MOOC
Objectif IPv6 !
vers l'internet nouvelle génération

Document Compagnon[1]

Séquence 1

L'adressage

Par **- Jacques Landru** TELECOM Lille / G6

- Bruno Di Gennaro G6

Licence Creative Nommons CC BY-SA 4.0 International

Attribution - Partage dans les Mêmes Conditions 4.0 International (CC BY-SA 4.0)

Avertissement Ce résumé n'indique que certaines des dispositions clé de la licence. Ce n'est pas une licence, il n'a pas de valeur juridique. Vous devez lire attentivement tous les termes et conditions de la licence avant d'utiliser le matériel licencié.

Creative Commons n'est pas un cabinet d'avocat et n'est pas un service de conseil juridique. Distribuer, afficher et faire un lien vers le résumé ou la licence ne constitue pas une relation client-avocat ou tout autre type de relation entre vous et Creative Commons.

Clause C'est un résumé (et non pas un substitut) de la licence.

http://creativecommons.org/licenses/by-sa/4.0/legalcode

Vous êtes autorisé à :

- **Partager** — copier, distribuer et communiquer le matériel par tous moyens et sous tous formats
- **Adapter** — remixer, transformer et créer à partir du matériel
- pour toute utilisation, y compris commerciale.

L'Offrant ne peut retirer les autorisations concédées par la licence tant que vous appliquez les termes de cette licence.

Selon les conditions suivantes :

Attribution — You must give **appropriate credit**, provide a link to the license, and **indicate if changes were made**. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

Partage dans les Mêmes Conditions — Dans le cas où vous effectuez un remix, que vous transformez, ou créez à partir du matériel composant l'Oeuvre originale, vous devez diffuser l'Oeuvre modifiée dans les même conditions, c'est à dire avec **la même licence** avec laquelle l'Oeuvre originale a été diffusée.

No additional restrictions — Vous n'êtes pas autorisé à appliquer des conditions légales ou des **mesures techniques** qui restreindraient légalement autrui à utiliser l'Oeuvre dans les conditions décrites par la licence.

Notes: Vous n'êtes pas dans l'obligation de respecter la licence pour les éléments ou matériel appartenant au domaine public ou dans le cas où l'utilisation que vous souhaitez faire est couverte par une **exception.**

Aucune garantie n'est donnée. Il se peut que la licence ne vous donne pas toutes les permissions nécessaires pour votre utilisation. Par exemple, certains droits comme l**es droits moraux, le droit des données personnelles et le droit à l'image** sont susceptibles de limiter votre utilisation.

Les informations détaillées sont disponibles aux URL suivantes :

- http://creativecommons.org/licenses/by-sa/4.0/deed.fr
- http://fr.wikipedia.org/wiki/Creative_Commons

Tables des activités

Activité 11 : Qu'est ce qu'une adresse IP?

Introduction à l'adressage

Le format et la représentation des adresses sont les éléments les plus directement visibles, de la nouvelle version du protocole, pour l'utilisateur et l'administrateur réseau. La pénurie des adresses IPv4 étant l'élément qui a motivé la création d'une nouvelle version du protocole, la définition du nouveau format d'adressage a conditionné certains choix techniques pour IPv6. Bien que les principes de base soient dérivés de ceux employés en IPv4, cet adressage apparaît de prime abord plus complexe. Il est important de se familiariser avec les règles et les principes de représentation et d'attribution avant d'aborder le nouveau protocole.

Fonctions d'une adresse réseau

Dans une architecture IP, une adresse sert en fait à deux fonctions distinctes:

- L'identification: Une adresse de niveau réseau identifie de manière unique la machine parmi les «N» machines du réseau, «N» pouvant être arbitrairement grand, dans l'Internet par exemple. L'identification permet à deux interlocuteurs de se reconnaître pendant un connexion. Cette vérification est mise en oeuvre dans les pseudo entêtes d'une connexion TCP ou dans les associations de sécurité IPSec.
- La localisation: La localisation est utilisée pour décider de la remise directe ou de la recherche d'un intermédiaire qui saura délivrer les datagrammes, selon le principe du routage en saut par saut . En fait elle ne varie qu'en cas de changement de prestataire IP ou de réorganisation de site. La localisation est découpée en deux parties: localisation globale, identifiant le réseau et localisation locale distinguant les machines sur un même réseau. Ces deux niveaux de localisation auront une influence déterminante dans la structuration du format des adresses, que nous verrons ultérieurement.

Lors des études initiales IPv6, il avait été envisagé de séparer les deux fonctions pour faciliter la résolution des problèmes liés à la renumérotation, la mobilité ou la multi-domiciliation. Pour l'instant, la séparation des fonctions est encore à l'état de recherche, et les premiers plans d'adressage IPv6 continuent, comme en Ipv4, à lier les deux fonctions. De même, comme en IPv4, on considérera qu'une adresse est associée à une interface. Une machine peut posséder plusieurs interfaces. De même une interface peut supporter plusieurs adresses.

Question de taille

Une adresse IPv6 est un mot de 128 bits (16 octets). Cette taille de 128 bits semble techniquement bien adaptée aux mots manipulés par les processeurs d'aujourd'hui. Les processeurs 32 bits et 64 bits sont aujourd'hui banalisés. Le quadruplement, comparativement à la version précédente d'IP, de la longueur binaire de l'adresse fait apparaître l'adressage IPv6 comme plus ardu. Cette complexité n'est qu' apparente, elle traduit la nécessaire adaptation au changement, pour laquelle la plupart d'entre nous montrons naturellement une réticence initiale. Certes la représentation des adresses de 16 octets a nécessité l'abandon de la notation

décimale pointée pour une nouvelle notation hexadécimale (cf séquence suivante), qui est un compromis raisonnable pour la manipulation des adresses par les administrateurs réseau. Pour le commun des utilisateurs l'auto-configuration et la banalisation des services de nommage (DNS Domain Name Service) et des annuaires réseaux suppléeront, comme pour IPV4, la nécessité d'avoir à manipuler directement les adresses.

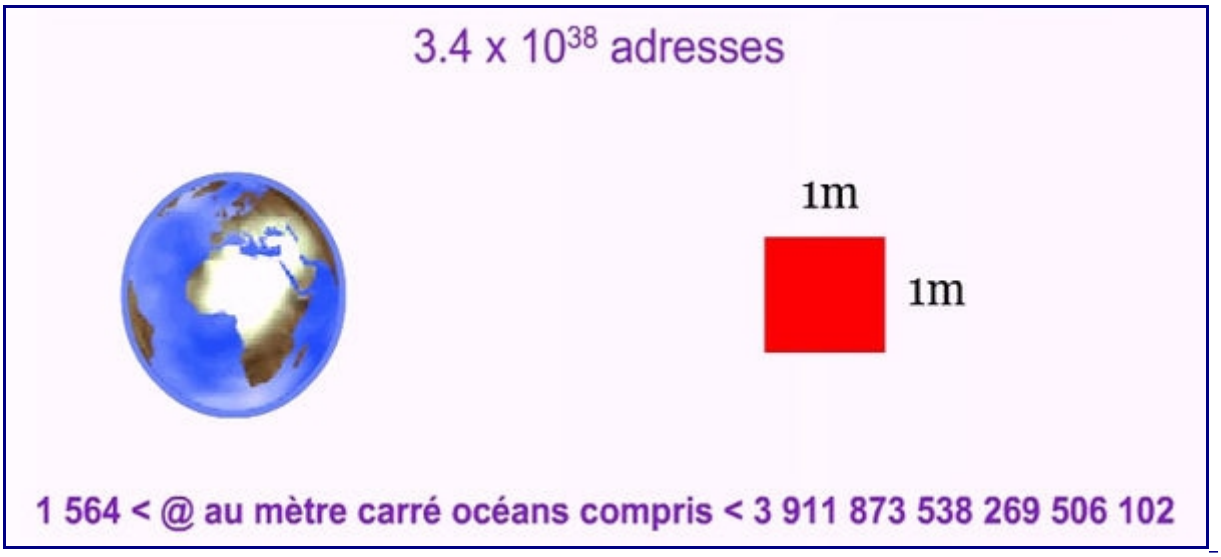
Les principes de structuration de cet adressage dérivent des techniques déjà utilisées en IPv4, à savoir une classification de divers plans d'adressage sur les parties hautes de l'adresse (c'est à dire sur les préfixes les plus courts), associée à une agrégation des tables de routage généralisant la méthode dite CIDR (Classless Inter Domain Routing) dans laquelle l'usage de divers masques de taille «élastique» permet une certaine souplesse dans la définition et l'attribution des préfixes, une optimisation de l'espace d'adressage limitant le gaspillage des larges portions d'adresses, comparativement à IPv4, ainsi qu'une optimisation du routage en facilitant sa hiérarchisation (les équipements des opérateurs de coeur de l'internet prennent leur décision de routage sur des préfixes courts, les «grandes directions», alors que les équipements de routage des opérateurs de distribution, en périphérie du réseau, routent sur des préfixes plus longs, ce qui a pour effet de contenir la taille des tables de routage de cœur du réseau dans des proportions raisonnables.

Toutefois, en IPv4, l'amélioration induite par CIDR semble limitée du fait que les adresses de 32 bits sont trop courtes pour permettre une bonne structuration et qu'il faut assumer le coût du passé où les adresses ont été allouées sans préoccupation d'organisation d'ordre hiérarchique ou géographique. Malgré ces limitations l'adressage IPv6 s'appuie de facto sur CIDR. La gestion des tables de routage, dans le cœur du réseau s'en trouvera quand même améliorée car:

- dès le début le plan d'adressage est hiérarchisé, éliminant les longs préfixes,
- les sites multi-domiciliés posséderont autant d'adresses que de fournisseurs de service,
- des mécanismes de renumérotation automatique faciliteront le changement de préfixes, lors du changement de fournisseur d'accès ou de basculement sur un nouveau plan d'adressage.

Le nombre de combinaisons possibles sur 128 bits (2 à la puissance 128) est astronomique, il dépasse les 3.4 x 10 puissance 38. Certaines estimations encadrent le nombre d'adresses disponibles par mètre carré de la surface terrestre, océans compris, entre 1 564 et 3 911 873 538 269 506 102 adresses au m2.

1 564 @ au mètre carré océans compris 3 911 873 538 269 506 102



Sans tomber dans l'optimisme béat de ces grandeurs, ni le pessimisme primitif rappelant qu'au début d'Arpanet (réseau ancêtre d'internet dans les années 1960) les 4 milliards d'adresses possibles d'IPv4 (2 puissance 32) paraissaient également une limite matériellement inaccessible; force est de constater que l'adressage IPv6 est largement dimensionné et qu'une organisation raisonnée de cet espace devrait lui offrir une certaine pérennité. Il est toutefois difficile de prévoir l'utilisation des adresses dans le futur. Ainsi, par exemple, le plan d'adressage actuellement mis en oeuvre utilise un identifiant d'équipement de 64 bits, c'est à dire la moitié de la taille de l'adresse. En fait ce genre de calcul n'est qu'un argument pour justifier l'usage de préfixes d'adresses de taille fixe, qui simplifie le traitement de l'en-tête des datagrammes.

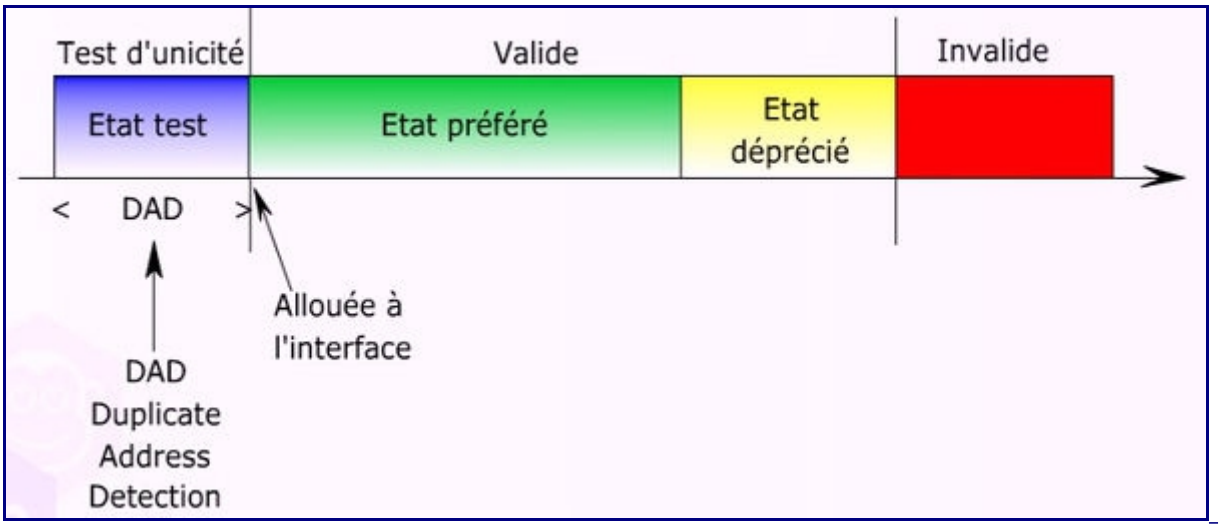
Durée de vie d'une adresse

IPv6 généralisant le plan d'adressage CIDR, les préfixes restent dans tous les cas la propriété des opérateurs. Il ne peuvent plus être attribués à vie aux équipements. Les adresses IPv6 sont donc «prêtées» aux interfaces des équipements. L'attribution d'une adresse à une interface est faite temporairement. Une durée de vie est associée à l'adresse qui indique le temps pendant lequel l'interface est dépositaire de l'adresse. Cela facilite la renumérotation des machines. Quand la durée de vie est épuisée, l'adresse devient invalide, elle est supprimée de l'interface et devient potentiellement assignable à une autre interface. Une adresse invalide ne doit jamais être utilisée comme adresse de communication. La valeur par défaut est de 30 jours, mais cette durée peut être étendue, voire portée à l'infinie (valeur réservée tous bits à 1). L'adresse lien-local a une durée de vie illimitée.

La renumérotation de l'interface d'un équipement consiste à passer d'une adresse à une autre. Lors de cette opération, il n'est pas souhaitable de changer brusquement d'adresse, sinon toutes les connexions TCP en cours, qui l'utilisent comme identificateur, seraient brutalement coupées. Ceci pourrait entraîner des perturbations applicatives. Pour faciliter cette transition, un mécanisme d'obsolescence est mis en place pour invalider progressivement une adresse. Ce mécanisme s'appuie sur la capacité d'affectation de plusieurs adresses valides à une même interface. Un état est associé à chaque adresse. Il intervient dans la sélection de l'adresse à utiliser. Cet état indique dans quelle phase de sa durée de vie une adresse se situe vis à vis de

l'interface. Une première phase consiste à vérifier l'unicité de l'adresse sur le lien à l'aide de l'algorithme de détection de duplication (DAD Duplicate Address Detection). En cas de succès de l'algorithme, l'adresse est effectivement allouée à l'interface. Durant cette phase de test l'adresse ne peut être utilisée pour communiquer (cf découverte des voisins).

