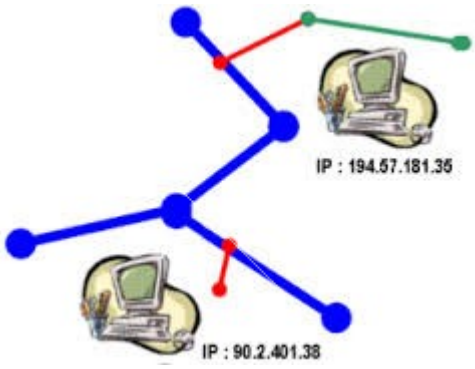
Adressage IP

Table des matières

L'Internet est un réseau virtuel, construit par interconnexion de réseaux physiques via des passerelles. L'adressage est le maillon essentiel des protocoles TCP/IP pour rendre transparents les détails physiques des réseaux et faire apparaître l'Internet comme une entité uniforme.



1. Introduction

Un système de communication doit pouvoir permettre à n'importe quel hôte de se mettre en relation avec n'importe quel autre. Afin qu'il n'y ait pas d'ambiguïté pour la reconnaissance des hôtes possibles, il est absolument nécessaire d'admettre un principe général d'identification.

Lorsque l'on veut établir une communication, il est intuitivement indispensable de posséder trois informations :

1. Le nom de la machine distante,
2. son adresse,
3. la route à suivre pour y parvenir.

Le nom dit « qui » est l'hôte distant, l'adresse nous dit « où »' il se trouve et la route « comment » on y parvient.

Les adresses IP (version 4) sont standardisées sous forme d'un nombre de 32 bits qui permet à la fois l'identification de chaque hôte et du réseau auquel il appartient. Le choix des nombres composants une adresse IP n'est pas laissé au hasard, au contraire il fait l'objet d'une attention particulière notamment pour faciliter les opérations de routage.

Chaque adresse IP contient donc deux informations basiques, une adresse de réseau et une adresse d'hôte. La combinaison des deux désigne de manière unique une machine et une seule sur l'Internet.

2. Délivrance des adresses IPv4

On distingue deux types d'adresses IP. Les adresses privées que tout administrateur de réseau peut s'attribuer librement pourvu qu'elle ne soient pas routées sur l'Internet, et les adresses publiques, délivrées par une structure mondiale qui en assure l'unicité.

Les adresses publiques (souvent une seule), sont le plus généralement fournies par le FAI. Qu'elles soient délivrées de manière temporaire ou attribuées pour le long terme, elles doivent être uniques sur le réseau.

C'est L'ICANN (Internet Corporation for Assigned Names and Numbers) qui est chargé au niveau mondial de la gestion de l'espace d'adressage IP. Il définit les procédures d'attribution et de résolution de conflits dans l'attribution des adresses, mais délègue le détail de la gestion de ces ressources à des instances régionales puis locales, dans chaque pays, appelées « Regional Internet Registries » ou RIR.

Il y a actuellement trois « Regional Internet Registries » opérationnels :

- l'APNIC pour la région Asie-Pacifique
- l'ARIN pour l'Amérique
- le RIPE NCC pour l'Europe

Remarque : l'AfriNIC pour l'Afrique ainsi que le LACNIC pour l'Amérique Latine sont en cours de création).

Les adresses IP sont allouées à l'utilisateur final qui en fait la demande par un « Local Internet Registry », ou LIR, autorisé par le RIPE NCC. Un LIR est généralement un FAI ou une grande organisation (entreprise multinationale). Il est sous l'autorité de l'instance régionale de gestion de

l'adressage. Ainsi pour un utilisateur (quelle que soit sa taille) changer de FAI implique aussi de changer de plan d'adressage IP, lorsque celles-ci ont été allouées statiquement par le LIR. Les adresses IP sont alors restituées puis ré-attribuées à d'autres utilisateurs.

On compte plus de 2000 de LIRs offrant leurs services en Europe selon le RIPE NCC

3. Anatomie d'une adresse IP

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.

Une adresse IP est un nombre de 32 bits que l'on a coutume de représenter sous forme de quatre entiers de huit bits, séparés par des points.

La partie réseau de l'adresse IP vient toujours en tête, la partie hôte est donc toujours en queue.

L'intérêt de cette représentation est immédiat quand on sait que la partie réseau et donc la partie hôte sont presque toujours codées sur un nombre entier d'octets. Ainsi, on a principalement les trois formes suivantes :

- Classe A : Un octet réseau, trois octets d'hôtes.
- Classe B : Deux octets réseau, deux octets d'hôtes.
- Classe C : Trois octets réseau, un octet d'hôte.

3.1. Décomposition en classes

Classe	Masque de sous réseau par défaut	Adresse réseau	Nombre de réseaux	Nombre d'hôtes
A	255.0.0.0	1.0.0.0 à 126.0.0.0	126 (= 2^7 - 2)	16 777 214
B	255.255.0.0	128.0.0.0 à 191.255.0.0	16 384 (=2^{14})	65 534
C	255.255.255.0	192.0.0.0 à 223.255.255.0	2 097 152 (=2^{21})	254
D	Non défini	224.0.0.0 à 239.255.255.0		
E	Non défini	240.0.0.0 à 255.255.255.0		

Pour distinguer les classes A, B, C, D et E il faut examiner les bits de poids fort de l'octet de poids fort. Ce premier octet désigne le numéro de réseau (NetID) et les 3 autres correspondent à l'adresse de l'hôte (HostID).

