Adressage IPv4

Philippe Latu
philippe.latu(at)inetdoc.net

http://www.inetdoc.net

Résumé

Le système d'adressage défini avec le protocole réseau du modèle TCP/IP est incontournable dans la mise en œuvre 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 1
2. Le protocole IP de la couche Réseau 2
3. Le format des adresses IP 2
4. Les classes d'adresses 3
5. Le découpage d'une classe en sous-réseaux 4
6. Le routage inter-domaine sans classe 6
7. Un exemple pratique 8
8. Les réseaux privés & la traduction d'adresses (NAT) 9
9. Exercices sur l'adressage IPv4 11
10. En guise de conclusion 15

1. Copyright et Licence

```
Copyright (c) 2000,2015 Philippe Latu.
Permission is granted to copy, distribute and/or modify this document under the
terms of the GNU Free Documentation License, Version 1.3 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) 2000,2015 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 1.3 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 ».
```

Méta-information

Cet article est écrit avec DocBook[1] XML sur un système Debian GNU/Linux[2]. Il est disponible en version imprimable au format PDF : `adressage.ipv4.pdf`[3].

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.

[1] http://www.docbook.org
[2] http://www.debian.org
[3] http://www.inetdoc.net/pdf/adressage.ipv4.pdf

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.

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 un exemple d'affichage de la configuration des interfaces réseau d'un hôte avec un système de type GNU/Linux. On a volontairement conservé l'affichage des multiples adresses réseau d'une même interface. L'exercice consiste ici à identifier les adresses IPv4 présentée dans le tableau ci-dessus.

```
$ ip addr ls
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo❶
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP \
                                                    group default qlen 1000
    link/ether ba:ad:00:ca:fe:00 brd ff:ff:ff:ff:ff:ff
    inet ❷192.168.1.1/24❸ brd 192.168.1.255❹ scope global eth0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:feb2:10:b8ad:ff:feca:fe00/64 scope global dynamic
       valid_lft 2591986sec preferred_lft 604786sec
    inet6 fe80::b8ad:ff:feca:fe00/64 scope link
       valid_lft forever preferred_lft forever
```

❶ 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.

❷ 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`.

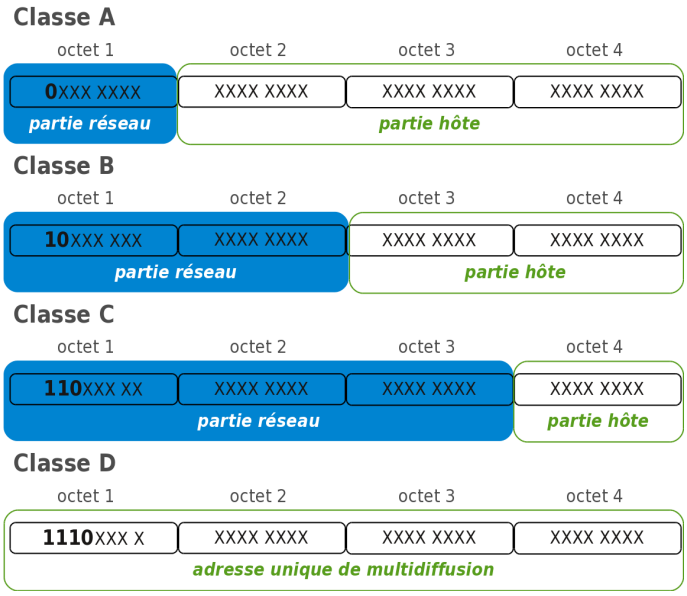
❸ Le masque réseau en notation CIDR est `/24` ; soit 24 bits consécutifs à 1 en partant de la gauche. En notation développée, il correspond à : `255.255.255.0`.

❹ L'adresse de diffusion est `192.168.1.255` compte tenu du masque réseau.

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 routage) 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.



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 égux à `111`. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion 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.

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
E	non défini	240.0.0.0 - 255.255.255.255	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 - 6.25%
- Classes E - 6.25%

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 simple 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 Micro$oft™ 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.

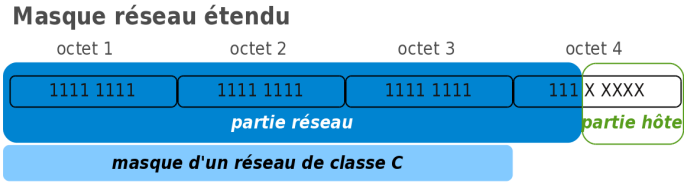


Tableau 3. adresse `192.168.1.0` avec subnetting **sur 3 bits**

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 `192.168.1.224`.

