Guide Pratique des Concepts du Réseau sous Linux

Rusty Russell
Titre original : '*Linux Networking-Concepts HOWTO*'
Traduction initiale : Emmanuel Roger
Dernière adaptation : Guillaume Audirac`guillaume POINT audirac CHEZ netpratique POINT fr`
Relecture : Thomas Nemeth`tnemeth CHEZ free POINT fr`
v1.13.fr.1.1, le 20 Mai 2004, traduction/adaptation

Ce document décrit ce qu'est un réseau (comme Internet), et les bases de son fonctionnement.

Table des matières

1 Introduction

Bienvenue, ami lecteur.

J'ai écrit un nombre conséquent de Guides Pratiques sur les réseaux dans le passé, et il m'est apparu qu'il y avait une sacrée pile de jargon dans ceux-ci. J'avais donc trois alternatives, dont deux étaient ignorer le problème ou bien expliquer les termes partout. Ni l'une, ni l'autre n'étaient satisfaisantes.

La principale **qualité** des Logiciels Libres réside dans la possibilité d'explorer et de jouer avec les systèmes que vous utilisez. À mon avis, permettre aux gens d'expérimenter cette liberté est un but noble ; pas seulement parce que l'aventure les enthousiasme (comme le fait de reconstruire un moteur), mais parce que la nature même de l'Internet moderne et des Logiciels Libres vous permet de partager votre expérience avec des millions de gens.

Mais on doit bien démarrer quelque part, alors allons-y.

2 Qu'est-ce Qu'un '*Réseau Informatique*' ?

Un réseau informatique est juste un ensemble de trucs qui permettent à des noeuds de se parler entre eux (par '*noeuds*', on entend ordinateurs, imprimantes, distributeurs de boissons ou n'importe quoi dans le genre). La **façon** dont ils sont connectés n'a pas vraiment d'importance : vous pouvez utiliser des câbles en fibre optique ou bien des pigeons voyageurs. Évidemment, certains choix sont meilleurs que d'autres (surtout si vous avez un chat).

En général, si vous connectez juste deux ordinateurs entre eux, on ne peux pas réellement appeler ça un réseau ; vous avez vraiment besoin d'en avoir au moins trois pour avoir un réseau. C'est un peu comme le mot 'groupe' : deux personnes forment un couple, mais à partir de trois on appelle ça un 'groupe'. En fait, les réseaux sont souvent reliés entre eux, pour en former de plus grands ; chaque petit réseau (appelé un 'sous-réseau') peut être un élément d'un plus grand réseau.

La connexion entre deux ordinateurs est souvent appelée un '*lien réseau*'. Si un câble sort de l'arrière de votre machine et que celui-ci va vers une autre machine, c'est un lien réseau.

Il y a quatre choses à prendre en compte lorsqu'on parle d'un réseau informatique :

La taille

Si vous avez connecté chez vous vos quatre ordinateurs ensemble, vous avez ce que l'on peut appeler un réseau local ou LAN ('Local Area Network'). Si vous devez marcher pour aller voir les autres machines, en général on appelle ça un LAN, peu importe le nombre de machines qui y sont connectées, et comment vous avez construit le réseau.

À l'autre bout du spectre se trouvent les réseaux étendus ou WAN ('Wide Area Network'). Si vous avez un ordinateur à Lahore au Pakistan, un à Birmingham en Angleterre, et un autre à Santiago au Chili, et que vous vous arrangez pour les connecter, alors vous obtenez ce que l'on appelle un WAN.

La topologie : la géométrie

Construisons une carte du réseau : les lignes sont 2 (les liens réseau), et chaque point est un noeud. Il est possible que chaque ligne mène à un noeud central comme une grosse étoile, ce qui veut dire que chacun communique à travers ce point ('réseau en étoile') :

```
    o    o    o
     \_  |  _/
       \ | /
 o-----o-----o
       _/|\_
     /   |   \
    o    o    o
```

Il est aussi possible que tout le monde communique en ligne, comme ceci :

```
    o------o------o-------o--------o
    |                              |
    |                              |
```

```
|                               o
|                               |
o                               |
                                o
```

Ou peut-être avez-vous trois sous-réseaux connectés via un seul noeud :

```
            o
o           |  o--o--o
|           |  |
o--o--o--o--o  o
       \       |
        o------o
       /       |
o--o--o--o--o  o
|           |  |
o           |  o--o
            o
```

Vous verrez beaucoup de topologies comme celles-ci dans la réalité, et parfois certaines seront encore plus compliquées.