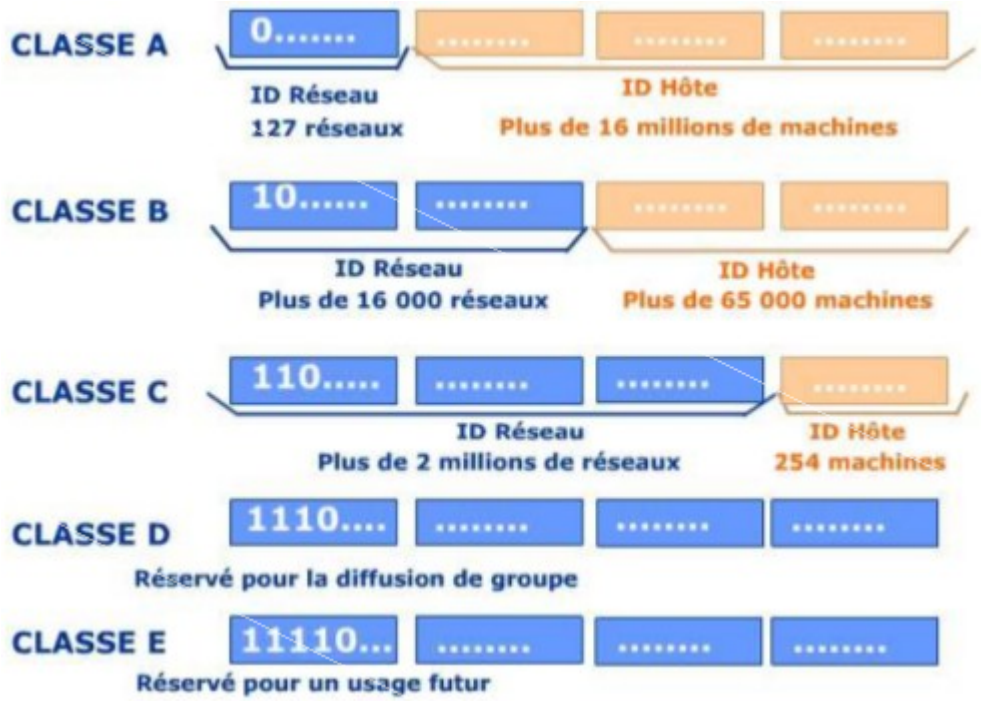
- Si le premier bit est 0, l'adresse est de classe A. On dispose de 7 bits pour identifier le réseau et de 24 bits pour identifier l'hôte. On a donc les réseaux de 1 à 127 et 224 hôtes possibles, c'est à dire 16 777 216 machines différentes (de 0 à 16 777 215).

  Remarque : l'adresse réseau 0.0.0.0 n'existe pas et le NetID « 127 » est réservée pour les communications en boucle locale (loopback), ce qui réduit de deux unités le nombre des machines nommables. Il reste donc seulement 16 777 214 machines adressables dans une classe A !

- Si les deux premiers bits sont 10, l'adresse est de classe B. Il reste 14 bits pour identifier le

réseau et 16 bits pour identifier la machine. Ce qui fait 2^{14}= 16 384 réseaux (128.0 à 191.255) et 65 534 (65 536 - 2) machines.

- Si les trois premiers bits sont 110, l'adresse est de classe C. Il reste 21 bits pour identifier le réseau et 8 bits pour identifier la machine. Ce qui fait 2^{21}=2 097 152 réseaux (de 192.0.0 à 223.255.255) et 254 (256 - 2) machines.
- Si les quatre premiers bits de l'adresse sont 1110 , il s'agit d'une classe d'adressage spéciale, la classe D. Cette classe est prévue pour faire du « multicast » ou multipoint.
- Si les quatre premiers bits de l'adresse sont 1111, il s'agit d'une classe expérimentale, la classe E.



3.2. Adresses particulières

Il existe un certain nombre d'adresses IP réservées :

- hostid = 0 désigne le réseau lui même

  L'hostid égal à 0 ne sera jamais affecté à un hôte mais il désigne le réseau lui même.

  Exemple : 192.145.56.0 est un réseau de classe C dont l'hostid est à 0 donc cette adresse désigne le réseau lui même.

- 0.0.0.0 désigne l'hôte lui même

  Lorsque tous les bits d'une adresse IP sont à 0, cela signifie "cet hôte-ci sur ce réseau". Cette adresse spéciale est utilisée par un hôte afin d'obtenir une adresse IP de manière dynamique dans le cas du protocole BOOTP.

- Tous les bits de l'hostid = 1 indique une diffusion dirigée

  Lorsque tous les bits de l'hostid sont égaux à 1, on est en présence non pas d'une adresse d'hôte mais d'une adresse de diffusion dirigée (direct broadcast) c'est à dire un message

destiné à tous les hôtes d'un réseau sans exception.

Exemple : 192.145.56.255 est une adresse de classe C dont la partie réservée à l'hostid est égale à 255 donc pour laquelle tous les bits sont à 1, on est donc en présence d'un message destiné à l'ensemble des hôtes du réseau 192.145.56.0.

- 255.255.255.255 = diffusion limitée

  Une diffusion limitée (limited broadcast) est un message qui est envoyé à tous les hôtes du réseau dont fait partie l'expéditeur. La diffusion limitée est représentée par l'adresse spéciale 255.255.255.255.