Après l'allocation de l'adresse à l'interface, le premier des états est qualifié de préféré: l'utilisation de l'adresse n'est alors pas restreinte. Peu avant sont invalidation l'adresse passe dans un état dit déprécié. Son utilisation est déconseillée mais pas interdite. Elle ne doit plus être utilisée comme adresse source pour de nouvelles communications (établissement de connexions TCP par exemple). Par contre elle peut encore servir d'adresse source pour les connexions existantes. Les datagrammes reçus à une adresse dépréciées continuent à être remis normalement. A la durée de validité, il est également associé une durée de son état préféré.



Ressources complémentaires à cette activité

Le lecteur intéressé par l'état des travaux sur la séparation des fonctions d'identification et de localisation des adresses, pourra consulter les références suivantes:

- Séparation de l'identificateur et du localisateur dans Internet, Blog S.Bortzmeyer
- Création du groupe de travail IETF sur LISP, Blog S.Bortzmeyer
- RFC 7215: LISP Network Element Deployment Considerations, Blog S.Bortzmeyer

Activité 12 : La notation des adresses IPv6

Notation

IPv6 a abandonné la notation décimale pointée, en usage pour les adresses IPv4 (en 32 bits, soit 4 octets , on indique la valeur décimale de chaque octet séparée par un point décimal; exemple l'adresse IPv4 192.168.0.1). Cette notation est en effet inadaptée pour des chaînes binaires de 16 octets. IPv6 a adopté la notation hexadécimale (*) couramment utilisée dans le monde informatique pour représenter des octets par des couples de nombres hexadécimaux.

(*) Le lecteur peu familier avec le système de numération hexadécimal pourra consulter avec intérêt les ressources complémentaires indiquées à la fin de cette séquence.

Notation des adresses par l'exemple

Les 16 octets (128 bits) des l'adresse IPv6 suivante se notent en binaire:

00100000 00000001 00001101 10111000 00000000 00000000 00000000 00000000 00000000 00001000 00001000 00000000 00100000 00001100 01000001 01111010

et s'écrivent en hexadécimal (*) sous la forme suivante:

20 01 0d b8 00 00 00 00 00 08 08 00 20 0C 41 7A

couramment notés (le préfixe 0x indiquant que la chaine suivante est en notation hexadécimale).

0x20010db80000000000080800200C417A

(*) Le lecteur peu familier avec le système de numération hexadécimal pourra consulter avec intérêt les ressources complémentaires indiquées à la fin de cette séquence. La représentation textuelle des adresses IPv6 se fait en segmentant le mot de 128 bits en 8 champs de 16 bits (2 octets) séparés par le caractère :. Chacun de ces champs est transcrit en 4 chiffres hexadécimaux. L'adresse précédente se note donc:

`2001:0db8:0000:0000:0008:0800:200C:417A`

Par convention, il n'est pas nécessaire d'écrire les zéros de poids fort placés en tête de champ (dans chaque mot de 16 bits les zéros de poids fort sont non significatifs). L'adresse peut donc prendre une notation plus compacte:

`2001:db8:0:0:8:800:200C:417A`

Plusieurs champs nuls consécutifs peuvent être abrégés par l'abréviation **::** (2 caractères ':' successifs, sans espace). **Attention: Pour éviter toute ambiguïté cette abréviation ne peut être utilisée u'une seule fois par adresse!**

Exemple	l'adresse	peut également s'écrire
Une adresse unicast	`2001:0db8:0:0:0:800:200c:4`	`2001:db8::800:200`

	17a	c:417a
Une adresse multicast	ff01:0:0:0:0:0:101	ff01::101
Adresse de bouclage (loopback address)	0:0:0:0:0:0:1	**::1**
Adresse non spécifiée (unspecified address)	0:0:0:0:0:0:0	::

Notation canonique pour l'affichage

Les adresses IPv6 peuvent donc avoir plusieurs représentations valides possibles. Le RFC 5952 fournit les recommandations pour une forme de représentation canonique des adresses. Cette forme est destinée aux procédures d'affichage (par les programmes, les appels systèmes inscrivant des événements dans les fichiers journaux (logs),...). Cette recommandation ne porte donc que sur les sorties d'adresses (affichage). En entrée (configuration d'équipement, passage de paramètres ...) un logiciel devrait toujours accepter les différentes formes valide. La saisie reste donc libre. (lecture recommandée http://www.bortzmeyer.org/5952.html).

Concrètement, selon cet RFC 5992 , une adresse devrait être affichée selon la forme suivante:

- Les zéros initiaux (non significatifs) doivent être supprimés;
- L'indication d'une suite de champs nuls consécutifs «::» doit être utilisée au maximum (sur la série nulle la plus longue). En cas d'égalité on l'applique sur la première:
  - 2001:db8:0:42 **:0:0:** 1 → 2001:db8:0:42 **::** 1
  - 2001:db8 **:0:0:** 42:0:0:1 → 2001:db8 **::** 42:0:0:1
- Les chiffres hexadécimaux doivent être en minuscules;
- si le numéro de port (TCP ou UDP) doit être indiqué, l'usage de crochets encadrant l'adresse devient obligatoire (auparavant cet usage ne l'était que pour les URL).

Notation des préfixes

La notation des préfixes définie par CIDR (RFC 1519) pour IPv4 est conservée pour IPv6. Le préfixe indique le nombre de bits de poids fort de l'adresse (la partie haute de l'adresse, c'est à dire dans le sens de lecture occidentale les chiffres à gauche de l'adresse) utilisés par la fonction de routage d'un équipement pour prendre sa décision de routage (vers quelle interface de sortie il doit réémettre le datagramme, cf notion de routage du MOOC Principes des Réseaux de Données)

La notation du préfixe d'adresse se fait en séparant l'adresse, du nombre de bits du préfixe par un caractère « / » (le caractère «diviseur» du pavé numérique de votre clavier).

Adresse-ipv6/longueur-en-bits-du-préfixe

Exemple: les trois notations suivantes de préfixe sont équivalentes, car le préfixe ne concerne que les 60 bits de poids fort de l'adresse

2001:db8:24:a1a1:8:800:200C:417a/60
2001:db8:0024:a1a1:0000:0000:0000:0000/60
2001:db8:24:a1a1:0008:0800:200c:417a/60
2001:db8:24:a1a1::/60

Dans l'affichage ci dessous, les chiffres hexadécimaux portant les bits de préfixe ont été graissés pour une meilleure lisibilité:

2001:db8:24:a1a 1:8:800:200C:417A/60
2001:db8:0024:a1a 1:0000:0000:0000:0000/60
2001:db8:24:a1a 1:0008:0800:200c:417a/60
2001:db8:24:a1a 1::/60

On peut combiner l'adresse d'une interface et la longueur du préfixe réseau associé (1 er exemple ci dessus) ou ne représenter que le préfixe (dernier exemple ci dessus) lorsque l'on donne explicitement sa valeur.

Concrètement:

Le noeud d'adresse	2001:db8:24:a1a1:8:800:200C:417a
avec un préfixe de sous réseau	2001:db8:24:a1a1::/60
peut se noter	2001:db8:24:a1a1:8:800:200C:417a/60

On notera une petite difficulté de cette convention de notation pour les préfixes qui ne sont pas alignés sur une frontière de mots de 16 bits, d'octet ou de demi octet,

2001:db8:7654:3::/51
2001:db8:7654:0000::/51
2001:db8:7654:0003::/51

Notation des URL: cas de la spécification du numéro de port

Une autre difficulté provient du fait que le caractère **:** est significatif dans certains contextes. Ce qui peut créer des ambiguïtés. C'est le cas des URL où il est utilisé comme séparateur entre l'adresse et le numéro de port (les adresses de niveau transport sont des numéros de port TCP ou UDP, cf MOOC Principes des Réseaux de Données).

Exemple l'URL suivante est ambiguë: `http://2001:db8:12::1:8000/` en effet, elle peut être interprétée de deux manières:

- le service web à l'écoute sur le port http par défaut (le port TCP 80 est le port implicite d'écoute du protocole http) sur la machine d'adresse `2001:db8:12::1:8000` .
- les service web (protocole http) à l'écoute sur le port TCP 8000 de la machine d'adresse `2001:db8:12::1`

Pour lever cette ambiguïté le RFC 3896 (Uniform Resource Identifier (URI) Generic Syntax)

propose d'inclure l'adresse IPv6 entre **[ ]** (crochets ouvrant et fermant).

Ainsi

- dans le premier cas l'URL serait `http://[2001:db8:12::1:8000]/`
- et dans le second `http://[2001:db8:12::1]:8000/`

Vadémécum de notation hexadécimale

Cet aide mémoire, librement inspiré de l' **article "Systéme hexadécimal" de Wikipedia, est destiné à l'accompagnement des auditeurs qui ne sont pas familiers avec cette notation concise des nombres binaires.**

Le système hexadécimal est un système de numération en base 16. Il utilise ainsi 16 symboles, en général les chiffres arabes pour les dix premiers chiffres et les lettres **"a"** à **"f"** pour les six suivants (en majuscules ou en minuscules, sans importance en principe, mais il vaut mieux par cohérence adopter l'un ou l'autre pour la notation). Ce système est couramment utilisé en informatique et en électronique numérique pour représenter des codes binaires utilisés par les ordinateurs, car il est

- commode: conversion facile binaire = hexadécimal du fait que 16 (nombre de chiffres dans la base hexadécimale) est lui-même une puissance de 2 (nombre de chiffres de la base binaire),
- facilement lisible par les opérateurs humains, car compact (il réduit le nombre de signes d'un facteur 4 par rapport au binaire). L'unité d'information couramment utilisée en informatique, à savoir l'octet (8bits), se note ainsi sous forme de 2 chiffres hexadécimaux.

La conversion de binaire en hexadécimal se fait en regroupant les chiffres binaires (les bits) par groupe de quatre également appelé "quartet" (ou nibble). Le mot binaire doit donc avoir une longueur multiple de quatre, au besoin, on le compléte par des zéros à gauche (0 de poids fort non significatifs). A chacune des 16 combinaisons binaires d'un quartet (2 puissance 4 = 16 décimal) correspond un chiffre hexadécimal.

binaire	Hexadécimal	décimal
0 0 0 0	**0**	0
0 0 0 1	**1**	1
0 0 1 0	**2**	2
0 0 1 1	**3**	3
0 1 0 0	**4**	4
0 1 0 1	**5**	5
0 1 1 0	**6**	6
0 1 1 1	**7**	7
1 0 0 0	**8**	8
1 0 0 1	**9**	9
1 0 1 0	**a**	10
1 0 1 1	**b**	11
1 1 0 0	**c**	12

1 1 0 1	**d**	13
1 1 1 0	**e**	14
1 1 1 1	**f**	15

Conversion

Ainsi le nombre binaire suivant 0010101011010101 composé de 4 quartets (nibbles) 0010 1010 1101 0101 se note 2ad5 en hexadécimal (0010 = **2** , 1010 = **a** , 1101 = **d** , 0101 = **5**).

Inversement le nombre hexadécimal 7c8f20 se traduit par la chaîne binaire 0111 1100 1000 1111 0010 0000 (**7** = 0111, **c** = 1100, **8** = 1000, **f** = 1111, **2** = 0010, **0** = 0000) et correspond au code binaire 011111001000111100100000.

Notation

Des notations sont utilisées, notamment dans les langages informatiques, pour différencier sans ambiguité les chiffres hexadécimaux des autres:

- notation préfixée: 0x123 (langage C et dérivés), h123 (BASIC), $123 (en Pascal, et dérivés comme le VHDL en électronique), mais aussi #123 (Common Lisp), 0h123 (Texas Instrument) ou X'123' (COBOL)
- notation suffixée: 123h, 123 **(16)** (arithmétique)

(nota: pour l'anecdote: Le chanteur et humoriste Boby Lapointe a inventé en 1968 un système de représentation hexadécimale, appelé système bibi-binaire à la fois drôle et cohérent, basé sur des symboles graphiques convenus en lieu et place des chiffres arabes et lettres (de 'a' à 'f').

quelques pointeurs pour aller plus loin

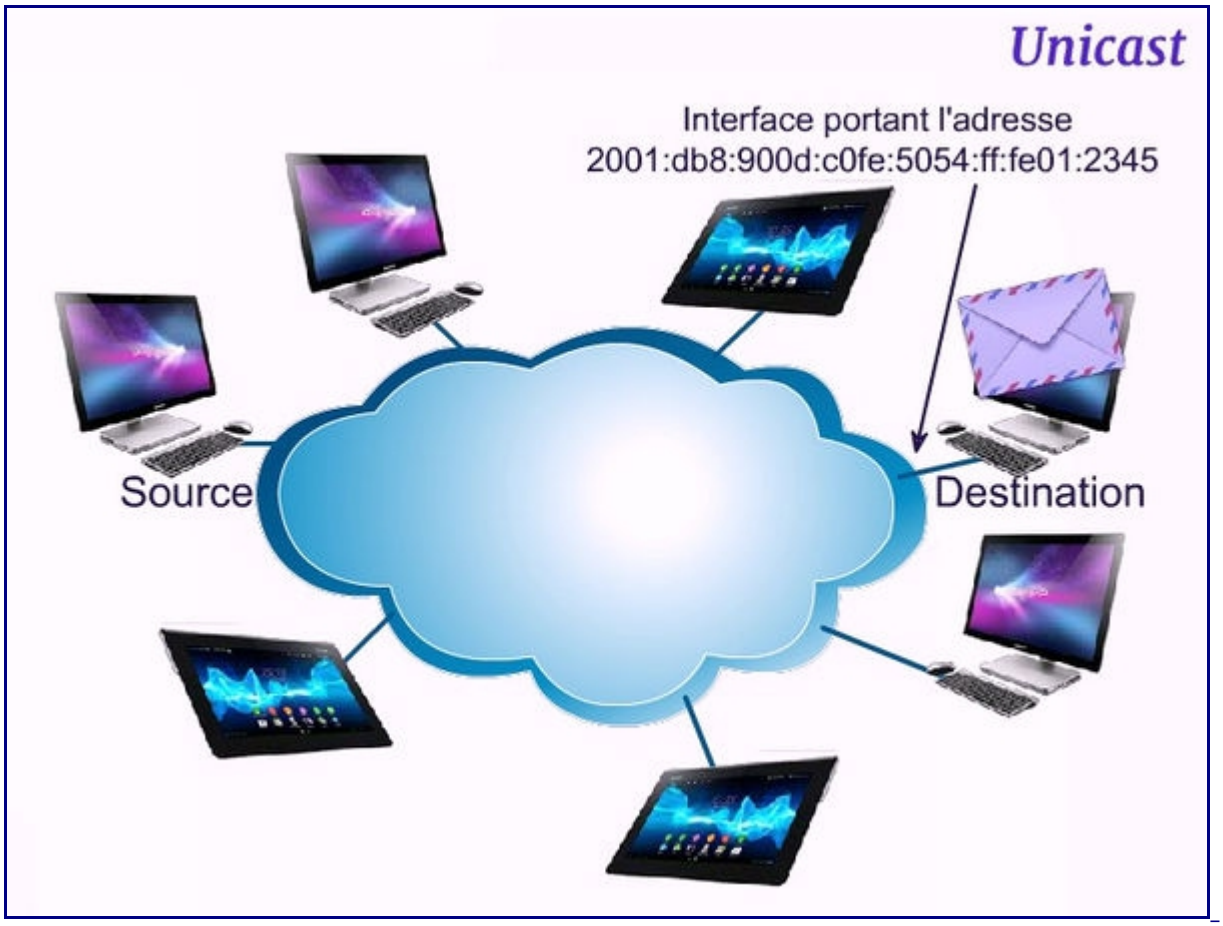
- Le système hexadécimal https://fr.wikipedia.org/wiki/Syst%C3%A8me_hexad%C3%A9cimal
- Le système bibi-binaire https://fr.wikipedia.org/wiki/Syst%C3%A8me_Bibi-binaire
- Nibble https://fr.wikipedia.org/wiki/Nibble
- Une autre forme, moins courante, de représentation des codes binaires: le système octal http://fr.wikipedia.org/wiki/Syst%C3%A8me_octal
- ...

