

Adressage IP v4

Préambule

Ce cours vous présente la conversion Binaire/Décimal indispensable pour aborder l'adressage IP. Il aborde également le principe des classes (privées, publiques), de l'adressage sans classe ainsi que le calcul des masques divisant, agrégeant ou de longueur variable.

La conversion base décimale en binaire

Un octet vaut 8 bits, un bit peut prendre la valeur 0 ou 1. Quand un bit prend la valeur 1 on indique la valeur du résultat de la puissance.

128	64	32	16	8	4	2	1
2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0

Rappel conversion décimal/binaire pour un octet

On représente dans ce tableau les 8 bits d'un octet de 2^0 jusqu'à 2^7 .

Ce qui veut dire que si l'on complète le tableau de bit à zéro, on ne compte rien et on obtient la valeur 0. Si l'on complète tous les bits à 1 on obtient $128+64+32+16+8+4+2+1$ soit 255. On peut alors dire qu'un octet aura 0 comme plus petite valeur et 255 comme plus grande valeur. De 0 à 255 on a bien 256 valeurs ce qui correspond au 2^8 (2 parce que c'est du binaire et puissance 8 parce qu'il faut 8 bits pour faire un octet)

Par exemple, pour traduire le nombre décimal 172, on additionne les valeurs de la première ligne qui permettent d'obtenir 172, puis on place les 1 sur la deuxième ligne avec les valeurs que l'on a retenues.

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

- 128 on garde car on ne dépasse pas la valeur recherchée (bit 1)
- $128+64 = 192$ trop grand on garde le 128 et on ignore le 64 (bit 1 0)
- $128+32 = 160$ on garde car on **ne dépasse** de la valeur recherchée (1 0 1)
- $128+32+16 = 176$ trop grand on ignore la valeur 16 (1 0 1 0)
- $128+32+8 = 168$ on garde car on ne dépasse de la valeur recherchée (1 0 1 0 1)
- $128+32+8+4=172$ on garde et on obtient la valeur recherchée (1 0 1 0 1 1)
- Maintenant on sait que le reste n'est pas à utiliser, on le complète les zéros.

172 vaut en binaire 10101100

Inversement, si l'on veut connaître la valeur décimale de **10110010**, il suffit de placer les 0 et les 1 sur la deuxième et d'additionner les valeurs décimales de la première ligne quand le bit est à 1.

128	64	32	16	8	4	2	1
1	0	1	1	0	0	1	0

10110010 vaut $128+32+16+2=178$

Les adresses IP

Une adresse Internet d'un équipement est codée sur 4 octets (32 bits) Elle contient à la fois un identifiant réseau et identifiant de l'équipement connecté à ce réseau (nommé **hôte**)

Le codage sur 32 bits permet d'avoir 2^{32} adresses soit 4 milliards d'adresses disponibles environ.

Pour des raisons évidentes de simplification, les adresses IP sont présentées sous forme décimale pointée sur 4 octets (chaque octet de l'adresse pouvant prendre la valeur de 0 à 255 soit $2^8=256$ possibilités) soit $2*2*2*2*2*2*2*2$

172 | **29** | **32** | **55**
 8 bits 8 bits 8 bits 8 bits

Les adresses IP sont regroupées par famille que l'on appelle des classes **devenues obsolètes**. Ces classes permettent de définir combien de bits seront utilisés pour l'identificateur réseau.

Pour repérer une classe il suffit de regarder la valeur du premier octet.



Le premier octet a une valeur comprise entre 0 et 127.

Dans la classe A, le premier octet désigne le numéro de réseau et les 3 autres correspondent à l'adresse de l'hôte.

Ce qui permet d'avoir 128 réseaux contenant chacun 16 millions de machines en théorie.



Le premier octet a une valeur comprise entre 128 e 191.

Dans la classe B, les 2 premiers octets désignent le numéro de réseau et les 2 autres

correspondent à l'adresse de l'hôte.

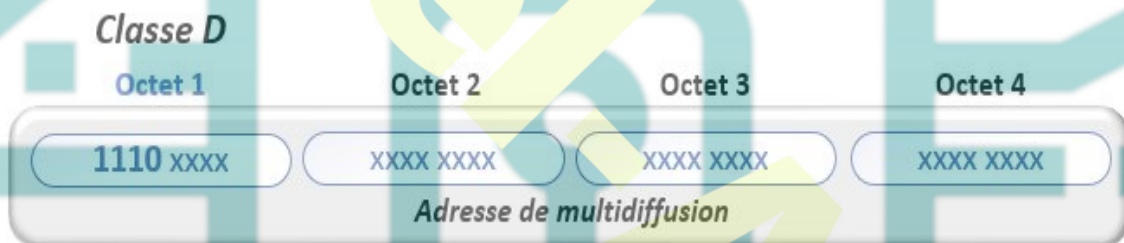
Ce qui permet d'avoir 16 384 réseaux contenant chacun 65536 machines en théorie.



