

# Adressage IPv4

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions		
\$Revision: 1379 \$	\$Date: 2009-04-16 23:19:32 +0200 (jeu 16 avr 2009) \$	\$Author: latu \$
Corrections et compléments sur l'utilisation du routage inter-domaine sans classe ou «Classless Interdomain Routing» (CIDR).		
Résumé		
Le système d'adressage défini avec le protocole réseau du modèle TCP/IP est incontournable dans la mise en oeuvre des réseaux actuels. L'objet de cet article est de décrire succinctement le fonctionnement et les possibilités de l'adressage IP.		

## Table des matières

1. Copyright et Licence .....	2
1.1. Méta-information .....	2
1.2. Conventions typographiques .....	2
2. Le protocole IP de la couche Réseau .....	2
3. Le format des adresses IP .....	2
4. Les classes d'adresses .....	4
5. Le découpage d'une classe en sous-réseaux .....	5
6. Le routage inter-domaine sans classe .....	6
7. Un exemple pratique .....	8
8. Les réseaux privés & la traduction d'adresses (NAT) .....	9
9. En guise de conclusion .....	10

# 1. Copyright et Licence

Copyright (c) 2000,2009 Philippe Latu.  
 Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2009 Philippe Latu.  
 Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

## 1.1. Méta-information

Cet article est écrit avec *DocBook*<sup>1</sup> XML sur un système *Debian GNU/Linux*<sup>2</sup>. Il est disponible en version imprimable aux formats PDF et Postscript : [adressage.ipv4.pdf](#)<sup>3</sup> | [adressage.ipv4.ps.gz](#)<sup>4</sup>.

## 1.2. Conventions typographiques

Tous les exemples d'exécution des commandes sont précédés d'une invite utilisateur ou *prompt* spécifique au niveau des droits utilisateurs nécessaires sur le système.

- Toute commande précédée de l'invite \$ ne nécessite aucun privilège particulier et peut être utilisée au niveau utilisateur simple.
- Toute commande précédée de l'invite # nécessite les privilèges du super-utilisateur.

# 2. Le protocole IP de la couche Réseau

Le rôle fondamental de la couche réseau (niveau 3 du **modèle OSI**) est de déterminer la *route* que doivent emprunter les paquets. Cette fonction de recherche de chemin nécessite une identification de tous les hôtes connectés au réseau. De la même façon que l'on repère l'adresse postale d'un bâtiment à partir de la ville, la rue et un numéro dans cette rue, on identifie un hôte réseau par une *adresse* qui englobe les mêmes informations.

Le modèle TCP/IP utilise un système particulier d'adressage qui porte le nom de la couche réseau de ce modèle : *l'adressage IP*. Le but de cet article est de présenter le fonctionnement de cet adressage dans sa version la plus utilisée IPv4.

De façon très académique, on débute avec le **format des adresses IP**. On définit ensuite les **classes d'adresses IP**, le premier mode de découpage de l'espace d'adressage. Comme ce mode de découpage ne convenait pas du tout au développement de l'Internet, on passe en revue la chronologie des améliorations apportées depuis 1980 : **les sous-réseaux ou subnetting**, **la traduction d'adresses ou Native Address Translation (NAT)** et enfin **le routage inter-domaine sans classe**.

# 3. Le format des adresses IP

Les adresses IP sont composées de 4 octets. Par convention, on note ces adresses sous forme de 4 nombres décimaux de 0 à 255 séparés par des points.

<sup>1</sup> <http://www.docbook.org>

<sup>2</sup> <http://www.debian.org>

<sup>3</sup> <http://www.linux-france.org/prj/inetdoc/telechargement/adressage.ipv4.pdf>

<sup>4</sup> <http://www.linux-france.org/prj/inetdoc/telechargement/adressage.ipv4.ps.gz>

L'originalité de ce format d'adressage réside dans l'association de l'identification du réseau avec l'identification de l'hôte.

- La partie réseau est commune à l'ensemble des hôtes d'un même réseau,
- La partie hôte est unique à l'intérieur d'un même réseau.

Prenons un exemple d'adresse IP pour en identifier les différentes parties :

**Tableau 1. Exemple : adresse IP 192.168.1.1**

Adresse complète	192.168. 1. 1
Masque de réseau	255.255.255. 0
Partie réseau	192.168. 1.
Partie hôte	1
Adresse Réseau	192.168. 1. 0
Adresse de diffusion	192.168. 1.255

#### Le masque de réseau

Le masque de réseau sert à séparer les parties réseau et hôte d'une adresse. On retrouve l'adresse du réseau en effectuant un ET logique bit à bit entre une adresse complète et le masque de réseau.

#### L'adresse de diffusion

Chaque réseau possède une adresse particulière dite de *diffusion*. Tous les paquets avec cette adresse de destination sont traités par tous les hôtes du réseau local. Certaines informations telles que les annonces de service ou les messages d'alerte sont utiles à l'ensemble des hôtes du réseau.

