Petit guide des sous-réseaux IP

Robert Hart, *hartr@interweft.com.au*
version française par Laurent Caillat-Vallet, *caillat@univ-lyon1.fr* v1.0, 31 Mars 1997

Ce document décrit pourquoi et comment découper un réseau IP en sous-réseaux - c'est à dire utiliser correctement une seule adresse de réseau de classe A, B ou C, pour plusieurs réseaux interconnectés.

Contents

1 Copyright

Ce document est directement supporté par InterWeft IT Consultants (Melbourne, Australie).
La dernière version de ce document est disponible sur le site WWW d'InterWeft: *http://www.interweft.com.au/* et depuis le Projet de Documentation de Linux (Linux Documentation Project, LDP): *http://sunsite.unc.edu/LDP* .

2 Introduction

Avec les numéros de réseau IP devenant rapidement une espèce en voie de disparition, l'utilisation efficace de ces ressources de plus en plus rares est importante.
Ce document décrit comment découper un numéro de réseau IP afin de l'utiliser pour plusieurs réseaux différents.
Ce document est focalisé sur les numéros de réseau IP de classe C - mais les principes s'appliquent de la même manière aux réseaux de classes A et B.

2.1 D'autres sources d'information

Il y a beaucoup d'autres sources d'informations utiles, pour des informations aussi bien détaillées que plus générales sur les numéros IP. Celles recommandées par l'auteur sont:

- Administration Réseau sous Linux *ftp://ftp.lip6.fr/pub/linux/french/books/nag.french.eoit-1.0.tar.gz* pour la version française, *http://sunsite.unc.edu/LDP/LDP/nag/nag.html* pour la version anglaise.
- Le Guide de l'Administration Système sous Linux (en anglais) *http://linuxwww.db.erau.edu/SAG/* .
- L'Administration de Réseau TCP/IP, de Craig Hunt, publié par O'Reilly and Associates *http://www.ora.com/catalog/tcp/noframes.html* .

3 L'anatomie des numéros IP

Avant de plonger dans les délices des sous-réseaux, nous devons poser les bases à propos des numéros IP.

3.1 Les numéros IP appartiennent aux Interfaces - PAS aux hôtes !

Tout d'abord, éclaircissons une cause classique de mauvaise compréhension - les numéros IP ne sont pas assignés aux hôtes. Les numéros IP sont assignés aux interfaces réseau sur les hôtes.
Hein? C'est quoi ça?
Alors que la plupart des ordinateurs (pour ne pas dire tous) d'un réseau IP ne possèderont qu'une seule interface réseau (et donc n'auront qu'une seule adresse IP), il n'en va pas toujours ainsi. Certains ordinateurs ou d'autres appareils peuvent avoir plusieurs (voire de nombreuses) interfaces réseau - et chaque interface a son propre numéro IP.
Donc un appareil avec 6 interfaces actives (comme un routeur) aura 6 numéros IP - un pour chaque interface vers chaque réseau sur lequel il est connecté. La raison en devient claire quand on regarde un réseau IP!

Malgré cela, la plupart des gens font référence à des adresses d'hôtes quand ils veulent faire référence à des numéros IP. Souvenez-vous juste que ce n'est qu'un raccourci pour le numéro IP de l'interface de cet hôte. La plupart (si ce n'est pas la majorité) des appareils sur Internet n'ont qu'une interface réseau, et donc qu'un numéro IP.

3.2 Les numéros IP sous forme de "quadruplets pointés"

Dans l'implémentation actuelle des numéros IP (IPv4), les numéros IP sont composés de 4 octects (de 8 bits) - fournissant un total de 32 bits d'information disponibles. Cela donne des numéros plutôt grands (même quand on les écrit en notation décimale). Donc pour la lisibilite (et pour des raisons organisationnelles), les numéros IP sont habituellement écrits sous la forme de "quadruplets pointés". Le numéro IP

```
192.168.1.24
```

en est un exemple - 4 nombres (décimaux) séparés par des points (.).
Comme chacun des quatre nombres est la représentation décimale d'un octet de 8 bits, chacun de ces nombres est compris entre 0 et 255 (c'est à dire qu'il peut prendre 256 valeurs - souvenez-vous que 0 est aussi une valeur).
De plus, une partie du numéro IP d'un hôte identifie le réseau sur lequel l'hôte est connecté, les bits restants du numéro IP indique l'hôte lui-même (oups - l'interface réseau). La classe de réseau détermine combien de bits sont utilisés par l'identificateur de réseau et combien sont disponibles pour identifier les hôtes.

