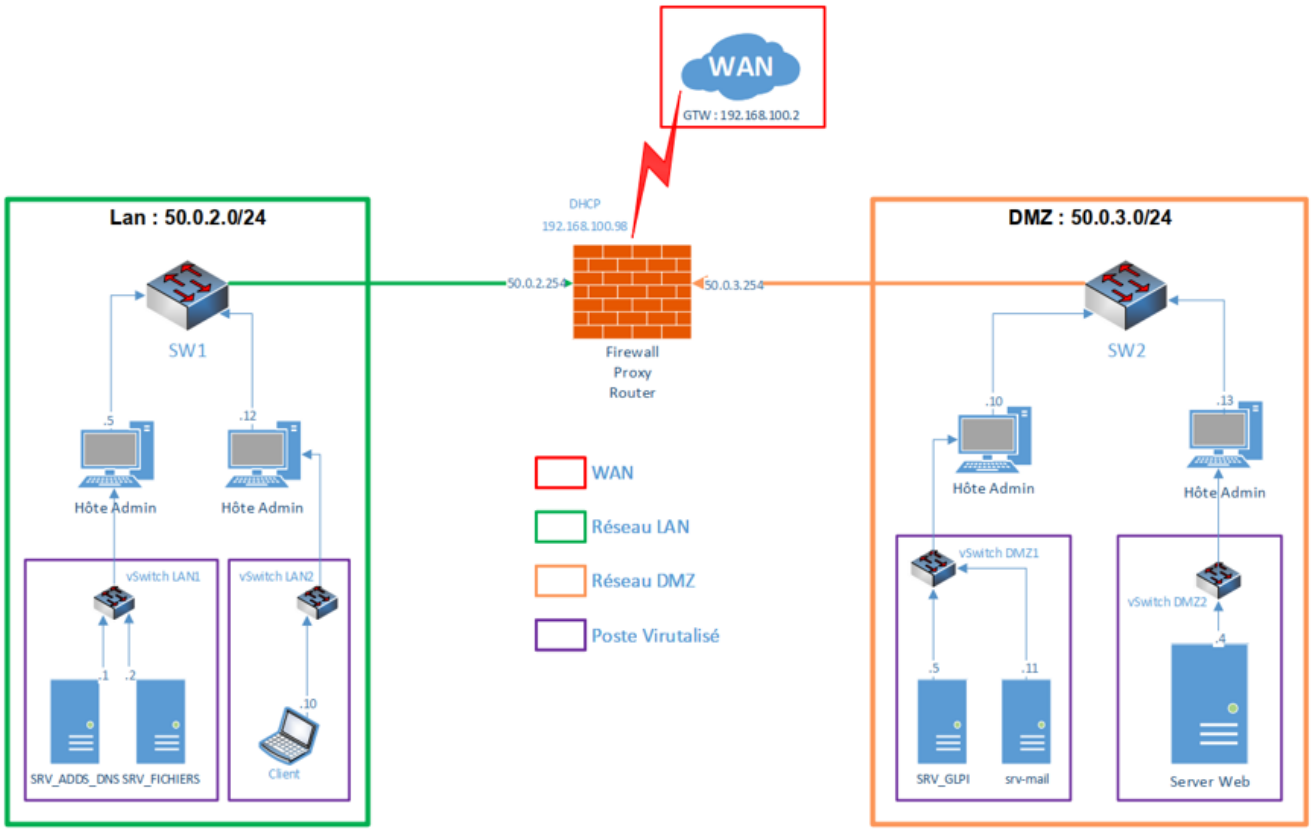
Contenue

Introduction

Un réseau informatique (en anglais, data communication network ou DCN) est un ensemble d'équipements reliés entre eux pour échanger des informations.

Ces données ce transmettront par le biais de câbles dans lesquels circulent des signaux électriques, l'atmosphère où circulent des ondes radio, ou des fibres optiques qui propagent des ondes lumineuses. Elles permettent de relier « physiquement » des équipements assurant l'interconnexion des moyens physiques qui sont définis par des protocoles. Les équipements d'un réseau sont connectés directement ou non entre eux, conformément à quelques organisations types connues sous le nom de topologie de réseau.



Protocoles et services

Les protocoles de communication définissent de façon formelle et interopérable la manière dont les informations sont échangées entre les équipements du réseau.

