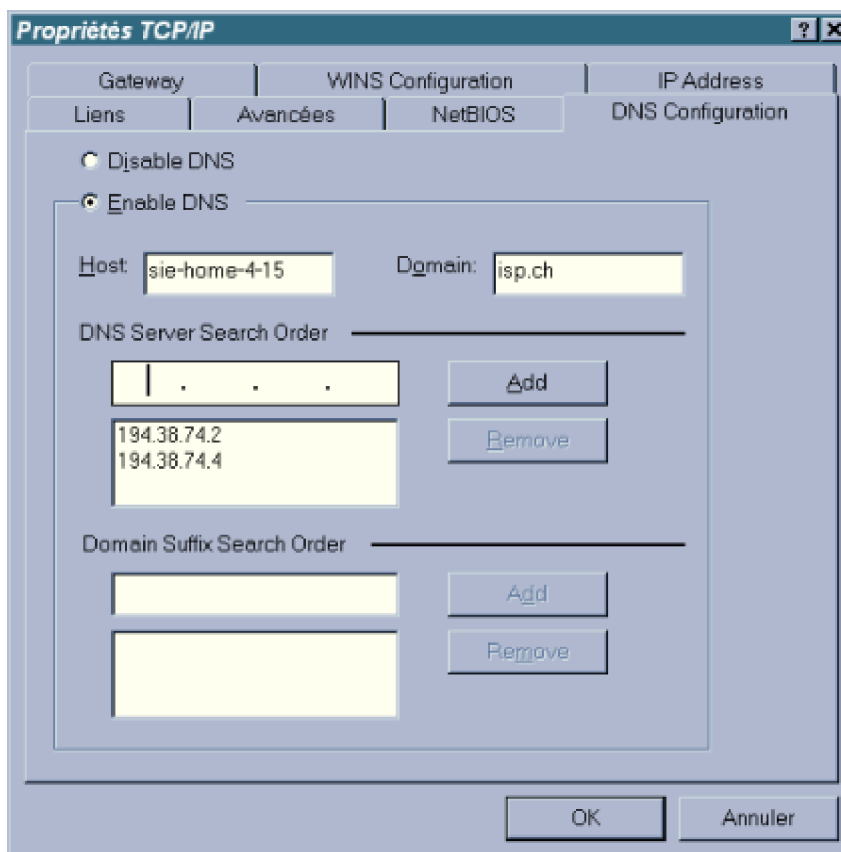
- soit par le télé-réseau si votre ISP est un câble opérateur; dans ce cas, vous aurez bien installé deux cartes réseaux, l'une travaillant sur le réseau interne (IP = 192.168.0.x, masque de sous-réseau = 255.255.255.0), l'autre travaillant sur Internet (IP et masque donnés par votre ISP). Là aussi, le protocole TCP-IP est logiquement dédoublé pour chacune des interfaces :

TCP/IP -> Carte NE2000

TCP/IP -> Carte NE2000

Quelques remarques s'imposent à ce niveau :

- Pour des raisons de commodités, attribuez l'IP 192.168.0.1 à l'ordinateur qui servira de Proxy.
- Si vous possédez un câble opérateur, vous aurez indiqué dans les propriétés de la carte réseau connectée à Internet les adresses IP des serveurs DNS :



Vous constaterez que ces données sur le DNS sont reprises sur la carte tournant sur le réseau interne (192.168.0.1): en effet, Windows n'attribue pas spécifiquement des valeurs DNS à une interface particulière.

- Pour une connexion par modem, les serveurs DNS de votre ISP sont configurés dans votre connexion Dial-up (dossier 'Accès réseau à distance').
- Expérience faite, Windows 95 supporte parfaitement l'installation de deux cartes réseaux (si vous avez un câble-opérateur et que vous voulez faire tourner Wingate sous Windows 95). Cependant, il se peut, si les cartes réseaux sont configurées en mode PnP, que Windows ne détecte les bons paramètres (I/O et IRQ) que pour une seule des deux cartes. Le mieux à faire dans ce cas est de configurer les deux cartes en mode 'jumperless' (grâce à l'utilitaire DOS livré avec vos cartes) et leur attribuer à chacune un port I/O et un IRQ de votre choix, que vous "forcerez" ensuite dans Windows 95.

3. Installation de Wingate

Note préalable : Wingate est un shareware. Dans sa version non enregistrée, il vous permet de configurer plusieurs utilisateurs, mais **un seul utilisateur peut "traverser" à la fois le Proxy**.

Si vous ne voulez donc connecter que deux ordinateurs à Internet en même temps, cette option est suffisante puisque l'ordinateur qui fait tourner Wingate peut se connecter *directement* à Internet (sans passer par le système Proxy); seul l'autre ordinateur traversera Wingate.

Si plus d'ordinateurs doivent pouvoir traverser simultanément le Proxy, vous devrez donc payer en conséquence (le prix de Wingate varie selon le nombre de connexions simultanées dont vous voulez bénéficier).

L'installation de Wingate ne pose pas de problème particulier. Configurez tous les services que le programme vous propose.

Le logiciel vous demande à un moment votre SMTP, c'est à dire le serveur de votre ISP qui accepte vos E-mails sortants (souvent une adresse de type mail.isp.com), ainsi que le serveur de News que vous voulez utiliser (vous pouvez prendre par exemple celui de votre ISP (news.isp.com), mais ce n'est pas une obligation). Laissez le champ blanc pour le serveur IRC.

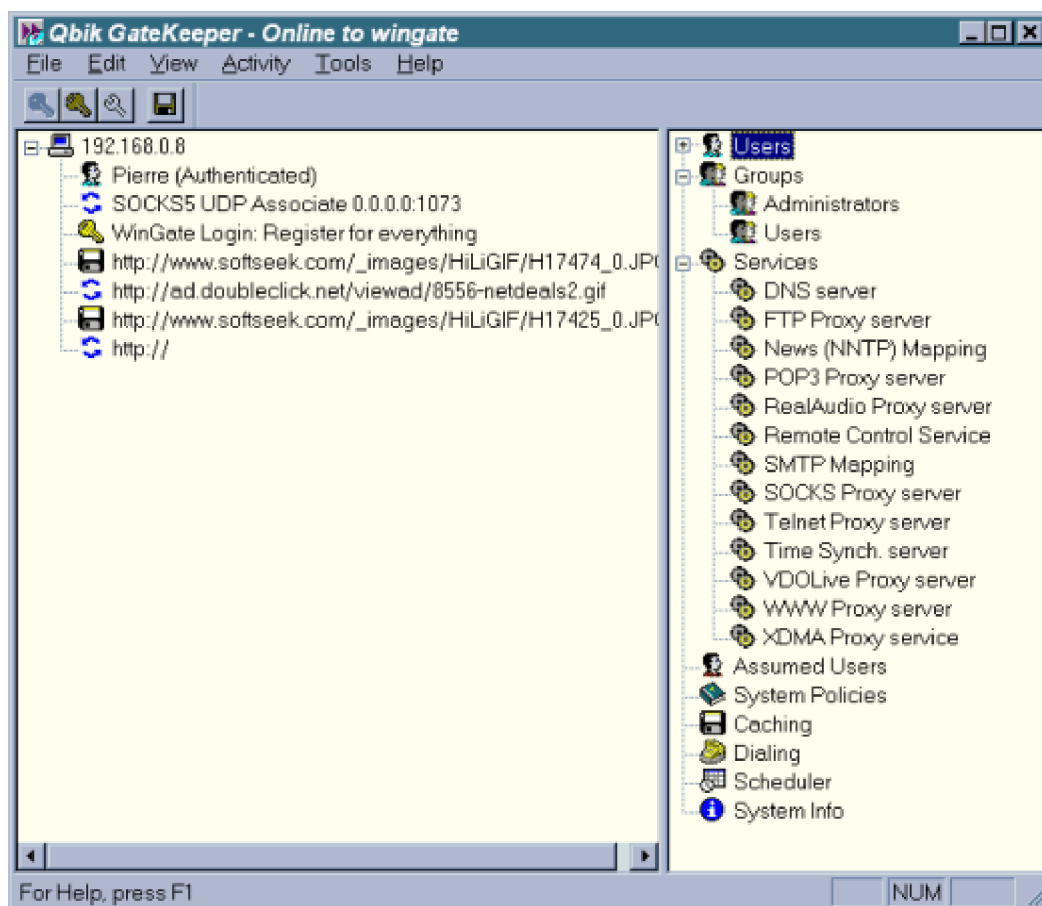
N'installez pas le système DHCP, sauf si vous en avez réellement besoin (adresses IP limitées) et que vous connaissez bien ce genre de services.

4. Configuration de Wingate

Wingate tourne, que ce soit sous 95 ou sous NT, comme un service, c'est à dire que vous ne verrez pas de programme ouvert vous signifiant que Wingate est actif.

Wingate se contrôle à l'aide du 'Gatekeeper'. Je vous donne un bref aperçu des possibilités de ce module :

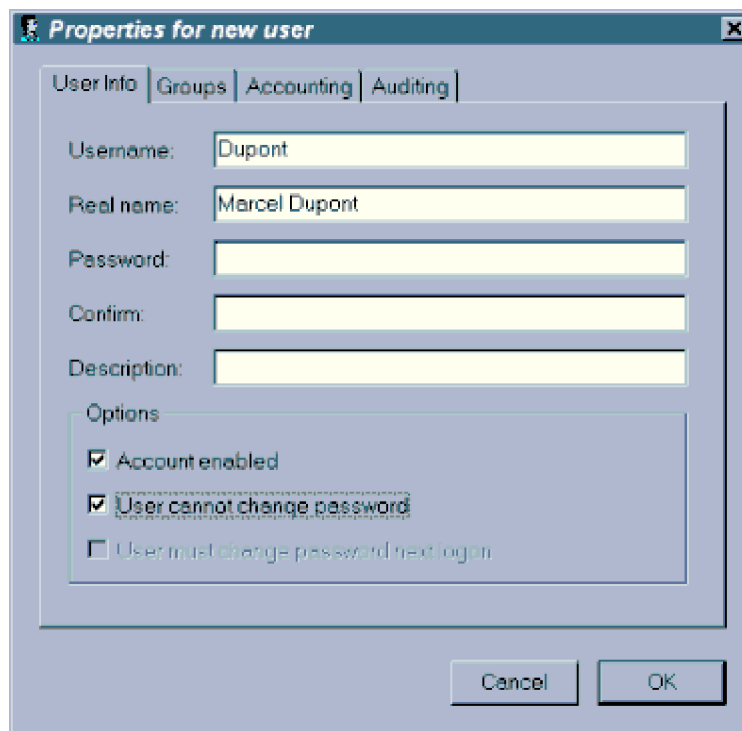
- A la première utilisation du Gatekeeper, vous êtes nommé "Administrator"; n'entrez aucun mot de passe pour l'instant. Le programme vous demandera d'en mettre un juste après.
- Le Gatekeeper se présente sur deux fenêtres : sur la gauche, vous voyez en temps réel tous les utilisateurs qui sont en train de "traverser" le serveur Proxy. Sur la droite, vous configurez les utilisateurs et les services.



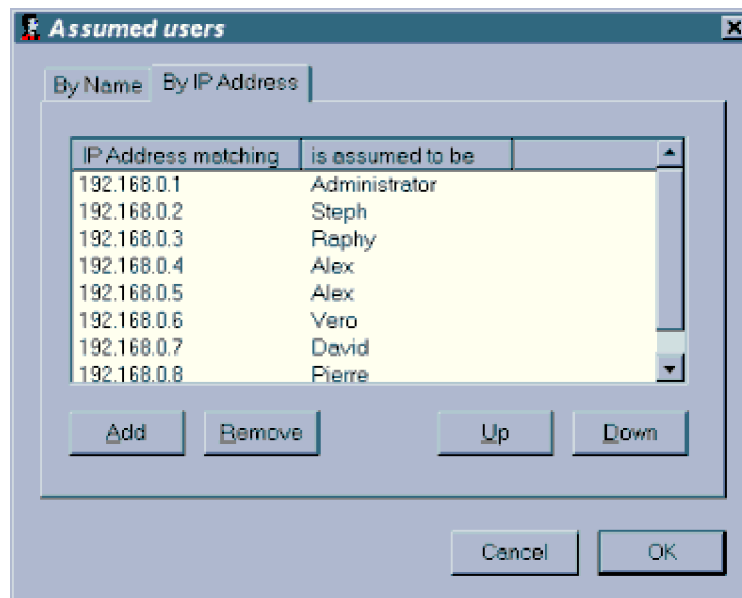
Je vous laisse découvrir par vous-même les possibilités de configuration offertes par ce programme. Voici cependant quelques conseils :

Pour la configuration des utilisateurs, vous pouvez

- soit rendre actif le compte 'Guest' (invité). Ainsi tous les ordinateurs du LAN sans distinction pourront se connecter à Wingate, mais vous ne pourrez pas savoir qui (tout le monde aura la dénomination 'guest')
- soit définir les utilisateurs qui ont le droit d'utiliser le Proxy. Pour cela, cliquer avec le bouton droit sur l'icône 'Users', faites New->User et introduisez les caractéristiques du nouvel utilisateur. Par défaut, ce dernier est placé dans le groupe 'Utilisateurs'.



Ensuite précisez à Wingate comment l'identifier via son adresse IP. Utilisez pour cela l'icône 'Assumed Users'.

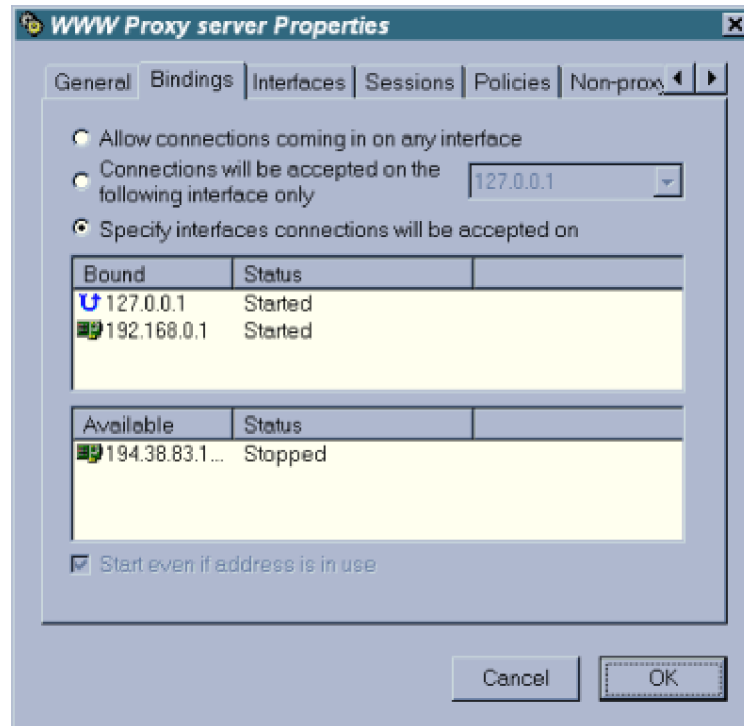


Manipulation:

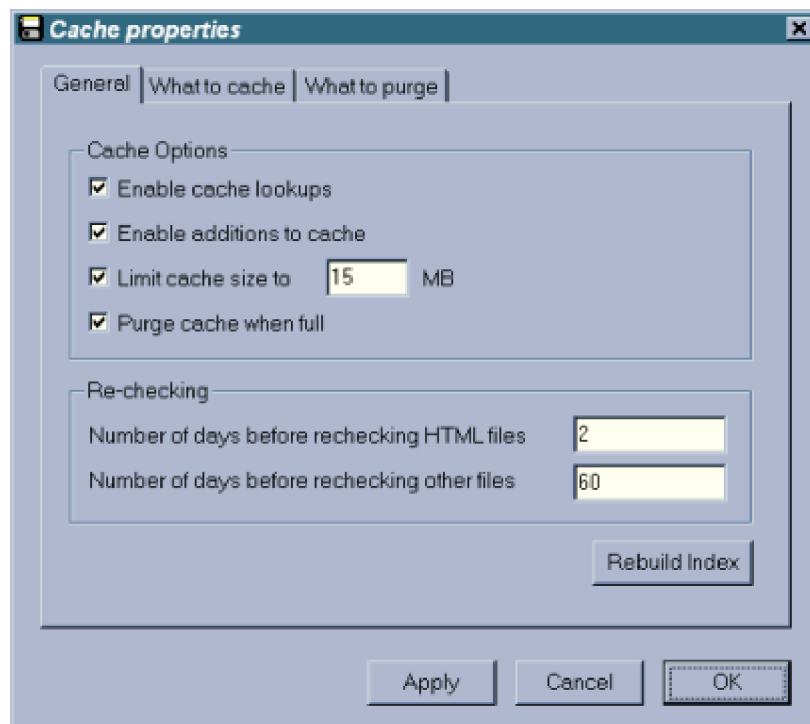
Définissez sur le serveur Proxy, les différents utilisateurs:

10.0.0.1 PosteR1
10.0.0.2 PosteR2
10.0.0.3

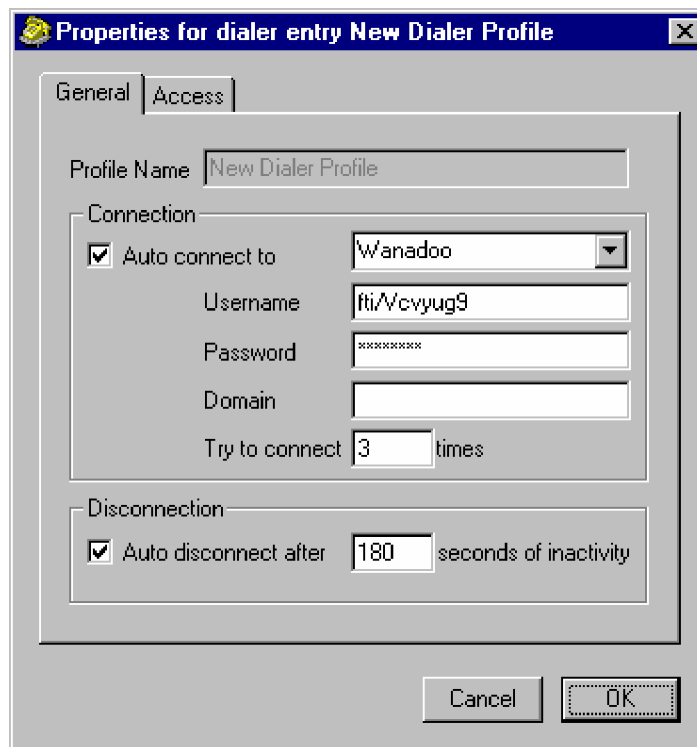
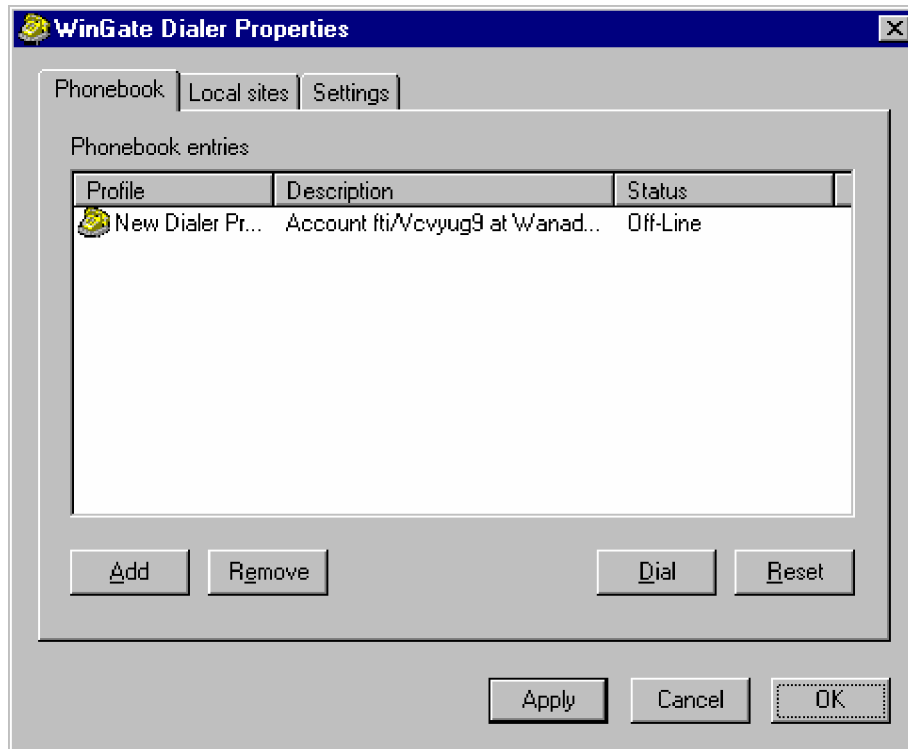
- Pour **chaque** service, n'autorisez, pour des raisons de sécurité, la connexion à Wingate que depuis le réseau interne (empêchez les accès externes; des petits malins peuvent causer beaucoup de tort).