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 et BGP 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 [4]) 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.

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 dont l'utilisation 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 bien au delà de la limite annoncée.

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 `94.20.0.0/16`, peut attribuer des sous-réseaux à ses clients (`94.20.1.0/24` à la société A, `94.20.2.0/24` à la société B, etc.) et publier l'adresse `94.20.0.0/16` 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 `94.20.0.0/17` 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 modernes sont largement suffisantes pour gérer cette croissance.

Le fait de réduire le nombre de bits à 1 du masque réseau permet d'optimiser le nombre des entrées dans une table de routage. Même si cette utilisation du routage inter-domaine sans classe dépasse le cadre de ce document, voici un exemple simplifié qui permet de regrouper les 4 réseaux de la liste ci-dessous en une seule entrée avec un masque réseau réduit.

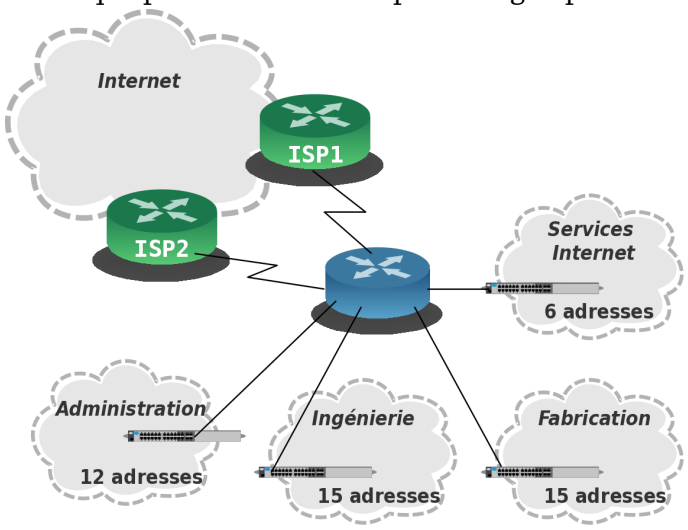
```
172.16.12.0/24 10101100.00010000.000011 00. 00000000
172.16.13.0/24 10101100.00010000.000011 01. 00000000
172.16.14.0/24 10101100.00010000.000011 10. 00000000
172.16.15.0/24 10101100.00010000.000011 11. 00000000
```

La technique du supernetting est basée sur l'identification des bits communs à toutes les adresses de réseau à synthétiser. Dans la liste des 4 réseaux ci-dessus les 22 premiers bits ne varient pas. L'adresse de réseau qui «synthétise» ces 4 entrées est donc :

[4] L'acronyme CIDR se prononce comme le «cidre» en anglais : cider.

```
Address:   172.16.12.0          10101100.00010000.000011 00.00000000
Netmask:   255.255.252.0 = 22   11111111.11111111.111111 00.00000000
```

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



Le fournisseur d'accès a attribué le réseau `198.51.100.0` avec le masque `255.255.255.128` ; soit l'adresse réseau `198.51.100.0/25`. On dispose donc de la moitié du réseau `198.51.100.0/24`. Suivant les contraintes issues du graphique ci-dessus, on peut découper ce réseau de la façon suivante :

Tableau 4. adresse `198.51.100.0` avec VLSM

Nom	Sous-réseau	Notation CIDR	Masque	Plage d'adresses	Nombre d'hôtes
Liaison ISP1	`198.51.100.0`	/30	`255.255.255.252`	`198.51.100.1` - `198.51.100.2`	2
Liaison ISP2	`198.51.100.4`	/30	`255.255.255.252`	`198.51.100.5` - `198.51.100.6`	2
Services Internet	`198.51.100.16`	/28	`255.255.255.240`	`198.51.100.17` - `198.51.100.30`	14
Administration	`198.51.100.32`	/27	`255.255.255.224`	`198.51.100.33` - `198.51.100.62`	30
Ingénierie	`198.51.100.64`	/27	`255.255.255.224`	`198.51.100.65` - `198.51.100.94`	30
Fabrication	`198.51.100.96`	/27	`255.255.255.224`	`198.51.100.97` - `198.51.100.126`	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 : `198.51.100.32/27`.