Voici le même exemple obtenu avec l'affichage de la configuration des interfaces réseau d'un hôte avec un système GNU/Linux :

```
# ifconfig
eth0      Lien encap:Ethernet  HWaddr 00:04:75:FD:13:CD
          inet adr:192.168.1.1①  Bcast:192.168.1.255②  Masque:255.255.255.0③
          adr inet6: fe80::204:75ff:fe8d:13cd/64 Scope:Lien
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:158 errors:0 dropped:0 overruns:0 carrier:158
          collisions:0 lg file transmission:1000
          RX bytes:0 (0.0 b)  TX bytes:9558 (9.3 KiB)
          Interruption:5 Adresse de base:0xe800

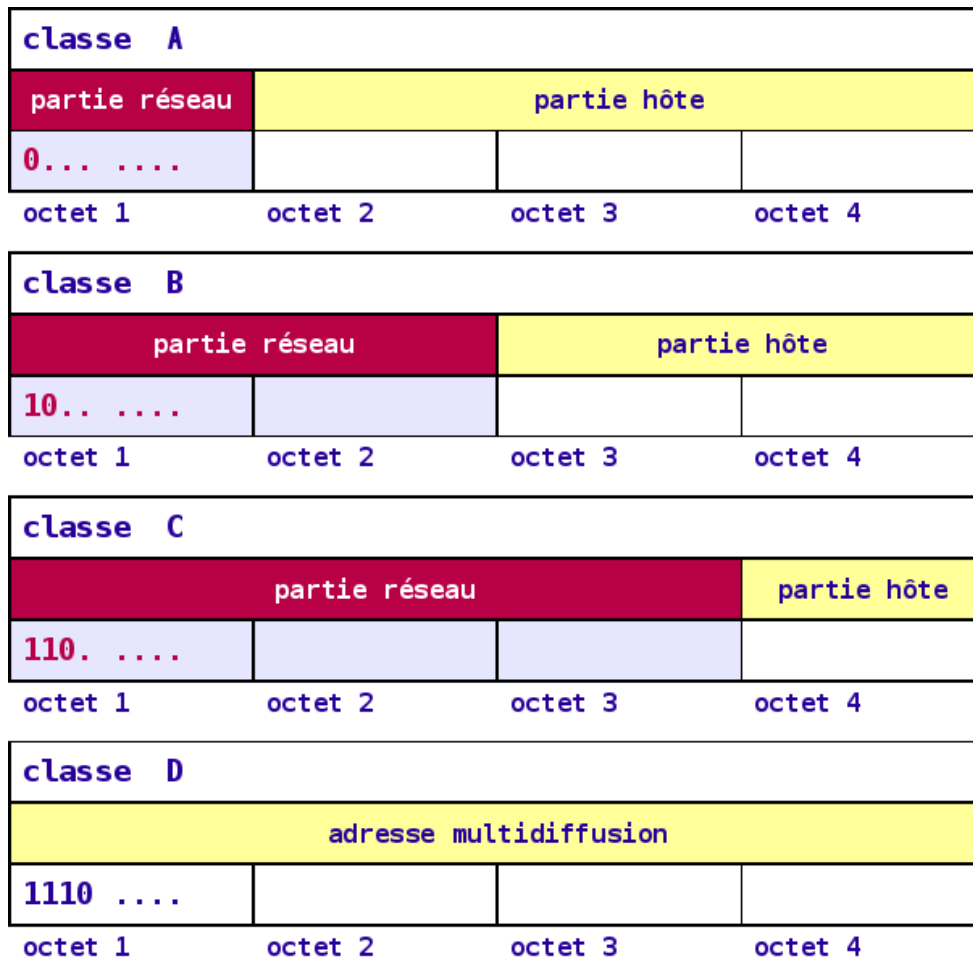
lo        Lien encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0④
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:4649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4649 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:1728470 (1.6 MiB)  TX bytes:1728470 (1.6 MiB)
```

- ① Les informations qui nous intéressent sont placées sur cette ligne. L'adresse 192.168.1.1 est l'adresse IP affectée à l'interface ethernet eth0.
- ② L'adresse de diffusion est 192.168.1.255 compte tenu du masque réseau.
- ③ Le masque réseau a pour valeur : 255.255.255.0.
- ④ L'interface de boucle locale lo joue un rôle très particulier. Elle est utilisée pour les communications réseau entre les processus locaux exécutés sur le système. Ces communications ne nécessitant aucun «contact» avec l'extérieur, aucune interface réseau physique ne doit être sollicitée.

Pour plus d'informations voir *Configuration d'une interface réseau*.

## 4. Les classes d'adresses

À l'origine, plusieurs groupes d'adresses ont été définis dans le but d'optimiser le cheminement (ou le *routing*) des paquets entre les différents réseaux. Ces groupes ont été baptisés *classes d'adresses IP*. Ces classes correspondent à des regroupements en réseaux de même taille. Les réseaux de la même classe ont le même nombre d'hôtes maximum.



Classes d'adresses IPv4 - image seule<sup>5</sup>

### Classe A

Le premier octet a une valeur comprise entre 1 et 126 ; soit un bit de poids fort égal à 0. Ce premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

L'adresse réseau 127.0.0.0 est réservée pour les communications en boucle locale.

### Classe B

Le premier octet a une valeur comprise entre 128 et 191 ; soit 2 bits de poids fort égaux à 10. Les 2 premiers octets désignent le numéro de réseau et les 2 autres correspondent à l'adresse de l'hôte.

### Classe C

Le premier octet a une valeur comprise entre 192 et 223 ; soit 3 bits de poids fort égaux à 110. Les 3 premiers octets désignent le numéro de réseau et le dernier correspond à l'adresse de l'hôte.