- Exemple : L'adresse de destination 255.255.255.255 indique que le message doit être envoyé à tous les hôtes du réseau dont fait partie l'expéditeur.

- netid = 0 indique que l'hôte fait partie du réseau

  Lorsque que la partie netid est égale à 0 et que la partie hostid est non nulle, cela signifie qu'on est en présence d'un message issu du même réseau.

  Exemple : Si un hôte d'adresse 192.14.25.56 reçoit un paquet à destination de 0.0.0.56, il considérera que ce paquet lui est bien destiné.

- 127.x.x.x = adresse de bouclage

  Le netid 127.0.0.0 qui aurait du normalement faire partie de la classe A est en fait utilisé pour désigner l'adresse de bouclage (loopback), peut importe le hostid utilisé. Un paquet envoyé à cette adresse ne passe pas par les interfaces réseau mais est déposé directement sur le tampon de réception de la machine elle même. Cette adresse de bouclage permet de vérifier la configuration de la couche logicielle TCP/IP d'une machine.

  Exemple : 127.0.0.1 désigne l'adresse de bouclage sur la machine elle même.

Quelques exemples d'adresses avec une signification particulière :

- 0.0.0.0 Hôte inconnu, sur ce réseau
- 0.0.0.1 L'hôte 1 de ce réseau
- 255.255.255.255 Tous les hôtes
- 138.195.52.1 L'hôte 52.1 du réseau 138.195.0.0
- 138.195.0.0 Cet hôte sur le 138.195.0.0
- 193.104.1.255 Tous les hôtes du 193.104.1.0
- 127.0.0.1 Cet hôte (boucle locale).

Remarque : les deux premières adresses, avec un numéro de réseau égal à 0, ne peuvent figurer que comme adresse source dans des cas bien particuliers comme le démarrage d'une station.

3.3. 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 1984.

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.

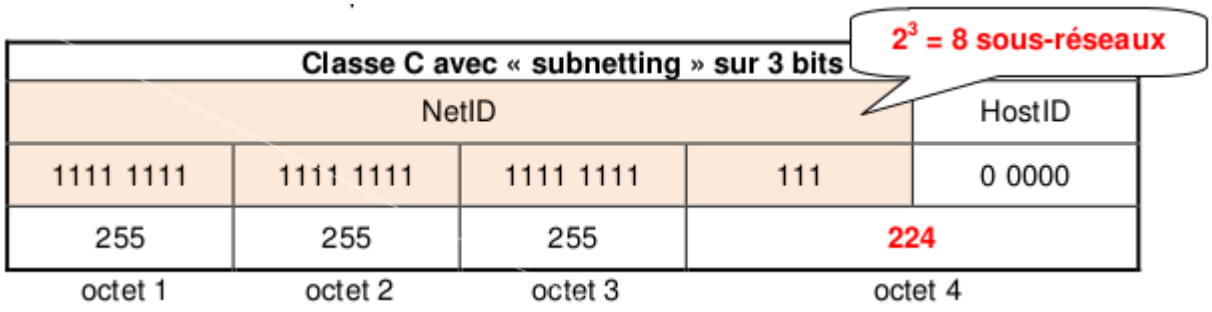
Le « subnet » utilise les bits de poids fort de la partie hôte de l'adresse IP, pour désigner un réseau. Le nombre de bits employés est laissé à l'initiative de l'administrateur.

Au quotidien, on évite l'engorgement des liens en limitant géographiquement les annonces de services faites par les serveurs de fichiers. 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, nous allons utiliser un exemple pratique. On reprend l'exemple de la classe C : 192.168.1.0 dont le masque de sous-réseau par défaut est 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 4 ème octet en complétant le masque de sous-réseau. De cette façon on augmente la partie réseau de l'adresse IP et on diminue la partie hôte.



Sous réseau	Masque	@ réseau	Plage d'@ utilisables	@ de diffusion
0	255.255.255.224	192.168.1.0	192.168.1.1 192.168.1.30	192.168.1.31
1		192.168.1.32	192.168.1.33 192.168.1.62	192.168.1.63
2		192.168.1.64	192.168.1.65 192.168.1.94	192.168.1.95
3		192.168.1.96	192.168.1.97 192.168.1.126	192.168.1.127
4		192.168.1.128	192.168.1.129 192.168.1.158	192.168.1.159
5		192.168.1.160	192.168.1.161 192.168.1.190	192.168.1.191
6		192.168.1.192	192.168.1.193 192.168.1.222	192.168.1.223
7		192.168.1.224	192.168.1.225 192.168.1.254	192.168.1.255

Nbre de s/réseaux = nbre de bits attribués en plus au netID[2]

On peut remarquer 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 de diffusion (broadcast) vers tous les hôtes du sous-réseau.

3.4. CIDR

En 1992 la moitié des classes B étaient allouées, et si le rythme avait continué, au début de 1994 il n'y aurait plus eu de classe B disponible et l'Internet aurait bien pu mourir par asphyxie ! De plus la croissance du nombre de réseaux se traduisait par un usage « aux limites » des routeurs.

Deux considérations qui ont conduit l'IETF a mettre en place le CIDR (Classless InterDomain Routing ou routage sans classe inter domaines) basé sur une constatation de simple bon sens :

- S'il est courant de rencontrer une organisation ayant plus de 254 hôtes, il est moins courant d'en rencontrer une de plus de quelques milliers.