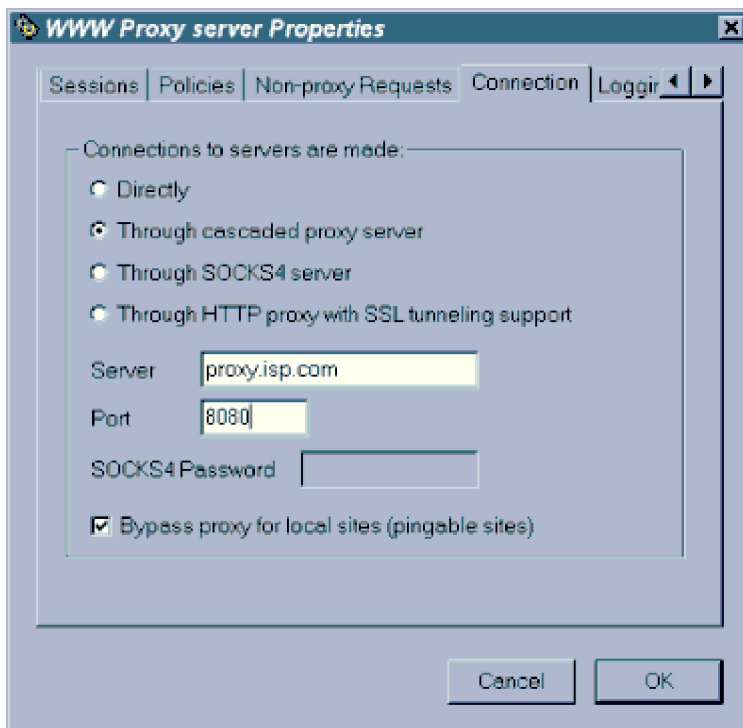
- Le système de cache de Wingate (analogue au cache de votre browser web) est assez performant et vous permet de gagner du temps lorsque vous surfez. Si vous utilisez cependant une vieille bécane pour le Proxy (par ex. un vieux DX2-66 MHz ou moins), ne dépassez pas 20 Mo de cache, car les disques durs de l'époque ont de la peine à se sortir des milliers de fichiers que Wingate peut produire. J'ai remarqué sur mon serveur que la limite de Mo n'était pas toujours respectée (mon cache était gonflé à 61 Mo alors que j'avais fixé une limite à 15 Mo !). J'ai donc personnellement désactivé ce service. A titre indicatif, l'efficacité du cache était d'environ 5% sur mon LAN (avec 5 utilisateurs); il faut donc beaucoup plus d'utilisateurs pour que ce service soit rentable.



ATTENTION: Ne pas oublier de valider la connexion au Provider (Wanadoo).
Celle-ci doit être activée par l'option "DIALING" de Gatekeeper



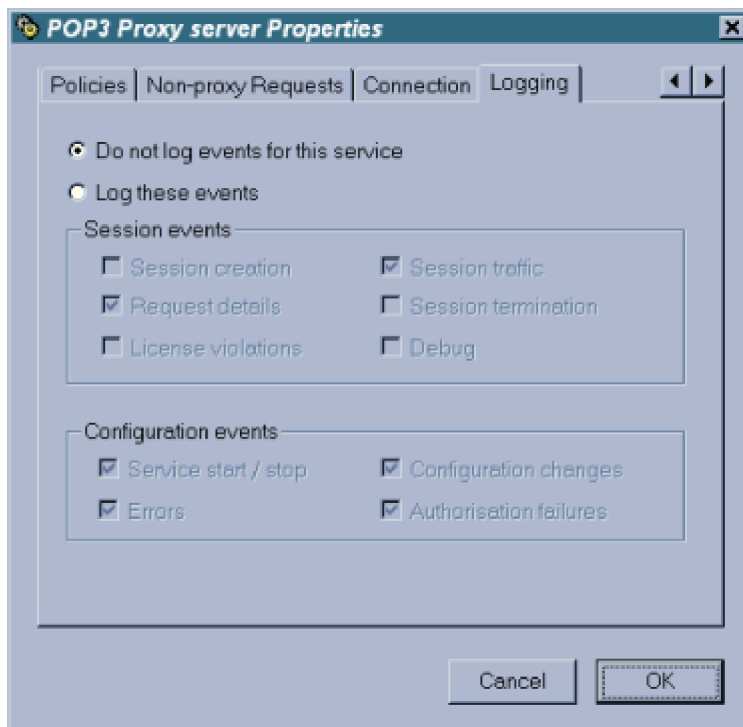
- Si votre ISP vous a donné les coordonnées de son propre serveur Proxy, sachez que Wingate peut l'utiliser; les utilisateurs du LAN passeront donc par un double Proxy (Wingate et le cache de votre ISP). Allez pour cela dans le service WWW, onglet 'Connection', cochez 'Through cascaded proxy server' et indiquez l'emplacement et le port (souvent 8080) du Proxy de votre ISP.



Remarque: il n'y a plus de cache pour Wanadoo

Notez bien que certaines applications n'aiment pas ce système de double Proxy. Par exemple, les premières versions de l'installation active de l'Explorateur 4 exigeait la désactivation temporaire de ce service.

- Désactivez, si vous n'en avez pas besoin, les systèmes de Logs des services qui viennent vite polluer votre disque dur.



5. La notion de ports d'écoute

Cette section décrit la manière particulière dont fonctionnent les applications Internet, et montre bien les limitations d'un serveur Proxy. Retenez bien cette chose essentielle : **le serveur Proxy ne permet pas de faire tout ce que l'on peut faire avec une connexion directe à Internet.**

Exemple concret : vous pouvez, à l'heure actuelle, faire un trait sur l'utilisation d'un logiciel comme Netmeeting à travers un Proxy. De même, les passionnés de jeux peuvent oublier les Gaming-zones d'Internet, comme le Battle.net de Blizzard. Seul le logiciel Kali (<http://www.kali.net>) leur permettra de jouer à travers le Proxy avec leurs amis sur Internet.

Ces limitations sont intrinsèques au fonctionnement même des applications réseaux, particulièrement à la notion de "*port d'écoute*" que j'essaie de vous exposer ci-après.

Une bonne approche des ports d'écoute (dits aussi "*sockets*") pourrait être de les comparer au fonctionnement des lignes numériques (type ISDN) de nos téléphones actuels : vous savez que ces téléphones peuvent recevoir plusieurs appels sur votre seul numéro (par exemple, vous pouvez téléphoner avec un ami, surfer sur Internet et recevoir un fax, le tout simultanément).

On peut faire l'analogie avec TCP-IP :

- Votre numéro de téléphone correspond à votre adresse IP sur Internet
- Les différentes lignes de votre téléphone correspondent aux différents sockets

La comparaison s'arrête là, car autant votre téléphone ISDN peut recevoir simultanément au plus 8 lignes, autant votre connexion à Internet comporte plusieurs milliers de ports d'écoute !

Ces ports ne sont pas totalement aléatoires : les différents types d'applications travaillent généralement sur des ports bien définis (même si, exceptionnellement, cela peut varier).

Je vous donne ci-dessous une liste non exhaustive des applications réseaux les plus courantes.

<i>Application/Service</i>	<i>Port usuel</i>
HTTP	80
FTP	21
POP3	110
SMTP	25
NNTP (News)	119
Telnet	23
SOCKS	1080
Real Audio	1090
VDO Live	9000
XDMA	8000
DNS	53

Bien évidemment, certaines personnes font parfois tourner certains de ces services sur d'autres ports. Par exemple, si vous tapez dans votre browser l'adresse :

`http://www.serveur.com:8080`

cela veut dire que vous essayez de vous connecter à un serveur web tournant sur le port 8080 au lieu du port 80 usuel. D'une manière plus générale, vous comprenez que la tâche du serveur Proxy est de rester attentif à toute connexion entrant chez lui sur des ports d'écoutes bien précis que vous avez configurés. Vous pouvez aussi voir cela d'une autre façon : le serveur Proxy "n'écoute" pas toutes les connexions; il ne s'intéresse qu'à celles pour lesquelles il a été configuré. Cette limitation a des avantages et des désavantages :

- Avantage, car le serveur Proxy devient un "*Firewall*" (pare-feu) qui **filtre** les informations le traversant. C'est une sécurité contre des attaques TCP-IP extérieures qui ont lieu généralement sur d'autres ports que ceux que je vous ai indiqués.
- Désavantage, car de nombreuses applications sophistiquées travaillent sur plusieurs ports en même temps, dont certains sont ouverts dynamiquement. C'est le cas de Netmeeting qui travaille sur 5 ports dont 3 dynamiques; un tel logiciel ne peut donc pas traverser Wingate. Même remarque pour les jeux se connectant sur des Gaming-zones sur Internet.
- Autre désavantage, car les commandes ICMP (comme 'ping' par exemple) ne dépassent pas le Firewall. Ainsi, si vous êtes derrière un Proxy et que vous tapez 'ping microsoft.com', vous obtiendrez probablement la résolution de noms 'pinging microsoft.com [207.46.131.16]...', mais vous aurez ensuite le message suivant : 'Destination host unreachable', car la commande ping ne peut traverser le Proxy. Comprenez par là que **le serveur Proxy n'est pas un routeur.**

6. Configuration des applications

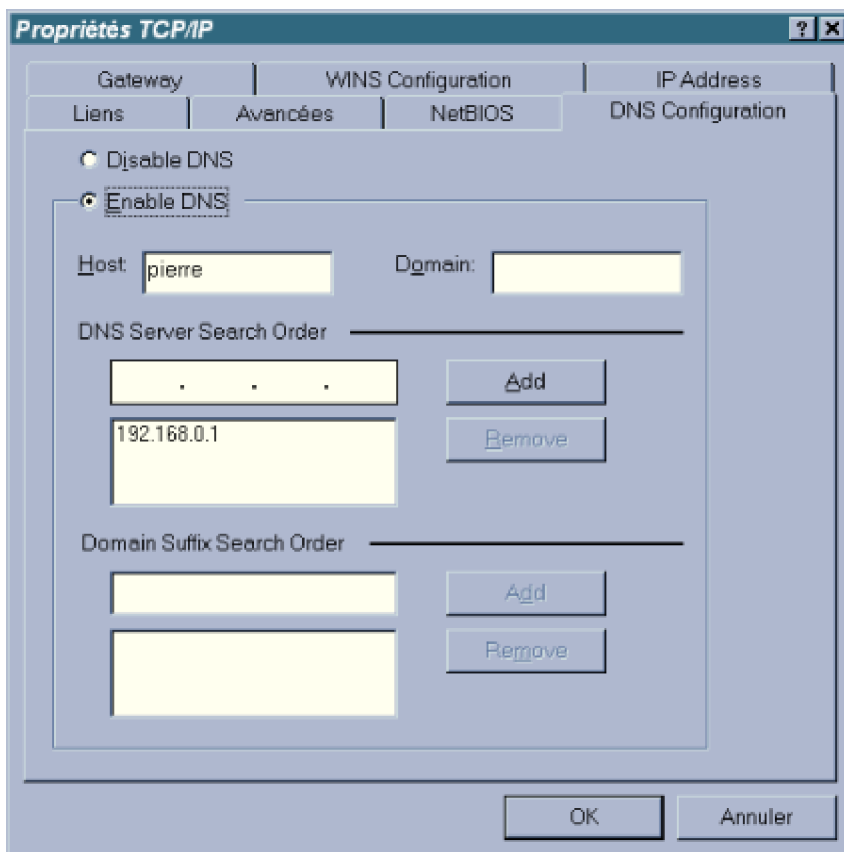
En-dehors du serveur Proxy, dont les applications n'ont pas besoin d'utiliser le système Proxy puisqu'elles sont directement connectées à Internet, toutes les applications des ordinateurs du réseau interne doivent être configurées spécifiquement pour traverser le Proxy.

Je vous donne ci-après un aperçu des applications courantes dont les services sont configurés automatiquement dans Wingate lorsque vous l'installez. Je suppose dans ces exemples que le serveur Proxy d'IP 192.168.0.1 s'appelle "Wingate" (indiqué dans le fichier Host).

Le système de désignation de noms (DNS)

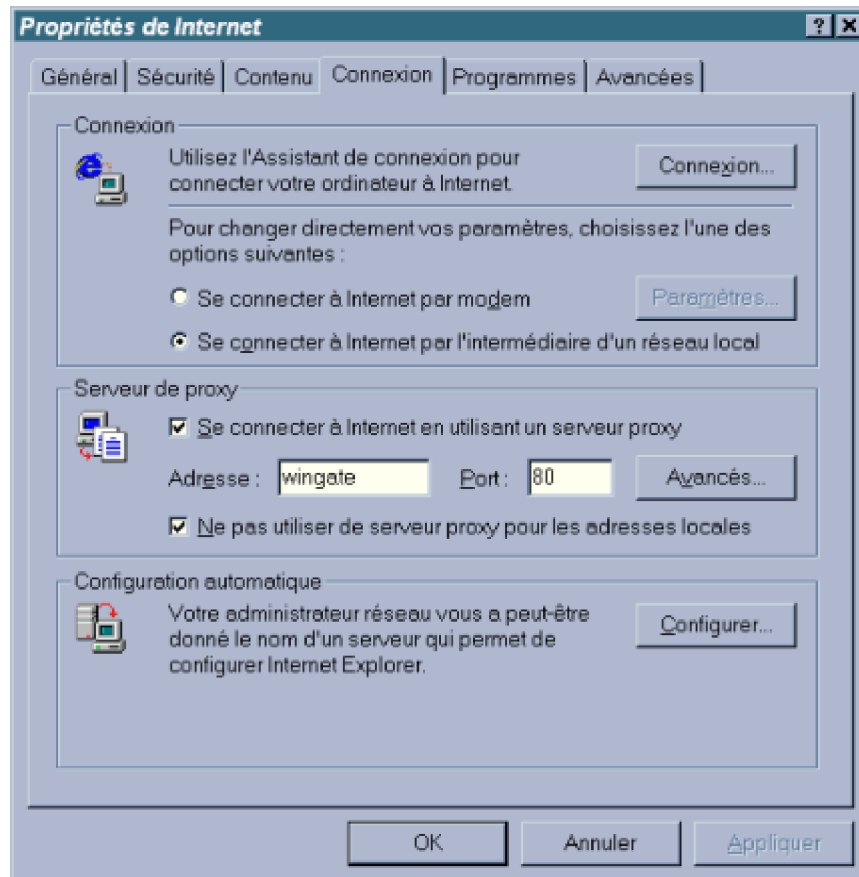
Ce service n'est pas une application à proprement parler, mais c'est lui qui permet de résoudre vos URL.

- Sur le serveur Proxy, vous avez déjà configuré le DNS vers votre ISP
- Par contre, les ordinateurs du réseau interne ne peuvent atteindre le(s) serveur(s) DNS de votre ISP, car Wingate n'est pas un routeur. Fort heureusement, Wingate propose son propre service DNS (vérifiez qu'il est bien présent dans les services). Pour les ordinateurs du LAN, vous indiquerez donc l'emplacement du serveur Proxy comme serveur DNS (panneau de configuration-Réseau-onglet DNS)

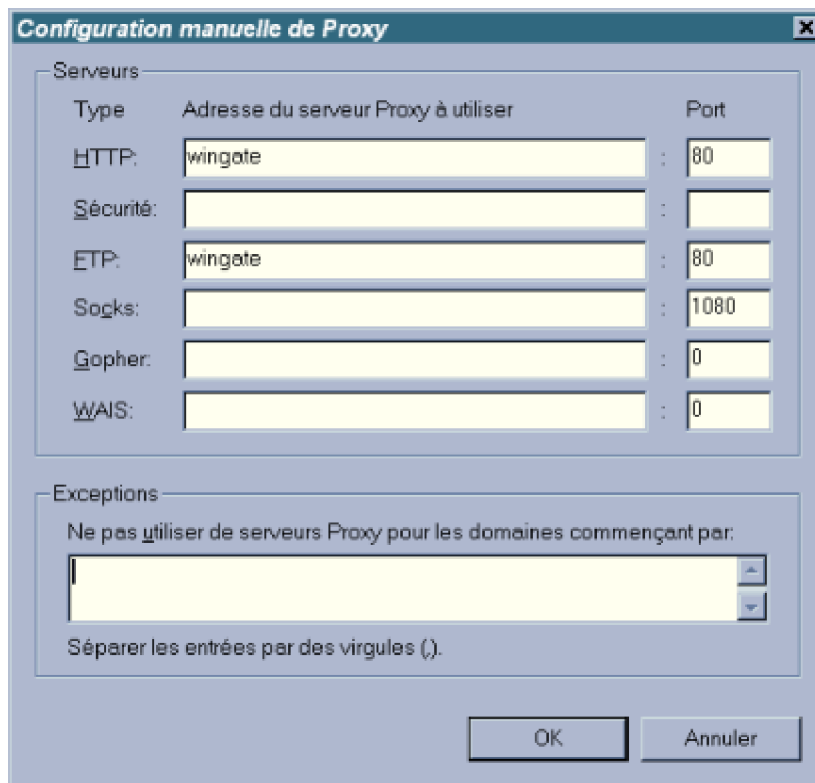


Les browsers web (Internet Explorer, Netscape Navigator, etc...)

- Pour Internet Explorer, allez dans le panneau de configuration-Internet, puis sous l'onglet 'connexion', indiquez l'emplacement du Proxy et le port d'écoute (80 par défaut); cochez éventuellement la case 'ne pas utiliser de serveur Proxy pour les adresses locales' si vous faites tourner un serveur Web sur votre LAN.

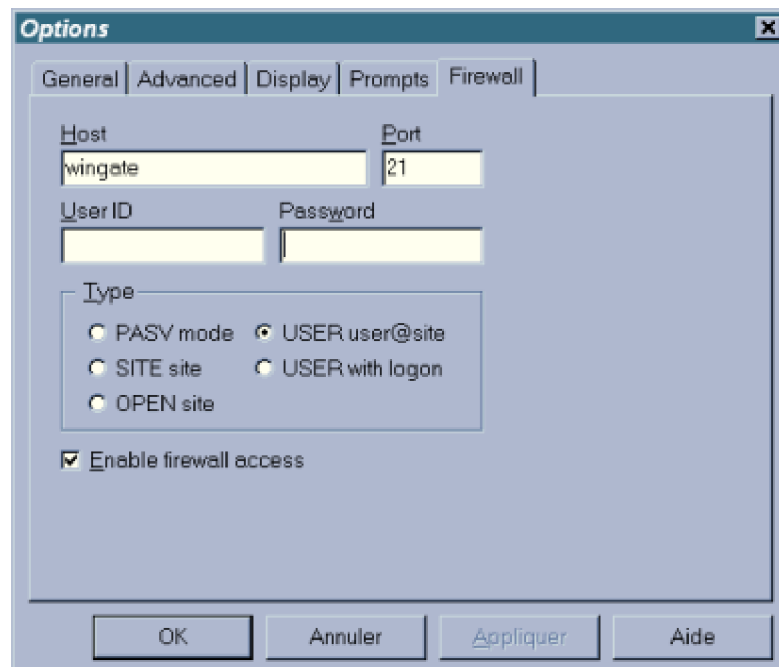


- Dans Netscape Navigator 4.x, allez sous Edition-Préférences-Avancées-Proxy, et cochez 'configuration manuelle du Proxy', puis appuyez sur le bouton 'Afficher', et indiquez l'emplacement du Proxy pour HTTP et FTP; laissez le reste blanc.



Les clients FTP (il y en a tellement...)

Vous trouverez le plus souvent un onglet ou boîte de dialogue pour une configuration via un serveur Proxy. Comme pour les clients Web, indiquez simplement l'emplacement du **Proxy et le port (21 par défaut)**. Comme type de connexion, utilisez 'USER user@site' sous CuteFTP, ou 'user w/out login' sur d'autres programmes.



Retenez cependant ceci : avec un client FTP utilisant le service FTP de Wingate, vous ne pourrez vous connecter qu'à des serveurs FTP travaillant en **port 21**. Si vous aviez l'habitude de vous connecter à des serveurs FTP travaillant sur des ports "exotiques" (comme 8021, 666, etc...), vous devrez utiliser un client FTP se connectant par le service **SOCKS** (voir plus loin).

Les clients de courrier électronique (Outlook Express, Eudora, etc...)

Quelques subtilités dans cette section :

1. Tout d'abord pour le mail sortant (SMTP) :
Configurez simplement pour le SMTP l'emplacement du serveur Proxy.
Dans Wingate, vous aurez préalablement configuré le "mapping" SMTP vers le serveur SMTP de votre ISP (souvent mail.isp.com).
Ainsi tous les gens du LAN qui envoient des mails le font sur le Proxy qui redirige le tout vers le SMTP de votre ISP. Wingate vous permet cependant de personnaliser le mapping SMTP selon l'utilisateur qui émet le mail.

2. Le plus "difficile", le mail entrant (POP3) :
Configurez l'emplacement du Proxy comme serveur POP3 de votre client E-mail.

Par contre, **votre username change**, et devient :

username#votre_serveur_pop3

Ainsi, si avant d'être derrière un Firewall vous vous connectiez à votre serveur POP3 en utilisant le username = sdupont et le serveur POP3 = mail.wanadoo.fr, derrière le Firewall votre nouveau serveur POP3 devient le Proxy et votre nouveau username sdupont#mail.wanadoo.fr.

