

Petit cours sur les masques de sous réseau

Eric LALITTE

5 juillet 2002

Table des matières

1	Introduction	4
1.1	Objet de ce cours	4
1.2	Réutilisation de ce cours	4
1.3	Décharge	4
1.4	Votre travail	4
2	Définitions	5
2.1	L'identification des machines	5
2.2	La segmentation des réseaux	5
2.3	Une seule adresse pour le prix de deux	5
2.4	Définition empirique du masque	6
2.5	Pourquoi maîtriser les masques?	6
3	Adresse IP et masque	7
3.1	L'adressage IP	7
3.2	Nombre de machines	7
3.3	La séparation grâce au masque	7
3.4	Le couple adresse IP et masque	7
4	Le codage	8
4.1	Le codage binaire	8
4.2	Pourquoi un codage binaire pour les ordinateurs?	8
4.3	Qu'est-ce qu'un octet?	8
4.4	Ecriture binaire de l'adresse IP	9
5	Les masques	10
5.1	Récapitulatif	10
5.2	Comment représente-t-on un masque?	10
5.3	Comment le masque et l'adresse IP sont ils associés?	10
5.4	Adresses spécifiques (réseau, broadcast)	11
5.5	Les bits à 1 et à 0 doivent ils être contigus?	11
5.6	Quelles adresses pour les masques?	12
5.7	Faire fi de l'écriture par octets	13
5.8	Quelle est cette notation avec un /, comme /24?	13

6	Comment bien choisir son masque ?	15
6.1	Partir de l'existant	15
6.2	En fonction du nombre de machines	15
6.3	Comment déterminer la plage d'adresses à partir du masque et d'une adresse ?	16
6.4	Une méthode simple pour trouver les adresses de réseau possibles	16
6.5	Comment découper une plage réseau quelconque comme somme de plusieurs plages ?	17
6.6	Plages réservées (RFC 1918)	18
7	Comment découper une plage d'adresses en plusieurs sous réseaux ?	19
7.1	Détermination des masques pour chacun des réseaux	19
7.2	Détermination des plages réseau	19
7.3	Le résultat	20
8	Que sont les classes d'adresses A, B, C, D... ?	21
8.1	Historique	21
8.2	Définitions	21
8.3	Y a-t-il une pénurie d'adresses IPv4 ?	22
8.4	Le système d'adressage par classes est-il viable ?	22
8.5	Qu'est-ce que l'adressage CIDR ?	22
9	Trucs et astuces avec les masques	23
9.1	Comment déterminer qu'une machine appartient à mon réseau ?	23
9.2	Des machines sur un même réseau peuvent elles avoir des masques différents ?	24
9.3	Puis-je utiliser un outil qui calcule pour moi ?	25
9.4	Tout ça c'est bien, mais quand est ce que je l'utilise ce masque moi ?	25
10	Mini lexique	27
11	Annexes	28
11.1	Ressources utilisées	28
11.2	Remerciements	28
11.3	Faq sur la NAT	28
12	Conclusion	29

1 Introduction

1.1 Objet de ce cours

Dans le monde des réseaux, on utilise souvent des termes inintelligibles pour le commun des mortels n'ayant pas une formation informatique poussée. Les masques en font partie, d'autant plus que leur compréhension et leur utilisation n'est pas toujours simple (au départ ;-) Le but de ce cours est de présenter de façon la plus compréhensible possible ce que sont les masques, à quoi ils servent, comment bien les utiliser et se familiariser avec.

Pour cela, nous traiterons aussi quelques sujets annexes qui nous permettront de mieux comprendre l'utilité des masques, comme les réseaux logiques, quelques notions de routage, etc.

1.2 Réutilisation de ce cours

Vous êtes libre d'utiliser de courts extraits de ce cours, dans la mesure où vous incluez un lien permettant d'avoir accès à l'ensemble du document. Ceci dans le but de permettre à vos lecteurs d'obtenir facilement un complément d'information. De même, vous êtes libre de copier ce cours dans son intégralité, à condition cependant d'en avertir l'auteur, et que cette utilisation soit exempte de tout caractère commercial (bannières publicitaires incluses). Cette restriction étant principalement due au plus élémentaire des respects : celui du temps que j'ai consacré à la rédaction de ce cours. Toute autre utilisation devra faire l'objet d'un accord préalable avec l'auteur.

1.3 Décharge

L'auteur décline toute responsabilité concernant la mauvaise utilisation ou compréhension du cours qui engendrerait l'écroulement de votre réseau ;-).

1.4 Votre travail

La seule et unique tâche que je vous demanderai d'accomplir sera de corriger mes erreurs (aussi bien dans la cohérence des éléments avancés que pour l'orthographe), me donner des conseils sur ce qui est mal expliqué pour le rendre plus accessible, ajouter des éléments qui ont attiré aux masques et rendent l'exposé plus complet, combler tout manque pour améliorer ce cours.

2 Définitions

2.1 L'identification des machines

Pour envoyer du courrier à un ami, vous utilisez son adresse postale. Ainsi vous êtes sûr que le paquet que vous envoyez arrivera à la bonne personne. Et bien pour les ordinateurs, c'est pareil. Quand vous connectez votre ordinateur à un réseau (Internet par exemple), il possède une adresse qui l'identifie d'une façon unique pour que les autres ordinateurs du réseau puissent lui envoyer des informations.

2.2 La segmentation des réseaux

Imaginez un énorme réseau comme Internet où chacune des machines serait obligée de connaître l'ensemble des millions d'autres machines (et notamment leurs adresses) et de savoir comment y accéder. Cela obligerait nos pauvres ordinateurs à avoir des tables énormes contenant l'ensemble de ces informations. Cela induirait aussi des temps de réponses très grands pour parcourir cette table.