  Les adresses allouées sont donc des classes C contiguës, attribuées par région ou par continent. En générale, 8 à 16 classes C mises bout à bout suffisent pour une entreprise. Ces blocs de numéros sont souvent appelés « supernet ».

  Ainsi par exemple il est courant d'entendre les administrateurs de réseaux parler d'un « slash 22 » (/22) pour désigner un bloc de quatre classes C consécutives...

- Il est plus facile de prévoir une table de routage pour un bloc d'adresses contiguës qu'adresse par adresse, en plus cela allège les tables.

Plus précisément, trois caractéristiques sont requises pour pouvoir utiliser ce concept :

1. Pour être réunies dans une même route, des adresses IP multiples doivent avoir les mêmes bits de poids fort.
2. Les tables de routages et algorithmes doivent prendre en compte un masque de 32 bits, à appliquer sur les adresses.
3. Les protocoles de routage doivent ajouter un masque 32 bits pour chaque adresse IP (Cet

ajout double le volume d'informations) transmise.

3.4.1. Supernetting

Nous avons la possibilité d'utiliser un seul réseau qui fusionne plusieurs sous-réseaux. Cette fusion de sous-réseaux, dite aussi supernetting, est l'essence même de CIDR. Cette technique est également appelée résumé de routes (route summarization en anglais).

Pour implémenter un réseau fondé sur l'adressage CIDR, il faut utiliser un protocole qui puisse le supporter. Il en existe plusieurs, tels que BGP et OSPF. Si le protocole ne supporte pas ce type d'adressage, le routage échouera dans ce réseau.

« Supernetter » un réseau est exactement le contraire de « subnetter » un réseau, sauf qu'ici, il ne s'agit plus de l'adressage par classes mais de l'adressage CIDR. Tous ces sous-réseaux peuvent donc être fusionnés et rassemblés sous un seul préfixe.

Si nous avons quatre subnets tels que :

- Subnet 1 : 192.168.0.0/24 soit 11000000. 10101000. 00000000.00000000/24
- Subnet 2 : 192.168.1.0/24 soit 11000000. 10101000. 00000001.00000000/24
- Subnet 3 : 192.168.2.0/24 soit 11000000. 10101000. 00000010.00000000/24
- Subnet 4 : 192.168.3.0/24 soit 11000000. 10101000. 00000011.00000000/24

Nous remarquons que ces quatre subnets ont bien le même préfixe /24 : nous pouvons les fusionner sous un seul préfixe. Par conséquent, nous obtenons la route suivante : 192.168.0.0/22.

3.4.2. Les masques à longueurs variables

VLSM, pour Variable Length Subnet Mask (soit masque de sous-réseaux à longueur variable) est une technique utilisée dans le but de mieux gérer les adresses IP, tout comme le CIDR. En fait, VLSM est une extension de CIDR. La différence est que le CIDR est plus utilisé au niveau internet et le VLSM est plus utilisé dans un réseau local, mais les deux permettent de minimiser la perte d'adresses.

Pour mettre en place un réseau aux masques à longueurs variables, il faut être sûr que les routeurs supportent les protocoles compatibles au VLSM. Quelques-uns de ces protocoles sont OSPF, EIGRP, RIPv2. IS-IS.

VSLM consiste à obtenir des sous réseaux dont les plages d'adresses sont de tailles différentes. En fait, il faut créer des sous-réseaux différents dans des sous-réseaux, c'est ce qu'on appelle subnetter un subnet (sous-réseauter un sous-réseau).

Voir exercice 4.

4. Adressage multicast

En règle générale l'adressage multicast est employé pour s'adresser en une seule fois à un groupe de machines.

Dans le cas d'un serveur vidéo/audio, cette approche induit une économie de moyen et de bande passante évidente quand on la compare à une démarche « unicast » : un seul datagramme est routé vers tous les clients intéressés au lieu d'un envoi massif d'autant de datagrammes qu'il y a de clients.

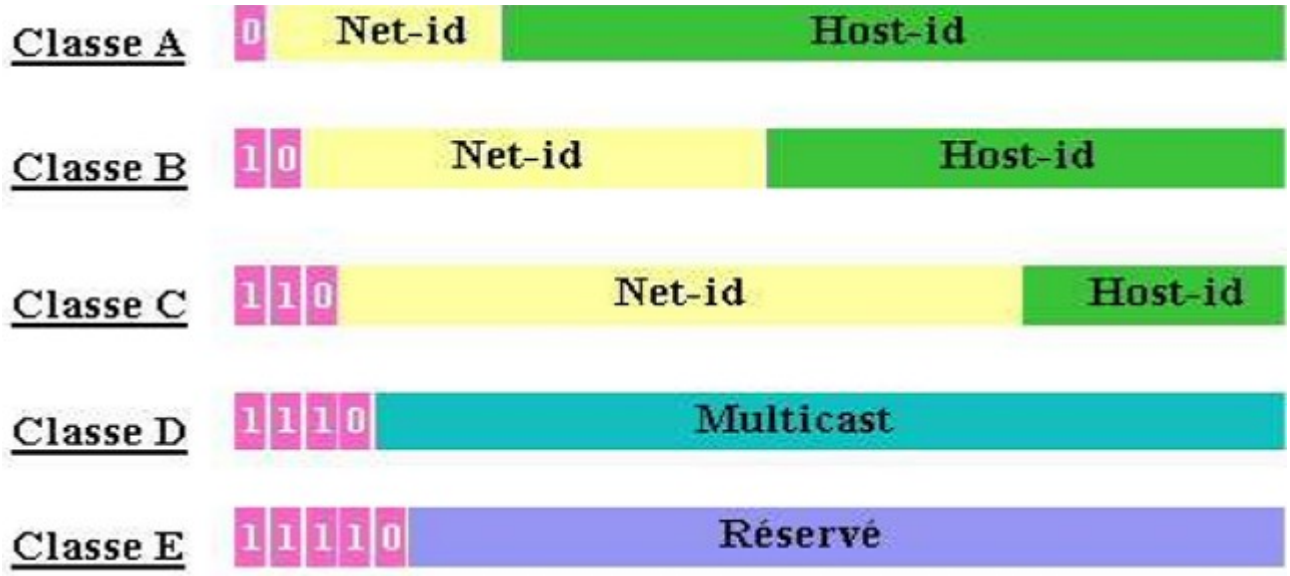
Les adresses de type « multicast » ont donc la faculté d'identifier un groupe de machines qui