### Classe D

Le premier octet a une valeur comprise entre 224 et 239 ; soit 3 bits de poids fort égaux à 111. Il s'agit d'une zone d'adresses dédiées aux services de multi-diffusion vers des groupes d'hôtes (*host groups*).

### Classe E

Le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

<sup>5</sup> <http://www.linux-france.org/prj/inetdoc/articles/modelisation/images/classes.adresses.ipv4.png>

**Tableau 2. Espace d'adressage**

Classe	Masque réseau	Adresses réseau	Nombre de réseaux	Nombre d'hôtes par réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255	126	16777214
B	255.255.0.0	128.0.0.0 - 191.255.255.255	16384	65534
C	255.255.255.0	192.0.0.0 - 223.255.255.255	2097152	254
D	240.0.0.0	224.0.0.0 - 239.255.255.255	adresses uniques	adresses uniques

Le tableau ci-dessus montre que la distribution de l'espace d'adressage est mal répartie. On ne dispose pas de classe intermédiaire entre A et B alors que l'écart entre les valeurs du nombre d'hôte par réseau est énorme. La répartition en pourcentages de l'espace total d'adressage IP est :

- Classes A - 50%
- Classes B - 25%
- Classes C - 12.5%
- Classes D - 12.5%

À cette mauvaise distribution de l'espace d'adressage, il faut ajouter les nombreuses critiques sur la façon dont les attributions de classes IP ont été gérées dans les premières années de l'Internet. Comme les classes ont souvent été attribuées sur demande sans corrélation avec les besoins effectifs, on parle d'un grand «gaspillage».

Au cours des années, plusieurs générations de solutions ont été apportées pour tenter de compenser les problèmes de distribution de l'espace d'adressage. Les sections suivantes présentent ces solutions dans l'ordre chronologique.

## 5. Le découpage d'une classe en sous-réseaux

Pour compenser les problèmes de distribution de l'espace d'adressage IP, la première solution utilisée a consisté à découper une classe d'adresses IP A, B ou C en sous-réseaux. Cette technique appelée *subnetting* a été formalisée en 1985 avec le document [RFC950](#).

Si cette technique est ancienne, elle n'en est pas moins efficace face aux problèmes d'exploitation des réseaux contemporains. Il ne faut jamais oublier que le découpage en réseaux ou sous-réseaux permet de cloisonner les domaines de diffusion. Les avantages de ce cloisonnement de la diffusion réseau sont multiples.

- Au quotidien, on évite l'engorgement des liens en limitant géographiquement les annonces de services faites par les serveurs de fichiers. Les services Microsoft™ basés sur netBT sont particulièrement gourmands en diffusion réseau. En effet, bon nombre de tâches transparentes pour les utilisateurs supposent que les services travaillent à partir d'annonces générales sur le réseau. Sans ces annonces par diffusion, l'utilisateur doit désigner explicitement le service à utiliser. Le service d'impression est un bon exemple.
- Il existe quantité de vers et/ou virus dont les mécanismes de propagation se basent sur une reconnaissance des cibles par diffusion. Le ver *Sasser* en est un exemple caractéristique. En segmentant un réseau en plusieurs domaines de diffusion, on limite naturellement la propagation de code malveillant. Le *subnetting* devient alors un élément de la panoplie des outils de sécurité.

Pour illustrer le fonctionnement du découpage en sous-réseaux, on utilise un exemple pratique. On reprend l'exemple de la classe C 192.168.1.0 dont le masque réseau est par définition 255.255.255.0. Sans découpage, le nombre d'hôtes maximum de ce réseau est de 254. Considérant qu'un domaine de diffusion unique pour 254 hôtes est trop important, on choisit de diviser l'espace d'adressage de cette adresse de classe C. On *réserve* 3 bits supplémentaires du 4ème octet en complétant le masque réseau. De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte.

classe C avec subnetting sur 3 bits			
partie réseau			partie hôte
110. ....			111 00000
255	255	255	224
octet 1	octet 2	octet 3	octet 4

Classe C avec subnetting - image seule<sup>6</sup>

Tableau 3. adresse 192.168.1.0 avec subnetting sur 3 bits

Adresse réseau	192.168. 1. 0	Plage d'adresses utilisables	Adresse de diffusion
Masque de réseau	255.255.255.224		
Sous-réseau 0	192.168. 1. 0	192.168.1. 1 - 192.168.1. 30	192.168.1. 31
Sous-réseau 1	192.168. 1. 32	192.168.1. 33 - 192.168.1. 62	192.168.1. 63
Sous-réseau 2	192.168. 1. 64	192.168.1. 65 - 192.168.1. 94	192.168.1. 95
Sous-réseau 3	192.168. 1. 96	192.168.1. 97 - 192.168.1.126	192.168.1.127
Sous-réseau 4	192.168. 1.128	192.168.1.129 - 192.168.1.158	192.168.1.159
Sous-réseau 5	192.168. 1.160	192.168.1.161 - 192.168.1.190	192.168.1.191
Sous-réseau 6	192.168. 1.192	192.168.1.193 - 192.168.1.222	192.168.1.223
Sous-réseau 7	192.168. 1.224	192.168.1.225 - 192.168.1.254	192.168.1.255

Selon les termes du document [RFC950](#), les sous-réseaux dont les bits de masque sont tous à 0 ou tous à 1 ne devaient pas être utilisés pour éviter les erreurs d'interprétation par les protocoles de routage dits *classful* comme RIPv1. En effet, ces protocoles de routages de «première génération» ne véhiculaient aucune information sur le masque sachant que celui-ci était déterminé à partir de l'octet le plus à gauche. Dans notre exemple ci-dessus, il y avait confusion aux niveaux de l'adresse de réseau et de diffusion.