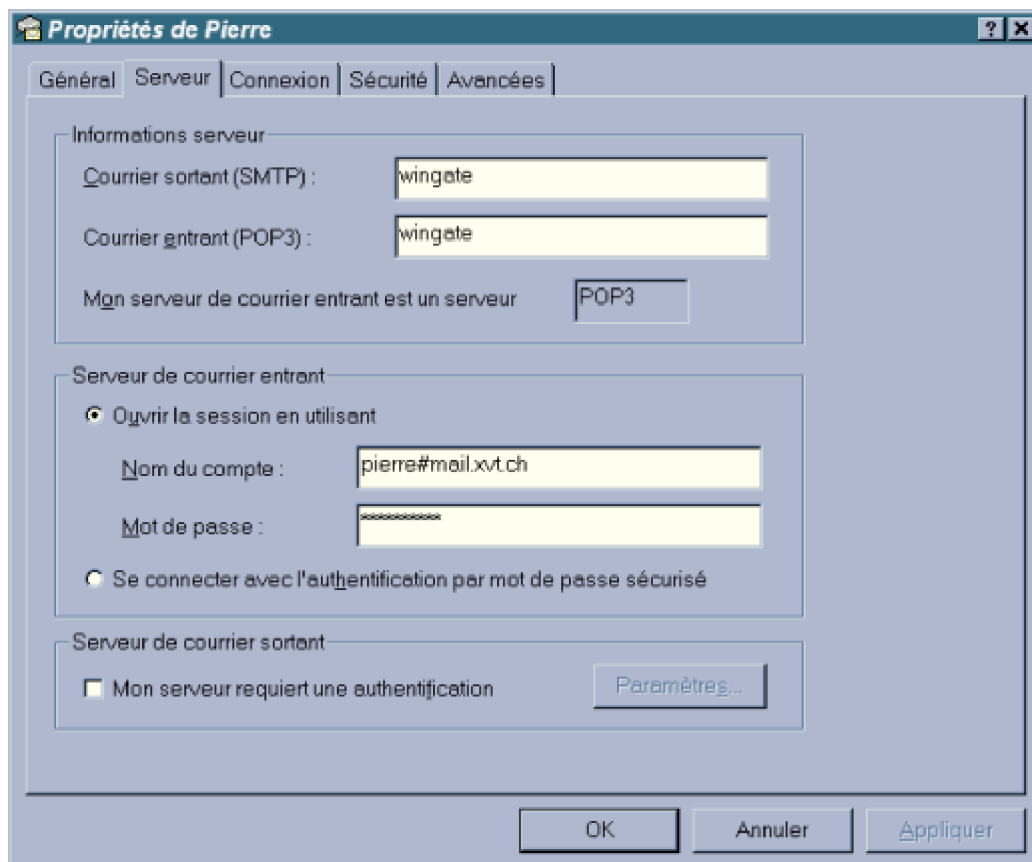
Dans un logiciel comme Eudora qui groupe le username et le serveur POP3 en un "pop-account", votre nouveau "pop-account" serait donc :
sdupont#mail.wanadoo.fr@wingate

En résumé, pour des clients E-mail derrière un Firewall,

POP3 et SMTP = emplacement du Proxy

username = username#votre_serveur_pop3

password = identique



Les clients News

Le Proxy devient le nouveau serveur de News pour les ordinateurs du LAN (port 119 par défaut). C'est dans Wingate que vous aurez configuré le Mapping NNTP par défaut (par exemple vers news.isp.com).

Le service SOCKS

SOCKS (4 et 5) est une petite révolution dans le système Proxy, dans le sens où les applications qui savent utiliser ce service peuvent se croire directement connectées à Internet. SOCKS5 a la possibilité d'ouvrir dynamiquement de nouveaux ports sur le serveur Proxy, et je vois dans cette possibilité la solution pour faire tourner prochainement des applications comme Netmeeting derrière un Firewall. J'attends impatiemment que les nouvelles routines DirectPlay sachent se servir de SOCKS (j'ai entendu dire que la mise à jour DirectX 6.1 apporterait ce service).

Pour le moment, SOCKS peut être utilisé très efficacement par certains clients FTP (comme AbsoluteFTP, LeapFTP, ...), ce qui leur permet de se connecter à des serveurs tournant sur des ports autres que 21.

SOCKS est aussi le meilleur système pour un logiciel IRC.

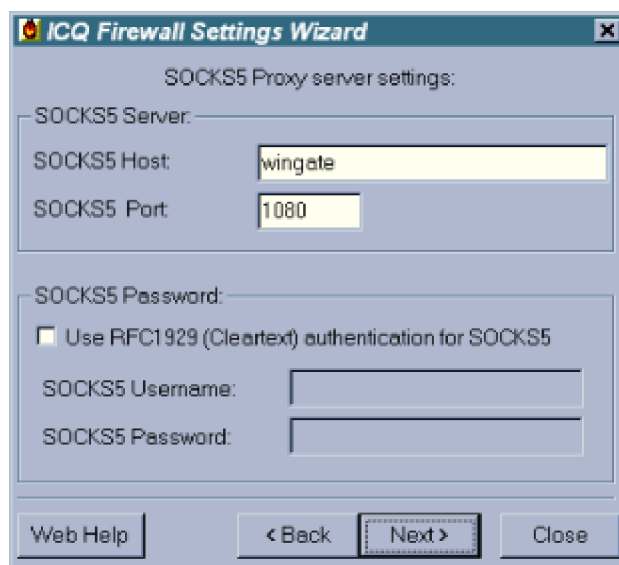
Le logiciels IRC (MIRC, PIRCH, VIRC, etc...)

Choisissez un logiciel qui supporte SOCKS, et configurez l'onglet idoine pour se connecter sur le serveur Proxy en port 1080.

NB : les vieilles versions de MIRC ne connaissent pas SOCKS et c'est un cauchemar que de pouvoir leur faire traverser le Firewall; téléchargez une version récente pour éviter la crise de nerfs.

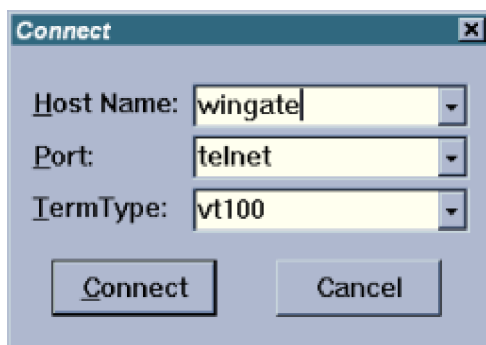
ICQ

Il aurait été criminel qu'un logiciel aussi fantastique qu' ICQ ne puisse pas traverser un Firewall. Heureusement, ce programme s'en sort magnifiquement avec une remarquable utilisation du service SOCKS5.



Telnet

Les gens utilisant Telnet utiliseront simplement une connexion initiale dirigée vers le serveur Proxy.



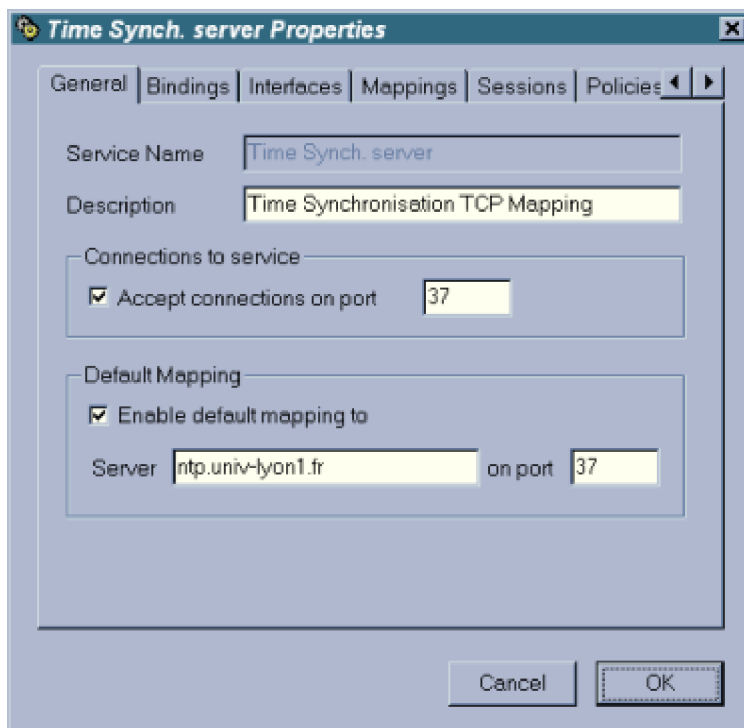
Il obtiendront ainsi un prompt "Wingate>" où ils taperont l'adresse Telnet à laquelle ils veulent se connecter.

Real Audio

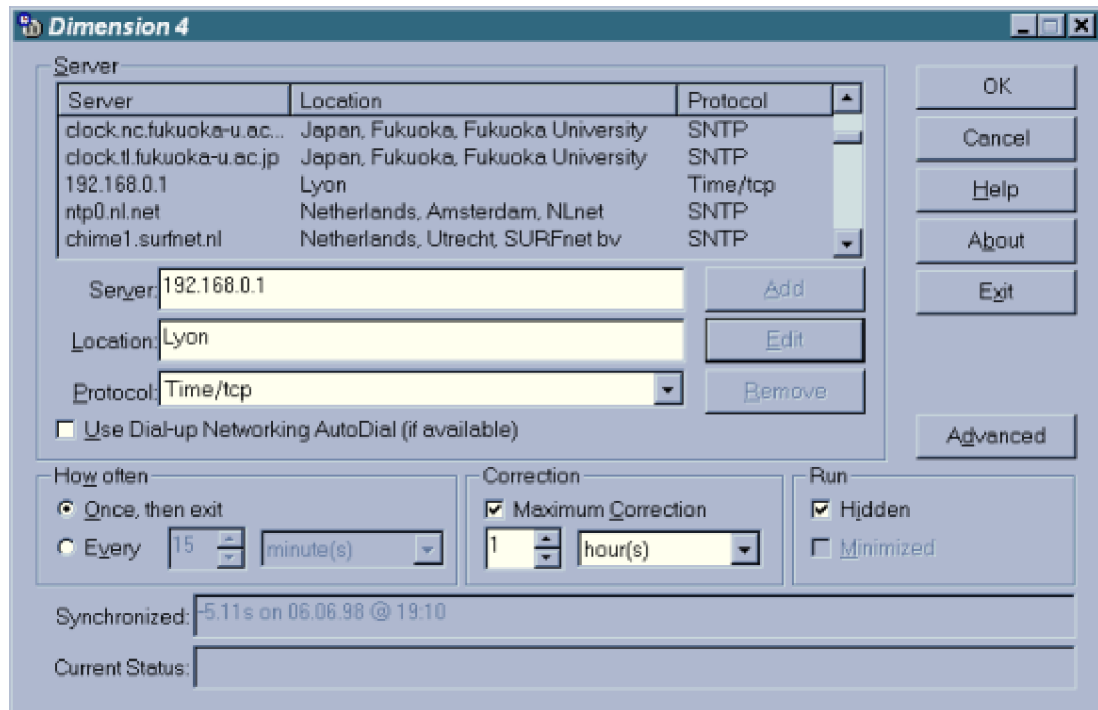
Real Audio traverse sans problème le Firewall. Configurez l'onglet adéquat vers le serveur Proxy en port 1090.

En résumé, retenez donc ceci : pour chaque application qui veut traverser le Firewall vous devez avoir configuré un service adéquat sur le Proxy.

Par exemple, vous pouvez configurer un service qui permet l'utilisation de synchronisateurs d'horloge PC (sur des serveurs-horloges d'Internet), en ajoutant dans Wingate un service TCP sur le port 37 Mappant sur l'adresse du serveur-horloge d'Internet.



Quant à l'application elle-même, vous la configurez pour se connecter sur le serveur Proxy en mode TCP.



7. Conclusions

Ouff ! Vous voilà enfin au terme de ce long chapitre. Au risque de me répéter, je vous rappelle ces deux choses essentielles :

1. **Le serveur Proxy (Firewall) a des limitations** : vous ne pourrez faire tout ce que vous faites avec une connexion directe.
Cette remarque pourrait tendre à disparaître peu à peu lorsque toutes les applications seront capables d'utiliser SOCKS.
2. **Toutes les applications tournant sur le réseau interne doivent être configurées de sorte à traverser le serveur Proxy.** Cette remarque ne concerne pas les applications installées sur le serveur Proxy lui-même qui peuvent accéder directement à Internet.

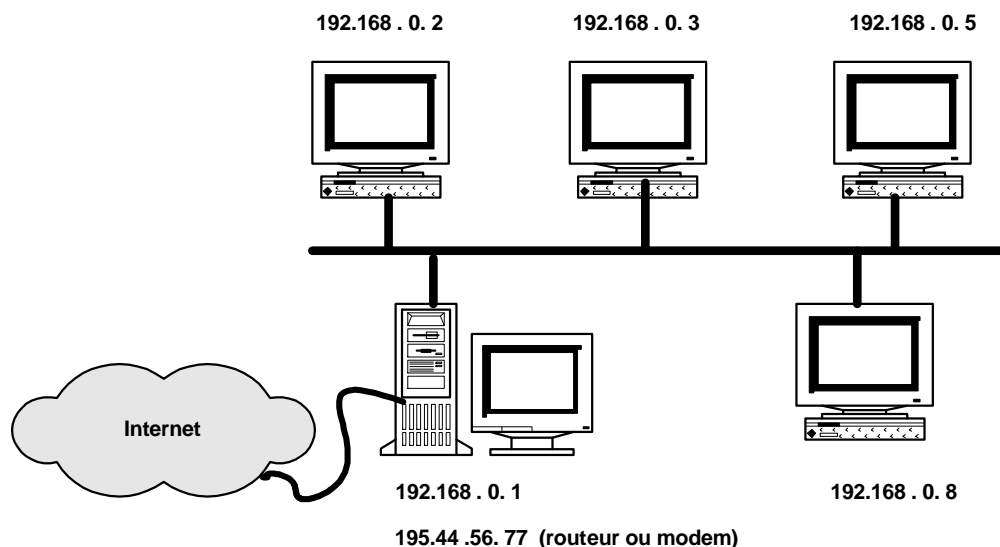
MISE EN PLACE D'UN ROUTEUR NAT PC + SOFT

1. *Récapitulatif*
2. *Rappel sur le partage d'une connexion unique*
3. *Approfondissement sur le transport IP*
4. *Le fonctionnement d'un routeur NAT*
5. *Mise en place de Winroute*
6. *Configuration des machines clientes*
7. *Particularités de configuration*

1. Récapitulatif sur le serveur Proxy

Résumons la manière dont fonctionne un serveur Proxy.

Considérons un réseau local connecté à un serveur Proxy lui-même connecté à Internet :



Admettons qu'un ordinateur du réseau local veuille télécharger une page Web sur Internet. Pour cela il ouvre une connexion vers le Proxy, sur le port d'écoute (socket) défini pour le service concerné (ici HTTP), et lui fait la demande de la page Web. A son tour, le Proxy ouvre une nouvelle connexion vers le serveur d'Internet concerné par la demande, récupère l'information et la retransmet aussitôt à l'ordinateur local.

Dans ce schéma, vous constatez que nous sommes en présence d'une connexion double. Comme je l'ai déjà mentionné, le modèle Proxy, par principe, a de nombreuses limitations. Tous les services que l'on veut utiliser (HTTP, FTP, POP, SMTP, etc.), pour autant qu'ils soient possibles, doivent être configurés un par un sur le serveur Proxy (avec un certain port d'écoute et des règles de "redirection" sur Internet), et toutes les applications sur les ordinateurs du réseau local doivent être en mesure d'utiliser le Proxy et être configurées dans ce sens. Comme je l'avais déjà mentionné, de nombreuses applications ne peuvent utiliser un Proxy; il s'agit généralement des applications travaillant simultanément sur plusieurs sockets, surtout si certains de ces derniers sont ouverts dynamiquement (par ex. Netmeeting, gaming-zones sur Internet, etc.). De même, toutes les commandes ICMP (par ex. ping) s'arrêtent net au Proxy.

2. Rappel sur le partage d'une connexion unique

Si vous avez bien lu mon chapitre sur le protocole TCP-IP et la mise en place d'un serveur Proxy, vous avez compris le gros problème qui survient dans le partage d'une connexion unique vers Internet, puisque vous ne pouvez identifier de manière univoque sur Internet les ordinateurs du LAN.

A ce problème, il existe deux solutions bien différentes :

1. Mettre en place un serveur Proxy
2. Mettre en place un routeur NAT (Network Address Translation)

C'est de cette deuxième solution, très élégante, dont je vais traiter ici.

Cependant, avant de se lancer immédiatement dans le vif du sujet, il me faut détailler un peu plus la manière dont les ordinateurs s'échangent des données sur Internet.

3. Approfondissement sur le transport IP

Si vous avez lu le point 6 de la mise en place d'un serveur Proxy, vous avez compris qu'une connexion Internet contient les paramètres suivants :

1. l'adresse IP du "destinataire" (serveur)
2. le socket de l'application serveur
3. l'adresse IP de "l'expéditeur" (votre ordinateur)
4. le socket de l'application client

Notez que je n'aime pas trop les termes "destinataire" et "expéditeur", vu que toute connexion sur Internet voit des paquets IP aller dans les deux sens.

Exemple : vous ouvrez une page Web dans votre navigateur (ex. <http://www.joliepageweb.fr>). Votre Browser tente alors de se connecter à l'adresse IP du serveur distant (résolue par le serveur DNS) sur le port 80 (généralement utilisé par les serveurs Web). A titre indicatif, je vous rappelle ici les ports les plus courants.

<i>Application/Service</i>	<i>Port usuel</i>
HTTP	80
FTP	21
POP3	110
SMTP	25
NNTP (News)	119
Telnet	23
DNS	53

Vous noterez que je n'ai pas encore précisé le port utilisé par l'application cliente. Contrairement à ce que vous auriez pu penser, *le port sur lequel l'application cliente fait sa requête n'a pas à être identique au port de l'application serveur.*

- D'une manière générale, on peut dire qu'une grande majorité d'applications serveurs tournent sur **un port inférieur à 1024** (HTTP: 80, FTP: 21, TELNET: 23, POP3: 110, etc.). Avec des exceptions toutefois, par exemple des serveurs FTP "pirates" (tournant sur des ports exotiques) ou certains serveurs Web (port 8080 par exemple).
- D'une manière générale, les applications clientes font leur requête sur **un port supérieur à 1024**.

Par exemple, un paquet IP envoyé par votre navigateur au site Microsoft aurait les paramètres suivants :

```

IP du destinataire : 207.46.131.135 (Microsoft)
port serveur Web : 80
IP de l'expéditeur : 195.2.200.149 (votre adresse IP)
port client Web : 7597

```

Ces quelques points un peu éclaircis, il me reste encore à vous dire quelques mots sur les types de protocoles IP présents sur Internet. Comme vous ne le savez peut-être pas, il y a deux types fondamentaux de protocoles IP : le protocole TCP et le protocole UDP.

- Les paquets IP les plus courants sur Internet sont les *paquets TCP* (Transmission Control Protocol). **Ce protocole est utilisé pour une transmission fiable de données**, c'est à dire sans pertes. C'est donc le protocole de la majorité des applications (HTTP, FTP, Mail, IRC, etc.).

J'ai déjà évoqué grossièrement le mécanisme de ce protocole. Rajoutons que dans ce protocole aucune donnée n'est transmise avant qu'une connexion n'ait été mise en place (à l'aide d'un flag (SYN)) entre les deux ordinateurs (qui font une sorte d'accord bilatéral de connexion). De même, lorsque toutes les données ont été transmises, la connexion est "officiellement" fermée. D'une manière analogue, un des ordinateurs peut, pour une raison ou pour une autre, clore la connexion (TCP reset; rappelez-vous du message "le serveur a réinitialisé la connexion" que vous avez sûrement vu quelquefois).

- Parallèlement, il circule sur le net des *paquets UDP* (User Datagram Protocol) qui **sont utilisés pour des transmissions non fiables de données**, c'est à dire où la perte de certains paquets IP est tolérée. Ce sont particulièrement les paquets émis par des serveurs de type Real Audio, MS Netshow, etc., bref toutes les applications qui vous permettent d'écouter du son ou voir de la vidéo en direct sur Internet. Dans ce cas, une fiabilité 100%, en d'autres termes la réception de l'intégralité des données, n'est pas exigée (au détriment bien évidemment de la qualité de réception). Lorsque vous utilisez ce genre de programmes, vous pouvez d'ailleurs voir le nombre de paquets perdus (souvent indiqués en %).
Notez que le protocole UDP, au contraire de TCP, n'exige pas l'établissement d'une connexion: le serveur envoie comme bon lui semble les paquets IP à l'adresse IP et sur le port de son choix.

4. Le fonctionnement d'un routeur NAT/PAT

Le routeur NAT, tout comme un serveur Proxy, est une machine à cheval sur le réseau Internet et sur le réseau local que vous voulez y connecter; il fait office de *passerelle (Gateway)*.

Le NAT tel qu'on l'entend à l'origine est un simple translation d'adresse. Donc, on a deux ensembles d'adresses: *les adresses privées internes au réseau de l'entreprise et les adresses publiques*. Le NAT consiste simplement à gérer une table de correspondances entre les deux types d'adresses.

Adresses privées		Adresses publiques
10.0.0.1	<--->	201.12.12.56
10.0.0.2	<--->	201.12.12.57
10.0.0.3	<--->	201.12.12.58

Donc virtuellement, chaque ordinateur a deux adresses: l'adresse privée et l'adresse publique. Le NAT sous cette forme est essentiellement orienté sécurité: il s'agit de forcer le passage par le serveur gérant le NAT et faisant office de firewall. Un ordinateur extérieur ne peut connaître l'adresse réelle d'un des ordinateurs du réseau privé. Il ne connaît que son adresse traduite et doit donc passer par le firewall.

Une autre technique est le **PAT (Port Address Translation)**.

On le confond souvent avec le NAT. Cette fois-ci, il n'y a qu'une **adresse publique pour tous les ordinateurs du réseau privé**. Nous l'appellerons **NAT/PAT**.

Cette méthode permet d'économiser des adresses publiques car plusieurs ordinateurs avec des adresses privées peuvent accéder à Internet via une seule adresse publique !!!