Le matériel : ce qui le compose

La seconde chose à prendre en compte est le matériel avec lequel est interconnecté votre réseau. Le moins cher est sans doute le '*réseau pédestre*' pour lequel des gens, souvent mal habillés, portent des disquettes d'une machine à l'autre. Le '*réseau pédestre*' est pratiquement toujours un 2 (LAN). Les disquettes coûtent moins de 1 Euro, et une solide paire de sandales peut se trouver pour 20 Euros.

Le lien réseau le plus souvent utilisé pour un usage domestique est le '*modem*' (pour MODulateur/DEModulateur). Il permet de transformer une ligne téléphonique standard en un lien réseau. Il convertit les données envoyées par l'ordinateur en sons et écoute les sons provenant de la ligne pour les retransformer en données compréhensibles par l'ordinateur. Comme vous pouvez l'imaginer, ce n'est pas très efficace, en partie parce que les lignes téléphoniques n'ont pas été conçues pour cela. Mais le modem est populaire car les lignes de téléphone sont répandues et bon marché : les modems se vendent pour moins de 50 Euros, et les lignes téléphoniques coûtent en général quelques centaines d'Euros par an.

La façon la plus courante de connecter des machines dans un LAN est d'utiliser une liaison Ethernet. Elle existe en plusieurs versions (listées de la plus ancienne à la plus récente) : Thinwire/Coax/10base2, UTP ('Unshielded Twisted Pair', paire torsadée non-blindée)/10baseT et UTP/100baseT. L'Ethernet Gigabit (le nom 1000baseT commence à devenir lourd) commence aussi à être déployé. Le fil 10base2 est généralement du câble coaxial noir, avec des connecteurs en T à visser : chaque poste est connecté à une grande ligne avec des connecteurs spéciaux 'de terminaison' à chaque extrémité. L'UTP est généralement du câble bleu, avec des connecteurs téléphoniques transparents à clipser dans des prises : chaque câble relie un noeud à un concentrateur ('*hub*') central. Le câble coûte quelques Euros le mètre, et les cartes 10baseT/10base2 (la plupart ont des connecteurs des deux types) sont difficiles à trouver neuves. Les cartes 100baseT, qui peuvent aussi communiquer en 10baseT, sont dix fois plus rapides, et coûtent environ 30 Euros.

A l'autre bout du spectre, on trouve la fibre optique, un fin filament de verre continu enrobé dans un revêtement protecteur qui peut être utilisé pour relier des continents. La fibre coûte des milliers d'Euros.

On appelle habituellement chaque connexion à un noeud une '*interface réseau*', ou '*interface*' pour faire plus court. Linux donne des noms comme '`eth0`' pour la première interface Ethernet, et '`fddi0`' pour la première interface fibre optique. La commande '`/sbin/ifconfig`' les liste.

Le protocole : quelle langue il parle

La dernière chose à prendre en compte est le langage qu'on utilise. Quand deux 2 (modems) parlent entre eux via une ligne téléphonique, ils ont besoin de s'entendre sur la signification des sons, autrement ils ne se comprendraient pas. Cette convention est appelée un 'protocole'. Au fur et à mesure que l'on inventait de nouvelles façons de coder les signaux numériques en sons plus courts, on créait de nouveaux protocoles : il en existe au moins une douzaine. La plupart des modems essayent plusieurs de ces protocoles avant d'en trouver un que leur collègue à l'autre bout du fil connaît aussi.

Un autre exemple est le réseau 2 (100baseT) mentionné ci-dessus : il utilise les mêmes 2 (liens réseau) physiques (2 (UTP)) que le précédent 2 (10baseT), mais communique dix fois plus vite.