Le premier octet a une valeur comprise entre 192 et 223.

Dans la classe C, les 3 premiers octets désignent le numéro de réseau et le dernier octet correspond à l'adresse de l'hôte.

Ce qui permet d'avoir 2 097 152 réseaux contenant chacun 256 machines en théorie.



Le premier octet a une valeur comprise entre 224 et 239. Il s'agit d'une zone d'adresses dédiées aux services de multidiffusion (multicast) vers des groupes d'hôtes.

Classe E

Le premier octet a une valeur comprise entre 240 et 247 (255 dans certaines documentations pour des questions de confort) Il s'agit d'adresses réservées aux expérimentations. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Adresses spéciales

Si l'adresse vaut 0.0.0.0, elle est réservée aux tables de routage pour indiquer tous les réseaux (passerelle par défaut)

Si l'adresse débute par 0, elle est interdite d'utilisation

Si l'adresse débute par 127, elle est réservée au bouclage, c'est à dire pour s'indiquer soi-même.

Si l'adresse vaut 255.255.255.255, elle est réservée au broadcast général.

Si une adresse de classe A finit par 0.0.0, une classe B par 0.0 et une classe C par 0, c'est qu'elle indique le réseau lui-même et non un hôte.

Inversement, si une classe A finit par .255.255.255, une classe B par .255.255 et une classe C par .255, cela indique une adresse de diffusion sur le réseau lui-même.

Toutes les adresses supérieures à la valeur 223 sont réservées.

Adresses publiques et privées

Les adresses **publiques** sont uniques sur Internet et sont louées auprès d'un fournisseur de services le plus souvent.

Ces adresses sont routables sur Internet.

Les adresses **privées** sont utilisables par tout le monde et ont été créées pour permettre aux entreprises d'utiliser un adressage interne souple sans conflit avec les adresses publiques.

Ces adresses ne sont pas directement routables sur Internet, il faut passer par l'intermédiaire de la technologie de NAT/PAT.

Sont disponibles pour l'adressage interne :

Une classe A, le réseau 10.0.0.0 (notée 10.0.0.0/8)

16 classes B, du réseau 172.16.0.0 au réseau 172.31.0.0 (notées 172.16.0.0/12)

256 classes C, du réseau 192.168.0.0 au réseau 192.168.255.0 (notées 192.168.0.0/16)

Le réseau 169.254.0.0 est un réseau particulier également réservé à l'adressage automatique appelé APIPA.

On peut utiliser les adresses publiques en interne à condition de ne pas être connecté à l'Internet, même si cela est fortement déconseillé.

catégorie d'adresses IP

Adresse **UNICAST** : permet d'identifier un équipement IP de façon unique.

Adresse **MULTICAST** : adresse de diffusion vers un groupe d'équipements IP.

Adresse **BROADCAST** : adresse de diffusion vers toutes les adresses IP d'un même sous- réseau.

Les méthodes de configuration de l'adressage IP

Méthodes	Avantages	Inconvénients
Manuelle	Permet de spécifier et de repérer les hôtes dans un réseau en fonction du type et du rôle. Obligatoire pour les serveurs et applications s'appuyant sur une adresse fixe.	Ingérable pour les clients mobiles. Impose une gestion des adresses déjà distribuées. Administration plus lourde.
Dynamique (RFC 1541)	Les adresses et les options sont centralisées. Supporte facilement les changements fréquents de paramètres. Obligatoire pour les appareils mobiles.	Ne convient pas à tous les réseaux et les hôtes. Impose la mise en œuvre d'une tolérance aux pannes pour le DHCP.
Automatique (RFC 1918)	Inutile actuellement	Risque de voir une machine utiliser l'adresse 168.254.x.x si elle n'arrive pas à contacter un serveur DHCP.

Les masques IP

Les masques de sous réseaux (subnetting)

Pour qu'un équipement réseau puisse détacher la partie réseau de la partie hôte d'une adresse IP, il utilise ce que l'on appelle un masque de sous réseau.

Il se contente de faire une opération binaire entre l'adresse et le masque.

Cette opération utilise la fonction ET (la sortie est égale à 1 si les deux variables sont égales à 1, sinon elle est égale à 0).