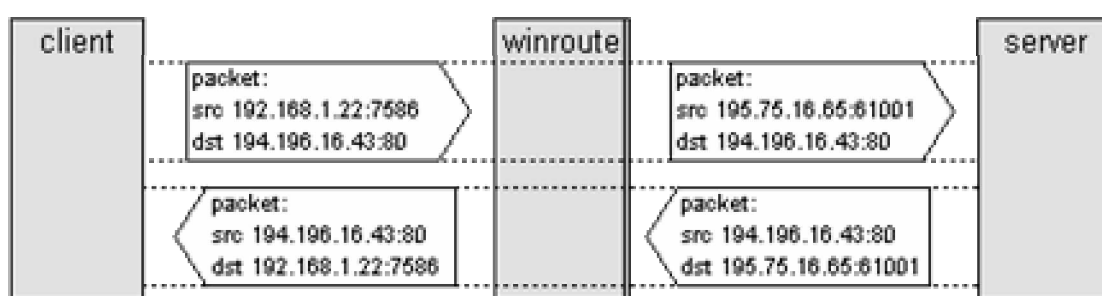
L'astuce est la suivante :

Lorsque le routeur NAT/PAT reçoit un paquet IP d'un des ordinateurs du LAN, il en modifie :

- l'adresse IP de l'expéditeur pour y mettre sa propre adresse (l'IP publique de votre connexion)
- le port de l'application cliente par une valeur particulière
- Le routeur NAT/PAT loge ensuite ces informations dans une table.












Lorsque le serveur d'Internet répond à la requête et renvoie des paquets IP sur le routeur, ce dernier vérifie dans ses tables qu'il possède bien l'entrée correspondante (par rapport au port de l'application cliente), puis y réécrit les coordonnées (IP + socket) de l'ordinateur du LAN. Le paquet IP peut ainsi rejoindre sa destination dans le LAN.

Le routeur NAT, fait réellement du routage de paquets IP, c'est à dire qu'il transmet bien les paquets reçus par un ordinateur du LAN vers Internet (et inversement), contrairement à un serveur Proxy qui ouvre une seconde connexion.














Autre exemple : votre ordinateur du LAN d'adresse IP privé 192.168.0.7 veut accéder à la page Web du serveur www.machin.com (d'adresse IP publique 124.40.67.43) via un routeur NAT travaillant sur l'IP 192.168.0.1 (locale) et l'IP 195.200.2.149 (Internet). Les deux tableaux suivants montrent précisément ce qui se passe.

Établissement de la connexion

Ordinateur	Interface	Coordonnées du paquet IP
 ordinateur	 192.168.0.7	destinataire : 124.40.67.43, 80
		expéditeur : 192.168.0.7, 7364
LAN		
 routeur NAT	 192.168.0.1	destinataire : 124.40.67.43, 80
	 195.200.2.149	expéditeur : 192.168.0.7, 7364
 routeur NAT	 195.200.2.149	destinataire : 124.40.67.43, 80
		expéditeur : 195.200.2.149, 61005
Internet		
 www.machin.com	 124.40.67.43	destinataire : 124.40.67.43, 80
		expéditeur : 195.200.2.149, 61005

Transfert des données

Ordinateur	Interface	Coordonnées du paquet IP
 www.machin.com	 124.40.67.43	destinataire : 195.200.2.149, 61005
		expéditeur : 124.40.67.43, 80
Internet		
 routeur NAT	 195.200.2.149	destinataire : 195.200.2.149, 61005
	 192.168.0.1	expéditeur : 124.40.67.43, 80
 routeur NAT	 192.168.0.1	destinataire : 195.200.2.149, 61005
		expéditeur : 124.40.67.43, 80
Internet		
 ordinateur	 192.168.0.7	destinataire : 192.168.0.7, 7364
		expéditeur : 124.40.67.43, 80

Quelques remarques s'imposent :

1. Les routeurs NAT travaillent souvent sur des ports "élevés". A titre d'exemple, le logiciel Winroute (<http://www.winroute.com>) utilise des ports de 61000 à 61600.
2. On peut se demander pourquoi le routeur NAT modifie le port de l'expéditeur puisqu'il retient de toute façon le port sur lequel l'application cliente a fait sa requête. En fait, cette modification est nécessaire pour éviter des désagréments dans le cas où plusieurs ordinateurs du LAN feraient une requête sur le même port.
3. L'inconvénient du routeur NAT est d'être très pointilleux sur les connexions entrantes : si le routeur NAT n'a pas dans ses tables une entrée concernant une connexion, il ne laisse rien "entrer". C'est en quelque sorte une mesure de sécurité, et aussi une conséquence de sa façon de fonctionner : si vous voulez faire tourner sur un ordinateur du LAN un serveur (par ex. HTTP ou FTP) qui soit accessible par Internet, il vous faudra configurer le routeur NAT pour accepter et rediriger correctement une connexion entrante.

Trêve de bavardages, installons sans tarder un routeur NAT sur notre Gateway !

5. Mise en place de Winroute

Sachez tout d'abord que vous pouvez acquérir un routeur NAT hardware pour un prix relativement modique. Pour la suite de ce chapitre, c'est d'un routeur NAT logiciel dont je vais parler : il s'agit de **Winroute**, disponible sur le site <http://www.winroute.com>.

Notez tout de suite que Winroute tourne aussi bien sur Windows 9x que sous Windows NT. Sous ce dernier, Winroute fonctionne comme un service (et non un programme), tout comme le fait Wingate. Bien évidemment, je vous recommande toujours d'utiliser NT sur le Gateway pour des raisons de stabilité. Cela dit, je n'ai pas encore testé Winroute sur Windows 9x; j'attends donc que quelqu'un m'informe ou me confirme sa stabilité sous ce système. Retenez encore qu'il vaut mieux ne pas faire cohabiter Wingate et Winroute; choisissez l'un ou l'autre, Winroute ayant la fâcheuse tendance de crasher Wingate !!

Préliminaires

Avant d'installer Winroute, je suppose que vous avez lu mon chapitre sur la mise en place d'un serveur Proxy, et que les points suivants sont respectés :

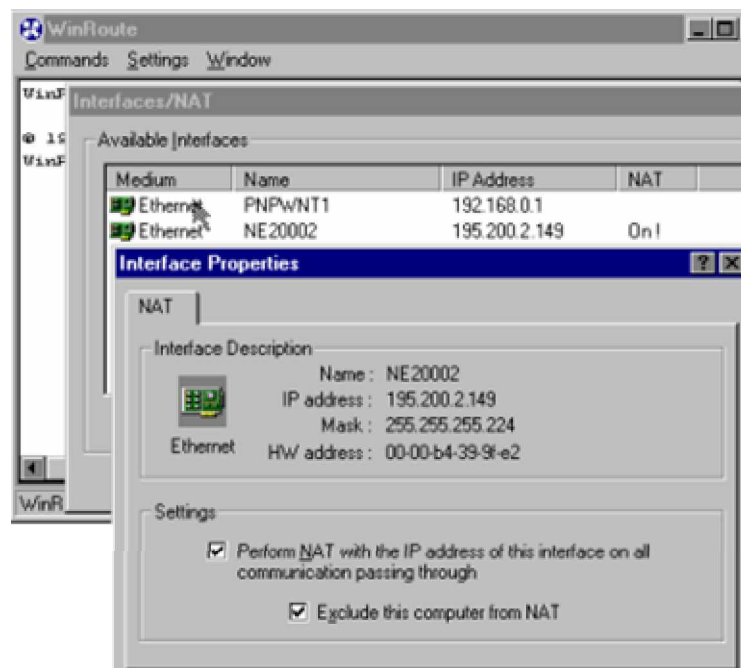
1. Comme TCP-IP est le langage d'Internet, vous avez correctement configuré votre LAN sous ce protocole après avoir assigné à chaque ordinateur une adresse IP propre de type 192.168.0.1, 192.168.0.2, etc... (masque de sous-réseau : 255.255.255.0) et créé le fichier Host adéquat sur chaque ordinateur.
2. Vous savez que votre ISP (Internet Service Provider) vous attribue une et une seule adresse IP lorsque vous vous connectez à Internet.
Cette adresse est souvent fixe (on dit "statique") dans le cas d'un câble-opérateur, et variable (on dit "dynamique") dans le cas d'une connexion par modem (votre ISP a une fourchette d'adresses IP disponibles et vous en attribue une de libre lorsque vous vous connectez).

Installation de Winroute

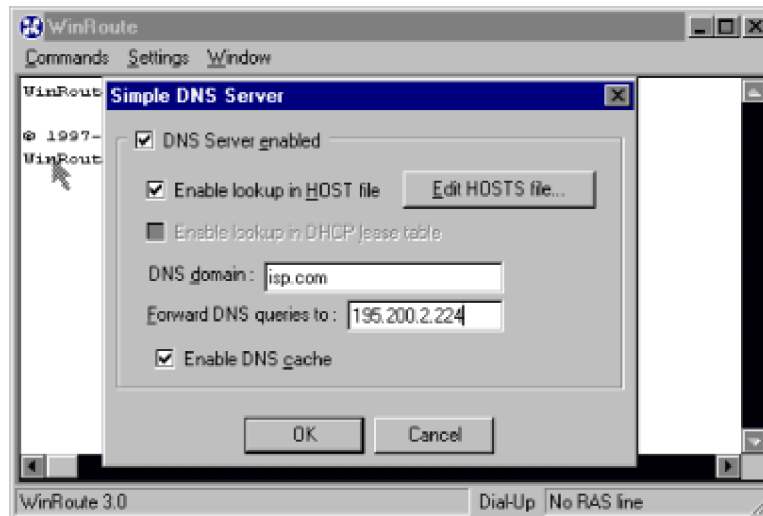
Vous pouvez maintenant installer Winroute sur votre gateway. Il n'y a pratiquement rien à y configurer.

NB : les explications et illustrations qui suivent concernent l'utilisation de Winroute sur un ordinateur connecté à Internet par une carte réseau (câble). Si vous faites cette installation avec un modem, la mise en place est légèrement plus compliquée (configuration RAS), mais ne change pas dans le fond.

- Enclenchez simplement le routage NAT sur l'interface Internet de la façon suivante : dans Winroute, allez sur Settings->Interface Table...->'Votre interface Internet (carte réseau ou ligne modem), et activez le routage NAT :



- Activez le service DNS. Winroute fournit en effet le service de serveur DNS nécessaire aux applications du LAN pour "retrouver leur chemin" sur Internet. Ce service s'active par : Settings->DNS Server. Vous y introduisez les valeurs DNS de votre Provider.



Si vous êtes un peu perfectionniste, vous pouvez donner des règles plus strictes sur le routage des paquets IP. Référez-vous pour cela au manuel on-line (très clair) de Winroute, chapitre "Packet filtering".

Notez aussi que vous pouvez faire en sorte que Winroute ne fasse pas de NAT pour certains ordinateurs. Cela peut être utile si une partie de votre LAN possède des adresses IP réglementaires sur Internet. Dans ce cas, Winroute peut agir comme un routeur simple (sans translation d'adresses). Je ne parle pas ici de ces réglages très particuliers, mais le manuel on-line est très clair sur ces points.

6. Configuration des machines clientes

Contrairement aux réglages parfois subtils qu'il fallait faire pour chaque application des ordinateurs du LAN si vous utilisez Wingate, il n'y a presque rien à faire si vous utilisez Winroute. Il vous faut simplement spécifier au système le serveur DNS et la passerelle.

1. Dans les propriétés du protocole TCP-IP (Panneau de configuration->Réseau->Protocole TCP-IP), sélectionnez l'onglet 'Configuration DNS' et ajouter l'adresse IP (LAN) de l'ordinateur qui fait tourner Winroute.



2. Dans l'onglet 'Passerelle', ajouter l'adresse IP (LAN) de l'ordinateur qui fait tourner Winroute.

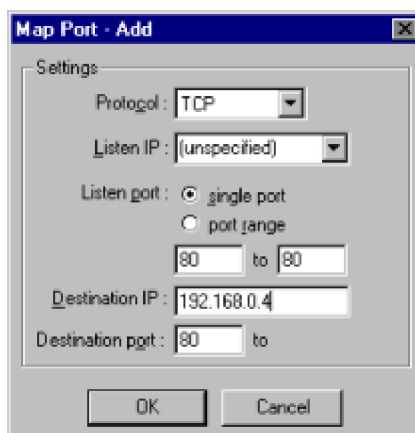


C'est tout ! Rebootez la machine; vous êtes sur Internet !

6. Particularités de configuration

- Si vous voulez faire tourner un serveur (HTTP, FTP, ...) sur une des machines de votre LAN et que vous voulez que ce dernier soit accessible depuis Internet, vous devez spécifier à Winroute un "mapping TCP" sur le port concerné vers l'IP de la machine du LAN.

Exemple : vous voulez faire tourner un serveur Web en port 80 sur la machine 192.168.0.4 de votre LAN. Dans Winroute, choisissez Settings->Advanced->Port Mapping->Add, et rajouter un mapping TCP sur le port 80 :



Notez que les deux ports (sur le routeur et sur l'ordinateur du LAN) n'ont pas besoin d'être identiques. Vous pourriez très bien faire tourner sur l'ordinateur 192.168.0.4 un serveur Web sur le port 8080 (accessible sur ce port dans l'intranet), mais accessible sur le port usuel 80 depuis Internet, et inversement.

- les logiciels susceptibles d'être "appelés" depuis Internet doivent être configurés en conséquence.

Le cas le plus connu est **ICQ**.

Si vous voulez pouvoir être contacté par ICQ, vous devez procéder de la manière suivante :

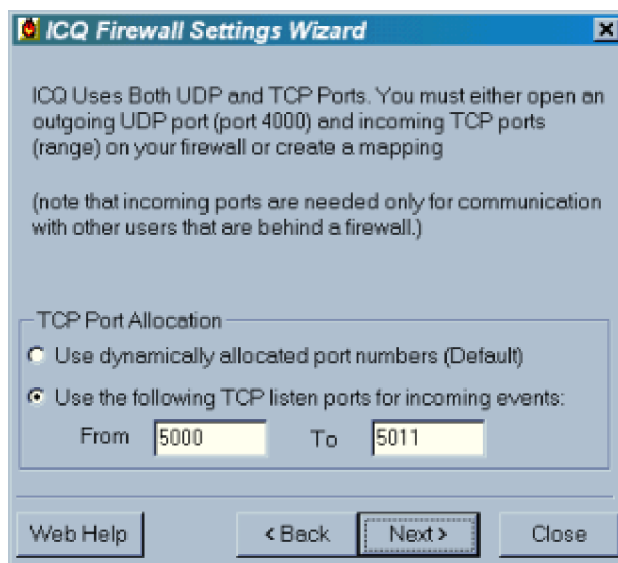
- Sur Winroute, établissez un mapping TCP (voir ci-dessus) sur un intervalle ("port range") de 5000 à 5011 vers l'ordinateur du LAN voulant utiliser ICQ



Pour chaque ordinateur du LAN voulant bénéficier d'ICQ, vous devez créer un intervalle similaire (par exemple, 5012-5023, 5024-5035, etc.)

- Sur le client ICQ de la machine du LAN, allez dans Preferences, onglet connexion, puis choisissez : Internet Connection Type->I am behind a Firewall or Proxy.

Puis dans les "Firewall settings", choisissez 'I don't use a SOCKS Proxy server on my Firewall or I am using another Proxy server', puis 'Use the following TCP listen ports for incoming events', et introduisez l'intervalle adéquat (par ex. 5000 to 5011) :



8. Infos fournies sur la fonction NAT

Utilisation de Winroute

WinRoute 3.04,

Tip: Use right mouse button to pop up a menu

Interface Table:

Medium	Name	IP address	NAT	Index
Ethernet	DC21X40000	10.0.0.140		3
WAN	PPPMAC0001	0.0.0.0		0

ras: Wanadoo connecting ...

ras: Wanadoo authenticated ...

ras: Wanadoo connected, ip address: 164.138.26.25

Interface Table:

Medium	Name	IP address	NAT	Index
Ethernet	DC21X40000	10.0.0.140		3
WAN	PPPMAC0001	164.138.26.25	on	2

TCP/IP stack's Routing Table:

Net	Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	164.138.26.25	PPPMAC0001	1
0.0.0.0	0.0.0.0	10.0.0.129	DC21X40000	2
10.0.0.128	255.255.255.192	10.0.0.140	DC21X40000	2
164.138.0.0	255.255.0.0	164.138.26.25	PPPMAC0001	1

NAT table :

Proto	Source	Through	Destination	Timeout	Bytes	Packets
TCP	10.0.0.141:1059	164.138.26.25:61003	207.46.18.30:80	39:00	41414	72
TCP	10.0.0.141:1060	164.138.26.25:61008	207.46.18.30:80	39:00	9710	40
TCP	10.0.0.141:1062	164.138.26.25:61009	207.46.16.221:80	38:56	11310	21
TCP	10.0.0.141:1066	164.138.26.25:61011	207.46.18.40:80	38:56	568	6
TCP	10.0.0.141:1067	164.138.26.25:61012	198.4.92.21:21	2879:20	850	22
TCP	10.0.0.141:1069	164.138.26.25:61014	198.4.92.21:21	2879:49	850	25

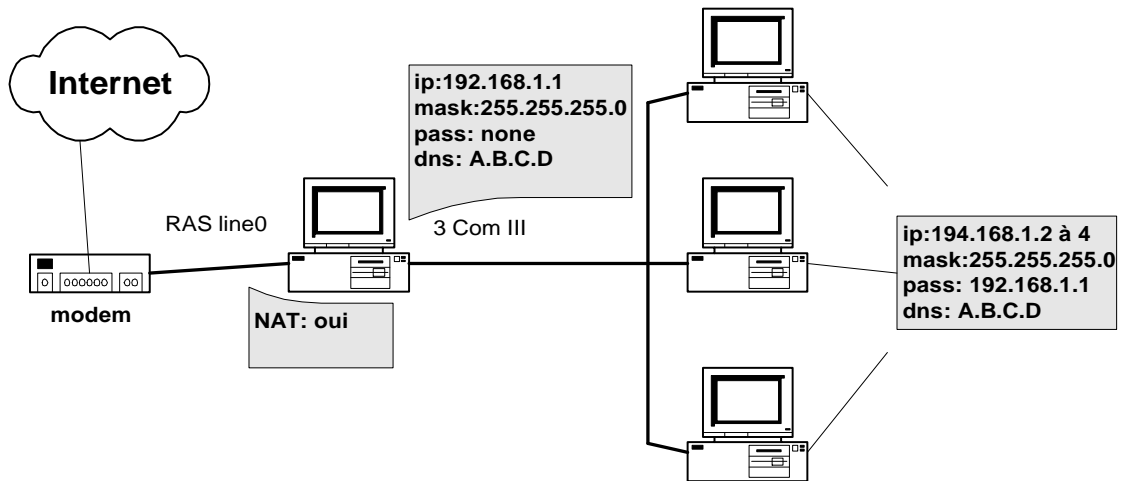
NAT table :

Proto	Source	Through	Destination	Timeout	Bytes	Packets
TCP	10.0.0.141:1067	164.138.26.25:61012	198.4.92.21:21	2875:13	850	22
TCP	10.0.0.143:1045	164.138.26.25:61027	193.252.19.30:119	40:00	750509	865
TCP	10.0.0.141:1072	164.138.26.25:61029	198.4.92.21:21	2879:51	854	22

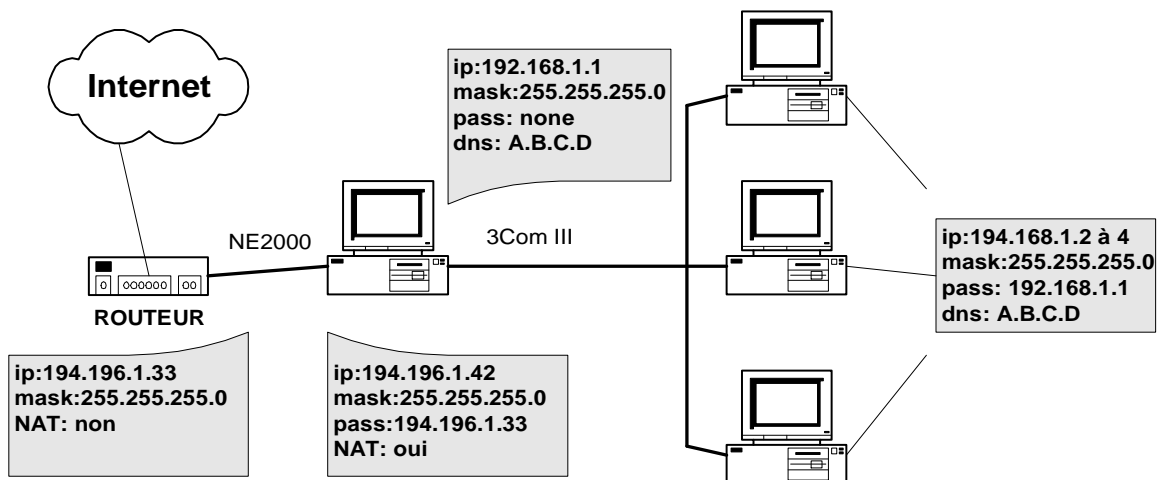
TCP/IP stack's Routing Table:

Net	Mask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	164.138.26.25	PPPMAC0001	1
0.0.0.0	0.0.0.0	10.0.0.129	DC21X40000	2
10.0.0.128	255.255.255.192	10.0.0.140	DC21X40000	2
164.138.0.0	255.255.0.0	164.138.26.25	PPPMAC0001	1