Ces protocoles sont appelés des protocoles de '*niveau lien*', c'est-à-dire qu'ils interviennent dans un voisinage réseau qui ne dépasse pas un '*saut*' autour de l'ordinateur. Le mot '*protocole*' peut aussi se référer à d'autres conventions, comme nous le verrons par la suite.

3 Qu'est-ce Qu''Internet' ?

Internet est un 2 (WAN) qui englobe le monde entier : c'est le plus grand réseau informatique qui existe depuis le commencement des temps. Le terme '*interréseautage*' ('internetworking') fait référence à la connexion de réseaux indépendants pour en construire un plus grand, ainsi '*Internet*' est uniquement un vaste ensemble de sous-réseaux connectés entre eux.

À présent, si on regarde la liste ci-dessus, on peut se demander : quelle est la taille d'Internet, quelle langue y parle-t-on, et de quoi est-il fait ?

La taille est implicite : il est mondial.

Les particularités matérielles sont variées : chaque petit sous-réseau est connecté différemment, avec une topologie et une nature différentes. Et les tentatives pour le cartographier se sont généralement soldées par de cuisants échecs.

Les protocoles utilisés par chaque lien sont souvent différents : on y trouve tous les 2 (protocoles de lien) dont nous avons parlé ci-dessus et bien plus encore.

3.1 Comment Fonctionne Internet ?

Une question s'impose : comment tous les noeuds d'Internet peuvent-ils communiquer entre-eux s'ils utilisent tous des protocoles de lien différents ?

La réponse est plutôt simple : on a besoin d'un autre protocole qui contrôle comment les choses transitent à travers le réseau. Le protocole de lien décrit comment aller d'un noeud à un autre s'ils sont directement connectés : dans le cas contraire, le 'protocole de réseau' nous dit comment aller d'un point à un autre dans le réseau en franchissant plusieurs liens si nécessaire.

Pour Internet, le protocole de réseau est l''*Internet Protocol*' (version 4), ou '*IP*'. Ce n'est pas le seul protocole existant (AppleTalk d'Apple, IPX de Novell, DECNet de Digital et NetBEUI de Microsoft), mais c'est le plus couramment adopté. Il y a une nouvelle version d'IP appelée IPv6, mais elle n'est pas encore très courante.

Ainsi, pour envoyer un message d'une région du monde à une autre, votre ordinateur rédige un peu de Protocole Internet, l'envoie à votre modem, qui utilise un protocole de lien modem pour l'envoyer au modem auquel il est connecté, qui est probablement branché à un serveur de terminaux (fondamentalement une grosse boîte de modems), qui l'envoie à un noeud du réseau de votre prestataire, qui l'envoie à un plus gros noeud, qui l'envoie au noeud suivant... et ainsi de suite. Un noeud connecté à deux réseaux ou plus est appelé un '*routeur*' : il aura une 2 (interface) pour chaque réseau.

On appelle cet alignement de protocoles une 'pile de protocoles'. Elle est généralement représentée comme ceci :

```
[ Application: Gère le porn ]       [ Couche Application: Sers le porn ]
```

```
              |                                     ^
              v                                     |
[ TCP: Gère la retransmission ]     [ TCP: Gère la retransmission ]
              |                                     ^
              v                                     |
    [ IP: Gère le routage ]             [ IP: Gère le routage ]
              |                                     ^
              v                                     |
[ Lien: Gère un seul saut ]           [ Lien: Gère un seul saut ]
              |                                     |
              +-------------------------------------+
```

Ainsi, dans le diagramme, on imagine Netscape (l'application en haut à gauche) qui télécharge une page Web d'un serveur Web (l'application en haut à droite). Pour faire cela, il va utiliser le *Protocole de Contrôle de Transmission* ('Transmission Control Protocol' ou '*TCP*') : plus de 90% du trafic Internet de nos jours est du TCP, comme pour les Méls et le Web.

Netscape envoie donc une requête pour une connexion TCP au serveur Web distant : cette demande est gérée par la couche TCP, qui ensuite la fait suivre à la couche IP, qui trouve où le paquet doit aller, et l'envoie à la couche lien appropriée, qui la transmet à l'autre bout du lien.