Pour répondre à cette problématique, on a segmenté cet énorme réseau en différents petits réseaux. Et c'est au sein de ces petits réseaux que l'on donne des adresses aux machines pour leur envoyer l'information. Ainsi, il suffit de connaître l'adresse du réseau pour envoyer l'information à une machine de celui-ci, et c'est à l'intérieur de ce réseau que l'information sera redirigée vers la bonne machine.

C'est exactement comme lorsque vous envoyez un paquet par la poste, vous mettez le nom de la ville, le paquet arrive à la poste de la ville, et c'est elle qui distribue le paquet à la bonne adresse.

2.3 Une seule adresse pour le prix de deux

Comme vous l'avez compris, il nous faut deux adresses pour identifier une machine, une pour le réseau et une pour la machine elle-même. Cependant, l'adressage qui a été choisi pour les machines ne définit qu'une seule adresse. Vous me direz que ce n'est pas suffisant. Et bien si ! Il suffit de segmenter cette adresse en deux parties distinctes, l'une pour le réseau, et l'autre pour

la machine. C'est la ou le masque entre en jeu, c'est lui qui joue le rôle de séparateur entre ces deux adresses.

2.4 Définition empirique du masque

Le masque est un séparateur entre la partie réseau et la partie machine d'une adresse IP.

2.5 Pourquoi maîtriser les masques ?

L'utilisation et la maîtrise des masques doit pouvoir vous permettre d'une part, de savoir ce que vous manipulez, et d'autre part d'optimiser le fonctionnement de votre réseau. Effectivement, l'utilisation des masques vous permettra de segmenter de la façon la plus correcte l'adressage de votre réseau, et ainsi de séparer les machines sensibles du reste du réseau, limiter les congestions, et prévoir l'évolution de votre réseau, etc.

Malheureusement, la séparation d'un réseau en plusieurs sous-réseaux n'a pas que des avantages. L'un des désavantages majeurs est notamment la complexification des tables de routage étant donné le plus grand nombre de réseaux à router.

3 Adresse IP et masque

3.1 L'adressage IP

Nous avons parlé d'adresses pour les machines, il est temps maintenant de définir ces adresses. On parle d'adresse IP (Internet protocol), car il s'agit du protocole qui permet d'identifier les machines et de router les informations sur Internet. Ces adresses sont codées sur 4 octets (voir chapitre 4 sur le codage binaire) et sont la plupart du temps écrite en numérotation décimale en séparant les octets par des points. Ca donne quelque chose comme ça : 192.168.132.24

3.2 Nombre de machines

En y regardant d'un peu plus près, on peut calculer le nombre de machines que l'on peut identifier à l'aide de cet adressage. Ainsi, on utilise 4 octets, soit 32 bits, soit encore 2^{32} adresses (2 à la puissance 32 adresses) Or $2^{32} = 4\ 294\ 967\ 296$, on peut donc définir plus de 4 milliards d'adresses!!!

3.3 La séparation grâce au masque

Cependant, nous avons vu qu'il fallait séparer cette adresse en deux parties pour pouvoir identifier à la fois le réseau et l'adresse. Le masque comme l'adresse IP est une suite de 4 octets, soit 32 bits. Chacun des ces bits peuvent prendre la valeur 1 ou 0. Et bien il nous suffit de dire que les bits à 1 représenteront la partie réseau de l'adresse, et les bits à 0 la partie machine. Ainsi, on fera une association entre une adresse IP et un masque pour savoir dans cette adresse IP quelle est la partie réseau et quelle est la partie machine de l'adresse.

3.4 Le couple adresse IP et masque

Le masque servant à faire la séparation en deux parties sur une adresse IP, il est donc indissociable de celle-ci. Une adresse seule ne voudra rien dire puisqu'on ne saura pas quelle est la partie réseau et quelle est la partie machine. De la même façon, un masque seul n'aura pas de valeur puisqu'on n'aura pas d'adresse sur laquelle l'appliquer.

4 Le codage

4.1 Le codage binaire

Nous utilisons tous les jours un système de numération décimale. Avec donc 10 symboles (0123456789) qui nous permettent d'énumérer toute sorte de nombre en les plaçant dans un certain ordre. Cette place est primordiale puisqu'elle représente le passage aux dizaines, centaines, milliers, etc. Ainsi, tout nombre peut se décomposer en puissances de 10, par exemple :

$$324 = 300 + 20 + 4 = 3*10^2 + 2*10^1 + 4*10^0.$$

Cependant, il existe d'autres modes selon la base dans laquelle on se place. Lorsque l'on utilise la base 2, on se place en numération binaire où seuls deux symboles sont utilisés. On peut, de la même façon, décomposer tout nombre en puissance de 2.

$$\begin{aligned} 324 &= 256 + 64 + 4 \\ &= 1*2^8 + 0*2^7 + 1*2^6 + 0*2^5 + 0*2^4 \\ &\quad + 0*2^3 + 1*2^2 + 0*2^1 + 0*2^0. \end{aligned}$$

4.2 Pourquoi un codage binaire pour les ordinateurs ?

Pour les ordinateurs, c'est ce choix du codage binaire qui a été fait. Pourtant, il aurait été plus simple d'utiliser la base 10 avec laquelle nous sommes familiers. Cependant, les informations liées aux ordinateurs circulent sur des fils électriques. Sur ces fils, il est difficile de distinguer plus de deux états pour le signal, on peut par exemple choisir un état à 0 volts, et un autre pour 5 volts. On se retrouve donc avec deux valeurs possibles. C'est pour cela qu'on a choisi un codage binaire avec deux valeurs possible, 0 et 1.