Activité 13 : Les adresses unicast

Types d'adresses

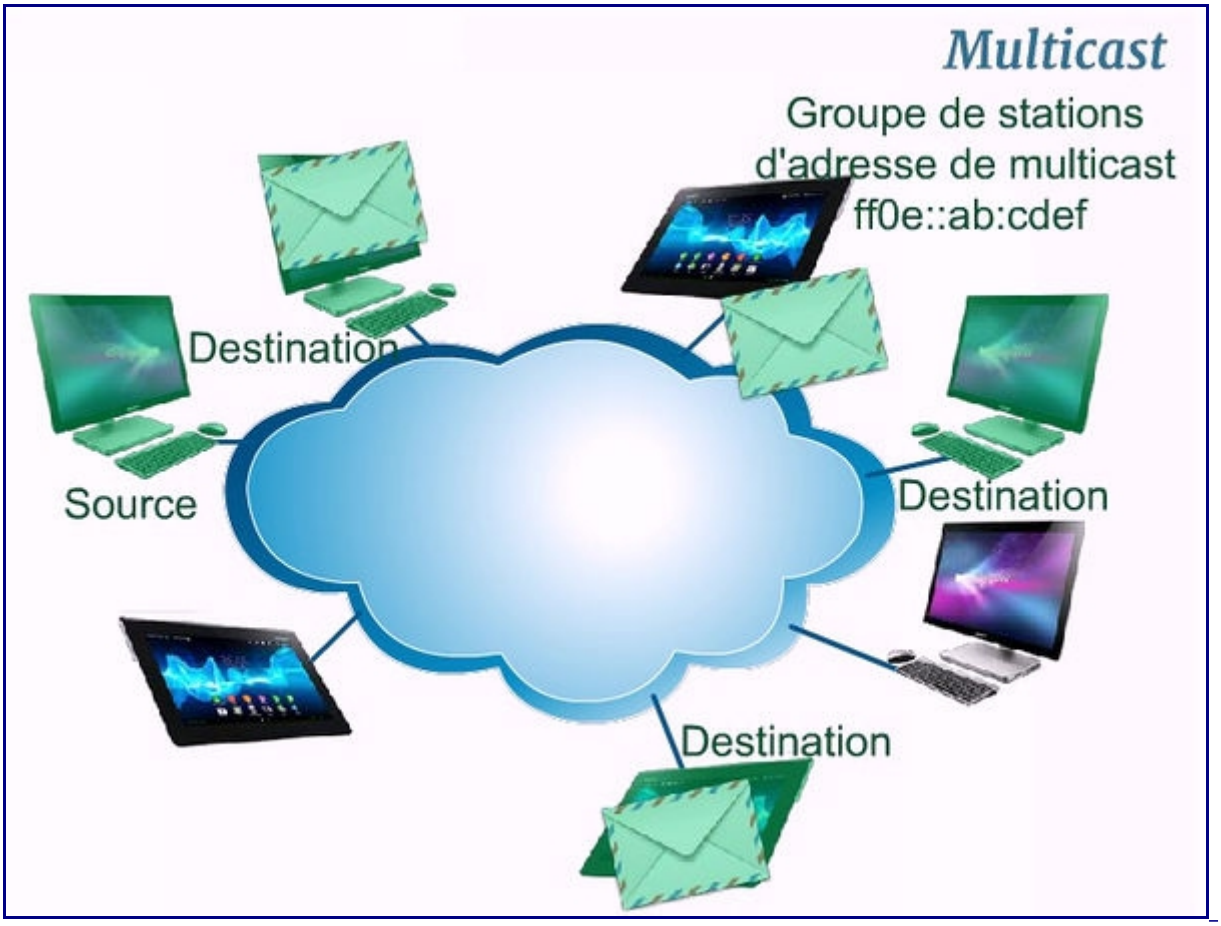
IPv6 définit trois types d'adresses: unicast, multicast, anycast.

- Le type **unicast** est le plus simple et désigne une interface unique. Le datagramme sera remis à l'interface identifiée de manière unique par son adresse. La portée d'une adresse unicast peut être
    - globale: unicité de l'identifiant sur l'ensemble de l'Internet (Global Unicast)
    - localement restreinte,: unicité de l'identifiant étendue à un espace privatif limité à un site ou un campus (Unicast Local)
    - restreinte à un lien ou domaine de diffusion de type VLAN (Link-Local Unicast).Une adresse de portée locale (site ou lien) ne sera pas routée sur l'internet.



- Une adresse de type **multicast** désigne un groupe d'interfaces appartenant à différents nœuds pouvant être situés n'importe où sur le réseau. Lorsqu'un datagramme a pour adresse de destination une adresse de multicast, il est acheminé par le réseau à toutes les interfaces appartenant au groupe. IPv6 ne dispose pas d'adresse spécifique de

diffusion générale (broadcast) au sens reconnu par IPv4, où le datagramme et reçu par toutes les interfaces du réseau ou du sous réseau et non pas toutes les interfaces de l'interconnexion. Le broadcast IPv4 est toujours restreint (confiné) à un réseau ou sous réseau. En IPv4 le broadcast est général et toutes les interfaces sont à l'écoute. En IPv6 la diffusion est beaucoup plus sélective, on peut s'adresser uniquement aux routeurs ou aux serveurs DHCP par exemple. Au niveau local (lien ou site) un groupe IPv6 permet de s'adresser à l'ensemble des interfaces, offrant par là la même fonction que le broadcast restreint d'IPv4.



- Une adresse de type **anycast** officialise la proposition faite pour IPv4 dans le RFC 1546 . Comme pour le multicast, une adresse anycast désigne un groupe d'interfaces. La différence est que le réseau va remettre le datagramme anycast à un membre du groupe et non pas à tous comme pour le multicast. La sélection du membre qui réceptionnera le datagramme est à la charge du réseau. Cela peut être le plus proche au sens du routage (nombre de sauts, RTD minimal…). Ce type d'adressage est encore l'objet de recherches, et reste pour l'instant essentiellement expérimental.

Identification des types d'adresses

Le type d'une adresse IPv6 est identifié par ses bits de poids fort.

Type	Préfixe binaire d'identification	Notation IPv6
Non spécifié	`00...0`	`::/128`
Adresse de bouclage (Loopback)	`00...1`	`::1/128`
Multicast	`1111 1111`	`ff00::/8`
Unicast lien local	`1111 1110 10`	`fe80::/10`
Unique Local unicat Address (ULA)	`1111 1101`	`fd00::/8`
Unicast globale (Plan d'adressage unicast global agrégé actuellement déployé)	`001`	`2000::/3` (soit toute adresse commençant par 2 ou 3)

Certains types d'adresses sont caractérisés par leur préfixe RFC 3513 . Le tableau suivant donne la liste de ces préfixes. La plage «réservée» du préfixe `0::/8` est utilisée pour les adresses spéciales (adresse indéterminée, de bouclage, mappée, compatible). On notera que

plus de 70% de l'espace disponible n'a pas été alloué, ce qui permet de conserver toute latitude pour l'avenir.

Préfixe IPv6	Allouer	Référence
0000::/8	Réservé pour la transition et loopback	RFC 3513
0100::/8	Réservé	RFC 3513
0200::/7	Réservé (ex NSAP)	RFC 4048
0400::/6	Réservé (ex IPX)	RFC 3513
0800::/5	Réservé	RFC 3513
1000::/4	Réservé	RFC 3513
2000::/3	Unicast Global	RFC 3513
4000::/3	Réservé	RFC 3513
6000::/3	Réservé	RFC 3513
8000::/3	Réservé	RFC 3513
a000::/3	Réservé	RFC 3513
c000::/3	Réservé	RFC 3513
E000::/4	Réservé	RFC 3513
f000::/5	Réservé	RFC 3513
F800::/6	Réservé	RFC 3513
fc00::/7	Unique Local Unicast	RFC 4193
fe00::/9	Réservé	RFC 3513
fe80::/10	Lien-local	RFC 3513
fec0::/10	Réservé	RFC 3879
ff00::/8	Multicast	RFC 3513

Une interface possèdera généralement plusieurs adresses IPv6. En IPv4 ce comportement est exceptionnel, il est banalisé en IPv6.

Les adresses anycast ne sont pas distinguées des adresses unicast de quelque portée (globale, locale, lien) que ce soit.

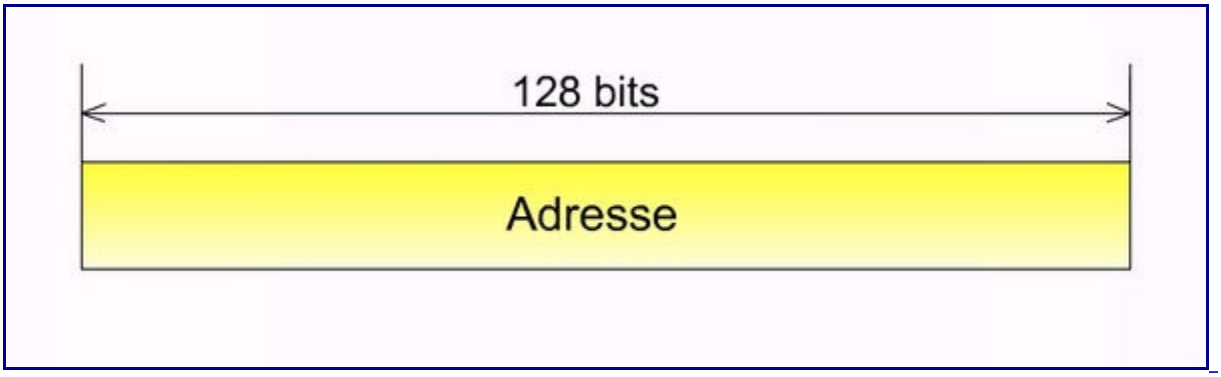
Structure de l'adresse unicast

Le plan d'adressage agrégé actuellement en vigueur est défini dans le RFC 3587 . Il s'inspire des recommandations de la politique d'allocation d'adresse des autorités régionales (RIR Régional Internet Registry), définie dans le documents ripe-267 et de le RFC 3177 qui est un

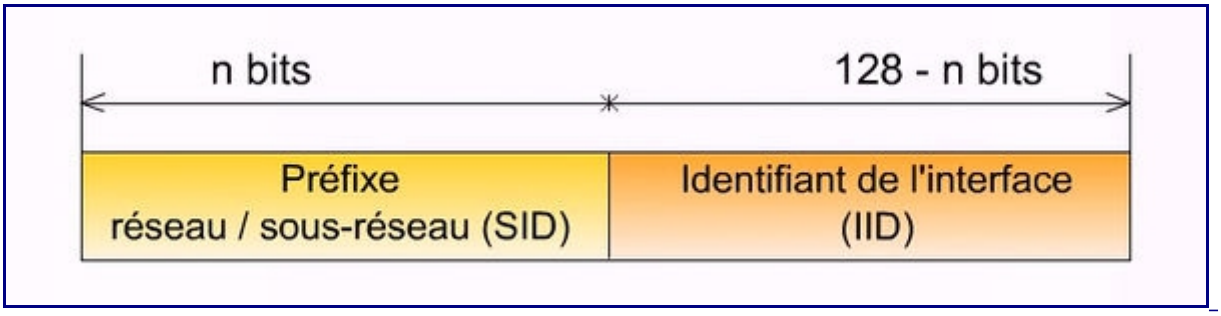
plaidoyer pour un préfixe de taille fixe de 48 bits.

Les adresses IPv6 peuvent être agrégées avec des préfixes de longueur quelconque, de manière similaire aux mécanismes mis en oeuvre dans les architectures CIDR (Classeless InterDomain Routing) d'IPv4.

Un noeud peut avoir une connaissance minimale de la structuration interne de l'adresse, en fonction de son rôle dans l'interconnexion. Un hôte ou un routeur n'a ainsi pas la même vision de la structure de l'adresse. Au minimum un noeud peut considérer l'adresse unicast comme un simple mot binaire de 128 bits sans aucune structure particulière.



Un premier niveau de hiérarchisation découpe l'adresse en deux parties logiques, un préfixe réseau/sous-réseau, qui sera utilisé pour acheminer le datagramme à travers le réseau, et un identifiant d'interface qui sera utilisé sur le dernier saut pour remettre le datagramme à l'interface de destination.



Différents types d'adresse unicast

L'adresse non spécifiée

L'adresse `0:0:0:0:0:0:0:0` ou `::/128` est définie comme l'adresse non spécifiée. Elle ne doit jamais être affectée à un noeud. Elle indique l'absence d'adresse. Elle est utilisée comme adresse source par les paquets d'initialisation lors de l'auto-configuration d'une station. Elle ne doit jamais être utilisée comme adresse de destination d'un paquet.