- L'adresse du sous-réseau 192.168.1.0 peut être considérée comme l'adresse réseau de 2 réseaux différents : celui avec le masque de classe C (255.255.255.0) et celui avec le masque complet après découpage en sous-réseaux (255.255.255.224).
- De la même façon, l'adresse de diffusion 192.168.1.255 est la même pour 2 réseaux différents : 192.168.1.0 ou 192.168.100.224.

Depuis la publication du document [RFC950](#), en 1985, les protocoles de routage qui servent à échanger les tables d'adresses de réseaux connectés entre routeurs ont évolué. Tous les protocoles contemporains sont conformes aux règles de routage inter-domaine sans classe (CIDR). Les protocoles tels que RIPv2, OSPF, BGP, etc. intègrent le traitement des masques de sous-réseaux. Ils peuvent même regrouper ces sous-réseaux pour optimiser le nombre des entrées des tables de routage. Pour appuyer cet argument, le document [RFC1878](#) de 1995 spécifie clairement que la pratique d'exclusion des sous-réseaux *all-zeros* et *all-ones* est obsolète.

## 6. Le routage inter-domaine sans classe

Le routage inter-domaine sans classe ou *Classless Inter-Domain Routing* (CIDR <sup>7</sup>) a été discuté par l'IETF à partir de 1992. Certaines projections de croissance de l'Internet prévoyaient une saturation complète de l'espace d'adressage IP pour 1994 ou 1995.

L'utilisation de cette technique a débuté en 1994 après la publication de 4 documents RFC : [RFC1517](#), [RFC1518](#), [RFC1519](#) et [RFC1520](#).

<sup>6</sup> <http://www.linux-france.org/prj/inetdoc/articles/adressage.ipv4/images/subnetting.ipv4.png>

<sup>7</sup> L'acronyme CIDR se prononce comme le «cidre» en anglais : *cider*.

Le principale proposition du document [RFC1519](#) publié en Septembre 1993 était de s'affranchir de la notion de classe en s'appuyant sur la notion de masque réseau qui était déjà très répandue à l'époque.

Le document [RFC1519](#) permet aux administrateurs réseau d'aller au delà du simple *subnetting* en donnant la capacité de faire du *supernetting*. En utilisant n'importe quel masque de sous-réseau ou masque de super-réseau possible, on ne se limite plus aux masques classiques des classes : 255.0.0.0, 255.255.0.0 et 255.255.255.0. Cette technique de *supernetting* associée au masque réseau de longueur variable (*Variable Length Subnet Mask* ou VLSM) a résolu les problèmes d'attribution de l'espace d'adressage IPv4 et d'accroissement des tables de routage de l'Internet.

Le problème d'attribution de l'espace d'adressage IPv4 a été diminué parce que l'*Internet Assigned Numbers Authority* n'a plus été contraint au déploiement d'espaces adresses «pleins» (*classful*). Au lieu d'avoir la moitié de l'espace d'adressage IPv4 réservé pour les gros réseaux massifs de classe A, cet espace a été découpé en tranches de plus petites tailles, plus faciles à utiliser. Le routage inter-domaine sans classe (CIDR), associé à la traduction d'adresses de réseau (NAT, document [RFC1631](#) de 1994), a permis au protocole IPv4 de survivre plus de dix ans au delà de la limite annoncée. Alors que les spécialistes sont encore préoccupés par l'attribution de l'espace d'adressage et la migration vers le nouveau protocole IPv6 qui utilise des adresses sur 128 bits (au lieu de 32 bits pour IPv4), plus personne ne parle de catastrophe due à l'épuisement de cet espace d'adressage.