Le protocole probablement le plus répandu est IP qui permet l'acheminement des paquets jusqu'à leur destination. Deux protocoles de niveau supérieur UDP et TCP permettent le transport de données. Le premier permet l'envoi de données d'une manière non fiable (aucune garantie de la réception du paquet par le destinataire). L'autre permet au contraire une transmission fiable des données (garantie de la réception du paquet par le destinataire et aussi par accusés de réception). Les services réseau se basent sur les protocoles pour fournir, par exemple :

- Des transferts de textes (SMS…) ;
- Ou de données (Internet…) ;
- Des communications vocales (téléphone…) ; VoIP
- Des diffusions d'images (télé…) : TNT-HD principalement.

Sous-réseau

Un réseau (ne pas confondre ce terme avec celui qui sert à désigner la couche no 3 dans le modèle OSI de l'ISO ou la couche Réseau dans la pile de protocoles Internet) ou sous-réseau peut être composé de plusieurs réseaux ou sous réseaux à base d'équipements matériels. Dans le protocole IP les membres d'un même sous réseau ou réseau possèdent le même identifiant, calculable à partir de l'adresse IP et du masque de sous réseau. L'utilisation d'une architecture comprenant des sous-réseaux permet une gestion du parc informatique plus aisée (un sous-réseau par service ou par salle, par exemple)

IPV 4 – IPV6

IPv4 est le protocole le plus couramment utilisé en 2022, sur Internet tout comme sur les réseaux privés. IPv6 est son successeur.

IPv4 utilise des adresses codées sur 32 bits (soit en théorie 4 294 967 296 adresses possibles) tandis qu'IPv6 les code sur 128 bits (soit en théorie 3,4 × 1038 adresses possibles).

Adressage

1. Adresse IP

2 PC ou serveurs ne peuvent pas avoir la même adresse IP sur un même réseau ! En revanche, sur des réseaux différents, cela peut-être le cas et ceci grâce à la notion de routage.

Par exemple, la Freebox possède toujours l'adresse IP interne 192.168.1.254 quand elle est livrée chez les particuliers. Cette adresse est une adresse privée. Elle dispose également d'une adresse publique, différente chez tous les utilisateurs.

a. Classe d'adresse IP

Chaque adresse IP appartient à une classe qui correspond à une plage d'adresses IP. Ces classes d'adresses sont au nombre de 5 c'est-à-dire les classes A, B, C, D et E.

- La classe A de l'adresse IP 0.0.0.0 à 126.255.255.255 (privées et publiques).
- La classe B de l'adresse IP 128.0.0.0 à 191.255.255.255 (privées et publiques).
- La classe C de l'adresse IP 192.0.0.0 à 223.255.255.255 (privées et publiques).
- La classe D de l'adresse IP 224.0.0.0 à 239.255.255.255 (adresses de multicast).
- La classe E de l'adresse IP 240.0.0.0 à 255.255.255.255 (réservées par l'IETF, « Internet Engineering Task Force »).

b. Adresses réservées

Dans le Protocole Internet Version 4, certaines adresses ne peuvent pas être attrinuées, car elles sont réservées pour le fonctionnement du réseau.

- 0.0.0.0 : est une méta-adresse non-routable utilisée pour désigner une destination invalide, inconnue ou non-atteignable.
- 127.0.0.0 : Adresses de bouclage (localhost). Le nom localhost est associé à l'adresse IPv6 « ::1 » et à la plage d'adresses IPv4 127.0.0.0/8 (toutes les adresses IPv4 comprises entre 127.0.0.1 et 127.255.255.255 dont la plus utilisée est 127.0.0.1). L'interface réseau virtuelle utilisée dans cette situation se nomme l'interface de loopback (abrégée par lo sous Unix) ou boucle locale.
- Broadcast, « 192.168.1.255 – 255.255.255.0 » : Adresse de diffusion qui permet de diffuser des données à plusieurs machines en même temps (multicast), au contraire d'une communication « Point à Point » (unicast)

2. Tableau Binaire – Décimal

Une adresse IPv4 ou le masque est composée de 4 octets délimités par des points avec une valeur allant de "0" à "255" pour chaque bloc. Une adresse IPv4 est codée sur 4 octets c'est-à-dire un total de 32 bits : 4 x 8 bits.