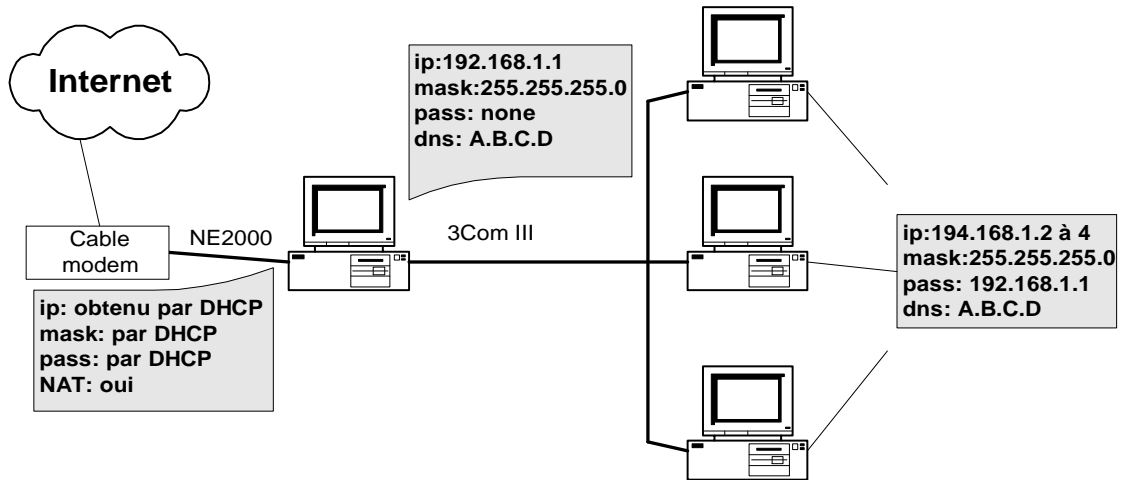
Exemple 1 : LAN 3 machines + 1 machine routeur + 1 accès RAS (RTC ou RNIS)



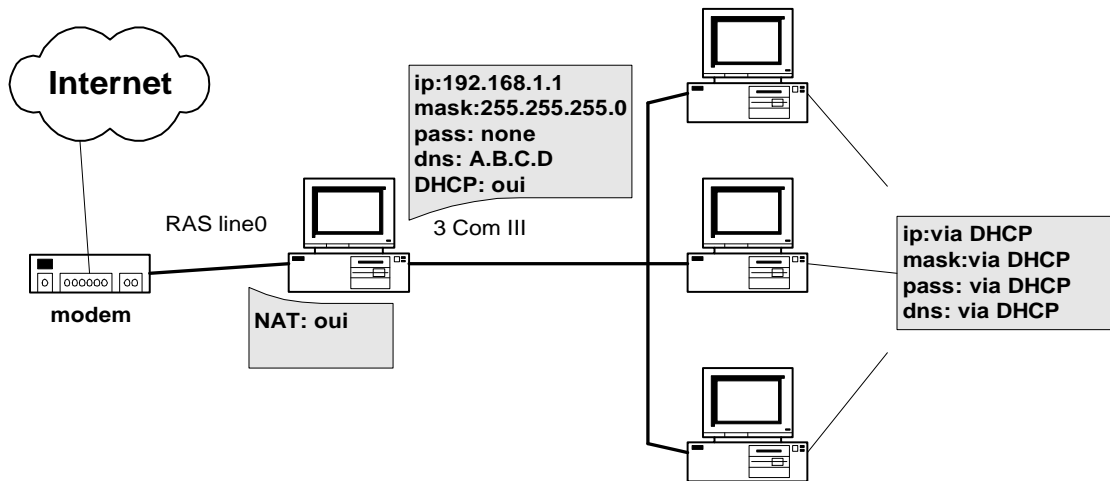
Exemple 2 : LAN 3 machines + 1 machine routeur avec NAT + 1 accès via routeur RNIS



Exemple 3 : LAN 3 machines + 1 machine routeur + 1 accès modem câble



Exemple 4 : LAN 3 machines + 1 machine routeur avec DHCP + 1 accès RAS (RTC ou RNIS)

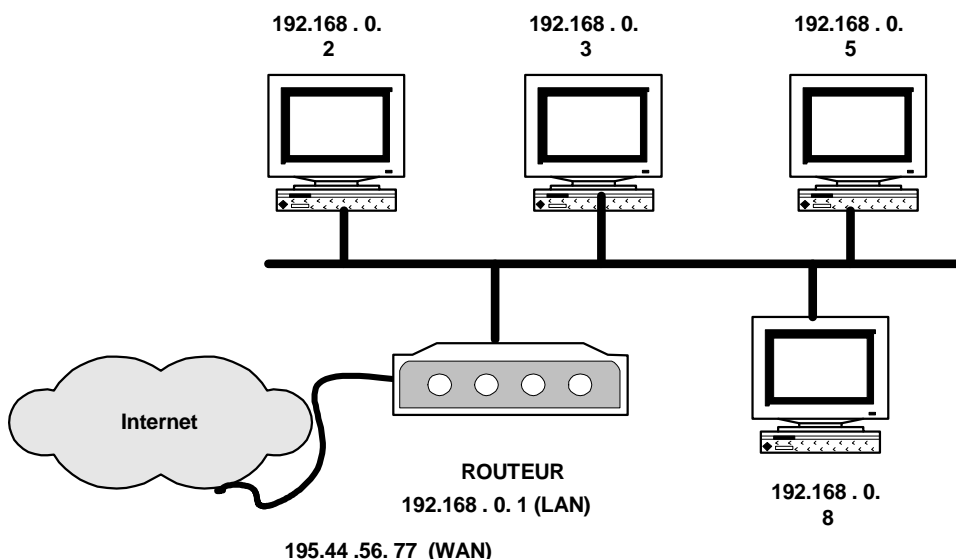


MISE EN PLACE D'UN ROUTEUR AUTONOME

1. Branchement du Routeur
2. Rappels sur le partage d'une connexion unique de la fonction NAT
3. Les principaux critères de sélection d'un Routeur RNIS
4. Résumé
5. L'authentification PAP ou CHAP
6. Comment filtrer les accès
7. Exemples de filtres créés pour le routeur Ascend P50
8. Caractéristiques du routeur Ascend P50

1. Branchement du boîtier

Considérons un réseau local connecté à un **routeur** lui-même connecté à Internet :



Notez que le routeur possède 2 types d'interface réseau:

- LAN (192.168.0.1) il possède une adresse IP du réseau LAN 192.168
- WAN (194.44.56.77) adresse IP généralement attribuée de façon dynamique par le provider

2. Rappels:

- sur le partage d'une connexion unique

Voir routeur soft

- approfondissement sur le transport IP

Voir routeur soft

- le fonctionnement d'un routeur NAT

Voir routeur soft

3. LES PRINCIPAUX CRITERES d'un Routeur RNIS

Devant l'accroissement du nombre de connexions et du volume d'informations à échanger, l'accès à Internet par un modem atteint ses limites. Le routeur d'accès RNIS devient alors essentiel pour les communications de l'entreprise. Avec un routeur RNIS, l'entreprise se dote d'un matériel de communication pour partager, de façon non exclusive, une connexion à Internet, relier plusieurs sites ou autoriser l'accueil d'utilisateurs extérieurs sur le réseau de l'entreprise.

Modems sur ligne téléphonique classique, routeurs ou cartes sur liaison numérique RNIS, routeurs sur lignes louées, tels sont les modes de connexion à Internet les plus courants.

Quand le nombre d'utilisateurs s'accroît, les accès qui allient RTC et modem deviennent rapidement inadaptés à une utilisation professionnelle. Ils entraînent des problèmes de sécurité et de gestion de multiples comptes utilisateurs. S'il est possible de partager un modem sur un réseau local, les débits supportés restent néanmoins limités. Le choix de la ligne louée (de 64 Kb/s à plusieurs mégabits) apparaît plus adaptée et plus souple. Par ailleurs, cette solution n'est pas tributaire du temps de connexion. Mais des coûts élevés découragent les entreprises qui ne considèrent pas le WEB comme un média stratégique.

Le routeur d'agence **SOHO** (*Small Business & Home Office*) RNIS est un compromis technique et financier intéressant pour les groupes d'utilisateurs de quelques personnes. Cet équipement présente de nombreux avantages. Du point de vue économique notamment, l'intérêt est double. Le routeur autorise plusieurs utilisateurs à partager un même accès Internet. Cet équipement est suffisamment évolué pour optimiser la communication RNIS. Si le trafic est nul, le routeur raccroche la ligne et ne la rouvre qu'au moment opportun, ce qui réduit le prix de la facture téléphonique.

Côté performances, tous les routeurs RNIS peuvent travailler sur plusieurs canaux B, c'est à dire à des débits multiples de 64 Kb/s. Cette agrégation de canaux apporte une certaine souplesse et autorise une augmentation du nombre de personnes connectées. Certains modèles supportent même plusieurs adaptateurs RNIS et offrent ainsi des débits de 64, 128, 192, 256 KB/S pour deux cartes RNIS.

Etant donné la diversité et la complexité des routeurs, il m'a semblé nécessaire de préciser les principales caractéristiques que doivent posséder ces appareils. Pour certains critères quelques informations techniques sont fournies pour leur bonnes compréhensions.

Le symbole Y, signifie présent sur le routeur Ascend p50.

PORTS D'ENTREE/SORTIE

- I LAN
 - Hub Ethernet
 - Connecteur RJ45Y; DIXY; BNC

- I WAN
 - RNIS (x voies) Y
 - LS
 - RTC (sortie analogique)
 - Port sérieY

PARAMETRAGE & ADMINISTRATION

Il doit être le plus convivial possible. Ceci n'est pas le cas sur des routeurs de "renom" Cisco ou Ascend !!

- I DOCUMENTATION
 - En français
 - Version papierY
 - CD-ROM (PDF)

- I LOGICIEL D'ADMINISTRATION
 - TelnetY
 - Terminal (via port série) Y
 - Web (HTML)
 - SNMP

- | MISE A JOUR de l'OS
 - Mémoire Flash Y
 - Mise à jour à distance (XModem ou TFTP Y)
 - Possibilité de sauvegarder les paramètres (en local ou à distance) Y

SPECIFICATIONS DE ROUTAGE/PONT

- | LAN
 - IPY, IPXY
 - Appletalk, MacIP
 - Decnet
- | WAN
 - PPPY
 - Multilink PPP (M-PPP) Y
 - Frame Relay (FR) Y
 - Cisco-HDLC

PPP a différents rôles lors du transport des données: l'encapsulation des données IP dans des trames asynchrones ou synchrones, et il permet le réglage des différents paramètres de liaison comme: *la compression; la définition des tailles des blocs et le contrôle du mot de passe.*

- | PROTOCOLE DE ROUTAGE
 - RIP et RIP ILY
 - NATY
 - OSPFY
 - BGP
 - Route statiqueY

SECURITE

- | AUTHENTIFICATION
 - Chap Y ou Chap périodique
 - MS-Chap (Chap de Microsoft)
 - PAPY
 - Secure ID

| NATY

Cette fonction protège votre réseau local des tentatives d'intrusion par le réseau Internet et permet à différents utilisateurs du réseau local d'accéder à Internet simultanément.

| FILTRAGE Y de paquets sur:

- IP source
- IP destination
- Adresse Mac
- Service (FTP; HTTP; TELNET, SMTP ...)
- IPX de Novell

| ENCRYPTAGE

Possibilité d'encrypter le trafic IP et de le transmettre vers des réseaux distants au travers d'Internet

| FIREWALL(Y en option)

- Filtrage plus souple et plus convivial

| RAPPEL ou CALLBACK

| MOT DE PASSE Y pour la fonction administration

COMPRESSION des EN-TÊTES et des DONNEES

- | PPP:4:1Y
- | STAC LZSY
- | Ascend LZSY

CONFIGURATION IP

- | NAT ou SUA (Single User Account) Y
- | Serveur DHCP Y
Permet la configuration automatique de tous les postes du réseau local
- | Services déportés (Static Mapping) Y
Réachemine les demandes d'Internet à des adresses IP privées (serveur WWW par exemple)

COÛTS DE COMMUNICATION

- | Ouverture et fermeture de la ligne RNIS en fonction du flux de données à transférer Y
- | Agrégation des 2 canaux 64 Kbps en fonction du trafic. Soit une transmission à 128 Kbps Y
- | Contrôle de la bande passante Y
 - Multilink PPP vous permet de combiner les canaux dans un "lot Multilink" de sorte à ce que les données puissent être transférées à la meilleure vitesse.
 - Être conforme à la norme BACP (pour dialoguer avec le distant)
- | " Spoofing"
Supprime certaines informations de Broadcast et d'état dans le LAN. Dans tout LAN, des paquets contenant des informations sur l'état du réseau et des stations sont envoyés périodiquement (qq secondes). Ceux-ci engendrent des coûts supplémentaires (prise de ligne RNSI) et sont donc éliminés grâce à la fonction de Spoofing.

DIVERS

- | Nombre de profils de connexion
 - de 1 à 16 Y
- | Nombre d'utilisateurs sur le LAN pouvant accéder à Internet (fonction NAT)
 - 5
 - illimité Y
- | Outils intégrés
 - Ping ;Traceroute Y
 - statistique Y
 - surveillance Y (qui est connecté ? depuis quand ? vers quel service ? ...)
 - autres ...Y
- | Accès à distance Y
 - autorise des appels entrants pour accéder aux ressources du LAN

4. Paramétrage du routeur Ascend P50

Paramétrage pour l'accès au Provider Wanadoo

```

Telnet - 10.0.0.120
Connexion Edition Terminal ?

lqqqqqq FTI/UCVYUG9 EDIT qqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqk
xConfigure... x x10-100 1 x x00-200 02:57:05 x
x>Switch Type=FRANCE ^x x Link X x x>M31 Line Ch x
x Chan Usage=Switch/Switch x x B1 . x x Call Terminated x
x My Num A=207 x x B2 . x x x
x My Num B=208 x lqqqqqqqqqqqqqqqqqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqk
x SPID 1=N/A x x20-100 Sessions x x20-500 DYN Stat x
x SPID 2=N/A x x> 0 Active x x Qual N/A 00:00:00 x
x Ans Voice Call=No x x x OK 0 channels x
x My Name=fti/Ucvyug9 x x x CLU 0% ALU 0% x
x My Addr=10.0.0.120/26 x lqqqqqqqqqqqqqqqqqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqk
x Rem Name=pm.wanadoo.fr x x20-300 WAN Stat x x20-400 Ether Stat x
x Rem Addr=10.0.0.120/26 x x>Rx Pkt: 8972^x x>Rx Pkt: 234983 x
x Dial #=00836019301 x x Tx Pkt: 8810 x x Tx Pkt: 231480 x
x Route=IP x x CRC: 19vx x Col: 40 x
x Bridge=No x lqqqqqqqqqqqqqqqqqqqqqqk lqqqqqqqqqqqqqqqqqqqqqqk
x Send Auth=PAP x x00-100 Sys Option x x00-400 HW Config x
x Send PW=***** x x>Security Prof: 1 ^x x>BRI Interface x
x Recv Auth=None x x Software +6.0.9+ x x Adrs: 00c07b716f1c x
x Recv PW=N/A vx x S/N: 7426012 vx x Enet I/F: AUI x

Press Ctrl-n to move cursor to the next menu item. Press return to select it.
Press Tab to move to another window --- thick border indicates active window.

```

Suite

Configure....

Recv PW=N/A

>SAVE=faire enter

Paramétrage du serveur DHCP

Mod Config

DHCP Spoofing

DHCP Spoofing=Yes

DHCP PNP Enabled=Yes

; accepte les requêtes DHCP client Windows NT et Win-95; Win-98

Renewal Time=65535

; durée de vie du bail exprimé en secondes (de 3 à 65535)

Become Def. Router=Yes

; le routeur devient la passerelle par défaut des postes clients

Dial if Link Down=No

;

Always Spoof=Yes

;

Validate IP=Yes

; recherche l'IP sur le LAN avant de l'attribuer à un client

Maximum no reply wait=5

; évite des conflits d'adresse (délais d'attente pour la réponse)

IP Group 1=10.0.0.80/26

; début de la plage d'adresse à attribuer

Group 1 count=20

; nombre de machines clientes

IP group 2=0.0.0.0/0

; possibilité de spécifier une seconde plage d'adresse

Group 2 count=0

;

Host 1 IP=0.0.0.0/0

; donne la possibilité d'imposer une adresse IP à un client à partir de son

Host 1 Enet=000000000000

; adresse MAC

Host 2 IP=0.0.0.0/0

; idem client 2

Host 2 Enet=000000000000

;

Host 3 IP=0.0.0.0/0

; idem client 3

Host 3 Enet=000000000000

;

TFTP Host Name=

;

Boot File Path=

;

DNS... (permet d'attribuer le(s) DNS aux clients

Domain Name= ; *nom de domaine du provider*
 Sec Domain Name= ; *nom de domaine secondaire*
 Pri DNS=193.252.19.3 ; *spécifie le DNS primaire*
 Sec DNS=193.252.19.4 ; *spécifie le DNS secondaire*
 Allow As Client DNS=Yes ; *affectation des DNS aux clients DHCP*
 List Attempt=Yes
 List Size=10
 Client Pri DNS=193.252.19.3
 Client Sec DNS=193.252.19.4
 Enable Local DNS Table=No
 Loc.DNS Tab Auto Update=No

Comment visualiser l'attributions des adresses IP aux machines ?

Passer en mode commande en pressant CTRL+D à partir du menu Config
 Activer l'option : E Termserv

show dhcp ? Display help information
 show dhcp lease Display DHCP lease Information
 show dhcp address Display DHCP Address Assignment Information

ascend% show dhcp addr

DHCP Configuration Data

DHCP PNP Enabled = Yes
 Renewal Time = 65535
 Become Default Router = Yes
 Dial if Link Down = No
 Always spoof = Yes
 Validate IP = Yes
 Maximum no-reply Wait = 5

IP Address	Hardware Address	Netmask	In Use
10.0.0.80	00:80:c8:58:7b:83	255.255.255.192	Y
10.0.0.81	00:60:97:e1:86:52	255.255.255.192	Y
10.0.0.82	00:a0:24:4a:ec:2b	255.255.255.192	Y
10.0.0.83	????????????????	255.255.255.192	Y
10.0.0.84	????????????????	255.255.255.192	Y
10.0.0.85	????????????????	255.255.255.192	Y
10.0.0.86	00:40:95:45:c6:cb	255.255.255.192	Y
10.0.0.87	????????????????	255.255.255.192	Y
10.0.0.88	????????????????	255.255.255.192	N
10.0.0.89	????????????????	255.255.255.192	N
10.0.0.90	????????????????	255.255.255.192	N
10.0.0.91	????????????????	255.255.255.192	N
10.0.0.92	????????????????	255.255.255.192	N
10.0.0.93	????????????????	255.255.255.192	N
10.0.0.94	????????????????	255.255.255.192	N
10.0.0.95	????????????????	255.255.255.192	N
10.0.0.96	????????????????	255.255.255.192	N
10.0.0.97	????????????????	255.255.255.192	N
10.0.0.98	????????????????	255.255.255.192	N
10.0.0.99	????????????????	255.255.255.192	N

ascend% show dhcp lease

IP Address	Hardware Address	Netmask	Renew in
10.0.0.84	????????????	255.255.255.192	64134
10.0.0.80	00:80:c8:58:7b:83	255.255.255.192	64071
10.0.0.81	00:60:97:e1:86:52	255.255.255.192	64088
10.0.0.83	????????????	255.255.255.192	64099
10.0.0.85	????????????	255.255.255.192	64378
10.0.0.87	????????????	255.255.255.192	64257
10.0.0.86	00:40:95:45:c6:cb	255.255.255.192	64143
10.0.0.82	00:a0:24:4a:ec:2b	255.255.255.192	65347

Comment activer la fonction NAT ?

Ethernet à NAT à NAT à

20-B01 NAT...

```

Routing=Yes           ; active la fonction NAT
Profile=pm.wanadoo.fr ; à partir du profile définit
FR address=0.0.0.0    ; pas de Frame Relay
Lan=Single IP addr    ; il faut activer cette fonction car l'adresse IP est unique et
                       ; dynamique
Static Mappings        ; établit des liens directs avec des serveurs actifs sur le LAN
                       ; (voir exemple)
Def Server=0.0.0.0    ;
Reuse last addr=No     ;
Reuse addr timeout=N/A ;

```

Exemple de Static Mappings

```

Static Mappings
Static Map 01
Static Map 02
Static Map 03
-----
Static Map 10

```

Static Map 01

```

Valid=Yes           ; active la première fonction de static mapping
Dst Port#=80        ; définit le port 80 (pour le serveur WWW)
Protocol=TCP         ; définit le protocole utilisé: ici TCP
Loc Port#=80        ; réserve le port 80 pour la machine
Loc Adrs=10.0.0.71  ; IP du serveur WWW du LAN

```

Cette fonction autorise l'accès au serveur WWW (10.0.0.71) du LAN par les internautes via l'IP attribuée par le provider au routeur.

Static Map 02

```

Valid=Yes           ; active la seconde fonction de static mapping
Dst Port#=21        ; définit le port 21 (pour le serveur FTP)
Protocol=TCP         ; définit le protocole utilisé: ici TCP
Loc Port#=21        ; réserve le port 21 pour la machine
Loc Adrs=10.0.0.71  ; IP du serveur FTP du LAN

```

Cette fonction autorise l'accès au serveur FTP (10.0.0.71) du LAN par les internautes via l'IP attribuée par le provider au routeur.