partagent un protocole commun par opposition à un groupe de machines qui partagent un réseau commun.

La plupart des adresses multicast allouées le sont pour des applications particulières comme par exemple la découverte de routeurs ou encore la radio ou le téléphone/vidéo sur Internet

4.1. Adresse de groupe multicast

Si une adresse multicast démarre avec les bits 1110 par contre pour les 28 bits suivants son organisation interne diffère de celle des classes A, B et C.



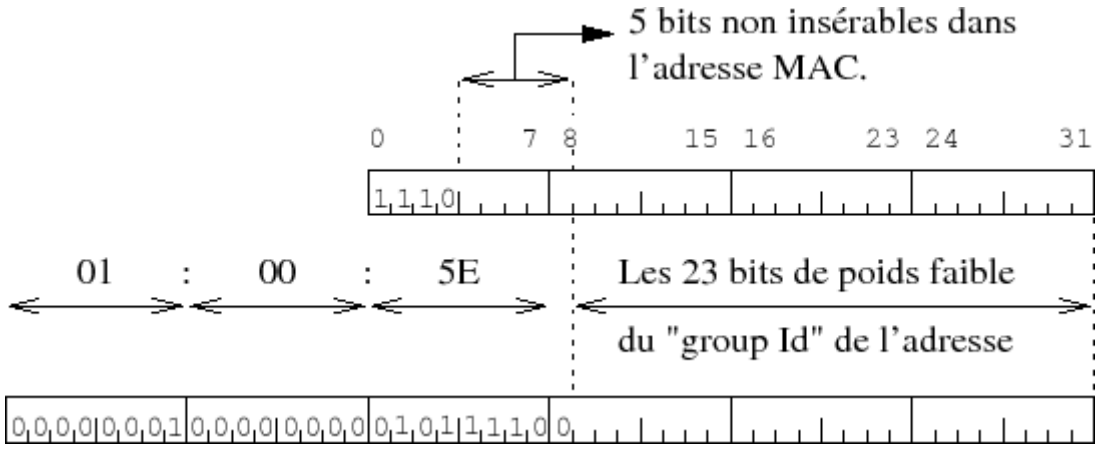
- Les 28 bits n'ont pas de structure particulière par contre on continue à utiliser la notation décimale pointée : 224.0.0.0 à 239.255.255.255.
- Un groupe d'hôtes qui partagent un protocole commun utilisant une adresse multicast commune peuvent être répartis n'importe où sur le réseau.
- L'appartenance à un groupe est dynamique, les hôtes qui le désirent rejoignent et quittent le groupe comme ils veulent.
- l n'y a pas de restriction sur le nombre d'hôtes dans un groupe et un hôte n'a pas besoin d'appartenir à un groupe pour lui envoyer un message.

4.2 Adresse multicast et adresse MAC

Une station Ethernet quelconque doit être configurée pour accepter le multicast, c'est à dire pour accepter les trames contenant un datagramme munis d'une adresse IP de destination qui est une adresse multicast.

Cette opération sous entend à juste titre que la carte réseau sait faire le tri entre les trames. En effet les trames multicast ont une adresse MAC particulière : elles commencent forcément par les trois octets 01:00:5E. Ceux-ci ne désignent pas un constructeur en particulier mais sont possédés par l'ICANN (ex IANA).

Restent trois octets, soit 24 bits dont le premier est forcément à 0 pour désigner les adresses de multicast, ce qui conduit au schéma suivant :



Du fait qu'il n'y a pas assez de place dans l'adresse MAC pour faire tenir les 28 bits du groupe multicast, cette adresse n'est pas unique. On peut même préciser que pour chaque trame comportant une adresse multicast il y a 25 adresses IP de groupes multicast possibles !

Ce qui signifie que si les 23 bits de poids faible ne suffisent pas à discriminer la trame il faudra faire appel au pilote de périphérique ou à la couche IP pour lever l'ambiguïté.

Quand une trame de type multicast est lue par la station Ethernet puis par le pilote de périphérique, si l'adresse correspond à l'une des adresses de groupe multicast préalablement configurées, le datagramme franchit la couche IP et une copie des données est délivrée aux processus qui ont « joint le groupe multicast ».