L'adresse de bouclage (loopback)

l'adresse unicast `0:0:0:0:0:0:0:1` ou `::1/128` est appelée adresse de bouclage (loopback) et correspond à l'adresse 127.0.0.1 d'IPv4. Elle est utilisée par un noeud pour s'envoyer des paquets à lui même. Elle ne doit jamais être affectée à une interface. Elle est

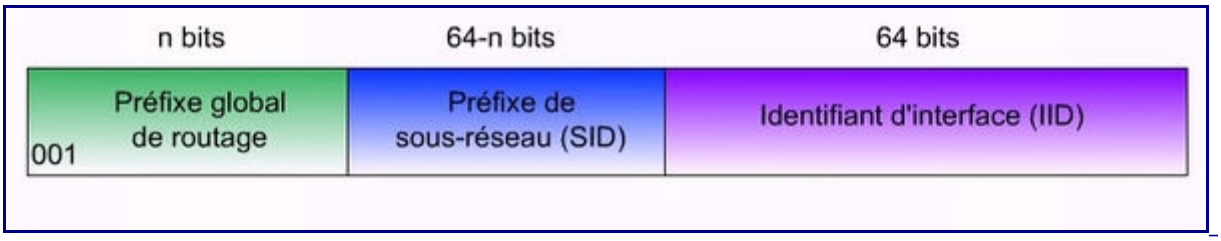
considérée comme ayant une étendue de type lien local et doit être vue comme une adresse unicast de lien local de l'interface virtuelle de bouclage (loopback interface). Elle ne doit jamais être utilisée comme adresse source, ou destination d'un paquet circulant sur le réseau, ou plus exactement un paquet circulant hors de la machine. Un paquet reçu sur une interface avec telle adresse de destination doit être détruit.

Les adresses unicast globales

Il s'agit des adresses globalement routables sur l'Internet V6, elles sont communément qualifiées «d'adresses publiques». Les adresses unicast globales sont issues du plan d'adressage agrégé, proposée dans le RFC 3587 . Elles sont identifiées par le préfixe binaire `0b0010` , soit `2000::/3` en notation IPv6; toute adresse IPv6 commençant 2xxx:: ou 3xxx:: est donc une adresse unicast globale.

Le RFC 3587 définit la structure d'adressage IPv6 définie dans le RFC 3513 en précisant les tailles de chacun des blocs. Il est géré hiérarchiquement de la même manière que CIDR en IPv4. Une adresse intègre trois niveaux de hiérarchie:

- une topologie publique (appelée Global Prefix) codée sur 48 bits, allouée par le fournisseur d'accès;
- une topologie de site codée sur 16 bits (appelée Subnet ID). Ce champ permet de coder les numéros de sous réseau du site;
- un identifiant d'interface sur 64 bits (appelé Interface ID) distinguant les différentes machines sur le lien.



A part le préfixe `2002::/16` qui est réservé au mécanisme de transition 6to4, cet espace est géré hiérarchiquement comme pour IPv4. L'IANA délègue aux 5 autorités régionales (RIR) des préfixes actuellement de longueur 12 [1] qui les redistribuent aux ISP de leur région. Suivant leur taille, les opérateurs reçoivent un préfixe plus ou moins long.

Il est maintenant admis que le préfixe attribué par un opérateur à ses clients peut également être un /56. En effet, si l'on garde l'attribution de préfixe de longueur 48 pour les sites terminaux, et que l'on intègre les réseaux domotiques, les opérateurs peuvent justifier d'un besoin important d'adresses que les autorités régionales ne peuvent leur refuser.

Nota: quelques préfixes du plan d'adressage agrégé du RFC 3587 ont un usage réservé.

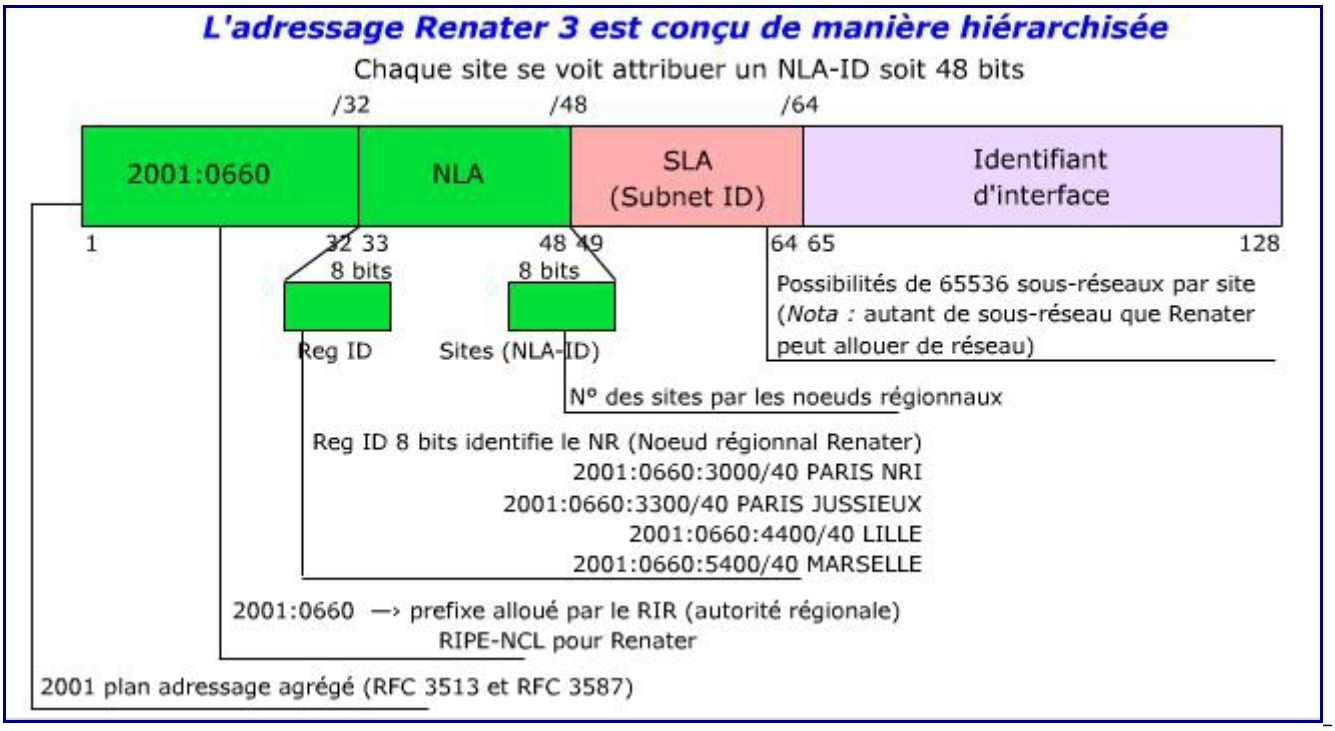
- préfixe `2002::/16` qui est est réservé au mécanisme de transition 6to4;
- préfixe `2001:db8::/32` est réservé pour la documentation. Ces adresses ne sont théoriquement pas routés par les opérateurs sur l'Internet public;
- préfixe `3ffe::/16` était le préfixe des adresses du réseau expérimental 6bone qui a

symboliquement été stoppé le 6 juin 2006 (06/06/06). ces adresses sont donc aujourd'hui dépréciées.

Le plan agrégé `2000::/3` , a été découpé en plusieurs plages d'adresses qui sont allouées par l'IANA aux différents RIR (Registres Internet Régionaux). Les RIR gèrent les ressources d'adressage IPv4 et IPv6 dans leur région (au niveau mondial). L'IANA alloue des blocs de taille /23 à /12 dans l'espace unicast global (`2000::/3`) aux cinq RIR. Ces derniers les allouent à leur tour aux LIR (fournisseur d'accès à internet) sous forme de blocs de taille minimale de /48. Les RIR peuvent choisir de subdiviser leur bloc /23 en 512 blocs /32, typiquement un par LIR. Le LIR peut à son tour assigner 65536 blocs /48 à ses clients, qui disposent alors chacun de 65536 réseaux /64.

La plage `2001::/16` du plan 0x2::/3 (001) avait été initialement attribuée pour l'adressage agrégé des RIR (Regional Internet Register). Cette plage a ensuite été étendue au fur et à mesure des besoins. La version actualisée du découpage du plan d'adressage agrégé est disponible auprès de l'IANA [1] .

Exemple concret le plan d'adressage IPv6 de Renater (le réseau national de l'enseignement et de la recherches, fournisseur d'accès de l'enseignement supérieur français):



Les adresses unicast locales

Il y a deux types d'adresse unicast qui sont utilisées localement.

- Les adresses locales de lien, dites «lien local» (Link Local Address), sont utilisées sur un lien ou sur un même domaine de diffusion de niveau 2 (domaine de «broadcast», c'est à dire VLAN);
- les adresses unicast locales uniques (ULA Unique Local unicast Address) sont restreintes à un site unique (analogues aux adresses privées IPv4 de le RFC 1918).

Elles sont couramment appelées adresses privées (à l'inverse des adresses unicast globales dites publiques). Elles sont routables à l'intérieur d'un espace privatif (réseau local de campus, réseau d'entreprise, réseau domestique, ...) mais ne peuvent pas en sortir. Elles sont filtrées par les fournisseurs d'accès et ne peuvent donc pas être routées sur l'Internet public.

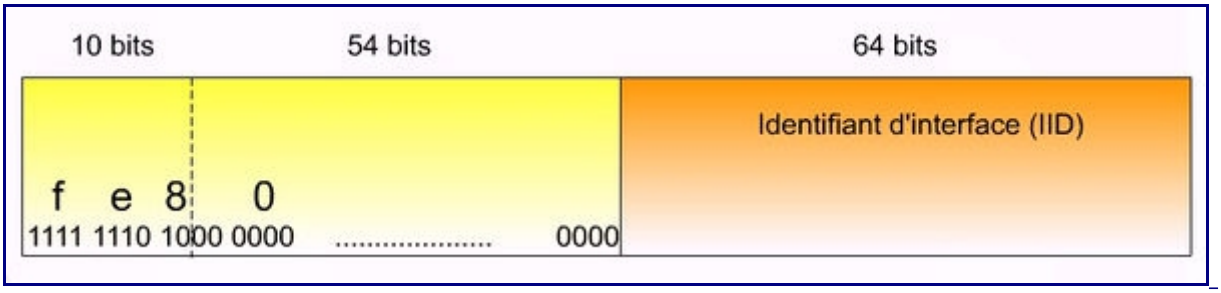
Les adresses locales de lien (link local address fe80::/64)

Les adresses lien-local, sont des adresses dont l'étendue de validité est restreinte au lien ou au domaine de diffusion de niveau 2 (domaine de broadcast, VLAN), c'est à dire l'ensemble des interfaces directement connectées (voisines et visibles entre elles) sans routeur intermédiaire: par exemple les deux extrémités d'une liaison PPP ou d'un tunnel, ou les machines connectées sur un même domaine de diffusion ethernet (VLAN Ethernet). Les adresses lien-local sont automatiquement configurées à l'initialisation de l'interface et permettent la communication entre nœuds voisins. Elles sont utilisées par les protocoles de configuration d'adresse globale, de découverte de voisins et de découverte de routeurs. Elles doivent être uniques sur leur étendue, un protocole de détection de duplication d'adresse permet de s'en assurer. Par contre la duplication d'une adresse lien-local entre deux liens différents est autorisée.

Ces adresses sont "non routables"; ainsi un routeur ne doit en aucun cas retransmettre un paquet ayant pour adresse source ou destination une adresse de type lien-local.

La portée restreinte de ces adresses les limite, dans la pratique, à un usage de démarrage automatique (boostrap) et aux mécanismes de configuration automatique. Leur usage ne devrait pas être généralisé dans les applications.

Le préfixe d'identification est `fe80::/10` . L'adresse lien-local a le format suivant: préfixe `fe80::/64` accolé au 64 bits de l'identifiant d'interface, généralement dérivée de l'adresse MAC de l'interface ethernet. Cela ne pose pas de problème de respect de le vie privée car, contrairement aux adresses globales, les adresses lien-local ne sortent jamais du réseau où elles sont utilisées.



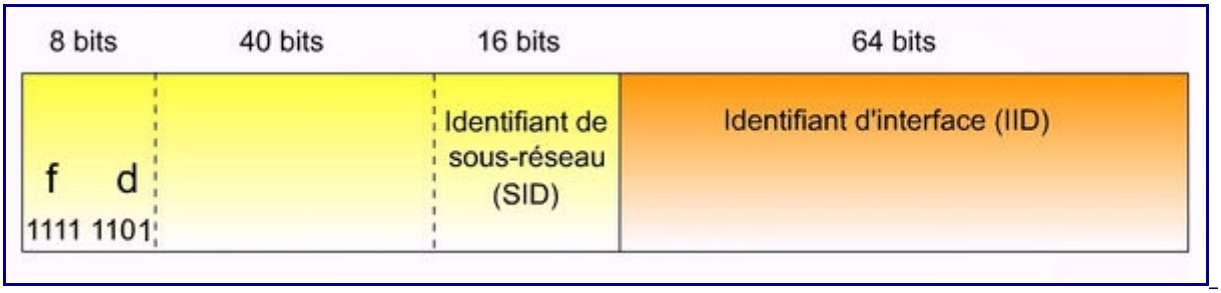
Nota: *Une adresse lien-local (ou multicast) n'indique pas intrinsèquement l'interface de sortie, puisque toutes les interfaces partagent le même préfixe fe80::/10. Il faut donc indiquer de manière explicite sur quelle* interface doivent être émis les paquets. Sur certains systèmes d'exploitation (BSD, Mac OS, Windows), il est possible de la spécifier en ajoutant à la fin de l'adresse le nom de l'interface voulue, précédé du caractère %. Sous Linux, un argument de commande réseau, généralement -I permet de la désigner.

Les adresses locales uniques (Unique Local unicast Addresse, ULA fc00::/7)

Le RFC 4193 définit un nouveau format d'adresse unicast: les adresses uniques locales (ULA: *Unique Local Address*). Ces adresses sont destinées à une utilisation locale. Elles ne sont pas définies pour être routées dans l'Internet public, mais seulement au sein d'une zone limitée (topologie privative) telle qu'un site ou entre un nombre limité de sites. La longueur du préfixe étant de 48 bits, elles peuvent se manipuler comme des adresses globales, avec un identifiant de sous-réseau (SID) sur 16 bits et un identifiant d'interface (IID) sur 64 bits.

Les adresses uniques locales sont créées en utilisant un identifiant global généré pseudo-aléatoirement, selon l'algorithme défini dans le RFC 4193 . Ces adresses suivent le format suivant:

- Prefix (7 bits): `fc00::/7` préfixe identifiant les adresses IPv6 locales (ULA);
- L (1 bit): Positionné à 1, le préfixe est assigné localement. La valeur 0 est réservée pour une utilisation future; (dans la pratique les adresses ULA en usage actuellement sont donc identifiées par le préfixe `fd00::/8`);
- Global ID (40 bits): Identifiant global utilisé pour la création d'un préfixe unique (Globally Unique Prefix);
- Subnet ID (16 bits): Identifiant d'un sous réseau à l'intérieur du site;
- Interface ID (64 bits): L'indentifiant d'interface tel que défini dans Identifiant d'interface.