3.3 Les classes des réseaux IP

Il y a trois classes de numéros IP

- Les numéros des réseaux IP de classe A utilisent les 8 bits les plus à gauche (le nombre le plus à gauche du quadruplet pointé) pour identifier le réseau, laissant 24 bits (les 3 nombres restants du quadruplet) pour identifier les interfaces des hôtes de ce réseau.
  Les adresses de classe A ont toujours le dernier bit à gauche à zéro - c'est à dire une valeur décimale entre 0 et 127 pour le premier nombre du quadruplet. Il y a donc un maximum de 128 numéros de réseaux de classe A disponibles, chacun d'eux contenant jusqu'à 16 777 214 interfaces (NDT: le mini-howto original indique 33 554 430 interfaces... petite erreur de calcul...).
  Toutefois, les réseaux 0.0.0.0 (appelé route par defaut) et 127.0.0.0 (le réseau de boucle de retour - loopback) ont des significations spéciales et ne sont pas disponibles pour identifier des réseaux. Il n'y a donc que 126 réseaux de classe A disponibles.

- Les numéros de réseaux IP de classe B utilisent les 16 bits les plus à gauche (les deux nombres de gauche du quadruplet) pour identifier le réseau, laissant 16 bits (les deux derniers nombres du quadruplet) pour identifier les interfaces des hôtes.
  Les adresses de classe B ont toujours les 2 bits les plus à gauche mis à 1 0. Cela laisse 14 bits pour spécifier l'adresse de réseau, donnant 32 767 réseaux de classe B disponibles. Les réseaux de classe B ont donc le premier nombre du quadruplet entre 128 et 191, chaque réseau pouvant contenir 65 534 interfaces (NDT: dans le document original: 32 766, encore une erreur...).

- Les numéros de réseau IP de classe C utilisent les 24 bits les plus à gauche (les trois nombres de gauche du quadruplet) pour identifier le réseau, laissant 8 bits (le nombre le plus à droite du quadruplet) pour identifier les interfaces des hôtes.
  Les adresses de classe C commencent toujours avec les 3 bits les plus à gauche positionnés à 1 1 0, soit un intervalle de 192 à 256 pour le nombre le plus à gauche du quadruplet. Il y a donc 4 194 303 numéros de réseaux de classe C disponibles, chacun contenant 254 interfaces. (Les réseaux de classe C avec le premier octet superieur à 223 sont toutefois réservés et non disponibles.)

En résumé:

```
Classe de reseau  Intervalle des valeurs (decimales) utilisables du 1er octet
      A                        1 a 126
      B                      128 a 191
      C                      192 a 254
```

Il y a aussi des adresses spéciales, qui sont réservées pour des réseaux 'non-connectés' - c'est à dire des réseaux qui utilisent IP mais ne sont pas connectés à l'Internet. Ces adresses sont:

- Un réseau de classe A: 10.0.0.0

- 16 réseaux de classe B: 172.16.0.0 - 172.31.0.0
- 256 réseaux de classe C: 192.168.0.0 - 192.168.255.0

Vous remarquerez que dans tout ce document, on utilise ces intervalles pour ne pas créer de confusion avec de 'vrais' réseaux et de 'vrais' hôtes.

3.4 Numéros de réseaux, adresses d'interface, et adresses de diffusion

Les numéros IP peuvent avoir trois significations:

- l'adresse d'un réseau IP (un groupe d'appareils IP partageant un accès commun à un médium de transmission - en étant par exemple sur un même segment Ethernet). Un numéro de réseau aura toujours les bits d'interface (hôte) de l'espace d'adressage positionnés à 0 (sauf si le réseau est découpé en sous-réseaux, comme nous le verrons plus tard);
- l'adresse de diffusion d'un réseau IP (l'adresse utilisée pour 'parler' simultanément à tous les appareils d'un réseau IP). Les adresses de diffusion d'un réseau ont toujours les bits d'interface (hôte) de l'espace d'adressage positionnés à 1 (encore une fois, sauf si le réseau est découpé en sous-réseaux, comme nous le verrons plus tard);
- l'adresse d'une interface (comme une carte Ethernet ou une interface PPP sur un hôte, un routeur, un serveur d'impression etc...). Ces adresses peuvent avoir n'importe quelle valeur pour les bits d'hôte, sauf tous à 0 ou tous à 1 - car avec tous les bits à 0, c'est l'adresse d'un réseau, et avec tous les bits à 1, c'est l'adresse de diffusion d'un réseau.