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 (temporairement) de la catastrophe ; elles sont aussi un outil très utile pour l'optimisation de l'utilisation de l'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` :

Q1 Quel est le masque réseau de cette adresse ?

R : La notation condensée `/21` indique que le 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`.

Q2 Combien de bits ont été réservés pour les sous-réseaux privés relativement à la définition historique de classe ?

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.

Q3 Combien de sous-réseaux privés sont disponibles relativement à la définition historique de classe ?

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. On parle alors de routage classful.

  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. On parle alors de routage classless.

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

Q4 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.

Q5 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`.

Q6 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 on 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 jamais 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`
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 :

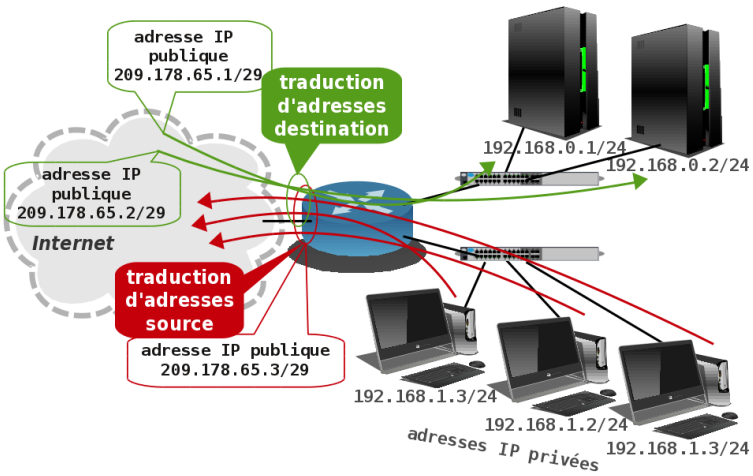
- partager une interface unique du réseau public Internet entre tous les hôtes du réseau privé,
- rendre un serveur situé dans le réseau privé accessible depuis l'Internet avec un bon niveau de sécurité.

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.



- **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. Exercices sur l'adressage IPv4

Voici quelques exercices très classiques sur l'adressage IPv4. Ils sont tous basés sur le fait que la partie réseau d'une adresse définit un groupe logique dont tous les hôtes partagent un même domaine de diffusion. Toutes les questions sont relatives aux limites de ces groupes logiques.

Q7. Soit l'adresse `192.16.5.133/29`. Combien de bits sont utilisés pour identifier la partie réseau ? Combien de bits sont utilisés pour identifier la partie hôte ?

Correction :

```
Address:   192.16.5.133          11000000.00010000.00000101.10000 101
Netmask:   255.255.255.248 = 29  11111111.11111111.11111111.11111 000
```

Partie réseau : 29 bits - partie hôte : 3bits

Q8. Soit l'adresse `172.16.5.10/28`. Quel est le masque réseau correspondant ?

Correction :

```
Address:   172.16.5.10           10101100.00010000.00000101.0000 1010
Netmask:   255.255.255.240 = 28  11111111.11111111.11111111.1111 0000
```

Masque réseau : `255.255.255.240`

Q9. On attribue le réseau `132.45.0.0/16`. Il faut redécouper ce réseaux en 8 sous-réseaux.

a. Combien de bits supplémentaires sont nécessaires pour définir huit sous-réseaux ?

b. Quel est le masque réseau qui permet la création de huit sous-réseaux ?

c. Quelle est l'adresse réseau de chacun des huit sous-réseaux ainsi définis ?

d. Quelle est la plage des adresses utilisables du sous-réseau numéro 3 ?

e. Quelle est l'adresse de diffusion du sous-réseau numéro 4 ?

Correction :

```
Address:   132.45.0.0            10000100.00101101. 00000000.00000000
Netmask:   255.255.0.0 = 16      11111111.11111111. 00000000.00000000
```

a. Pour découper l'adresse réseau de départ en huit sous-réseaux, 3 bits supplémentaires sont nécessaires (2^3 = 8).

b. Le nouveau masque réseau est `255.255.224.0`

```
Address:   132.45.0.0            10000100.00101101.000 00000.00000000
Netmask:   255.255.224.0 = 19    11111111.11111111.111 00000.00000000
```

c. Pour obtenir la liste des huit adresses de sous-réseaux, on construit la table des combinaisons binaires sur les 3 bits supplémentaires du masque réseau.