5. Adresses IPv6

Les adresses IPv6 utilisées sur Internet sont très structurées et hiérarchisées :

IANA	RIR	LIR	Client	Sous-réseau	Hôte
3 bits	20 bits	9 bits	16 bits	16 bits	64 bits

L'IANA est l'organisme qui gère les adresses IP sur Internet. Il a décidé que les adresses IPv6 utilisables sur Internet commenceraient par 2000::/3, puis il donne au RIR des valeurs sur 20 bits pour différentes zones géographiques. Chaque RIR donne ensuite aux LIR des valeurs pour chacun d'entre eux, qui eux-mêmes vont distribuer des valeurs aux clients, qui vont... etc.

En dehors des adresses de lien local et globales, il existe aussi quelques adresses particulières à connaître :

1. Les adresses courtes
   - ::1 : c'est l'adresse de la boucle locale (loopback). C'est l'équivalent de 127.0.0.1 en IPv4.
   - :: (ou ::0) : c'est l'adresse que prend la carte réseau avant de s'attribuer une adresse.
2. Les adresses de site local

   Ces adresses sont attribuées au sein d'un site mais ne sont pas accessibles depuis le réseau public (comme les adresses privées en IPv4). Elles commencent par FEC0::/10 et sont structurées de la manière suivante :

10 bits	54 bits	64 bits

1111 1110 11	identifiant du sous-réseau	identifiant de l'hôte

3. Les adresses multicast

   Elles commencent par FF00::/8 et servent à désigner et gérer des groupes d'hôtes.

   NB : Contrairement à IPv4, en IPv6, il n'existe pas d'adresse de broadcast !

4. Les adresses d'encapsulation 4/6

   IPv6 est compatible avec IPv4. On peut s'adresser à une adresse IPv4 même si on a juste une adresse IPv6 de cette manière :

10 octets	**2 octets**	**4 octets**
Que des zéros	0xFFFF	L'adresse IPv4

   Exemples :

Adresse IPv4	**Adresse IPv6 d'encapsulation**
42.13.37.42	::FFFF:42.13.37.42
192.168.2.1	::FFFF:192.168.2.1

6. Le routage

Deux hôtes ne se situant pas dans le même sous-réseau ne peuvent pas communiquer directement. Il faut une passerelle entre les deux pour transmettre à l'un, les données au nom de l'autre.

Dans un réseau comprenant plusieurs routeurs, la passerelle par défaut (default gateway, en anglais) est l'interface du routeur vers laquelle sont dirigés tous les paquets dont on ne connaît pas la route à emprunter pour atteindre le réseau dans lequel se trouve le destinataire. Chaque routeur a une table de routage constituée d'une liste des différentes "routes" (chemins) vers d'autres sous-réseaux.

Soient 2 ordinateurs : Azur-PC et Safran-PC dont les cartes réseau sont configurées ainsi :

Nom	**Adresse IP**	**Masque de sous-réseau**
Azur-PC	192.0.1.5	255.255.255.0
Safran-PC	72.40.2.1	255.0.0.0

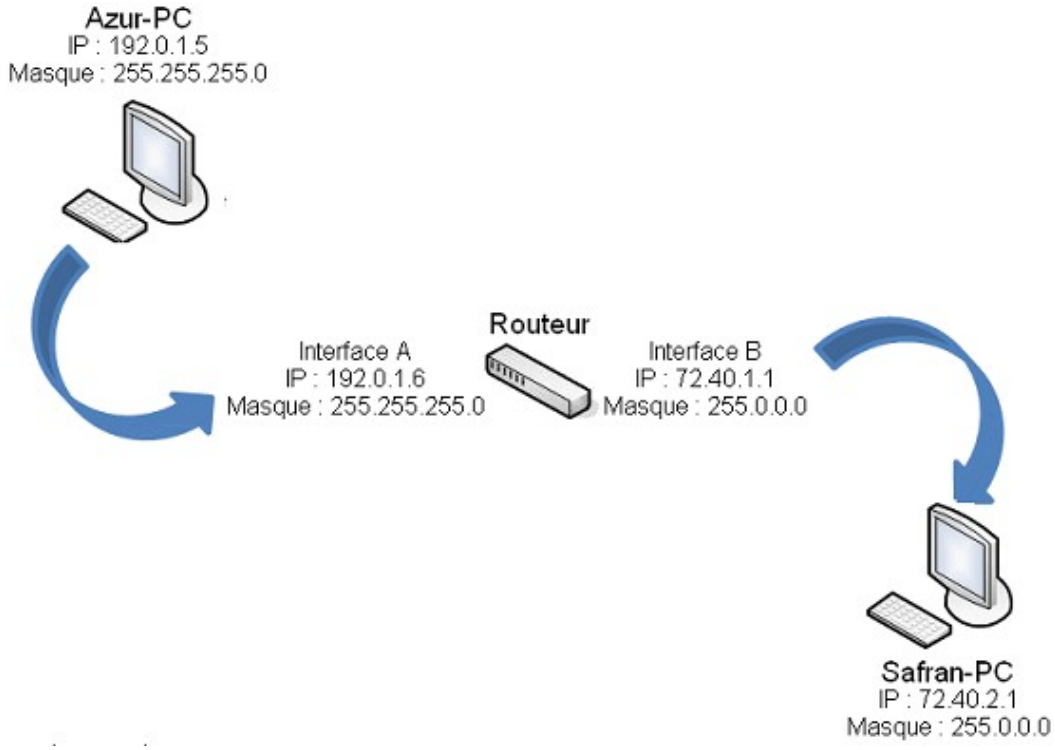
Azur-PC a recours à un processus nommé ANDing, pour déterminer si Safran-PC, avec qui il veut communiquer, est dans le même sous-réseau que lui. Il réalise que ce n'est pas le cas, il va donc transférer son message à la passerelle en lui indiquant l'adresse du destinataire.