En résumé et pour clarifier les choses

- Pour un réseau de classe A... (un octet pour l'espace d'adressage du réseau, suivi de trois octets pour l'espace d'adressage d'interface)
  10.0.0.0 est un numéro de réseau de classe A car tous les bits de l'espace d'adressage d'interface sont à 0
  10.0.1.0 est une adresse d'interface sur ce réseau
  10.255.255.255 est l'adresse de diffusion de ce réseau car tous les bits de l'espace d'adressage d'interface sont à 1
- Pour un réseau de classe B... (deux octets pour l'espace d'adressage du réseau, suivi de deux octets pour l'espace d'adressage d'interface)
  172.17.0.0 est un numéro de réseau de classe B 172.17.0.1 est une adresse d'interface sur ce réseau
  172.17.255.255 est l'adresse de diffusion de ce réseau
- Pour un réseau de classe C... (trois octets pour l'espace d'adressage du réseau, suivi d'un octet pour l'espace d'adressage d'interface)
  192.168.3.0 est un numéro de réseau de classe C
  192.168.3.42 est une adresse d'interface sur ce réseau
  192.168.3.255 est l'adresse de diffusion de ce réseau

Quasiment tous les numéros de réseaux IP encore disponibles de nos jours sont des adresses de classe C.

3.5 Le masque de réseau

Le masque de réseau devrait plutôt être appelé masque de sous-réseau. Toutefois, on y fait généralement référence comme masque de réseau.

C'est le masque de réseau et ses implications sur la manière d'interpréter les adresses IP localement sur un segment de réseau IP qui nous concernent le plus, puisque cela détermine le découpage en sous-réseau (s'il y en a un).
Le masque de (sous-)réseau standard est tous les bits de réseau d'une adresse placés à '1', et tous les bits d'interface placés à '0'. Cela signifie que les masques de réseaux standards pour les 3 classes de réseaux sont:

- masque de réseau de classe A: 255.0.0.0
- masque de réseau de classe B: 255.255.0.0
- masque de réseau de classe C: 255.255.255.0

Il faut se souvenir de deux choses importantes à propos des masques de réseau:

- le masque de réseau n'affecte que l'interprétation locale des numéros IP (où locale signifie sur un segment de réseau particulier);
- le masque de réseau n'est pas un numéro IP - il est utilisé pour modifier localement l'interprétation des numéros IP locaux.

4 Que sont les sous-réseaux?

Un sous-réseau est une façon de prendre une adresse d'un réseau, et de la découper localement pour que cette adresse de réseau unique puisse en fait être utilisée pour plusieurs réseaux locaux interconnectés. Souvenez-vous, un seul numéro de réseau IP ne peut être utilisé que sur un seul réseau.
Le mot important ici est "localement": du point de vue du monde extérieur aux machines et réseaux physiques couverts par le réseau découpé en sous-réseaux, absolument rien n'a changé - cela reste un unique réseau IP.
Ceci est important - le découpage en sous-réseaux est une configuration locale et invisible au reste du monde.

5 Pourquoi découper en sous-réseaux?

Les raisons derrière ce type de découpage remontent aux premières spécifications d'IP - où il n'y avait que quelques sites fonctionnant sur des numéros de réseau de classe A, ce qui permettait des millions d'hôtes connectés.
C'est évidemment un trafic énorme et des problèmes d'administration si tous les ordinateurs IP d'un important site doivent être connectés sur le même réseau: essayer de gérer un tel monstre serait un cauchemar et le réseau s'écroulerait (de manière quasi-certaine) sous la charge de son propre trafic (saturé).

Arrive le découpage en sous-réseaux: l'adresse de réseau de classe A peut être découpée pour permettre sa distribution à plusieurs (voire beaucoup de) réseaux séparés. La gestion de chaque réseau séparé peut facilement être déléguée de la même façon.