Numéro 0 : `10000100.00101101.000 00000.00000000` soit `132.45.0.0`
Numéro 1 : `10000100.00101101.001 00000.00000000` soit `132.45.32.0`
Numéro 2 : `10000100.00101101.010 00000.00000000` soit `132.45.64.0`
Numéro 3 : `10000100.00101101.011 00000.00000000` soit `132.45.96.0`
Numéro 4 : `10000100.00101101.100 00000.00000000` soit `132.45.128.0`
Numéro 5 : `10000100.00101101.101 00000.00000000` soit `132.45.160.0`
Numéro 6 : `10000100.00101101.110 00000.00000000` soit `132.45.192.0`
Numéro 7 : `10000100.00101101.111 00000.00000000` soit `132.45.224.0`

d. Adresse du sous-réseau numéro 3 : `132.45.96.0`

```
Network:   132.45.96.0/19       10000100.00101101.011 00000.00000000
HostMin:   132.45.96.1          10000100.00101101.011 00000.00000001
HostMax:   132.45.127.254       10000100.00101101.011 11111.11111110
```

e. Adresse de diffusion du sous-réseau numéro 4 : `132.45.159.255`

```
Network:   132.45.128.0/19      10000100.00101101.100 00000.00000000
HostMin:   132.45.128.1         10000100.00101101.100 00000.00000001
HostMax:   132.45.159.254       10000100.00101101.100 11111.11111110
Broadcast: 132.45.159.255       10000100.00101101.100 11111.11111111
```

Q10. On attribue le réseau `200.35.1.0/24`. Il faut définir un masque réseau étendu qui permette de placer 20 hôtes dans chaque sous-réseau.

a. Combien de bits sont nécessaires sur la partie hôte de l'adresse attribuée pour accueillir au moins 20 hôtes ?

b. Quel est le nombre maximum d'adresses d'hôte utilisables dans chaque sous-réseau ?

c. Quel est le nombre maximum de sous-réseaux définis ?

d. Quelles sont les adresses de tous les sous-réseaux définis ?

e. Quelle est l'adresse de diffusion du sous-réseau numéro 2 ?

Correction :

a. Il est nécessaire de réserver un minimum de 5 bits pour pouvoir définir au moins 20 adresses d'hôte. Sachant que l'espace total d'adressage occupe 32 bits, il reste 27 bits pour la partie réseau (32 - 5 = 27).

b. La relation entre le nombre de bits (n) de la partie hôte d'une adresse IPv4 et le nombre d'adresses utilisables est : 2^n - 2. Les deux combinaisons retirées sont l'adresse de réseau (tous les bits de la partie hôte à 0) et l'adresse de diffusion (tous les bits de la partie hôte à 1).

   Dans le cas présent, avec 5 bits d'adresses pour la partie hôte, le nombre d'adresses utilisables est 30 (2^5 - 2 = 30).

c. Le masque du réseau attribué occupe 24 bits et le masque étendu 27 bits (voir question précédente). Le codage des adresses de sous-réseau utilise donc 3 bits. Avec 3 bits, on peut coder 8 (2^3) combinaisons binaires soit 8 sous-réseaux.

d. Pour obtenir la liste des huit adresses de sous-réseaux, on construit la table des combinaisons binaires sur les 3 bits supplémentaires du masque réseau.

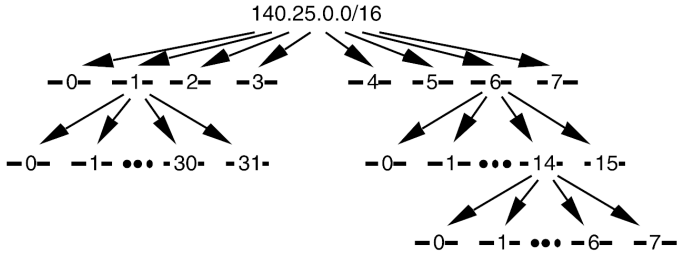
   Numéro 0 : `11001000.00100011.00000001.000 00000` soit `200.35.1.0`
   Numéro 1 : `11001000.00100011.00000001.001 00000` soit `200.35.1.32`
   Numéro 2 : `11001000.00100011.00000001.010 00000` soit `200.35.1.64`
   Numéro 3 : `11001000.00100011.00000001.011 00000` soit `200.35.1.96`
   Numéro 4 : `11001000.00100011.00000001.100 00000` soit `200.35.1.128`
   Numéro 5 : `11001000.00100011.00000001.101 00000` soit `200.35.1.160`
   Numéro 6 : `11001000.00100011.00000001.110 00000` soit `200.35.1.192`
   Numéro 7 : `11001000.00100011.00000001.111 00000` soit `200.35.1.224`