Rappel : 1 octet = 8 bits

Puissance	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Décimale	128	64	32	16	8	4	2	1	Somme Décimal 255
Binaire	1	1	1	1	1	1	1	1	Somme Binaire 8

Exemple pour l'adresse 192.168.1.1 avec le masque 255.255.255.0 ou en CIDR /24

Puissance	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Décimale	128	64	32	16	8	4	2	1
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
1	0	0	0	0	0	0	0	1
1	0	0	0	0	0	0	0	1

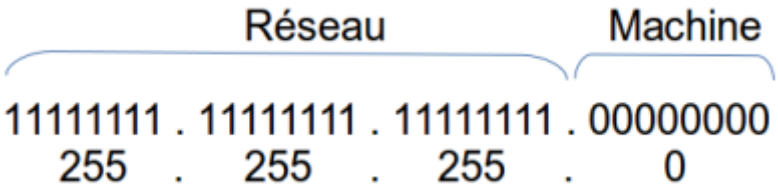
La valeur binaire de l'adresse est : 11000000. 10101000.00000001.00000001

Puissance	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Décimale	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

La valeur binaire du masque est : 11111111.11111111.11111111.00000000

3. Le Masque

Une adresse IP est toujours associée à un masque de sous-réseau. Il est un séparateur entre la partie réseau et la partie machine d'une adresse IP. Le masque, comme l'adresse IP, est une suite de 4 octets, soit 32 bits. Chacun de ces bits peut prendre la valeur 1 ou 0. Pour définir le masque, il nous suffit de dire que les bits à 1 représenteront la partie réseau (Net-ID) de l'adresse, et les bits à 0 la partie machine (Host-ID). 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.



Ainsi, dans l'exemple ci-dessus, il nous reste 8 bits à 0, on aura donc la possibilité d'avoir 2^8 = 256 adresses dans ce sous-réseau, ont enlève l'adresse réseau et de diffusion donc 2, ce qui nous revient à 254 adresses utilisables.

Un autre exemple avec un masque différent :

255.255.0.0 > Nous avons 16 bits à 0, donc ont fait 2^{16} – 2 = 65 536 adresses utilisables

4. Notation CIDR

Une autre notation est souvent utilisée pour représenter les masques, c'est la notation CIDR (Classless Inter-Domain Routing).

On la rencontre souvent car elle est plus rapide à écrire. Dans celle-ci, on compte directement le nombre de bits à 1, 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 255.255.255 correspond à 3 x 8 bits à 1 en binaire, 24 bits sont donc significatifs de la partie réseau de l'adresse.

Notez que sur chaque ligne, il y a deux adresse hôtes supprimés, car ces deux adresses sont toujours réservées pour le réseau et broadcast.

Notation CIDR	Nombre total d'adresses	Nombre d'hôtes	Masque de réseau
/30	4	2	255.255.255.252
/29	8	6	255.255.255.248
/28	16	14	255.255.255.240
/27	32	30	255.255.255.224
/26	64	62	255.255.255.192
/25	128	126	255.255.255.128
/24	256	254	255.255.255.0
/23	512	510	255.255.254.0
/22	1,024	1,022	255.255.252.0
/21	2,048	2,046	255.255.248.0
/20	4,096	4,094	255.255.240.0
/19	8,192	8,190	255.255.224.0
/18	16,384	16,382	255.255.192.0
/17	32,768	32,766	255.255.128.0
/16	65,536	65,534	255.255.0.0
/15	131,072	131,070	255.254.0.0
/14	262,144	262,142	255.252.0.0
/13	524,288	524,286	255.248.0.0
/12	1,048,576	1,048,574	255.240.0.0
/11	2,097,152	2,097,150	255.224.0.0
/10	4,194,304	4,194,302	255.192.0.0
/9	8,388,608	8,388,606	255.128.0.0
/8	16,777,216	16,777,214	255.0.0.0
/7	33,554,432	33,554,430	254.0.0.0
/6	67,108,864	67,108,862	252.0.0.0
/5	134,217,728	134,217,726	248.0.0.0
/4	268,435,456	268,435,454	240.0.0.0
/3	536,870,912	536,870,910	224.0.0.0
/2	1,073,741,824	1,073,741,822	192.0.0.0
/1	2,147,483,648	2,147,483,646	128.0.0.0
/0	4,294,967,296	4,294,967,294	0.0.0.0

La notation CIDR est calculée à partir du nombre des uns dans le masque de sous-réseau lorsqu'il est converti en binaire. Par exemple, pour le masque de sous-réseau par défaut 255.255.255.0, il est converti en 11111111.11111111.11111111.00000000 en binaire. Additionnez-les et vous obtenez 24. Dans la notation CIDR, ça serait /24. Un masque de sous-réseau de 255.255.255.128 convertis en binaire est 11111111.11111111.11111111.10000000, qui contient 25, donc le préfixe de l'adresse IP sera /25.

5. Déterminer l'adresse du réseau et l'adresse de diffusion

a. Adresse réseau

L'adresse de réseau permet de savoir si 2 machines peuvent communiquer entre elles. Si ces 2 machines ont une adresse réseau identique, alors, elles appartiennent au même réseau et elles peuvent communiquer.