4.3 Qu'est-ce qu'un octet ?

Un octet est une séquence de huit bits. C'est donc un nombre codé avec huit bits. Ainsi, si on transpose sa valeur en décimal, on obtient un nombre qui peut varier entre 0 et 255. Donc, dans une adresse IP, on ne pourra pas trouver d'autre nombre que ceux compris entre 0 et 255. Une adresse comme 192.65.25.428 ne peut pas être une adresse IP valide vu que son dernier octet n'est pas compris entre 0 et 255.

4.4 Écriture binaire de l'adresse IP

Nous avons vu que l'adresse IP était composée de 4 octets écrits en notation décimale, séparés par des points, par exemple : 192.168.25.132. Cette adresse peut aussi bien s'écrire en binaire :

11000000.10101000.00011001.10000100

Nous verrons par la suite pourquoi il est utile de revenir à cette notation pour bien comprendre le fonctionnement des masques.

5 Les masques

5.1 Récapitulatif

Nous avons déjà vu plusieurs aspects importants des masques qu'il faudra toujours essayer de garder à l'esprit :

- Codés sur 4 octets, soit 32 bits,
- Ils permettent de faire la séparation entre la partie réseau et la partie machine de l'adresse IP,
- La partie réseau est représentée par des bits à 1, et la partie machine par des bits à 0,
- Le masque ne représente rien sans l'adresse IP à laquelle il est associé.

5.2 Comment représente-t-on un masque ?

Comme le masque est codé sur 32 bits, voici un exemple possible de masque :

```
-----Réseau-----      Machine
|                         | |   |
11111111.11111111.11111111.00000000
```

Maintenant, plusieurs questions peuvent se poser. Jusqu'ici je comprends, mais comment je peux associer ce masque à une adresse IP, et quel sera le résultat ? Pourquoi les bits à 1 sont séparés de ceux à 0 ?

5.3 Comment le masque et l'adresse IP sont ils associés ?

Prenons par exemple une machine qui a pour adresse IP 192.168.25.147. Il nous faut lui associer un masque pour savoir quelle partie de cette adresse représente le réseau. Associons lui le masque précédent 255.255.255.0. On remarque que les bits des trois premiers octets sont à 1, ils représentent donc la partie réseau de l'adresse, soit 192.168.25, le 147 permettant d'identifier la machine au sein de ce réseau. Dans cet exemple, on remarque qu'un octet a été réservé pour l'adresse machine, ce qui nous donne $2^8 = 256$ adresses disponibles pour les machines sur le réseau 192.168.25.

Les adresses disponibles pour les machines seront donc :

192.168.25.0 (réservée pour le réseau, voir 5.4)
192.168.25.1
...
192.168.25.254
192.168.25.255 (réservée pour le broadcast, voir 5.4)

On observe donc que c'est le masque qui détermine le nombre de machines d'un réseau. Ainsi, on verra par la suite qu'on choisira le masque en fonction du nombre de machines que l'on veut installer.

5.4 Adresses spécifiques (réseau, broadcast)

Il existe des adresses spécifiques au sein d'un réseau. La première adresse d'une plage ainsi que la dernière ont un rôle particulier. La première adresse d'une plage représente l'adresse du réseau. Celle-ci est très importante car c'est grâce à elle qu'on peut identifier les réseaux et router les informations d'un réseau à un autre. La dernière adresse d'une plage représente ce que l'on appelle l'adresse de broadcast. Cette adresse représente en fait l'ensemble des adresses du réseau. Ainsi, quand on veut envoyer une information à toutes les machines, on utilise cette adresse.

Dans notre exemple, l'adresse de réseau sera donc 192.168.25.0, et l'adresse de broadcast 192.168.25.255. On remarque donc qu'il ne nous reste plus que 254 adresses pour identifier nos machines. Ainsi, à chaque fois que l'on choisira un masque en fonction du nombre de machines que l'on veut adresser, il faudra tenir compte de ces deux adresses...

5.5 Les bits à 1 et à 0 doivent ils être contigus ?

Dans l'exemple de masque que nous avons choisi, nous avons vu que les bits à 0 et à 1 étaient regroupés. Cela n'est pas une obligation, mais cela facilite énormément l'exploitation du réseau. En conservant la contiguïté des bits, les adresses de nos machines au sein du réseau se suivent. Ce ne serait pas le cas si l'on avait choisi un masque avec des bits non contigus.

Exemple, si on choisit le masque suivant :

11111111.11111111.11111110.00000001

Ici, on a comme précédemment 8 bits qui représentent la partie machine, par contre, ils ne sont plus à la même place. Cela se traduit en décimal par le masque suivant 255.255.254.1. On voit donc que les adresses dont le dernier bit est a 1 ne seront pas dans le même réseau que celles dont le dernier bit est a 0. Ce qui veut dire que les adresses dont le dernier octet est impair ne seront pas dans le même réseau que les adresses paires. Dans cet exemple, cela reste encore facile de différencier les adresses paires et impaires, mais lorsque l'on fait des mélanges plus compliqués entre les bits significatifs, cela devient très vite inextricable.

On conservera donc toujours la contiguïté des bits significatifs!!!

5.6 Quelles adresses pour les masques ?

Etant donné que l'on conserve la contiguïté des bits, on va toujours rencontrer les mêmes nombres pour les octets du masque. Ce sont les suivants :

```
11111111
11111110
11111100
...
10000000
00000000
```

Soit en décimal :

255, 254, 252, 248, 240, 224, 192, 128, et 0.