Pour détacher les bits de la partie réseau des bits de la partie hôte, le masque utilise les bits à 1 pour représenter le réseau et des bits à 0 pour représenter l'hôte.

Pour structurer l'architecture du réseau interne en disposant d'une seule adresse réseau référencée, on peut utiliser des masques de sous-réseaux afin d'introduire plusieurs niveaux de hiérarchie.

Cette technique permet de définir plusieurs adresses de réseau IP à partir d'une adresse réseau de classe donnée. Pour cela, on étend le champ de l'identifiant réseau en réduisant obligatoirement celui de l'identifiant de l'équipement.

Par exemple, pour l'adresse 20.20.20.20 le masque utilisé 255.255.255.0 permet d'identifier l'adresse IP du réseau en 20.20.20.0

Si l'on souhaite structurer le réseau du site en plusieurs réseaux IP à partir de cette adresse référencée, on pourra utiliser 3 bits du champ identifiant de l'hôte pour l'affecter au réseau.

Réseau	@Réseau	Plage	@Broadcast
Subnet 0	20.20.20.0	20.20.20.1 - 20.20.20.30	20.20.20.31
Subnet 1	20.20.20.32	20.20.20.33 - 20.20.20.62	20.20.20.63
Subnet 2	20.20.20.64	20.20.20.65 - 20.20.20.94	20.20.20.95
Subnet 3	20.20.20.96	20.20.20.97 - 20.20.20.126	20.20.20.127
Subnet 4	20.20.20.128	20.20.20.129 - 20.20.20.158	20.20.20.159
Subnet 5	20.20.20.160	20.20.20.161 - 20.20.20.190	20.20.20.191
Subnet 6	20.20.20.192	20.20.20.193 - 20.20.20.222	20.20.20.223
Subnet 7	20.20.20.224	20.20.20.255 - 20.20.20.254	20.20.20.255

Découpage des réseaux

Exemple de calcul

Adresse IP réseau : 172.20.0.0 – Masque /16 ou 255.255.0.0

Nombre de sous réseaux que l'on veut obtenir : $n=4$

Etape 1 : Donner le nouveau masque de sous réseau

1. Dans notre cas : $n = 2^2 = 4$

2. Ensuite, on additionne le nombre de bits trouvés au masque actuel

/16 + 2 = /18 soit 8 bits à 1 sous le premier octet + 8 bits à 1 sous le deuxième octet + 2 bits à 1 sous le troisième octet.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Conversation sur le troisième octet

3. Le résultat est donc 255.255.192.0 ou /18

Étape 2 : De combien d'adresses IP disposeront nous par sous-réseau ?

1. Pour déterminer le nombre d'adresses disponibles dans un sous-réseau, il faut se servir du masque de sous-réseau.

Sa valeur max étant de 32 bits, il faut soustraire la valeur max du masque à la valeur du nouveau masque pour donner le nombre de bits disponibles pour l'adressage IP de la partie hôte : $32 - 18 = 14$ bits

2. Ensuite calculer avec le nombre de bits disponibles : $2^{14} - 2 = 16382$ (on soustrait 2, car on omet l'adresse de broadcast, la dernière et l'adresse du réseau, la première)

3. Ce qui nous fait 16382 adresses disponibles pour chaque sous-réseau.

On aurait également pu compter le nombre de bits à zéro restant dans le tableau.

Étape 3 : Quelles sont les plages de ses nouveaux réseaux ?

1. Pour déterminer ce qu'on appelle la valeur du pas, on regarde la valeur décimale sous le dernier bit à 1 du masque. Dans notre cas, le dernier bit du masque se trouve sous la valeur 64. On sait maintenant que les 4 réseaux ont un pas de 64, c'est à dire que le réseau changera toutes les 64 valeurs.

1 – 172.20.0.0 jusqu'à 172.20.63.255

2 -172.20.64.0 jusqu'à 172.20.127.255

3 – 172.20.128.0 jusqu'à 172.20.191.255

4 – 172.20.192.0 jusqu'à 172.20.255.255

Pour trouver la valeur du pas, on aurait également pu faire, 256 (valeur de l'octet) divisé par 4 (nb de réseaux) et on aurait obtenu 64.

<https://www.youtube.com/watch?v=RnpSaDSSjR4>

Toujours pas très clair, regardez cette vidéo

<https://www.youtube.com/watch?v=TItwuvhArHk>

Une autre méthode de calcul

Notation CIDR

Le CIDR (Classless Inter Domain Routing) supprime l'usage des classes A, B et C pour généraliser celui du préfixe réseau étendu. Les classes A, B ou C n'existent plus.