Pour cela ont va utiliser la méthode « ET logique » qui consiste à utiliser l'opérateur « ET ». L'adresse du réseau est obtenue en appliquant l'opérateur « ET » entre l'adresse IPv4 et le masque du réseau. L'adresse de l'hôte à l'intérieur du sous-réseau est quant à elle obtenue en appliquant l'opérateur ET entre l'adresse IPv4 et le complément à un du masque.

Exemple avec l'adresse 192.168.1.2 et le masque 255.255.255.0

0 ET 0 = 0 - 0 ET 1 = 0 - 1 ET 0 = 0 - 1 ET 1 = 1

```
192.168.1.2 & 255.255.255.0 = 192.168.1.0
192.168.1.2 & 0.0.0.255     = 0.0.0.2
```

< Adresse réseau
< Adresse hôte

Soit en binaire :

```
  11000000.10101000.00000001.00000010        11000000.10101000.00000001.00000010
& 11111111.11111111.11111111.00000000      & 00000000.00000000.00000000.11111111
= 11000000.10101000.00000001.00000000      = 00000000.00000000.00000000.00000010
```

b. Adresse de diffusion ou de broadcast

L'adresse de broadcast est une adresse IP qui termine en .255 dans des réseaux de classe A, B ou C, cette adresse est celle qui permet de faire de la diffusion à toutes les machines du réseau. Ainsi, quand on veut envoyer une information à toutes les machines, on utilise cette adresse.

L'adresse de diffusion ou de broadcast correspond à l'adresse IP la plus haute d'un réseau.

Exemple avec l'adresse 192.168.0.0 et le masque 255.255.255.0 ou /24

L'adresse de diffusion et 192.168.255.255 /24

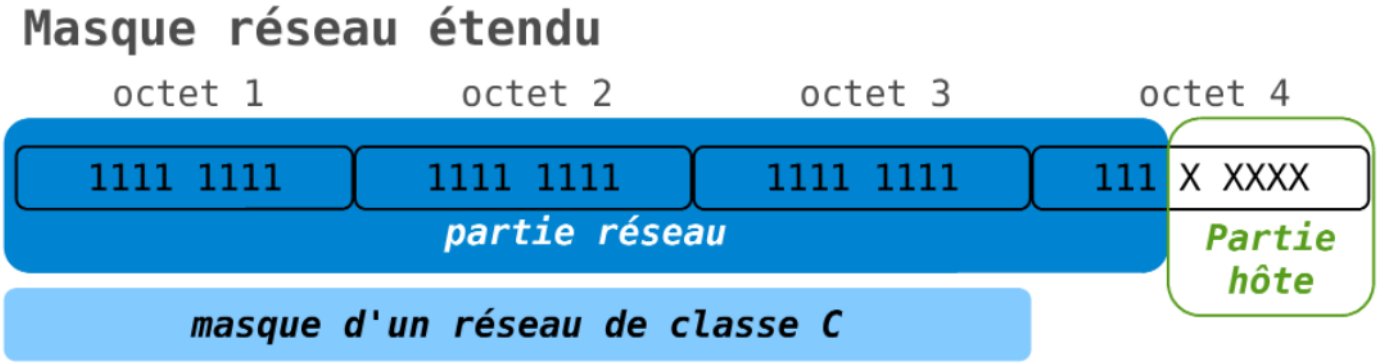
Sous-réseaux

Pour compenser les problèmes de distribution de l'espace d'adressage, la première solution utilisée consisté à découper une classe d'adresses A, B ou C en sous-réseaux. Cette technique appelée « Subnetting » a été formalisée en 1985 avec le document RFC950.

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

- Au quotidien, on évite l'engorgement des liens en limitant les annonces de services faites par les serveurs. 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 une 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.



Certaines adresses sont réservées à un usage particulier (RFC 5735[11]) :