Ainsi, on peut tout de suite dire si un masque semble valide au premier coup d'oeil. Un masque en 255.255.224.0 sera correct alors qu'un masque en 255.255.232.0 ne le sera pas (à moins de ne pas vouloir respecter la contiguïté des bits)

Vous pouvez aller voir tous les masques possibles dans la RFC suivante : <http://www.faqs.org/rfcs/rfc1878.html>

5.7 Faire fi de l'écriture par octets

L'écriture de l'adresse IP selon 4 octets séparés par un point est facile à utiliser. Mais quand on se penche sur le problème d'un peu plus près, on se rend compte qu'elle n'est pas très adaptée...

Elle a deux défauts principaux :

- Écriture en décimal alors que l'on résonne en binaire.
- Séparation des octets par des points.

Ainsi, lorsqu'on utilise des masques où la séparation réseau/machine se fait sur un octet (tous les bits des octets sont soit à 1, soit à 0) cela est simple. Prenons par exemple le réseau 192.168.25.0/255.255.255.0.

Toutes les machines commençant par 192.168.25 appartiendront à ce réseau. Si l'on prend le réseau 192.168.25.32/255.255.255.248 et que je vous demande si la machine 192.168.25.47 appartient à ce réseau ? ça devient plus compliqué...

Pour bien comprendre, il faut alors revenir en binaire. Etant donné que les trois premiers octets du masque ont tous leurs bits à 1, c'est sur le quatrième que va se faire la différentiation. Il s'écrit 248, soit 11111000 en binaire. Donc les 5 premiers bits de cet octet représenteront la partie réseau.

Pour notre réseau, le dernier octet vaut 32, soit 00100000, pour notre machine, il vaut 47, soit 00101111. On voit que les 5 premiers bits de ces deux octets ne sont pas identiques (00100 = 00101) et donc que ces deux adresses n'appartiennent pas au même réseau.

Cela peut sembler très compliqué, mais on verra par la suite des méthodes simples pour déterminer rapidement l'appartenance à un réseau.

5.8 Quelle est cette notation avec un /, comme /24 ?

Une autre notation est souvent utilisée pour représenter les masques. On la rencontre souvent car elle est plus rapide à écrire. Dans celle-ci, on note directement le nombre de bits significatifs en décimal, en considérant que la contiguïté est respectée. Ainsi, pour notre exemple 192.168.25.0/255.255.255.0, on peut aussi écrire 192.168.25.0/24, car 24 bits sont significatifs de la partie réseau de l'adresse.

De même, les écritures suivantes sont équivalentes :

$$10.0.0.0/255.0.0.0 = 10.0.0.0/8$$

$$192.168.25.32/255.255.255.248 = 192.168.25.32/29$$

Etant donné que le masque détermine le nombre de machines qu'il pourra y avoir sur un réseau, c'est souvent de cette information que l'on part pour choisir le masque. Etant donné que l'on travaille en binaire, le nombre de machines possible au sein d'un réseau sera une puissance de 2. Pour un nombre de machines donné, il faudra donc choisir la puissance de 2 supérieure pour pouvoir adresser les machines. De plus, il faudra prévoir un certain nombre d'adresses supplémentaires pour accueillir de nouvelles machines.

Ainsi, disons que l'on possède le réseau 193.225.34.0/255.255.255.0 et que l'on veut faire un réseau de 60 machines au sein de celui-ci. On veut 60 machines, il faut ajouter deux adresses pour le réseau et le broadcast, ce qui fait 62 adresses au total. La puissance de 2 supérieure à 62 est 64, mais cela ne nous laisserait que 2 adresses pour évoluer, ce qui est un peu juste. On préférera donc un réseau de 128 adresses. Pour identifier 128 adresses, il nous faut 7 bits ($128 = 2^7$) Donc dans notre masque, 7 bits seront à 0 pour identifier la partie machine, et les 25 bits restants seront à 1. Ce qui donne :

11111111.11111111.11111111.10000000

et en décimal 255.255.255.128 .

6 Comment bien choisir son masque ?

6.1 Partir de l'existant

La plupart du temps, le choix de l'adressage se fait en fonction des besoins exprimés, et des limites de ce que l'on a le droit de faire. Une certaine plage vous est allouée par votre fournisseur d'accès. Vous pourrez alors découper cette plage en différents réseaux, mais ne surtout pas dépasser de celle-ci. Ainsi, si vous possédez une plage de 128 adresses et que vous voulez adresser 500 machines, vous aurez quelques petits problèmes...

6.2 En fonction du nombre de machines

Etant donné que le masque détermine le nombre de machines qu'il pourra y avoir sur un réseau, c'est souvent de cette information que l'on part pour choisir le masque. Etant donné que l'on travaille en binaire, le nombre de machines possible au sein d'un réseau sera une puissance de 2. Pour un nombre de machines donné, il faudra donc choisir la puissance de 2 supérieure pour pouvoir adresser les machines. De plus, il faudra prévoir un certain nombre d'adresses supplémentaires pour accueillir de nouvelles machines.

Ainsi, disons que l'on possède le réseau 193.225.34.0/255.255.255.0 et que l'on veut faire un réseau de 60 machines au sein de celui-ci. On veut 60 machines, il faut ajouter deux adresses pour le réseau et le broadcast, ce qui fait 62 adresses au total. La puissance de 2 supérieure à 62 est 64, mais cela ne nous laisserait que 2 adresses pour évoluer, ce qui est un peu juste. On préférera donc un réseau de 128 adresses. Pour identifier 128 adresses, il nous faut 7 bits ($2^7 = 128$). Donc dans notre masque, 7 bits seront à 0 pour identifier la partie machine, et les 25 bits restants seront à 1. Ce qui donne :

```
11111111.11111111.11111111.10000000
```

et en décimal 255.255.255.128

6.3 Comment déterminer la plage d'adresses à partir du masque et d'une adresse ?

Nous avons vu précédemment que le masque devait être associé à une adresse IP pour avoir une valeur. Le choix de la plage d'adresses sur laquelle il s'applique est donc tout aussi important!! Nous avons choisi un masque qui nous permettra d'identifier 128 machines. Mais nous possédons une plage d'adresses de 256 adresse. Ou faut-il placer nos 128 adresses dans cette plage? Peut-on les placer n'importe où ?