Supposons que ce soit un routeur qui offre ce service. Il a 2 interfaces. Pour que la communication puisse avoir lieu, une de ses interfaces doit être dans le même sous-réseau que Azur-PC et l'autre dans le même que Safran-PC. Voici une configuration possible pour ce routeur :

Interface	**Adresse IP**	**Masque de sous-réseau**
A	192.0.1.6	255.255.255.0
B	72.40.1.1	255.0.0.0

Avec une telle configuration, Azur-PC et Safran-PC peuvent à présent communiquer. Quand Azur-PC voudra parler à Safran-PC, il vérifiera grâce au ANDing si le destinataire est dans le même sous-

réseau. Si oui, il enverra son message directement à son adresse IP, sinon, il l'envoie à la passerelle en lui demandant de transmettre à bon port.



Déterminer si l'adresse IP du destinataire est dans le même sous-réseau que celle de l'émetteur est assez simple. La carte réseau de l'émetteur connaît son adresse IP, son masque de sous-réseau et l'adresse IP du destinataire. Elle fait un ET logique (AND) entre l'adresse IP de l'émetteur et son masque de sous-réseau pour trouver son network ID. Ensuite, elle fait un ET logique entre l'adresse IP du destinataire et le masque de sous-réseau de l'émetteur et compare le résultat avec le network ID obtenu précédemment. Si les deux valeurs sont identiques, alors l'émetteur et le destinataire sont dans le même sous-réseau. Sinon, ils sont dans des sous-réseaux différents.

Nom	Azur-PC	
Adresse IP	192.0.1.5	`11000000.00000000.00000001.00000101`
masque	255.255.255.0	`11111111.11111111.11111111.00000000`
	AND	`11000000.00000000.00000001.00000000`
Adresse réseau	192.1.0.0	

Nom	Safran-PC	
Adresse IP	72.40.2.1	`10010000.00101000.00000010.00000001`
masque	255.0.0.0	`11111111.00000000.00000000.00000000`
	AND	`10010000.00000000.00000000.00000000`
Adresse réseau	72.0.0.0	

Nous n'obtenons pas les mêmes valeurs. Par conséquent, ces deux adresses IP (142.20.1.15 et 92.40.1.14) ne sont pas dans le même sous-réseau.

7. Exercices

7.1. Énoncé

1. 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.

   Question 1.1 : Quel est le masque réseau de cette adresse ?

   Question 1.2 : Combien de bits ont été réservés pour les sous-réseaux privés ?

   Question 1.3 : Combien de sous-réseaux privés sont disponibles ?

   Question 1.4 : Quelle est l'adresse du sous-réseau de l'exemple ?

   Question 1.5 : Quelle est l'adresse de diffusion du sous-réseau de l'exemple ?

2. Considérons le réseau 40.0.0.0.

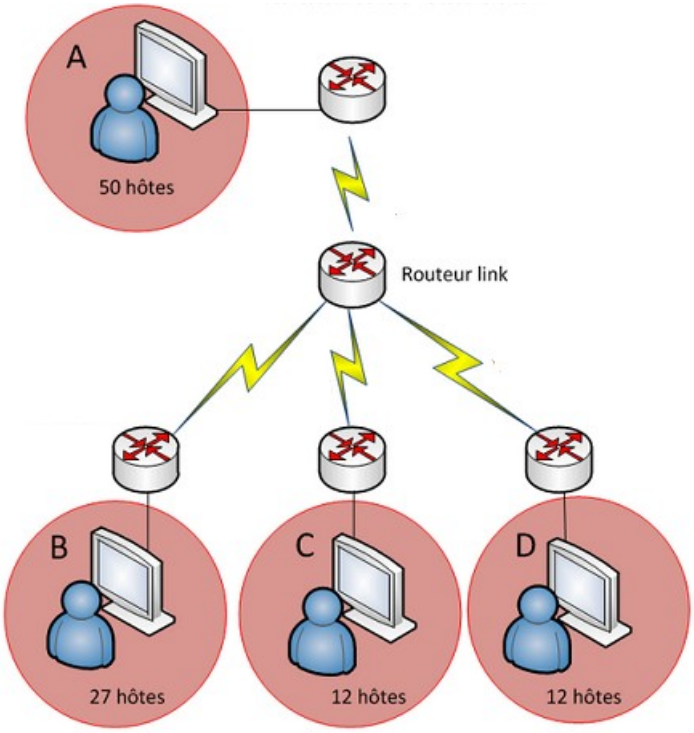
   Question 2 : Donner le plan d'adressage pour le diviser en 20 sous-réseaux.

3. Considérons le réseau 158.37.0.0.

   Question 3 : Donner le plan d'adressage pour avoir 1800 hôtes par sous-réseau.

4. Considérons le sous-réseau 192.168.100.0/24. On souhaite une segmentation par fonctions :

   - Un sous-réseau de 50 hôtes, uniquement pour les secrétaires de l'entreprise.
   - Deux sous-réseaux de 12 hôtes chacun, pour les techniciens et les comptables.
   - Un sous-réseau de 27 hôtes pour les développeurs d'applications.