e. L'adresse de diffusion du sous-réseau numéro 2 correspond à la combinaison binaire pour laquelle tous les bits de la partie hôte sont à 1 et l'adresse réseau `200.35.1.64`.

```
Address:   200.35.1.64          11001000.00100011.00000001.010 00000
Netmask:   255.255.255.224 = 27 11111111.11111111.11111111.111 00000
Broadcast: 200.35.1.95          11001000.00100011.00000001.010 11111
```

   Cette adresse de diffusion correspond à l'adresse du sous-réseau suivant moins 1. Partant de l'adresse du sous-réseau numéro 3 : `200.35.1.96` on enlève 1 pour obtenir l'adresse de diffusion du sous-réseau numéro 2 : `200.35.1.95`.

Q11. On attribue le réseau `140.25.0.0/16` et on étudie le déploiement de sous-réseaux avec des masques réseau de longueur variable ou Variable Length Subnet Mask (VLSM). Voici le schéma de découpage de ces sous-réseaux.



Pour aboutir à ce découpage en sous-réseaux, le premier travail consiste à diviser le préfixe réseau initial en 8 sous-réseaux de même taille. Parmi ces 8 sous-réseaux, le réseau numéro 1 est à nouveau découpé en 32 sous-réseaux et le réseau numéro 6 en 16 sous-réseaux. Enfin, le sous-réseau numéro 14 du dernier sous-ensemble est lui même découpé en 8 sous-réseaux.

a. Quelle est la liste des adresses des 8 sous-réseaux issus du découpage de premier niveau ?

b. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 3 ?

c. Quelle est la liste des adresses des 16 sous-réseaux obtenus à partir du sous-réseau numéro 6 ?

d. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 6 - 3 ?

e. Quelle est l'adresse de diffusion du sous-réseau numéro 6 - 5 ?

f. Quelle est la plage des adresses utilisables pour le sous-réseau numéro 6 - 14 - 2 ?

g. Quelle est l'adresse de diffusion du sous-réseau numéro 6 - 14 - 5 ?

Correction :

a. La masque du réseau attribué occupe 16 bits et il faut utiliser 3 bits supplémentaires pour définir 8 sous-réseaux. On liste donc les adresses des réseaux obtenus avec un masque sur 19 bits.

Numéro 0 : `10001100.00011001.000 00000.0000000` soit `140.25.0.0`
Numéro 1 : `10001100.00011001.001 00000.0000000` soit `140.25.32.0`
Numéro 2 : `10001100.00011001.010 00000.0000000` soit `140.25.64.0`
Numéro 3 : `10001100.00011001.011 00000.0000000` soit `140.25.96.0`
Numéro 4 : `10001100.00011001.100 00000.0000000` soit `140.25.128.0`
Numéro 5 : `10001100.00011001.101 00000.0000000` soit `140.25.160.0`
Numéro 6 : `10001100.00011001.110 00000.0000000` soit `140.25.192.0`
Numéro 7 : `10001100.00011001.111 00000.0000000` soit `140.25.224.0`

b. La plage des adresses utilisables pour le sous-réseau numéro 3 (`140.25.96.0/19` est obtenue en ajoutant 1 à l'adresse de ce réseau et en soustrayant 2 à l'adresse du réseau suivant.

```
Network:   140.25.96.0/19       10001100.00011001.011 00000.00000000
HostMin:   140.25.96.1          10001100.00011001.011 00000.00000001
HostMax:   140.25.127.254       10001100.00011001.011 11111.11111110
```

c. La masque du sous-réseau numéro 6 occupe 19 bits et il faut utiliser 4 bits supplémentaires pour définir 16 sous-réseaux. On liste donc les adresses des réseaux obtenus avec un masque sur 23 bits.