Remarque: les ports réservés ici 80 et 21 doivent être unique; ce qui n'autorise qu'un accès WWW et FTP par LAN

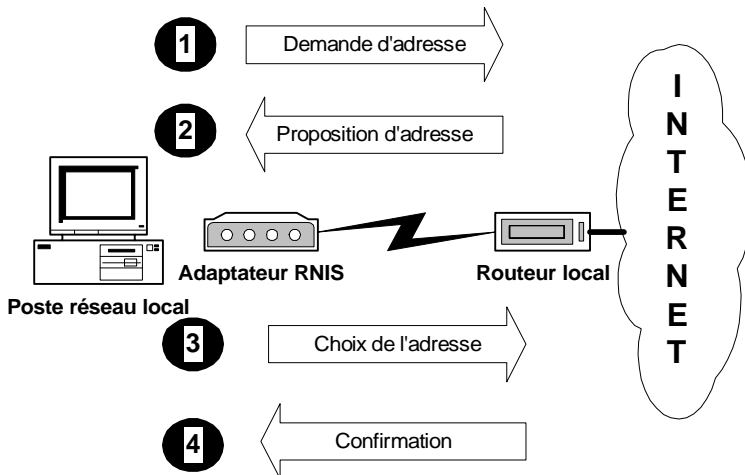
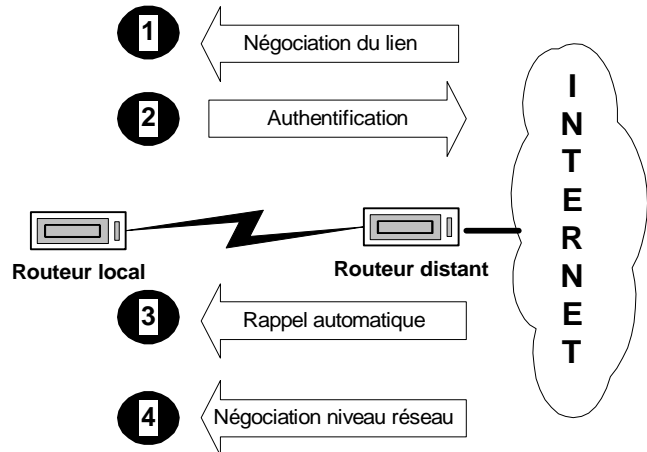
5. RESUME

Les fonctions et les protocoles de l'accès INTERNET par RNIS

Conçu pour fonctionner sur des lignes permanentes, le protocole IP s'est enrichi de toute une série de solutions techniques pour exploiter les modems, les accès RNIS. Aujourd'hui, l'accès via ce réseau est fiable et performant et offre une alternative viable aux lignes louées pour un coût inférieur.

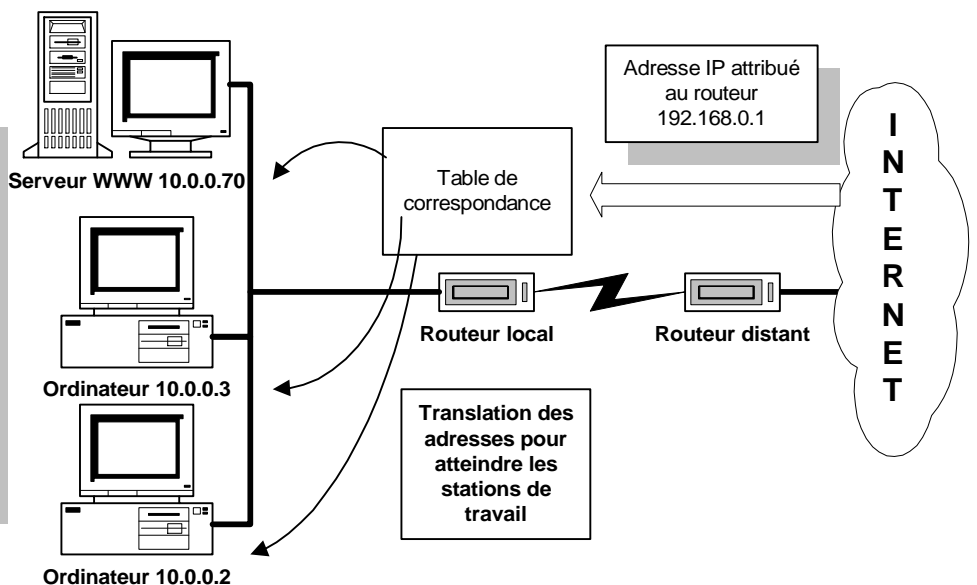
LA CONNEXION A INTERNET

Le protocole PPP (Point to Point Protocol) est l'un des plus utilisés dans l'accès Internet. C'est lui qui gère la transmission d'un routeur ou d'un modem à un autre. Apte à fonctionner avec un grand nombre de protocoles réseau (dont IP), PPP est notamment implémenté sur tous les routeurs RNIS. Il prend en charge la négociation (1) de la transmission, l'authentification (2), éventuellement le rappel automatique (3), et enfin l'établissement de la connexion au niveau réseau (4).



Le protocole DHCP permet de n'utiliser qu'une adresse IP pour tout un réseau local. Le routeur délivre une adresse locale à chaque station. Lui seul peut alors faire la correspondance entre l'adresse délivrée par le fournisseur d'accès (qui peut aussi être dynamiquement allouée) et l'adresse finale des stations. Le routeur se comporte soit comme un serveur d'adresse, soit comme un relais DHCP (celui du fournisseur d'accès, par exemple). L'avantage économique de la solution est évident: on n'utilise qu'un abonnement de type personnel, beaucoup moins coûteux qu'un abonnement d'entreprise où une plage d'adresse réservée est délivrée. En revanche, on ne peut héberger de site WEB visible de l'extérieur, son adresse étant susceptible de changer à chaque connexion.

La translation d'adresse (NAT pour Network Address Translation) partage une même adresse IP entre plusieurs stations, donc présente un avantage économique certain. D'autre part, elle masque l'adresse interne du réseau local. Cette propriété assure un nouveau de sécurité supplémentaire. Cette technique est utilisée autant dans les équipements d'accès distant que dans les logiciels de sécurité tels que les coupe-feu.



6. L'AUTHENTIFICATION PAP et CHAP

La plupart des routeurs acceptent PAP et CHAP. Ces deux protocoles sont de véritables standards, le plus souvent assez performants pour garantir un filtrage efficace. D'autres solutions utilisant des serveurs d'accès d'authentification, sont accessibles via une passerelle, mais, pour bénéficier de cette technique, il faut investir dans des logiciels et des matériels coûteux.

PAP (Password authentication protocol).

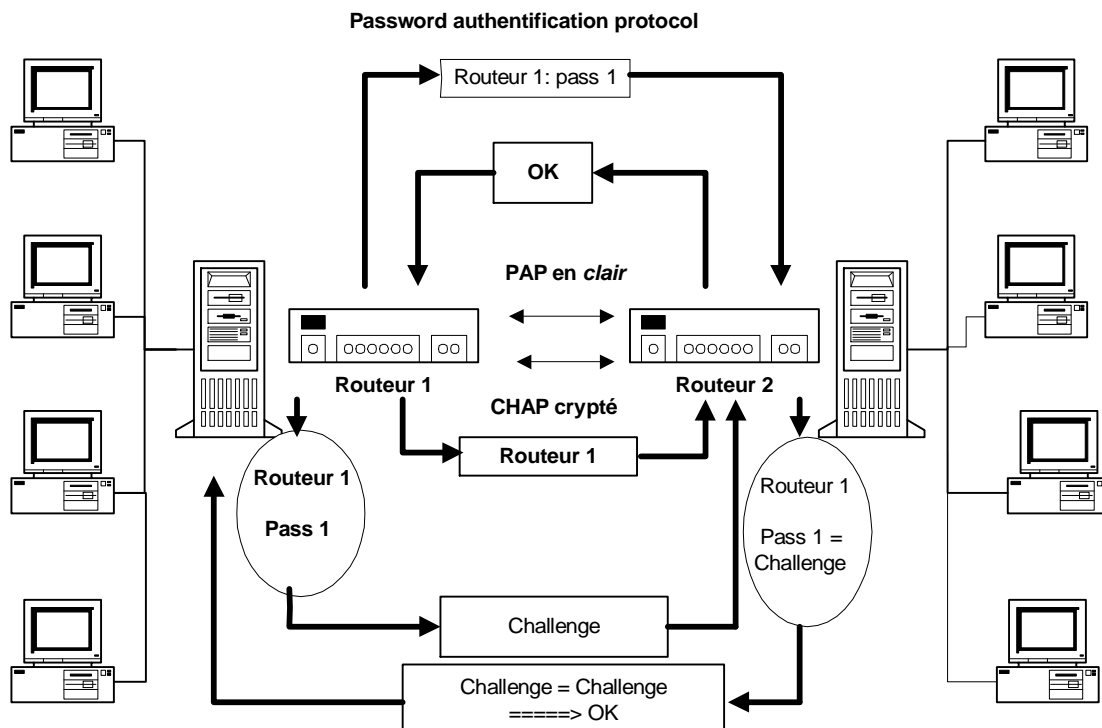
Son principe est simple; il consiste à comparer le nom et le mot de passe fournis par l'utilisateur qui se connecte avec les listes inscrites dans les tables du routeur. Si une correspondance est trouvée, l'authentification est accordée et le réseau est ouvert.

CHAP (Challenge handshake authentication protocol).

Ce protocole présente deux avantages: d'une part, les informations ne sont plus échangées en clair sur le réseau, et, d'autre part, les données transmises ne permettent pas de connaître le nom du routeur ni le mot de passe. Lorsqu'un routeur appelé reçoit une demande d'authentification, son protocole CHAP utilise les informations d'identification inscrites dans ses tables de références pour calculer une valeur appelée *challenge*. Le routeur appelant calcule de son côté un challenge et le transmet au routeur qu'il appelle. Le routeur de destination compare alors les deux challenges et vérifie qu'ils sont identiques. Si c'est le cas la connexion est autorisée. Le challenge est calculé à l'aide d'une fonction mathématique. A aucun moment il n'y a donc échange en clair sur le réseau, non plus que d'informations que l'on peut reconstituer, puisque les fonctions utilisées ne le permettent pas. La sécurité est donc relativement bien assurée.

CHAP périodique. Le routeur identifiant peut, en cours de communication, relancer une authentification CHAP pour s'assurer que la machine qui a été identifiée est bien la même que celle qui est maintenant connectée.

Les protocoles d'identification les plus courants: PAP ou CHAP



7. INFORMATIONS SUR LES LIAISONS SERIE (SLIP; PPP et PPTP)

Il s'agit de liaisons série point à point utilisées principalement sur des liaisons WAN.

Ces 2 protocoles peuvent fonctionner sur des liaisons asynchrones ou des liaisons synchrones.

SLIP (RFC 1055).

C'est un protocole série rudimentaire pour transmettre les datagrammes IP (défini à l'origine pour Unix BSD 4.3 mais non standardisé). Il émet des octets et utilise 2 caractères particuliers :

- **END** (code 192 décimal)
- **ESC** (code 219 décimal). A noter que ces codes ne sont pas les codes ASCII équivalents.

Si un octet de données vaut END, SLIP le remplace par 2 ESC suivi de 220 (décimal).

Si un octet de données vaut ESC, SLIP le remplace par 2 ESC suivi de 221 (décimal).

Quand le datagramme est entièrement transmis, il envoie un code END.

La taille maxi des paquets est de 1006 octets pour BSD, mais ce n'est pas obligatoirement respecté par les autres implémentations.

PPP (RFC 1171). C'est le plus utilisé aujourd'hui.

PPP (point to point protocol) est un protocole standard pour liaisons synchrones ou asynchrones (utilisé par exemple sur Transfix et sur Internet pour les accès via un modem en mode Dial-Up).

Il est basé sur 3 composants : encapsulation de type HDLC, protocole de contrôle de liaison (LCP) et protocoles de contrôle de réseau (NCP). LCP initialise la communication, les protocoles NCP servent à configurer les différents protocoles réseau possibles (IP,...) sur les 2 noeuds de la liaison. Une fois ces paramètres effectués, les datagrammes sont transmis dans des trames de type HDLC simplifié.

La trame PPP (simplification de HDLC) comprend :

- un **Flag** de début de trame (voir HDLC) sur 1 octet de valeur 07h.
- un champ **adresse** de 1 octet fixé tout à 1 (champ inutile puisqu'il n'y a pas d'ambiguïté sur le correspondant).
- un champ **Contrôle** de 1 octet ayant pour valeur 3 (trame UI, mode Datagramme)
- un champ **protocole** sur 2 octets pour identifier le protocole des couches supérieures
- un champ **données** qui comprend le datagramme IP de longueur maxi 1500 octets.
- un champ **FCS** de 2 octets (CRC16)
- un champ **Flag** identique au premier.

Flag	Adresse	Contrôle	Protocole	Données	FCS	Flag
------	---------	----------	-----------	---------	-----	------

Les valeurs possibles pour le champ protocole sont (en hexa) :

0021	IP
0023	CLNP (ISO)
0025	IDP (Xerox)
0027	Decnet Phase 4
0029	Appletalk
002B	IPX (Novell)
8021	IPCP
C021	LCP (Link Control Protocol)

On voit que PPP n'est pas limité à TCP/IP.

LCP est un protocole de gestion de la liaison. Il fonctionne sur la couche liaison. Il comporte 4 phases :

- 1 - Etablissement de la liaison et négociation de la configuration. C'est l'émission de trames pour négocier la longueur maxi du paquet, la méthode d'encryptage, etc...
- 2 - Détermination de la qualité de la liaison. c'est une phase optionnelle pour déterminer si la liaison est de qualité suffisante pour supporter le protocole de réseau choisi.
- 3 - Négociation de la configuration du protocole réseau, pour configurer la couche réseau
- 4 - Pilotage de la fin de la liaison.

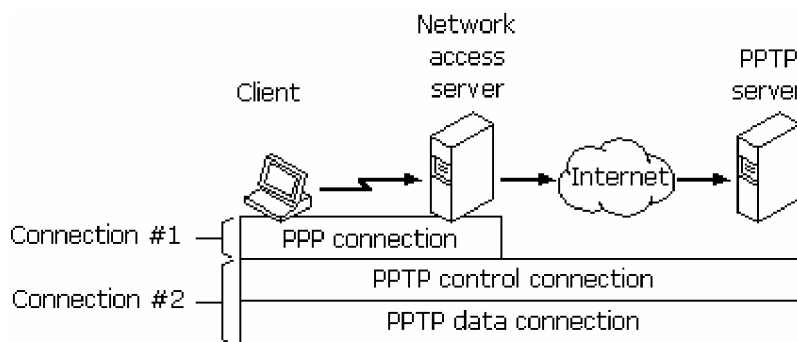
Il a une trame d'établissement et une autre de fin de la liaison. Ces trames comportent le champ protocole à C021h.

IPCP (IP Control Protocol) est un protocole de la famille NCP (le seul défini dans un RFC) qui sert à initialiser le protocole IP (niveau réseau) à chaque extrémité de la liaison avant l'échange des datagrammes IP. Ces trames spécifiques ont le champ protocole à 8021h.

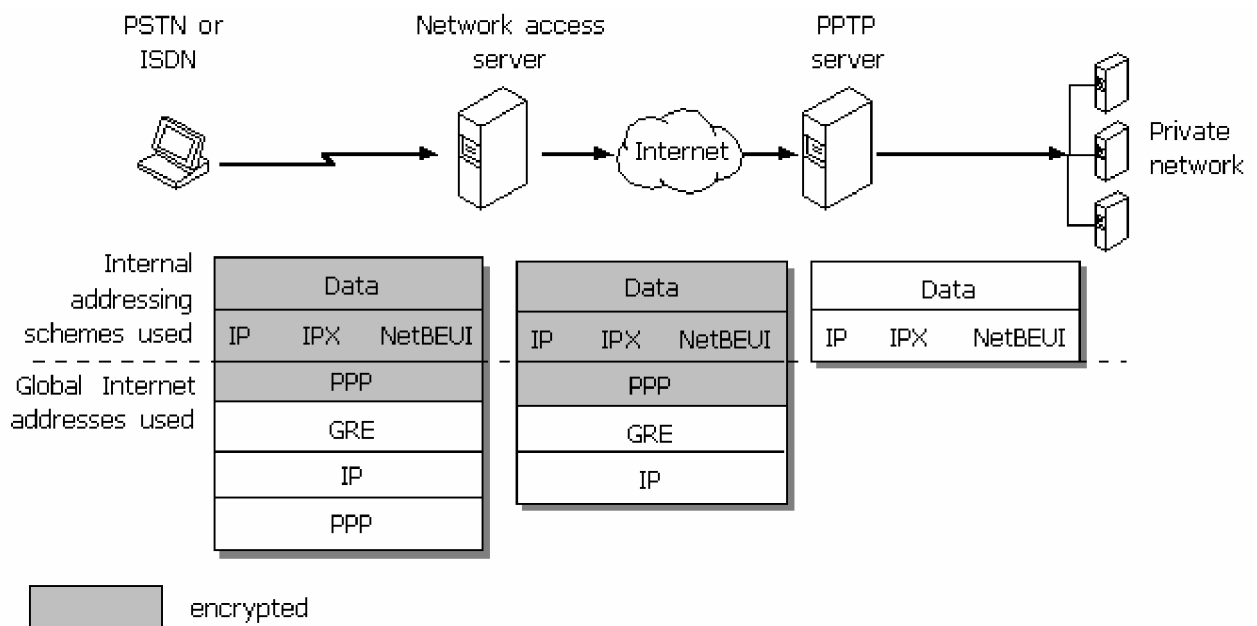
Une 'session PPP' commence d'abord par la mise en œuvre de LCP, puis de IPCP suivi des échanges IP. Pour la libération, c'est l'inverse : phase IPCP puis LCP.

PPTP (Point to Point Tunnelling Protocol)

Ce protocole apporte un moyen d'utiliser des réseaux de données publics, tels Internet pour créer des réseaux privés virtuels (VPN) connectant des PC clients à des serveurs.

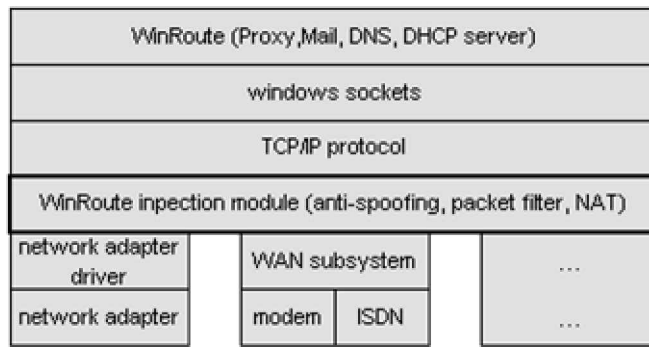


Il offre l'encapsulation de protocole pour supporter de multiples protocoles via des connexions TCP/IP et l'encryptage de données pour les rendre privées, ce qui sécurise l'envoi d'informations sur des réseaux non sécurisés tel qu'Internet. Cette technologie étend les possibilités de connexion à distance en permettant l'accès distant et en étendant les réseaux privés de façon plus sûre sur Internet sans devoir changer de logiciel client.



Ce protocole développé par Microsoft est le plus répandu. Il est intégré en standard dans les systèmes d'exploitation NT 4.0 et Windows 98.

8. Filtrage de paquets TCP/IP

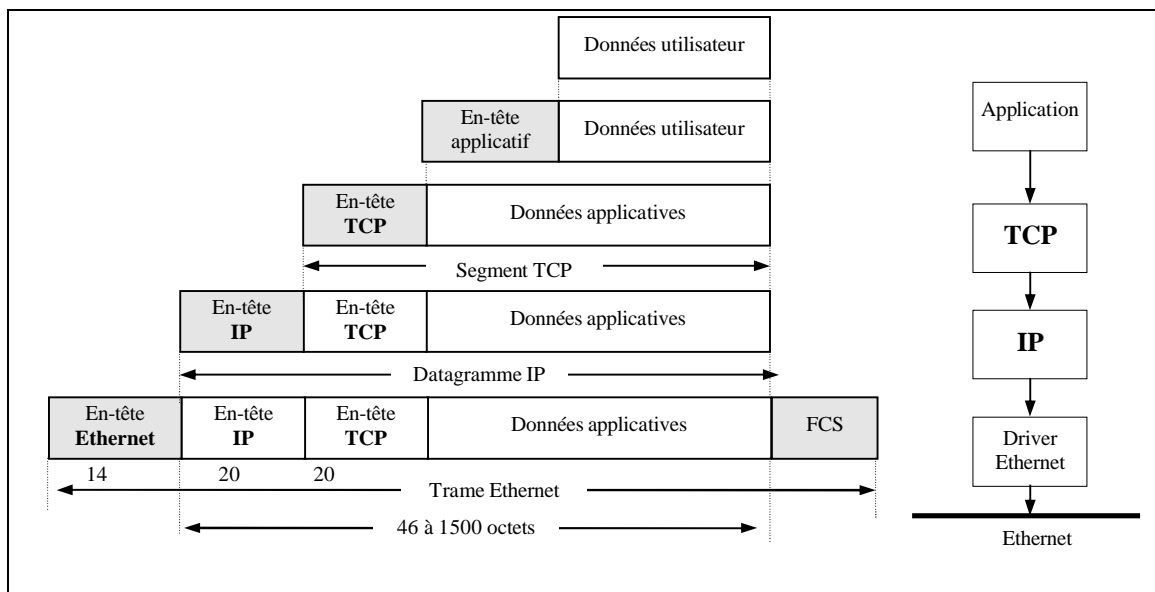


Il est important de bien comprendre comment les paquets TCP/IP sont manipulés au niveau des couches du protocole TCP/IP

Dans chaque couche, le contenu d'un paquet peut être divisé en deux parties : *l'entête et les données* (data).