Une fois le paquet arrivé à l'autre extrémité, la couche lien envoie le paquet à la couche IP, qui voit qu'il est destiné à cet hôte (si ce n'est pas le cas, il sera redirigé vers une couche lien différente pour aller au noeud suivant), le transmet à la couche TCP, qui l'envoie au serveur.

On obtient alors la situation suivante :

1. L'application (Netscape, ou le serveur Web à l'autre bout) décide à qui elle veut parler et ce qu'elle veut envoyer.
2. La couche TCP envoie des paquets spéciaux pour engager la conversation avec l'autre bout, ensuite elle encapsule les données dans un '*paquet*' TCP : un paquet est juste un terme pour désigner un bloc de données qui traverse un réseau. La couche TCP dirige ce paquet vers la couche IP : elle continue à l'envoyer à la couche IP jusqu'à ce que la couche TCP à l'autre bout en accuse réception. On appelle cela, la '*retransmission*', celle-ci est basée sur des règles complexes qui contrôlent l'instant de retransmission, les temps d'attentes, etc... Elle numérote aussi chaque paquet, ce qui permet de réordonner les paquets à l'autre extrémité.
3. La couche IP examine la destination du paquet, et en déduit le noeud suivant auquel elle doit l'envoyer. On appelle cela le '*routage*', et cela va du plus simple (si vous avez un modem et aucune carte réseau, tous les paquets sortent par le modem) au plus complexe (si vous avez 15 grands réseaux directement connectés à votre machine).

4 Cette Chose IP

Donc le rôle de la couche IP est de décider comment 'router' les paquets vers leur destination finale. Pour rendre cela possible, chaque interface sur le réseau a besoin d'une 'adresse IP'. Une adresse IP est constituée de quatre nombres séparés par des points, comme '167.216.245.249'. Chaque nombre est compris entre zéro et 255.

Les interfaces sur le même réseau tendent à avoir des adresses IP voisines. Par exemple, '167.216.245.250' est situé près de la machine qui a l'adresse '167.216.245.249'. Souvenez-vous aussi qu'un routeur est un noeud avec des interfaces sur plus d'un réseau, donc le routeur aura une adresse IP différente pour chaque interface.

De plus, la couche IP du noyau Linux garde une table des différentes 'routes', qui décrit comment accéder aux différents groupes d'adresses IP. La plus simple de ces routes est appelée la route par défaut ('*default* *route*') : si la couche IP ne sait pas trop, c'est par là qu'elle enverra le paquet. On peut voir une liste des routes en utilisant la commande '/sbin/route'.

Les routes peuvent pointer soit vers un lien, soit vers un noeud particulier qui est connecté à un autre réseau. Par exemple, quand vous appelez votre prestataire, votre route par défaut pointera vers le lien modem, parce que c'est par là que vous pouvez joindre le monde entier.

```
Modem de          Modem du ~~~~~~~~
 Rusty        prestataire {        }
    o------------------o {  Le Net  }
                          {        }
                           ~~~~~~~~
```

Mais si votre machine est connectée en permanence à Internet, c'est un peu plus compliqué. Dans le diagramme ci-dessous, ma machine peut communiquer directement avec les machines de Tridge et de Paul, et aussi avec le pare-feu, mais elle a besoin de savoir que les paquets qui sont destinés au reste du monde doivent passer par le pare-feu, qui les enverra plus loin. Cela veut dire que vous avez besoin de deux routes : une qui dit 'si la destination est sur mon propre réseau, envoie-les directement' et une route par défaut qui dit 'sinon, envoie-les au pare-feu'.

```
                        o  Machine de
                        |    Tridge           ~~~~~~~~
Machine de              |                    {        }
 Rusty         o--------+-----------------o--{  Le Net  }
                        |            Pare-feu {        }
                        |                     ~~~~~~~~
                        o  Machine de
                             Paul
```

4.1 Les Groupes d'Adresses IP : Les Masques Réseaux

Il y a une dernière particularité : il existe une notation standard pour les groupes d'adresses IP, parfois appelée une 'adresse réseau'. Exactement comme un numéro de téléphone qui peut être divisé en un préfixe de zone et le reste, on peut diviser les adresses IP en un préfixe réseau et le reste.