Ce type d'adresse permet d'isoler la numérotation externe et interne. En IPv4, l'utilisation d'un préfixe privé issu du RFC 1918 (comme `10.0.0.0/8`) évite à un site de renuméroter son réseau s'il change de fournisseur d'accès. Un NAT (que nous appellerons NAT44 dans la suite de ce document) permet de passer de l'adressage privé vers l'adressage public.

Avec les adresses de type ULA, il est possible de reproduire ce comportement en IPv6. Un dispositif en bordure de réseau va convertir le préfixe privé en préfixe public. Cet équipement, initialement appelé NAT66 a été renommé NPTv6 (*Network Prefix Translation*) car il ne possède pas les mêmes limitations que le NAT d'IPv4 du fait qu'il n'intervient pas au niveau de la couche de transport.

Comme pour le RFC 1918 d'IPv4, l'objectif est de permettre un adressage à usage privatif non routé sur l'infrastructure publique. Mais à la différence du RFC 1918 , où le risque de collision élevé est problématique en cas de connexion de deux sites utilisant ces adresses (lors de fusions d'entreprises par exemple), il s'agit de générer des préfixes quasi uniques. Dans un espace réservé, `fc00::/7` , le site qui souhaite des adresses quasi uniques tire un préfixe de 48 bits au hasard, suivant l'algorithme décrit dans le RFC 4193 en se basant sur l'heure

courante et une adresse MAC d'une de ses interfaces. La probabilité de collision est donc très faible, vue la taile de l'espace d'adressage d'IPv6.

Ces adresses sont dites locales et ne doivent pas être routées sur l'Internet global. Elles sont routables sur un espace limité tel un site, elles peuvent également être routées entre un nombre limité de sites (sur la même aire interne d'un IGP comme OSPF, ou au travers de tunnels point à point reliant les sites). Elles ont les caractéristiques suivantes:

- préfixe globalement unique (très forte probabilité d'unicité);
- un préfixe bien connu `fc00::/7` facilitant le filtrage aux frontières du sites;
- limitation des conflits ou des opérations de réadressage lors de la fusion de sites où l'interconnexion privée de sites;
- indépendance des préfixes vis à vis des fournisseurs d'accès ou des opérateurs;
- indépendance vis à vis des applications, elles s'utilisent de la même manière que les adresses unicast globales;
- en cas de débordement géographique accidentel (mauvaise configuration de l'annonce des routeurs ou des filtres, affichage accidentel dans un DNS public) l'unicité garantit l'absence de conflit avec d'autres adresses.

L'identifiant global de 40 bits ne doit pas être choisi de manière séquentielle ou selon un algorithme permettant de déduire un préfixe en fonction des autres préfixes du site. Il ne doit pas, non plus être choisi par facilité mnémotechnique en «hexspeak» (amusement consistant a générer des jeux de mots pour les codes hexadécimaux en mixant les lettres héxadécimales [a..f] et le chiffres les chiffres 1 (pour 'i' ou 'l') 0(pour 'o') 5(pour 's') 6 ou 9 (pour 'g') 7 (pour 't'). Les plus connus étant 'bad:f00d:' «bad food», '600d:cafe' «good cafe», 'dead:beef' «dead beef», ou encore 'defe:ca7e:d «...» et bien d'autres (source http://en.wikipedia.org/wiki/Hexspeak)

Le préfixe de l'adresse IPv6 locale unique est créée en s'appuyant sur un mécanisme pseudo aléatoire. Le RFC 4193 propose l'algorithme suivant.

1. Prendre l'heure courante dans le format 64 bits du protocole NTP;
2. prendre un identifiant EUI-64, au besoin dérivé de l'adresse MAC, de l'une des interfaces de l'équipement générant le préfixe;
3. concaténer l'heure et l'identifiant d'interface pour créer une clé;
4. calculer l'empreinte SHA-1 (digest) de 160 bits de cette clé;
5. prendre les 40 bits de poids faible de l'empreinte comme identifiant global de 40 bits;
6. préfixer l'identifiant global avec le préfixe fc00::/7, et positionner le bit L (8 ième bit de poids fort) à 1. dans la pratique les préfixes ULA débutent donc par «fd».

Le script, sous licence libre GPL, développé par Hartmut Goebel, disponible à l'URL http://forschung.goebel-consult.de/ipv6/createLULA.py , peut vous générer une série de préfixes conforme en utilisant une des adresses MAC ethernet de votre poste de travail.

Ces préfixes ne devraient pas pouvoir être agrégés. Afin de renforcer la non «routabilité» globale sur l'Internet. Par défaut, l'étendue de ces adresses est globale. Ce qui signifie qu'elles ne souffrent pas de l'ambiguité lévée par l'adresse site-local (qu'est ce qu'un site?). La limite de «routabilité» est fixée au site et à toutes les routes explicitement définies avec d'autres sites

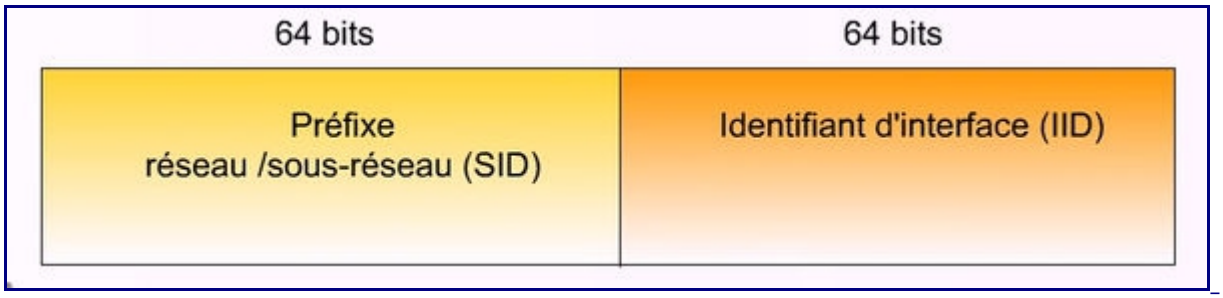
privés (soit dans la même aire d'IGP, soit au travers de tunnels). Pour les protocoles de routage extérieur (EGP *Exterior Gateway Protocol'), tel BGP, mis en oeuvre par les fournisseurs d'accès, la consigne est d'ignorer la réception et l'annonce de préfixes* `fc00::/7` .

Références bibliographiques

1. ↑ 1.0 1.1 IANA. IPv6 Global Unicast Address Assignments

Activité 14 : L'utilisation des adresses sur une interface réseau

Lors de l'activité précédente nous avons vu que les adresses unicast sont construites hiérachiquement. Un premier niveau de hiérarchisation découpe l'adresse en deux parties logiques, un préfixe réseau/sous-réseau, qui sera utilisé pour acheminer le datagramme à travers le réseau, et un identifiant d'interface qui sera utilisé sur le dernier saut pour remettre le datagramme à l'interface de destination.



Identifiant d'interface

Les identifiants d'interface des adresses unicast sont utilisés pour identifier de manière unique les interfaces des équipements sur un lien ou un domaine de diffusion de niveau 2 (VLAN). Ils doivent absolument être uniques pour le domaine couvert par un sous réseau. Toutefois l'unicité d'un identifiant d'interface peut être de portée beaucoup plus large, voire globale, à l'image des adresses MAC dont l'unicité est mondiale. Dans certains cas, l'identifiant d'interface sera dérivé directement de l'adresse de niveau liaison de données (adresse MAC de la carte ethernet par exemple).

Pour les adresses unicast, à l'exception des adresses non spécifiées ou de l'adresse de bouclage (loopback) (celles commençant par 000), l'identifiant d'interface doit avoir une longueur de 64 bits. La taille de 64 bits permet d'approcher une probabilité de conflit quasi nulle.

Si initialement pour des raisons d'auto-configuration, l'identifiant d'interface devait nécessairement être dérivé de l'adresse de niveau 2 (adresse matérielle), c'est de moins en moins le cas. Il existe plusieurs méthodes pour construire cette valeur de 64 bits:

- manuelle;
- basée sur l'adresse de niveau 2 de l'interface;
- aléatoire;
- cryptographique.

Manuel

Pour les serveurs les plus utilisés, il est préférable d'assigner manuellement des adresses aux interfaces, car dans ce cas l'adresse IPv6 est facilement mémorisable, et le serveur peut être accessible même si le DNS n'est pas actif.

Nota: Le résolveur DNS est le cas le plus emblématique. Chaque machine sur le réseau doit

être configurée avec son client DNS pointant vers l'adresse du serveur DNS. Si celui ci a un identifiant d'interface basé sur l'adresse de niveau 2, en cas de changement de la carte réseau sur le serveur DNS, l'ensemble des machines du domaine devrait être reconfiguré. Si l'on ne souhaite pas utiliser de protocole de configuration automatique de tel DHCPv6, il est préférable d'attribuer au serveur DNS une valeur manuelle d'identifiant d'interface. Cette valeur statique sera stable dans le temps et pourra être utilisée pour référencer le resolveur DNS sur la configuration de l'ensemble des machines du réseau.

Il existe plusieurs techniques plus ou moins mnémotechniques

- incrémenter l'identifiant d'interface à chaque nouveau serveur créé

```
2001:db8:1234:1::1

2001:db8:1234:1::2
```

- reprendre le dernier octet de l'adresse IPv4 comme identifiant d'interface. Par exemple si un serveur a comme adresse IPv4 192.0.2.123, son adresse IPv6 pourra être:

```
2001:db8:1234:1::7B
```

ou plus simplement

```
2001:db8:1234:1::123
```

- reprendre l'adresse IPv4 comme identifiant d'interface, bien que cela ait l'inconvénient de conduire à des adresses plus longues à saisir:

```
2001:db8:1234:1::192.0.2.123
```

Dérivé de l'adresse matérielle de l'interface

L'avantage d'utiliser une adresse de niveau 2 pour construire un identifiant d'interface est que l'unicité de cette valeur est presque toujours assurée. En plus, cette valeur est stable tant que la carte réseau de la machine n'est pas changée. Par contre, ces valeurs sont difficilement mémorisables.

Les adresses lien-local sont, en général, construites en utilisant ce type d'identifiant. Par contre pour les adresses globales, il est conseillé de ne les utiliser que pour les machines clientes et de préférer les identifiants d'interface manuels pour les serveurs.

Ces identifiants d'interface étant stables dans le temps, à chaque fois qu'un individu change de réseau, il change de préfixe, mais garde le même identifiant d'interface. Ce dernier pourrait donc servir à tracer les déplacements d'un individu. Ce sujet de traçabilité et de respect de la vie privée a fait l'objet d'une prise de conscience collective suite à une actualité récente (affaire Snowden, surveillance de masse par les états, écoute de la NSA,...). Mais la traçabilité par l'identifiant d'interface, n'en est qu'un des éléments, car les cookies mis en place par les serveurs web ou les recoupements des infos personnelles déposées sur les réseau sociaux sont bien plus efficaces, mais ils ne s'agit plus d'un problème réseau. Autre désavantage,

comme les adresses MAC contiennent l'identification du matériel, il est possible d'indiquer à l'extérieur du réseau quel type de materiel est utilisé et donner des indications.

Si ces inconvénients sont jugés importants par l'entreprise, l'identifiant d'interface pour les adresses globales peut être généré aléatoirement.

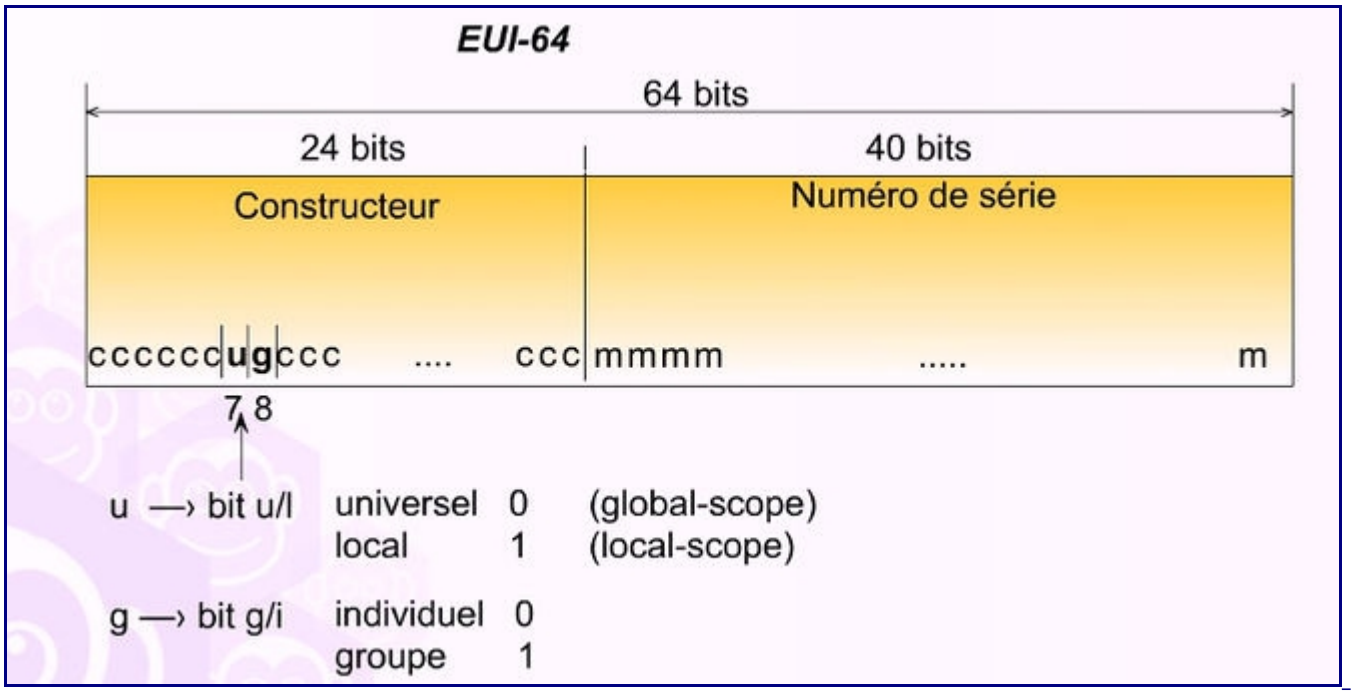
EUI-64

L'IEEE a défini un identificateur global à 64 bits (format EUI-64) pour les réseaux IEEE 1394 (firewire) ou IEEE 802.15.4 (réseau de capteurs) qui vise une utilisation dans le domaine de la domotique. L'IEEE décrit les règles qui permettent de passer d'un identifiant MAC codé sur 48 bits à un EUI-64.