- **L'entête** contient des informations de contrôle de la couche concernée.
- **Le champ Data** contient pour sa part les données qui doivent être envoyées à la couche supérieure.

Chaque couche ajoute sa propre entête, c'est ainsi que le paquet TCP/IP ressemble à ce qui est représenté ci-dessous.

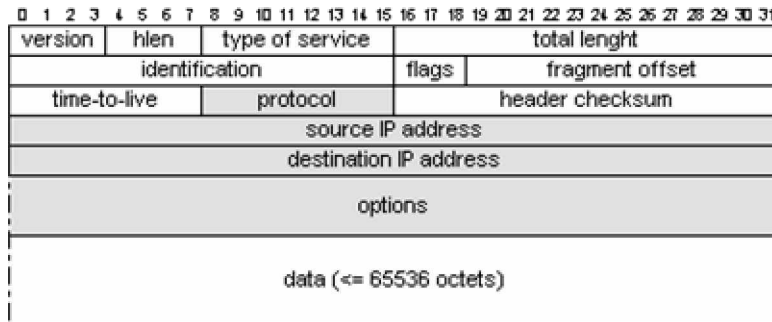


Filtrage à partir de la couche IP (couche réseau)

..... définition : Ce protocole détermine le chemin à emprunter par les paquets pour arriver à destination.

Informations pouvant être utilisées pour la conception de filtre :

- adresse IP source
- adresse IP destination
- type du protocole de la couche supérieure utilisé (TCP, UDP, ICMP ...)
- champ IP option

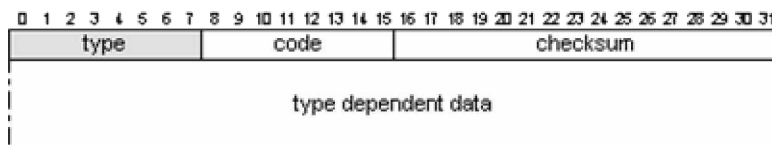


Filtrage à partir de la couche ICMP (couche réseau)

..... définition : Ce protocole est utilisé pour transmettre des messages d'erreur et de contrôle entre chaque station.

Informations pouvant être utilisées pour la conception de filtre :

- ICMP type de message

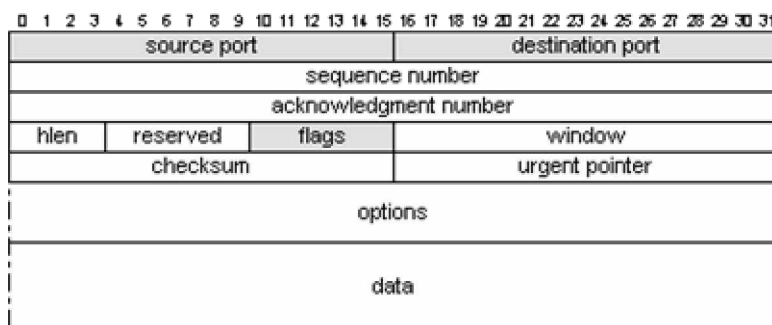


Filtrage à partir de la couche TCP (couche transport)

..... définition : Ce protocole permet d'effectuer une transmission fiable des données (mode connecté + accusé de réception des paquets reçus).

Informations pouvant être utilisées pour la conception de filtre :

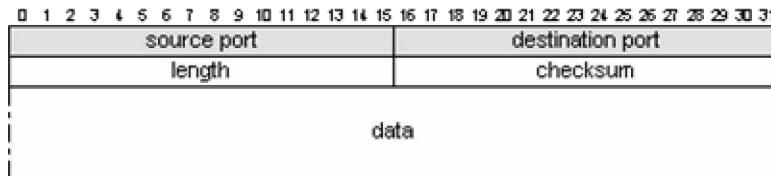
- PORT source
- PORT destination
- Flags



Filtrage à partir de la couche UDP (couche transport)

..... définition : Ce protocole permet d'effectuer une transmission non sécurisée (mode non connecté et pas d'accusé de réception des paquets reçus).

- PORT source
- PORT destination



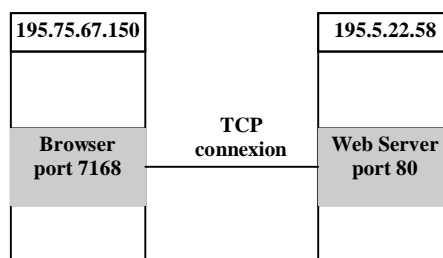
Attribution des numéros de port utilisés par chaque application

Dans l'environnement Internet, il existe deux sortes d'applications :

- application **Client**
- application **Serveur**

C'est ainsi qu'un navigateur WWW (Microsoft explorateur) est une application client, tandis qu'un serveur WWW est évidemment une application serveur.

Pour communiquer, l'application cliente établit une connexion avec un des serveurs. Les différentes applications du serveur attendent une requête d'un client sur un **port fixe** dont le numéro est généralement inférieur à 1024. Il en va autrement des applications client qui elles ne nécessitent pas de numéros de port fixe, c'est ainsi qu'un numéro de port dynamique leurs est attribuées. Les numéros de port dynamique attribués sont supérieurs à 1024.



Principe de filtrage:

- **1.** On filtre ce que l'on ne veut pas, on laisse passer le reste; tout ce qui n'est pas interdit est autorisé.
- **2.** On laisse passer certains trafics, on interdit tout le reste; tout ce qui n'est pas permis est interdit.

Le 2. Est bien plus efficace que 1. Comme protection.

Tous les routeurs filtrent sur les adresses IP et sur les champs significatifs de la trame. Ces sécurités ne constituent qu'une première ligne de défense.

Le filtrage consiste en une analyse de la trame reçue. On identifie d'abord les adresses source et destination, les protocoles (services) et les numéros de ports sollicités.

Puis on les confronte à un ensemble de règles de rejet ou d'acceptation.

Dans ce cas, il convient d'organiser, si possible, l'ordre d'exécution des filtres. Le parcours séquentiel restant le plus consommateur de temps CPU.

Enfin, un filtrage sur les adresses IP ou sur les numéros de ports TCP et UDP apporte une sécurité limitée.

Le routeur reste aveugle aux protocoles des couches supérieures. Ainsi, sur Telnet, il ignore les noms des utilisateurs autorisés ainsi que leur mot de passe.

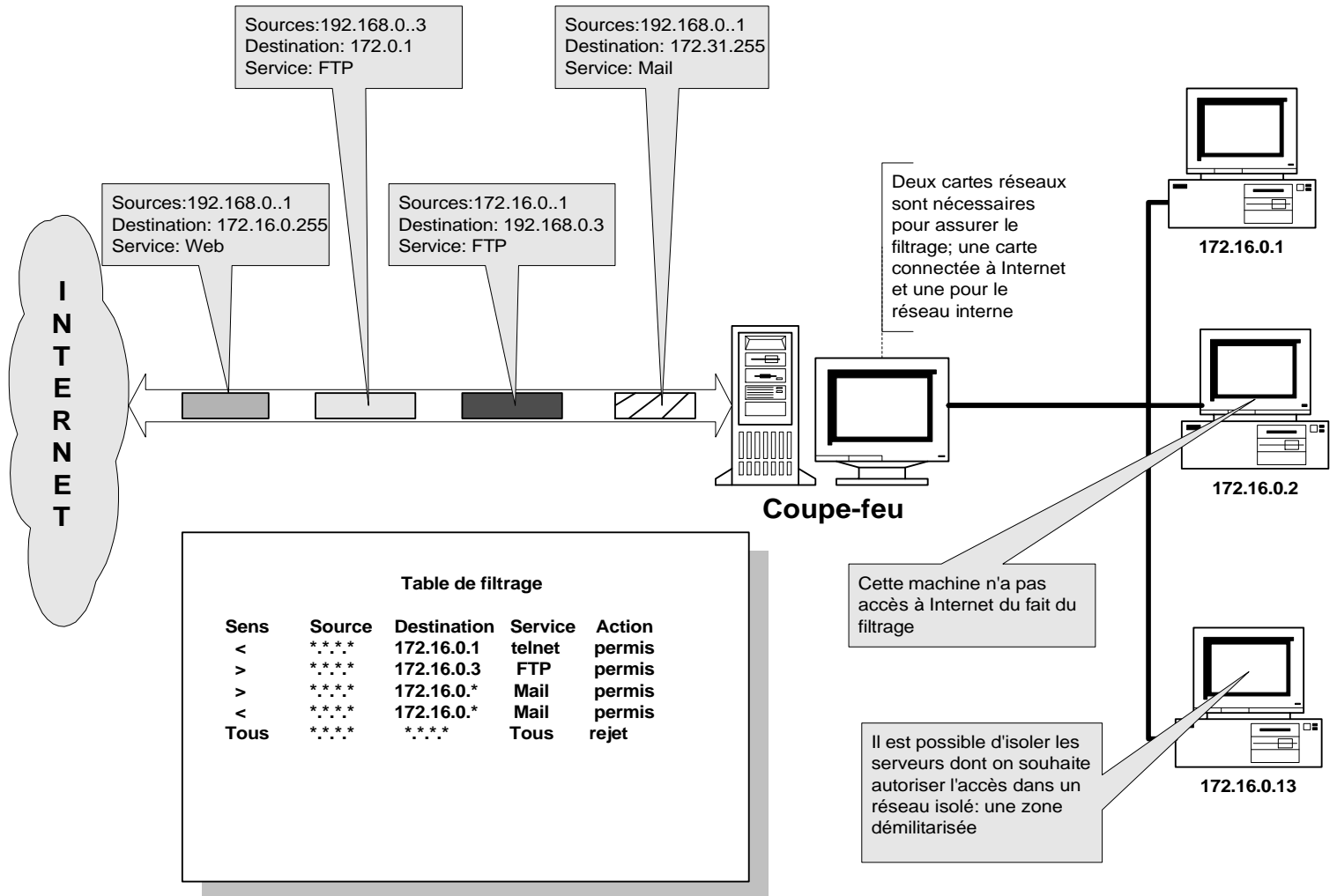
Le filtrage effectué par un routeur ne constitue qu'un des composants de la sécurité.

8.. EXEMPLES DE FILTRES créés pour le routeur Ascend P50

Principe de filtrage par paquet

Avec l'ouverture des entreprises à Internet, la sécurisation des accès est devenue un besoin essentiel. Les coupe-feu (fire-wall) sont une solution.

Le coupe-feu doit trier à la volée les informations entrant et sortant en fonction des règles établies.

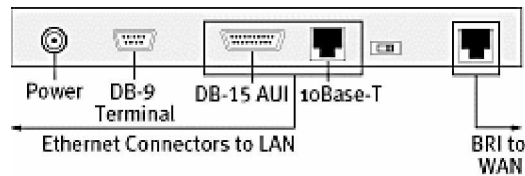


Le coupe-feu n'est pas l'arme absolue pour contrer les accès indésirables. Une politique doit être mise en place afin de formaliser les services ouverts à l'extérieur ainsi que les droits de chaque utilisateurs à accéder aux services tant internes que sur Internet.

Le paramétrage est essentiel dans l'efficacité d'un coupe-feu. Une configuration erronée ou incomplète ne pourra garantir l'efficacité globale du système. La configuration initiale du coup-feu doit être effectuée par un spécialiste.

Généralant peu de charge réseau, le coupe-feu peut se contenter d'un serveur d'entrée de gamme lorsque l'on privilégie le filtrage des informations au format IP. Toutefois, il est préférable de dédier exclusivement cette machine à cette tâche.

9. Spécifications techniques du routeur Ascend P50



Hardware Specifications:

Dimensions 8.63 in. X 6.19 in. x 1.25 in./22 cm x 15.7 cm x 3.2 cm

Weight 2.5 lbs / 1.13 kg

LAN Interface 10 Mbps Ethernet (AUI, 10Base-T)

WAN Interfaces BRI U Interface (model: P50-1UBRI) BRI S/T Interface (model: P50-1SBRI)

Software Upgrade Via built-in flash RAM

Power Requirements 90-130VAC, 0.4A 220-240VAC, 0.2A 47-63HZ

Operating Requirements Temperature: 32-104°F/0-40°C Altitude: 0-14,800 feet/0-4,500 meters Relative Humidity: 5-90% (non-condensing)

Safety Certifications FCC Class B, CSA, UL

EMI/RF FCC Part 68, FCC Part 15

Software Specifications:

Protocols Supported TCP/IP, IPX and AppleTalk routing, BCP standard bridging of all protocols, Network Address Translation, DHCP

WAN Protocols Supported PPP, Multilink PPP (MP), Multilink Protocol Plus (MP+)

Bandwidth Management MP, MP+, TCP header compression, STAC data compression, Bandwidth Allocation Control Protocol (BACP)

Security PAP, CHAP, Callback, Telnet password, token-based security, CLID, packet filtering, optional Secure Access Firewall

Encryption Integrated dynamic firewall (optional)

Management SNMP, Telnet, Syslog, Ascend's remote management protocol, direct serial cable connection (DB-9)

Advanced Remote Networking Solution for Small and Remote Offices

Digital technology provides reliable remote network connections

The Pipeline 50 uses an ISDN BRI line to make resilient remote connections to the corporate LAN or the Internet. Simultaneous connections to different locations can be made using a single digital line.

- Standard U interface (National ISDN 1 compliant) eliminates the need for an external NT1 device (S/T model also available)
- Certified for operation in more than 40 countries worldwide

Centralized Management Capabilities Simplify Maintenance of Remote Sites

Remote management capabilities reduce the cost of installation and ongoing support by enabling network managers to monitor and troubleshoot remote user problems directly from the central site. Network managers can continuously "finetune" the network at anytime, either locally or remotely.

- SNMP MIB II support
- NavisAccess™ software for extensive and complete control of all devices, components and services
- Telnet remote management
- Ascend remote management protocol
- Syslog
- WAN loopback
- Flash memory for easy software upgrades

Concurrent routing and bridging ensures efficient connectivity to all LANs and the Internet

Concurrent routing and bridging eliminates the need for two separate devices by providing one configurable solution for accessing any LAN and the Internet.

- IP, IPX, and AppleTalk routing
- BCP standard multiprotocol bridging
- PPP, Multilink PPP, Multilink Protocol Plus™ (MP+) and Bandwidth Allocation Control Protocol (BACP)

SmoothConnect ensures easy and cost-effective connectivity

SmoothConnect™ provides all the features and functionality that make it easy and cost-effective to connect to a corporate headquarters or the Internet. It allows even novice users to configure and setup their Pipeline for access, removing the barriers that used to make remote connectivity cumbersome. In addition, SmoothConnect reduces costs by making efficient use of protocols and bandwidth. This new functionality includes the following ease-of-use and cost savings features:

- The Java-based Pipeline Configurator (JBPC) is a state-of-the-art configuration utility for graphical point-and-click Pipeline setup and configuration
- Touch tone configuration of ISDN B-channel telephone numbers using an analog telephone
- AutoSwitch and AutoSPID detection automatically detects the ISDN switch type and SPID numbers
- Ascend's patented Dynamic Bandwidth Allocation™ saves money by increasing/decreasing bandwidth as needed for the duration of your connection
- Integrated idle timer allows Pipeline users to remain connected without paying for telecommunications resources when they aren't being used
- Network Address Translation (NAT) eliminates the need to pay for a dedicated TCP/IP address by allowing the Pipeline to accept a dynamically assigned address from a central-site pool of addresses
- Dynamic Host Configuration Protocol (DHCP) spoofing allows network managers to configure and dynamically assign IP addresses across multiple clients from the Pipeline
- Data compression that boosts throughput up to 512 Kbps to handle bandwidth-intensive files

Comprehensive security for iron-clad remote networking

Support for user authentication makes it easy to manage the security of large-scale remote access applications

- Authentication profiles: PAP, CHAP, Calling Line ID (CLID)
- Token-based security with support for multiple vendors' products
- Callback assures connections are made with known users
- Transmit and receive packet filtering
- Ascend Secure Access™ Firewall and encryption option provides complete network protection
- Telnet password

Built-in Ethernet interface maximizes performance and compatibility

The Ethernet interface gives you the flexibility to connect any type of computer directly to the Pipeline 50. With 10 Mbps Ethernet, you can take advantage of the full throughput of an ISDN BRI line.

- Supports multiple platforms (PC, UNIX workstation, or Macintosh)
- Supports varying software configurations

Network Address Translation

Pipeline 50, 75, 85, 130 and 220 users can avoid paying for a dedicated IP address with the Network Address Translation (NAT) capability. When a Pipeline user connects to the Internet or any other IP network, a network address can be transparently assigned to the user for the duration of the connection session. And when NAT is used in conjunction with the Dynamic Host Configuration Protocol (DHCP) spoofing, IP address management becomes a breeze. Network managers can configure and dynamically assign IP addresses to multiple workstations on the remote office LAN in one easy step

ACCELERATION DE LA CONNEXION A INTERNET

Si vous avez lu mon chapitre sur le protocole TCP-IP, vous avez compris que l'information qui circule sur Internet est découpée en de nombreux petits morceaux qu'on appelle des paquets IP.

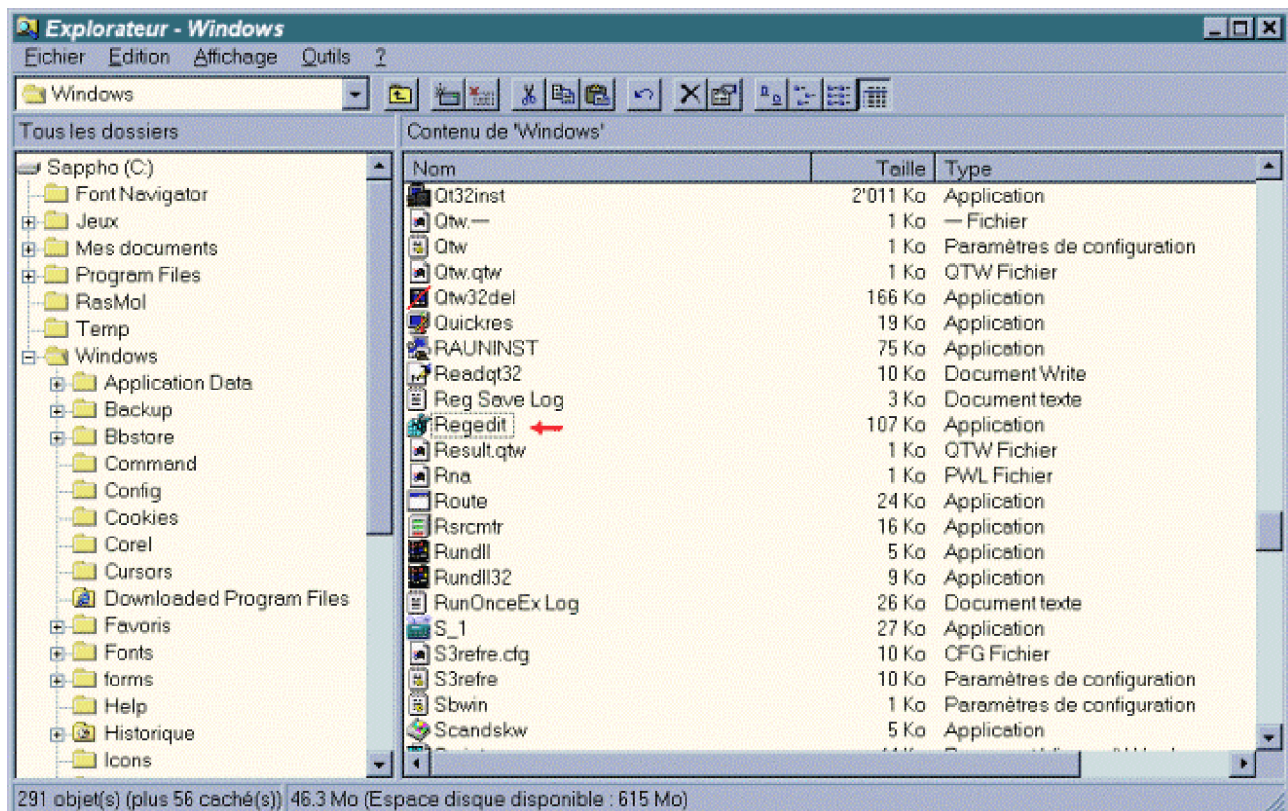
Sans rentrer dans les détails, ces paquets sont censés être suffisamment petits pour se "faufiler" facilement à travers les routeurs d'Internet. Fait incompréhensible : la taille des paquets IP utilisés par un ordinateur sous Windows 95 est beaucoup trop importante. En fait, Microsoft a attribué aux paquets IP devant circuler sur Internet la même taille qu'aux paquets qui circulent sur un réseau local (beaucoup moins "encombré") !

Heureusement, la taille de ces paquets peut être redéfinie dans la base de registre. De cette façon, il est possible d'accélérer, sans rien payer, sa connexion à Internet. N'attendez pas cependant un doublement des performances ! Dans de nombreux cas, vous ne verrez même pas de différence; dans certains cas, vous pouvez attendre jusqu'à 10% d'amélioration, pas beaucoup plus, mais c'est toujours ça !