Il est courant d'entendre parler du 'réseau 1.2.3', ce qui fait référence en réalité aux 256 adresses de 1.2.3.0 à 1.2.3.255. Ou, si ce n'est pas suffisant, du 'réseau 1.2' qui signifie toutes les adresses IP de 1.2.0.0 à 1.2.255.255.

Habituellement, on n'écrit pas '1.2.0.0 - 1.2.255.255'. On le raccourcit en '1.2.0.0/16'. Ce '/16' (masque réseau ou 'netmask') requiert quelques explications.

Les nombres entre les points dans une adresse IP sont en réalité 8 chiffres binaires (de 00000000 à 11111111). On les écrit sous forme décimale pour qu'ils soient plus lisibles. Le '/16' veut dire que les 16 premiers chiffres binaires sont l'adresse du réseau. En d'autres termes, la partie '1.2.' est l'adresse du réseau (rappelez-vous : chaque nombre décimal représente 8 chiffres binaires). Ceci signifie que chaque adresse IP commençant par '1.2.' fait partie du réseau : '1.2.3.4' et '1.2.3.50' en font partie, mais pas '1.3.1.1'.

Pour rendre la vie plus facile, on utilise en général des réseaux se terminant par '/8', '/16' et '/24'. Par exemple '10.0.0.0/8' est un grand réseau contenant les adresses de 10.0.0.0 à 10.255.255.255 (plus de 16 millions d'adresses !). 10.0.0.0/16 est plus petit, contenant seulement les adresses de 10.0.0.0 à 10.0.255.255. Et 10.0.0.0/24 est encore plus petit, contenant les adresses de 10.0.0.0 à 10.0.0.255.

Pour rendre les choses encore plus confuses, il y a une autre manière d'écrire les masques réseaux. On peut les écrire comme des adresses IP :

```
10.0.0.0/255.0.0.0
```

Enfin, l'adresse IP la plus haute dans le réseau est réservée comme *adresse de diffusion* ('broadcast address'), qui peut être utilisée pour envoyer un message à tout le monde dans le réseau en une fois.

Voici une table des masques réseaux :

Forme Courte	Forme Complète	Nb Max de Machines	Commentaire
/8	/255.0.0.0	16,777,215	Appelé 'un réseau de classe A'
/16	/255.255.0.0	65,535	Appelé 'un réseau de classe B'
/17	/255.255.128.0	32,767	
/18	/255.255.192.0	16,383	
/19	/255.255.224.0	8,191	
/20	/255.255.240.0	4,095	
/21	/255.255.248.0	2,047	
/22	/255.255.252.0	1,023	
/23	/255.255.254.0	511	
/24	/255.255.255.0	255	Appelé 'un réseau de classe C'
/25	/255.255.255.128	127	
/26	/255.255.255.192	63	
/27	/255.255.255.224	31	
/28	/255.255.255.240	15	
/29	/255.255.255.248	7	
/30	/255.255.255.252	3	

5 Noms de Machines et Adresses IP

Ainsi, chaque interface sur chaque noeud a une adresse IP. On réalisa assez rapidement que les humains n'avaient pas la mémoire des nombres, il a donc été décidé (exactement comme pour les numéros de téléphone) d'avoir un répertoire de noms. Mais comme on utilise des ordinateurs de toute façon, il est plus pratique que ce soit l'ordinateur qui convertisse automatiquement les noms pour nous.

De là est né le Système des Noms de Domaines ou 'Domain Name System' (DNS). Il y a des noeuds qui ont des adresses IP connues de tous auxquels les programmes peuvent demander la conversion des noms en adresses IP. À peu près tous les programmes que vous allez utiliser sont capables de faire cela, c'est pour cette raison que vous pouvez entrer 'www.linuxcare.com' dans Netscape au lieu de '167.216.245.249'.

Naturellement, vous avez besoin de l'adresse IP d'au moins un de ces 'serveurs de noms' : habituellement, ils sont conservés dans le fichier '/etc/resolv.conf'.