Bloc (adresse de début et taille CIDR)	(adresse de fin correspondante)	Usage	Référence
0.0.0.0/8	0.255.255.255	*Ce réseau*	RFC 5735[11], RFC 1122[12]
10.0.0.0/8	10.255.255.255	Adresses privées[n 1]	RFC 1918[13]
100.64.0.0/10	100.127.255.255	Espace partagé pour Carrier Grade NAT	RFC 6598[14]
127.0.0.0/8	127.255.255.255	Adresses de bouclage (localhost)	RFC 1122[12]
169.254.0.0/16	169.254.255.255	Adresses de liaisons locales autoconfigurées (APIPA)	RFC 3927[15]
172.16.0.0/12	172.31.255.255	Adresses privées[n 2]	RFC 1918[13]
192.0.0.0/24	192.0.0.255	Réservé par l'IETF	RFC 5736[16]
192.0.2.0/24	192.0.2.255	Réseau de test TEST-NET-1 / documentation	RFC 5737[17]
192.88.99.0/24	192.88.99.255	6to4 anycast	RFC 3068[18]
192.168.0.0/16	192.168.255.255	Adresses privées[n 3]	RFC 1918[13]
198.18.0.0/15	198.19.255.255	Tests de performance	RFC 2544[19]
198.51.100.0/24	198.51.100.255	Réseau de test TEST-NET-2 / documentation	RFC 5737[17]
203.0.113.0/24	203.0.113.255	Réseau de test TEST-NET-3 / documentation	RFC 5737[17]
224.0.0.0/4	239.255.255.255	Multicast « Multidiffusion »	RFC 5771[20]
240.0.0.0/4	255.255.255.254 (*)	Réservé à un usage ultérieur non précisé (*sauf l'adresse ci-dessous)	RFC 1112[21]
255.255.255.255/32	255.255.255.255	broadcast limité	RFC 919[22]

Adressage : 169.254.0.0

D'après la **RFC 3927** la tranche 169.254.0.1-169.254.255.254 /16 est réservé pour le "*Link-Local*". C'est à dire pour les postes d'un réseau local qui sont dans l'incapacité de recevoir une adresse IP d'un tiers (par exemple : un serveur DHCP). Ce type d'adresse n'est pas géré par les routeurs, il n'est donc pas possible d'aller sur internet avec. Et forcément, les adresses étant de la même tranche, elles peuvent discuter entre elles.

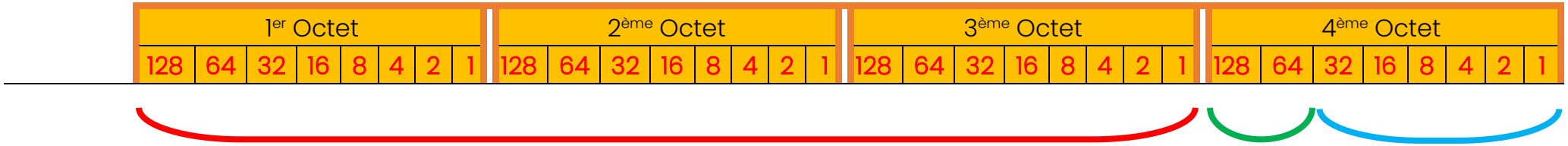
Partant de cette RFC, le système appelé **APIPA** (**A**utomatic **P**rivate **IP** **A**ddressing, Adressage automatique d'IP privée) a été créé. Il est implémenté dans tous les Windows récents et Linux. APIPA a pour rôle d'attribuer automatiquement une adresse IP en piochant des adresses dans la tranche 169.254.0.1-169.25.255.254.

Partons du réseau 192.168.1.0/24, que nous allons découper en plusieurs sous-réseaux dans le but d'accueillir entre 30 et 50 machines sur chaque sous-réseau.

Si l'on utilise le masque par défaut qui est associé à la classe C, à savoir /24, nous avons qu'un seul sous-réseau : 192.168.1.0/24.

Maintenant, si l'on change le masque et que l'on prend un masque de sous-réseau en /26 (255.255.255.192), on va découper notre réseau d'origine en sous-réseau.

Nous obtenons alors le découpage suivant avec un masque de sous-réseau avec 26 bits à 1 :



Réseau 192.168.1.0	1	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Masque sous réseau	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0

On se retrouve avec deux bits de sous-réseaux à "1" pour gérer la partie sous-réseau. Ces deux bits correspondent aux valeurs décimales 128 et 64. Le dernier bit où le masque s'arrête et le bits significatif, c'est grâce à lui qu'ont pourras trouver le réseau suivant.

En reprenant notre adresse 192.168.1.0 nous avons créer 4 sous réseaux en ajoutant 2 bits sur le dernier octet.

- 1er réseau > 192.168.1.0 à 192.168.63
- 2ème réseau > 192.168.1.64 à 192.168.1.127
- 3ème réseau > 192.168.1.128 à 192.168.1.191
- 4ème réseau > 192.168.1.192 à 192.168.1.255

Note : chaque bit ajouté nous permet de diviser le réseau en deux.

Concrètement :

1 bit = 2 réseaux, 2 bits = 4 réseaux, 3 bits = 8 réseaux …

IPV6

IPv6 (Internet Protocol version 6) est un protocole réseau sans connexion de la couche 3 du modèle OSI (Open Systems Interconnection).

Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4 (plus de 340 sextillions, ou 340.10^{36}, soit près de $7,9 \times 10^{28}$ de fois plus que le précédent).

1. Adressage IPV6

Une adresse IPv6 est longue de 128 bits, soit 8 octets, contre 32 bits / 4 octets pour IPv4. La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une écriture hexadécimale, où les 8 groupes de 2 octets (16 bits par groupe) sont séparés par un signe deux points :

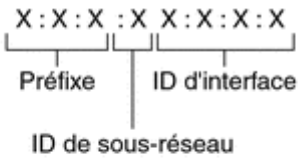
2001:0db8:0000:85a3:0000:0000:ac1f:8001

Il est permis d'omettre d'un à trois chiffres zéros non significatifs dans chaque groupe de quatre chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à la suivante :

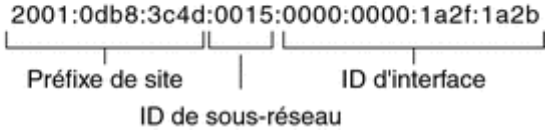
2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de 16 bits tous nuls peut être omise, en conservant toutefois les signes deux-points de chaque côté de la suite de chiffres omise, c'est-à-dire une paire de deux points « :: » (RFC 2373 et RFC 4291). Ainsi, l'adresse IPv6 ci-dessus peut être abrégée en la suivante :

2001:db8:0:85a3::ac1f:8001



Exemple :



Les réseaux sont identifiés en utilisant la notation CIDR : la première adresse du réseau est suivie par une barre oblique « / » puis par un entier compris entre 0 et 128, lequel indique la longueur en bits du préfixe du réseau, à savoir de la partie commune des adresses déterminées par ledit réseau.

Voici des exemples d'adresses réseau IPv6 avec leurs ensembles d'adresses déterminées :

- Le préfixe 2001:db8:1f89::/48 représente l'ensemble des adresses qui commence à 2001:db8:1f89:0:0:0:0:0 et finit à 2001:db8:1f89:ffff:ffff:ffff:ffff:ffff.
- Le préfixe 2000::/3 représente les adresses de 2000:0:0:0:0:0:0:0 à 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
- Le préfixe fc00::/7 représente les adresses de fc00:0:0:0:0:0:0:0 à fdff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
- Le préfixe fe80::/10 représente les adresses de fe80:0:0:0:0:0:0:0 à febf:ffff:ffff:ffff:ffff:ffff:ffff:ffff.

Certains préfixes d'adresses IPv6 jouent des rôles particuliers :

Préfixe IPv6	Description	Terme anglais	Détail	Équivalent IPv4
::1/128	Boucle Locale	Node-local Loopback	Adresse de bouclage, utilisée lorsqu'un hôte se parle à lui-même (ex : envoi de données entre 2 programmes sur cet hôte).	127.0.0.1
fe80::/10	Liaison Locale	Link-Local	Envoi individuel sur liaison locale (RFC 4291). Obligatoire et indispensable au bon fonctionnement du protocole.	169.254.0.0/16
2000::/3	Monodiffusion Mondiale	Global Unicast	Plage d'adresse publique, routable sur Internet, globalement uniques (doublon impossible) - Hors exceptions mentionnées ci-dessous.	
fc00::/7	Localement Unique	Unique Local	Plage d'adresse privée, réservée à l'utilisation sur les réseaux locaux domestiques et d'entreprises. Elles ne sont pas globalement uniques (doublon possible, réutilisées sur plusieurs réseaux IP privés).	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16
ff00::/8	Multidiffusion	Multicast	Diffusion groupée (RFC 4291)	224.0.0.0/4
2001:db8::/32	Documentation	Documentation	Plage réservée pour utilisation comme valeurs d'exemple ou dans de la documentation technique. Ne devrait jamais être utilisée sur de vrais réseaux.	192.0.2.0/24 198.51.100.0/24 203.0.113.0/24
::/128	Non spécifié	Unspecified	Utilisée comme adresse source par un hôte en cours d'acquisition de son adresse réseau.	0.0.0.0
::/8	Réservé	Reserved		

2. Binaire – Décimale – Hexadécimale

Les notations décimale, binaire ou hexadécimale sont des systèmes différents pour noter des valeurs quantitatives. Dans tous ces systèmes, la première valeur est toujours la valeur 0.