Il existe plusieurs méthodes pour construire l'identifiant:

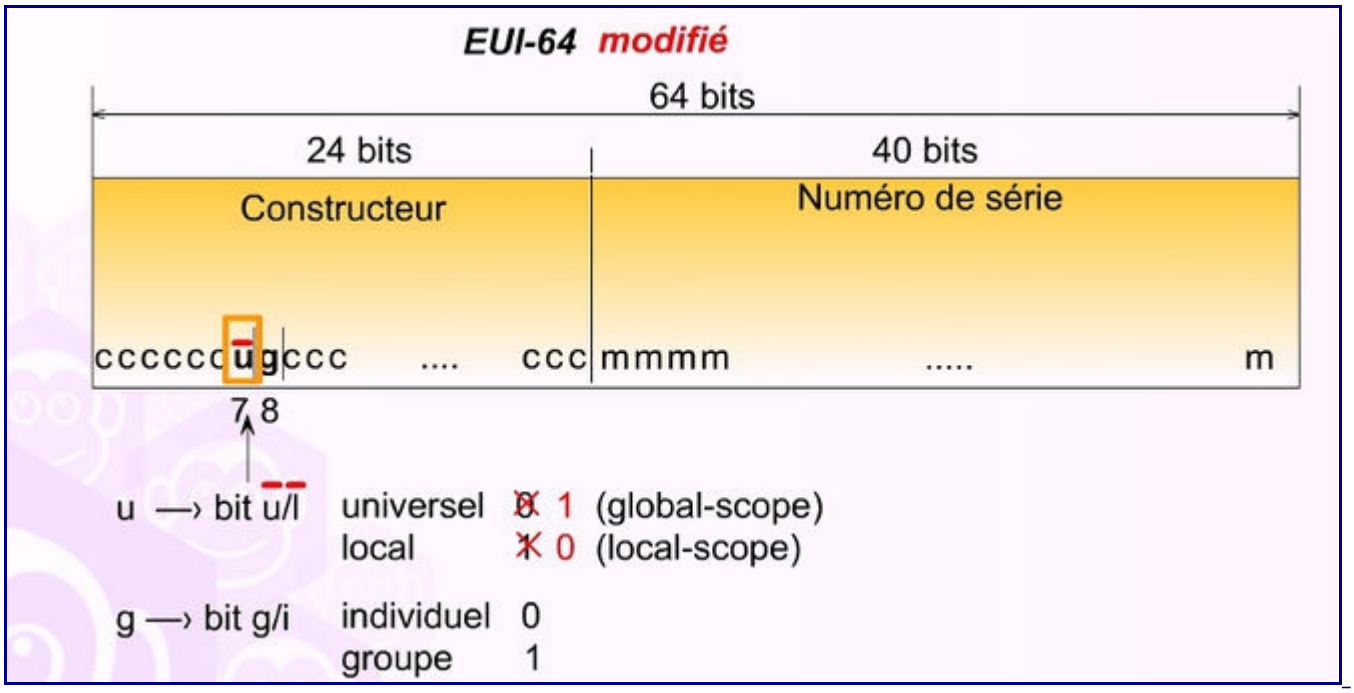
Si une machine ou une interface possède un identificateur global IEEE EUI-64, celui-ci a la structure suivante: Les 24 premiers bits de l'EUI-64, comme pour les adresses MAC IEEE 802.3, identifient le constructeur et les 40 autres bits identifient le numéro de série (les adresses MAC IEEE 802 n'en utilisaient que 24). Les 2 bits u (septième bit du premier octet) et g (huitième bit du premier octet) ont une signification spéciale:

- u (Universel) vaut 0 si l'identifiant EUI-64 est universel,
- g (Groupe) indique si l'adresse est individuelle (g = 0), c'est-à-dire désigne un seul équipement sur le réseau, ou de groupe (g = 1), par exemple une adresse de multicast.



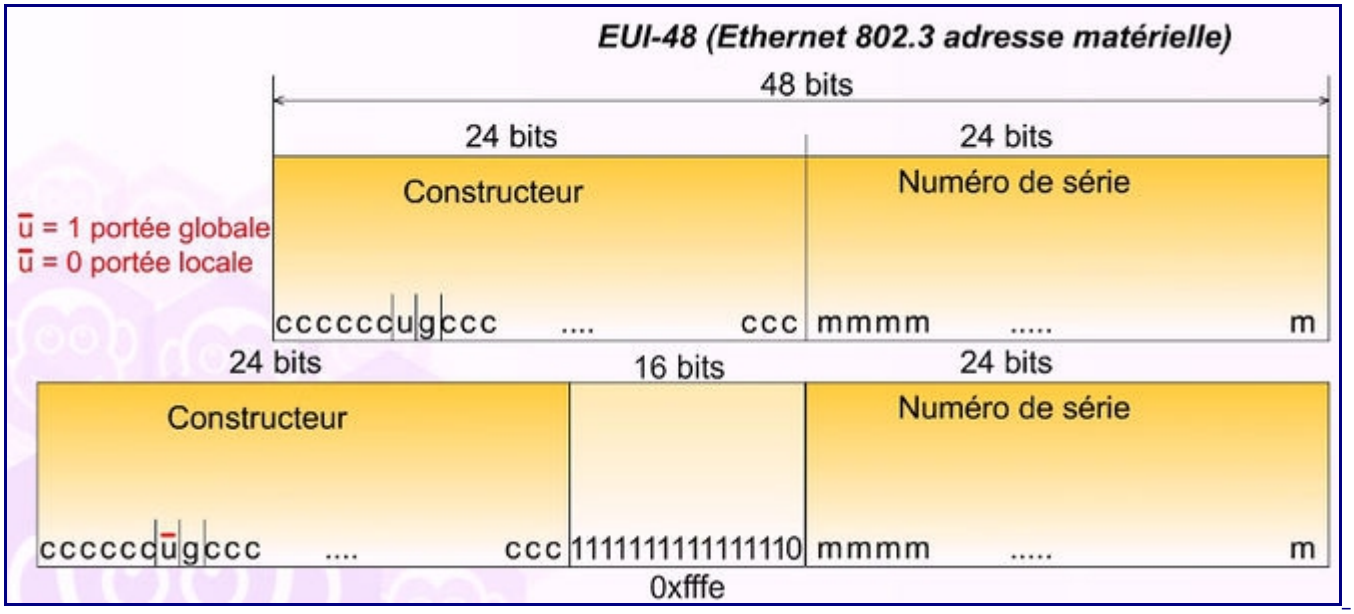
L'identifiant d'interface à 64 bits d'une adresse IPv6 est dérivé de l'EUI-64 en inversant le bit u . En effet, pour la construction des adresses IPv6, on a préféré utiliser 1 pour marquer l'unicité mondiale. Cette inversion de la sémantique du bit permet de garder la valeur 0 pour une numérotation manuelle, autorisant à numéroter simplement les interfaces locales à partir de

1.



MAC-48

Si une interface possède une adresse MAC IEEE 802 à 48 bits universelle (cas des interfaces Ethernet ou Wi-Fi). L'adresse est tout d'abord convertie en EUI-64, par l'insertion de 16 bits à la valeur 0xfffe, puis le bit u est mis à 1 comme dans le cas précédent. La figure ci-contre illustre ce processus.



Cas Particuliers

Si une interface ne possède aucune adresse (par exemple l'interface utilisée pour les liaisons PPP; Point to Point Protocol utilisé sur les liens point à point), et si la machine n'a pas

d'identifiant EUI-64, il n'y a pas de méthode unique pour créer un identifiant d'interface. La méthode conseillée est d'utiliser l'identifiant d'une autre interface si c'est possible (cas d'une autre interface qui a une adresse MAC), ou une configuration manuelle ou bien une génération aléatoire, avec le bit u positionné à 0. S'il y a conflit (les deux extrémités ont choisi la même valeur), il sera détecté lors de l'initialisation de l'adresse lien-local de l'interface, et devra être résolu manuellement.

Valeur aléatoire

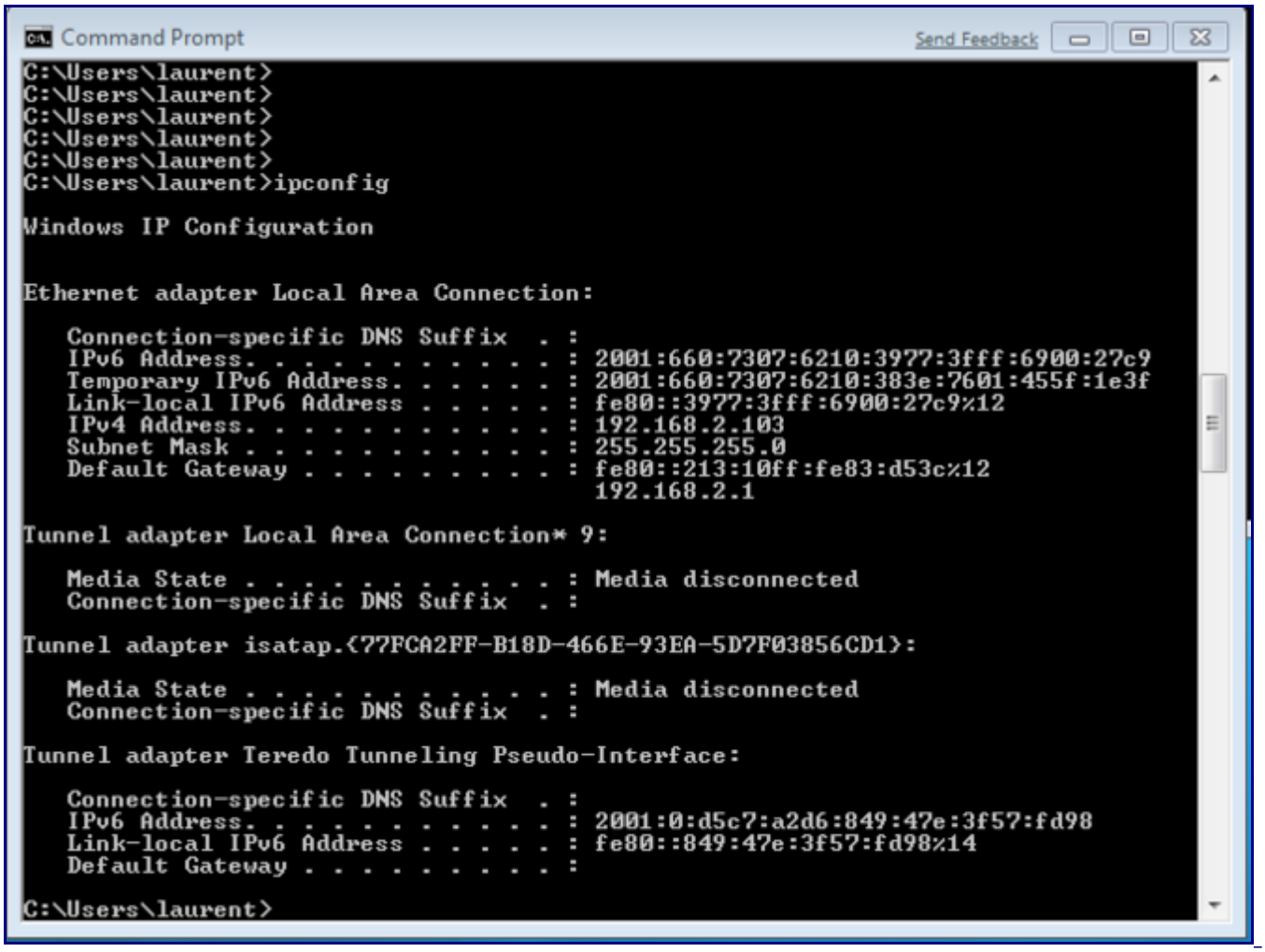
L'identifiant d'interface basé sur des adresses MAC, comme indiqué précédemment, pourrait poser des problèmes pour la vie privée. Il identifie fortement la machine d'un utilisateur, qui même s'il se déplace de réseau en réseau garde ce même identifiant. Il serait alors possible de traquer un individu mobile utilisant un portable, chez lui, au bureau, lors de ses déplacements.

Pour couper court à toute menace de boycott d'un protocole qui «menacerait la vie privée», il a été proposé d'autres algorithmes de construction d'un identifiant d'interface basé sur des tirages aléatoires (voir RFC 3041). Un utilisateur particulièrement méfiant pourrait valider ces mécanismes. L'identifiant d'interface est soit choisi aléatoirement, soit construit par un algorithme de hachage comme MD5 à partir des valeurs précédentes, soit tiré au hasard si l'équipement ne peut pas mémoriser d'information entre deux démarrages. Périodiquement l'adresse est mise dans l'état «déprécié» et un nouvel identifiant d'interface est choisi. Les connexions déjà établies continuent d'utiliser l'ancienne valeur tandis que les nouvelles connexions utilisent la nouvelle adresse.

Cette solution a été adoptée par Microsoft. Dans Windows XP, l'interface possède deux adresses IPv6 globale. La première a un identifiant d'interface dérivé de l'adresse MAC. Elle sert aux applications attendant des connexions sur la machine (i.e. les applications serveur). Cette adresse est stable et peut être publiée dans le DNS. La seconde possède un identifiant d'interface tiré aléatoirement. Elle est changée tous les jours ou à chaque redémarrage de la machine et sert aux applications client. Dans Windows 7, ce comportement est généralisé car l'identifiant d'interface de l'adresse permanente est également issu d'un tirage aléatoire. Cela permet d'éviter de donner la marque de la machine ou le type de carte contenue dans les premiers octets de l'identifiant d'interface. Elle est également présente, mais de manière optionnelle, sur Linux et les systèmes d'exploitation BSD ou Mac OS.

Bien entendu pour que ces mécanismes aient un sens, il faut que l'équipement ne s'enregistre pas sous un même nom dans un serveur DNS inverse ou que l'enregistrement de cookies dans un navigateur Web pour identifier l'utilisateur soit impossible.

En contre partie, il est plus difficile à un administrateur réseau de filtrer les machines puisque celles-ci changent périodiquement d'adresses.