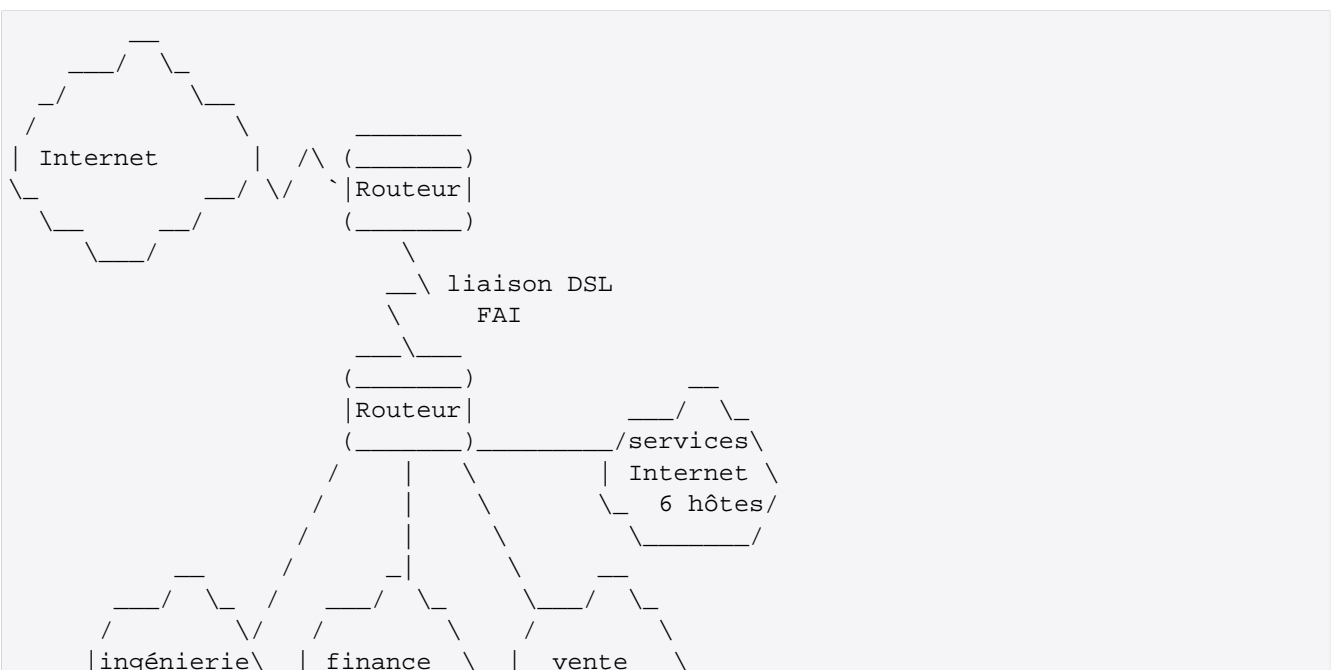
Le problème des tailles de table de routage a été également résolu à l'aide des techniques CIDR et VLSM. Le *supernetting* fournit aux administrateurs un masque unique pour représenter des réseaux multiples en une seule entrée de table de routage.

Par exemple, un fournisseur d'accès Internet (FAI) à qui on a assigné le réseau 94.20.0.0, peut attribuer des sous-réseaux à ses clients (94.20.1.0 à la société A, 94.20.2.0 à la société B, etc.) et injecter l'adresse 94.20.0.0/255.255.0.0 dans les tables de routage pour représenter tous ses réseaux.

La technique de masque réseau de longueur variable (VLSM) permet à un client de n'acquérir que la moitié de cet espace ; par exemple le réseau 94.20.0.0/255.255.128.0 attribue la plage d'adresses allant de 94.20.0.0 à 94.20.127.0. La plage 94.20.128.0 - 94.20.254.0 peut être vendue à une autre société.

La capacité de synthétiser (*summarize*) de multiples sous-réseaux en une adresse et un masque de super-réseau réduit significativement les tailles des tables de routage. Bien que ces tailles de tables augmentent encore, les capacités (mémoire et traitement) des équipements d'interconnexion sont maintenant suffisantes pour gérer cette croissance plus lente.

La technique VLSM n'est pas seulement utile aux principaux fournisseurs d'accès Internet (FAI). Un administrateur possédant plus d'un sous-réseau peut utiliser cette technique pour utiliser son espace assigné plus efficacement. Considérons l'exemple ci-dessous :



$\backslash$  15 hôtes /     $\backslash$  12 hôtes /     $\backslash$  15 hôtes /  
 $\backslash$                     /     $\backslash$                     /     $\backslash$                     /

Le fournisseur d'accès a attribué le réseau 120.1.50.0 avec le masque 255.255.255.128. On dispose donc de la deuxième moitié du réseau 120.1.50.0. On peut alors redécouper ce réseau de la façon suivante :

**Tableau 4. adresse 120.1.50.0 avec VLSM**

Nom	Sous-réseau	Masque	Plage d'adresses	Nombre d'hôtes
Liaison FAI	120.1.50.0	255.255.255.240	120.1.50.1 - 120.1.50.14	14
Services Internet	120.1.50.16	255.255.255.240	120.1.50.17 - 120.1.50.30	14
Ingénierie	120.1.50.32	255.255.255.224	120.1.50.33 - 120.1.50.62	30
Finance	120.1.50.64	255.255.255.224	120.1.50.65 - 120.1.50.94	30
Finance	120.1.50.96	255.255.255.224	120.1.50.97 - 120.1.50.126	30

On note que le nombre maximum d'adresses d'hôtes disponibles correspond à l'espace d'adressage du sous-réseau moins deux. C'est parce que la première adresse désigne le réseau et que la dernière est l'adresse spéciale de diffusion vers tous les hôtes du sous-réseau. Lorsque l'on planifie les espaces d'adressage VLSM, il est préférable de doubler le nombre d'adresses disponibles de chaque sous-réseau pour prévoir les évolutions futures.

Pour s'affranchir des masques des classes d'adresses IP, une nouvelle notation a été introduite. Elle consiste à noter le nombre de bits à 1 du masque après le caractère '/' à la suite de l'adresse.

En reprenant l'exemple précédent de découpage d'une adresse de classe C en sous-réseaux, on peut noter le troisième sous-réseau sous la forme : 120.1.50.32/27.

La notation /27 correspond à 27 bits de masque réseau à 1 ; soit un masque complet de 255.255.255.224.

Les techniques de routage inter-domaine sans classe (CIDR) et de masque réseau de longueur variable (VLSM) n'ont pas seulement sauvé l'Internet de la catastrophe ; elles sont aussi un outil très utile pour l'optimisation de l'utilisation de votre propre espace d'adressage IPv4.