La réponse est bien sur non. Nous n'avons que deux possibilités pour choisir notre plage, les adresses de 0 à 127, et les adresses de 128 à 255. Choisir une plage de 32 à 160 serait une erreur, et le réseau ne fonctionnerait pas.

Voici l'explication :

La différenciation du réseau va se faire sur le premier bit du dernier octet (vu que nos trois premiers octets sont fixés à 193.225.34) Si ce bit est à 0, cela correspond aux adresses de 0 à 127. S'il est à 1, cela correspond aux adresses de 128 à 255. Ainsi, si l'on choisit une plage d'adresses de 32 à 160, les adresses de 32 à 127 auront le premier bit de leur dernier octet à 0, alors que les adresses de 128 à 160 auront ce même bit à 1, elles seront alors considérées comme étant dans deux réseaux différents!!!

Ainsi, quel que soit le nombre de machines à placer dans une plage, on ne peut pas choisir l'adressage n'importe comment.

PS : Dans notre cas, les deux choix possibles sont identiques, mais l'on verra par la suite que ce n'est pas toujours le cas pour des plages plus petites...

6.4 Une méthode simple pour trouver les adresses de réseau possibles

Il n'est pas toujours évident de savoir si une adresse correspond bien à celle d'un réseau selon le masque que l'on a choisi. Avec la méthode suivante, vous devriez pouvoir vous en sortir. Il faut avant tout que vous ayez déterminé le masque selon le nombre de machines dont vous avez besoin. Ensuite, selon l'octet significatif (qui n'est pas à 0 ou 255) faites $256 - \text{cet octet} = X$. l'adresse de réseau devra alors être un multiple de X. Un petit exemple pour mettre être un peu plus clair. On veut par exemple 50 machines, on choisit donc un masque en 255.255.255.192. C'est le dernier octet qui est significatif, on fait donc $256 - 192 = 64$.

Il faut donc que le dernier octet de l'adresse de réseau soit un multiple de 64. Si on prend la plage 10.0.0.0/255.255.255.192, on pourra choisir les adresses de réseau suivantes :

10.0.0.0
10.0.0.64
10.0.0.128
10.0.0.192

6.5 Comment découper une plage réseau quelconque comme somme de plusieurs plages ?

Nous avons vu qu'une plage réseau ne pouvait pas être choisie n'importe comment. Etant donné que les masques et les adresses IP se basent sur un codage binaire, les chiffres utilisés dans les adresses résultantes ne pourront que être des multiples de puissances de 2 en accord avec le masque. Ainsi, une plage 70.0.0.0 ne pourra pas avoir un masque qui définisse plus de deux chiffres sur le premier octet, car 70 est un multiple de 2, mais pas de 4.

Ce n'est pas clair ? un exemple devrait vous aider à mieux comprendre. Disons que l'on veut décrire la plage d'adresses allant de 69.0.0.0 à 79.255.255.255. La question est de savoir quel masque associer à quelle adresse de réseau nous permettra de définir cette plage ?

Le premier octet varie de 69 à 79. Il prend donc 11 valeurs. 11 n'étant pas une puissance de 2, on sait d'ores et déjà que l'on ne pourra pas définir cette plage avec un seul réseau, mais qu'il va falloir la découper en une somme de plusieurs réseaux. Le but est cependant d'optimiser cette somme de réseaux pour en avoir le moins possible. On pourrait simplement utiliser 11 réseaux avec des masques 255.0.0.0, mais on doit sûrement pouvoir faire plus propre et regrouper plusieurs de ces réseaux en un seul.

La première puissance de 2 inférieure à 11 est 8. Il faut maintenant savoir si l'on peut placer un réseau, dont le premier octet décrira 8 valeurs, dans cette plage. Le seul multiple de 8 de cette plage est 72. On décrirait alors un réseau dont le premier octet varierait de 72 à 79, ce qui est bien compris dans notre plage d'origine. Le réseau 72.0.0.0/248.0.0.0 est donc bien adapté pour décrire notre plage, mais il reste encore à décrire les adresses de 69.0.0.0 à 71.255.255.255.

On effectue le même raisonnement. (Ici le premier octet prend 3 valeurs, la puissance de 2 inférieure à 3 est 2, et le multiple de 2 de cette plage est

70).

On trouve donc le réseau 70.0.0.0/254.0.0.0

Il ne nous reste plus qu'à décrire la plage 69.0.0.0 à 69.255.255.255 qui peut être définie par 69.0.0.0/255.0.0.0.

Et voilà !! Nous avons découpé notre plage d'origine qui allait de 69.0.0.0 à 79.255.255.255 en trois sous réseaux :

69.0.0.0/255.0.0.0

70.0.0.0/254.0.0.0

72.0.0.0/248.0.0.0

6.6 Plages réservées (RFC 1918)

Certaines plages d'adresses ont été réservées pour une utilisation locale. Ainsi, pour configurer un réseau local quand on n'a pas de plage d'adresses publiques à disposition, on doit utiliser ces plages d'adresses privées. Si vous voulez avoir plusieurs réseaux, c'est à vous de faire le découpage au sein de ces plages comme bon vous semble.