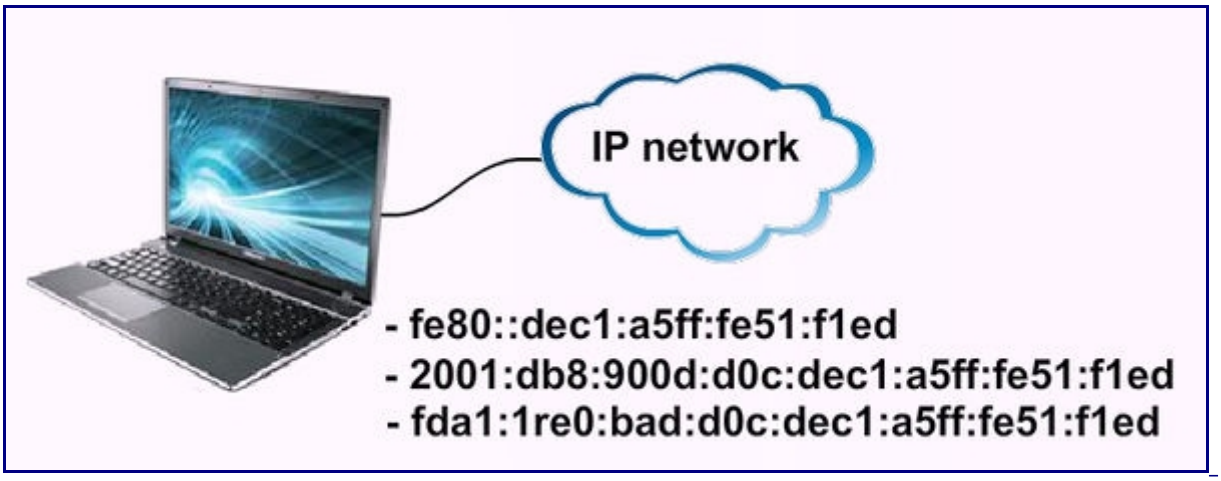
Cryptographique

Si un identifiant aléatoire permet de rendre beaucoup plus anonyme la source du paquet, des propositions sont faites à l'IETF pour lier l'identifiant d'interface à la clé publique de l'émetteur du paquet. Le RFC 3972 définit le principe de création de l'identifiant d'interface (CGA: Cryptographic Generated Addresses) à partir de la clé publique de la machine. Elles pourraient servir pour sécuriser les protocoles de découverte de voisins ou pour la gestion de la multi-domiciliation.

Adressage multiple des interfaces

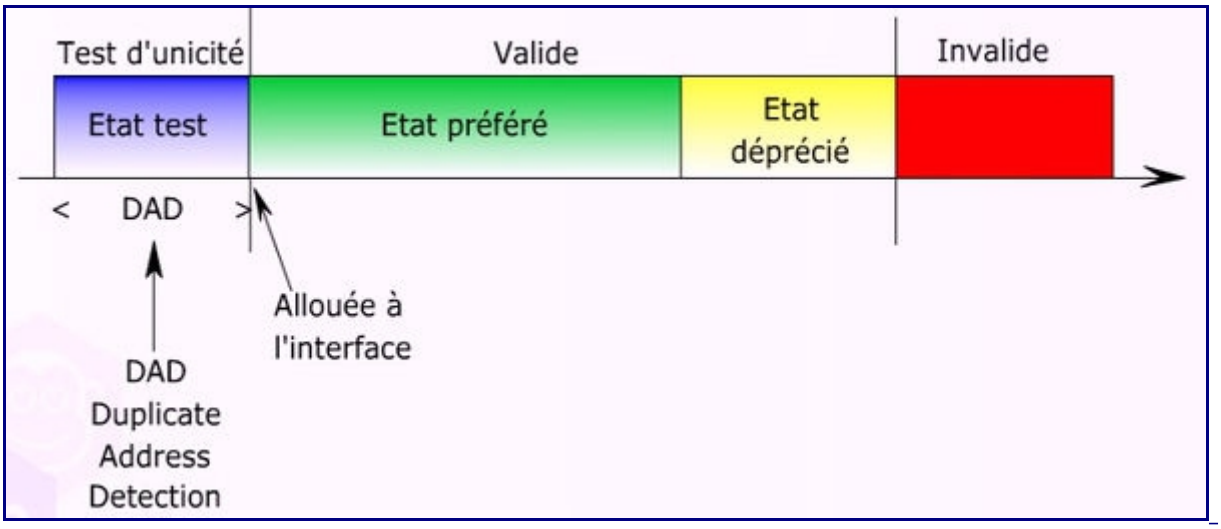
En IPv6 les interfaces des équipements disposent simultanément de plusieurs adresses. Ainsi, comme nous l'avons vu dans l'activité précédente, une interface dispose au moins d'une adresse purement locale sur son lien de rattachement (l'adresse lien local). Celle ci est automatiquement affectée à l'interface lors de la phase d'activation de cette dernière par le système. Selon la nature du lien de rattachement (liaison point à point, domaine de diffusion ethernet filaire ou wifi, ...) l'interface peut également disposer d'une (ou plusieurs) adresse(s) routable(s) soit localement (cas des adresses ULA) soit globalement (cas des adresses globales), en associant le préfixe d'adresse du lien support à l'identifiant d'interface.

L'affectation de ces adresses routables peut être assurée soit par l'administrateur système de la machine soit gérée automatiquement par le réseau en s'appuyant sur les mécanismes d'autoconfiguration avec ou sans état, comme nous le verrons dans un séquence ultérieure.



Gestion de la durée de validité de l'adresse

L'activité introductive de la séquence ("Quest ce qu'une adresse IP?") nous a présenté les différents états de validité d'une adresse (test, préféré, déprécié, invalide) qui régissent la durée de vie de l'adresse. Comme nous venons de le voir avec les adresses aléatoires respectueuses de la vie privée, certaines adresses sont temporaires et doivent être renouvelées périodiquement. C'est système d'exploitatation (OS) gérant l'interface qui assure la cohérence, notamment en passant une adresse dans l'état déprécié pour permettre la cloture des sessions et connexions existantes, parallèlement à la procédure d'activation d'une nouvelle adresse valide pour les nouvelles connexions ou sessions applicatives.



compléments récents à intégrer prochainement

- [RFC7136 Significance of IPv6 Interface Identifiers http://www.bortzmeyer.org/7136.html]

- [RFC7217 A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) http://www.bortzmeyer.org/7217.html]

Activité 15 : Les adresses multicast

Communications multicast

Les adresses multicast, également appelées adresses de groupe, permettent de communiquer avec un ensemble d'interfaces. Le datagramme émis avec une destination multicast sera écouté par toutes les interfaces appartenant au groupe. C'est une manière efficace de s'adresser à un ensemble de machines. Une communication multicast est une communication dans laquelle un même paquet de données peut être envoyé à un groupe de récepteurs, quelque soit leur localisation. Dans le modèle Internet IPv6, une station peut potentiellement émettre un paquet multicast vers n'importe quel groupe. Comparé aux communications point à point (unicast), le multicast évite la duplication des paquets de données au niveau de la source, et minimise l'utilisation de la bande passante au niveau du réseau. De plus, il offre un service insensible à l'augmentation du nombre et la localisation des membres d'un groupe. Le multicast peut être utilisé pour la distribution de logiciels, la téléconférence, les applications d'enseignement à distance, la radio ou la télévision sur Internet, les simulations interactives distribuées, les jeux multimédia interactifs, les applications militaires, etc.

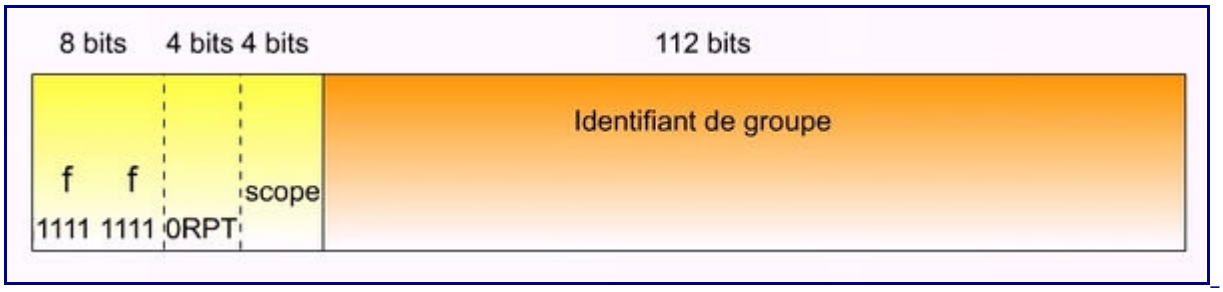
Pour le multicast, on distingue deux modèles de communication:

- le modèle ASM (Any-Source Multicast): dans le modèle ASM, un récepteur s'abonne à un groupe, et reçoit les données émises par n'importe quelle source pour ce groupe. Ce modèle s'applique par exemple dans le cas de visioconférences avec de nombreux participants qui ne sont pas connus à 'avance.
- le modèle SSM (Source-Specific Multicast): dans le modèle SSM, les sources sont connues à l'avance et les récepteurs s'abonnent à un groupe et un ensemble de sources. Ce modèle s'applique par exemple à la diffusion de la télévision ou radio sur Internet, où il n'y a qu'une seule source connue de tous.

Le fonctionnement détaillé des protocoles multicast dépassent le cadre de cette présentation. Cette séquence ne présente que le format des adresses IPv6 de ces protocoles.

Format des adresses multicast IPv6

Pour initier une session multicast, le groupe de récepteurs intéressés, appelé aussi groupe multicast, doit être formé. Un groupe multicast est identifié par une adresse IP multicast. Chaque adresse a une portée spécifique, qui limite la propagation du trafic multicast.



Les adresses multicast IPv6 sont dérivées du préfixe `ff00::/8` . Le champ drapeaux (flags) de 4 bits, qui suivent les 8 bits d'identification, est défini de la manière suivante:

- Seul le bit T (comme Transient) du champ drapeaux était initialement décrit dans le RFC 3513 . La valeur 0 indique une adresse multicast bien connue gérée par une autorité, en l'occurence l'IANA. La valeur 1 indique une valeur temporaire.
- Les bits P et R sont décrits dans le RFC 3306 et le draft Internet sur «embedded»-RP (RFC 3956).
- Le bit de poids fort du champ drapeaux n'est pas encore attribué.

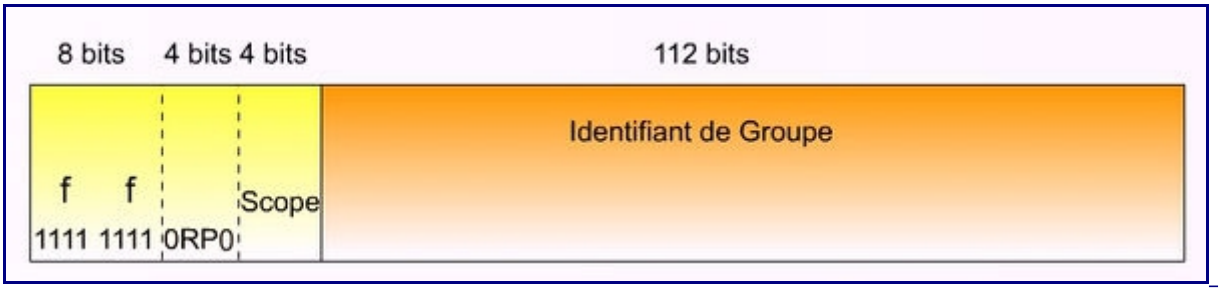
Le champ drapeaux permet de définir plusieurs types d'adresses multicast IPv6 qui seront décrits dans les sections suivantes.

Le champ étendue (scope) permet d'en limiter la portée (scope en anglais) de «diffusion» de l'adresse multicast IPv6. Cela permet de maîtriser le confinement des datagrammes dans une zone déterminée. Cette méthode est plus rigide mais plus sure que la classe D d'IPv4, où la portée est limitée uniquement par le champ durée de vie (TTL Time To Live). Les valeurs suivantes sont définies:

- 1 - node-local
- 2 - link-local
- 3 - subnet-local
- 4 - admin-local
- 5 - site-local
- 8 - organisation-local
- e - global
- Les portées 0 et F sont réservées.

Adresses multicast IPv6 permanentes

Une adresse multicast IPv6 avec le bit T du champ drapeaux à 0 correspond à une adresse multicast permanente, allouée par l'IANA.



Lorsque le multicast IPv6 sera déployé à grande échelle, certains organismes pourraient avoir des émissions permanentes. Des chaînes de télévision ou stations de radio pourront par exemple se voir attribuer des adresses permanentes par l'IANA dans le préfixe `ff00::/12` .

Le RFC 2375 définit déjà certaines adresses IPv6 multicast. Deux types d'adresses multicast permanentes sont à distinguer:

- des adresses correspondant à des services de niveau réseau (comme NTP, DHCPv6, cisco-rp-announce, SAP,...);
- des adresses correspondant davantage à des services applicatifs commerciaux permanents comme la distribution des chaînes de télévision.

Le RFC 3307 définit les procédures pour l'allocation des adresses multicast permanentes. Une adresse multicast permanente a un sens quelque soit son étendue (scope), son identifiant de groupe est réservé pour toutes les portées. Ainsi l'identifiant 0x101 réservé pour les serveurs NTP (Network Time Protocol).

Adresse de mutlicast	Population concernée
`ff01::101`	Tous les serveurs NTP de la même interface (c.à.d. Le même noeud) que l'émetteur;
`ff02::101`	Tous les serveurs NTP du même lien que l'émetteur;
`ff05::101`	Tous les serveurs NTP du même site que l'émetteur;
`ff0E::101`	Tous les serveurs NTP de l'Internet.

Cependant par précaution, certains identifiants mutlicast prédéfinis ne sont valables que sur un nombre limité de portées. Exemple les identifiants multicast raltifs au groupe des noeuds ou des routeurs sont limités aux portées lien-local ou site-local. D'autres, en général les services bien connus, tels que NTP cité ci dessus sont valides pour toutes les portées. Le document suivant http://www.iana.org/assignments/ipv6-multicast-addresses liste l'ensemble des valeurs réservées et les portées pour lesquelles elles peuvent s'appliquer.

- L'identifiant de groupe «tout à zéro» est réservé quelque soit la portée et ne doivent jamais être utilisé `ff0x:0:0:0:0:0:0:0` avec x variant de '0' à 'f'.
- Le groupe d'identifiants multicast à 1 concerne tous les nœuds, il est limité aux étendues (scope) interface-local et link-local. On ne peut donc pas diffuser sur l'ensemble des noeuds de l'Internet (sage précaution, sinon il aurait très facilement permis des attaques de type déni de service par bombardement massif en diffusion)

Adresse de mutlicast	Population concernée
`ff01::1`	Toutes les interfaces du noeud;
`ff02::1`	Toutes les noeuds sur le même lien que l'interface émettrice (correspond au broadcast 255.255.255.225 d'IPv4).

- Le groupe d'identifiants multicast à 2 concerne l'ensemble des routeurs, il est limité aux étendues (scope) interface-local, link-local et site-local. On ne peut donc pas diffuser sur l'ensemble des routeurs de l'Internet (sage précaution bis, pour limiter les attaques en déni de service).

Adresse de mutlicast	Population concernée
`ff01::2`	Tous les routeurs du noeud;
`ff02::2`	Tous les routeurs du lien;
`ff05::2`	Tous les routeurs du site.