L'idée de ces systèmes de notation consiste à identifier une valeur à partir de différents « signes ». Par exemple, dans le système décimal, chaque valeur est notée avec un système à 10 « signes » qui sont 0, 1, 2, 3, 4, 5, 6, 7, 8 et 9. On utilise donc une combinaison de ces signes (ces signes sont appelés des chiffres) pour définir un nombre (qui est composé de plusieurs chiffres, donc). Dans le cas du système de notation binaire, on n'a que deux signes utilisables : 0 et 1.

Dans le système hexadécimal, on va utiliser 16 signes qui sont : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

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

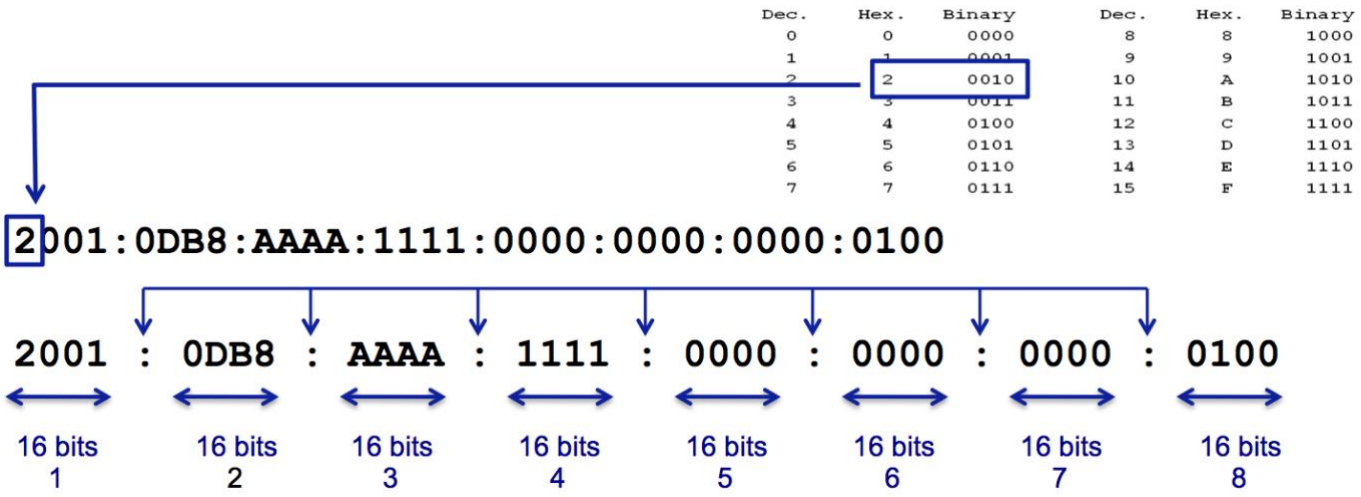
Décimale	Hexa	Binaire « 8421 »
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

On voit bien la difficulté de manipuler une adresse en notation binaire. Ce que l'on va faire pour noter une adresse IPv6, c'est grouper les bits 4 par 4 et séparer chaque groupe de 16 bits par le symbole « : » (deux points).

0010 0000 0000 0001 : 0000 1101 1011 1000 : 1010 1010 1010 1010 : 0001 0001 0001 0001 : 0000 0000 0000 0000 : 0000 0000 0000 0000 : 0000 0000 0000 0000 : 0000 0001 0000 0000

Note : les groupes de 16 bits (entre les deux points) sont parfois appelés des **hextets**.

Et maintenant, on n'a plus qu'à utiliser la notation hexadécimale pour les groupes de 4 bits que l'on a identifiés (il suffit de chercher la valeur dans la table de correspondance présentée précédemment).



L'adresse IPv6 utilisée pour notre exemple devient donc :

2001:0DB8:AAAA:1111:0000:0000:0000:0100

3. Règles IPV6

Règle n°1 : suppression des valeurs 0 inutiles

Dans toutes les notations, les symboles 0 (zéro) utilisés à gauche d'un nombre n'ont aucune utilité. Par exemple, 00127 peut se noter 127. Nous allons faire exactement la même chose sur la notation hexadécimale IPv6.