Toutes les adresses des réseaux sont annoncées avec leur préfixe qui peut être de taille arbitraire. Les routeurs ne se basent plus sur les 3 premiers bits de chaque adresse pour déterminer la classe du réseau : seul le préfixe fait loi.

Au lieu d'avoir une adresse de type 131.107.0.0 255.255.0.0 on utilisera 131.107.0.0/16. Soit un masque de 16 bits à 1.

On doit considérer les adresses comme des blocs contenant plus ou moins d'adresses dans un réseau avec plus ou moins d'hôtes.

Par exemple, une adresse 10.20.0.0/18 permet de déterminer la taille des blocs. En effet, on considère que les 2 premiers octets sont figés à la valeur 10.20 car le masque ne contient que des bits à 1, ce qui a pour effet de n'avoir qu'un bloc possible sur le premier octet 10 (tout autre valeur que 10 appartient à un autre réseau) et pour le deuxième octet même constat avec la valeur 20. Par contre qu'en est-il sur le troisième octet ?

/18 contient les 16 bits affectés au premier (8) et deuxième octet (8) + 2 bits affectés au troisième octet.

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

Bloc réseau de 64 valeurs sur le 3ème

On a donc des blocs regroupant 64 valeurs communes (le dernier bit à 1 est positionné sous la valeur décimale 64) ce qui fait sur un total de 256 valeurs (un octet=2 puissance 8 bits=256 combinaisons de 0 à 255) 4 blocs possibles (256/64) soit 4 réseaux différents (de **10.20.0.0** à 10.20.63.255 puis **10.20.64.0** jusqu'à 10.20.127.255, de **10.20.128.0** à 10.20.191.255 et enfin de **10.20.192.0** jusqu'à 10.20.255.255

Prenons maintenant l'adresse 172.0.0.0/12, on considère que le premier octets est figé à la valeur 172 car le masque ne contient que des bits à 1, ce qui a pour effet de n'avoir qu'un

bloc possible sur le premier octet 172 (tout autre valeur que 172 appartient à un autre réseau) et pour le deuxième octet on a utilisé que 4 bits.

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

Bloc réseau de 16 valeurs sur le 2^{ème} octet

On a donc des blocs regroupant 16 valeurs communes (le dernier bit à 1 est positionné sous la valeur décimale 16) ce qui fait sur un total de 256 valeurs (un octet=2 puissance 8 bits=256 combinaisons de 0 à 255) 16 blocs possibles (256/16) soit 16 réseaux différents (de 172.0 à 172.15 puis de 172.16 à 172.31 puis de 16 en 16 jusqu'au dernier réseau de la liste 172.240 jusqu'à 172.255)

Les masques extrêmes

1. Le masque en /32

Ce masque indique combien de blocs ? C'est simple on fixe tous les octets ce qui implique que l'on aura 2 puissance 32 blocs différents soit plus de 4 milliards de blocs. En fait, cette notation est utilisée pour indiquer une adresse et une seule dans des tables de routage ou de filtrage (ex. 192.168.22.55/32 représente une adresse unique. La moindre modification sur n'importe lequel de ces octets indique un autre bloc)

2. Le masque en /0

Ce masque représente un seul bloc (on a aucun bit à 1) contenant 2 puissance 32 adresses soit 4 milliards d'adresses (toutes les adresses IP au final). En fait, cette notation est utilisée pour indiquer n'importe quelle adresse (réseau ou hôte) dans une table de routage ou de filtrage (ex. 0.0.0.0/0 représente toutes les adresses IP)

Technique d'agrégation de réseaux (supernetting)

Le supernetting IP est l'opération inverse du subnetting. Ce principe permet d'agréger des réseaux IP pour une meilleure gestion des espaces d'adressage dans un système autonome. Le principal atout du supernetting est la réduction des tables de routage et la gestion des plages dans les firewalls.

Exemple Routage

Imaginons le cas d'une entreprise disposant du bloc d'adresses 206.0.64.0 jusqu'à 206.0.67.0 soit 4 réseaux. Lorsqu'un routeur doit pointer vers cette entreprise, le routeur doit avoir 4 entrées dans sa table de routage une pour chacun de ces réseaux.

Avec la notation CIDR, il est possible de réduire les 4 entrées en une seule et unique entrée.

Ex. 206.0.64.0/22 soit un masque sur 22 bits soit 255.255.252 en valeur décimale. 252 donne bien une valeur de regroupement de 4 puisque le dernier bit à 1 du masque se trouve sous la valeur 4.