L'IANA tient un registre des adresses multicast réservées. Il peut être consulté à cette URL: http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xthml

Adresses mutlicast IPv6 temporaires

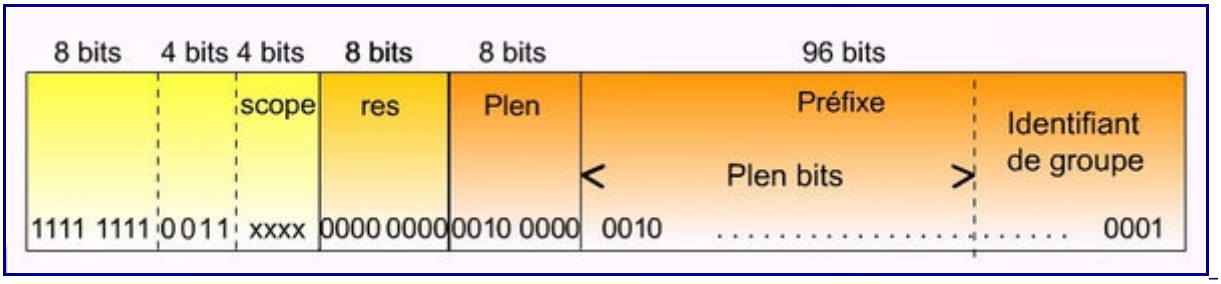
Les adresses multicast temporaires sont des adresses multicast IPv6 dont le bit T est positionné à 1. A l'inverse des adresse mutlicast permanentes, une adresse multicast temporaire n'a de signification que dans la portée donnée. Exemple l'adresse multicast site-local `ff15::999` sur un site n'a aucune relation avec un groupe utilisant la même adresse multicast sur un autre site. Il existe plusieurs types d'adresses temporaires: générales, dérivée d'un préfixe unicast IPv6 et par point de rendez-cous (Embedded-RP)

Adresses multicast temporaires générales

Ce sont des adresses avec tous les bits du champ "flags" à 0 sauf le bit T positionné à 1. Il n'y a pas de recommandations pour l'utilisation de ces adresses. Des scénarios d'utilisation peuvent être, par exemple, les visioconférences ponctuelles.

Addresses multicast temporaires dérivées d'un préfixe unicast IPv6

Le RFC 3306 définit une méthode pour dériver une adresse multicast IPv6 à partir d'un préfixe unicast.



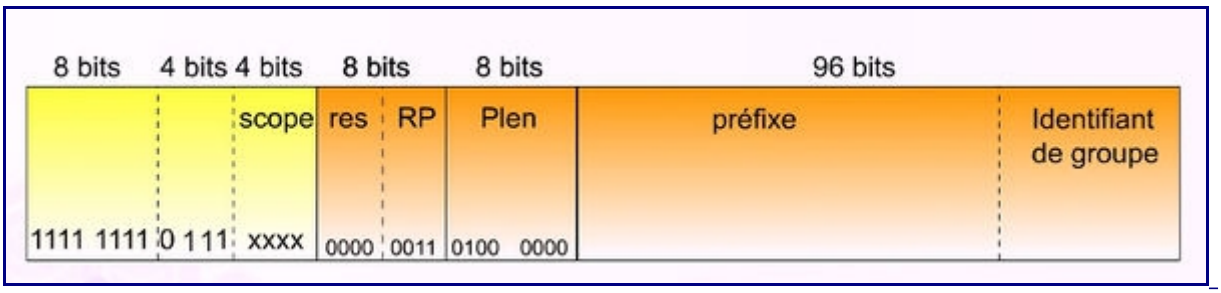
- `res` (*reserved*): tous les bits de ce champ doivent être positionnés à `0` .
- `Plen` (*prefix length*): ce champ contient la longueur du préfixe unicast utilisé pour en dériver une adresse multicast.

- `prefix` : ce champ contient la valeur du préfixe du réseau utilisé pour en dériver une adresse multicast.
- `group-ID` : ce champ de 32 bits contient l'identifiant de groupe.

Par exemple, une adresse multicast peut être dérivée à partir du préfixe de RENATER (`2001:660::/32`). Le champ prefix prend la valeur `2001:0660` et le champ Plen, la valeur `0x20` (32 en décimal). Les adresses multicast IPv6 à choisir seront de type `ff3x:20:2001:660::aabb:ccdd` (`aabb:ccdd` étant le group-ID choisi dans l'exemple et 'x' une des valeurs valides de la portée (scope)). Cette méthode permet la création potentielle de 2 puissance 32 adresses multicat par préfixe.

Adresses multicast «Embedded-RP»

Le RFC 3956 définit une méthode pour inclure l'adresse du RP (Point de Rendez-Vous servant à la construction de l'arbre multicast) dans l'adresse multicast IPv6. Le schéma Structure d'une adresss IPv6 Multicast embedded RP montre la structure d'une telle adresse, aussi appelée adresse embedded-RP.



Ainsi pour un point de rendez-vous qui possède l'adresse `2001:660:3307:125::3` , une adresse multicast correspondante peut être dérivée de la façon suivante:

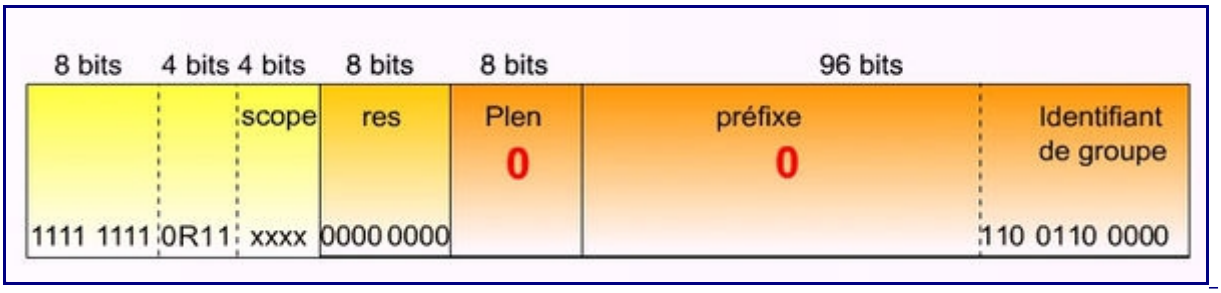
- `res` (Reservé): Les 4 bits de ce champ sont positionnés à 0.
- `RPad` : Ce champ contient les 4 derniers bits de l'adresse du RP. Dans cet exemple, RPad prend la valeur 3.
- `Plen` (Longueur du préfixe): Ce champ contient la longueur du préfixe réseau du RP à prendre en compte. Dans cet exemple, la valeur est de `0x40` (soit 64 en décimal),
- `prefix` (Préfixe) : Ce champ contient le préfixe réseau du RP. Ici, cette valeur est 2001:660:3007:125
- `group-ID` : ce champ de 32 bits contient l'identifiant de groupe, détaillé au chapitre Identifiant de groupe.

Une adresse multicast dérivée de ce point de rendez-vous sera donc de la forme ff `7x:340:2001:660:3007:125:aabb:ccdd` (`aabb:ccdd` étant le group-ID choisi dans cet exemple et 'x' une des valeurs valides de la portée (scope)).

Les adresses multicast SSM

Les adresses SSM (Source Specific Multicast) sont décrites également dans le RFC 3306 . Si le préfixe `ff3x::/32` a été réservé pour les adresses multicast SSM, seules les adresses

dérivées du préfixe `ff3x::/96` doivent être utilisées dans un premier temps. Ce sont des adresses multicast basées sur le préfixe unicast où les champs Plen et prefix sont positionnés à 0.



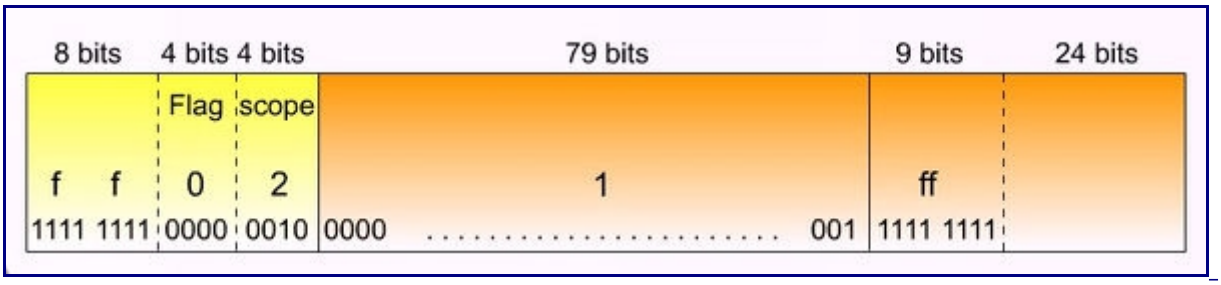
Les adresses multicast sollicité

L'adresse de multicast sollicité (Solicited-node address) est un type d'adresse multicast prédéfinie. IPv6 interdit l'utilisation de la diffusion généralisée (Broadcast) lorsque le multicast est disponible. Ainsi les protocoles de découverte de voisins (Neighbor Discovery), chargé de faire la correspondance entre les adresses IPv6 et les adresses MAC (à l'instar d'ARP en IPv4) doivent utiliser une adresse multicast. Pour être plus efficace, au lieu d'utiliser l'adresse `ff02::1` (tous les équipements sur le lien), l'utilisation des adresses de multicast sollicité permet de réduire considérablement le nombre d'équipements qui recevront la requête de découverte de voisin.

L'adresse de multicast sollicté se construit automatiquement à partir d'une adresse IPv6 unicast (ou anycast) en concaténant le préfixe réservé `ff02::1:ff00:0 /104` au 24 bits de poids faible de l'adresse unicast ou anycast.

Un équipement, à partir de chacune de ses adresses IPv6 (unicat et anycast) construit une adresse de multicast sollicité et écoute les paquets émis vers cette adresse. Les autres stations sur le même lien (ou domaine de diffusion de niveau 2: VLAN) connaissant son adresse IPv6 mais ignorant son adresse MAC peuvent utiliser l'adresse de multicast sollicité pour le joindre. Ces adresses sont utilisées par les protocoles de détection d'adresse dupliquée et de découverte de voisins, qui seront abordés ultérieurement.

Plusieurs équipements sur le lien peuvent avoir la même adresse de multicast sollicité. Mais dans la pratique la probabilité de trouver sur le même lien physique deux équipements avec les trois derniers octets de l'identifiant d'interface identiques est très faible. Cela permet donc de limiter le nombre d'équipements qui traiteront la requête de sollicitation de voisins. Ces adresses permettent de ne plus utiliser la diffusion généralisée (adresse MAC ff:ff:ff:ff:ff:ff) qu'utilise le protocole ARP en IPv4. Pour une station donnée une adresse de multicast sollicité peut regrouper plusieurs adresses IPv6 par exemple l'adresse lien local et l'adresse unicast globale si cette dernière est construite à partir de l'identifiant d'interface dérivé de l'adresse MAC de la carte Ethernet.



correspondance avec les adresses de multicast de niveau 2

Le RFC 3307 précise également la correspondance entre les adresses IPv6 multicast et les adresses de niveau 2. Sur un réseau de niveau 2 ethernet, l'adresse MAC de mutlicast est déduite de l'adresse multicast IPv6 en concatenant les 32 derniers bits (4 octets) de l'adresse multicast IPv6 au préfixe MAC préfédini 33-33.

Par exemple, à l'adresse multicast IPv6 `ff0e:30:2001:660:3001:4002:ae45:2C56` correspondra à l'adresse MAC `33-33-AE-45-2C-56` . La probabilité que deux adresses multicast IPv6 utilisées sur un même lien correspondent à la même adresse MAC existe mais est très faible et les conséquences minimes. Restreindre le champ group-ID à 32 bits a toutefois un intérêt car cela apporte une homogénéité entre les différents types d'adresses décrits précédemment. En effet, dans le cas des adresses dérivées d'un préfixe unicast, ce champ a une longueur de 32 bits.

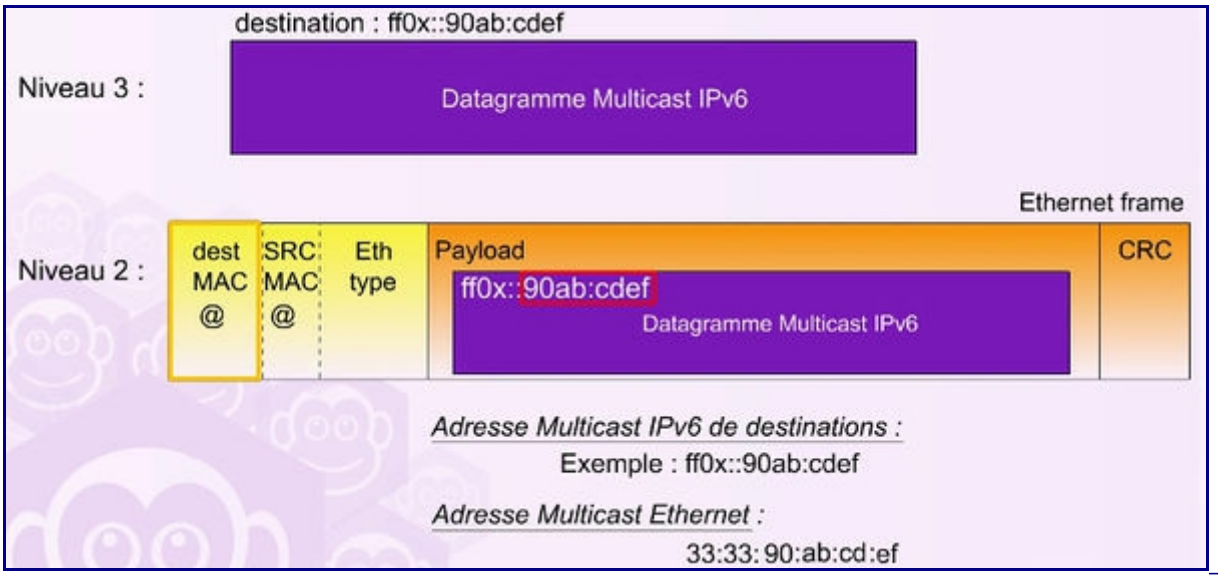


Tableau Récapitulatif des types d'adresses multicast

Le tableau suivant récapitule les préfixes associés aux différents types d'adresses multicast décrit précédement.

Préfixe	Usage
`ff0 x ::/16`	Adresses IPv6 multicast permanentes;
`ff1 x ::/16`	Adresses IPv6 multicast temporaires générales;

ff3 **x** ::/16	Adresses multicast dérivées d'un préfixe unicast (temporaires);
ff3 **x** ::/96	Adresses SSM (temporaires);
ff7 **x** ::/16	Adresses IPv6 multicast Embedded-RP (temporaires);
ff02::1:ff00:0/104	Adresses de multicast sollicité (préfixe prédéfini, portée limitée au lien).

(**x** une des valeurs valides de la portée (scope))