Numéro 00 : `10001100.00011001.1100000 0.00000000` soit `140.25.192.0`
Numéro 01 : `10001100.00011001.1100001 0.00000000` soit `140.25.194.0`
Numéro 02 : `10001100.00011001.1100010 0.00000000` soit `140.25.196.0`
Numéro 03 : `10001100.00011001.1100011 0.00000000` soit `140.25.198.0`
Numéro 04 : `10001100.00011001.1100100 0.00000000` soit `140.25.200.0`

Numéro 05 : `10001100.00011001.1100101 0.00000000` soit `140.25.202.0`
Numéro 06 : `10001100.00011001.1100110 0.00000000` soit `140.25.204.0`
Numéro 07 : `10001100.00011001.1100111 0.00000000` soit `140.25.206.0`
Numéro 08 : `10001100.00011001.1101000 0.00000000` soit `140.25.208.0`
Numéro 09 : `10001100.00011001.1101001 0.00000000` soit `140.25.210.0`
Numéro 10 : `10001100.00011001.1101010 0.00000000` soit `140.25.212.0`
Numéro 11 : `10001100.00011001.1101011 0.00000000` soit `140.25.214.0`
Numéro 12 : `10001100.00011001.1101100 0.00000000` soit `140.25.216.0`
Numéro 13 : `10001100.00011001.1101101 0.00000000` soit `140.25.218.0`
Numéro 14 : `10001100.00011001.1101110 0.00000000` soit `140.25.220.0`
Numéro 15 : `10001100.00011001.1101111 0.00000000` soit `140.25.222.0`

d. La plage des adresses utilisables pour le sous-réseau numéro 6 - 3 (`140.25.198.0/23` est obtenue en ajoutant 1 à l'adresse de ce réseau et en soustrayant 2 à l'adresse du réseau suivant.

```
Network:   140.25.198.0/23      10001100.00011001.1100011 0.00000000
HostMin:   140.25.198.1         10001100.00011001.1100011 0.00000001
HostMax:   140.25.199.254       10001100.00011001.1100011 1.11111110
```

e. L'adresse de diffusion du sous-réseau numéro 6 - 5 est obtenue en soustrayant 1 à l'adresse du sous-réseau numéro 6 - 6.

```
Network:   140.25.202.0/23      10001100.00011001.1100101 0.00000000
Broadcast: 140.25.203.255       10001100.00011001.1100101 1.11111111
```

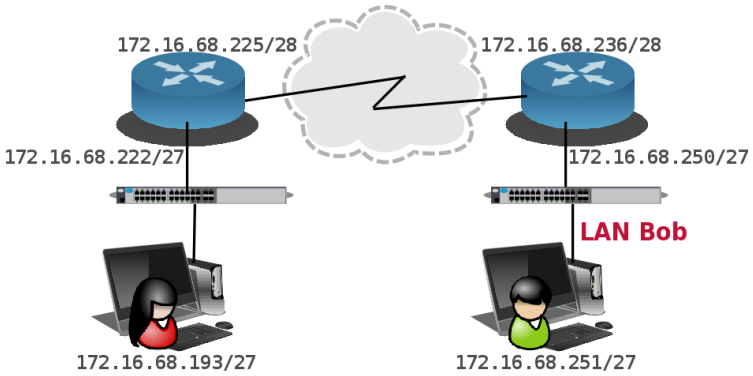
f. L'adresse du sous-réseau numéro 6 - 14 est donnée dans la liste ci-dessus : `140.25.220.0/23`. Comme ce sous-réseau est lui même découpé en 8 nouveau sous-réseaux, le masque occupe 26 bits. En suivant la même méthode que dans les cas précédents, on obtient l'adresse du sous-réseau numéro 6 - 14 - 2 : `140.25.220.128/26`. On en déduit la plage des adresses utilisables.

```
Network:   140.25.220.128/26    10001100.00011001.11011100.10 000000
HostMin:   140.25.220.129       10001100.00011001.11011100.10 000001
HostMax:   140.25.220.190       10001100.00011001.11011100.10 111110
```

g. L'adresse de diffusion du sous-réseau numéro 6 - 5 est obtenue en soustrayant 1 à l'adresse du sous-réseau numéro 6 - 14 - 6.

```
Network:   140.25.221.64/26     10001100.00011001.11011101.01 000000
Broadcast: 140.25.221.127       10001100.00011001.11011101.01 111111
```

Q12. Alice est au bord de la crise de nerfs ! Aucun des messages envoyés à Bob n'est arrivé à destination. Bob est lui aussi sur le point de craquer ! Il essaie désespérément d'envoyer des messages à Alice sans succès. Il faut absolument faire quelque chose pour les aider.



Quelle erreur a été commise dans l'affectation des adresses (et|ou) des masques réseau ?