Avant de "bidouiller" quoi que ce soit, **je dois vous mettre en garde** : la base de registre de Windows est un objet sensible; des modifications hasardeuses PEUVENT RUINER TOUT VOTRE SYSTEME ! Je vous prie donc de ne pas modifier des paramètres que vous ne connaissez pas ou dont vous n'êtes pas ABSOLUMENT sûr. Bien évidemment, je décline tout accident qui pourrait arriver sur votre ordinateur à la suite de modifications dans votre base de registre. Cependant, je veux quand même rassurer ceux qui transpirent déjà à l'idée de toucher la "Sainte Base de Registre" : les quelques modifications à effectuer ne portent pas préjudice à des éléments systèmes, mais uniquement à des paramètres réseaux. Il est possible n'importe quand de tout annuler.

Dans votre intérêt, je vous prie de noter les valeurs initiales des différentes clés que vous allez modifier (si elles existaient déjà) avant de faire une quelconque modification. Vous pourrez ainsi à tout moment remettre vos anciens paramètres si vous n'êtes pas satisfait de la manipulation. Trêve de bavardages, voici donc la manière de procéder.

Rappel : pour ceux qui n'ont jamais entendu parler de la "base de registre" de Windows, cette dernière est une sorte de base de données qui contient tous les réglages du système d'exploitation et des différentes applications. Elle est composée de deux fichiers cachés qu'on trouve sous c:\windows\, *system.dat* et *user.dat*. Ces fichiers ne sont pas interprétables directement dans un bloc-note; par contre, Windows 95 est fourni avec un programme qui permet de lire la base de registre et en modifier certaines entrées : REGEDIT.EXE, qu'on trouve dans le répertoire c:\windows\. Pensez à en créer un raccourci sur le bureau si vous comptez souvent la consulter.



La base de registre se présente sous la forme d'une arborescence en arbre complexe. Je ne vais pas m'attarder ici sur les différents "chapitres" (ou "clés") qui la constituent, mais vous pouvez trouver de nombreux ouvrages qui en parlent. Il vous suffit de suivre les points suivants pour le cas qui nous concerne.

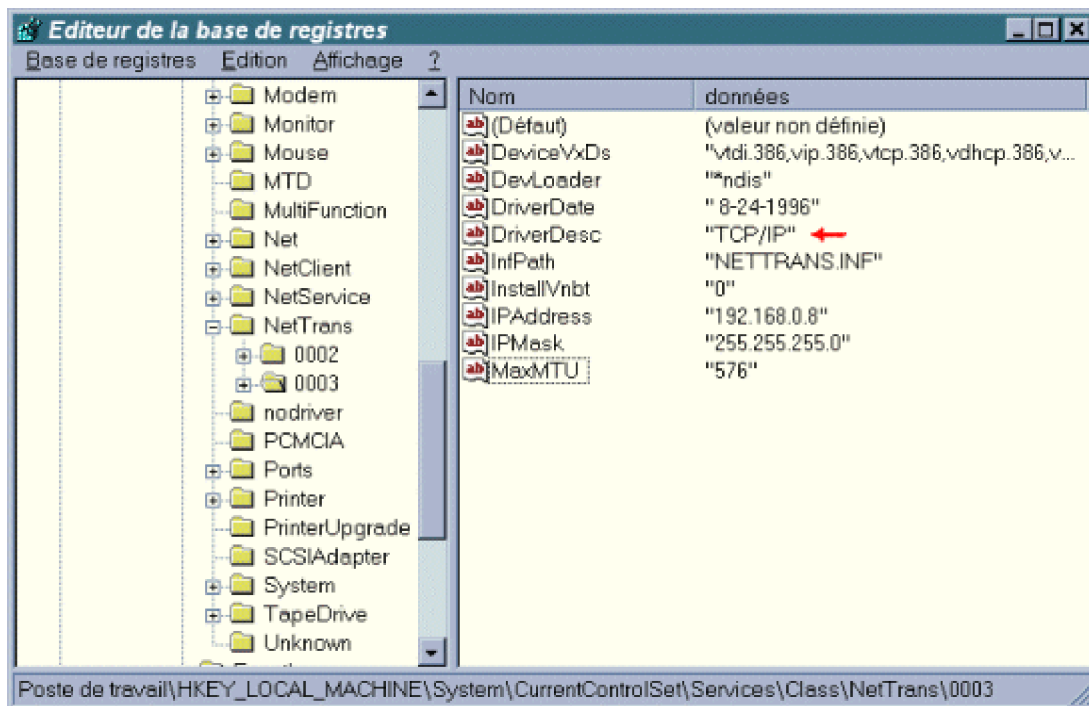
1. Diminution de la taille MTU (Maximum Transmission Unit)

Dans la base de registre de Windows 95, développez l'arborescence :

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/Class/Nettrans/000x/

où 000x (exemple 0002) correspond à la carte communiquant avec Internet (c'est la branche où vous trouvez une clé nommée "DriverDesc" qui a pour valeur "TCP/IP").

Rajoutez la valeur chaîne "MaxMTU" (en faisant Edition, nouveau, valeur-chaîne), et attribuez-lui (en double-cliquant dessus) la valeur 576.



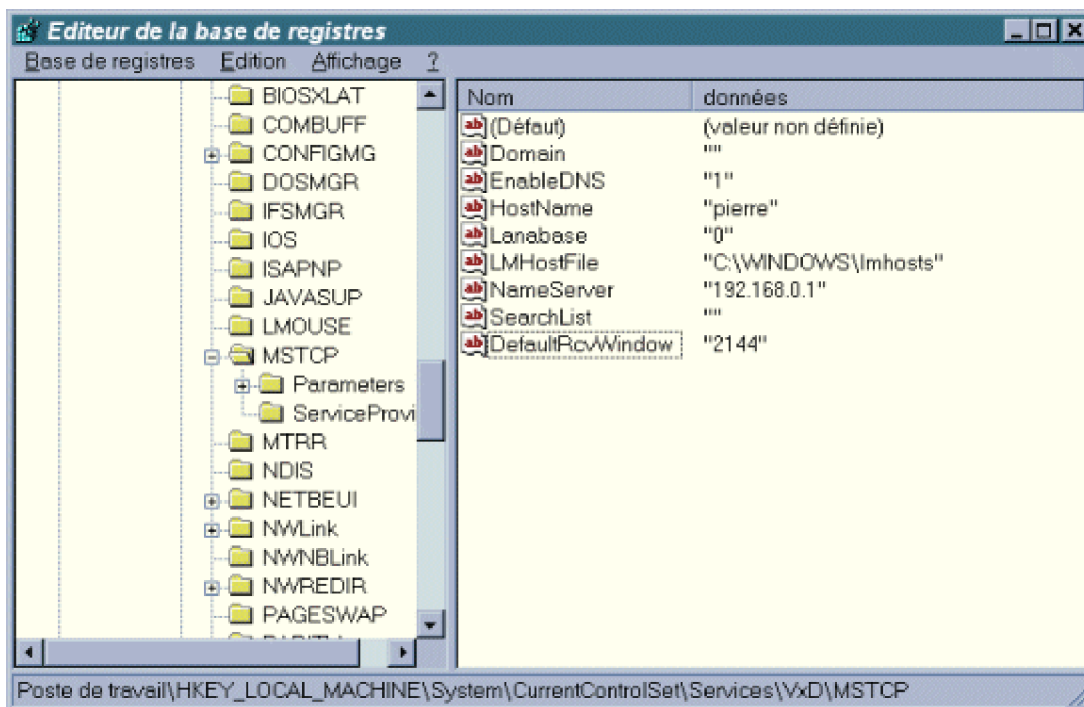
NB : la valeur MTU par défaut est de 1500 bytes; cette valeur est jugée trop importante pour que les paquets IP puissent passer partout (routeurs, ISP, ...) sans problème.

2. Modification de *RWIN* (*Receive WINDOW*)

Dans la base de registre de Windows 95, développez l'arborescence :

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/VxD/MSTCP/

Créez, ou modifiez si elle existe déjà, la valeur chaîne "DefaultRcvWindow" en 2144.



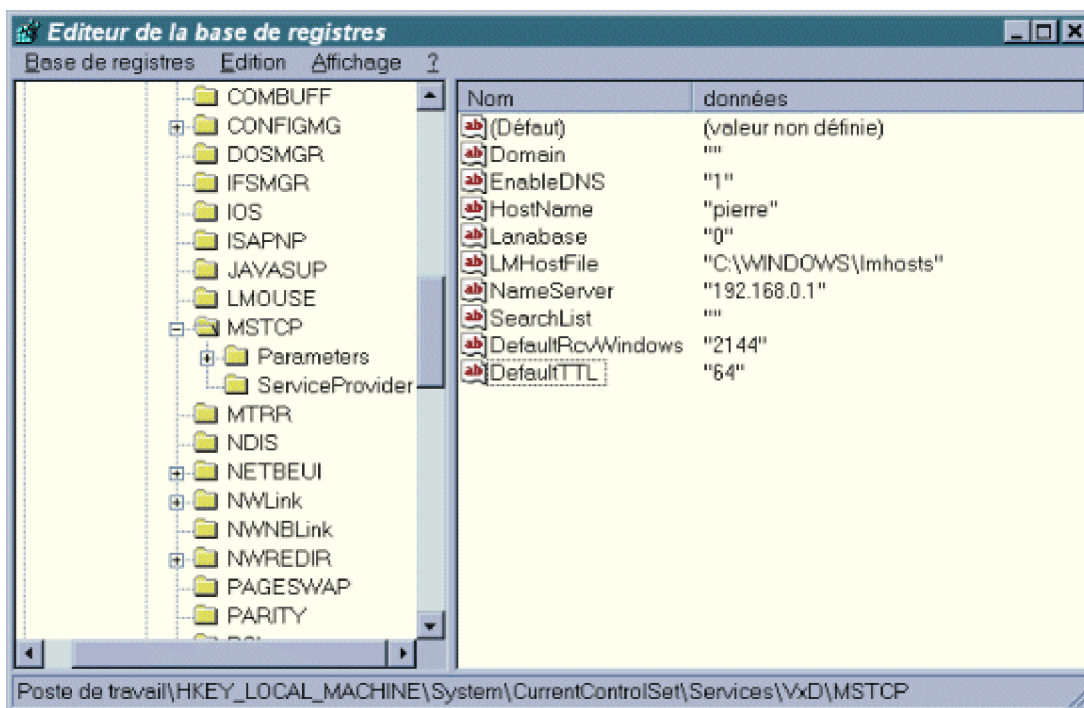
NB : la valeur de base RWIN prescrite par Microsoft est 8192 (typique d'un LAN).

3. Modification de *TTL* (*Time To Live*)

Dans la base de registre de Windows 95, développez l'arborescence :

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services/VxD/MSTCP/

Rajoutez la valeur chaîne "DefaultTTL", et attribuez-lui la valeur 64.



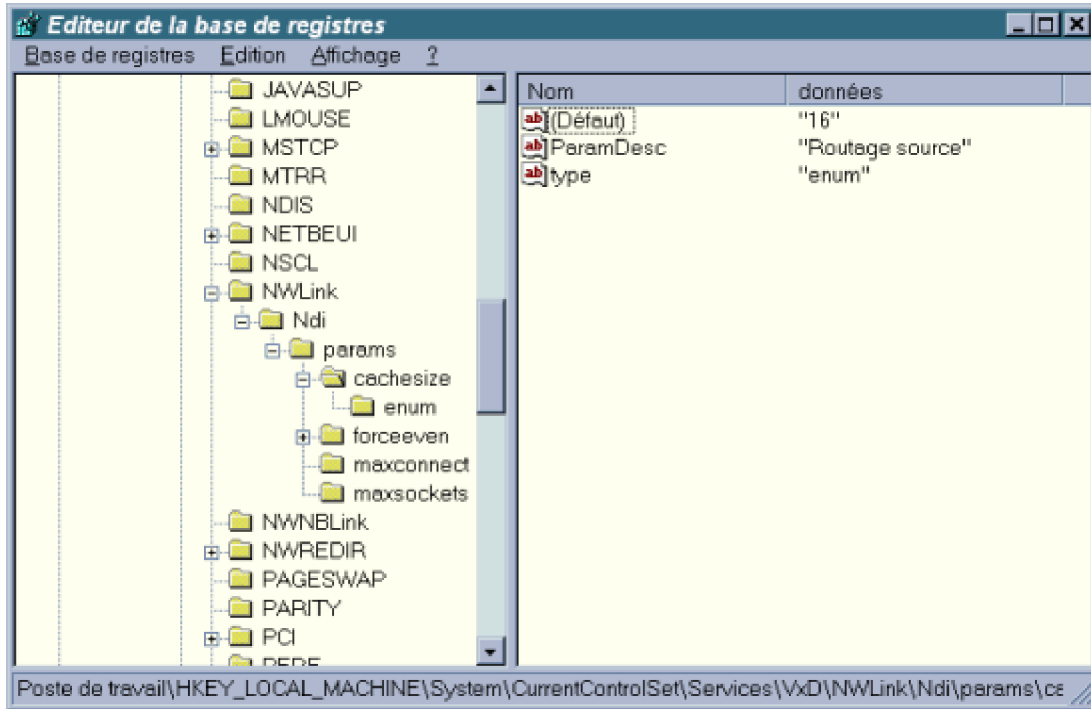
4. Modification de NDI

NB : personne ne comprend rien au pourquoi de cette modification, mais CERTAINES personnes trouvent qu'elle améliore sensiblement les performances. A vous de voir !

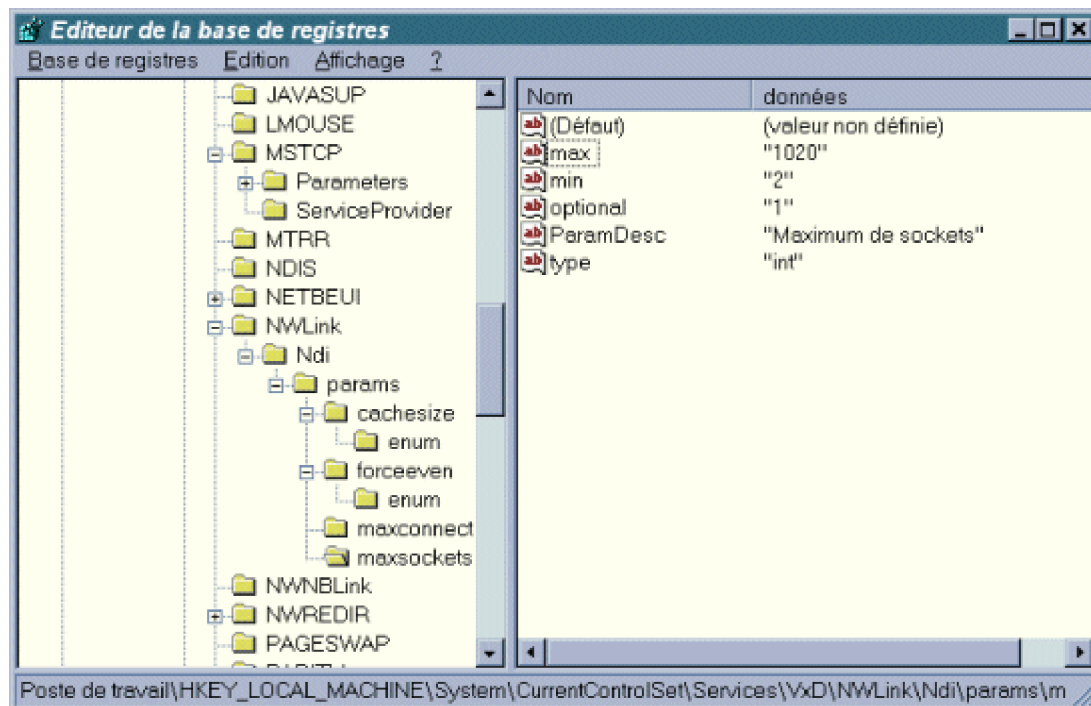
Dans la base de registre de Windows 95, développez l'arborescence :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\Nwlink\Ndi\params

- Sous le répertoire **"/cachesize/"**, modifier la valeur chaîne "(Défaut)" (initialement 0) en 16.



- Sous le répertoire **"/maxsockets/"**, modifier la valeur chaîne "max" (initialement 255) en 1020.



Voilà, c'est tout. Testez votre système **après chaque modification** pour voir s'il y a de l'amélioration.

Je vous rappelle à ce propos que les modifications ne prennent effet qu' APRES LE REDEMARRAGE DE WINDOWS.

J'aimerais encore rajouter que des logiciels (comme MTU-Speed, etc.) sont censés effectuer automatiquement ces opérations. Personnellement, je vous conseille de faire la manipulation vous-même, comme je l'ai expliqué : en effet, certains de ces logiciels ne repèrent pas la bonne arborescence pour la carte d'accès distant et ajoutent des valeurs à une entrée qui ne sert à rien; de plus, j'ai toujours préféré avoir moi-même un contrôle sur ce genre de modifications système (je n'aime pas les logiciels qui "bidouillent dans mon dos").

Voici une liste plus exhaustive des Sockets IP pour les intéressés.

echo 7/tcp
echo 7/udp
discard 9/tcp sink null
discard 9/udp sink null
sysstat 11/tcp
sysstat 11/tcp users
daytime 13/tcp
daytime 13/udp
netstat 15/tcp
qotd 17/tcp quote
qotd 17/udp quote
chargen 19/tcp ttytst source
chargen 19/udp ttytst source
ftp-data 20/tcp
ftp 21/tcp
telnet 23/tcp
smtp 25/tcp mail
time 37/tcp timserver
time 37/udp timserver
rpl 39/udp resource # resource location
name 42/tcp nameserver
name 42/udp nameserver
whois 43/tcp nickname # usually to sri-nic
domain 53/tcp nameserver # name-domain server
domain 53/udp nameserver
nameserver 53/tcp domain # name-domain server
nameserver 53/udp domain
mtp 57/tcp # deprecated
bootp 67/udp # boot program server
tftp 69/udp
rje 77/tcp netrjs
finger 79/tcp
link 87/tcp ttylink
supdup 95/tcp
hostnames 101/tcp hostname # usually from sri-nic
iso-tsap 102/tcp
dictionary 103/tcp webster
x400 103/tcp # ISO Mail
x400-snd 104/tcp
csnet-ns 105/tcp
pop 109/tcp postoffice
pop2 109/tcp # Post Office
pop3 110/tcp postoffice
portmap 111/tcp
portmap 111/udp
sunrpc 111/tcp
sunrpc 111/udp
auth 113/tcp authentication
sftp 115/tcp
path 117/tcp
uucp-path 117/tcp
nntp 119/tcp usenet # Network News Transfer
ntp 123/udp ntpd ntp # network time protocol (exp)
nbtname 137/udp
nbdatagram 138/udp
nbssession 139/tcp

NeWS 144/tcp news
sgmp 153/udp sgmp
tcprepo 158/tcp repository # PCMAIL
snmp 161/udp snmp
snmp-trap 162/udp snmp
print-srv 170/tcp # network PostScript
vmnet 175/tcp
load 315/udp
vmnet0 400/tcp
sytek 500/udp
biff 512/udp comsat
exec 512/tcp
login 513/tcp
who 513/udp whod
shell 514/tcp cmd # no passwords used
syslog 514/udp
printer 515/tcp spooler # line printer spooler
talk 517/udp
ntalk 518/udp
efs 520/tcp # for LucasFilm
route 520/udp router routed
timed 525/udp timeserver
tempo 526/tcp newdate
courier 530/tcp rpc
conference 531/tcp chat
rvd-control 531/udp MIT disk
netnews 532/tcp readnews
netwall 533/udp # -for emergency
broadcasts
uucp 540/tcp uucpd # uucp daemon
klogin 543/tcp # Kerberos
authenticated rlogin
kshell 544/tcp cmd # and remote shell
new-rwho 550/udp new-who # experimental
remotefs 556/tcp rfs_server rfs # Brunhoff remote filesystem
rmonitor 560/udp rmonitord # experimental
monitor 561/udp # experimental
garcon 600/tcp
maitrd 601/tcp
busboy 602/tcp
acctmaster 700/udp
acctslave 701/udp
acct 702/udp
acctlogin 703/udp
acctprinter 704/udp
elcsd 704/udp # errlog
acctinfo 705/udp
acctslave2 706/udp
acctdisk 707/udp
kerberos 750/tcp kdc # Kerberos
authentication--tcp
kerberos 750/udp kdc # Kerberos
authentication--udp
kerberos_master 751/tcp # Kerberos authentication
kerberos_master 751/udp # Kerberos authentication
passwd_server 752/udp # Kerberos passwd server
userreg_server 753/udp # Kerberos userreg server
krb_prop 754/tcp # Kerberos slave
propagation
erlogin 888/tcp # Login and environment

passing
kpop 1109/tcp # Pop with Kerberos
phone 1167/udp
ingreslock 1524/tcp
maze 1666/udp
nfs 2049/udp # sun nfs
knetd 2053/tcp # Kerberos
de-multiplexor
eklogin 2105/tcp # Kerberos encrypted
rlogin
rmt 5555/tcp rmtd
mtb 5556/tcp mtbd # mtb backup
man 9535/tcp # remote man server
w 9536/tcp
mantst 9537/tcp # remote man server,
testing
bnews 10000/tcp
rscs0 10000/udp
queue 10001/tcp
rscs1 10001/udp
poker 10002/tcp
rscs2 10002/udp
gateway 10003/tcp
rscs3 10003/udp
remp 10004/tcp
rscs4 10004/udp
rscs5 10005/udp
rscs6 10006/udp
rscs7 10007/udp
rscs8 10008/udp
rscs9 10009/udp
rscsa 10010/udp
rscsb 10011/udp
qmaster 10012/tcp
qmaster 10012/udp