## 7. Un exemple pratique

Pour configurer l'interface d'un hôte qui doit se connecter à un réseau existant, on nous donne l'adresse 172.16.19.40/21 :

**Q :** Quel est le masque réseau de cette adresse ?

**R :** La notation condensée /21 indique que la partie réseau de l'adresse occupe 21 bits. On décompose ces 21 bits en 8 bits . 8 bits . 5 bits ; ce qui donne : 255.255.248.0.

**Q :** Combien de bits ont été réservés pour les sous-réseaux privés ?

**R :** La valeur du premier octet de l'adresse étant comprise entre 128 et 192, il s'agit d'une adresse de classe B. Le masque réseau d'une classe B étant 255.255.0.0, 5 bits ont été réservés sur le troisième octet pour constituer des sous-réseaux.

**Q :** Combien de sous-réseaux privés sont disponibles ?

**R :** Le nombre de valeurs codées sur 5 bits est de  $2^5$  soit 32. Suivant la génération du protocole de routage utilisé, on applique deux règles différentes.

- Historiquement, on devait exclure le premier (*all-zeros*) et le dernier (*all-ones*) sous-réseau conformément au document [RFC950](#) de 1985. Cette règle suppose que les protocoles de routage utilisent uniquement la classe du réseau routé sans tenir compte de son masque et donc de sa longueur variable.

Dans ce cas, le nombre de sous-réseaux utilisables est 30.

- Dans les réseaux contemporains, on peut retenir l'ensemble des sous-réseaux sachant que les protocoles de routage véhiculent les masques de longueurs variables dans chaque entrée de table de routage. Cette règle est applicable depuis la publication des documents standard relatifs au routage inter-domaine sans classe (*CIDR*) notamment le [RFC1878](#) de 1995.

Dans ce cas, le nombre de sous-réseaux utilisables est 32.

**Q :** Combien d'hôtes peut contenir chaque sous-réseau ?

**R :** Les adresses des hôtes sont codées sur les bits à 0 du masque réseau. Avec le masque /21, il reste :  $32 - 21 = 11$  bits. Le nombre de valeurs codées sur 11 bits est de  $2^{11}$  soit 2048. Chaque sous-réseau peut contenir 2046 hôtes. On a retiré la valeur 0 puisqu'elle sert à identifier l'adresse du réseau et non celle d'un hôte ainsi que la valeur avec les 11 bits à 1 qui sert à la diffusion sur le sous-réseau.

**Q :** Quelle est l'adresse du sous-réseau de l'exemple ?

**R :** Les deux premiers octets étant compris dans la partie réseau, ils restent inchangés. Le quatrième octet (40) étant compris dans la partie hôte, il suffit de le remplacer par 0. Le troisième octet (19) est partagé entre partie réseau et partie hôte. Si on le convertit en binaire, on obtient : 00010011. En faisant un ET logique avec la valeur binaire correspondant 5 bits réseau (11111000) on obtient : 00010000 ; soit 16 en décimal. L'adresse du sous-réseau est donc 172.16.16.0.

**Q :** Quelle est l'adresse de diffusion du sous-réseau de l'exemple ?

**R :** Les deux premiers octets étant compris dans la partie réseau, ils restent inchangés. Le quatrième octet (40) étant compris dans la partie hôte, il suffit de le remplacer par 255. Le troisième octet (19) est partagé entre partie réseau et partie hôte. Si on le convertit en binaire, on obtient : 00010011. On effectue cette fois-ci un OU logique avec la valeur binaire correspondant aux 3 bits d'hôtes à un (00000111). On obtient : 00010111 ; soit 23 en décimal. L'adresse de diffusion du sous-réseau est donc 172.16.23.255.

## 8. Les réseaux privés & la traduction d'adresses (NAT)

Les réseaux privés se sont développés en «réaction» à deux évolutions de l'Internet : la mauvaise utilisation de l'espace d'adressage IPv4 et les besoins de sécurisation des réseaux d'entreprises.

Ces évolutions ont conduit à la conception de réseaux dits privés n'ayant que peu ou pas d'interfaces exposées sur le réseau public l'Internet.

Pour planifier l'adressage d'un réseau privé, il faut distinguer deux cas de figure :

- Si le réseau privé n'est *jamaïs* interconnecté avec d'autres réseaux (notamment l'Internet), on peut utiliser n'importe quelle adresse.
- Si le réseau privé peut être interconnecté avec d'autres réseaux via un routeur, on doit utiliser les adresses réservées à cet usage. Ces adresses sont données dans le document [RFC1918](#).

Dans la pratique, c'est le second cas de figure que l'on retrouve le plus souvent.

**Tableau 5. Réseaux privés**

Classe	Masque réseau	Adresses réseau	Notation CIDR
A	255.0.0.0	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	255.240.0.0	172.16.0.0 - 172.31.255.255	172.16.0.0/12

Classe	Masque réseau	Adresses réseau	Notation CIDR
C	255.255.0.0	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Aujourd'hui, un fournisseur d'accès Internet (FAI) attribue dynamiquement une ou plusieurs adresses IP à l'interface de l'équipement qui réalise la connexion (modem dans le cas d'une connexion téléphonique ou ADSL). Il est possible, avec ce type de configuration, de partager la connexion Internet entre tous les hôtes du réseau privé et/ou de mettre à disposition un serveur sur le réseau public. C'est grâce à la traduction d'adresses que ces fonctions sont réalisées.