Cela permet d'établir des réseaux petits et gérables - en utilisant, c'est tout à fait possible, des technologies de réseaux différentes. Souvenez-vous, vous ne pouvez pas mélanger Ethernet, Token Ring, FDDI, ATM, etc... sur le même réseau physique - ils peuvent toutefois être interconnectés !

Les autres raisons du découpage en sous-réseaux sont:

- La topographie d'un site peut créer des restrictions (longueur de câble) sur les possibilités de connexion de l'infrastructure physique, nécessitant des réseaux multiples. Le découpage en sous-réseaux permet de le faire dans un environnement IP en n'utilisant qu'un seul numéro de réseau IP. En fait, c'est très souvent utilisé de nos jours par les fournisseurs d'accès Internet qui veulent donner à leurs clients connectés en permanence des numéros de réseau local IP statiques.
- Le trafic réseau est suffisamment élevé pour provoquer des ralentissements significatifs. En découpant le réseau en sous-réseaux, le trafic local à un segment de réseau peut être gardé localement - réduisant le trafic global et améliorant la connectivité du réseau sans nécessiter effectivement plus de bande passante pour le réseau.
- Des nécessités de sécurité peuvent très bien imposer que les différentes classes d'utilisateurs ne partagent pas le même réseau - puisque le trafic d'un réseau peut toujours être intercepté par un utilisateur compétent. Le découpage en sous-réseaux donne un moyen d'empêcher que le département marketing espionne le trafic sur le réseau de R & D (ou que les étudiants espionnent le réseau de l'administration)!

6 Comment découper un numéro de réseau IP en sous-réseaux

Ayant décidé que vous aviez besoin d'un découpage en sous-réseau, que faut-il faire pour le mettre en place? Le paragraphe suivant est une présentation des étapes qui seront expliquées ensuite en détail:

- mettre en place la connectivité physique (câblage de réseau, interconnexions de réseaux - comme les routeurs)
- choisir la taille de chaque sous-réseau en termes de nombre d'appareils qui y seront connectés - i.e. combien de numéros IP sont nécessaires pour chaque segment.
- calculer les masques et les adresses de réseau appropriés
- donner à chaque interface sur chaque réseau sa propre adresse IP et le masque de réseau approprié.
- configurer les routes sur les routeurs et les passerelles appropriés, les routes et/ou routes par défaut sur les appareils du réseau.
- tester le système, régler les problèmes, et ensuite se reposer!

Pour les besoins de cet exemple, nous supposerons que nous allons découper un numéro de réseau de classe C: 192.168.1.0

Ce numéro permet un maximum de 254 interfaces connectées (hôtes), plus les numéros obligatoires de réseau (192.168.1.0) et de diffusion (192.168.1.255).

6.1 Mettre en place la connectivité physique

Vous devrez installer l'infrastructure de câblage correcte pour tous les appareils que vous voulez interconnecter, définie pour correspondre à vos dispositions physiques.

Vous aurez aussi besoin d'un dispositif pour interconnecter les différents segments (routeurs, convertisseurs de médium physique etc...)

Une discussion détaillée de ceci n'est évidemment pas possible ici. Si vous avez besoin d'aide, il existe des consultants pour la conception et l'installation de réseau qui fournissent ce genre de service. Des conseils gratuits sont également disponibles sur un bon nombre de groupes de discussion Usenet (comme *comp.os.linux.networking*).

6.2 Choisir la taille des sous-réseaux

C'est un compromis entre le nombre de sous-réseaux que vous créez et le nombre de numéros IP 'perdus'.

Chaque réseau IP utilise deux adresses qui ne sont plus disponibles pour les adresses d'interfaces (hôtes) - le numéro de réseau IP lui-même, et l'adresse de diffusion sur ce réseau. Quand vous découpez en sous-réseaux, chaque sous-réseau a besoin de ses propres adresses de réseau et de diffusion - et celles-ci doivent être des adresses valides, dans l'intervalle fourni par le réseau IP que vous découpez.

Donc, en découpant un réseau IP en deux sous-réseaux séparés, on a alors deux adresses de réseau et deux adresses de diffusion - augmentant le nombre d'adresses 'inutilisables' pour les interfaces (hôtes); créer 4 sous-réseaux crée huit adresses inutilisables, et ainsi de suite...