Voici ces plages d'adresses :

- 10.0.0.0/255.0.0.0 soit plus de 16 millions d'adresses.
- 192.168.0.0/255.255.0.0 soit près de 65000 adresses.
- 172.16.0.0/255.255.240.0 soit 4080 adresses.

Si après vous ne trouvez pas votre bonheur, c'est que vous avez un sacrément grand réseau, ou que vous vous y prenez mal...

7 Comment découper une plage d'adresses en plusieurs sous réseaux ?

7.1 Détermination des masques pour chacun des réseaux

Il est souvent nécessaire de découper une plage d'adresses en plusieurs sous-réseaux. Pour cela, il vaut souvent mieux envisager le découpage des réseaux dans son ensemble plutôt que de les faire chacun séparément et de se rendre compte à la fin qu'ils sont incompatibles...

Ainsi nous allons encore partir du nombre de machines dans chacun des réseaux. Prenons l'exemple précédent du réseau 193.225.34.0/255.255.255.0. On désire comme précédemment faire un sous réseau de 60 machines, mais aussi un réseaux de 44 machines et un dernier de 20 machines. De la même façon que nous l'avons vu précédemment, pour 44 machines, il faudra réserver 64 adresses, soit un masque 255.255.255.192. Pour 20 machines, il faudra réserver 32 adresses, soit un masque 255.255.255.224.

7.2 Détermination des plages réseau

Nous allons donc devoir placer trois plages de 128, 64 et 32 adresses dans une plage de 256 adresses, cela ne devrait pas poser de problème. On commence par la plage la plus grande de 128 adresses. Si on commençait par la plus petite et qu'on la plaçait n'importe où, cela pourrait poser problème. Imaginons que l'on place la plage de 32 adresses de 0 à 31, et celle de 64 adresses de 128 à 192, il ne nous restera plus de place pour la plage de 128 adresses!!! On a donc deux choix pour cette plage de 128 adresses, soit les adresses de 0 à 127, soit de 128 à 255. A priori, les deux choix sont possibles et non déterminants. On choisit de 0 à 127. Ainsi, notre sous réseau sera caractérisé par 193.225.34.0/255.255.255.128. Pour la seconde plage de 64 adresses, il nous reste deux plages d'adresses possibles, de 128 à 191, et de 192 à 255. Là encore le choix n'est pas déterminant. On choisit de 128 à 191. Ainsi, notre sous réseau sera caractérisé par 193.225.34.128/255.255.255.192 (ici, la première adresse de notre plage (1 adresse du réseau) est celle en 128 et le dernier octet du masque en 192 nous indique que ce sous-réseau contient 64 adresses)

Enfin, pour la dernière plage de 32 adresses, il nous reste encore deux possibilités de 192 à 223 ou de 224 à 255. On choisit de 192 à 223. Ainsi, notre sous-réseau sera caractérisé par 193.225.34.192/255.255.255.224.

7.3 Le résultat

Nous avons donc découpé notre réseau d'origine 193.225.34.0/255.255.255.0 en trois sous réseaux

193.225.34.0/255.255.255.128

193.225.34.128/255.255.255.192

193.225.34.192/255.255.255.224

Il nous reste même une plage de 32 adresses non utilisées de 224 à 255.

8 Que sont les classes d'adresses A, B, C, D... ?

8.1 Historique

Comme nous l'avons vu dans le paragraphe 2, le masque de sous réseau permet de segmenter l'ensemble des adresses de l'Internet en différents réseaux. Mais cette segmentation ne s'est pas faite n'importe comment !

On a découpé la plage d'adresses disponible en cinq parties distinctes. Les classes A, B, C, D et E, que l'on appelle aussi adresses globales.

8.2 Définitions

- Classe A : premier bit de l'adresse à 1, et masque de sous réseau en 255.0.0.0. Ce qui donne la plage d'adresse 0.0.0.0 à 126.255.255.255 soit 16 777 214 adresses par réseau de classe A.
- Classe B : Deux premiers bits de l'adresse à 10 (1 et 0), et masque de sous réseau en 255.255.0.0. Ce qui donne la plage d'adresse 128.0.0.0 à 191.255.255.255 soit 65 534 adresses par réseau de classe B.
- Classe C : Trois premiers bits de l'adresse à 110, et masque de sous réseau en 255.255.255.0. Ce qui donne la plage d'adresse 192.0.0.0 à 223.255.255.255 soit 255 adresses par réseau de classe C.
- Classe D : Quatre premiers bits de l'adresse à 1110, et masque de sous réseau en 255.255.255.240. Ce qui donne la plage d'adresse 224.0.0.0 à 239.255.255.255 soit 255 adresses par réseau de classe C.
- Classe E : Quatre premiers bits de l'adresse à 1111, et masque de sous réseau en 255.255.255.240. Ce qui donne la plage d'adresse 240.0.0.0 à 255.255.255.255 .

Les classes A, B et C, sont réservées pour les utilisateurs d'Internet (entreprises, administrations, fournisseurs d'accès, etc). La classe D est réservée pour les flux multicast et la classe E n'est pas utilisée aujourd'hui (du moins, je n'en ai pas connaissance...). Ainsi, une entreprise demandant 80 000 adresses

se voyait attribuer un réseau de classe A, et gâchait par la même occasion (16 777 214 - 80 000=) 16 697 214 adresses!!! Inutile alors de vous montrer combien d'adresses étaient perdues de la sorte...

8.3 Y a-t-il une pénurie d'adresses IPv4 ?

La réponse est non.