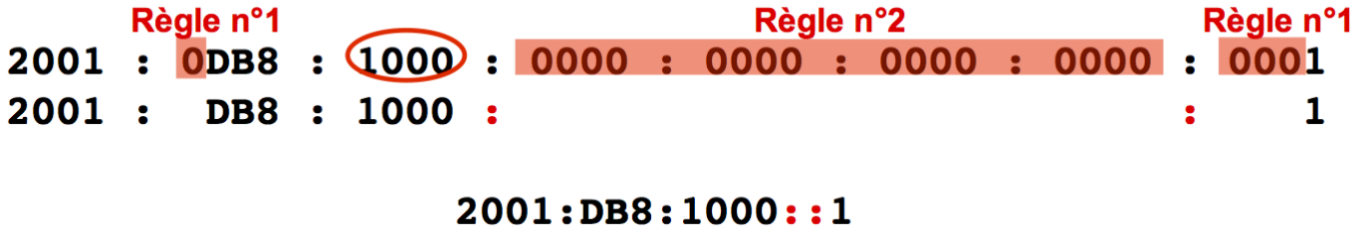
```
2001 : 0DB8 : 0001 : 1000 : 0000 : 0000 : 0ef0 : bc00
2001 :  DB8 :    1 : 1000 :    0 :    0 :  ef0 : bc00

2001 : 0DB8 : 010d : 000a : 00dd : c000 : e000 : 0001
2001 :  DB8 :  10d :    a :   dd : c000 : e000 :    1

2001 : 0DB8 : 0000 : 0000 : 0000 : 0000 : 0000 : 0500
2001 :  DB8 :    0 :    0 :    0 :    0 :    0 :  500
```

Règle n°2 : suppression d'une longue suite de 0

Cette règle consiste à remplacer un ou plusieurs groupes de :0000: par « :: » (double symbole deux points)



Attention : la notation « :: » ne peut s'utiliser qu'une seule fois dans une adresse IPv6 ; ceci afin de permettre de retrouver la notation complète sans erreur possible.

Et dans le cas de 2001:DB8:0000:0000:1234:0000:0000:0001 (les deux suites de 0 sont de même longueur) ?

La notation a privilégiée sera : 2001:DB8::1234:0000:0000:0001

Adresse MAC

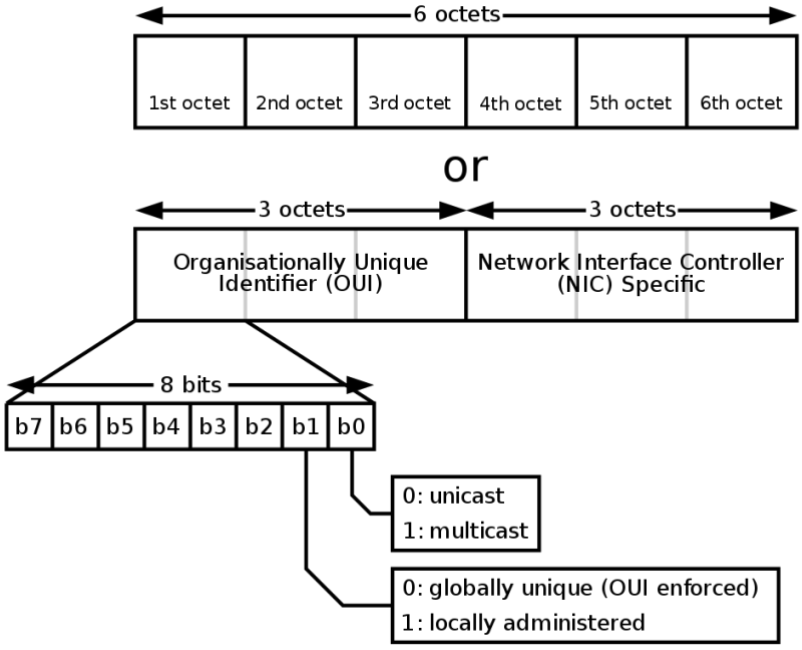
Une adresse MAC (de l'anglais Media Access Control1), parfois nommée adresse physique, est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, elle est unique au monde.

Une adresse MAC est constituée de 48 bits sur 6 octets et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point.

Par exemple : *5E:FF:56:A2:AF:15*

Ces 48 bits sont répartis de la façon suivante :

- 1 bit I/G : indique si l'adresse est individuelle, auquel cas le bit sera à 0 (pour une machine unique, unicast) ou de groupe (multicast ou broadcast), en passant le bit à 1 ;
- 1 bit U/L : 0 indique si l'adresse est universelle (conforme au format de l'IEEE) ou locale, 1 pour une adresse administrée localement ;
- 22 bits réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur ;
- 24 bits : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur).



1. Adresses MAC particulières

FF:FF:FF:FF:FF:FF	Adresse broadcast
01:00:0C:CC:CC:CC	Cisco Discovery Protocol
01:80:C2:00:00:00	Spanning Tree Protocol
33:33:xx:xx:xx:xx	Adresses multicast IPv6
01:00:5E:xx:xx:xx	Adresses multicast IPv4
00:00:0c:07:ac:xx	Adresses HSRP
00:00:5E:00:01:XX	Adresses VRRP