En fait, le plus petit sous-réseau utilisable est composé de 4 numéros IP:

- deux numéros IP d'interface - un pour l'interface du routeur sur ce réseau, et un pour l'unique hôte de ce réseau.
- un numéro de réseau.
- une adresse de diffusion.

Maintenant, pourquoi quelqu'un voudrait créer un si petit réseau est une autre question! Avec un seul hôte sur ce réseau, toute communication en réseau devra sortir vers un autre réseau. Néanmoins, cet exemple montre le principe de diminution du nombre d'adresse d'interfaces qui s'applique au découpage en sous-réseaux.

En théorie, on peut découper son numéro de réseau IP en 2^n (où n est le nombre de bits d'interface dans votre numero de réseau, moins 1) sous-réseaux de tailles égales (vous pouvez aussi découper un sous-réseau et combiner des sous-réseaux).
Soyez donc réalistes en concevant votre réseau - vous devriez vouloir le nombre minimal de réseaux locaux séparés, qui corresponde à vos contraintes physiques, de gestion, d'équipement, et de sécurité!

6.3 Calculer le masque de sous-réseau et le numéro de réseau

Le masque de réseau est ce qui produit la magie du découpage d'un réseau IP en sous-réseaux.

Le masque de réseau pour un réseau IP non découpé est simplement un "quadruplet pointé" dont tous les 'bits de réseau' du numéro de réseau sont positionnés à '1', et tous les bits d'interface à '0'.

Donc, pour les trois classes de réseau IP, les masques de réseau sont:

- classe A (8 bits de réseau): 255.0.0.0

- classe B (16 bits de réseau): 255.255.0.0
- classe C (24 bits de réseau): 255.255.255.0

Pour mettre en oeuvre le découpage en sous-réseaux, on réserve un ou plusieurs bits parmi les bits d'interface, et on les interprète localement comme faisant partie des bits de réseau. Donc, pour diviser un numéro de réseau en deux sous-réseaux, on réservera un bit d'interface en positionnant à '1' le bit approprié dans le masque de réseau: le premier bit d'interface (pour un numéro de réseau 'normal').

Pour un réseau de classe C, cela donnera le masque de réseau:

```
11111111.11111111.11111111.10000000
```

ou 255.255.255.128

Pour notre numéro de réseau de classe C 192.168.1.0, voici quelqu'unes des options de découpage en sous-réseaux possibles:

```
Nombre de     Nbre d'hotes Masque de
sous-reseaux  par reseau   reseau
2             126          255.255.255.128 (11111111.11111111.11111111.10000000)
4             62           255.255.255.192 (11111111.11111111.11111111.11000000)
8             30           255.255.255.224 (11111111.11111111.11111111.11100000)
16            14           255.255.255.240 (11111111.11111111.11111111.11110000)
32            6            255.255.255.248 (11111111.11111111.11111111.11111000)
64            2            255.255.255.252 (11111111.11111111.11111111.11111100)
```

En théorie, il n'y a aucune raison de suivre la façon de découper ci-dessus, où les bits du masque de réseau sont ajoutés du bit d'interface le plus significatif au moins significatif. Néanmoins, si on ne le fait pas de cette façon, les numéros IP seront dans un ordre étrange! Cela rend extrêment difficile pour nous, humains, la decision du sous-réseau auquel appartient un numéro IP, puisque nous ne sommes pas spécialement doués pour penser en binaire (les ordinateurs d'un autre côté le sont, et utiliseront indifféremment tout schema que vous leur direz d'utiliser).