Proposer une solution pour rendre les communications possibles.

Correction :

On étudie les plages d'adresses utilisables pour chacun des réseaux : le LAN d'Alice, la liaison WAN et le LAN de Bob.

a. L'espace d'adressage du LAN d'Alice a les limites suivantes.

```
Network:   172.16.68.192/27     10101100.00010000.01000100.110 00000
HostMin:   172.16.68.193        10101100.00010000.01000100.110 00001
HostMax:   172.16.68.222        10101100.00010000.01000100.110 11110
```

Les adresses affectées aux interfaces du poste de travail et du routeur sont bien comprises dans les limites du réseau `172.16.68.192/27`. Le problème ne vient pas de ce réseau.

b. L'espace d'adressage de la liaison WAN a les limites suivantes.

```
Network:   172.16.68.224/28     10101100.00010000.01000100.1110 0000
HostMin:   172.16.68.225        10101100.00010000.01000100.1110 0001
HostMax:   172.16.68.238        10101100.00010000.01000100.1110 1110
```

Les adresses affectées aux interfaces WAN des deux routeurs sont bien comprises dans les limites du réseau `172.16.68.224/28`. Les adresses de réseau du LAN d'Alice et de la liaison WAN ne se recouvrent pas. Le problème ne vient pas non plus de ce réseau.

c. L'espace d'adressage du LAN de Bob a les limites suivantes.

```
Network:   172.16.68.224/27     10101100.00010000.01000100.111 00000
HostMin:   172.16.68.225        10101100.00010000.01000100.111 00001
HostMax:   172.16.68.254        10101100.00010000.01000100.111 11110
```

Si les adresses affectées aux interfaces du poste de travail et du routeur de Bob sont bien comprises dans les limites du réseau `172.16.68.224/27`, le LAN de Bob et la liaison WAN partagent le même espace d'adressage. Le routeur de Bob est donc bien incapable de prendre une décision d'acheminement des paquets d'un réseau vers l'autre. Le problème vient donc de ce dernier réseau.

Une solution simple consiste à compléter le masque réseau du LAN de Bob de façon à ce qu'il n'y ait plus chevauchement avec la liaison WAN. Avec un masque sur 29 bits on aurait les caractéristiques suivantes. Alice et Bob pourraient enfin échanger des messages.

```
Network:   172.16.68.248/29     10101100.00010000.01000100.11111 000
HostMin:   172.16.68.249        10101100.00010000.01000100.11111 001
HostMax:   172.16.68.254        10101100.00010000.01000100.11111 110
```

10. En guise de conclusion

Cette présentation étant limitée à l'adressage du protocole de couche réseau IP en version 4, 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 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[5] 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[6] 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.

[5] http://www.inetdoc.net/articles/modelisation/
[6] http://www.inetdoc.net/pdf/501302.pdf

Internet Assigned Numbers Authority, IANA
: L' Internet Assigned Numbers Authority[7] 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 Pratique du NAT[8] : 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[9] 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[10] : 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[11] : 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)[12] : 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..
- RFC1518 An Architecture for IP Address Allocation with CIDR[13] : cet article fournit une architecture et un plan d'affectation des adresses 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[14] : cette note discute des stratégies d'affectation d'adresses IP de l'espace existant dans

[7] http://www.iana.org/
[8] http://www.netfilter.org/documentation/HOWTO/fr/NAT-HOWTO.html
[9] http://www.inetdoc.net/travaux_pratiques/config.interface.lan/
[10] https://www.rfc-editor.org/rfc/rfc950.txt
[11] https://www.rfc-editor.org/rfc/rfc1878.txt
[12] https://www.rfc-editor.org/rfc/rfc1517.txt
[13] https://www.rfc-editor.org/rfc/rfc1518.txt
[14] https://www.rfc-editor.org/rfc/rfc1519.txt

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[15] : 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 d'un domaine dans le cas où un du domaine est CIDR-capable et l'autre pas. Ensuite, il traite des conséquences de l'utilisation des protocoles de routage inter-domaine (BGP-4, IDRP) dans le 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)[16] : 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 inter-domaine sans classe (CIDR). 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[17] : 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.

[15] https://www.rfc-editor.org/rfc/rfc1520.txt
[16] https://www.rfc-editor.org/rfc/rfc1631.txt
[17] https://www.rfc-editor.org/rfc/rfc1918.txt