Il n'y a pas aujourd'hui de pénurie d'adresses IP. Cependant, il est certain qu'étant donné le développement rapide d'Internet, on va vite arriver à une situation critique. C'est aussi pour cela qu'une nouvelle version d'IP a été créée et sera bientôt déployée.

8.4 Le système d'adressage par classes est-il viable ?

La réponse est encore non, et a déjà été depuis bien longtemps étudiée et transformé. Nous avons vu qu'en se basant sur ce système de classes, nous risquons de gâcher un très grand nombre d'adresses. Les classes d'adresses globales se sont donc rapidement avérées obsolètes et on a du créer un nouveau modèle, l'adressage CIDR

8.5 Qu'est-ce que l'adressage CIDR ?

Etant donné que l'adressage par classes s'est avéré incompatible avec l'évolution d'Internet, il a fallu imaginer un nouveau modèle qui simplifierait à la fois le routage et permettrait un adressage plus fin. Pour cela, on a créé l'adressage CIDR (Classless Inter-Domain Routing) Cet adressage ne tient pas compte des classes globales et autorise l'utilisation de sous-réseaux au sein de toutes les classes d'adresses.

Ainsi, une entreprise désirant 80 000 adresses ne se verra plus attribuer une classe A complète, mais un sous réseau de cette classe A. Par exemple, on lui fournira non plus 16 millions d'adresses, mais 130 000 (la puissance de deux supérieure à 80 000) Ainsi les 16 millions d'adresses restantes pourront être utilisées pour d'autres entités.

L'adressage CIDR ne tient donc plus du tout compte des masques associés aux classes d'adresses globales. On s'affranchit ainsi du découpage arbitraire et peu flexible en classes.

On peut très bien trouver un réseau de classe B avec un masque de classe C, par exemple 164.23.0.0/255.255.255.0.

9 Trucs et astuces avec les masques

9.1 Comment déterminer qu'une machine appartient à mon réseau ?

C'est très simple. pour cela, il va falloir déterminer si l'adresse de la machine appartient à la plage d'adresses définie par mon adresse et mon masque.

Pour cela, je fais un ET logique entre mon adresse et mon masque réseau, j'en déduis donc l'adresse de mon réseau (pour une explication du ET logique, regarder le paragraphe 10.4)

Je fais pareil avec l'adresse de l'autre machine et MON masque réseau, et j'obtiens une adresse de réseau. Si les deux adresses de réseau sont les mêmes, ça veut dire que la machine appartient bien au même réseau.

Disons par exemple que ma machine ait pour adresse 192.168.0.140/255.255.255.128 et je veux savoir si les machines A et B ayant pour adresses 192.168.0.20(A) et 192.168.0.185(B) sont sur le même réseau ? Je fais

$$\begin{array}{r} 192.168.0.140 \\ \text{ET } 255.255.255.128 \\ \hline = 192.168.0.128 \end{array}$$

de même avec les deux autres adresses

– Pour A :

$$\begin{array}{r} 192.168.0.20 \\ \text{ET } 255.255.255.128 \\ \hline = 192.168.0.0 \end{array}$$

– et pour B :

$$\begin{array}{r} 192.168.0.185 \\ \text{ET } 255.255.255.128 \\ \hline = 192.168.0.128 \end{array}$$

On voit ainsi que les nombres obtenus sont les mêmes pour ma machine et B. On en déduit donc que B est sur le même réseau, et que A est sur un réseau différent.

9.2 Des machines sur un même réseau peuvent elles avoir des masques différents ?

A priori, la réponse est non. Cependant, il peut y avoir des cas dans lesquels une telle configuration peut être utile.

Pour comprendre cela, il faut comprendre ce qui se passe au niveau de la communication entre machines, et notamment sur le fonctionnement du modèle TCP/IP. Celui-ci ne faisant pas partie de l'objet du cours, nous ne ferons que survoler le sujet.

En fait, ce ne sont pas les mêmes mécanismes qui gèrent une communication entre deux machines sur un même réseau, et deux machines sur deux réseaux distincts. Une communication a lieu dans les deux sens, c'est à dire que pour communiquer ensemble, une machine A doit voir une machine B ET la machine B doit voir la machine A.

Prenons l'exemple de trois machines A, B et C et de la plage d'adresses 192.168.0.0/24. A doit pouvoir communiquer avec B et C, mais B ne doit pas pouvoir communiquer avec C. Pour cela, on peut jouer sur les masques des machines et les plages d'adresses réseau auxquelles elles appartiennent.

Grâce aux masques, on peut découper cette plage en deux, et on obtient ainsi, non plus une plage d'adresses... mais trois !

1. 192.168.0.0/255.255.255.0
soit de 192.168.0.0 à 192.168.0.255
2. 192.168.0.0/255.255.255.128
soit de 192.168.0.0 à 192.168.0.127
3. 192.168.0.128/255.255.255.128
soit de 192.168.0.128 à 192.168.0.255

En fait, la première plage englobe les deux autres, ainsi, une machine de la première plage pourra voir toutes les autres machines des autres plages, mais une machine de la seconde plage ne pourra pas voir toutes les machines de la première plage (seulement la moitié des adresses...)

Ce n'est pas clair ? regardons alors un exemple :

On donne les adresses suivantes aux machines A, B et C.

- A : 192.168.0.129/255.255.255.0
- B : 192.168.0.130/255.255.255.128
- C : 192.168.0.1/255.255.255.0

D'après ce que l'on a vu précédemment, A et C considèrent que la machine B est sur leur réseau. Par contre, B considère que C n'est pas sur son réseau. Ainsi, C peut envoyer un paquet à B, mais B ne pourra pas lui répondre. Cette configuration correspond donc bien à ce que l'on cherchait à faire. Cependant, une telle configuration n'est pas conseillée et ne doit être utilisée que s'il n'y a pas d'autres solutions. En dehors de cas exotiques comme celui exposé, on ne doit jamais avoir deux machines appartenant à un même réseau ayant des masques différents !