Vous étant décidé sur le masque de réseau approprié, vous devez maintenant trouver quelles sont les différentes adresses de réseau et de diffusion - et l'intervalle de numéros IP pour chacun de ces réseaux. A nouveau, en ne considerant qu'un numéro de réseau IP de classe C et en ne listant que la partie finale (la partie d'interface), on a:

```
Masque de   Sous-reseaux  Reseau Diffusion MinIP MaxIP Nbre    Nbre total
reseau                                             d'hotes d'hotes
128         2             0      127       1     126   126
                          128    255       129   254   126     252

192         4             0      63        1     62    62
                          64     127       65    126   62
                          128    191       129   190   62
                          192    255       193   254   62      248

224         8             0      31        1     30    30
                          32     63        33    62    30
                          64     95        65    94    30
```

96	127	97	126	30	
128	159	129	158	30	
160	191	161	190	30	
192	223	193	222	30	
224	255	225	254	30	240

Comme on peut le voir, il y a un ordre simple pour ces nombres, ce qui permet de les vérifier très facilement. L'"inconvénient" du découpage est aussi visible en termes de réduction du nombre total d'adresses d'interfaces (hôtes) disponibles, au fur et à mesure que le nombre de sous-réseaux augmente.

Avec ces informations, vous pouvez maintenant assigner les numéros IP d'interfaces et de réseaux, et les masques de réseau.

7 Le routage

Si vous utilisez un PC sous Linux avec deux interfaces réseaux pour router le trafic entre deux (ou plus) sous-réseaux, vous devez avoir compilé votre noyau avec l'option "IP Forwarding". Taper la commande:

```
cat /proc/ksyms | grep ip_forward
```

Vous devriez avoir quelque chose comme...

```
00141364 ip_forward_Rf71ac834
```

Si ce n'est pas le cas, alors vous n'avez pas activé l'option IP Forwarding lors de la compilation de votre noyau, et vous devrez recompiler et installer un nouveau noyau.

Pour le bien de cet exemple, supposons que vous ayez décidé de découper votre adresse de réseau IP 192.168.1.0 en 4 sous-réseaux (chacun d'eux comprenant 62 numéros IP d'interfaces/hôtes). Toutefois, deux de ces réseaux sont combinés en un unique plus grand sous-réseau, donnant trois réseaux physiques. C'est à dire:

Reseau	Diffusion	Masque de reseau	Hotes
192.168.1.0	192.168.1.63	255.255.255.192	62
192.168.1.64	192.168.1.127	255.255.255.192	62
182.168.1.128	192.168.1.255	255.255.255.126	124 (voir la note)

Note: la raison pour laquelle le dernier réseau n'a que 124 adresses utilisables (et pas 126 comme on pourrait le supposer d'après le masque de réseau) est que c'est en fait un 'super réseau' composé de deux sous-réseaux. Les hôtes sur les deux autres sous-réseaux interprèteront 192.168.1.192 comme l'adresse de réseau du sous-réseau 'inexistant'. De la même manière, ils interprèteront 192.168.1.191 comme l'adresse de diffusion du sous-réseau 'inexistant'.

Donc, si vous utilisez 192.168.1.191 ou 192 comme des adresses d'interfaces dans le troisième sous-réseau, alors les machines des deux autres sous-réseaux ne pourront pas communiquer avec ces interfaces.

Ceci illustre un point important du découpage en sous-réseaux - les adresses utilisables sont déterminées par le PLUS PETIT sous-réseau dans l'espace d'adressage du réseau.

7.1 Les tables de routage

Supposons qu'un ordinateur fonctionnant sous Linux serve de routeur pour ce réseau. Il aura trois interfaces réseau vers les réseaux locaux, et éventuellement une troisième interface vers Internet (qui devrait être sa route par défaut).

Supposons que l'ordinateur sous Linux utilise les plus petites adresses IP disponibles sur chaque sous-réseau pour son interface sur ce réseau. On configurerait ses interfaces réseau ainsi:

```
Interface       Adresse IP      Masque de reseau
eth0            192.168.1.1     255.255.255.192
eth1            192.168.1.65    255.255.255.192
eth2            192.168.1.129   255.255.255.128
```

Le routage utilisé serait:

```
Destination    Passerelle   Masque          Interface
192.168.1.0    0.0.0.0      255.255.255.192 eth0
192.168.1.64   0.0.0.0      255.255.255.192 eth1
192.168.1.128  0.0.0.0      255.255.255.128 eth2
```

Sur chacun des sous-réseaux, les hôtes seraient configurés avec leur propre adresse IP et masque de réseau (appropriés pour le réseau particulier). Chaque hôte déclarerait le PC sous Linux comme son routeur/passerelle, en spécifiant l'adresse IP de l'interface du PC sous Linux sur ce réseau particulier.

Robert Hart Melbourne, Australia March 1997.