Dans le monde GNU/Linux, les mécanismes de traduction d'adresses sont inclus dans la partie filtrage, appelée `netfilter`, des fonctions réseau du noyau Linux.

La conception des fonctions de traduction d'adresses introduites dans le noyau Linux est très intéressante sur le plan pédagogique. On distingue très bien les deux usages de ces fonctions :

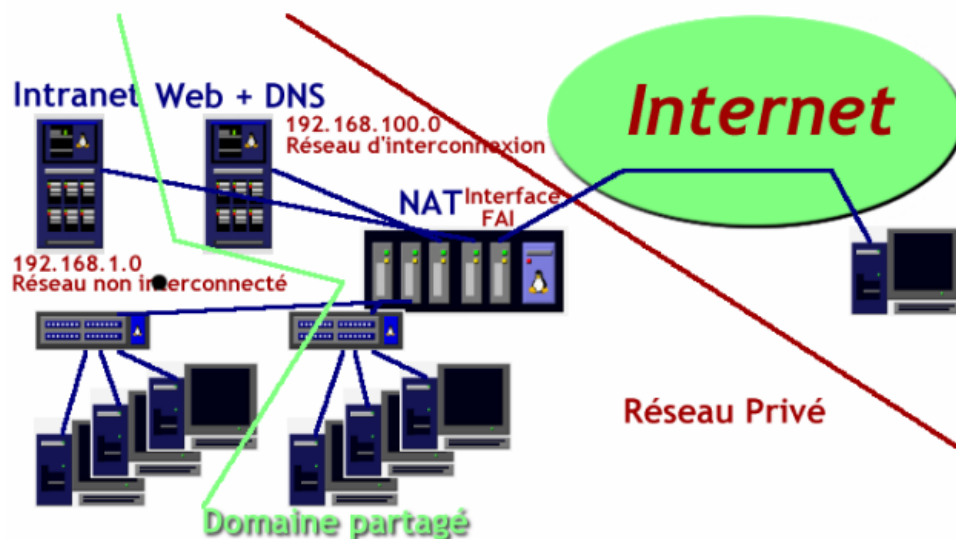
- partager une interface unique du réseau public Internet entre tous les hôtes du réseau privé,
- rendre un serveur situé dans le réseau privé accessible depuis l'Internet avec un bon niveau de sécurité.

Dans le premier cas, on parle de *traduction d'adresses source* (S-NAT). Ce sont les adresses sources des paquets IP émis par les hôtes du réseau privé qui sont réécrites avec une adresse IP publique.

Dans le second cas, on parle de *traduction d'adresses destination* (D-NAT). Une adresse IP destination publique est réécrite avec une adresse IP privée en fonction du service Internet demandé.

Ces usages des fonctions de traduction d'adresses avec Linux ont été décrits pour la première fois dans le document de référence *Guide Pratique du NAT sous Linux*.

Le mécanisme général de «réutilisation d'adresses IP» a été décrit dans le document standard [RFC1631](#).



Traduction d'Adresses IP - image seule<sup>8</sup>

- **Accès depuis le réseau privé vers l'Internet.**  
Les adresses des hôtes du réseau privé sont *traduites* avec l'adresse de l'interface connectée à Internet.
- **Accès depuis l'Internet vers le réseau privé.**  
Les appels de services (HTTP, DNS, courrier, etc.) sont *traduites* avec l'adresse du serveur concerné dans le réseau privé.

## 9. En guise de conclusion

Cette présentation étant limitée à l'adressage du protocole de couche réseau IP, elle doit être complétée par une étude des mécanismes de fonctionnement du protocole et de l'intégration de ce protocole dans la pile des protocoles du modèle

<sup>8</sup> <http://www.linux-france.org/prj/inetdoc/articles/adressage.ipv4/images/nat.png>

Internet TCP/IP. Voici donc quelques pistes pour avancer dans la compréhension du fonctionnement des technologies réseau utilisées sur l'Internet.

#### Modélisations réseau

Le document *Modélisations réseau*<sup>9</sup> compare les deux principaux modèles : OSI et TCP/IP puis présente une synthèse baptisée «modèle contemporain» associant les avantages de chacun.

#### Understanding IP addressing

Pour aller plus loin dans l'étude de l'adressage IP, n'oubliez pas de lire l'article *Comprendre l'adressage IP*<sup>10</sup> signé Chuck Semeria.

Les exemples de problèmes d'adressage IP donnés dans les annexes B, C, D et E sont d'excellents exercices d'entraînement sur l'étude des plans d'adressage.

#### Internet Assigned Numbers Authority, IANA

L' *Internet Assigned Numbers Authority*<sup>11</sup> est l'organisme, situé au sommet de l'Internet, chargé de l'attribution des plages d'adresses IP, de l'enregistrement des numéros de ports des protocoles et des serveurs de noms de domaines de niveau haut.

#### Guide Pratique du NAT sous Linux

*guide NAT-HOWTO*<sup>12</sup> : ce document décrit comment réaliser du camouflage d'adresse IP, un serveur mandataire transparent, de la redirection de ports ou d'autres formes de Traduction d'Adresse Réseau (*Network Address Translation* ou NAT) avec le noyau Linux.

#### Configuration d'une interface réseau

Le support *Configuration d'une interface de réseau local*<sup>13</sup> décrit pas à pas les étapes de configuration d'une interface réseau sur un système GNU/Linux.