Comme les requêtes et les réponses DNS sont plutôt petites (1 paquet chacune), le protocole TCP n'est pas vraiment utilisé : il permet d'assurer les retransmissions automatiques, le réordonnancement des paquets et la fiabilité générale, mais avec un surcoût sur le nombre de paquets envoyés. À la place, on utilise le Protocole de Datagramme Utilisateur ('User Datagram Protocol' ou *UDP*) qui est plus simple car il évite les garanties de TCP dont nous n'avons pas l'utilité ici.

6 Différents Services : Mél, Web, FTP, Serveur de Noms

Dans l'exemple précédent, nous avons vu comment Netscape envoie une requête TCP à un serveur Web tournant sur un autre noeud. Mais imaginez que le noeud qui fait tourner un serveur Web dispose aussi d'un serveur de messagerie, d'un serveur FTP et d'un serveur de noms : comment savoir à quel serveur est destinée la connexion TCP ?

C'est pour cela que les protocoles TCP et UDP possèdent un concept de 'ports'. Chaque paquet contient une zone où il stocke son '*port de destination*', qui dit à quel service le paquet est adressé. Par exemple, le port TCP 25 est le serveur de courrier, et le port TCP 80 le serveur Web (bien qu'on puisse parfois trouver des serveurs Web sur des ports différents). Une liste de ports peut être trouvée dans le fichier '/etc/services'.

De même, lorsque deux fenêtres Netscape accèdent chacune à une partie différente d'un même site Web, comment fait la machine Linux pour trier les paquets TCP provenant du serveur Web ?

C'est ici que le 'port source' entre en jeu : chaque nouvelle connexion TCP reçoit un port source différent, pour que chacune puisse être différenciée, même si elles sont dirigées vers la même adresse IP et le même port de destination. Habituellement, le premier port source donné sera le port 1024 et sera incrémenté au fur et à mesure des connexions.

7 Interface de Connexion : PPP

Quand vous composez le numéro de votre prestataire sur votre modem et que vous vous connectez au modem de votre prestataire, le noyau ne fait pas que lui envoyer des paquets IP. Il y a un protocole appelé 'Protocole Point-à-Point' ou 'PPP', qui est utilisé pour négocier avec l'autre bout avant qu'un paquet de données ne soit envoyé. Ce protocole est utilisé par le prestataire pour identifier l'appelant : sur votre machine Linux, un programme appelé le 'daemon PPP' gère votre partie de la négociation.

Comme il y a beaucoup d'utilisateurs de modems dans le monde, ils n'ont en général pas leur propre adresse IP : la plupart des prestataires vous en attribueront une temporairement quand vous les appellerez (le démon PPP l'obtiendra pendant la négociation). On appelle souvent cela une 'adresse IP dynamique', à l'inverse d'une 'adresse IP statique' qui est une adresse permanente. Généralement, une adresse IP statique est attribuée à chaque modem du prestataire ; à chaque appel, vous vous connectez à un modem différent du lot de modems, et vous recevez donc une adresse IP différente.

8 À Quoi Ressemblent les Paquets

Pour les gens exceptionnellement curieux (et curieusement exceptionnels), voici une description de ce à quoi les paquets ressemblent. Il y a plusieurs outils pour voir quels paquets entrent et sortent de votre machine Linux. Le plus courant est '*tcpdump*' (qui comprend de nos jours d'autres protocoles en plus de TCP), mais il en existe un plus agréable : 'ethereal'. De tels programmes sont appelés des 'renifleurs de paquets' ('packet sniffers').

Le début de chaque paquet indique où il va, d'où il vient, le type du paquet et d'autres détails administratifs. Cette partie est appelée l''en-tête' du paquet. Le reste du paquet, qui contient les données à transmettre, est appelé le 'corps' du paquet.

Ainsi, tout paquet IP commence par un 'en-tête IP' long d'au moins 20 octets. Il ressemble à ceci (le diagramme a été honteusement copié à partir de la RFC 791) :

```
.-------+-------+---------------+-------------------------------.
|Version|  IHL  |Type de Service|        Longueur Totale        |
|-------+-------+---------------+-------------------------------|
|         Identification        |Fanions| Décalage du Fragment  |
|---------------+---------------+-------------------------------|
|  Durée de vie |    Protocole  |  Somme de Contrôle d'En-Tête  |
|---------------+---------------+-------------------------------|
|                     Adresse de la Source                      |
|---------------------------------------------------------------|
|                     Adresse de la Destination                 |
```

```
`--------------------------------------------------------------'
```

Les champs importants sont le protocole, qui indique si c'est un paquet TCP (numéro 6), un paquet UDP (numéro 17) ou autre, l'adresse IP de source, et l'adresse IP de destination.