Les réseaux B, C, D ne peuvent communiquer qu'avec A.

Question 4 : Déterminer le plan d'adressage pour réaliser ce cahier des charges.

7.2. Correction

Question 1.1 :

La notation /21 indique que le netID occupe 21 bits. On décompose ces 21 bits en 8 bits + 8 bits + 5 bits ; ce qui donne : 255.255.248.0.

Question 1.2 :

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 par défaut d'une classe B étant 255.255.0.0, 5 bits (1111 1000) ont été réservés sur le troisième octet pour constituer des sous-réseaux.

Question 1.3 :

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 routée sans tenir compte de son masque et donc de sa longueur variable.

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

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

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

Question 1.4 :

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 correspondante 5 bits réseau (11111000) on obtient : 00010000 ; soit 16 en décimal.

L'adresse du sous-réseau est donc 172.16.16.0.

Question 1.5 :

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.

Question 2 :

On remarque que $2^4 - 1 < 20 < 2^5 - 1$; **5** bits suffisent pour le masquage.

Nous obtenons ainsi :

réseau	40	0	0	0
adresses	ssssssss	**sssss**hhh	hhhhhhhh	hhhhhhhh

masque	255	248	0	0

Chaque sous réseaux seront séparés de $2^{n-1} = 2^3 = 8$ intervalles (ou 255 – 248).

Nous avons donc :

Ordinal	**Adresse du sous-réseau**	**Première adresse IP d'hôte**	**Dernière adresse IP d'hôte**
1er	40.0.0.0	40.0.0.1	40.7.255.254
2ème	40.8.0.0	40.8.0.1	40.15.255.254
3ème	40.16.0.0	40.16.0.1	40.23.255.254
…	…	…	...
Dernier	40.240.0.0	40.240.0.1	40.247.255.254

Question 3 :

On remarque que $2^{10} – 2 < 1800 < 2^{11} – 2$; **11** bits suffisent pour le masquage.

NB : on doit exclure l'adresse réseau et celle de diffusion.

Nous obtenons ainsi :

réseau	158	37	0	0
adresses	ssssssss	ssssssss	sssss**hhh**	**hhhhhhhh**
masque	255	255	248	0

Chaque sous réseaux seront séparés de $2^{n-1} = 2^3 = 8$ intervalles (ou 255 – 248).

Nous avons donc :

Ordinal	**Adresse du sous-réseau**	**Première adresse IP d'hôte**	**Dernière adresse IP d'hôte**
1er	158.37.0.0	158.37.0.1	158.37.7.254
2ème	158.37.8.0	158.37.8.1	158.37.15.254
3ème	158.37.16.0	158.37.16.1	158.37.23.254
…	…	…	...
Dernier	158.37.240.0	158.37.240.1	158.37.247.254

Voilà donc un certain nombre de sous-réseaux avec 2046 adresses d'hôtes dans chaque. On n'en voulait que 1800, mais ce n'était pas possible de les avoir précisément, donc on a pris la valeur possible immédiatement supérieure.

Question 4 :

Considérons d'abord le sous-réseau qui a le plus grand nombre d'hôtes : $2^6 – 2 = 62 > 50$.

Nous obtenons ainsi :

réseau	192	168	100	0
adresses	11000000	10101000	01100100	**nn**hhhhhh

Une fois résolu le plus grand sous-réseau, il faut choisir quel subnet ID donner à ce sous-réseau. Avec 2 bits pour le sous-réseau, nous obtenons le network ID pour chaque sous-réseau :

host ID	**Network ID/masque**
00hhhhhh	192.168.100.0/26

01hhhhhh	192.168.100.64/26
10hhhhhh	192.168.100.128/26
11hhhhhh	192.168.100.192/26

Nous prendrons arbitrairement 192.168.100.64 pour le sous-réseau A ; les autres sous-réseaux devront se contenter des trois sous-réseaux restants.

Le second plus grand sous-réseau contient dans notre exemple 27 hôtes pour les développeurs d'applications. Il s'agit du sous-réseau B. Nous aurons besoin d'au moins 5 bits pour les hôtes ($2^5 - 2 = 30 > 27$.

Nous prendrons arbitrairement 192.168.100.128/26 et nous réallouerons le 6ème bit au sous-réseau 10**n**hhhhh :

host ID	**Network ID/masque**
100hhhhh	192.168.100.128/27
101hhhhh	192.168.100.160/27

Enfin, pour les réseau C et D, 4 bits suffisent pour les hôtes : $2^4 - 2 = 14 > 12$.

Nous prendrons arbitrairement 192.168.100.160 et nous réallouerons le 5ème bit au sous-réseau 101**n**hhhh :

host ID	**Network ID/masque**
1010hhhh	192.168.100.160/28
1011hhhh	192.168.100.176/28

En résumé :

- 00000000 = .0/26 | subnet libre pour être re-subnetté
- 01000000 = .64/26 | déjà utilisé par le sous-réseau A
- 10000000 = .128/26 | inutilisable, car re-subnetté
- 11000000 = .192/26 | subnet pour un futur agrandissement
- 10000000 = .128/27 | déjà utilisé pour le sous-réseau B
- 10100000 = .160/27 | inutilisable, car re-subnetté
- 10100000 = .160/28 | sous-réseau C
- 10110000 = .176/28 | sous-réseau D

Il reste à déterminer les Network ID pour les interfaces de liaison du routeur routeur_link, soit deux interfaces de liaison par réseau.