9.3 Puis-je utiliser un outil qui calcule pour moi ?

Non!!! Enfin si, mais bon, vous me décevriez beaucoup;-) Car après ce que nous avons vu, vous devriez être capable de calculer n'importe quel masque correct aussi vite qu'une machine. Et il est toujours mieux de bien maîtriser ce qu'on utilise. A force d'utiliser des automates, on perd les notions de ce que l'on manipule.

D'autre part, un logiciel ne corrigera pas vos erreurs! La plupart des logiciels de calcul de masque ne font qu'un calcul bête et méchant qui peut s'avérer faux. Prenons l'exemple du 6.3, où l'on veut une plage commençant en 192.168.0.32, et une centaine de machines. Un mauvais logiciel vous sortira le réseau 192.168.0.32/255.255.255.128, et hop, ça marchera pas...

9.4 Tout ça c'est bien, mais quand est ce que je l'utilise ce masque moi ?

Effectivement, quand vous allez sur Internet, vous utilisez un masque sans le savoir. Sous windows, que vous soyez connecté à un réseau local, ou directement par un modem, vous pourrez voir les propriétés de vos interfaces réseau en allant dans une fenêtre DOS et en entrant la commande "ipconfig /all" Vous pouvez aussi modifier ces propriétés en allant dans les propriétés de votre carte réseau, puis propriétés TCP/IP, et là, vous devriez voir votre adresse IP, ainsi que le masque associé, et votre passerelle par défaut. Vous pouvez modifier ces informations, mais votre réseau risque de ne plus fonctionner (et en plus il faudra rebooter sous 98..) donc attention!!

Le masque définit donc les machines (ou plus précisément, les interfaces) appartenant à un même réseau. Pour dialoguer avec ces machines, vous utiliserez un protocole de couche 2 du modèle OSI, alors que pour dialoguer avec les machines d'un autre réseau, vous utiliserez un protocole de couche 3... Il est donc primordial de ne pas se tromper dans le choix du masque.

Mais ça, ça ne fait pas partie intégrante du sujet ;-)

10 Mini lexique

1. Adresse IP : L'adresse IP est un numéro codé sur 4 octets permettant d'identifier une machine de façon unique sur le réseau.

2. Réseau logique

On appelle réseau logique un ensemble d'adresses IP appartenant à une même plage d'adresses. Cette plage est notamment définie par l'adresse de réseau et le masque associé.

3. Sous-réseau

On définit un sous-réseau comme un sous-ensemble d'une plage d'adresses réseau. C'est grâce au masque que l'on peut définir un sous-réseau au sein d'un réseau, et ainsi découper un réseau en plusieurs sous-réseaux.

4. Le ET logique

La fonction de ET logiques est souvent utilisée dans les masques. Elle se base en binaire sur le principe suivant :

```
0 ET 0 = 0
1 ET 0 = 0
0 ET 1 = 0
1 ET 1 = 1
```

On peut donc en déduire au niveau des masques 192.168.0.140 ET 255.255.255.128 décomposé en :

```
11000000.10101000.00000000.10001100
ET 11111111.11111111.11111111.10000000
-----
= 11000000.10101000.00000000.10000000
```

soit 192.168.0.128

Ici, on voit que les trois premiers octets du masque ont tous leurs bits à 1, donc les trois premiers octets du résultat ne seront pas modifiés par rapport à l'adresse d'origine, et on obtient facilement 192.168.0. Pour le dernier octet, il faut regarder plus en détail.

11 Annexes

11.1 Ressources utilisées

Je n'ai pas utilisé beaucoup de documents aussi bien en ligne que sur papier. Les réponses et connaissances apportées proviennent en majeure partie des informations que j'ai pu glaner en furetant sur le net, et notamment sur les newgroups `fr.comp.reseaux.ip` et `fr.comp.reseaux.ethernet`.

Je me suis quand même inspiré de quelques documents :

Les RFCs 943, 1517, 1518, 1519, 1878. Le site <http://www.captage.com/tajan/articles/ip.htm>

Et l'excellente faq sur les firewalls de Stéphane Catteau dont je me suis inspiré pour la mise en forme. Disponible sur : <http://fr.comp.securite.free.fr/firewall.txt> N'hésitez pas à la consulter, on y apprend plein de choses.

11.2 Remerciements

Je remercie notamment les personnes suivantes pour leur lecture assidue du cours durant sa réalisation et leurs conseils précieux.

Jad Chantiri, Pierrick Vodoz, Laurent de Soras, Stéphane Catteau, Cédric Blancher, Ohmforce, Franck Bacquet, Olivier Lamer, Diane Guinnepain, JC, Alain Winestel, — thierry Bellemare, Anne-Gaël de Fyn.

11.3 Faq sur la NAT

Si cette faq vous a plu et que vous avez appris des choses, j'en ai fait une autre sur la NAT (traduction d'adresses) disponible là : <http://www.lalitte.com/nat>

12 Conclusion

J'ai fait de mon mieux pour rendre la notion de masques la plus abordable possible et traiter le sujet de la meilleure façon. Je me rends compte que ce cours est assez fourni en information et pas toujours facile à digérer. Vos remarques sont donc encore et toujours les bienvenues, aussi bien pour y ajouter des idées, que pour enlever le superflu. Maintenant, si je revois passer des questions sur les masques, j'aurai au minimum un droit de flagellation sur les personnes incriminées ;-)