Maintenant, si le champ protocole indique que c'est un paquet TCP, alors un en-tête TCP suivra immédiatement cet en-tête IP. L'en-tête TCP est aussi long de 20 octets au moins :

```
.-------------------------------+-------------------------------.
|          Port Source          |       Port Destination        |
|-------------------------------+-------------------------------|
|                      Numéro de Séquence                       |
|---------------------------------------------------------------|
|                    Numéro d'Acquittement                      |
|-------------------+-+-+-+-+-+-+-------------------------------|
|Décalage|          |U|A|P|R|S|F|                               |
|  des   | Réservé  |R|C|S|S|Y|I|            Fenêtre            |
|Données |          |G|K|H|T|N|N|                               |
|--------+----------+-+-+-+-+-+-+-------------------------------|
|       Somme de Contrôle       |        Pointeur Urgent        |
`---------------------------------------------------------------'
```

Les champs les plus importants sont ici les ports source et destination, qui disent à quel service le paquet est destiné (d'où il vient, dans le cas de paquets de réponses). Les numéros de séquence et d'acquittement sont utilisés pour garder les paquets dans l'ordre, et pour dire à l'autre bout quels paquets ont été reçus. Les labels ACK, SYN, RST et FIN sont des bits utilisés pour négocier l'ouverture (SYN), l'acquittement (ACK) et la fermeture (RST ou FIN) des connexions.

À la suite de cet en-tête vient le message réel que l'application a envoyé (le corps du paquet). La taille d'un paquet IP normal est au maximum de 1500 octets. Ce qui veut dire que la place maximum réservée aux données est 1460 octets (20 octets pour l'en-tête IP, et 20 autres pour l'en-tête TCP). Soit plus de 97%.

9 Résumé

Ainsi, l'Internet moderne utilise des paquets IP pour communiquer, et la plupart de ces paquets IP encapsulent des paquets TCP. Des noeuds spéciaux appelés 'routeurs' connectent tous les petits réseaux entre eux, formant ainsi de plus grands réseaux, et font suivre les paquets vers leur destination. La plupart des machines normales sont seulement attachées à un seul réseau (c'est-à-dire possèdent une seule interface) et ne sont donc pas des routeurs.

Chaque interface a une adresse IP unique, qui ressemble à '1.2.3.4' : les interfaces d'un même réseau ont des adresses IP voisines, avec le même préfixe, comme pour les numéros de téléphone d'une même zone. Les adresses réseaux ressemblent aux adresses IP, avec un '/' pour préciser combien de chiffres binaires font partie du préfixe. Par exemple, '1.2.0.0/16' signifie que les deux premiers nombres décimaux (ou les 16 premiers chiffres binaires) représente l'adresse réseau.

Les machines peuvent être désignées par des noms grâce au Service de Noms de Domaines : les programmes demandent aux serveurs de noms de leur fournir l'adresse IP équivalente à un nom donné (comme 'www.linuxcare.com'). Cette adresse IP est ensuite utilisée comme l'adresse IP destination pour parler à ce noeud.

Rusty se trouve vraiment médiocre pour rédiger de la documentation, et spécialement lorsqu'elle s'adresse à des débutants.

Profitez-en !

Rusty.

10 Remerciements

Mes remerciements à Alison pour avoir lu le premier brouillon, et m'avoir dit quel foutoir c'était, de la façon la plus gentille possible.

11 Commentaires et Corrections

Merci de faire parvenir en anglais à l'auteur vos questions et commentaires relatifs à la version originale de ce document à l'adresse *netfilter@lists.samba.org* .

N'hésitez pas à faire parvenir tout commentaire relatif à la version française de ce document à *commentaires CHEZ traduc POINT org* en précisant le titre et la version de ce document.

12 Index