#### Documents standards RFC sur le découpage en sous-réseaux

- Ces documents standard sont référencés dans la section **Section 5, « Le découpage d'une classe en sous-réseaux »**.
- *RFC950 Internet Standard Subnetting Procedure*<sup>14</sup> : ce document traite de l'utilité des sous-réseaux (*subnets*). Ce sont des sous-ensembles logiques d'un réseau Internet unique.

À l'époque de la publication de ce document, les protocoles de routage tels que RIPv1 utilisaient la classe du réseau routé dans les mécanismes d'acheminement des paquets IP. L'usage du premier sous-réseau *all-zeros* était exclu sachant qu'il était impossible de distinguer l'adresse réseau du réseau complet de l'adresse de ce premier sous-réseau. L'usage du dernier sous-réseau (*all-ones*) était aussi exclu sachant qu'il était impossible de distinguer l'adresse de diffusion du réseau de l'adresse de ce dernier sous-réseau.

- *RFC1878 Variable Length Subnet Table For IPv4*<sup>15</sup> : ce document apporte une clarification sur les difficultés relatives au découpage en sous-réseaux des réseaux IP. Il fournit une table standard de sous-réseaux.

Depuis la publication de ce document, il est possible d'utiliser l'ensemble des sous-réseaux sachant que les protocoles de routage véhiculent le masque que chaque entrée de réseau.

#### Documents standards RFC sur le routage inter-domaine sans classe

- Ces documents standard sont référencés dans la **Section 6, « Le routage inter-domaine sans classe »**.
- *RFC1517 Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)*<sup>16</sup> : point de départ des discussions au sein de l'IETF sur une réforme de la gestion de l'espace d'adressage IP à partir des 3 arguments avancés au début des années 90 : épuisement de l'espace d'adressage de classe B du fait de l'absence de classe de taille intermédiaire entre classe B et classe A, surcharge des tables de routage des routeurs de l'Internet et épuisement de l'espace d'adressage IP sur 32 bits..

<sup>9</sup> <http://www.linux-france.org/prj/inetdoc/articles/modelisation/>

<sup>10</sup> <http://www.linux-france.org/prj/inetdoc/telechargement/501302.pdf>

<sup>11</sup> <http://www.iana.org/>

<sup>12</sup> <http://www.linux-france.org/prj/inetdoc/guides/NAT-HOWTO/NAT-HOWTO-4.html#ss4.1>

<sup>13</sup> <http://www.linux-france.org/prj/inetdoc/cours/config.interface.lan/>

<sup>14</sup> <http://www.faqs.org/rfcs/rfc950.html>

<sup>15</sup> <http://www.faqs.org/rfcs/rfc1878.html>

<sup>16</sup> <http://www.faqs.org/rfcs/rfc1517.html>

- **RFC1518 *An Architecture for IP Address Allocation with CIDR***<sup>17</sup> : cet article fournit une architecture et un plan d'affectation des adresses d'IP sur l'Internet. Cette architecture et le plan sont prévus pour jouer un rôle important en orientant l'Internet vers l'affectation d'adresses avec une stratégie d'agrégation.
- **RFC1519 *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy***<sup>18</sup> : cette note discute des stratégies d'affectation d'adresses IP de l'espace existant dans le but de préserver l'espace d'adressage et de limiter la croissance explosive des tables de routage dans les routeurs «sans route par défaut».
- **RFC1520 *Exchanging Routing Information Across Provider Boundaries in the CIDR Environment***<sup>19</sup> : le but de ce document est double. D'abord, il décrit diverses solutions pour échanger l'information de routage inter-domaine à travers les limites de domaine, où un du domaine est «CIDR-capable» et l'autre pas. Ensuite, il traite des implications d'exécution des protocoles de routage inter-domaine «CIDR-capable» (par exemple, BGP-4, IDRP) relativement au routage intra-domaine.

#### Documents standards RFC sur la traduction d'adresses

- Ces documents standard sont référencés dans la **Section 8, « Les réseaux privés & la traduction d'adresses (NAT) »**.
- **RFC1631 *The IP Network Address Translator (NAT)***<sup>20</sup> : ce document propose une autre solution à court terme (ndt. pour répondre au problème de saturation de l'espace d'adressage IPv4 en 1994), la réutilisation d'adresse, qui complète le routage interdomaine sans classe (CIDR) ou même le rend inutile. La solution de réutilisation d'adresse consiste à placer des traducteurs d'adresse de réseau (NAT) aux frontières des réseaux d'extrémités (*stub networks*).
- **RFC1918 *Address Allocation for Private Internets***<sup>21</sup> : ce document décrit l'attribution d'adresse pour les réseaux privés. L'attribution permet la pleine connectivité de couche réseau parmi tous les centres serveurs à l'intérieur d'une entreprise aussi bien que parmi tous les centres serveurs publics de différentes entreprises.

---

<sup>17</sup> <http://www.faqs.org/rfcs/rfc1518.html>

<sup>18</sup> <http://www.faqs.org/rfcs/rfc1519.html>

<sup>19</sup> <http://www.faqs.org/rfcs/rfc1520.html>

<sup>20</sup> <http://www.faqs.org/rfcs/rfc1631.html>

<sup>21</sup> <http://www.faqs.org/rfcs/rfc1918.html>