128	64	32	16	8	4	2	1
1	1	1	1	1	1	0	0

$$128+64+32+16+8+4=252$$

On aurait eu 16 adresses à regrouper de 172.16.0.0 jusqu'à 172.31.0.0

On aurait utilisé le masque /12 ou 255.240.0.0 (le dernier bit à 1 est sous la valeur 16)

Exemple Firewall

Un autre exemple permet de regrouper dans une table de firewall, tous les réseaux qui commencent par le préfixe 192.168 quelles que soient les valeurs du 3 et 4ème octet.

Dans ce cas, on peut utiliser le masque 255.255.0.0 pour l'adresse 192.168.0.0 alors, le système comprendra tout ce qui commence par 192.168.

De même, si l'on met un masque en 255.0.0.0 le système comprendra tout ce qui commence par 192.

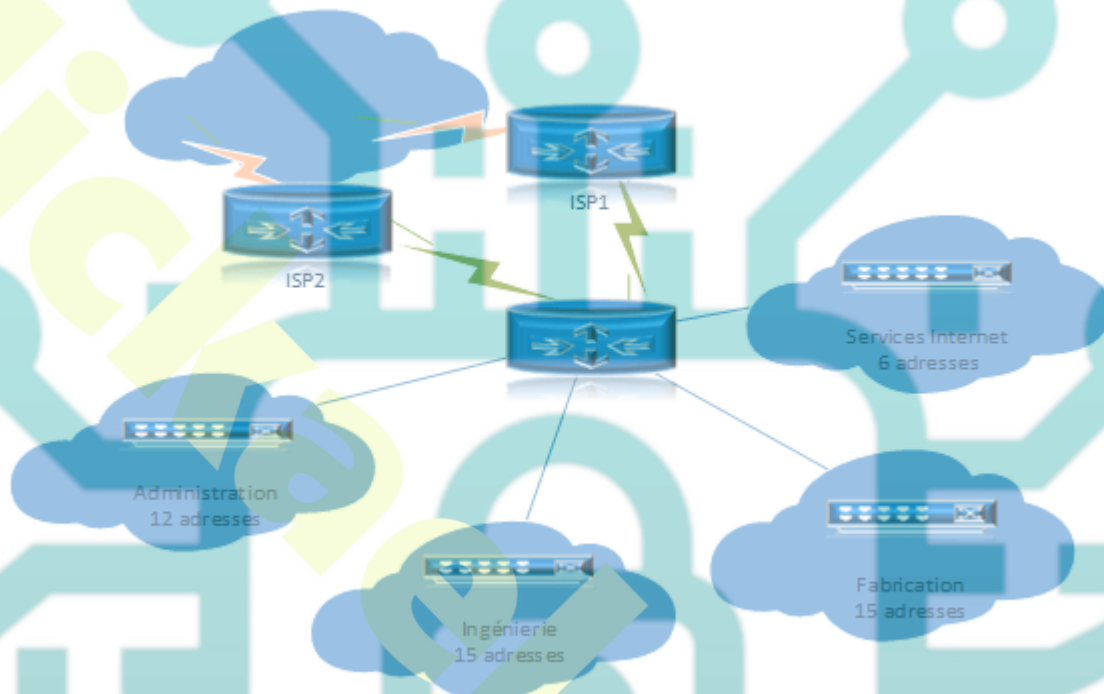
Le routage inter-domaine sans classe

Cette technique de supernetting associée au masque réseau de longueur variable (Variable Length Subnet Mask ou VLSM) a résolu en partie les problèmes d'attribution de l'espace d'adressage IPv4 et d'accroissement des tables de routage de l'Internet.

La technique VLSM n'est pas seulement utile aux principaux fournisseurs d'accès Internet. En effet, un administrateur possédant plus d'un sous-réseau peut utiliser cette technique pour utiliser son espace 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 :

Nom	Sous-réseau	CIDR	Masque	Plage d'adresses	Nombre d'hôtes
Liaison ISP1	200.80.100.0	/30	255.255.255.252	200.80.100.1 200.80.100.2	2
Liaison ISP2	200.80.100.4	/30	255.255.255.252	200.80.100.5 200.80.100.6	2
Services Internet	200.80.100.16	/28	255.255.255.240	200.80.100.17 200.80.100.30	14
Administration	200.80.100.32	/27	255.255.255.224	200.80.100.33 200.80.100.62	30
Ingénierie	200.80.100.64	/27	255.255.255.224	200.80.100.65 200.80.100.94	30
Fabrication	200.80.100.96	/27	255.255.255.224	200.80.100.97 200.80.100.126	30